Introduction to SharePoint and OneDrive in Microsoft 365 for administrators

SharePoint and OneDrive in Microsoft 365 are cloud-based services that help organizations share and manage content, knowledge, and applications to:

- Empower teamwork
- Quickly find information
- Seamlessly collaborate across the organization

The resources on this page are designed to get you started. Depending on the needs of your organization, you may want to read about migration and governance options before you start rolling SharePoint and OneDrive out to your users.

If you're ready to get started with SharePoint and OneDrive, read Plan for SharePoint and OneDrive in Microsoft 365 and follow the planning and rollout articles that are listed in that article.

If you're just starting out with SharePoint and OneDrive, learn about the FastTrack onboarding and adoption services, find a SharePoint certified partner, or visit the SharePoint community.

Once you're using SharePoint and OneDrive, get the OneDrive sync app and the mobile app.

Migration

If you have files that you need to move to SharePoint and OneDrive, the resources in this section can help you get started.

Expand table

If you're looking for this information:	Go to this resource:
Learn how to include migration as part of your plan to roll out SharePoint and OneDrive	Migration planning for SharePoint and OneDrive rollout
How to migrate content from file shares or other cloud providers using Migration Manager	Migrate your content to Microsoft 365
How to migrate SharePoint Server sites and content	Overview of the SharePoint Migration Tool (SPMT)

Governance

If your organization has legal or other requirements that govern the handling of data, or if you have sensitive or confidential information that you want to protect, these references can help you configure SharePoint for your governance standards and policies.

Expand table

If you're looking for this information:	Go to this resource:
How to plan your compliance requirements for SharePoint and OneDrive	Plan compliance requirements for SharePoint and OneDrive
How to ensure that you retain files for a specified period of time, or delete them on a specified schedule	Overview of retention policies OneDrive retention and deletion
How to classify documents based on the sensitivity of the information	Overview of sensitivity labels Enable sensitivity labels for Office files in SharePoint and OneDrive
How to prevent the loss or exfiltration of important data in documents emails	Learn data loss prevention
Search for in-place items such as email, documents, and instant messaging conversations	Content Search in Microsoft 365

If you use OneDrive in your organization and you want to protect important files by saving them to the cloud, govern how much storage space users get, or govern how users sync file, these references will help you configure your policies.

Expand table

If you're looking for this information:	Go to this resource:
Protect important files on users' desktops or in their Documents folder	Redirect and move Windows known folders to OneDrive and Redirect and move macOS Desktop and Documents folders to OneDrive
Control how users sync files to their devices	Use Group Policy to control OneDrive sync settings and Deploy and configure the OneDrive sync app for Mac
Configure the amount of storage space users have in OneDrive	Set the default storage space for OneDrive users

Microsoft Teams

SharePoint is deeply integrated into Teams. Files that are stored in Teams are stored in SharePoint sites. When you administer SharePoint sites in the SharePoint admin center, you may find that many of them are connected to teams. Use these resources to understand how SharePoint and Teams are integrated.

Expand table

If you're looking for this information:	Go to this resource:
Learn about how Teams and SharePoint work together	Overview of Teams and SharePoint integration
Learn how to manage settings and permissions when Teams and SharePoint are integrated together	Manage settings and permissions when SharePoint and Teams are integrated

Collaboration

SharePoint and OneDrive provide a rich collaboration environment where people inside and outside your organization can work together, coauthoring documents. Microsoft 365 provides a variety of options to help you create a secure and productive file collaboration environment that meets the needs of your organization. Use these resources to get started.

Expand table

If you're looking for this information:	Go to this resource:
Learn about secure collaboration in Microsoft 365	Set up secure collaboration with Microsoft 365
Learn about file collaboration and how to plan your implementation	Intro to file collaboration in Microsoft 365 File collaboration in SharePoint with Microsoft 365
Learn about collaborating with people outside your organization	External sharing overview Collaborate with guests
Use the security and compliance features in Microsoft 365 to help secure your guest sharing environment	Create a secure guest sharing environment

Modern intranet

SharePoint provides a rich set of tools to help you create and maintain your organization's intranet. Use these resources to get started.

Expand table

If you're looking for this information:	Go to this resource:
Learn about the different types of SharePoint sites	Plan your SharePoint site
Select whether to allow users to create their own sites	Manage site creation
Learn how to plan an intelligent intranet for your organization	Plan an intelligent SharePoint intranet Planning your SharePoint hub sites

Training

Administrators are often called upon to teach others in the organization how to use new technologies. Use these resources to help your users be successful with SharePoint and OneDrive.

Expand table

If you're looking for this information:	Go to this resource:
Get a list of training resources for your users	Training and change management for rolling out SharePoint and OneDrive
Set up a customizable training portal with Microsoft training content for your organization	Microsoft 365 learning pathways
Show your users the basics of SharePoint	SharePoint help & learning
Show your users the basics of OneDrive	OneDrive help & learning

Customization

SharePoint provides a wide range of options for customization. We recommend using the out-of-box features and functionality as much as possible to meet your organization's needs. If you do need to customize SharePoint, see these references.

Expand table

If you're looking for this information:	Go to this resource:
Understand how to customize SharePoint using modern tools and techniques	Customizing SharePoint
Build SharePoint Framework solutions, apps, add-ins, and solutions	SharePoint development

Related topics

SharePoint Limits

Getting started with the SharePoint Online Management Shell

Microsoft Partner Center

Tips and tricks for navigating Microsoft 365 technical documentation

---

Last updated on 04/17/2025

Intro to file collaboration in Microsoft 365, powered by SharePoint

Article • 05/13/2025

Are you getting the most out of file collaboration in Microsoft 365, or are your users still storing files locally or on network file shares and sending them around in email? Maybe you're paying for another cloud storage service and not taking advantage of the space you get with your Microsoft 365 subscription. This article describes the benefits and key features of file collaboration in Microsoft 365. It also covers the steps to plan for and adopt Microsoft 365 file collaboration in your organization.

The file collaboration capabilities in Microsoft 365 are available to you whatever the size of your organization. If you have a small organization, each user can store their files in their individual library in OneDrive and you might want only a single team in Microsoft Teams for everyone in the organization.

Why use Microsoft 365 cloud file storage?

By taking full advantage of SharePoint-powered file storage in Microsoft 365, you can avoid purchasing cloud storage from other providers and enjoy:

Anywhere access to files

Enterprise-grade security

Secure sharing outside the organization

Real-time collaboration and file versioning

Intelligence that helps users discover files

Anywhere access

When users keep files on their local device or on a network share, they're out of luck when they don't have the device with them or don't have a connection to your network. If something happens to a user's device, the data might not be recoverable. If a user's device is upgraded, local data must be migrated. By storing files in the cloud, users can access them from all their devices, such as their phone and their home computer (depending on what you allow). They can even access files in a browser from other devices they trust. For example, if two colleagues

travel to a customer site and one of their two laptops runs out of battery, they can both access all their files by signing in to portal.office.com on the other laptop. Get the SharePoint mobile app.

> **Note**
>
> If you're concerned about users signing in from kiosks or other shared, unmanaged devices, you might want to enable idle session sign-out.

Enterprise-grade security

Files stored in SharePoint and OneDrive in Microsoft 365 are encrypted in transit and in rest. (You can encrypt files by using your own key if you want.) Files are also scanned for viruses. As an admin, you can use tools in Microsoft 365 to further secure and monitor files:

- **Microsoft Purview Data loss prevention policies**. Warn or prevent users from sharing files that have specific labels outside the organization. See Learn about data loss prevention
- **Retention labels**. Classify files to be retained, permanently deleted, or marked as a record. See Overview of retention labels
- **Sensitivity labels**. Classify and protect highly confidential files with encryption and permissions. See Learn about sensitivity labels
- **Reports**. Monitor activity and usage in SharePoint and OneDrive. See Which activity reports are available in the admin center
- **Microsoft 365 Advanced Threat Protection (ATP)**. Protect against malicious files.
- **Files Restore**. If a location is affected by malicious software, or someone deletes important files, you can restore a document library to an earlier point in time.

Plan for these features

Secure sharing outside the organization

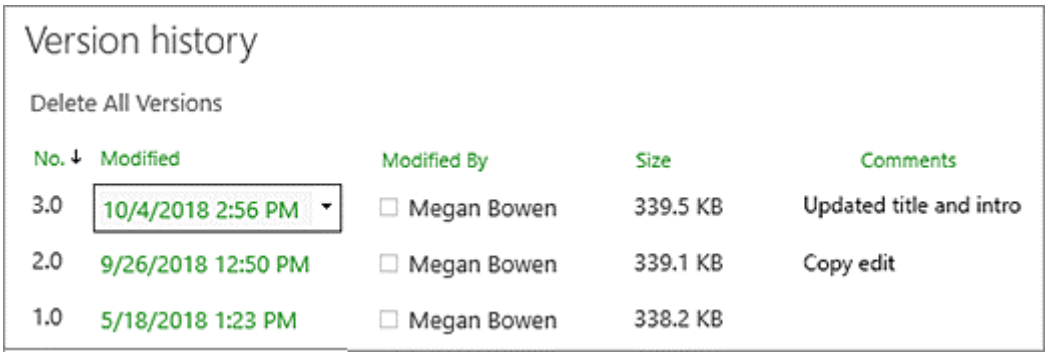
SharePoint powers secure file sharing in Microsoft 365. You can specify if you want people outside the organization to be able to access files without authenticating (signing in or providing a verification code). You can even block external sharing altogether. We recommend using the most permissive sharing option that you can for each set of content. If you heavily

restrict sharing and it blocks user productivity, users will typically find other ways to collaborate that provide you less oversight and control. For more info, see Control sharing.

Real-time collaboration and version management

When users store Office files in Microsoft 365, they can avoid the hassle of managing changes in different copies of files. Instead, they can collaborate on a single version by using either the desktop apps or the web versions of Office. People don't even need to have the Office desktop apps installed to edit Office files. Learn more about document collaboration and coauthoring. When multiple users edit an Office file at the same time, a notification will show them that other people are working in the file and they can see where in the file others are working.

Version history is also on by default, so users can view earlier changes and roll back as necessary. Learn more about working with version history.



Intelligence that helps users discover files

When users in the organization regularly store files in Microsoft 365, they can quickly find recent files and other files that might be of interest. For example, they can discover files that coworkers or frequent collaborators are working on.

Key features

Most of the file collaboration features in Microsoft 365 are available to you regardless of your subscription type or the size of your organization.

- Migration tools
- Modern attachments
- Access to all files in OneDrive
- Syncing for offline access
- Integration with Microsoft Office
- Private and shared channels in Teams
- Auditing and reporting
- Hybrid
- Multi-geo

A hub for teamwork: Microsoft Teams

In the past, users would have to frequently switch between tools to collaborate. For example, users would write a document in Word. Then they would switch to Outlook to share the document as an attachment. Or they would open a browser to upload the document to a SharePoint site. In Microsoft 365, users can use Teams to chat, make calls, and have online meetings. They don't have to leave Teams to view or even edit the files they share. Learn more about file collaboration in Teams.

> **Note**
>
> When a user attaches a file to a chat, it's automatically uploaded to the user's OneDrive. When a user attaches a file to a Teams channel, it's automatically uploaded to the SharePoint library for that team. Files shared with Viva Engage groups are also saved in SharePoint.

Access to all files in OneDrive

When your users use OneDrive, they can access their SharePoint or Microsoft Teams files on the web or in the mobile app without leaving OneDrive.

Because individual libraries in OneDrive are powered by SharePoint, users can easily move files between locations. For example, if a user drafts a file in their individual library in OneDrive, and later wants a team to own the file, the user can simply move the file to the team's library.

Sync for offline access

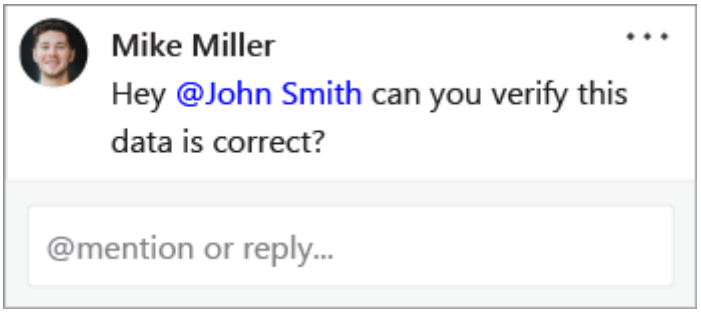
With the OneDrive sync app, users can sync files between their computer and Microsoft 365. When users add, change, or delete a file or folder locally, the file or folder is added, changed, or deleted in Microsoft 365 and vice versa. Users can work with synced files directly in File Explorer and the apps they use. Whenever the user is online, any changes that they or other users make will sync automatically. With Files On-Demand, users can easily browse and organize files in OneDrive and SharePoint by using File Explorer or Finder, but the files don't take up space on the local computer. Learn more about Files On-Demand.

Modern attachments in Outlook

If your users are used to sharing files as attachments in Outlook, they can use the same steps they're familiar with to share a link to a file instead of emailing a copy. Within Outlook, users can even change the permission they give to the recipient. Learn more about attaching files.

Integrate with Microsoft Office

In the Office apps, users can easily open files saved in Microsoft 365 and save documents to OneDrive. Learn more about working together on Office documents. When users comment on an Office document and use the @ sign with someone's name, the person mentioned receives mail with a link to the comment. Clicking the link brings them into the document and into the conversation.



Private and shared channels in Teams

Teams has workspaces for chat and file collaboration called channels. While standard channels include everyone in the team, private channels allow you to collaborate with a subset of team members and shared channels allow you to collaborate with people outside the team. All

channel types allow you to collaborate with people outside your organization. Each private and shared channel has its own SharePoint site for file storage and collaboration.

Migration tools

You can choose one or more of the following options, depending on the number and location of files that you want to migrate.

- **Migration Manager**. Copy file shares or content from other cloud providers to Microsoft 365. Learn more about migrating content to Microsoft 365.
- **SharePoint Migration Tool**. To migrate SharePoint Server sites and content, you can use the SharePoint Migration Tool. For info, see Overview of the SharePoint Migration Tool.
- **Known Folder Move**. If your users save most of their files to their Desktop, Documents, and Pictures folders, you can seamlessly move them to OneDrive using Known Folder Move so users can continue working in the locations they're used to.
- **FastTrack migration benefit**. FastTrack provides you with a set of best practices, tools, resources, and experts. Guidance includes migrating content from file shares, Box, or Google Drive source environments, and introducing capabilities at the pace that works for you. The FastTrack data migration benefit will also perform specific data migration activities on your behalf if you have 500 or more licenses. See more details in the FastTrack Center Benefit Overview. To get started, go to FastTrack.Microsoft.Com, review resources, and submit a request for assistance.

Multi-geo

If you're a multinational organization with data residency requirements, you can use Multi-Geo in Microsoft 365 to specify where files are stored. For info, see Multi-Geo Capabilities in OneDrive and SharePoint in Microsoft 365.

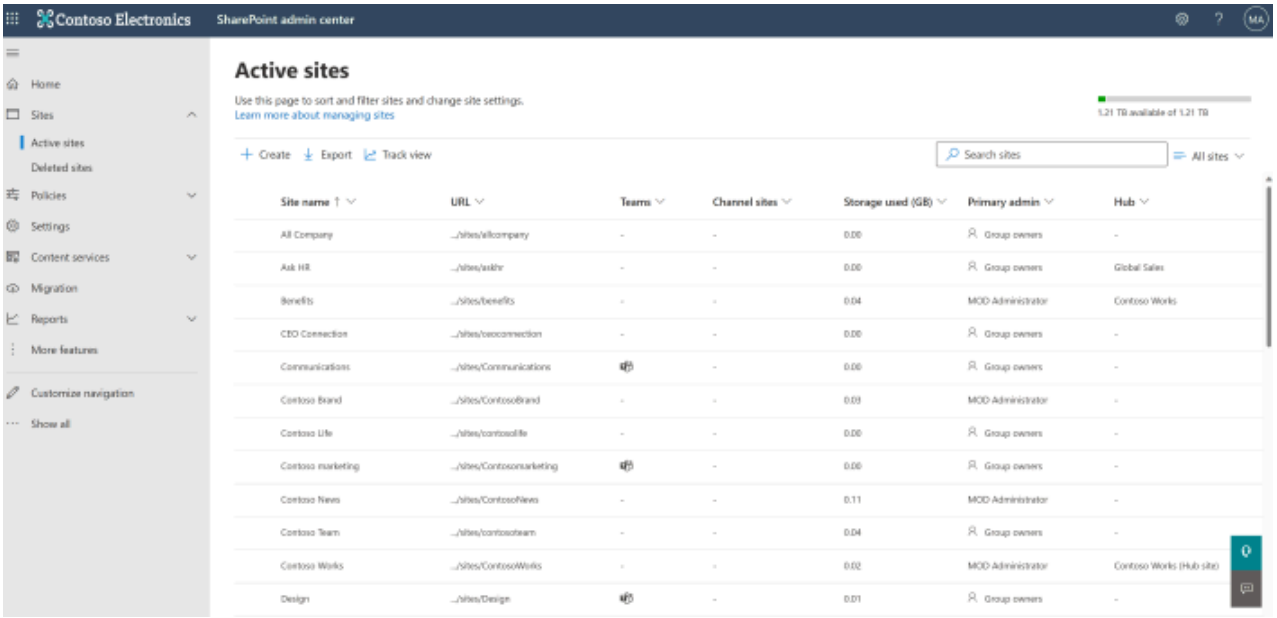
Unified search

Microsoft Search helps users find files within modern SharePoint sites and from the SharePoint start page, Office.com, Bing, and more. Learn more about the modern search experience in SharePoint.

Management options

As a SharePoint Administrator and above for your organization, you have a couple of options for managing SharePoint sites and settings:

- **SharePoint admin center**. In the SharePoint admin center, you can create and delete sites, manage site settings, and manage organization-level settings for SharePoint and OneDrive. The **Active sites** page of the SharePoint admin center lets you view the SharePoint sites in your organization, including communication sites, Teams private and shared channel sites, and sites that belong to Microsoft 365 Groups. It also lets you sort and filter sites, search for a site, and create new sites.



- **Microsoft PowerShell**. The SharePoint Online Management Shell is a PowerShell module that lets you run command-line operations. It makes performing batch operations more efficient, and is the only way to perform some management tasks in SharePoint and OneDrive. Get started with the SharePoint Online Management Shell.

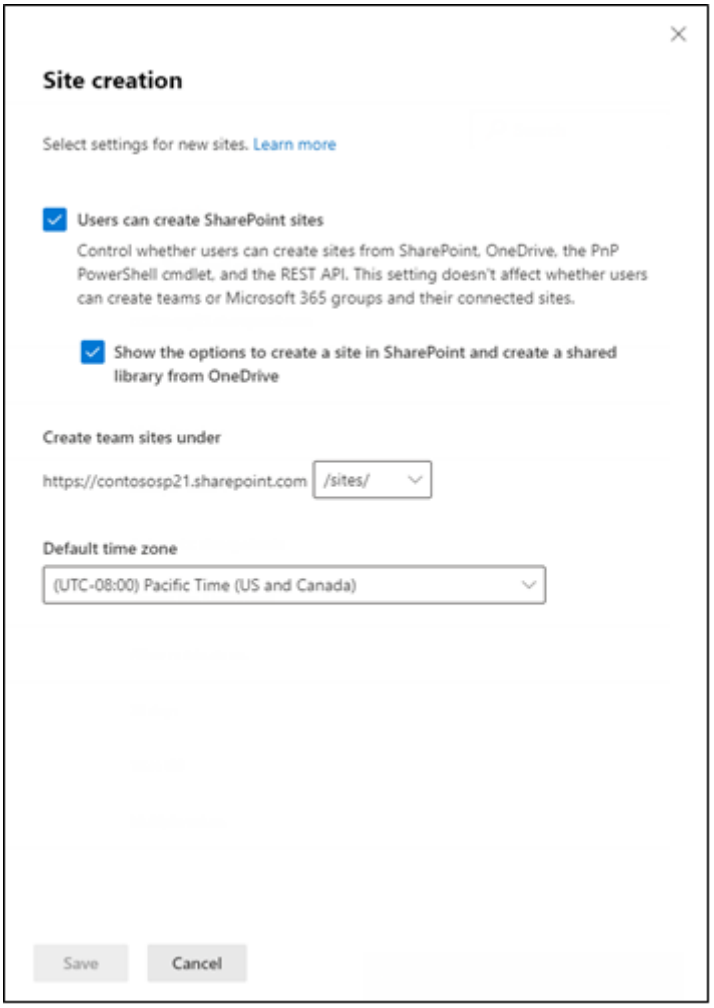
Configure settings

To prepare for file collaboration in Microsoft 365, configure the following settings.

Create sites

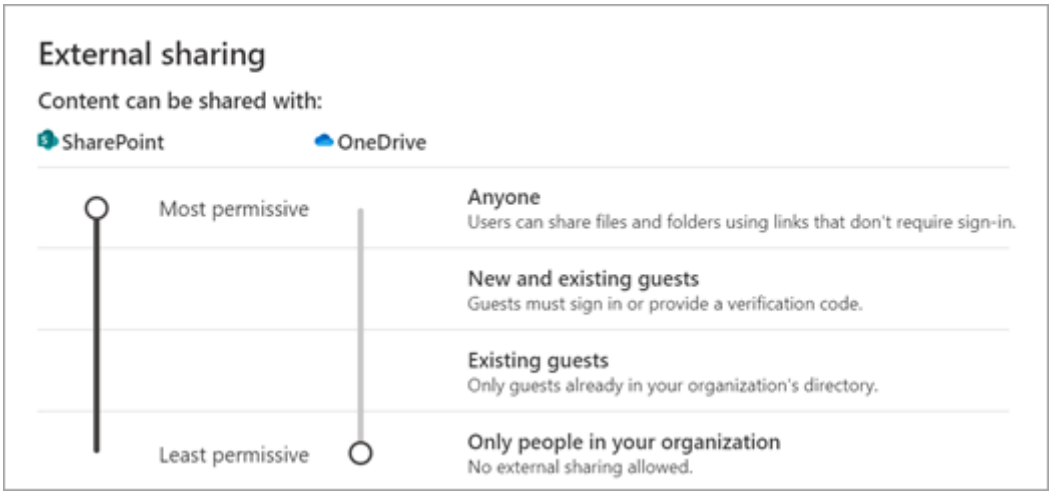
When a Microsoft 365 group is created from anywhere within Microsoft 365, a SharePoint site is automatically created. You can let all users create groups, only some users, or you can block group creation and manage it centrally in your IT department. For info, see Manage who can create Office groups. You can also use a naming policy for groups and set an expiration period so that groups that are no longer being used will be deleted. For more info, see Plan for governance in Microsoft 365 Groups. If you allow users to create groups, you can also allow

them to create team sites from the SharePoint start page and from OneDrive and manage default site settings. For info, see Manage site creation.



Sharing

To set up external sharing in your organization, you need to make sure that settings across multiple admin centers are set the way you want. Sharing with people outside your organization is enabled by default in SharePoint, OneDrive, and Teams. See Collaborate with guests in a team and Collaborate with external participants in a channel for information about configuring sharing settings.



Storage

By default, file storage for team sites is managed automatically. If you prefer to control storage manually, see Manage site storage limits. For info about setting the default storage space for individual libraries in OneDrive, see Set the default storage space for OneDrive users. For information about the amount of storage that comes with your plan, see SharePoint limits.

Specify team site libraries to sync automatically

To let users easily access team site files from File Explorer (as they might have previously accessed network file shares), you can specify particular team site libraries to sync on your users' computers automatically. To do this, use the OneDrive Group Policy object "Configure team site libraries to sync automatically."

Related topics

- Invalid file names and file types
- SharePoint help & learning (for end users)

Overview of OneDrive in Microsoft 365

Article • 03/27/2025

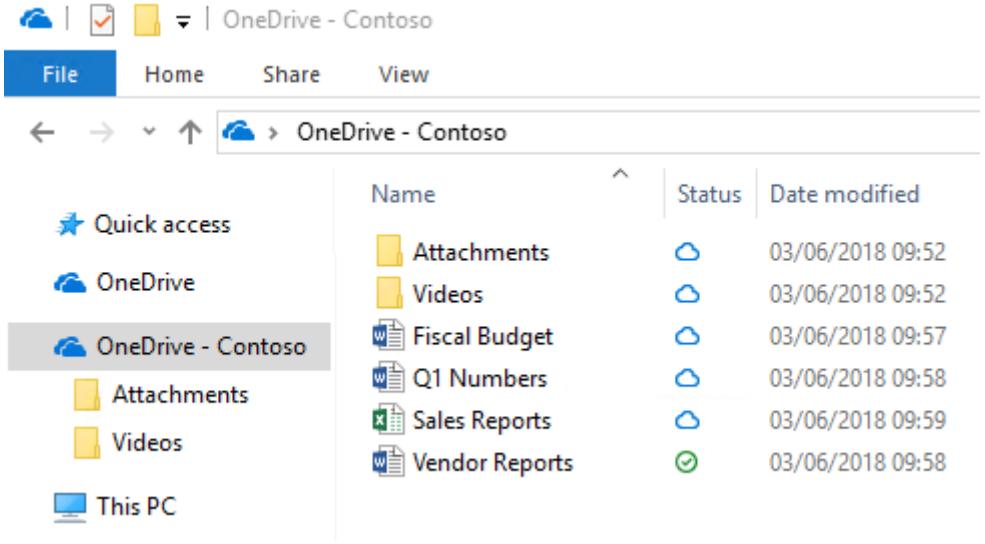
OneDrive is a robust but simple-to-use cloud storage platform for small businesses, enterprises, and everything in between. Unlike other cloud storage providers, most of the advanced enterprise-focused features in OneDrive are available for every subscription type, enabling organizations to use OneDrive in whatever way benefits them the most. This guide describes the features available and how they can benefit your organization.

Key OneDrive features

The features listed in this section address common customer concerns or specific compliance requirements, or provide unique functionality available only in OneDrive. For a full list of features available across OneDrive plans, see Microsoft OneDrive.

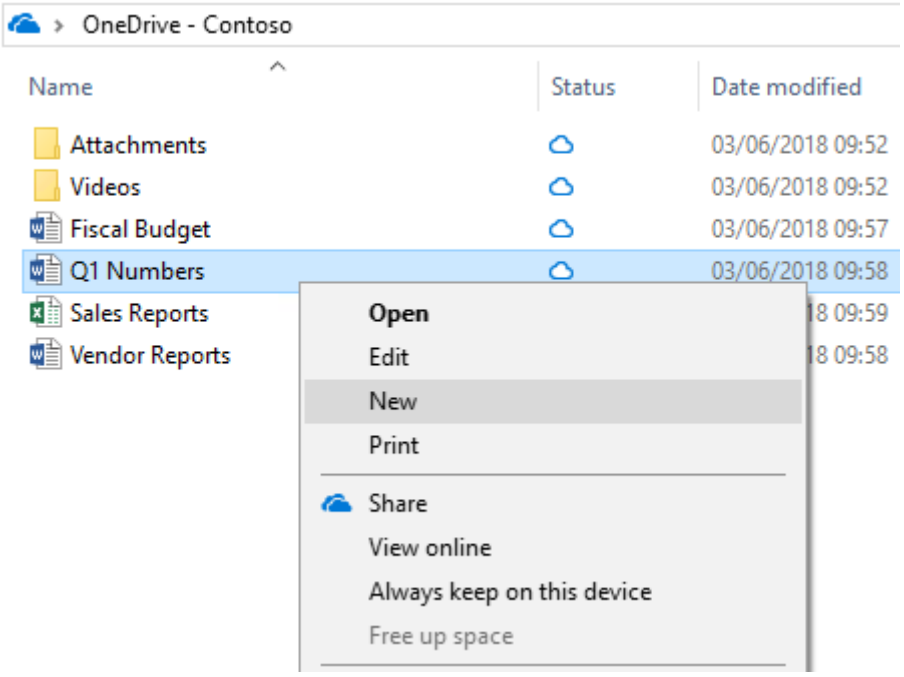
OneDrive Files On-Demand

OneDrive Files On-Demand enables users to view, search for, and interact with files stored in OneDrive from within File Explorer, without downloading all the files to their device. The feature provides a seamless look and feel for both OneDrive and local files without taking up space on the local hard drive. As shown in the following screenshot, files that haven't been downloaded have a cloud icon for their status. For those files that have been downloaded, the status shows a green checkmark.



By default, files are downloaded only when you need to access them. However, if you plan to access a file while disconnected from the internet, make the file available offline by right-clicking it, and then selecting **Always keep on this device**. Alternatively, if you

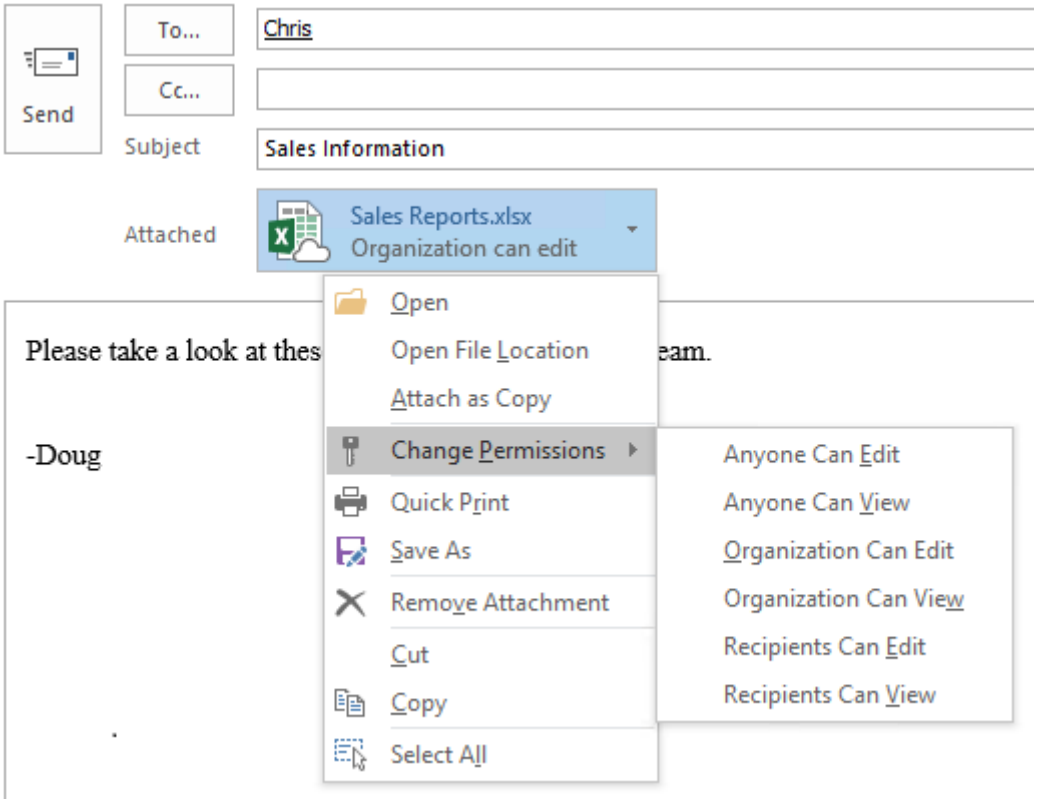
want to free space on your device and remove the downloaded copy of a file, right-click the file, and then select **Free up space**. The following screenshot shows the right-click menu for OneDrive files on a device running Windows.



For more information about OneDrive Files On-Demand, see Learn about OneDrive Files On-Demand.

Modern attachments

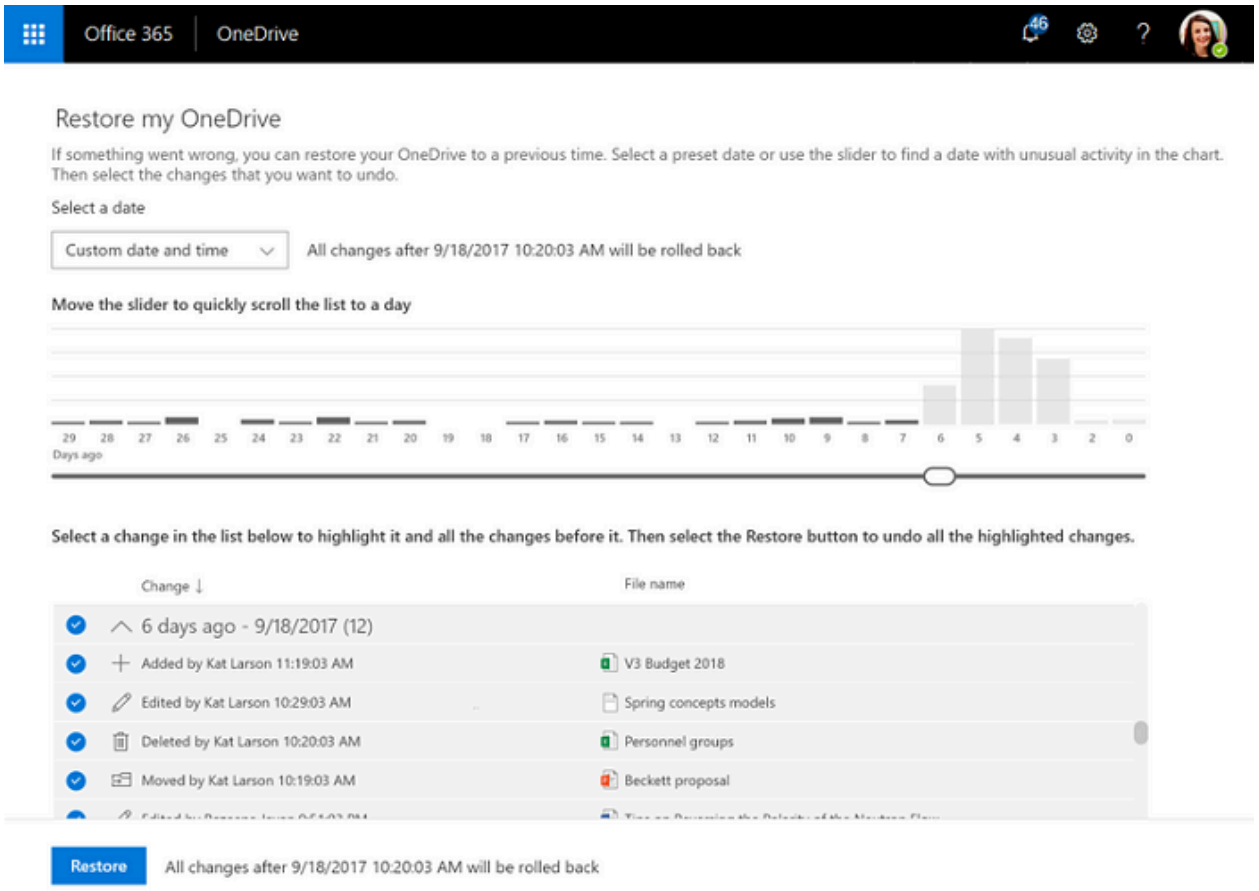
OneDrive integrates with Microsoft Outlook to enable easy sharing of OneDrive files that appear just like email attachments. This feature provides a familiar sharing experience but centralizes storage of attachments in OneDrive. This allows your users to all collaborate on the same file instead of sending different versions back and forth in email. In addition, you can configure sharing permissions on the files directly from within Outlook.



To reduce the potential for confusion when users choose to add a copy versus a link to attached OneDrive files, you can set the default behavior of Outlook, as demonstrated in How to control default attachment state when you attach a cloud file in Outlook 2016 .

Files Restore

The OneDrive Files Restore feature lets users restore files to any point over the past 30 days. To select the desired recovery time, OneDrive presents you with a histogram that shows file activity so that you can determine which recovered time meets your needs. From there, select the file history entry to which you want to restore, and all changes after that point will be rolled back.



In addition, because the histogram shows individual activity on a file, users can use this feature to quickly view their files' modification history. For more information about this feature, see Restore your OneDrive .

Recycle bin

OneDrive has a recycle bin similar to the one available in Windows. Deleted files are moved to the recycle bin and kept for a designated time before being permanently deleted. For work or school accounts, deleted files are purged after 93 days unless configured otherwise. For a demonstration of how the recycle bin works, see Restore deleted files or folders in OneDrive .

Known Folder Move

Known Folder Move enables Windows and Mac users to select commonly used folders, such as their desktop and documents to automatically synchronize to OneDrive. You can add this feature during the initial setup of OneDrive or after it has been configured. This capability provides a simple migration option for users looking to add known folders to their existing list of synchronized folders. For more information about Known Folder Move, see Redirect and move Windows known folders to OneDrive and Redirect and move macOS Desktop and Documents folders to OneDrive.

Syncing files

Users can upload, download, and interact with OneDrive files from a web browser, but the ideal OneDrive experience comes from the Windows and Mac sync apps and the iOS and Android mobile apps. With these clients and apps, saving files to OneDrive and interacting with them is easier than visiting a website each time you need something. Through this experience, you can seamlessly integrate OneDrive into your existing file interaction experiences.

For information about planning and deploying the sync app for your organization, see Plan file sync for SharePoint and OneDrive in Microsoft 365.

Manage OneDrive

Many organizations use OneDrive without changing any of the options. To change these settings, use the SharePoint admin center.

- **Sharing.** Go to Sharing to set sharing settings at the organization level. To learn more, see Manage sharing settings.
- **Sync.** Go to Settings and select **Sync**. You can require that synced computers be joined to your domain or block uploads based on file type.
- **Storage limit.** Go to Settings and select **Storage limit**. Set the default storage space for all new and existing users who are licensed for a qualifying plan and for whom you haven't set specific storage limits.
- **Retention.** Go to Settings and select **Retention**. Configure how long to keep data for users whose accounts have been deleted (the default is 30 days).
- **Access control.** Go to Access control to control access from unmanaged devices or based on network location.
- **Compliance.** View the compliance and risk management solutions available in Microsoft 365
- **Notifications.** Go to Settings and select **Notifications**. For information about this setting, see Control notifications.

Get help with OneDrive

If you need help with OneDrive, you have many ways to find solutions to common issues or request help:

- **Tech community.** Find helpful information from other customers in the community by reviewing the discussions in the OneDrive Tech Community and the Microsoft OneDrive Blog.
- **Support documentation.** For a list of recent issues in OneDrive and how to resolve or work around them, see Fixes or workarounds for recent issues in OneDrive. For getting started info, see Get started with OneDrive, Employee file storage (video training) and Why use OneDrive to store your docs.
- **Microsoft Support.** If you need help from Microsoft to troubleshoot an issue or configure or deploy OneDrive, see Contact Microsoft.

Feedback

Was this page helpful? Yes No

Provide product feedback

Microsoft OneDrive commercial office hours

Article • 10/17/2024

The OneDrive product and engineering team now offers monthly office hours for commercial and education IT Admins and partners. You can join this one-hour Teams meeting to ask us questions, share your feedback, and learn more about the features we're building for the future. You can see the latest topics and register every month here: Register for Office Hours.

OneDrive office hours

When: Third Wednesday of each month, 8:00am – 9:00am PST

Where: Teams meeting

How to sign up: Every month a new call will be on our events page. Follow our blogs for the latest updates.

Agenda: The typical agenda for the meeting looks like this:

- **Roadmap:** We'll discuss and demo upcoming features on the public roadmap (5-10 mins)
- **Feedback:** We'll present a topic and ask for your feedback usually via a single-question poll in Teams (2-5 mins)
- **Q&A:** we'll answer OneDrive questions and field your questions and suggestions. (~45 mins)

You may opt out of OneDrive office hours at any time.

You can opt out of the meeting invitation list. This will ensure that you no longer get office hours meeting invitations, though any information submitted prior to leaving, such as messages in meeting chat, will persist. To opt out of office hours just reply to the office hours meeting invite and let us know that you'd like to unsubscribe.

A note on privacy

OneDrive office hours are Microsoft Teams meetings. All meeting participants including Microsoft employees will be able to see each other's name and work email address

while in the office hours meeting and in the meeting chat. The meetings will be recorded and available on Microsoft channels for on-demand viewing.

Feedback

Was this page helpful? Yes No

Provide product feedback

Guide to the modern experience in SharePoint

Microsoft SharePoint's modern experience is built to be engaging, adaptable, and faster. The modern experience lets anyone make attractive, lively sites and pages that are ready for mobile devices. But how do the classic and modern experiences differ, and how can you create a modern experience for your organization? This guide is an introduction for people who know the classic experiences in SharePoint to help you understand the modern experience and how you can start using it.

Information architecture and hub sites

Classic SharePoint architecture is typically built using a hierarchical system of site collections and subsites, with inherited navigation, permissions, and site designs. Once built, this structure can be inflexible and difficult to maintain. In the modern SharePoint experience, every site is a site collection and can be associated to a hub, which is a flat collection of sites that share navigation, branding, and other elements. This type of structure is far more flexible and adaptive to the changing needs of your organization. Learn about how to plan for Hub sites.

Navigation

The most effective SharePoint sites (and web sites in general) help visitors find what they need quickly so that they can use the information they find to make decisions, learn about what is going on, access the tools they need, or engage with colleagues to help solve a problem. The fundamental principles and good practices for site and page navigation are equally applicable to both classic and modern SharePoint architectures. However, your options for implementing navigation differ based on the framework for your sites and intranet. For example, the "inherited" navigation experiences available in classic SharePoint site hierarchies (sites with subsites) aren't available in the modern experience, but *hubs* provide a great way to achieve the cross-site navigation features previously available in managed navigation and site hierarchies in classic SharePoint.

No matter which framework you're using, you can use the guidance in Plan navigation in the modern experience to help make good decisions for navigation.

Branding

In the classic SharePoint experience, there's a set of default themes and site designs that can require a considerable amount of customization to get them to match your organization's brand. Also, they aren't very responsive, making the experience on different devices inconsistent. Most site branding requires the use of custom master pages or alternate CSS configurations. SharePoint includes an updated set of default site themes and site designs (or templates) that are responsive and look great on any device. With site themes, you can customize your site's logo and colors to match your brand. You can also align the mobile SharePoint app for your users to match your company branding. Site designs provide specific layouts and other functionality for your site. Additional branding can be achieved using custom themes or site designs without worrying about something breaking when SharePoint is updated. To learn more about modern branding options, see Branding SharePoint sites in the modern experience.

Publishing

If you've implemented publishing sites or publishing-enabled sites in your organization, you know how important it's to create attractive and performant pages to distribute communication to a large number of people. In the modern experience, communication sites make it easy to create beautiful, dynamic, and performant sites and pages that are mobile-ready. There are differences from classic publishing, though, and things you want to think about planning your move to the modern experience. For more info, see Moving from Publishing sites to Communication sites.

Search

Search is an important part of any site – you want people to be able to find what they're looking for quickly and easily. SharePoint has both a classic and a modern search experience. Microsoft Search in SharePoint is the modern experience. The most visible difference is that the Microsoft Search box is placed at the top of SharePoint, in the header bar. Another difference is that Microsoft Search is personal and contextual. The results you see are different from what other people see, even when you search for the same words. You'll also see different results based on where you are when you search. For example, searching at the root of your tenant looks across all of SharePoint. Searching from a hub finds content in all sites associated to the hub. Searching from an individual site finds content on that site. Searching from a list or library finds content in the list or library. You'll also see results before you start typing in the search box, based on your previous activity and trending content in Microsoft 365, and the results update as you type. To learn more about the Microsoft Search experience for users, see Find what you need with Microsoft Search. There are other differences, especially around customization. To decide which experience your organization should use, see When to use which search experience.

Sharing and permissions

SharePoint continues to provide both SharePoint groups and security groups maintained by Microsoft Entra ID. Microsoft 365 also provides a third grouping option for SharePoint, Microsoft 365 groups. Microsoft 365 groups are similar to security groups, although Microsoft 365 groups include many extra benefits. Microsoft 365 groups are provided a group email address and more tools such as a group calendar, notebook, Planner, and a SharePoint Team site. Users assigned to a Microsoft 365 group may also be classified as either a group owner or a group member, in comparison to security groups where all group members have equal access under the group. To learn about the differences, benefits, and best practices for permissions and sharing in the modern experience, see Sharing and permissions in the SharePoint modern experience.

Performance

The modern experience in SharePoint is designed to be compelling, flexible and – importantly - more performant. Both SharePoint performance as a whole and the performance of individual SharePoint components such as search, lists, and document libraries are affected by many factors, all of which contribute to the decisive performance metric: perceived end-user latency, or the speed with which pages are rendered in the client browser. For more info, see Performance in the modern SharePoint experience.

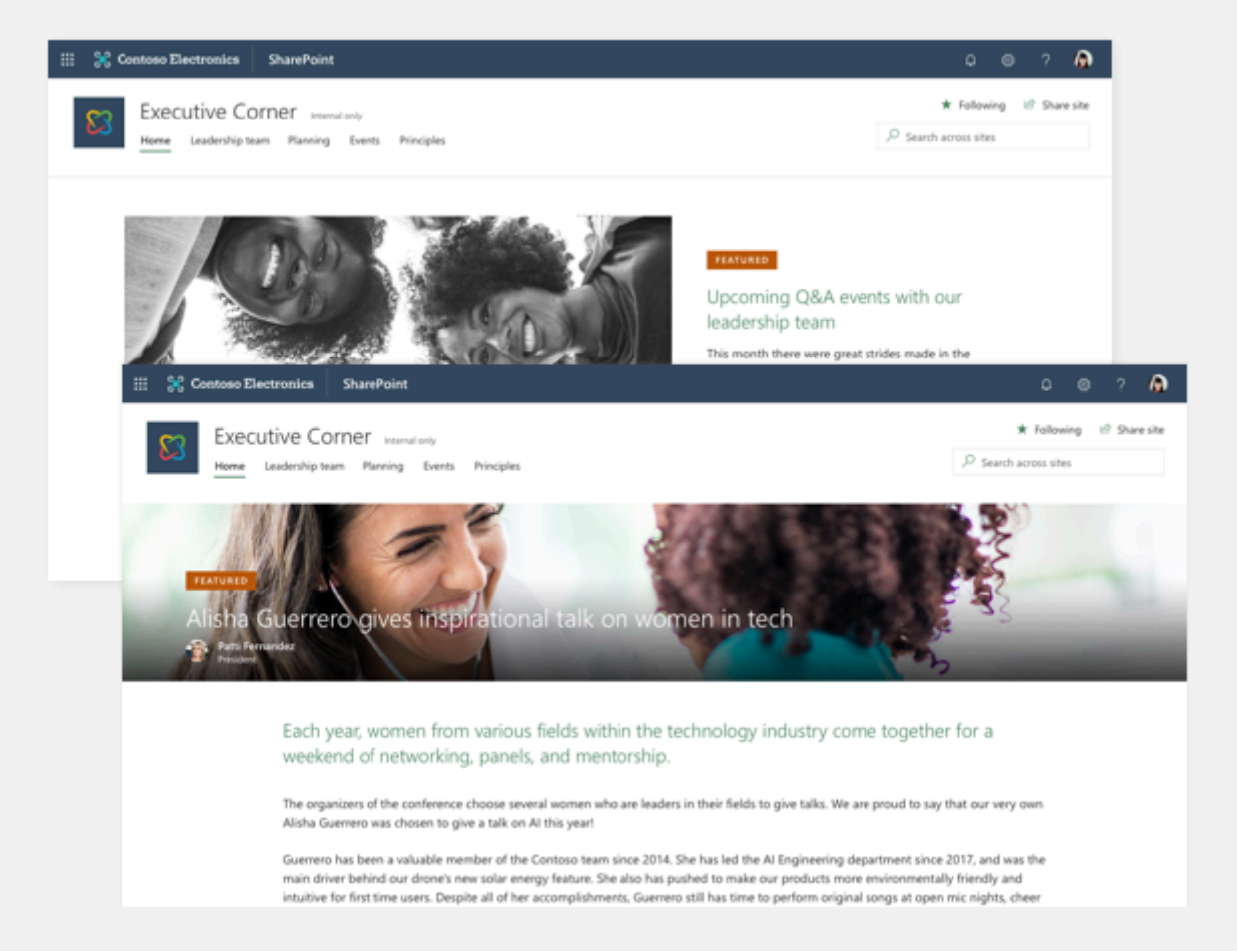
Multilingual

Classic SharePoint publishing sites can use a feature called variations to create a site that supports multiple languages. Modern communication sites use a multilingual experience to make content in your intranet sites available in multiple languages. User interface elements like site navigation, site title, and site description can be shown in the user's preferred language. Additionally, you can provide pages and news posts on communication sites that you translate and that are shown in the user's preferred language. One of the most important differences in the modern experience is that, unlike the variations feature, which creates a separate *subsite* for each language, the modern multilingual experience creates a corresponding page in the same site, but in a language-specific *folder* in the Site Pages library. To learn more, see Create modern multilingual communication sites, pages, and news.

Last updated on 06/24/2026

Branding your SharePoint site

In the modern SharePoint experience, you can easily change the look and feel of your site to match your company or organizational brand. You can customize the logo, colors, and navigation – often without writing a single line of code. Branding can be applied at the site level, to a group of sites, or to all sites within your organization.



> **Note**
>
> Branding your SharePoint site will not change the overall look of your Microsoft 365 service. For more info about branding Microsoft 365, see Customize the Microsoft 365 theme for your organization.

Site branding in the classic experience

In the classic SharePoint experience, there's a set of default themes that can require a considerable amount of customization to get them to match your organization's brand. Also,

they aren't responsive, making the experience on different devices inconsistent. Most site branding requires the use of custom master pages or alternate CSS configurations. Master pages provide a great deal of flexibility, but they can be problematic. For example, anytime updates are made to SharePoint, any customizations made to the master page may no longer work or may not work the way you expect them to. SharePoint ignores these customizations unless you're running in classic experience mode because they're incompatible with the modern user interface. To avoid this situation, use only the recommended modern approaches to brand your SharePoint sites.

Modern site branding

SharePoint includes an updated set of default site themes that are responsive and look great on any device. With site themes, you can customize your site's logo and colors to match your brand. Site templates provide specific layouts and other functionality for your site. More branding can be achieved using custom themes or site templates without worrying about something breaking when SharePoint is updated. Custom themes let you create more color schemes beyond the defaults. Custom site templates let you control the site theme and other customizations like the site navigation, default applications, and other settings. Custom themes or site templates can be applied to a new site when it's created or applied to an existing site or group of sites.

Branding hub sites

When you brand a SharePoint hub site, you can set it so the site branding is applied to any sites that associate with it. This includes any site theme or site template used by the hub site. This allows you to apply common navigation and branding across a set of sites and use accent colors to emphasize elements that need to stand out.

> **Note**
>
> Custom themes and logos in SharePoint *does not* automatically apply to group-connected team sites that are associated to a hub that has a custom theme applied. For group-connected team sites, you need to manually apply the custom theme or logo.

Classic experience vs. modern experience

The following is a summary of the differences between branding a site in the classic experience vs. branding in the modern SharePoint experience.

Expand table

Classic experience	Modern experience
Unresponsive, OOB themes that you can customize	Responsive themes that look great on any device and can be customized to match your brand
Use custom master pages and CSS that are ignored in the modern experience	Use the SharePoint Framework to add headers and footers. Site templates and tenant settings offer some custom options

Before you begin

Some things to consider before branding your classic experience sites in SharePoint are:

- Do you need a consistent brand across all sites or will different divisions, departments, or groups in your organization have their own?
- You should compile a list of all current sites, what site templates they use, any customizations that have been made to the master pages or CSS, and decide which of these customizations you need to keep. You can run the SharePoint "Modern" user interface experience scanner which does a deep analysis of all the sites in your organization and create reports that give you details about sites that have incompatible master pages or alternate CSS settings. SharePoint handles branding differently for classic site templates such as the publishing site. You want to troubleshoot any custom theme issues you run into.
- What areas do you want to customize (logo, colors, fonts, header/footer, navigation)?
- Who in your organization can brand a site? You'll need to make sure that they have site designer permissions or above to make these changes.

Ready to brand your classic SharePoint site using the modern experience?

Check out the below resources that provide more details about how to use the modern SharePoint experience to brand your site.

Change the look of your SharePoint site.

SharePoint site theming

Modernize site branding.

Modernize your classic SharePoint sites.

JSON schema

Last updated on 06/24/2026

SharePoint governance overview

Governance is the set of policies, roles, responsibilities, and processes that control how your organization's business divisions and IT teams work together to achieve its goals. We recommend that you consider governance first as you start working with SharePoint. Having a governance plan in place early can help your organization stay compliant with your business processes and regulations.

Two of the primary ways SharePoint is used in an organization are *intranet sites* and *collaboration*. See Planning intranet governance and Overview of collaboration governance in Microsoft 365 for a look at governance in these two areas.

Resources

Use these resources to further explore governance in Microsoft SharePoint and related services.

SharePoint

- Manage site creation for SharePoint in Microsoft 365
- SharePoint site designs & site script overview
- Learn about retention policies
- Managing sites in the new SharePoint admin center

Related services

SharePoint is tightly integrated with other Microsoft 365 services, including Microsoft 365 Groups, Teams, and Viva Engage. It's important to think about SharePoint governance in a way that's inclusive of these other services. Microsoft 365 includes various options to enable your governance policies across SharePoint and related services, including Teams, Planner, Stream, Outlook, Viva Engage and Microsoft 365 Groups.

To see how SharePoint governance capabilities overlap with other Microsoft 365 services, see:

- Settings interactions between Microsoft 365 Groups and SharePoint
- Settings interactions between Microsoft 365 Groups, Teams and SharePoint
- Get ready for Microsoft Copilot with SharePoint Advanced Management

For lifecycle guidance for SharePoint sites together with related Microsoft 365 services, see:

- Plan organization and lifecycle governance for Microsoft 365 groups and Microsoft Teams
- End of lifecycle options for groups, teams, and Viva Engage

Related articles

Manage who can create Microsoft 365 Groups

Microsoft 365 reports in the admin center – Microsoft 365 Groups

Create a secure guest sharing environment

Limit accidental exposure to files when sharing with people outside your organization

---

Last updated on 08/18/2026

Overview of Teams and SharePoint integration

In this article, learn about how Teams and SharePoint work together.

The basic parts of Teams and SharePoint

Here are the basic parts of Teams and SharePoint and how they relate to each other:

- **Teams** - Teams is a collaboration tool where you can chat with other people about a particular subject or task. Each team is connected to other tools that you can use to collaborate with others.
- **SharePoint** - SharePoint is a tool for creating web sites, publishing content, and storing files.
- **SharePoint site** - A SharePoint site is a web site in SharePoint where you can create web pages and store and collaborate on files. SharePoint sites can be used independently and can also be used by Teams for file storage (called *Teams-connected sites*). A Teams-connected site is created automatically whenever you create a team.
- **Team** - A team is a place in Teams where you can invite others to collaborate. Each team is connected to one or more SharePoint sites. These sites are where the team's files are stored.
- **Public team** - A public team is a team that anyone in the organization can join. Public teams don't require a team owner to invite someone to the team.
- **Private team** - A private team is a team that a person can only join when invited by a team owner. Both public teams and private teams offer the same channel types - standard, private, and shared.
- **Parent site** - The SharePoint site that is created when you create the team. This site is used for file storage for all standard channels. All team owners and members have access to this site.
- **Channel** - A channel is a location in a team where you can collaborate with others on a specific thing. A team can have multiple channels for different purposes. For example, you might have a team for marketing with different channels for different products or events. There are three types of channels in Teams: *standard*, *private*, and *shared*.

- **Standard channel** - A standard channel is a channel that all members of a team have access to. Each team comes with a standard channel called "General." Team owners and members can add additional standard channels. It always shows up first in a team's list of channels, and it can't be deleted (every team must have at least one channel).

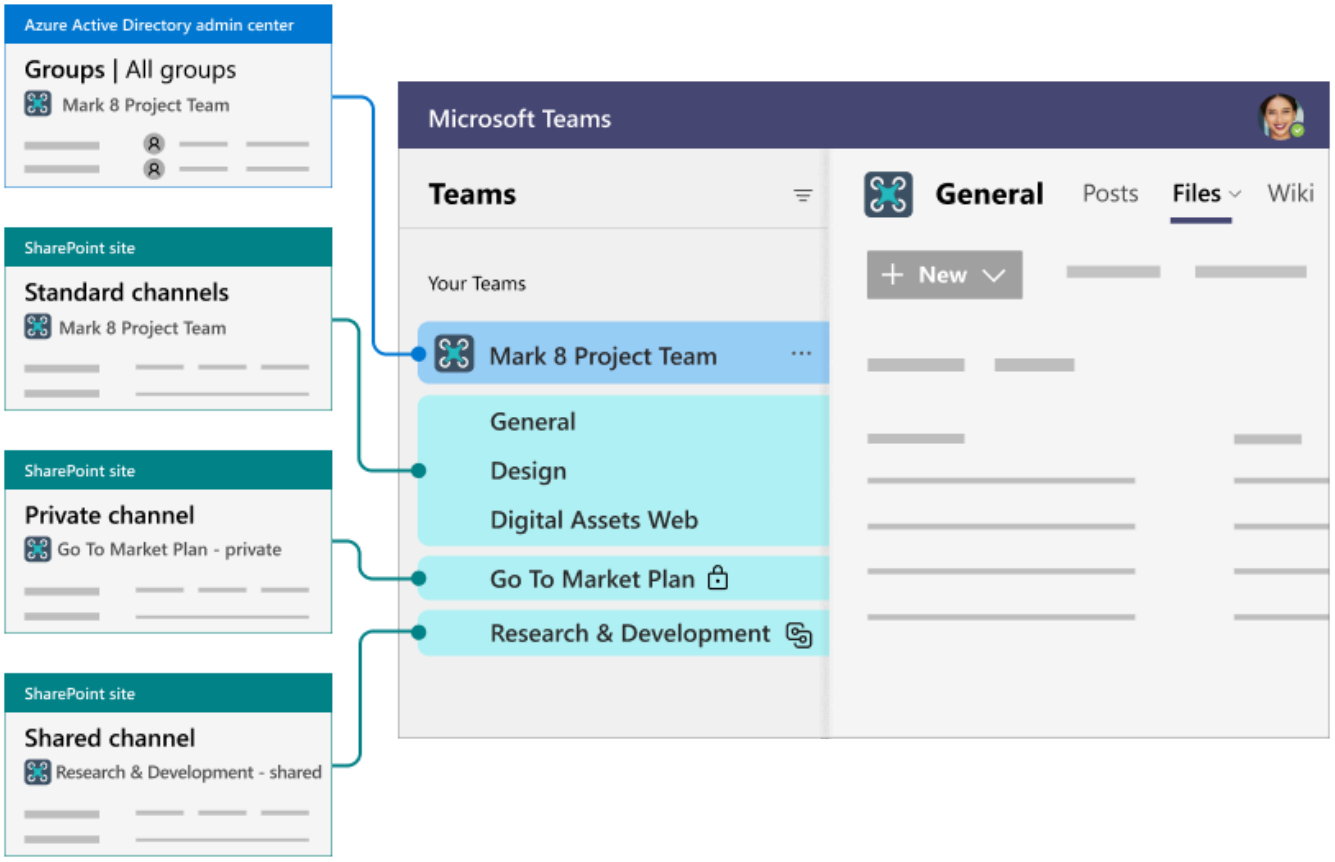
- **Private channel** - A private channel is a channel that only some of the team's members have access to. It's used for private conversations and collaboration. Each private channel has its own SharePoint site for file storage. Only members of the private channel can access this site.

- **Shared channels** - A shared channel is a channel that you can add anyone to, even if they're not a member of the team. It's used for broader collaboration with people outside the team. Each shared channel has its own SharePoint site for file storage. Only members of the shared channel can access this site.

- **Channel site** - The SharePoint site that is created when you create a private or shared channel in a team. Only owners and members of the private or shared channel have access to this site.

- **Microsoft 365 group** - A Microsoft 365 group is a membership group that gives people access to multiple Microsoft 365 services at the same time. The membership for each team is stored in a Microsoft 365 group and that group also gives those people access to the team's parent SharePoint site.

- **Microsoft Entra ID** - Microsoft Entra ID is the directory service where Microsoft 365 user accounts are stored. (You can manage these accounts from Microsoft 365 as well.) Microsoft 365 groups are also stored in Microsoft Entra ID. Microsoft Entra ID allows administrators to manage users and groups and to apply business rules to user accounts, such as requiring multi-factor authentication.



Each team is connected to a Microsoft 365 group in Microsoft Entra ID where the team membership is stored. The files you see on the **Files** tab in a team are stored in a SharePoint site. All standard channels in a team share the same SharePoint site, but each private channel has its own site.

https://learn-video.azurefd.net/vod/player?id=e4f94dfb-42ef-4616-9ded-3d3cd7040d2f&locale=en-us&embedUrl=%2FSharePoint%2Fteams-connected-sites

When do Teams and SharePoint get connected?

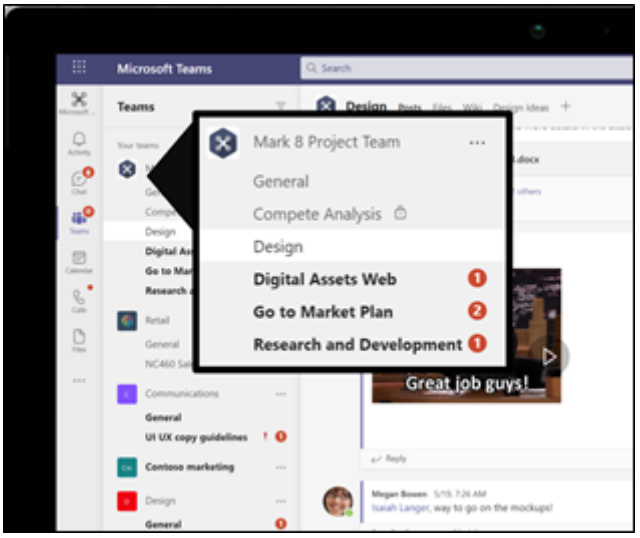
Teams and SharePoint are connected in the following scenarios:

- When you create a new team from scratch, a new SharePoint site is created and connected to the team.
- When you create a new team from an existing Microsoft 365 group, the team is connected to the SharePoint site associated with the group.
- When you add Teams to an existing SharePoint site, that site is connected to the new team.
- When you create a new private or shared channel, a new SharePoint site is created and connected to that channel.

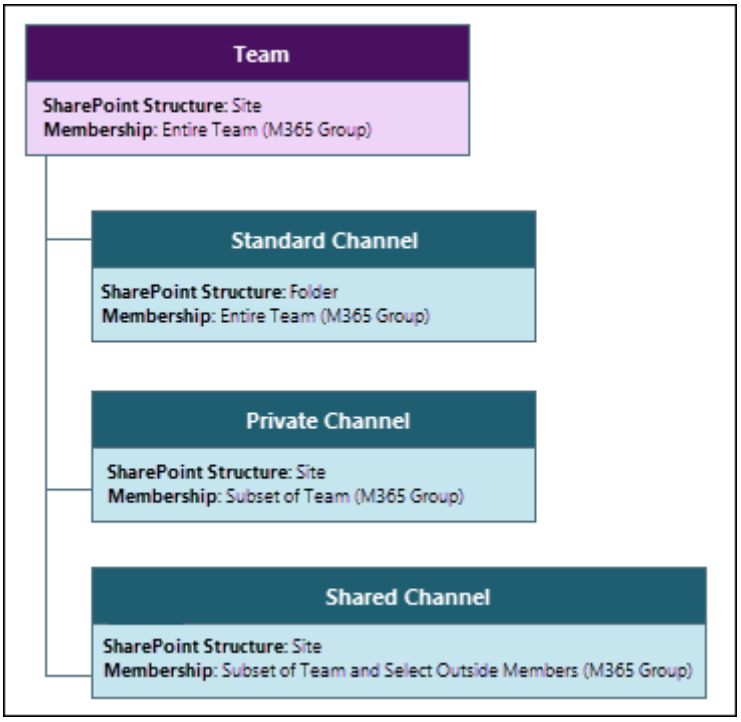
In Teams, the Files tab on each standard channel is connected to a folder in the parent site's default document library. The Files tab on each private and shared channel is connected to the default document library in the corresponding channel site. Whenever you add or update a file on the Files tab, you're accessing the SharePoint site.

Example of a team with multiple channel types

Contoso has a team called Mark 8 Project Team. This team has several standard channels, and one private channel called Compete Analysis.



The standard channels display as folders in the parent site. The private channel has its own channel site that is separate from the parent site.



Teams-connected sites and channel types

Teams-connected sites are a specialized type of SharePoint site that's been optimized for a Teams connection. This includes the parent site that is created when you create the team, and any channel sites that are created when you create a private or shared channel.

This table describes how site, file, and folder sharing work for each type of channel in Teams.

Expand table

Channel type	SharePoint site	Site sharing	File and folder sharing
Standard	One SharePoint site is shared by all standard channels. There's a separate folder for each channel.	Team owners and members are automatically included in the site owners and members permission groups. Sharing the site separately is possible but managing access through Teams is recommended for easiest user management and the best user experience.	Files and folders can be shared with anyone in the organization by using sharable links. If guest sharing is enabled, *Anyone* and *Specific people* links can be used to share with people outside the organization.
Private	Each private channel has its own SharePoint site.	Channel owners and members are automatically included in the site owners and members permission groups. The site can't be shared separately.	Files and folders can be shared with anyone in the organization by using sharable links. If guest sharing is enabled, *Anyone* and *Specific people* links can be used to share with people outside the organization.
Shared	Each shared channel has its own SharePoint site.	Team owners and members are automatically included in the site owners and members group. The site can't be shared separately.	Files and folders can be shared with anyone in the organization and external participants in the channel by using sharable links. Sharing with people outside the organization who aren't channel members isn't supported.

Where to manage Teams and SharePoint settings

Teams-connected sites are managed differently than the typical SharePoint site. Certain site settings can only be managed from Teams. For channel sites, some settings are inherited from the parent site and can't be changed. This table describes where SharePoint settings are managed for Teams-connected sites.

Expand table

Setting	Parent site	Channel site
Site permissions	Team permissions are synced with the site. Team and site owners can add additional people directly to the site. (Managing all permissions through Teams is recommended.)	Channel site permissions are inherited from the channel itself. Site permissions can't be managed in SharePoint, but will display permissions in read-only mode.
Site sharing settings	Team and site owners can set the sharing settings for files, folders, and the site. This is a SharePoint-specific setting.	
Guest access expiration	Guest access expiration can be set in the SharePoint admin center.	
Sensitivity	Sensitivity labels can be applied either to the team or the parent site. The same label is used for both and a change made in either location is reflected in the other.	Sensitivity of channel sites is inherited from the parent site.
Site quota	The site quota can be set in the SharePoint admin center.	The site quota can be set in the SharePoint admin center.
Default sharing link type	The default sharing link type can be set in the SharePoint admin center.	The default sharing link type can be set in the SharePoint admin center.

Related topics

Create a Microsoft Team from SharePoint

Teams can have standard or private channels

Overview of security and compliance

Manage teams policies in Teams

Manage team settings and permissions in Teams

Last updated on 06/25/2026

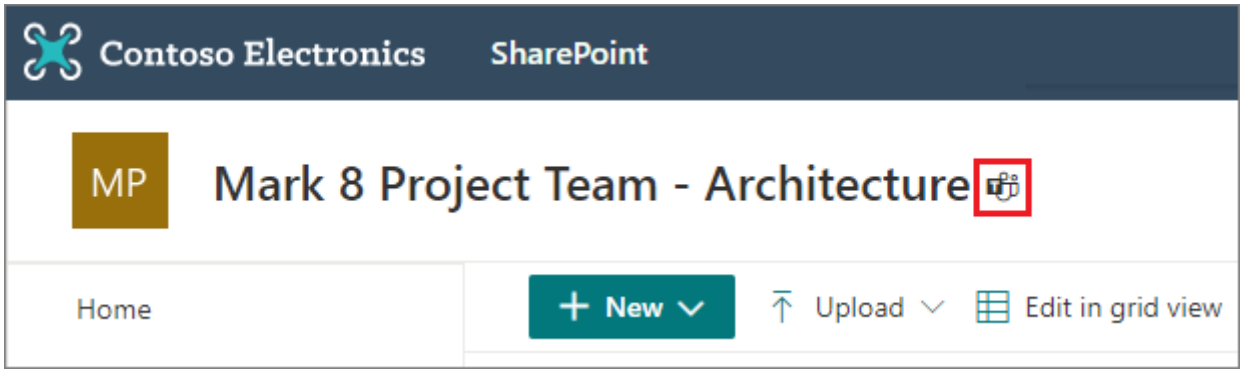
Manage settings and permissions when SharePoint and Teams are integrated

Article • 05/07/2024

In this article, learn how to manage settings and permissions when Teams and SharePoint are integrated together. Learn more about integrations between SharePoint and Teams, basic terminology, and structure.

How to identify and navigate between SharePoint and Teams

Teams-connected sites include additional information to indicate the connection to Teams. In the SharePoint site header, you'll see the Teams icon following the site logo and site title.



In the site, the **In channels** section is available in the command bar when viewing document libraries. You can select to open each channel's folder. When hovering over each folder, you can select the Teams icon next to folder to navigate to the Teams channel. For example, the Teams icon next to the "General" folder leads you to Teams and the general channel for the team.

Additionally, from teams and channels in Microsoft Teams, you can select the **Files** tab at the top of the channel and then **Open in SharePoint** to navigate to the Teams connected team site or channel site in SharePoint.

Manage settings and permissions

When SharePoint sites and Teams are integrated, certain setting and classifications need to be managed in the settings in Microsoft Teams. You notice that when you navigate

to **Settings** in SharePoint site, certain options aren't editable, like **Permissions**. Learn more about viewing and managing settings in Microsoft Teams.

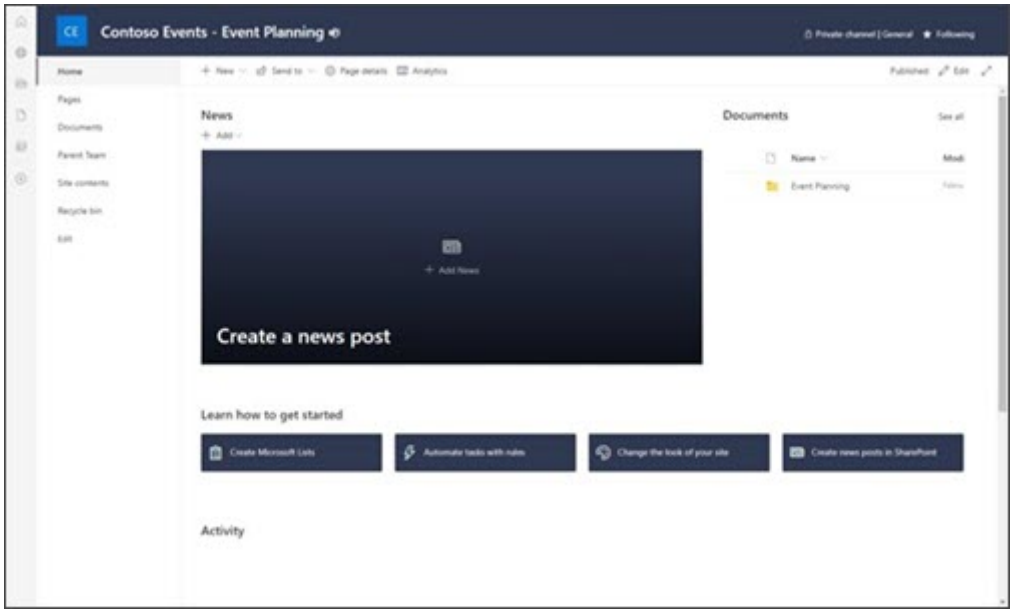
Expand table

Settings managed in SharePoint	Settings managed in Teams
- Site name - Site description - Hub association	- Site permissions - Sensitivity classification - Private channel membership

> **Note**
>
> Channel sites display site permissions in the SharePoint site permissions panel in read-only mode. Site owners can access and update site sharing or guest expiration options in the panel, but they need to go to Microsoft Teams to manage site permissions.

Channel site home page layout

For private and shared channel sites, you'll find a unique home page layout that is designed to encourage and guide usage of typical SharePoint tasks. You'll find easy access to the News web part, Documents web part, and links to documentation for creating lists, automating tasks, and changing the look of your site.

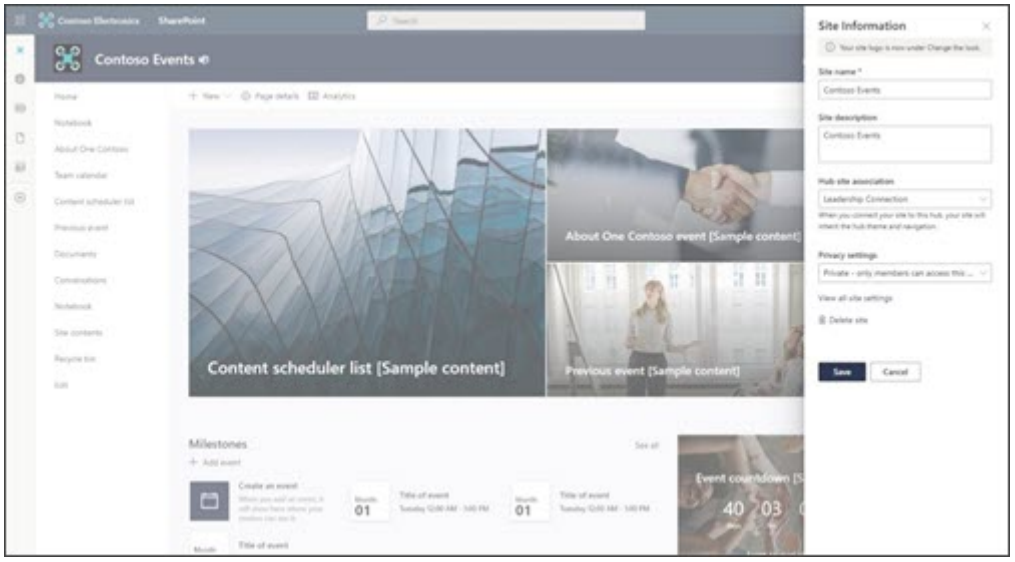


Channel sites and hub associations

Just like typical SharePoint sites, channel sites can be associated to a SharePoint hub sites from the parent team site. Upon associating the parent team to the hub, all channel sites (private and shared) are also associated to the hub.

When channel sites get associated with a hub, the hub navigation gets inherited across the parent team and channel sites. The entire team (parent team and channels) is treated as one entity.

> **Note**
>
> Hub site association doesn't appear in the Site information panel for channel sites. Hub site associations are managed from the parent team site.



How to maximize the benefits of SharePoint and Teams integration

- **Upload and share files in Teams** - Share a file in a team or channel and the file will become accessible to everyone in the team. The file will also automatically sync to the corresponding SharePoint site document library. Learn more about file sharing in Teams and how to coauthor content with your team.
- **Pin resources from SharePoint as a tab in Teams** - Add published SharePoint pages, lists, and document libraries as individual tabs in a Teams channel. Learn more.
- **Use team templates in Teams and SharePoint** - Teams has team templates that can be used to quickly create a new team and connected site that come prepopulated with resources and folders. Learn more about how to create a new team using a template

Learn more

Overview of SharePoint and Teams integration

Manage policies in Teams

Manage settings and permissions in Teams

Create a Microsoft Team from SharePoint

Microsoft Teams can have standard or private channels

Feedback

Was this page helpful? Yes No

Provide product feedback

Plan for SharePoint and OneDrive in Microsoft 365

Article • 09/17/2024

This article and the other articles in this section include the core planning considerations for rolling out OneDrive and SharePoint in a medium to large organization.

SharePoint is deeply integrated with Microsoft Teams. As part of your SharePoint and OneDrive rollout, we recommend that you review Microsoft Teams deployment overview.

As you plan your rollout, in addition to the technical planning considerations provided here, consider these questions:

- What are your high-level goals for rolling out OneDrive and SharePoint?
- What are the file storage and collaboration needs of your organization?
- How do you want to transition from your current tools to OneDrive and SharePoint?
- How important is migration of content as part of your rollout?
- Should your administrators specialize in a particular area of OneDrive or SharePoint or should they work from a shared queue of tasks?

After you review this article, see these articles for additional planning information:

- Identify business requirements for SharePoint and OneDrive
- Hybrid OneDrive and SharePoint in Microsoft 365
- Plan file sync for SharePoint and OneDrive in Microsoft 365
- Migration planning for SharePoint and OneDrive rollout
- Create a compliant SharePoint and OneDrive environment
- Plan sharing and collaboration options in SharePoint and OneDrive
- Training and change management for rolling out SharePoint and OneDrive
- Roll out SharePoint and OneDrive

Migrate content

An important part of rolling out SharePoint and OneDrive is migrating content from your existing storage locations. This may include gradual migration of content over time as you roll SharePoint and OneDrive out to different groups in your organization. You can find complete information about migration at Migrate your content to Microsoft 365.

Migrate with FastTrack

FastTrack is a Microsoft benefit that is included in your subscription. FastTrack provides you with a set of best practices, tools, resources, and experts committed to helping you deploy Microsoft 365. Guidance around SharePoint and OneDrive onboarding, migration, and adoption are included in the benefit offering. This guidance includes: help to discover what's possible, creating a plan for success, and onboarding new users, providing guidance on migrating content, and introducing capabilities at a flexible pace.

FastTrack guidance provides enablement of both SharePoint and OneDrive as well as getting the source environment ready for your transition. For more details, see FastTrack Center Benefit Overview. Interested in getting started? Visit the FastTrack web site, review resources, and submit a Request for Assistance.

Sites, hubs and architecture

You can let your users create and administer their own SharePoint sites, choose what kind of sites they can create, and specify the location of the sites. By default, users can create communication sites and Microsoft 365 group-connected team sites. You can restrict this if you want to manage this through IT or a business process. Plan sharing and collaboration options in SharePoint and OneDrive for more information.

SharePoint uses hub sites to help you organize sites in a hierarchy that matches your organization or business processes. While it's not critical to plan your hub site layout as part of your SharePoint rollout, we recommend reviewing Planning your SharePoint hub sites to understand how hub sites work.

We recommend including planning for hub sites as part of your process for rolling out an intelligent intranet.

Network utilization

Various factors can impact the amount of network bandwidth used by SharePoint and OneDrive. For the best experience, we recommend that you assess this impact before you start your rollout. The article Network utilization planning for the OneDrive sync app

includes the recommended process for determining your network bandwidth needs for OneDrive. Be sure to include this as part of your deployment plan.

These references can also help with planning your rollout:

- Networking roadmap for Microsoft 365
- Office 365 URLs and IP address ranges
- Use the Office 365 Content Delivery Network (CDN) with SharePoint Online

Change management

Rolling out SharePoint and OneDrive means new processes and procedures for the users in your organization. An important part of the rollout is making sure users are trained in the new ways of doing tasks as well as entirely new tasks that SharePoint and OneDrive enable. See Training and change management for rolling out SharePoint and OneDrive for considerations around change management and resources that you can share with your users on how to work with SharePoint and OneDrive.

Customizing SharePoint

SharePoint offers many customization options, including:

- Branding SharePoint sites
- Navigation between sites
- Custom page layouts
- Custom apps
- Workflows

We recommend that you review Customizing SharePoint to determine if you want to include any of these customizations as part of your SharePoint rollout.

Next steps

Identify business requirements

Related topics

OneDrive Adoption

SharePoint Adoption

Feedback

Was this page helpful? Yes No

Provide product feedback

SharePoint storage planning

SharePoint is the most trusted and flexible platform for your content, providing enterprise-grade security and compliance tooling, built-in high availability and disaster recovery, point-in-time restore, and much more. Depending on your business scenarios, it's important that you plan your content storage strategy to maximize user value and to optimize storage costs. This article highlights ways to gather data for insights into storage usage, tools to help manage or reduce storage footprint of less valuable content, and premium offerings for a richer experience.

> **Note**
>
> Storage values can differ across SharePoint experiences because they measure different aspects of content. For example, a document library typically shows the size of the current file, while Storage Metrics and other storage reports reflect the total storage consumed by that content. Storage consumption can include version history and other storage-related data associated with a file. As a result, the storage reported for a site, library, or folder might be larger than the combined size of the current files displayed in a document library.

Understand storage drivers

As storage grows over time, it's important to understand what drives storage growth and to identify the areas that could need your attention. There are options to review storage trends, ranging from usage reports in the Microsoft 365 admin center, which provide easy-to-consume visuals, to rich datasets available through Microsoft Graph Data Connect (MGDC).

- Review storage used by active sites, archived sites, and deleted sites in the SharePoint admin center. The upper right side of the Active sites page shows the amount of storage used across all sites, and the total storage for your subscription. If your organization has configured Multi-Geo in Microsoft 365, the bar also shows the amount of storage used across all geo locations.

- Use SharePoint dataset from Microsoft Graph Data connect to analyze site lifecycle, ownership, and storage used by SharePoint sites and OneDrive accounts. Answer questions such as which type of site uses the most storage, how much storage was used by previous versions, and how many sites haven't changed in the past year. File level data is also available now through the SharePoint Files dataset. (*)

- Explore storage trends through the SharePoint Admin Agent. The storage skill can help analyze your SharePoint storage usage and provide actionable insights for storage management. (*)

> **Note**
>
> Deleted sites in the Recycle Bin do not count toward the organization's total storage usage. It takes up to 48 hours for the storage usage to update.

Set up storage configurations

Configure the site storage limits, version history limits, and retention policies that meet your organization's needs. Whether that's automatic limits for simplicity or custom limits for maximum control, setting up these limits is fundamental for storage management.

- Set site storage limits to **Automatic** to simplify site storage management, or to **Manual** for custom limits. Site limits cap the allocation of pooled tenant storage resources among sites within the organization.
- Update organization version history limits to **Automatic** for optimal version restore and storage.
- Review retention policies for SharePoint to manage compliance requirements with storage use.

Optimize storage usage

Increase available storage by cleaning up low-value versions and inactive sites or by moving inactive content to a lower cost archive storage solution.

- Archive inactive content to reduce active storage costs using Microsoft 365 Archive.
- Trim existing low-value versions to reduce storage.
- Recover storage from deleted items by emptying site recycle bin.
- Leverage retention settings to automatically delete files after a specified period.
- Manage site lifecycle policies through SharePoint Advanced Management. Set up an inactive site policy to automatically detect inactive sites and send notifications to site owners via email. (*)

Purchase additional storage

To increase SharePoint storage capacity, purchase additional storage in one-gigabyte increments or acquire more SharePoint licenses.

- Purchase SharePoint user licenses, adding 10 GB per license to the storage limit. SharePoint user licenses are included in plans, such as Microsoft 365 for business or enterprise.[(*)]
- Set up Microsoft 365 SharePoint Storage, a pay-as-you-go solution for additional storage usage above the tenant quota. (*)
- Purchase additional storage at a cost per gigabyte (GB) per month.[(*)]

[(*)]: Additional licensing/charges might apply

FAQs

1. How is the SharePoint storage quota calculated?
   SharePoint storage quota for the tenant starts at 1 TB and each additional SharePoint license purchased adds 10 GB. For more information, see SharePoint limits - Service Descriptions.

2. What happens if my tenant exceeds the SharePoint storage quota?
   When the SharePoint storage quota is exceeded, you might need to purchase additional storage or manage existing storage more efficiently through deletion or archival. In addition, classic site creation and site creation through PowerShell is blocked.

3. How does version trimming work with the preservation hold library?
   Version trimming doesn't impact the files in the preservation hold library since the original copies of the files are preserved. For more information on how retention settings work in SharePoint, see Learn about retention for SharePoint and OneDrive.

Related articles

- Microsoft 365 Archive (ideal for inactive content)
- Versioning overview
- Site lifecycle management
- Microsoft Graph Data Connect for SharePoint

Last updated on 09/29/2026

View SharePoint files with File Explorer in Microsoft Edge

Article • 11/25/2024

> **Important**
>
> In June 2022, we stopped supporting Internet Explorer 11 (IE 11) at Microsoft 365 apps and services. As a result, we no longer recommend View in File Explorer and encourage using the OneDrive sync client. The OneDrive sync client provides Files On-Demand, which allows you to access all your files in SharePoint without using up local storage space. For info about using OneDrive to sync SharePoint files, visit SharePoint file sync.

By default, the View in File Explorer menu option won't be visible to you or users in the SharePoint modern document library interface. In certain cases, organizations may still need to use View in File Explorer to access modern document libraries. Starting in Microsoft Edge Stable version 93, you can enable the View in File Explorer capability on SharePoint for modern document libraries.

Configure View in File Explorer with Microsoft Edge

Follow the steps below to use View in File Explorer in Microsoft Edge:

1. Verify that devices are on Microsoft Edge build 93 or later using Find out which version of Microsoft Edge you have.

2. Ensure that Windows instances are joined to a Microsoft Active Directory domain, Windows 10 Pro, or Enterprise instances that are enrolled for device management.

3. Enable the ConfigureViewInFileExplorer policy for Microsoft Edge that allows URLs with the viewinfileexplorer: scheme to open WebDAV URLs in Windows File Explorer.

   Use the options below to enable View in File Explorer using group policy or Intune:

   - **To enable by using group policy**:

     a. Configure Microsoft Edge policy settings by following the steps at Configure Microsoft Edge policy settings on Windows.

b. Make sure you've downloaded the Microsoft Edge administrative template based on the operating system version or you may not see the policy listed.

c. Once the template is downloaded, open the Group Policy Object Editor. Right-click **Administrative Templates** in the Computer Configuration or User Configuration node and select **Add/Remove Templates** and browse to the downloaded template.

d. When applying the policy, ensure you update the domain to your tenant domain or use **sharepoint.com** if you plan on visiting multiple SharePoint tenants.

e. Enabling the group policy may require a refresh of client group policy settings. After changing the group policy settings, refresh the settings. From a Command Prompt, enter **GPUpdate.exe /force**.

   Following is an example of the Group Policy value:

   ```
   [{"cookies": ["rtFa", "FedAuth"], "domain": "sharepoint.com"}]
   ```

   For more examples, see ConfigureViewInFileExplorer on Microsoft Edge policy reference.

- **To enable by using Intune**:

  Configure Microsoft Edge policy settings by following the steps at Configure Microsoft Edge policy settings with Microsoft Intune.

4. Verify the policy has been enabled by opening Microsoft Edge and navigating to **Microsoft Edge://policy/**.

> **Tip**
>
> You may need to close and re-open Microsoft Edge for the policy to appear.

5. As a tenant administrator, update your SharePoint Online tenant configuration via SharePoint Online Management Shell to allow the "View in File Explorer" option to be visible in the Microsoft Edge Browser interface with these steps:

   a. Connect to SharePoint Online Management Shell by running:

   ```
   PowerShell
   ```

```
Connect-SPOService -Url https://contoso-admin.sharepoint.com
```

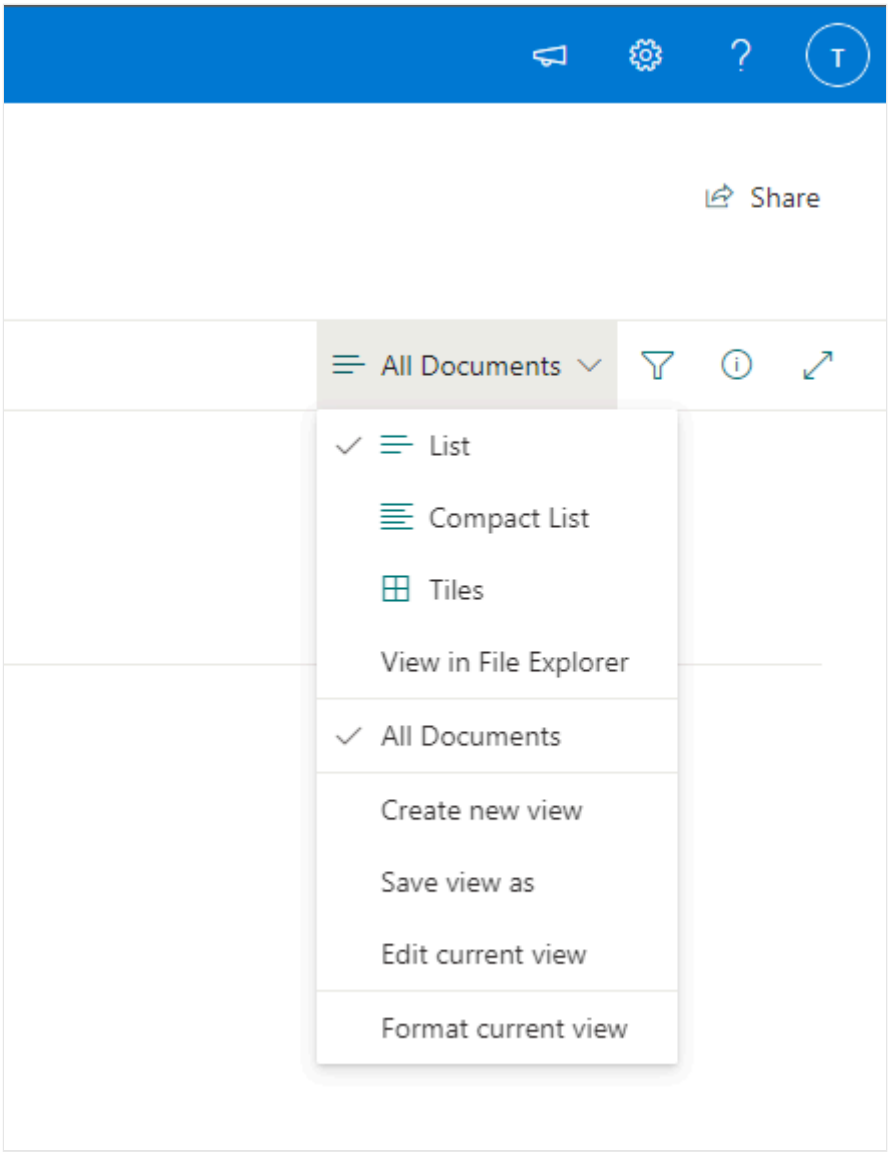
b. Run the following cmdlet to show the "View in File Explorer" menu option:

```PowerShell
Set-SPOTenant -ViewInFileExplorerEnabled $True
```

> **Note**
>
> Ensure the management shell version is 16.0.21610.12000 or higher or the ViewInFileExplorerEnabled option will not be available.

6. **(Required)** *View in File Explorer* requires persistent cookies to operate correctly; when you sign in, select **Yes** when the **Stay signed in?** prompt appears.

   You can locate the View in Explorer button by navigating to the **Library** > select the **Library View Menu** on the right-hand side > select **View In File Explorer**.



> **Note**
>
> Once the tenant setting has been enabled, it may take up to 15 minutes for the View in Explorer button to appear in the SharePoint interface.

Troubleshooting

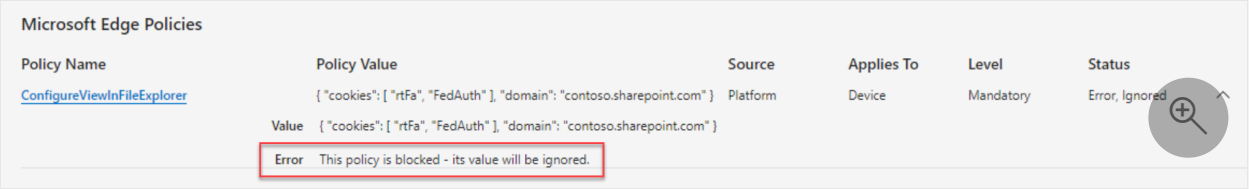
How can I confirm that the ConfigureViewInFileExplorer policy has been applied?

You can verify that the policy has been applied by navigating to **edge://policy**.

The error message *This policy is blocked - its value will be ignored* appeared while checking to see if the policy was applied via edge://policy. What's wrong?

This error occurs when you attempt to apply this policy to a nondomain joined device. Currently, the ConfigureViewInFileExplorer policy can only be applied to Windows

instances that are joined to a Microsoft Active Directory domain, Windows 10 Pro, or Enterprise instances enrolled for device management.

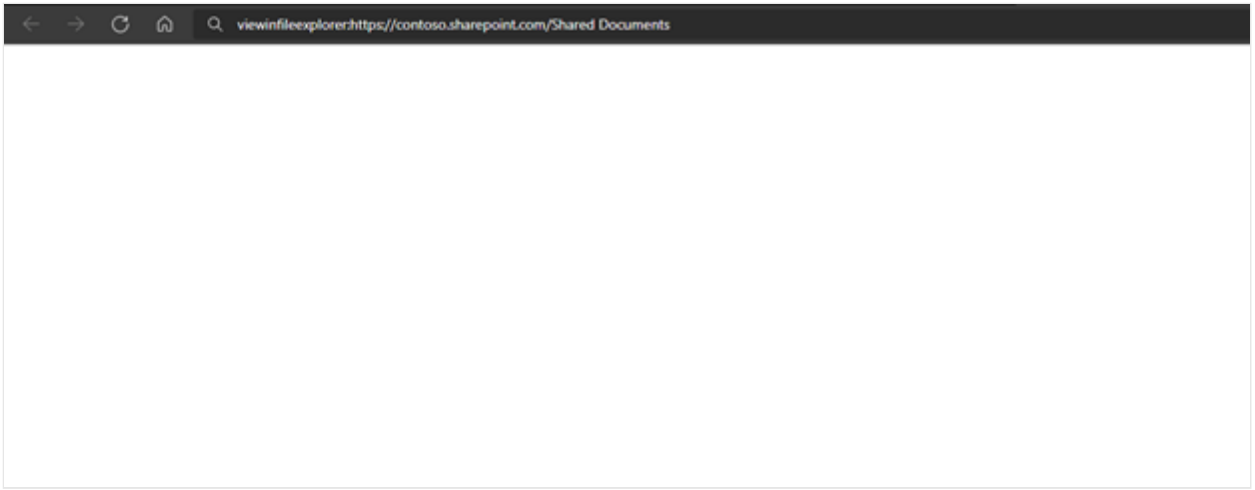


What happens if I have the policy applied without the tenant setting enabled?

If you don't enable ViewInFileExplorerEnabled via Set-SPOTenant, the View in File Explorer button won't appear in the interface of the SharePoint site.

What happens if the tenant setting is enabled without the Edge policy applied?

If you have enabled ViewInFileExplorerEnabled, you may see the View In File Explorer button appear in your SharePoint library, however, clicking the button results in a blank screen.



When running Set-SPOTenant -ViewInFileExplorerEnabled $True I received the error "The requested operation is part of an experimental feature that is not supported in the current environment". What's wrong?

You may receive this error if this functionality isn't supported in your current environment. We're still rolling out functionality to all Production environments and will update this article once worldwide rollout has been completed.

Learn More

- Sync SharePoint and Team files with your computer
- View and open SharePoint with File Explorer
- Troubleshoot View in File Explorer
- Set-SPOTenant

- OneDrive sync reports in the Apps Admin Center

Feedback

Was this page helpful? Yes No

Provide product feedback

Identify business requirements for SharePoint and OneDrive

Article • 02/21/2023

This article provides an overview of SharePoint and OneDrive capabilities that can help you determine how to best take advantage of these services you your organization. Use this information to help you plan your rollout and also to find new capabilities that your current solutions might not offer.

Best practices for requirements gathering

Define user journeys and core use cases. How do people in your organization collaborate now? Where do they store files? How do they share news and other information? An important part of planning for SharePoint and OneDrive is documenting how your organization does collaboration tasks today. You can then map those tasks to new processes using SharePoint and OneDrive. These tasks can then become test cases for your initial pilot rollout. For information about how Microsoft 365 improves productivity for different industries, see the Productivity Library.

Evaluate your migration needs. Most organizations have files and other content that they want to move to Microsoft 365. Some of this content may be in use every day by the people in your organization. Moving it all can take time. As you plan your rollout, plan for how you can migrate content while keeping the people in your organization productive. See Migration planning for SharePoint and OneDrive rollout for more information. If you use SharePoint Server on-premises, see Hybrid OneDrive and SharePoint in Microsoft 365. If you have paper records to import, see Introduction to Microsoft SharePoint Syntex.

Involve legal and compliance teams early. Most organizations have legal or compliance requirements around how they handle various kinds of data. Microsoft 365 offers many options to help you maintain compliance in your organization. As you plan your rollout, involve your legal or compliance team early in the process to help maintain your compliance requirements as you transition to SharePoint and OneDrive. See Create a compliant SharePoint and OneDrive environment for more information.

Drive agreement across stakeholders. Securing the participation and buy-in of key people within your organization is critical to successful user adoption. This support can come from business-focused leaders, IT leadership, or anyone else who has a vested interest in seeing Microsoft 365 succeed in the organization. It is important to have both executive or business leader support and product champions to help carry the

knowledge to their peers. Whether you're formally delegating the product champion role or allowing it to grow organically, champions are mission critical to user adoption.

Core SharePoint and OneDrive use cases

Core use cases for SharePoint and OneDrive include:

- File storage
- File collaboration
- Sites for team collaboration
- Sites for news and intranet

If you're currently using other software or services to enable these use cases in your organization, we recommend mapping each of your current use cases with the capabilities of SharePoint and OneDrive. This will help ensure a smooth transition as you roll SharePoint and OneDrive out and provide you with a list of process changes to communicate with your users. (Training and change management for rolling out SharePoint and OneDrive provides a list of resources that you can share with your users to help them get started with SharePoint and OneDrive.)

The sections below provide an overview of these use cases with links to more in-depth information.

File storage

The file storage options in Microsoft 365 are SharePoint and OneDrive.

Personal work files are stored in OneDrive. With OneDrive, each user has a location where they can store their personal work files. These files are not shared with anyone by default, but can be easily shared with others for collaboration.

Shared files are stored in SharePoint. SharePoint sites can be used to store files that will be accessed by multiple people. People who have access to the site have access to the files.

Microsoft Teams uses SharePoint sites to store files. When you upload a file to the Teams **Files** tab, it's stored in a SharePoint site. (For more information about how Teams and SharePoint interact, see Overview of Teams and SharePoint integration)

File collaboration

In SharePoint and OneDrive, user can use Microsoft 365 Apps (a version of Office that's available through many Microsoft 365 plans) to create and edit documents. Other applications can be used to create and edit other file types. These files can easily be shared with others - including people outside your organization (if you allow it).

Share OneDrive files using sharable links. In OneDrive, a user's files are private by default. Users can share OneDrive files with others by using *sharable links* which give others access to the file. Links can be created that grant access to particular people or to anyone in your organization. The person who shared the file can remove others' access by editing or deleting the link.

Collaborate in a site or team. In a SharePoint site or a Microsoft Teams team, all the members of the site or team have access to - and can easily collaborate on - the files stored there.

Share SharePoint files using sharable links. If a user needs to share a SharePoint file with someone outside the site or team, they can use sharable links in the same way that they do in OneDrive.

Sync files for offline access. With the OneDrive sync app, users can sync files between their computer and the Microsoft 365 cloud. When users add, change, or delete a file or folder locally, the file or folder is added, changed, or deleted in the cloud and vice versa. Users can work with synced files directly in File Explorer or Finder and the apps they use. Whenever the user is online, any changes that they or other users make will sync automatically.

For more details on file collaboration in SharePoint and OneDrive, see Intro to file collaboration in Microsoft 365, powered by SharePoint and File collaboration in SharePoint with Microsoft 365.

Intranet

One of the core capabilities of SharePoint is a wide variety of options and tools to create intranet sites for your organization. Your intranet might include your organization's main landing page, portals for corporate communications, and individual sites for departments or divisions (like IT or HR).

Moving your intranet to SharePoint in Microsoft 365 might take a while, particularly if you already have extensive intranet content. We recommend undertaking this task after you've completed your rollout of SharePoint and OneDrive.

For details about how to create an intranet using SharePoint, see Intelligent intranet introduction and roadmap and Plan an intelligent SharePoint intranet.

Governance and compliance

Governance and compliance are key for many organizations. As part of planning for SharePoint and OneDrive, consider which compliance features you want to roll out ahead of time. By having compliance features in place ahead of time, you can reduce the risk of compliance incidents. See Create a compliant SharePoint and OneDrive environment for details on which compliance features to consider as part of your SharePoint and OneDrive rollout.

Keys to successful user adoption

User adoption is important to the overall success of any new application or service. Ideally, to feel that you have maximized your investment in SharePoint and OneDrive, you need to maximize user engagement with them.

Creating awareness through awareness campaigns such as announcements, launch events, newsletters, town hall meetings, contests, and giveaways is a critical path to maximizing adoption. In addition, providing users with knowledge through classroom-style sessions and self-help guides helps them feel empowered to use OneDrive and SharePoint.

For more information about user adoption and change management when rolling out SharePoint and OneDrive, see Training and change management for rolling out SharePoint and OneDrive

Next steps

Plan for hybrid OneDrive and SharePoint

Related topics

Plan for SharePoint and OneDrive in Microsoft 365

Feedback

Was this page helpful? Yes No

Provide product feedback

Microsoft 365 pay-as-you-go terms of service

Article • 01/14/2025

Users can use consumption-based services for specific Microsoft 365 features by opting for pay-as-you-go billing through an Azure subscription. Here are the pricing details for the service(s).

When you link your Azure subscription to a service for pay-as-you-go billing in the Microsoft 365 admin center, you're billed on a pay-as-you-go basis for the service you set up. You can cancel or delete your subscription at any time to stop processing and billing.

In the future, new features using pay-as-you-go billing will be announced via a message center post. When the features become available, users in your organization will be able to take advantage of those capabilities. Pay as you go billing is disabled by default. A global admin or owner to the subscription can enable or disable Microsoft 365 pay-as-you-go features in the Microsoft 365 admin center.

Prerequisites for Microsoft 365 pay-as-you-go services

- Have an administrator role for the Microsoft 365 app. For instance, a SharePoint administrator role is necessary to configure pay-as-you-go billing for a SharePoint agents pay-as-you-go service.
- Have an owner or contributor Azure role to an Azure subscription to set up the pay-as-you-go service(s).
- Have an owner or contributor Azure role to an Azure resource group linked to the same Azure subscription to set up the pay-as-you-go service(s).

The organization's consumption of the pay-as-you-go service can be monitored at the Cost Management center for each of the Microsoft 365 pay-as-you-go services that you use. Billing for services is done through the Azure subscription that you associate to the service.

> **Note**
>
> Microsoft 365 pay-as-you-go is not available for Office 365 government plans or Office 365 operated by 21Vianet to and for PRC-located users.

Feedback

Was this page helpful? Yes No

Provide product feedback

Microsoft 365 Pay-as-you-go services pricing with Azure subscription

Article • 04/09/2025

When you use a Microsoft pay-as-you-go service linked to an Azure subscription, the service gets billed using the Azure subscription that you specified when you set up billing.

The following table describes the service, its pricing, and how it measures usage. When you connect your Azure subscription to the service you've set up for pay-as-you-go billing, users in your organization are able to take advantage of the service right away. Your tenant is billed according to the details shown in the following table:

Expand table

Service	What's Counted?	What's billed? (USD)
Agents in SharePoint	The number of messages used.	$0.01/message

> **Note**
>
> Each interaction includes a question and an answer. A successful interaction uses 32 messages.

Hybrid OneDrive and SharePoint in Microsoft 365

Article • 02/21/2023

If you use SharePoint Server on-premises, there are several options for integrating that environment with SharePoint in Microsoft 365 to provide your users with a more seamless environment when navigating back and forth between the two. You can configure these options to improve your users' experience during a migration from on-premises to the cloud, or you can use them in the long term if you plan to continue using SharePoint Server.

If you have a SharePoint Server environment, we recommend setting up SharePoint Server hybrid as part of your SharePoint and OneDrive in Microsoft 365 rollout. For complete details on setting up SharePoint and OneDrive hybrid, see Hybrid for SharePoint Server and Explore SharePoint Server hybrid.

Hybrid features

The following hybrid features are available for integrating SharePoint Server with Microsoft 365:

- **OneDrive** - OneDrive links are provided in SharePoint Server which direct users to OneDrive in Microsoft 365.
- **Site following** - Followed sites from both locations are consolidated in the SharePoint in Microsoft 365 followed sites list.
- **Profiles** - Profiles exist in both locations, but SharePoint Server links to users' profiles redirect to profiles in Microsoft 365.
- **Extensible app launcher** - The SharePoint Server app launcher includes several tiles that link to Microsoft 365.
- **Hybrid self-service site creation** - Users going to the default SharePoint Server site creation page are redirected to the Microsoft 365 Groups creation page, allowing them to create sites in SharePoint in Microsoft 365.
- **Search** - Cloud hybrid search crawls on-premises content and indexes it in the search index in Microsoft 365. Users can search the Microsoft 365 index from either location.

- **Taxonomy and content types** - Enables you to have a single taxonomy and content types list that spans SharePoint Server and SharePoint in Microsoft 365. See Plan hybrid SharePoint in Microsoft 365 taxonomy and hybrid content types for more information.

See SharePoint hybrid sites and search for more details on these options.

Hybrid OneDrive

If you currently use OneDrive or MySites in SharePoint Server, we highly recommend deploying hybrid OneDrive. With hybrid OneDrive, users are redirected from their on-premises OneDrive to OneDrive in Microsoft 365. Hybrid OneDrive allows for seamless navigation to OneDrive in the cloud from both SharePoint Server and Microsoft 365.

When you deploy hybrid OneDrive, the OneDrive links in the SharePoint Server ribbon and app launcher will point to OneDrive in Microsoft 365.

If you don't use OneDrive in SharePoint Server, but you do have an on-premises SharePoint environment, you may still want to consider deploying hybrid OneDrive. Doing so will update the OneDrive navigation links in SharePoint Server to point to OneDrive in Microsoft 365 – again, giving your users seamless navigation to OneDrive in the cloud from either location.

> **Important**
>
> If your users have files in on-premises OneDrive, they may have trouble accessing them unless they've bookmarked the old URL. It's important to have a migration plan for these files before you deploy hybrid OneDrive.

For more info about how to configure OneDrive in a hybrid scenario and how it works, see Plan hybrid OneDrive.

Next steps

Plan file sync

Related topics

Plan for SharePoint and OneDrive in Microsoft 365

Feedback

Was this page helpful? Yes No

Provide product feedback

Plan file sync for SharePoint and OneDrive in Microsoft 365

Even though users can upload, download, and interact with SharePoint and OneDrive files from a web browser, the ideal experience comes with the OneDrive sync app for Windows and Mac, and the iOS and Android mobile apps.

The OneDrive sync app has a variety of configuration options for compliance, performance, user experience, and disk space management. While these can be configured at any time, it's important to consider some of them as part of your rollout plan.

Key decisions for sync:

- How do you want to deploy the sync app?
- How do you want to manage sync on Windows computers?
- Which update ring do you want to use?
- Do you want to limit network utilization for sync?
- Do you want to sync commonly used folders with OneDrive
- Do you want to limit which organizations users can sync with?
- Do you want to allow users to sync their personal OneDrive?
- Do you want to prevent specific files or folders from being uploaded?
- Do you need to sync files in a hybrid environment with SharePoint Server?
- Do you want to limit sync to computers joined to a specific domain?

For information about the recommended configuration options for the sync app, see Recommended sync app configuration.

How do you want to deploy the sync app?

You have several different options for deploying the OneDrive sync app: manually, using scripting, using Windows Autopilot (for the sync app on Windows), using a mobile device management solution such as Intune, or using Microsoft Endpoint Configuration Manager.

The OneDrive sync app is included as part of Windows 10, Windows 11, and Office 2016 or higher. You do not need to deploy the sync app to devices running these, though you may need to update the sync app to the latest version.

To deploy the OneDrive sync app to Windows using Microsoft Endpoint Configuration Manager, see Deploy OneDrive apps by using Microsoft Endpoint Configuration Manager.

If you need to install the sync app on a single computer, see Install the sync app per machine.

For a full list of OneDrive sync app requirements, see OneDrive sync app system requirements.

How do you want to manage sync on Windows computers?

You can manage OneDrive sync app settings on Windows computers using Windows Group Policy or by using administrative templates in Intune. Using group policy requires that Windows computers be joined to an Active Directory domain. Using Intune requires that the device be managed by Microsoft Intune.

For information, see:

- Use OneDrive policies to control sync settings
- Use administrative templates in Intune

Mac settings are configured using .plist files. For information, see Deploy and configure the OneDrive sync app for Mac.

Which update ring do you want to use?

You can select how soon your users receive updates we release for the sync app.

- **Insiders ring** - In this ring, users get the first changes that are released to the public. We recommend selecting several people in your IT department to join this ring.
- **Production ring** – In this ring, users get fixes and new features in a timely fashion. We recommend leaving everyone else in the organization in this ring.
- **Enterprise ring** – In this ring, you have more control over the deployment of updates, but users have to wait longer to receive fixes and new features.

Configure the following policy to set the sync app update ring.

Expand table

Policy	Windows GPO	Mac
Set the sync app update ring	GPOSetUpdateRing	Tier

For details about the update process for the OneDrive sync app, see The OneDrive sync app update process.

Do you want to limit network utilization for sync?

Depending on your network capacity, you may want to consider limiting how much network bandwidth the sync app can use. This can be useful during a migration phase when large amounts of content are being synced.

Use the following policies to limit the network bandwidth used by the sync app.

Expand table

Policy	Windows GPO	Mac
Limit the sync app upload rate to a percentage of throughput	AutomaticUploadBandwidthPercentage	AutomaticUploadBandwidthPercentage
Enable automatic upload bandwidth management for OneDrive	EnableAutomaticUploadBandwidthManagement	N/A

Do you want to sync commonly used folders with OneDrive?

Users often save files to their documents folder or desktop. They may not realize that they should save these files in OneDrive. You can automatically sync these commonly used folders to OneDrive, prompt users to do so, or prevent them from doing so.

Use the following policies to configure how users commonly used folders are synced with OneDrive.

Expand table

Policy	Windows GPO	Mac
Silently move commonly used folders to OneDrive	KFMSilentOptIn	KFMSilentOptIn
Prompt users to move their commonly used folders to OneDrive	KFMOptInWithWizard	KFMOptInWithWizard
Prevent users from stopping sync of their commonly used folders to OneDrive	KFMBlockOptOut	KFMBlockOptOut
Prevent users from moving their commonly used folders to OneDrive	KFMBlockOptIn	KFMBlockOptIn

For more information about syncing commonly used folder with OneDrive, see Redirect and move Windows known folders to OneDrive and Redirect and move macOS Desktop and Documents folders to OneDrive.

Do you want to limit which organizations users can sync with?

By default, users can sync shared libraries from other organizations. You can limit this to specific organizations or disable it all together.

Use the following policies to configure which organizations users can sync with.

Expand table

Policy	Windows GPO	Mac
Allow syncing OneDrive accounts for only specific organizations	AllowTenantList	AllowTenantList
Block syncing OneDrive accounts for specific organizations	BlockTenantList	BlockTenantList
Prevent users from syncing libraries and folders shared from other organizations	BlockExternalSync	BlockExternalSync

For more information about syncing with other organizations, see B2B Sync.

Do you want to allow users to sync their personal OneDrive?

Depending on your governance practices, you can prevent users from syncing their personal OneDrive accounts to devices managed by your organization.

Use the following policies to specify if users can sync personal OneDrive accounts.

Expand table

Policy	Windows GPO	Mac
Prevent users from syncing personal OneDrive accounts	DisablePersonalSync	DisablePersonalSync

Do you want to prevent specific files or folders from being uploaded?

You can specify files or folders that the sync app should leave on the local device instead of uploading. Use the following policies to configure these exclusions.

Expand table

Policy	Windows GPO	Mac
Exclude specific kinds of files from being uploaded	EnableODIgnoreListFromGPO	EnableODIgnore
Exclude specific kinds of folders from being uploaded	EnableODIgnoreFolderListFromGPO	EnableODIgnoreFolders

File-type exclusions can also be configured in the SharePoint admin center. For more information, see Block syncing of specific file types.

Do you need to sync files in a hybrid environment with SharePoint Server?

If your organization uses SharePoint Server 2019 or SharePoint Server Subscription Edition, you can sync files using the OneDrive sync app. For information, see Configure syncing with the new OneDrive sync app.

If you are using the previous OneDrive sync app (Groove.exe), see Transition from the previous OneDrive for Business sync app for information on how to move to the new OneDrive sync app.

Do you want to limit sync to computers joined to a specific domain?

To make sure that users sync OneDrive files only on managed computers, you can configure OneDrive to sync only on PCs that are joined to specific domains. For more information, see Allow syncing only on computers joined to specific domains.

Next steps

Plan for content migration

Related topics

Plan for SharePoint and OneDrive in Microsoft 365

Last updated on 08/24/2026

Migration planning for SharePoint and OneDrive rollout

Article • 02/21/2023

A key task in deploying SharePoint and OneDrive for your organization is a plan to migrate your users' existing files. Depending on where these files are kept, there are several options, discussed below. You can choose one or more of these options depending on the number and location of files that you need to migrate.

The following types of data can be migrated with Microsoft tools:

- Files and folders (from on-premises or other cloud providers)
- SharePoint Server sites and content
- SharePoint Server 2010 workflows

We recommend that you have the people in your organization review the content that they're planing to migrate to SharePoint and OneDrive. There may be old content that isn't needed anymore and can be deleted or archived. This can help you save migration time and storage space in Microsoft 365.

Keep in mind that migrating content may result in a surge of network activity as large amounts of data is moved to SharePoint and OneDrive.

For complete information on migrating content to SharePoint and OneDrive, see Migrate your content to Microsoft 365.

Automation and workflows

If you have automated processes or workflows around files or other content, you may need to consider how to integrate those processes with Microsoft 365 or migrate them there entirely. Consider using SharePoint Framework solutions or Microsoft Power Platform.

If you have SharePoint Server 2010 workflows, you can migrate them to Power Automate by using the SharePoint Migration Tool. See Overview: Migrate SharePoint Server 2010 workflows to Power Automate for more information.

Hybrid

If you use SharePoint Server on-premises, you may want to set up a hybrid environment with SharePoint in Microsoft 365 while you migrate or as a long term solution. See

Hybrid OneDrive and SharePoint in Microsoft 365 for more information.

Migrating users' personal work files to OneDrive

As part of your rollout, you may be migrating your users' personal work files to OneDrive. As part of this process, you may need to pre-provision users' OneDrive libraries.

Normally, a user's OneDrive is created the first time they access OneDrive. If you will be migrating your users' files on their behalf before they begin using OneDrive, you'll need to pre-provision OneDrive for each of them. See Pre-provision OneDrive for users in your organization for details.

Files in on-premises OneDrive or MySites libraries

If users' existing files are in on-premises SharePoint Server, OneDrive, or MySites, you can use the SharePoint Migration Tool to migrate the files to Microsoft 365. For info, see Overview of the SharePoint Migration Tool (SPMT).

Files in users' commonly used folders

If user files are located in their Windows or Mac Desktop or Documents folders, you can move and redirect these locations to OneDrive. You can enable this feature during the initial rollout of OneDrive or sometime later. For more info, see Redirect and move Windows known folders to OneDrive and Redirect and move macOS Desktop and Documents folders to OneDrive.

Files in other local disk folders

If users have other work files in various locations on their computers, it's often easiest for them to manually move the files to OneDrive. After you deploy the OneDrive sync app to your users' computers, you can instruct them to move their work files to the OneDrive folder on their computer. For more information, see Move files from OneDrive to OneDrive for work or school.

Migrating sites from SharePoint Server to SharePoint in Microsoft 365

If you have sites in SharePoint Server, you can migrate them to SharePoint in Microsoft 365 by using the SharePoint Migration Tool. You can do this as part of your SharePoint and OneDrive rollout, or you can do it later. For details, see Overview of the SharePoint Migration Tool (SPMT).

Migrating files in file shares or hosted on other cloud providers

For files located in file shares or other cloud providers, you can use Migration Manager to migrate them to SharePoint and OneDrive. For details, see Migrate files shares to Microsoft 365 with Migration Manager.

See these references for specific instructions on how to migrate from different locations:

- Migrate from file shares
- Migrate from Box
- Migrate from Google Workspace
- Migrate from Dropbox
- Migrate from Egnyte
- Migrate SharePoint Server sites and content
- Migrate SharePoint Server workflows

Next steps

Create a compliant SharePoint and OneDrive environment

Related topics

Plan for SharePoint and OneDrive in Microsoft 365

Feedback

Was this page helpful? Yes No

Provide product feedback

Plan compliance requirements for SharePoint and OneDrive

Most organizations have business or legal requirements that govern how data is used, shared, and retained. Some organizations also have data residency requirements or regulatory requirements that restrict communication between certain users and groups.

Microsoft 365 has a wide range of governance and compliance features to address these needs. This article provides an overview of features you may want to consider as part of your OneDrive and SharePoint rollout.

Data lifecycle management

Use data lifecycle management capabilities in Microsoft Purview to govern your OneDrive and SharePoint content for compliance or regulatory requirements. The following table describes the capabilities to help you keep the content you need you and delete what you don't need.

Expand table

Capability	What problems does it solve?	Get started
Retention policies and retention labels Learn about retention for SharePoint and OneDrive	Retain or delete content with policy management for SharePoint and OneDrive documents	Create and configure retention policies Create retention labels for exceptions to your retention policies

Deleted users' data

When a user leaves your organization and you've deleted that user's account, what happens to the user's data? When considering data retention compliance, determine what needs to happen with the deleted user's data. For some organizations, retaining deleted user data could be important continuity and preventing critical data loss.

If a user's Microsoft 365 account is deleted, their OneDrive files are preserved for 30 days. To change this setting, Set the OneDrive retention for deleted users.

By default, when a user is deleted, the user's manager is automatically given access to the user's OneDrive. To change this, see OneDrive retention and deletion.

Information protection

Microsoft Purview Information Protection capabilities help you discover, classify, and protect sensitive information in OneDrive and SharePoint. The following table describes these capabilities. Consider if you want to implement any of these capabilities as part of your OneDrive and SharePoint rollout.

Expand table

Capability	What problems does it solve?	Get started
Sensitive information types	Identifies sensitive data by using built-in or custom regular expressions or a function. Corroborative evidence includes keywords, confidence levels, and proximity.	Customize a built-in sensitive information type
Trainable classifiers	Identifies sensitive data by using examples of the data you're interested in rather than identifying elements in the item (pattern matching). You can use built-in classifiers or train a classifier with your own content.	Get started with trainable classifiers
Sensitivity labels	A single solution across apps, services, and devices to label and protect your data as it travels inside and outside your organization. Sensitivity labels can be used to protect files themselves or individual SharePoint sites and teams.	Enable sensitivity labels for Office files in SharePoint and OneDrive Use sensitivity labels to protect content in Microsoft Teams, Microsoft 365 Groups, and SharePoint sites
Data loss prevention	Helps prevent unintentional sharing of sensitive items.	Get started with the default DLP policy

File sync

The OneDrive sync app has policies that you can use to help you maintain a compliant environment. Consider configuring these policies before you roll out SharePoint and OneDrive.

Expand table

Policy	Windows GPO	Mac
Allow syncing OneDrive accounts for only specific organizations	AllowTenantList	AllowTenantList
Block syncing OneDrive accounts for specific organizations	BlockTenantList	BlockTenantList
Prevent users from syncing libraries and folders shared from other organizations	BlockExternalSync	BlockExternalSync
Prevent users from syncing personal OneDrive accounts	DisablePersonalSync	DisablePersonalSync
Exclude specific kinds of files from being uploaded	EnableODIgnoreListFromGPO	EnableODIgnore
Exclude specific kinds of folders from being uploaded	EnableODIgnoreFolderListFromGPO	EnableODIgnoreFolders

Data residency

Multi-Geo is Microsoft 365 feature that allows organizations to span their storage over multiple geo locations and specify where to store users' data. For multinational customers with data residency requirements, you can use this feature to ensure that each user's data is stored in the geo location necessary for compliance. For more info about this feature, see Multi-Geo Capabilities in OneDrive and SharePoint.

Features such as file sync and mobile device management work normally in a multi-geo environment. There's no special configuration or management needed. The multi-geo experience for your users has minimal difference from a single-geo configuration. For details, see User experience in a multi-geo environment.

For more information about Microsoft 365 Multi-Geo, see Microsoft 365 Multi-Geo.

Information barriers

Microsoft Purview Information Barriers is a compliance solution that allows you to restrict two-way communication and collaboration between groups and users in Microsoft Teams, SharePoint, and OneDrive. Often used in highly regulated industries, information barriers can help to avoid conflicts of interest and safeguard internal information between users and organizational areas.

When information barrier policies are in place, users who shouldn't communicate or share files with other specific users won't be able to find, select, chat, or call those users. Information barrier

policies automatically put checks in place to detect and prevent unauthorized communication and collaboration among defined groups and users.

If your business requires information barriers, see Learn about information barriers and Use information barriers with SharePoint to get started.

Next steps

Plan sharing and collaboration options

Related topics

Plan for SharePoint and OneDrive in Microsoft 365

B2B Sync

Implement compliance in Microsoft 365

Protect your enterprise data using Windows Information Protection (WIP)

Control OneDrive and SharePoint access based on network authentication or app

---

Last updated on 08/19/2026

Plan and deploy a file collaboration environment - SharePoint

By using Microsoft 365 services, you can create a secure and productive file collaboration environment for your users. SharePoint powers much of this environment, but the capabilities of file collaboration in Microsoft 365 go beyond the traditional SharePoint site. Teams, OneDrive, and various governance and security options all play a role in creating a rich environment where users can collaborate easily and where your organization's sensitive content remains secure.

In the following sections, you find the options and decisions that you as an administrator should consider when setting up a collaboration environment:

- How SharePoint relates to other collaboration services in Microsoft 365, including OneDrive, Microsoft 365 Groups, and Teams.
- How you can create an intuitive and productive collaboration environment for your users.
- How you can protect your organization's data by managing access through permissions, data classifications, governance rules, and monitoring.

This article is part of the broader Microsoft 365 collaboration story:

- Secure collaboration with Microsoft 365
- Collaboration governance
- Meetings, webinars, and live events

Download the Microsoft Teams and related productivity services in Microsoft 365 for IT architects poster and refer to it while you read this article. This poster provides detailed illustrations of how the collaboration services in Microsoft 365 relate to each other and interact.

Creating a successful collaboration experience

Choose technical implementation options for file collaboration in Microsoft 365 that balance what can seem to be contradictory requirements:

- Protecting your intellectual property
- Enabling self-service
- Creating a smooth user experience

Protecting your intellectual property

Several options discussed later in this article can help you protect your intellectual property. These options include limiting who can share files, applying governance policies by using sensitivity labels, and managing the devices that users use to access content.

Consider a balanced approach when choosing options:

A configuration that allows users to share content freely can lead to accidental sharing of confidential data. However, a user experience that's difficult to use or too restrictive can lead to users finding alternative collaboration options that circumvent your governance policies, ultimately leading to even greater risk.

By using a combination of features – depending on the sensitivity of your data – you can create a collaboration environment that's easy to use and provides the security and auditing controls that you need.

Enabling self-service

In Microsoft 365, allow users to create Teams, Microsoft 365 Groups, and SharePoint sites as needed. Use sensitivity labels to enforce permissions governance, take advantage of compliance features that protect your content, and use expiration and renewal policies to make sure unused sites don't accumulate.

By choosing options that favor user self-service, you can minimize the impact on your IT staff while creating an easier experience for your users.

Creating a smooth user experience

The key to creating a smooth user experience is to avoid creating barriers for your users that they don't understand or that they must escalate to your help desk. For example, turning external sharing off for a site might cause user confusion or frustration. Labeling the site and its contents as confidential and using data loss prevention policy tips and emails to educate your users in your governance policies can lead to a smoother experience for them.

SharePoint, Microsoft 365 Groups, and Teams

In SharePoint in Microsoft 365, each SharePoint team site is part of a Microsoft 365 group. A Microsoft 365 group is a single permissions group that's associated with various Microsoft 365 services, including a SharePoint site, an instance of Planner, a mailbox, a shared calendar, and others. When you add owners or members to the Microsoft 365 group, they get access to the SharePoint site along with the other connected services.

While you can continue to manage SharePoint site permissions separately by using SharePoint groups, manage permissions for SharePoint by adding people to or removing them from the associated Microsoft 365 group. This approach provides easier administration and gives users access to a host of related services that they can use for better collaboration.

Microsoft Teams provides a hub for collaboration by bringing together all the Microsoft 365 group-related services, plus various Teams-specific services, in a single user experience with persistent chat. Teams uses the associated Microsoft 365 group to manage its permissions. Within the Teams experience, users can directly access SharePoint along with the other services without having to switch applications. This approach provides a centralized collaboration space with a single place to manage permissions. Teams uses the SharePoint site that is connected to the Microsoft 365 group for files in standard channels and creates separate SharePoint sites for each private or shared channel. For collaboration scenarios in your organization, use Teams rather than using services such as SharePoint independently.

For details about how SharePoint and Teams interact, see Overview of Teams and SharePoint integration and Manage settings and permissions when SharePoint and Teams are integrated.

Collaboration in client applications

Office applications such as Word, Excel, and PowerPoint provide a wide variety of collaboration features, including coauthoring and @mentions. These applications also integrate with sensitivity labels and data loss prevention (discussed later).

Deploy Microsoft 365 Apps for enterprise. Microsoft 365 Apps for enterprise provides an always up-to-date experience for your users, with the latest features and updates delivered on a schedule that you can control.

For details about deploying Microsoft 365 Apps for enterprise, see Deployment guide for Microsoft 365 Apps.

OneDrive libraries

While SharePoint provides shared libraries for shared files that teams can collaborate on, users also have an individual library in OneDrive where they can store files that they own.

When a user adds a file to OneDrive, that file isn't shared with anyone else. OneDrive provides the same sharing capabilities as SharePoint, so users can share files in OneDrive as needed.

A user's individual library can be accessed from Teams, and from the OneDrive web interface and mobile application.

On devices running Windows or macOS, users can install the OneDrive sync app to sync files from both OneDrive and SharePoint to their local disk. This sync app allows them to work on files offline and also provides the convenience of opening files in their native application (such as Word or Excel) without the need of going to the web interface.

The two main decisions to consider for using OneDrive in collaboration scenarios are:

- Do you want to allow Microsoft 365 users to share files in OneDrive with people outside your organization?
- Do you want to restrict file sync in any way – such as only to managed devices?

You can configure these settings in the SharePoint admin center.

Securing your data

A significant part of a successful collaboration solution is making sure your organization's data remains secure. Microsoft 365 provides various features to help you keep your data secure while enabling a seamless collaboration experience for your users.

To help protect your organization's information, you can:

- **Control sharing** by configuring sharing settings for each site that are appropriate to the type of information in the site, you can create a collaboration space for users while securing your intellectual property.
- **Classify and protect information** by classifying the types of information in your organization, you can create governance policies that provide higher levels of security to information that is confidential compared to information that is meant to be shared freely.
- **Manage devices** with device management, you can control access to information based on device, location, and other parameters.
- **Monitor activity** by monitoring the collaboration activity happening in Teams and SharePoint, you can gain insights into how your organization's information is being used. You can also set alerts to flag suspicious activity.
- **Protect against threats** by using policies to detect malicious files in SharePoint, OneDrive, and Teams, you can help ensure the safety of your organization's data and network.

These options are discussed in more detail in the following sections. Depending on the needs of your organization, choose the options that give you the best balance of security and usability. If you're in a highly regulated industry or work with highly confidential data, you might want to put more of these controls in place. If your organization's information isn't sensitive, you might want to rely on basic sharing settings and malicious file alerts.

Control sharing

The sharing settings that you configure for SharePoint and OneDrive determine who your users can collaborate with, both inside and outside your organization. Depending on your business needs and the sensitivity of your data, you can:

- Disallow sharing with people outside your organization.
- Require people outside your organization to authenticate.
- Restrict sharing to specified domains.

You can configure these settings for the entire organization, or for each site independently (except private or shared channel sites). For detailed information, see Turn sharing on or off and Turn sharing on or off for a site.

For more guidance about sharing with people outside your organization, see Limit accidental exposure to files when sharing with guests.

When users share files and folders, they create a shareable link that has permissions to the item. There are three primary link types:

- *Anyone* links that work for anyone and don't require sign-in
- *People in your organization* links that work for users in your organization
- *Specific people* links that work for the people specified when the link is created

For more information about these link types, see How shareable links work in OneDrive and SharePoint in Microsoft 365.

Unauthenticated access with *Anyone* links

Anyone links are a great way to easily share files and folders with people outside your organization. However, if you're sharing sensitive information, this option might not be the best choice.

If you require people outside your organization to authenticate, users can't use *Anyone* links and you can audit guest activity on shared files and folders.

Though *Anyone* links don't require people outside your organization to authenticate, you can track the usage of *Anyone* links and revoke access if needed.

If you want to allow *Anyone* links, several options provide a more secure sharing experience.

You can restrict *Anyone* links to read-only. You can also set an expiration time limit, after which the link stops working.

Another option is to configure a different link type to be displayed to the user by default. This option can help minimize the chances of inappropriate sharing. For example, if you want to allow *Anyone* links but are concerned that they only be used for specific purposes, you can set the default link type to *Specific people* links or *People in your organization* links instead of *Anyone* links. Users must then explicitly select *Anyone* links when they share a file or folder.

You can also use data loss prevention to restrict *Anyone* link access to files that contain sensitive information.

People in your organization links

People in your organization links are a great way to share information within your organization. *People in your organization* links work for anyone in your organization, so users can share files and folders with people who aren't part of a team or members of a site. When redeemed, the link gives access to the particular file or folder and can be passed around inside the organization. This access allows for easy collaboration with stakeholders from groups that might have separate teams or sites – such as design, marketing, and support groups.

Creating a *People in your organization* link doesn't make the associated file or folder appear in search results, be accessible via Copilot, or grant access to everyone within the organization. Simply creating this link doesn't provide organizational-wide access to the content. For individuals to access the file or folder, they must possess the link and activate it through redemption. A user redeems the link by clicking on it, or in some instances, the link might be automatically redeemed when sent to someone via email, chat, or other communication methods. The link doesn't work for guests or other people outside your organization.

Specific people links

Specific people links are best for circumstances where users want to limit access to a file or folder. The link only works for the person specified and they must authenticate in order to use it. These links can be internal or external (if you enable guest sharing).

Classify and protect information

Microsoft Purview Data Loss Prevention provides a way to classify your teams, groups, sites, and documents, and to create a series of conditions, actions, and exceptions to govern how they're used and shared.

By classifying your information and creating governance rules around them, you can create a collaboration environment where users can easily work with each other without accidentally or intentionally sharing sensitive information inappropriately.

With data loss prevention policies in place, you can be relatively liberal with your sharing settings for a given site and rely on data loss prevention to enforce your governance requirements. This approach provides a friendlier user experience and avoids unnecessary restrictions that users might try to work around.

For detailed information about data loss prevention, see Learn about data loss prevention.

Sensitivity labels

Sensitivity labels provide a way to classify teams, groups, sites, and documents with descriptive labels that you can use to enforce a governance workflow.

Using sensitivity labels helps your users share information safely and maintain your governance policies without needing to become experts in those policies.

For example, you could configure a policy that requires Microsoft 365 groups classified as confidential to be private rather than public. In such a case, a user creating a group, team, or SharePoint site would only see the **private** option when they choose a classification of confidential. For information about using sensitivity labels with teams, groups, and sites, see Use sensitivity labels to protect content in Microsoft Teams, Microsoft 365 groups, and SharePoint sites.

Conditions and actions

By using data loss protection conditions and actions, you can enforce a governance workflow when a given condition is met.

Examples include:

- If customer information is detected in a document, users can't share that document with guests.
- If a document contains the name of a confidential project, guests can't open the document even if it is shared with them.

For more information, see Learn about data loss prevention.

Conditional access

Microsoft Entra Conditional Access provides extra controls to prevent users from accessing your organization's resources in risky situations, such as untrusted locations or devices that aren't up to date.

Examples include:

- Block guests from signing in from risky locations.
- Require multifactor authentication for mobile devices.

Create access policies specifically for guests to mitigate risk for people who most likely have unmanaged devices.

For detailed information, see What is Conditional Access?.

Monitoring with reports

Microsoft 365 offers a variety of reports to help you monitor site usage, document sharing, governance compliance, and a host of other events.

For information about how to view reports on SharePoint site usage, see Microsoft 365 Reports in the Admin Center - SharePoint site usage.

For information about how to view data loss prevention reports, see View the reports for data loss prevention.

For information on reports that can help you monitor content sharing, see Data access governance reports for SharePoint sites.

Related articles

Create a secure guest sharing environment

Best practices for sharing files and folders with unauthenticated users

Microsoft SharePoint - SharePoint Advanced Management overview

---

Last updated on 05/07/2026

Sharing and permissions in the SharePoint modern experience

Article • 10/09/2024

Traditionally, SharePoint permissions have been managed through a set of permissions groups within a site (Owners, Members, Visitors, etc.). In SharePoint in Microsoft 365, this remains true for some types of sites, but additional options are available and SharePoint is part of a much broader set of capabilities for secure collaboration with Microsoft 365.

The main types of sites in SharePoint are:

- **Team sites** - Team sites provide a collaboration environment for your teams and projects. Each team site, by default, is part of a Microsoft 365 group, which includes a mailbox, shared calendar, and other collaboration tools. Team sites may also be part of a team in Microsoft Teams. Permissions for team sites are best managed through the associated Microsoft 365 group or Teams team.
- **Channel sites** - Channel sites are team sites that are associated with a specific channel in a Teams team. Both private and shared channels create separate SharePoint sites just for the channel.
- **Communication sites** - Communication sites are for broadcasting news and status across the organization. Communication site permissions are managed by using the SharePoint Owners, Members, and Visitors groups for the site.
- **Hub sites** - Hub sites are team sites or communication sites that the administrator has configured as the center of a hub. They're designed to provide connection between related sites through shared navigation. Permissions for hub sites can be managed through the Owners, Members, and Visitors groups, or through the associated Microsoft 365 group if there is one. Special permissions are needed to associate sites to a hub.

Team site permissions and Microsoft 365 Groups

By default, each SharePoint team site is part of an Microsoft 365 group. A Microsoft 365 group is a single permissions group that is associated with various Microsoft 365 services. This includes a SharePoint site, an instance of Planner, a mailbox, a shared calendar, and others.

When you add owners or members to the Microsoft 365 group, they're given access to the SharePoint site along with the other group-connected services. Group owners become site owners, and group members become site members.

It's possible to manage SharePoint site permissions separately from the Microsoft 365 group by using SharePoint groups, unless it's a channel site. (We recommend against this for the simplest management experience.) In such a case, group members will continue to have access to the site, but users added directly to the site won't have access to any of the group services. Microsoft 365 groups don't have view-only access, so any users you wish to have view permissions on the site must be added directly to the Visitors group on the site.

Using team sites with Teams

Microsoft Teams provides a hub for collaboration by bringing together various services including a SharePoint team site. Within the Teams experience, users can directly access SharePoint along with the other services. Each team is associated with a Microsoft 365 group and Teams uses that group to manage its permissions.

For scenarios where a SharePoint site is used with Teams, we recommend doing all permission management through Teams. As with Microsoft 365 groups, team owners become site owners and team members become site members.

For private or shared channel sites, permission management must be done in Teams. Channel owners become sites owners in SharePoint and channel members become site members. Permissions in SharePoint can't be managed separately and will display in read-only mode.

For details about how SharePoint and Teams interact, see Overview of Teams and SharePoint integration and Manage settings and permissions when SharePoint and Teams are integrated.

Communication site permissions

Communication sites aren't connected to Microsoft 365 groups and use the standard SharePoint permissions groups:

- Owners
- Members
- Visitors

Normally with communication sites, you'll have one or more owners, a relatively small number of members who create the content for the site, and a large number of visitors who are the people you're sharing information with.

You can give people permissions to the site by adding individual users, security groups, or Microsoft 365 groups to one of the three SharePoint groups. (Nested security groups can cause performance issues and are not recommended.)

If a communication site is used by members of a team in Teams, you may want to add the Microsoft 365 group associated with the team to the members group of the communication site. This will allow members of the team to create content in the communication site.

The visitors group is a good place to use security groups. In many organizations, this is the easiest way to add large numbers of users to a site.

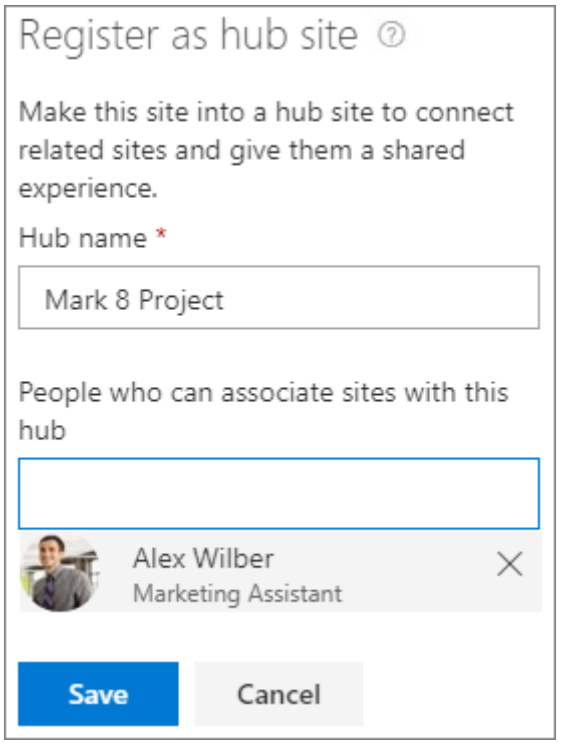
For information about how to share a site, see Share a site .

Hub site permissions

Managing the permissions of a hub site is dependent on the underlying type of site. If the site is a group-connected team site, then you should manage permissions through the Microsoft 365 group. If it's a communication site, then you should manage permissions through the SharePoint groups.

Hub site owners define the shared experiences for hub navigation and theme. Hub site members create content on the hub as with any other SharePoint site. Owners and members of the sites associated with the hub create content on their individual sites.

The SharePoint Administrator must specify which users can connect other sites to the hub. This is done in the SharePoint admin center and cannot be changed by site owners.



Shareable links

Giving people permissions to a site, group, or team gives them access to all site content. If you want to share an individual file or folder, you can do so with shareable links. There are three primary link types:

- *Anyone* links give access to the item to anyone who has the link, including people outside your organization. People using an *Anyone* link don't have to authenticate, and their access can't be audited. *Anyone* links can't be used with files in a Teams shared channel site.
- *People in your organization* links work for only people inside your Microsoft 365 organization. (They don't work for guests or external participants in Teams shared channels).
- *Specific people* links only work for the people that users specify when they share the item. For files in a Teams shared channel site, *specific people* links can't be sent to people outside the organization unless they're in the channel.

You can change the type of link that is presented to users by default for each site.

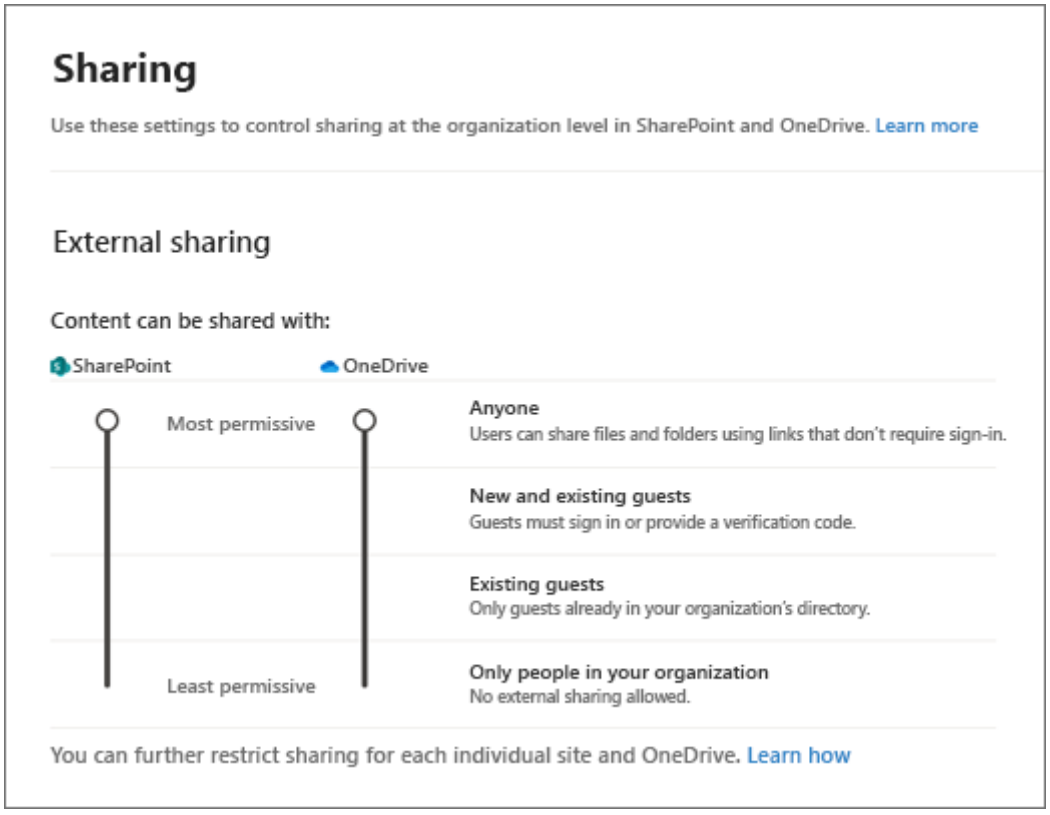
For more about the different types of sharing links, see Securing your data.

Guest sharing

The external sharing features of SharePoint let users in your organization share content with people outside the organization (such as partners, vendors, clients, or customers).

Planning for external sharing should be included as part of your overall permissions planning for SharePoint.

SharePoint has external sharing settings at both the organization level and the site level (previously called the "site collection" level). To allow external sharing on any site, you must allow it at the organization level. You can then restrict external sharing for other sites.



Whichever option you choose at the organization or site level, the more restrictive functionality is still available. For example, if you choose to allow sharing using *Anyone* links, users can still share with guests, who sign in, and with internal users.

External sharing is turned on by default for your organization. Default settings for individual sites vary depending on the type of site. See Site level settings for more information.

Shared channels in teams do not use guest accounts for sharing with people outside the organization. However, external sharing must be enabled for people outside the organization to be invited to shared channels.

To set up guest sharing for a site, see Collaborate with guests in a site.

Security and privacy

If you have confidential information that should never be shared externally, we recommend storing the information in a site that has external sharing turned off. Create

additional sites as needed to use for external sharing. This helps you to manage security risk by preventing external access to sensitive information.

SharePoint and OneDrive integration with Microsoft Entra B2B

Microsoft Entra B2B collaboration provides authentication and management of guests. Authentication happens via one-time passcode when they don't already have a work or school account or a Microsoft account (MSA).

With SharePoint and OneDrive integration with Microsoft Entra B2B, the Azure B2B collaboration one-time passcode feature is used for external sharing of files, folders, list items, document libraries, and sites. (Shared channels in Teams don't use Azure B2B collaboration, but rather Azure B2B direct connect.)

Related topics

External sharing overview

Manage sharing settings

Collaborating with people outside your organization

Share SharePoint files or folders

Limit sharing in Microsoft 365

Shared channels in Microsoft Teams

Microsoft 365 guest sharing settings reference

Feedback

Was this page helpful? Yes No

Provide product feedback

Manage Permission Scopes in SharePoint

Article • 02/11/2025

Effectively managing permissions in SharePoint is essential for security and proper user access. As the number of documents in SharePoint sites increases, poor design and implementation can quickly lead to permission scope limits, negatively affecting performance. This article explains permission scopes and access control mechanisms, offering best practices for designing and managing permission scopes efficiently within SharePoint. First, let's review some key components related to permission scopes.

Key concepts and components

- Access Control List—An Access Control List (ACL) is composed of a set of Access Control Entries (ACEs).
- Access Control Entry—An Access Control Entry (ACE) in SharePoint is a combination of a principal and a rights mask (read, read/write).
- Principal—A principal can be an individual user or a group. If a group is present in an ACE within an ACL, all members of that group are granted the permission level specified by the ACE.
- Permission scope—A permission scope is a uniquely secured object. This means that its ACL can be set differently from its parent. Files and folders can have the same permissions if they're all part of the same directory tree. You can have up to 50,000 unique ACLs within a document library, but for best performance it's recommended that you keep it under 5,000.
- Permission inheritance—By default, a site collection contains multiple sites. Each site can have one or more lists and document libraries, all of which inherit their permissions from the site collection. Similarly, folders, lists, and documents inherit permissions from the parent object that contains them. For more information, see Customize permissions for a SharePoint list or library.
- Unique permissions—By default, a file or folder inherits the permissions of the library or folder that contains it. When a file is assigned "unique permissions," it stops inheriting permissions from its parent and can have its permissions set independently. This means that the file or folder now has its own permission scope.

Permission scope and permission inheritance

In SharePoint, ACLs are used to manage permissions for objects (files and folders). Each ACL consists of multiple ACEs, which specify the permissions for a principal.

When a document library is created, it has a single permission scope, meaning all files and folders within the document library inherit their ACL from the root of the document library and share the same permissions. The initial scope count is 1.

Breaking inheritance

Breaking inheritance on a file or folder creates a new permission scope, increasing the scope count by 1.

You can break the inheritance using two methods:

- You can break inheritance manually by going to the settings of the library.
- If you share a file or folder, this action breaks permission inheritance on the file or folder, allowing its ACL (and the content within the folder) to differ from its parent.

This article discusses the implications of breaking inheritance using the second method and outlines best practices for minimizing the addition of excessive scope counts in a library.

For example, if you create a document library, then make a folder, share the folder (which breaks inheritance), and upload 75,000 files to the folder, the document library's scope count is 2. This is because all 75,000 files in the folder share the folder's permission scope and therefore its ACL. There are only two unique ACLs in the document library: the ACL at the root and the ACL on the folder. If you create multiple files and share each one individually with a user, you add a scope count each time. To avoid this, put all the files in the same folder and share the folder instead.

Sharing folders with large item counts

A folder can only break its inheritance if it has 100,000 or fewer items. If a folder exceeds this limit and isn't uniquely shared, it can't be uniquely shared later. Therefore, share large folders before they hit 100,000 items. Ideally, share a folder when it contains zero items if you know it needs unique sharing.

Shared ACLs for files with inherited permissions

If two files have the equivalent ACL because they both inherit from the parent folder, then they share an ACL. Only the parent folder counts. However, if two files have the

same ACL because they were shared separately with the same principals, they'll have two permission scopes with identical permissions.

Impact of breaking inheritance on scope count

If a folder has two files in it and you share them both with a user, that will cost you three scopes: one for the parent folder and one for each of the files that was shared individually. It doesn't matter that you shared both files with the user and the ACLs of the files are identical. Once you break the inheritance of a file or folder from its parent, you create a unique scope.

Efficient sharing to avoid exceeding scope limits

If you have 10,000 files that you want to share with a user and you share each file individually, that will cost 10,000 scopes, degrading performance as you have exceeded the recommended 5,000 limit. However, if you make a folder, share the folder with the user, and then move all 10,000 files into that folder, it will only cost you one additional scope (for the folder). If you had previously shared each of those 10,000 files individually, one by one, and move them to a common folder that has an identical ACL, you would have still exceeded the limit (the system doesn't "clean up" these permissions on your behalf by restoring permission inheritance).

Understanding the scope limit

The recommended 5,000 limit for ACLs means you can have up to 5,000 unique ACLs. It doesn't mean you can only have 5,000 files or folders with ACLs. If two files inherit the same ACL from their parent folder, they share that ACL. In this case, only the parent folder's ACL counts towards the limit. However, if two files have the same ACL, but it's explicitly set, not via inheritance from their parent folder, each file’s ACL, plus the parent folder’s ACL, counts towards the limit. Actual performance can vary depending on factors like the size of the ACLs. If the ACLs are small (fewer than 10 ACEs per ACL), you can exceed 5,000 scopes without encountering issues. However, with larger ACLs (up to 5,000 ACEs), you might experience performance problems before reaching the limit.

Example scenarios

Scenario: Sharing files

Sharing two files in a folder with a single user uses three scopes: one for the parent folder and one for each of the two files. Even though both files are shared with the same user and have the same ACL, breaking inheritance from the parent folder creates unique scopes. Therefore, if you have 10,000 files to share with the user and share each one individually, it requires 10,000 additional scopes. However, if you place all the files into a single folder, share that folder with the user, and then move the files into the folder, it will only require one additional scope for the folder. One important point to consider is co-authoring. If a user is working on a file in Microsoft Word and wants to co-author with someone, they can still invite them if the file is in SharePoint. Doing so uses one of the remaining ACLs available. This is an additional factor to consider.

Scenario: Moving files

Imagine a situation where 10,000 files have been shared with an individual one by one. If these files are later moved into a single folder, the system doesn't automatically consolidate the permission entries to apply only the folder's permissions. Instead, the permissions remain cluttered unless the user manually corrects them. This is because automatic restoration of the permission hierarchy isn't implemented due to security concerns. In this scenario, before the files are moved, the recipient can view each of the 10,000 files individually shared with them. After moving the files into a folder, the recipient can still see the 10,000 files along with the containing folder, which changes the access structure. This means that without manual cleanup, extensive sharing from one's OneDrive could lead to performance issues or even operational failure once the limit of 50,000 items is reached. However, careful management, where files are organized into folders with matching ACLs, can help mitigate these issues. It's also important to note that exposing the actual folder hierarchy to users might be undesirable, especially when using metadata to represent everything instead of traditional folders.

Scenario: Creating a document library with minimal scopes

You create a document library that has a single permission scope, meaning that all items within it initially share the same access control settings. Next, you add a folder to this document library. To share this folder with specific individuals or groups, you break the inheritance of permissions from the document library. This action creates a new, unique permission scope for the folder, allowing you to set different access controls than those applied to the document library. With the folder's permissions set, you proceed to upload 75,000 files into this folder. Each of these files inherits the folder's ACL, ensuring that they all have the same permissions as the folder itself. As a result, the document

library now has two unique permission scopes: one for the root of the document library and another for the folder. This setup allows for more granular control over who can access the files within the folder, while maintaining a simpler permission structure for the rest of the document library.

Scenario: Managing permissions for multiple folders

To efficiently map categories to folders, you decide to create 20 folders within each document library. Each of these folders is designated for a specific type of document, such as contracts or invoices, allowing for better organization and easier access. To ensure that each folder has its own unique permissions, you set up individual ACL settings for each one. This results in a total of 21 unique permission scopes within the document library: one for the root of the document library and one for each of the 20 folders. By doing this, you can control who has access to each category of files, providing a more secure and organized structure. To avoid performance issues and stay within the system's limits, you minimize the number of individual files with unique permissions. This means that the majority of files inherit the permissions of their respective folders, keeping the total number of unique permission entries well within the 5,000 limit.

Tips for managing permission scopes

To effectively manage permission scopes in SharePoint, follow these recommendations:

- Minimize the number of unique permission scopes by leveraging inheritance.
- Share folders instead of individual files to reduce the number of unique scopes.
- Ensure folders that need unique permissions are shared before they exceed 100,000 items.
- For developers, regularly review and minimize unique permission scopes, use groups, and monitor performance to maintain optimal SharePoint performance.
- For end users, use default permission groups, review access requests, and conduct regular audits to keep SharePoint permissions clean and efficient.
- Use SharePoint groups and Microsoft Entra for managing user references and permissions efficiently.

Resources

- SharePoint Limits - Service Descriptions

Feedback

Was this page helpful? Yes No

Provide product feedback

Plan sharing and collaboration options in SharePoint and OneDrive

Article • 02/21/2023

SharePoint and OneDrive provide a platform for collaboration through file and folder storage and sharing.

As you plan your SharePoint and OneDrive rollout, these are the primary decision areas around collaboration:

- **Site creation** - do you want to allow your users to create SharePoint sites or do you want to manage this through IT or a business process?
- **External sharing** - do you want to allow users to share files, folders, or sites with people outside your organization?
- **File and folder sharing defaults** - what sharing defaults do you want to use to make sharing easy while you help protect sensitive information?

For details about collaboration governance in Microsoft 365, see What is collaboration governance?.

For an in-depth look at file collaboration in SharePoint, see Intro to file collaboration in Microsoft 365, powered by SharePoint and File collaboration in SharePoint with Microsoft 365.

Keep in mind that the settings you choose for collaboration in SharePoint can also affect Teams. For more information, see Overview of Teams and SharePoint integration.

Site creation and lifecycle

By default, users can create new team sites and communication sites in SharePoint and shared libraries in OneDrive. We recommend keeping this setting and using expiration policies to manage the number of unused sites.

If you don't want to allow users to create sites directly, you can disable user site creation. For details, see Manage site creation in SharePoint.

Even if you turn off sites creation for users in SharePoint, they can still create Microsoft 365 group-connected team sites by creating a Microsoft 365 group or any of its related services, such as a team in Microsoft Teams. If you don't want to allow users to create Microsoft 365 Groups or related services, including group-connected team sites, see Manage who can create Microsoft 365 Groups.

As part of your SharePoint rollout, we recommend that you create your own custom guidance for SharePoint site owners on how sites are set up and managed in your organization. See Create guidelines for site usage for more information.

External sharing

External sharing in SharePoint and OneDrive uses Microsoft Entra B2B collaboration to create guest accounts for people outside the organization. Guests can be given access to SharePoint sites or to individual files and folders in SharePoint and OneDrive.

External sharing is enabled by default in Microsoft 365, including SharePoint and OneDrive. We recommend leaving external sharing enabled. Microsoft 365 external sharing options can provide a more secure and governable sharing environment than sending attachments through email or using consumer sharing services.

Use the Sharing page in the SharePoint admin center to configure your sharing options. For details, see Manage sharing settings.

For details about how to configure guest collaboration in SharePoint sites, see Collaborate with guests in a site.

Organization level sharing settings

The organization level sharing settings for SharePoint and OneDrive provide a default setting for sites and OneDrive libraries. Individual sites can be locked down further, but cannot be made more permissive than, the organizational settings.

A key decision for your SharePoint and OneDrive rollout is who content can be shared with:

- **Anyone** - Users can share files and folders using links that don't require sign-in.
- **New and existing guests** - Guests are added to the directory when an item is shared and must sign in or provide a verification code to access the content.
- **Existing guests** - Users can only share with guests already in your organization's directory. (This setting is not recommended because guests can be added to the directory in various ways outside of SharePoint and OneDrive.)
- **Only people in your organization** - No external sharing is allowed.

These settings can be set separately for SharePoint and OneDrive, though the OneDrive setting cannot be more permissive than the SharePoint setting.

Important decisions:

- Do you want to allow external sharing? If not, choose the **Only people in your organization** option.
- Do you want to allow users to create sharing links that allow unauthenticated (anonymous) people to access files or folders? If so, choose **Anyone**.

External sharing restrictions

You can restrict external sharing with these options:

- Restrict which domains users can share with.
- Limit external sharing to people in a specific security group.
- Expire guest access after a specified period.
- Require reauthentication after a specified period for users using a verification code.

If you want to restrict which domains users can share with, you can choose the **Limit external sharing by domain** setting. For details, see Restrict sharing of SharePoint and OneDrive content by domain. Note that this setting only affects SharePoint and OneDrive. If you want to set this for all the services in Microsoft 365, you can configure the restriction in Microsoft Entra ID. See Allow or block invitations to B2B users from specific organizations for details.

If you don't want all of your users to be able to share externally, you can restrict external sharing to specific security groups. Choose the **Allow only users in specific security groups to share externally** option and choose the groups you want to allow.

If you want guest access to expire after a given period, use the **Guest access to a site or OneDrive will expire automatically after this many days** setting. The users who shared the content will have the option to extend the expiration by the period you specify before guests lose access. For more information see, Manage guest expiration for a site.

Guests with non-Microsoft email addresses, such as Gmail, are sent a verification code when they attempt to access shared content. You can require that these guests reauthenticate after a specified period. Use the **People who use a verification code must reauthenticate after this many days** setting to configure this.

File and folder sharing

To create an easy sharing experience for your users while reducing the risk of oversharing, you can choose from these options for file and folder sharing links:

- Choose the default link type that users see when they share a file or folder.

- Choose if the default sharing link allows recipients to edit the files.
- Choose if *Anyone* links expire after a given period.
- Choose if *Anyone* links allow recipients to edit the files.

When users share a file or folder, they can choose from several types of sharing links that offer different levels of permissions. You can choose which link type is shown by default:

- *Specific people* links require the user to specify a list of people who will have access to the file or folder.
- *Only people in your organization* links provide access to the file or folder to anyone in your organization who has the link.
- *Anyone* links (if you've enabled them in your organization level sharing settings) provide anonymous access to anyone who has the link, including people outside your organization.

You can also choose the default permission level - view or edit - for sharing links.

These options can also be configured for individual sites. See Change the sharing settings for a site for details.

If you've enabled *Anyone* links, you can choose if these links should expire after a given period and if they should allow edit access or just view access.

Next steps

Training and change management

Related topics

Plan for SharePoint and OneDrive in Microsoft 365

Set up secure file sharing and collaboration with Microsoft Teams

Overview of external collaboration options in Microsoft 365

SharePoint and OneDrive file sync

Create a more secure guest sharing environment

Feedback

Was this page helpful? Yes No

Provide product feedback

Features available for PDFs in OneDrive in Web and mobiles/iPads

08/27/2025

This article lists the PDF-based features supported for the mobile application of OneDrive and for the Web-based application of OneDrive.

Categories

The features introduced for PDFs in OneDrive are categorized into:

- Freemium
- Premium

Freemium

The following table lists the PDF-based features in OneDrive that are available free of cost:

Expand table

Feature	Description	OneDrive for home	OneDrive for work/school
Annotation and markup tools	Easily collaborate and share feedback by using digital ink, highlighting text, drawing shapes, and inserting sticky notes directly onto your PDF files.	Yes	Yes
Bookmark PDF pages	Navigate effortlessly through lengthy documents by adding bookmarks to important sections, just like using tabs in a physical book.	Yes (OneDrive for iOS/iPadOS and Android only.)	Yes (OneDrive for iOS/iPadOS and Android only.)
Change the appearance of your PDF	Enhance your reading experience by adjusting the background color of your PDFs to dark mode, sepia mode, or light mode. Ideal for reading in different lighting conditions.	Yes (OneDrive for Android only.)	Yes (OneDrive for Android only.)
Rotate PDF pages	Correct the orientation of scanned documents by rotating individual or multiple pages 90° clockwise. Perfect for fixing upside-down or sideways pages.	Yes	Yes

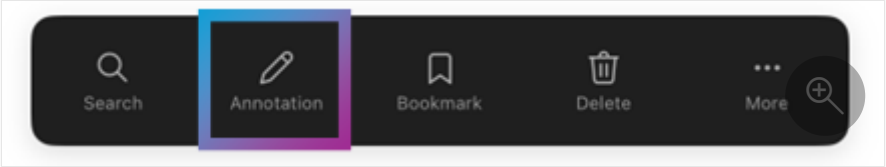
Feature	Description	OneDrive for home	OneDrive for work/school
Jump to specific PDF page using Table of Contents	Quickly access specific sections by jumping directly to any page in your PDF documents using a clickable table of contents.	Yes	Yes

Annotation and markup tools for enhancing collaboration

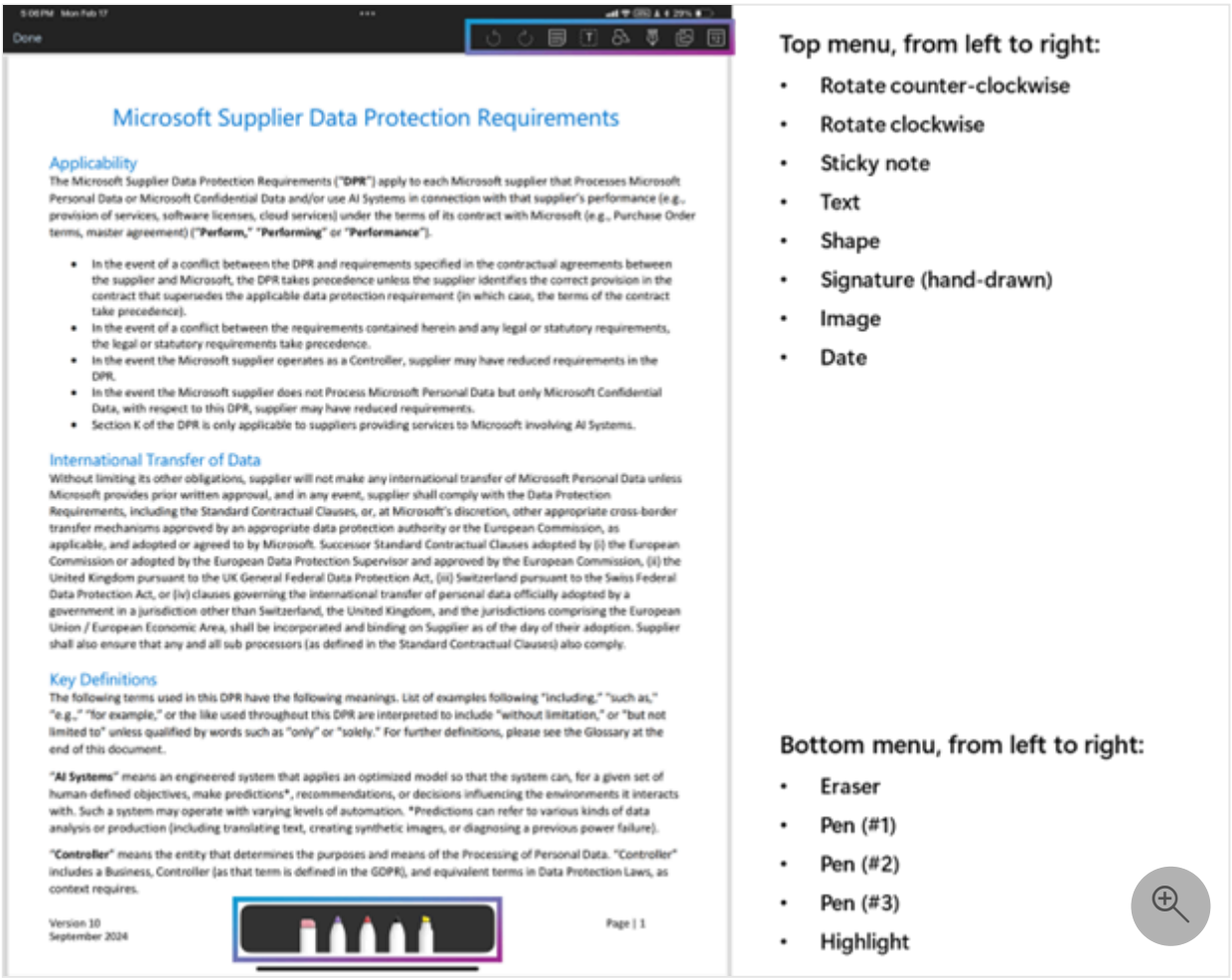
The "Annotation and Markup Tools" feature facilitates an optimized collaboration for a team that uses a PDF as a medium of communication in the project. This feature helps the team members to allow annotations, editing tools in the PDF to represent their suggestions/ideas/views about the project within their team. This feature enables the team members avoid using collaboration sessions to convey each suggestion/idea/view. This feature enables reduction in the count of sessions of collaboration about the project for each member to share (if they have any) suggestion/idea/view about any specific facet in the project.

To annotate a PDF in OneDrive using markup tools, perform the following steps:

1. Find the PDF you want to annotate in your OneDrive and select it for the PDF to launch.
2. Select **Annotation** to enter "editing" mode at the bottom of the PDF screen:



3. Select an annotation tool from the bottom of the screen or a drawing markup tool from the top of the screen.

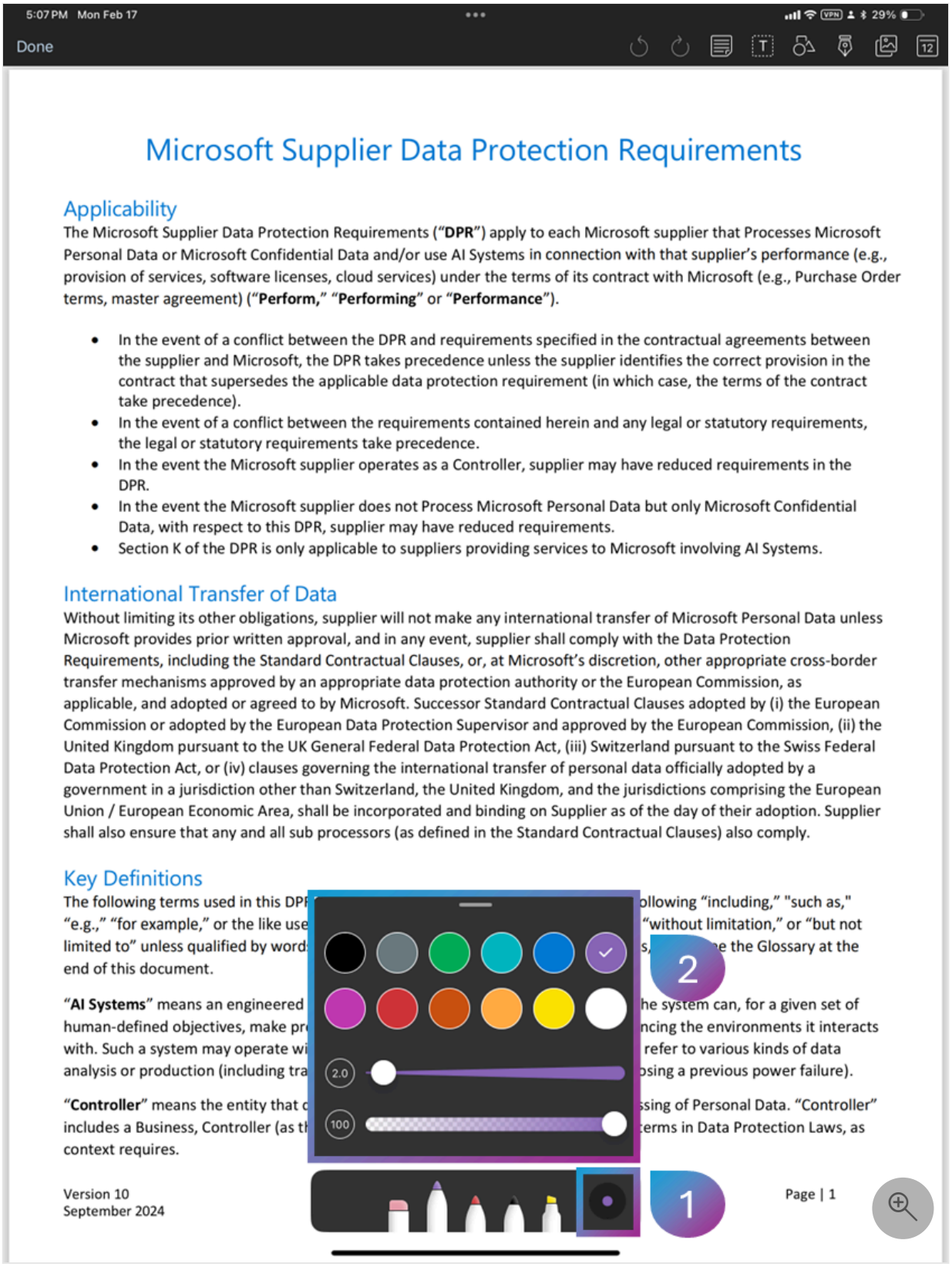


4. Change the pen color. You can do this by performing the following steps:

   a. Select the color picker at the bottom of the screen (the pane in the following screenshot that is marked as 1).

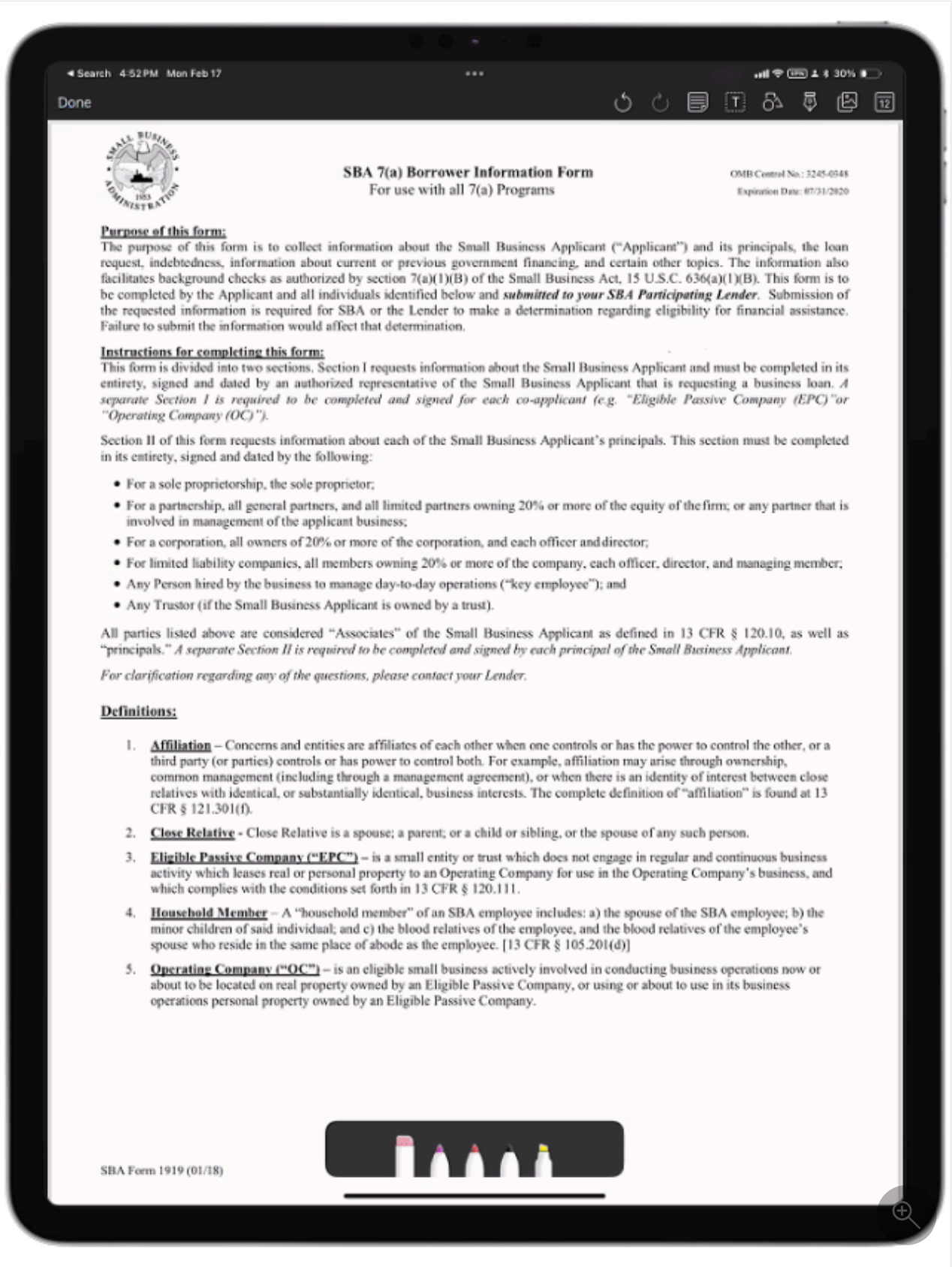
   b. Choose from any of the preset colors in the color picker.

> ⓘ **Note**
>
> You can also adjust the thickness and transparency of the ink from the bottom pane in the following screenshot (pane marked as 2):



5. Select **Done** at the top–left of the PDF screen, and then select **Save** at the top–right of the PDF screen to save your changes back to OneDrive.

   The following screenshot displays the process of annotating the PDF:



Search 4:52 PM Mon Feb 17

Done

SBA 7(a) Borrower Information Form
For use with all 7(a) Programs

OMB Control No.: 3245-0348
Expiration Date: 07/31/2020

Purpose of this form:
The purpose of this form is to collect information about the Small Business Applicant ("Applicant") and its principals, the loan request, indebtedness, information about current or previous government financing, and certain other topics. The information also facilitates background checks as authorized by section 7(a)(1)(B) of the Small Business Act, 15 U.S.C. 636(a)(1)(B). This form is to be completed by the Applicant and all individuals identified below and ***submitted to your SBA Participating Lender***. Submission of the requested information is required for SBA or the Lender to make a determination regarding eligibility for financial assistance. Failure to submit the information would affect that determination.

Instructions for completing this form:
This form is divided into two sections. Section I requests information about the Small Business Applicant and must be completed in its entirety, signed and dated by an authorized representative of the Small Business Applicant that is requesting a business loan. *A separate Section I is required to be completed and signed for each co-applicant (e.g. "Eligible Passive Company (EPC)" or "Operating Company (OC)").*

Section II of this form requests information about each of the Small Business Applicant's principals. This section must be completed in its entirety, signed and dated by the following:

- For a sole proprietorship, the sole proprietor;
- For a partnership, all general partners, and all limited partners owning 20% or more of the equity of the firm; or any partner that is involved in management of the applicant business;
- For a corporation, all owners of 20% or more of the corporation, and each officer and director;
- For limited liability companies, all members owning 20% or more of the company, each officer, director, and managing member;
- Any Person hired by the business to manage day-to-day operations ("key employee"); and
- Any Trustor (if the Small Business Applicant is owned by a trust).

All parties listed above are considered "Associates" of the Small Business Applicant as defined in 13 CFR § 120.10, as well as "principals." *A separate Section II is required to be completed and signed by each principal of the Small Business Applicant.*

For clarification regarding any of the questions, please contact your Lender.

Definitions:

1. **Affiliation** – Concerns and entities are affiliates of each other when one controls or has the power to control the other, or a third party (or parties) controls or has power to control both. For example, affiliation may arise through ownership, common management (including through a management agreement), or when there is an identity of interest between close relatives with identical, or substantially identical, business interests. The complete definition of "affiliation" is found at 13 CFR § 121.301(f).
2. **Close Relative** - Close Relative is a spouse; a parent; or a child or sibling, or the spouse of any such person.
3. **Eligible Passive Company ("EPC")** – is a small entity or trust which does not engage in regular and continuous business activity which leases real or personal property to an Operating Company for use in the Operating Company's business, and which complies with the conditions set forth in 13 CFR § 120.111.
4. **Household Member** – A "household member" of an SBA employee includes: a) the spouse of the SBA employee; b) the minor children of said individual; and c) the blood relatives of the employee, and the blood relatives of the employee's spouse who reside in the same place of abode as the employee. [13 CFR § 105.201(d)]
5. **Operating Company ("OC")** – is an eligible small business actively involved in conducting business operations now or about to be located on real property owned by an Eligible Passive Company, or using or about to use in its business operations personal property owned by an Eligible Passive Company.

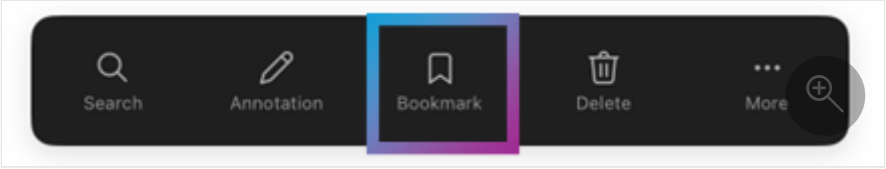
SBA Form 1919 (01/18)

Bookmark PDF pages

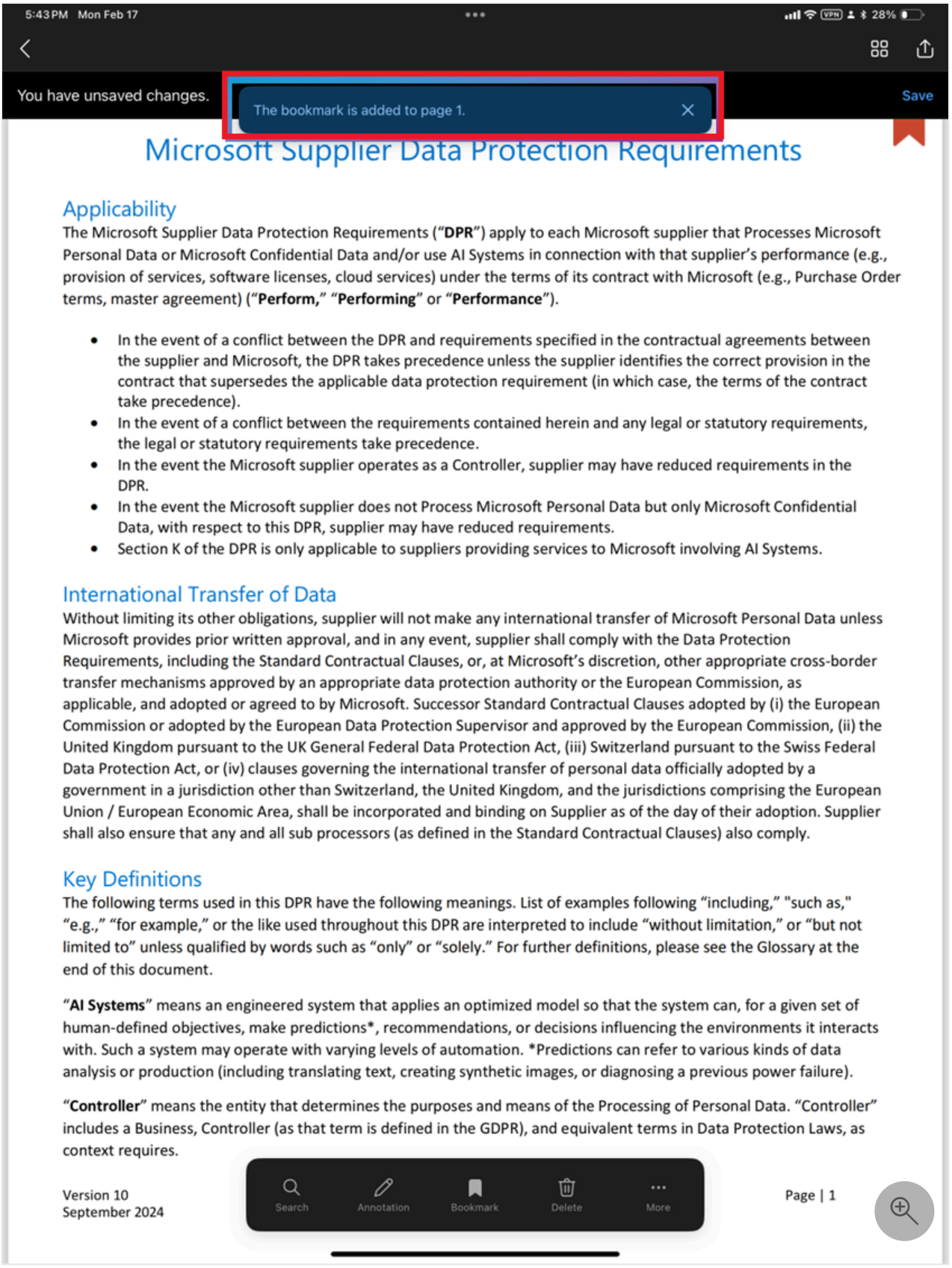
The "Bookmarks" feature for the PDFs in OneDrive enables easier and faster navigation to the specific sections in the PDF. This feature enhances the reading experience for the PDF users.

To add a bookmark in a PDF, perform the following steps:

1. Select **Bookmark** at the bottom of the PDF screen to add a bookmark to the current page you’re viewing.



Once you’ve added the bookmark, you'll see a dialog box displaying a confirmation message at the top of the screen as shown in the following screenshot:

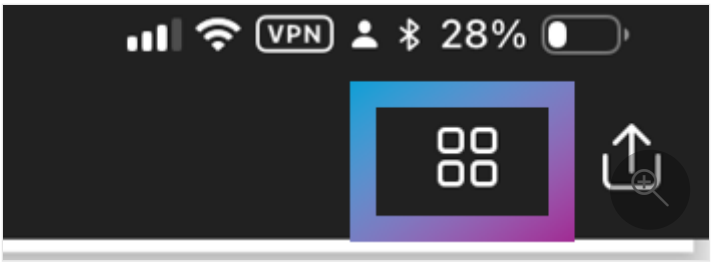


You can add bookmark to any page and any number of pages of choice by implementing the preceding step.

Viewing bookmarks added to multiple pages

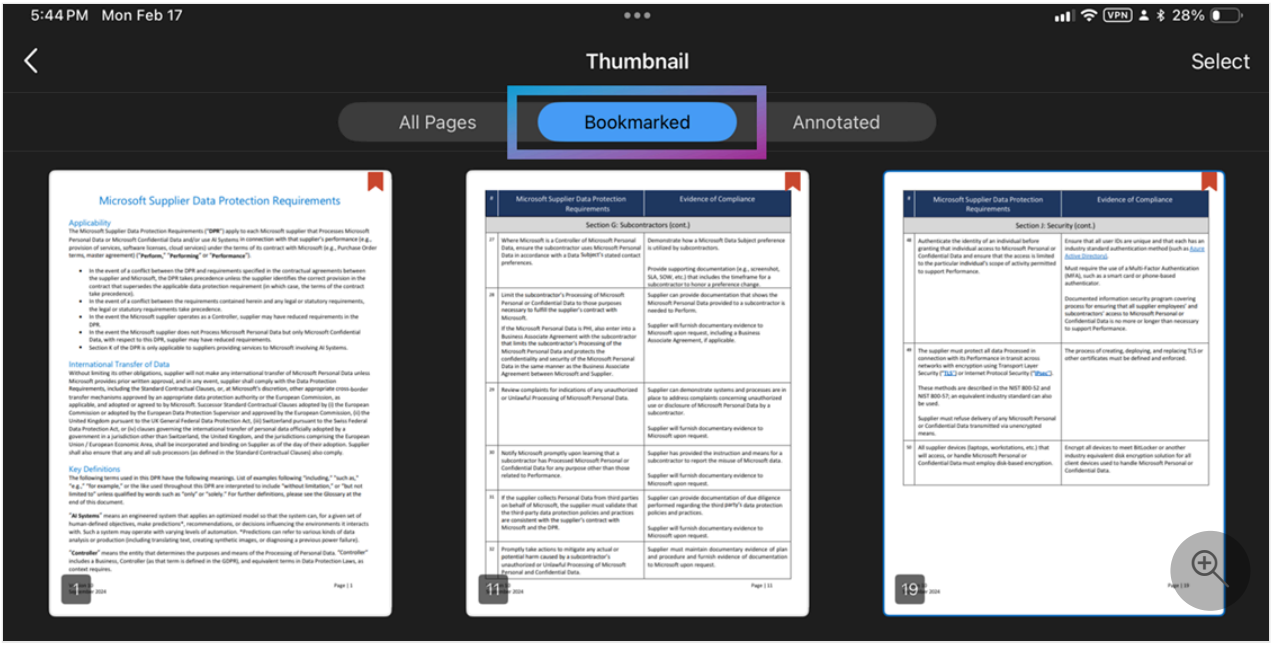
If you've added bookmarks to multiple pages and want to view those bookmarks, perform the following steps:

1. Select the **Thumbnail** icon at the top–right of the screen.



The page shows the **All Pages**, **Bookmarked**, and **Annotated** options in "thumbnail" view.

2. Select the **Bookmarked** option from the page shown in "thumbnail" view.



Adding bookmarks to multiple pages or deleting bookmarks from multiple pages

You can also add bookmarks to multiple pages or delete existing bookmarks from pages.

To add bookmarks to multiple pages, perform the following steps:

1. Select the **All Pages** option from the page shown in "thumbnail" view.
2. Select a page (or multiple pages) from the **All Pages** screen to which you want to add a bookmark.
3. Select **Bookmark** at the bottom of the screen on the page to which you want to add a bookmark.

To delete existing bookmarks from the pages, perform the following steps:

1. Select the **Bookmarked** option from the page shown in "thumbnail view". This page displays the pages that have been bookmarked.
2. Select the page (or pages) for which you want to delete the bookmark, and then select **Delete**. The bookmarks for the selected pages are deleted.

The whole process of managing bookmarks in PDFs on OneDrive is depicted in the following screenshot:

Microsoft Supplier Data Protection Requirements

Applicability

The Microsoft Supplier Data Protection Requirements ("**DPR**") apply to each Microsoft supplier that Processes Microsoft Personal Data or Microsoft Confidential Data in connection with that supplier's performance (e.g., provision of services, software licenses, cloud services) under the terms of its contract with Microsoft (e.g., Purchase Order terms, master agreement) ("**Perform**," "**Performing**" or "**Performance**").

- In the event of a conflict between the DPR and requirements specified in the contractual agreements between the supplier and Microsoft, the DPR takes precedence unless the supplier identifies the correct provision in the contract that supersedes the applicable data protection requirement (in which case, the terms of the contract take precedence).
- In the event of a conflict between the requirements contained herein and any legal or statutory requirements, the legal or statutory requirements take precedence.
- In the event the Microsoft supplier operates as a Controller, supplier may have reduced requirements in the DPR.
- In the event the Microsoft supplier does not Process Microsoft Personal Data but only Microsoft Confidential Data, with respect to this DPR, supplier may have reduced requirements.
- Section K of the DPR is only applicable to suppliers providing services to Microsoft involving AI Systems.

International Transfer of Data

Without limiting its other obligations, supplier will not make any international transfer of Microsoft Personal Data unless Microsoft provides prior written approval, and in any event, supplier shall comply with the Data Protection Requirements, including the Standard Contractual Clauses, or, at Microsoft's discretion, other appropriate cross-border transfer mechanisms approved by an appropriate data protection authority or the European Commission, as applicable, and adopted or agreed to by Microsoft. Successor Standard Contractual Clauses adopted by (i) the European Commission or adopted by the European Data Protection Supervisor and approved by the European Commission, (ii) the United Kingdom pursuant to the UK General Federal Data Protection Act, (iii) Switzerland pursuant to the Swiss Federal Data Protection Act, or (iv) clauses governing the international transfer of personal data officially adopted by a government in a jurisdiction other than Switzerland, the United Kingdom, and the jurisdictions comprising the European Union / European Economic Area, shall be incorporated and binding on Supplier as of the day of their adoption. Supplier shall also ensure that any and all sub processors (as defined in the Standard Contractual Clauses) also comply.

Key Definitions

The following terms used in this DPR have the following meanings. List of examples following "including," "such as," "e.g.," "for example," or the like used throughout this DPR are interpreted to include "without limitation," or "but not limited to" unless qualified by words such as "only" or "solely." For further definitions, please see the Glossary at the end of this document.

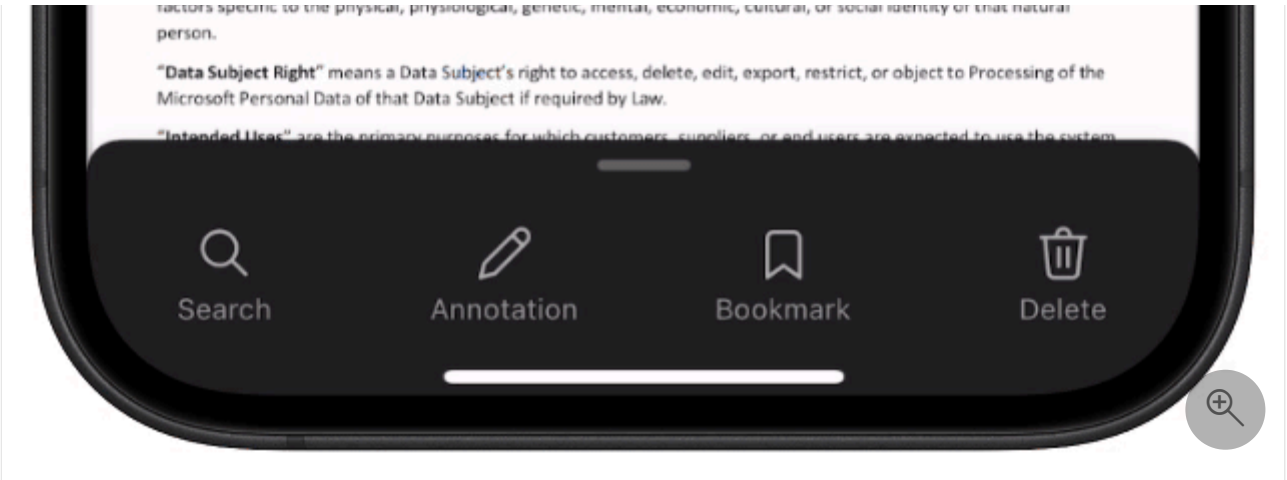
"**AI Systems**" means an engineered system that applies an optimized model so that the system can, for a given set of human-defined objectives, make predictions*, recommendations, or decisions influencing the environments it interacts with. Such a system may operate with varying levels of automation. *Predictions can refer to various kinds of data analysis or production (including translating text, creating synthetic images, or diagnosing a previous power failure).

"**Controller**" means the entity that determines the purposes and means of the Processing of Personal Data. "Controller" includes a Business, Controller (as that term is defined in the GDPR), and equivalent terms in Data Protection Laws, as context requires.

"**Cookies**" are small text files stored on devices by websites and/or applications that contain information used to recognize a Data Subject or a device.

"**Data Incident**" means (1) a breach of security leading to the accidental or Unlawful destruction, loss, alteration, unauthorized disclosure of, or access to, Microsoft Personal Data or Microsoft Confidential Data transmitted, stored or otherwise Processed by Supplier or its Subcontractors, or (2) security vulnerability related to Supplier's handling of Microsoft Personal Data or Microsoft Confidential Data or confidentiality incident as defined under Bill 64 (2021, chapter 25).

"**Data Subject**" means an identifiable natural person who can be identified, directly or indirectly, in particular by referencing an identifier such as a name, an identification number, location data, an online identifier, or to one or more



Change the appearance of your PDF - Optimize PDF viewing by using various reading modes

The "Optimized PDF Viewing with Reading Mode" feature can be applied when the default view of the PDF isn't conducive to be read in the current environment/surroundings the user is in. This feature enables the user to customize the PDF's background to sync with the environment in which you're going to read the PDF.

Customizing PDFs' background refers to changing the PDF's default mode for reading (the mode as is on your PC or mobile when you open the PDF) to "dark" mode, "sepia" mode, or "light" mode.

To change a PDF's background, perform the following steps:

1. Open a PDF in OneDrive for Android and click anywhere to expand the bottom sheet of the screen.
2. Select **Appearance**.
3. Select a colored circle that corresponds to the reading mode that you want to set for the PDF.

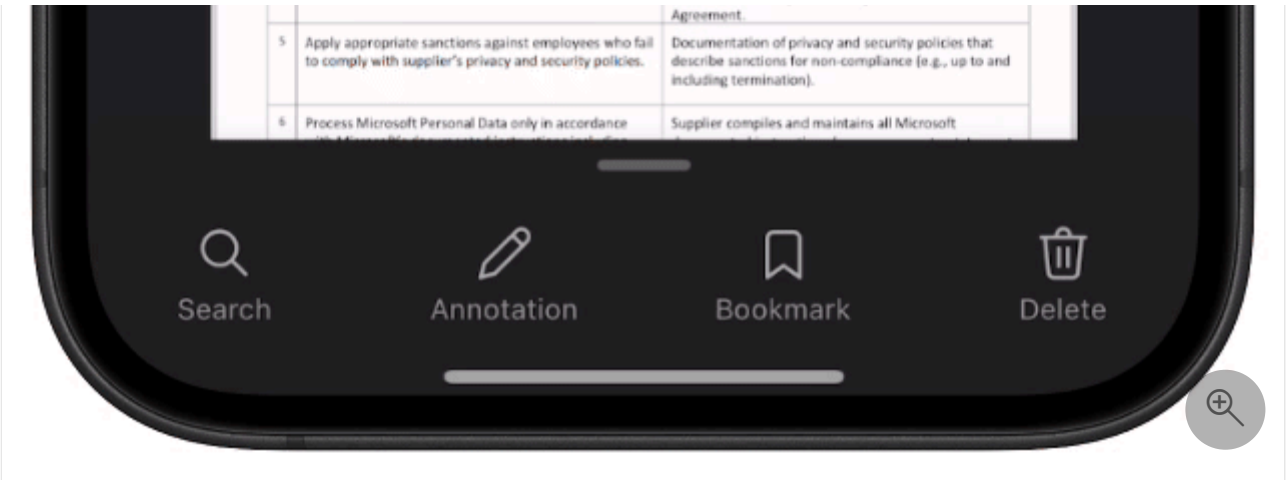
Rotating PDF pages to adjust a PDF pages' orientation

The "Page Rotation" feature enables the user to adjust a PDF page's orientation wherein a page that has been saved upside down or sideways is rotated to bring it to the "straight" position. This feature is especially useful when there are multiple pages that have been saved upside down or sideways.

The process of applying the "rotate" feature is depicted in the following screenshot:

#	Microsoft Supplier Data Protection Requirements	Evidence of Compliance
	Section A: Management	
1	Each applicable agreement between Microsoft and the supplier (e.g., master agreement, statement of work, purchase orders and other orders) contains privacy and security data protection language with respect to Microsoft Confidential and Personal Data, as applicable, including prohibitions on the sale of Microsoft Personal Data and Processing of Microsoft Personal Data outside the direct business relationship between Microsoft and supplier. For companies operating as Processors or Subprocessors in connection with the Performance, with respect to Microsoft Personal Data, the agreement must include the subject-matter and duration of the Processing, the nature and purpose of the Processing, the type of Microsoft Personal Data and categories of Data Subjects and the obligations and rights of Microsoft.	Supplier must present the applicable contract between Microsoft and Supplier. For Processors and Subprocessors, the Processing descriptions are contained in the applicable agreement (e.g., statement of work, purchase orders). If Microsoft confirms that your engagements involve the processing of PHI, Supplier must have a Business Associate Agreement and/or other agreement in place with Microsoft. Note: Companies with in-flight purchase orders may have the necessary description of Processing activities added later in the purchasing process.
2	Where Microsoft confirms that your engagements fulfill a Subprocessor role, Supplier must have applicable data protection agreements in place with Microsoft. Note: Microsoft will post these designations to your profile when they apply.	Standard Contractual Clauses, Online Customer Data Addendum, Supplier and Partner Professional Services Data Processing Addendum, and/or Business Associate Agreement.
3	Assign responsibility and accountability for compliance with the DPR to a designated person or group within the company.	Name the role of the person or group charged with ensuring compliance to the Microsoft Supplier DPR. A document describing the authority and accountability of this person or group that demonstrates a privacy and/or security role.

#	Microsoft Supplier Data Protection Requirements	Evidence of Compliance
	Section A: Management (cont.)	
4	Establish, maintain, and perform annual privacy and security training for anyone (system administrators, operations staff, management, third parties, etc.) that will have access to Microsoft Personal or Confidential Data. If your company does not have prepared content, you can use this storyboard outline and adapt it for your company. Note: Supplier personnel may be required to complete additional trainings provided by Microsoft divisions.	Annual records of attendance are available and can be provided to Microsoft upon request. Training content is regularly updated and includes privacy and security principles like incident prevention awareness including safeguarding passwords, log-in monitoring, risks associated with downloading malicious software, and other relevant security reminders. Documentation of compliance with training requirements will include evidence of training related to privacy regulatory requirements, security obligations, and compliance with applicable contract requirements and obligations. IT staff must have training for incident response and simulated events and automated mechanisms to facilitate effective response to crisis situations. If the Microsoft Personal Data Processed by supplier includes PHI, training content must include HIPAA training, security reminders, address log-in monitoring, safeguarding passwords, and supplier's permitted uses and disclosures as permitted by the Business Associate



Rotating a single page that has a sideways' or upside-down orientation

To rotate a single page, perform the following steps:

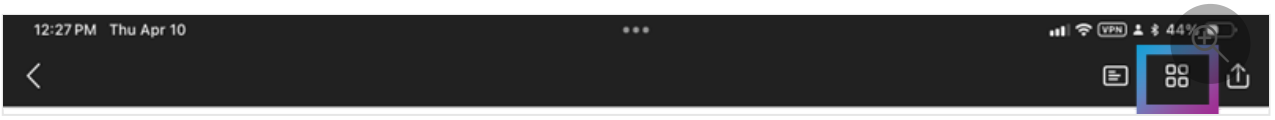
1. Open the OneDrive app on your iOS or Android mobile; then open the PDF containing the page you want to rotate.
2. Scroll to the page that you want to rotate and click on an area where no text is there. A dialog box pops up.
3. Select **Rotate** to rotate the page 90 degrees clockwise. Keep selecting Rotate for more 90-degree turns until the page reaches the straight orientation.

Rotating multiple pages with a sideways' or upside-down orientation

To rotate multiple pages, perform the following steps:

1. Open the OneDrive app on your iOS or Android mobile; then open the PDF containing the pages you want to rotate.

2. Select the **Thumbnail** icon at the top of the screen to show a thumbnail view of the PDF's pages.



3. Select **Select**. The screen containing all the pages of the PDF (opened in Step-1) appears.

4. Click on the pages you want to rotate (pages get selected for rotation on being clicked) OR select **Select all** if you want to rotate all the pages.

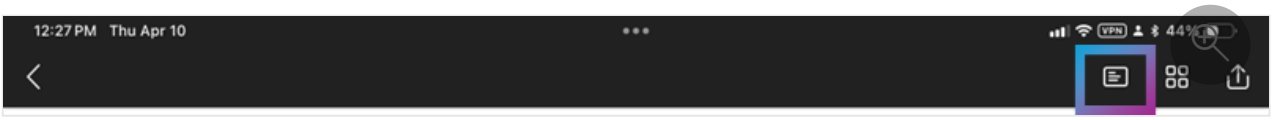
5. Click the **Rotate** icon on the toolbar at the bottom of your screen to rotate the pages you have selected 90 degrees clockwise.

Jump to specific PDF page using Table of Contents

The “Quick page-navigation using Table of Contents (TOC)” feature enables smooth/easy navigation in a lengthy/large PDF. This feature displays each chapter’s/section’s title along with their page numbers. This provision enables the user to navigate quickly to the desired chapter section on account of they knowing the page number.

To view a PDF’s TOC to use its clickable chapter's/section's page numbers, perform the following steps:

1. Select the **TOC** icon at the top–right of the PDF screen.



> **Note**
>
> This icon is displayed if the PDF includes TOC-related data irrespective of which location in the PDF hosts the TOC-related data. If the TOC-related data isn't found anywhere in a PDF, then such a PDF won't display the TOC icon on the UI.

The TOC—with clickable chapters and sections—is displayed on the left side of the screen.

The Impact of Generative AI on Critical Thinking: Self-Reported Reductions in Cognitive Effort and Confidence Effects From a Survey of Knowledge Workers

Hao-Ping (Hank) Lee
Carnegie Mellon University
Pittsburgh, Pennsylvania, USA
haopingl@cs.cmu.edu

Advait Sarkar
Microsoft Research
Cambridge, United Kingdom
advait@microsoft.com

Lev Tankelevitch
Microsoft Research
Cambridge, United Kingdom
levt@microsoft.com

Ian Drosos
Microsoft Research
Cambridge, United Kingdom
t-iandrosos@microsoft.com

Sean Rintel
Microsoft Research
Cambridge, United Kingdom
serintel@microsoft.com

Richard Banks
Microsoft Research Cambridge
Cambridge, United Kingdom
rbanks@microsoft.com

Nicholas Wilson
Microsoft Research
Cambridge, United Kingdom
niwilson@microsoft.com

Abstract

The rise of Generative AI (GenAI) in knowledge workflows raises questions about its impact on critical thinking skills and practices. We survey 319 knowledge workers to investigate 1) when and how they perceive the enaction of critical thinking when using GenAI, and 2) when and why GenAI affects their effort to do so. Participants shared 936 first-hand examples of using GenAI in work tasks. Quantitatively, when considering both task- and user-specific factors, a user's task-specific self-confidence and confidence in GenAI are predictive of whether critical thinking is enacted and the effort of doing so in GenAI-assisted tasks. Specifically, higher confidence in GenAI is associated with less critical thinking, while higher self-confidence is associated with more critical thinking. Qualitatively, GenAI shifts the nature of critical thinking toward information verification, response integration, and task stewardship. Our insights reveal new design challenges and opportunities for developing GenAI tools for knowledge work.

CCS Concepts

• **Human-centered computing → Empirical studies in HCI.**

Keywords

Critical thinking, Generative AI tools, Knowledge worker, Bloom's taxonomy, Survey

ACM Reference Format:
Hao-Ping (Hank) Lee, Advait Sarkar, Lev Tankelevitch, Ian Drosos, Sean Rintel, Richard Banks, and Nicholas Wilson. 2025. The Impact of Generative AI on Critical Thinking: Self-Reported Reductions in Cognitive Effort and Confidence Effects From a Survey of Knowledge Workers. In *CHI Conference on Human Factors in Computing Systems (CHI '25), April 26–May 01, 2025, Yokohama, Japan.* ACM, New York, NY, USA, 23 pages. https://doi.org/10.1145/3706598.3713778

This work is licensed under a Creative Commons Attribution 4.0 International License.
CHI '25, Yokohama, Japan
© 2025 Copyright held by the owner/author(s).
ACM ISBN 979-8-4007-1394-1/25/04
https://doi.org/10.1145/3706598.3713778

1 Introduction

Generative AI (**GenAI**) tools, defined as any *"end user tool […] whose technical implementation includes a generative model based on deep learning"*,[1] are the latest in a long line of technologies that raise questions about their impact on the quality of human thought, a line that includes writing (objected to by Socrates), printing (objected to by Trithemius), calculators (objected to by teachers of arithmetic), and the Internet.

Such consternation is not unfounded. Used improperly, technologies can and do result in the deterioration of cognitive faculties that ought to be preserved. As Bainbridge [7] noted, a key irony of automation is that by mechanising routine tasks and leaving exception-handling to the human user, you deprive the user of the routine opportunities to practice their judgement and strengthen their cognitive musculature, leaving them atrophied and unprepared when the exceptions do arise.

In response, research has begun looking closely at how different activities are impacted by GenAI and the extent to which cognitive offloading [8] occurs, and whether this may be an undesirable thing. Some work has focused, for instance, on studying the effects of GenAI use on memory (e.g., [1, 106]) and on creativity (e.g., [28, 100]). Moreover, design research has also been developing interventions that *improve* the ability of people to think in certain ways (e.g., [24]). We review these lines of work in Section 2.

In this paper, we focus on a higher-level concept that captures another aspect of thought considered desirable and worthy of preservation: *critical thinking* (defined in Section 2). The effect of the use

[1] While there is no broad consensus on how to define this now-common term, for clarity we adopt this definition, a rationale for which is given in [115].

© Owner/Author 2025. This is the author's version of the work. It is posted here for your personal use. Not for redistribution.
The definitive version was published in CHI 2025, https://doi.org/10.1145/3706598.3713778.

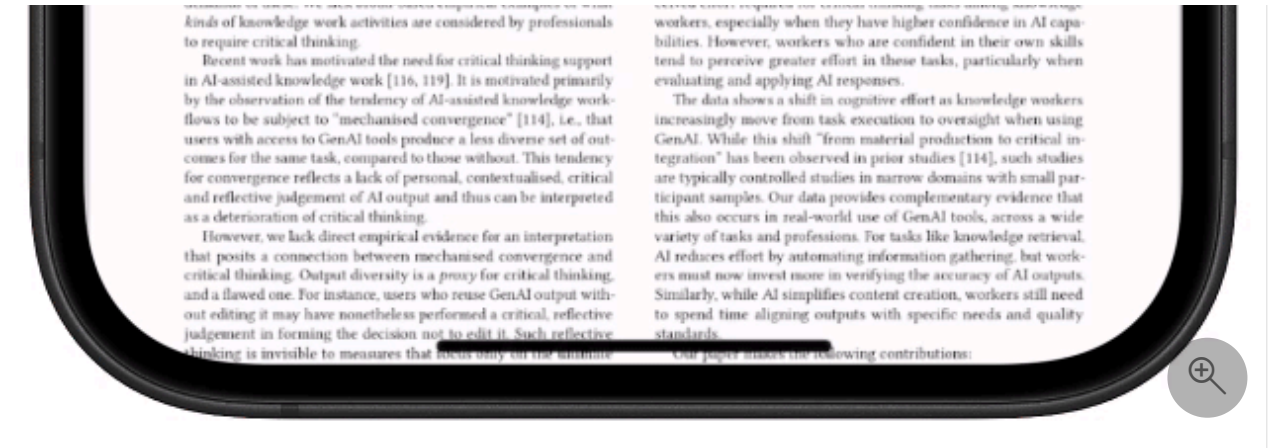
of GenAI tools on critical thinking, as a direct object of inquiry, has not yet been explored.

Moreover, we focus on critical thinking for *knowledge work* (as conceptualised by Drucker [30] and Kidd [67]). Much research on the effect of GenAI on thinking skills is focused on educational settings, where concern for skill cultivation is most acute (e.g., the effect of GenAI code completion tools on programming and computer science education [107]). As previously noted [116, 119], critical thinking has been operationalised in detail in certain specific disciplines, such as academic history, clinical psychology, and nursing. But the ostensible shifts in critical thinking behaviours brought about by GenAI extend to a broad set of professions and knowledge workflows — GenAI tools are now widely used in knowledge work [13] — and little is known about the critical thinking demands of these. We lack broad-based empirical examples of what

as setting clear goals, refining prompts, and assessing AI-generated content to meet specific criteria and standards. Their reflective approach involves verifying outputs against external sources and their own expertise, especially in tasks that require higher accuracy.

The data identify key motivators for critical thinking: the desire to enhance work quality, avoid negative outcomes, and develop skills. However, several barriers inhibit this reflective process, including lack of awareness, limited motivation due to time pressure or job scope, and difficulty improving AI responses in unfamiliar domains. Surprisingly, while AI can improve efficiency, it may also reduce critical engagement, particularly in routine or lower-stakes tasks in which users simply rely on AI, raising concerns about long-term reliance and diminished independent problem-solving.

Regarding RQ2 (Section 5), GenAI tools appear to reduce the perceived effort required for critical thinking tasks among knowledge



kinds of knowledge work activities are considered by professionals to require critical thinking.

Recent work has motivated the need for critical thinking support in AI-assisted knowledge work [116, 119]. It is motivated primarily by the observation of the tendency of AI-assisted knowledge workflows to be subject to "mechanised convergence" [114], i.e., that users with access to GenAI tools produce a less diverse set of outcomes for the same task, compared to those without. This tendency for convergence reflects a lack of personal, contextualised, critical and reflective judgement of AI output and thus can be interpreted as a deterioration of critical thinking.

However, we lack direct empirical evidence for an interpretation that posits a connection between mechanised convergence and critical thinking. Output diversity is a *proxy* for critical thinking, and a flawed one. For instance, users who reuse GenAI output without editing it may have nonetheless performed a critical, reflective judgement in forming the decision not to edit it. Such reflective thinking is invisible to measures that focus only on the ultimate

workers, especially when they have higher confidence in AI capabilities. However, workers who are confident in their own skills tend to perceive greater effort in these tasks, particularly when evaluating and applying AI responses.

The data shows a shift in cognitive effort as knowledge workers increasingly move from task execution to oversight when using GenAI. While this shift "from material production to critical integration" has been observed in prior studies [114], such studies are typically controlled studies in narrow domains with small participant samples. Our data provides complementary evidence that this also occurs in real-world use of GenAI tools, across a wide variety of tasks and professions. For tasks like knowledge retrieval, AI reduces effort by automating information gathering, but workers must now invest more in verifying the accuracy of AI outputs. Similarly, while AI simplifies content creation, workers still need to spend time aligning outputs with specific needs and quality standards.

Our paper makes the following contributions:

Premium

The following table lists the PDF-based features in OneDrive that are available on the payment of a premium:

Expand table

Feature	Description	OneDrive for home[1]	OneDrive for work/school[2]
Extract PDF pages	Easily extract specific pages from your PDF documents to create new, smaller files. Ideal for sharing only the most relevant sections.	Yes	Yes
Merge PDFs	Seamlessly combine multiple PDFs into a single, organized document. Perfect for consolidating reports, presentations, and more.	Yes	Yes

[1] Premium features are available to OneDrive users with Microsoft 365 Basic, Microsoft 365 Personal, and Family subscriptions.
[2] Premium features are accessible to all OneDrive commercial users with SharePoint in their subscription plan.

Extract PDF pages

The "Extract PDF pages" feature enables the Microsoft 365 paid customers to extract specific pages from the main PDF and create a smaller PDF from the extracted pages. You can apply the "Extract PDF pages" feature using the following methods:

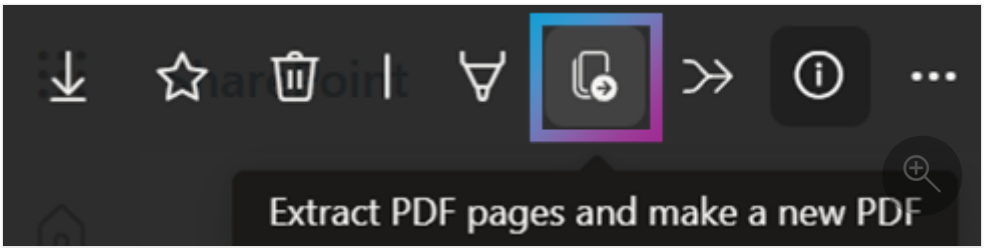
- Web browser
- Mobile phones and iPads (having iOS and Android operating systems).

Extract PDF pages using Web browser

To extract pages from a PDF file on a Web browser, perform the following steps:

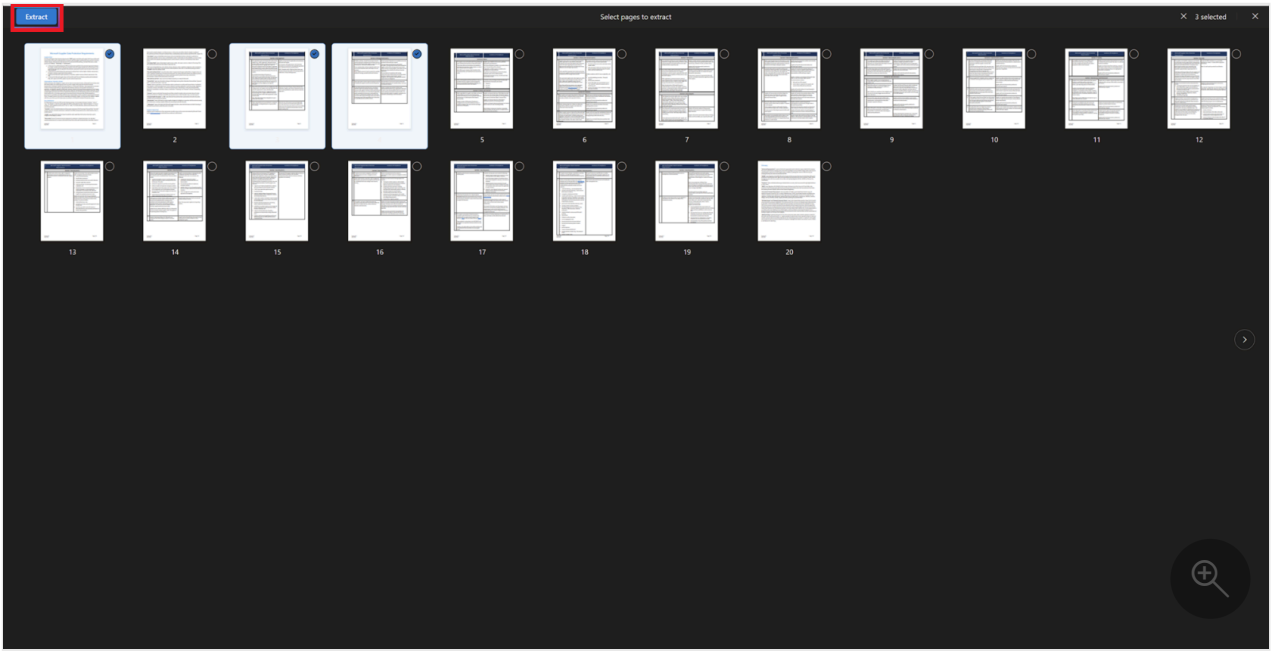
1. Open the PDF file from which you want to extract pages.

2. Select the **Extract** icon from the top portion of the screen.



   The pages are displayed in “thumbnail” view.

3. Select the pages that you want to extract, and then select **Extract** on the top–left of the screen.



> ⓘ **Note**
>
> Once you extract pages (even a single page) from the PDF, a new PDF file is generated containing these extracted pages.

4. Choose the location where you’d want to save the generated PDF file from the dialog box that pops up.

5. Provide a name to the file (if you want to rename it and not use the system-generated name) in the text box at the bottom of the **Save** dialog box.

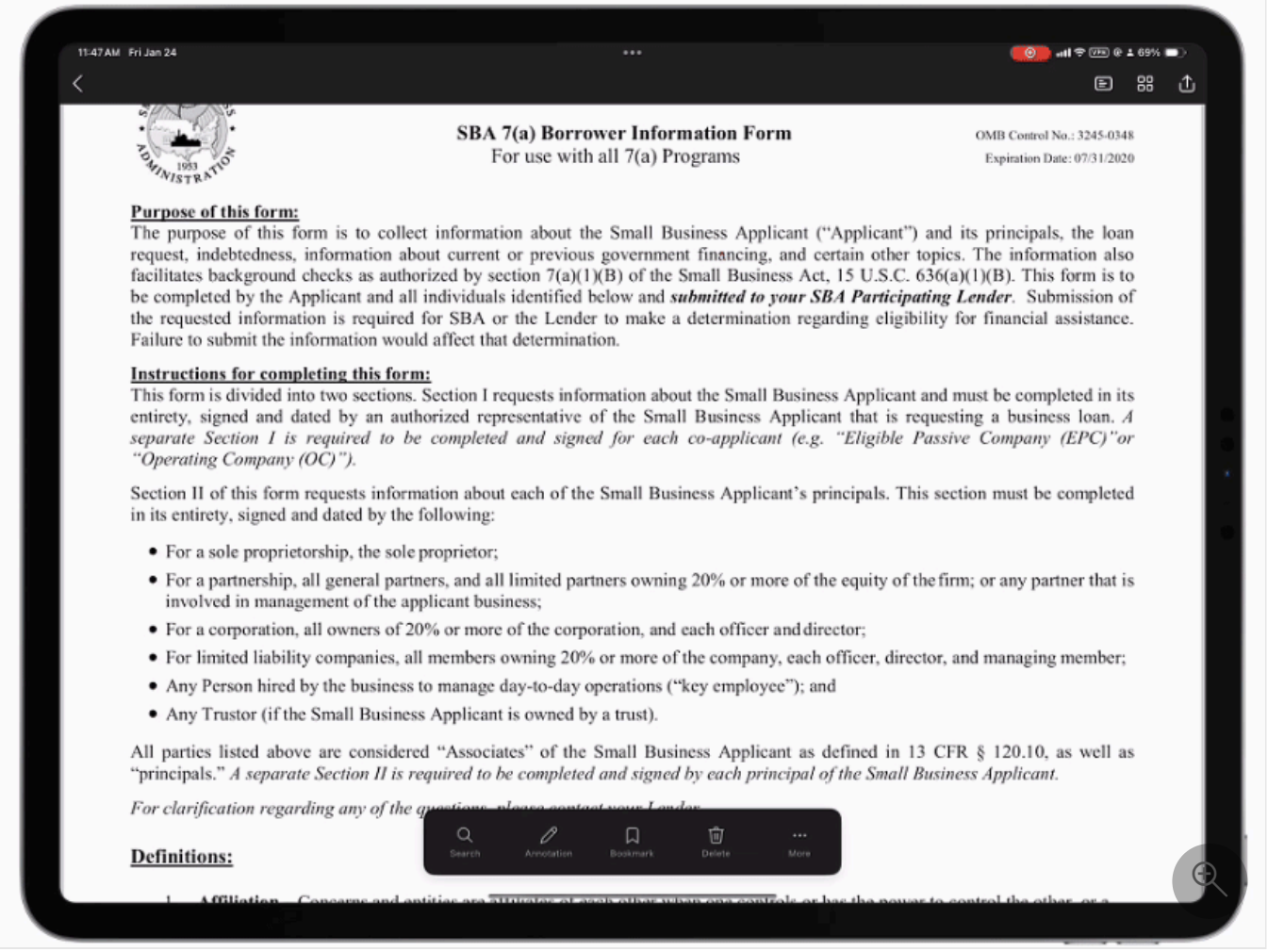
6. Select **Save**. A dialog box with a confirmation message appears at the bottom of the screen, stating that the extracted pages have been successfully saved as another PDF file with the name you provided (in the earlier step).

Extract PDF pages using iOS/Android mobile phones and/or iPads

To extract pages from a PDF from the OneDrive app on a mobile phone/iPad (with iOS/Android operating systems), perform the following steps:

1. Open the PDF file from which you want to extract pages.
2. Select the **...** icon at the top–left of the screen to view the new menu.
3. Select **Extract** from the new menu.
4. Choose the location where you'd want to save the generated PDF file from the dialog box that pops up.
5. Provide a name to the file (if you want to rename it and not use the system-generated name) in the text box at the bottom of the **Save** dialog box.
6. Select **Save**. A dialog box with a confirmation message appears at the bottom of the screen, stating that the extracted pages have been successfully saved as another PDF file with the name you provided (in the earlier step).

The following screenshot depicts the process of "page extraction from PDFs" on mobile/iPad:



SBA 7(a) Borrower Information Form
For use with all 7(a) Programs

OMB Control No.: 3245-0348
Expiration Date: 07/31/2020

Purpose of this form:
The purpose of this form is to collect information about the Small Business Applicant ("Applicant") and its principals, the loan request, indebtedness, information about current or previous government financing, and certain other topics. The information also facilitates background checks as authorized by section 7(a)(1)(B) of the Small Business Act, 15 U.S.C. 636(a)(1)(B). This form is to be completed by the Applicant and all individuals identified below and ***submitted to your SBA Participating Lender***. Submission of the requested information is required for SBA or the Lender to make a determination regarding eligibility for financial assistance. Failure to submit the information would affect that determination.

Instructions for completing this form:
This form is divided into two sections. Section I requests information about the Small Business Applicant and must be completed in its entirety, signed and dated by an authorized representative of the Small Business Applicant that is requesting a business loan. *A separate Section I is required to be completed and signed for each co-applicant (e.g. "Eligible Passive Company (EPC)"or "Operating Company (OC)").*

Section II of this form requests information about each of the Small Business Applicant's principals. This section must be completed in its entirety, signed and dated by the following:

- For a sole proprietorship, the sole proprietor;
- For a partnership, all general partners, and all limited partners owning 20% or more of the equity of the firm; or any partner that is involved in management of the applicant business;
- For a corporation, all owners of 20% or more of the corporation, and each officer and director;
- For limited liability companies, all members owning 20% or more of the company, each officer, director, and managing member;
- Any Person hired by the business to manage day-to-day operations ("key employee"); and
- Any Trustor (if the Small Business Applicant is owned by a trust).

All parties listed above are considered "Associates" of the Small Business Applicant as defined in 13 CFR § 120.10, as well as "principals." *A separate Section II is required to be completed and signed by each principal of the Small Business Applicant.*

For clarification regarding any of the questions, please contact your Lender.

Definitions:

Merge multiple PDFs

The “Merge multiple PDFs” feature enables the Microsoft 365 paid customers to merge multiple PDFs into a single PDF. You can apply the “Merge multiple PDFs” feature using the following methods:

- Web browser
- Mobile phones and iPads (having iOS and Android operating systems)

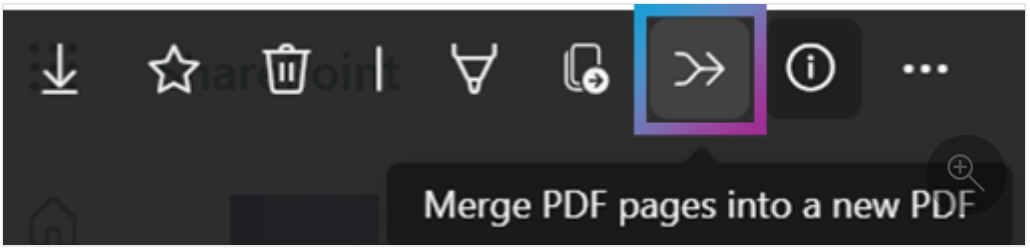
Merge multiple PDF files into a single PDF using Web browser

To merge multiple PDFs into a single PDF on a Web browser, perform the following steps:

1. Open one of the PDF files you want to combine in OneDrive for Web.

   > **Note**
   >
   > This PDF file that is opened is the file into which you'll merge other PDFs that you'll choose in the subsequent steps.

2. Select the **Merge** icon.

   A dialog box pops up, displaying other PDFs in "thumbnail" view.

3. Select two or more PDF files by clicking on those files, which you want to merge with the PDF file that was chosen in Step 1.

   > **Note**
   >
   > You can drag and drop the files to rearrange the order.

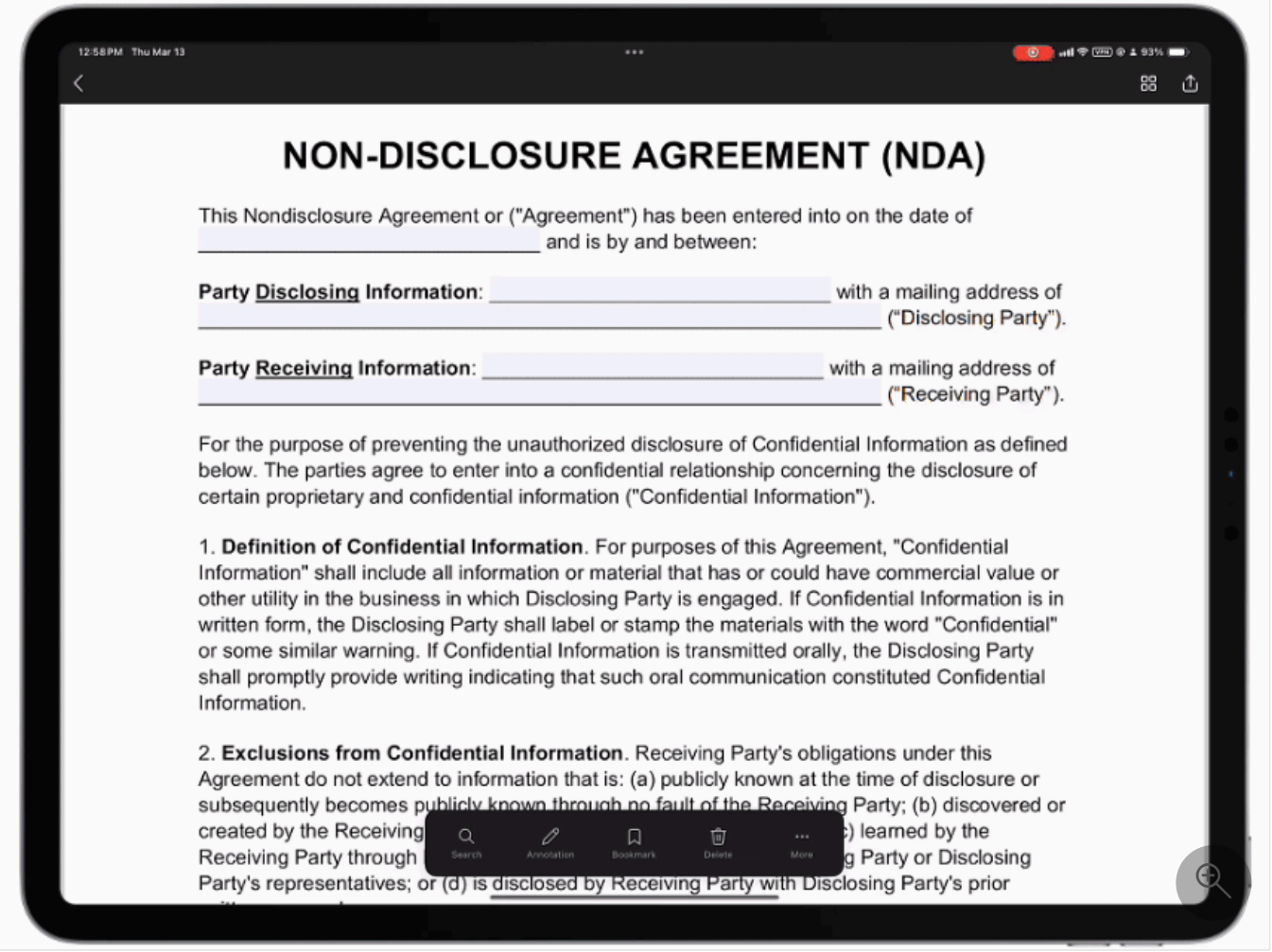
4. Select **Next**.

5. Choose the location where you’d want to save the generated PDF file from the dialog box that pops up.

6. Provide a name to the file (if you want to rename it and not use the system-generated name) in the text box at the bottom of the **Save** dialog box.

7. Select **Save**. A dialog box with a confirmation message appears at the bottom of the screen, stating that merged PDF files have been successfully saved as another PDF file with the name you provided (in the earlier step).

The following screenshot displays the process of implementing the steps in this section:



Merge multiple PDF files into a single PDF using mobile phones/iPads

To merge multiple PDFs into a single PDF from the OneDrive app on a mobile phone/iPad (with iOS/Android operating systems), perform the following steps:

1. Open one of the PDF files you want to combine from the OneDrive app on your mobile/iPad.

> ⓘ **Note**
>
> This PDF file is the file into which you'll merge other PDFs that you'll choose in the subsequent steps.

2. Select the **...** icon from the top–left of the screen to view the new menu.

3. Select **Merge** from the new menu's options.

A dialog box pops up, displaying other PDFs in "thumbnail" view.

4. Select two or more PDF files by clicking on those files, which you want to merge with the PDF file that was chosen in Step 1.

> ⓘ **Note**
>
> You can drag and drop the files to rearrange the order.

5. Select **Next**.

6. Choose the location where you'd want to save the generated PDF file from the dialog box that pops up.

7. Provide a name to the file (if you want to rename it and not use the system-generated name) in the text box at the bottom of the **Save** dialog box.

8. Select **Save**. A dialog box with a confirmation message appears at the bottom of the screen, stating that merged PDF files have been successfully saved as another PDF file with the name you provided (in the earlier step).

Training and change management for rolling out SharePoint and OneDrive

Article • 03/18/2024

Using SharePoint and OneDrive can be a significant change for your users, depending on what your current systems are. Spend time understanding your user journeys - those sequences of tasks that users regularly follow in the course of their work. Determine how using SharePoint and OneDrive fit into these journeys and use that information to create a transition plan and resources to help your users.

As part of your change management plan, review how your users do core tasks such as:

- Where to save personal work files
- Where to save shared files
- How to share files with others in the organization
- How to share files with people outside the organization
- How to create a site or other location for collaboration with others

Your users need to learn how to do these tasks in SharePoint and OneDrive. The resources in this article can help users learn how to do these and other tasks. If you have specific business processes around these tasks, you may need to create separate documentation for your users to incorporate that.

If you are using both your existing solution and Microsoft 365 during your rollout, consider how users navigate back and forth and include that in the guidance you give your users.

Consider these options for helping your users navigate the transition to SharePoint and OneDrive:

- Office hours where users can attend or call in to ask questions.
- Special support channels for users in the process of migrating to SharePoint and OneDrive.
- Single-page or brief printouts or electronic documents that give steps to core tasks.
- Before and after guidance that shows the old and new way of doing tasks.

Resources for your users

The training resources in this section can help your users learn the everyday tasks they need to know to be successful with SharePoint and OneDrive.

Getting started

These resources can help your users learn the basics of SharePoint and OneDrive.

SharePoint help & learning

OneDrive help & learning

Get started with OneDrive

Should I save files to OneDrive or SharePoint?

Save a file to a SharePoint library

Protect your files by saving them to OneDrive

Transfer files to your personal OneDrive with the Mover Transfer Wizard

Training

OneDrive training - Intro to OneDrive

SharePoint training - SharePoint Quick Start

SharePoint video training

Use OneDrive in Microsoft 365

Collaboration spaces

If you choose to allow your users to create SharePoint sites and other related collaboration spaces such as teams, these resources can help them learn how.

- Create a team site in SharePoint
- Create a communication site in SharePoint
- Create a team from scratch

Training

Collaborate with SharePoint in Microsoft 365

Sharing

These references can help your users learn how to use the sharing and collaboration options in SharePoint and OneDrive.

Share SharePoint files or folders

Share OneDrive files and folders

SharePoint sharing and permissions

Share and collaborate with OneDrive

Viva Learning

Viva Learning is a centralized learning hub in Microsoft Teams where your users can discover, share, recommend, and learn from content libraries provided by both your organization and others. Viva Learning makes it easy to create learning resources for your users about how to use OneDrive and SharePoint in your organization.

For more information about Viva Learning, see Overview of Microsoft Viva Learning and Viva Learning Overview.

Next steps

Roll out SharePoint and OneDrive

Related articles

Plan for SharePoint and OneDrive in Microsoft 365

Feedback

Was this page helpful? Yes No

Provide product feedback

Guided Walkthrough - Create a communication site for your organization

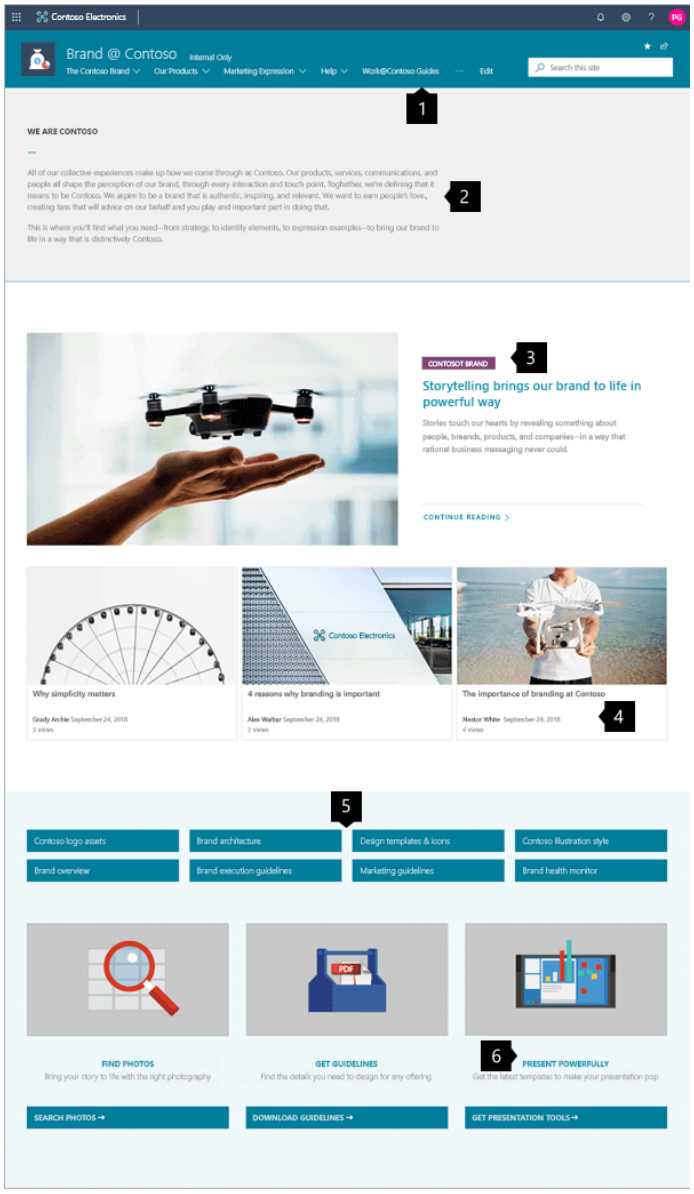
In this article, we show you elements of a communication site to inspire you and help you learn how to create similar sites for your own organization. In this example, the site is optimized to communicate your strategy and guide employees in how to express your brand in their work.

First, if you haven't already created a Communication site, check out the Create a communication site in SharePoint.

Once you create your site and know how to edit pages, you can use the following steps to add the elements shown.

Example communication site

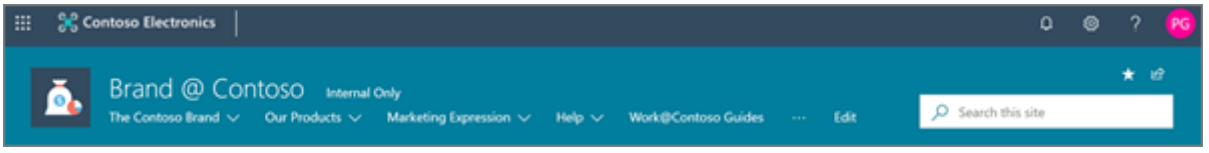
Expand table

Image of the homepage	Customization instructions
	**1. Make discovery of content easy** Quickly guide visitors with navigation. *Learn how* **2. Set the mission** A text web part highlights the mission. *Learn how* **3. Feature content** Emphasize ideas with the Hero web part. *Learn how* **4. Display topical news** Show the latest news. *Learn how* **5. Offer important links** Show related resources with Quick links. *Learn how* **6. Call-to-action** Combine web parts to increase impact. *Learn how*

Create clear and useful navigation

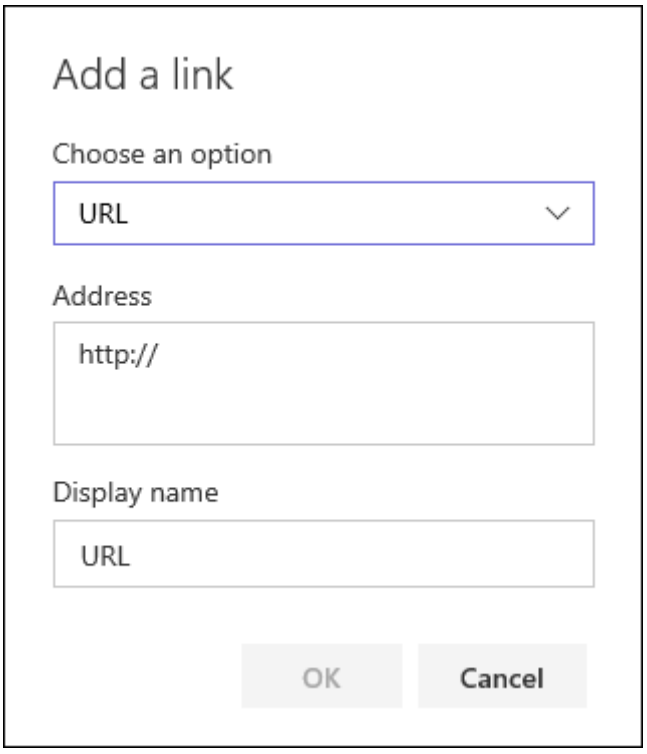
Phases of change management:

Make your site easy to get around so users can find what they're looking for, or to help users discover more content.



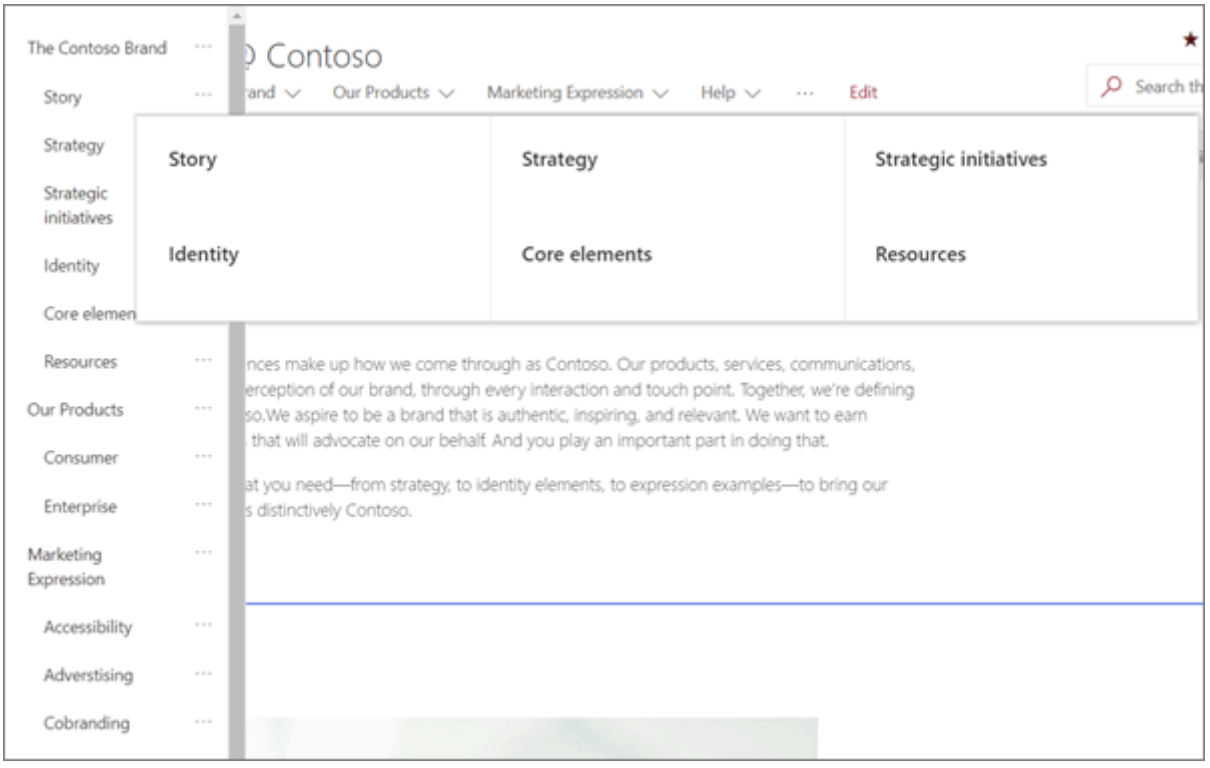
Select **Edit** to the right of the top menu, hover over the location in the menu where you want to add a link, and select +. Then add the type of link, your link, and a name to display in the navigation bar in the **Add a link** dialog box. Want to reorder your navigation links? Just drag

them into the position you want. Learn more about how to customize the navigation on your SharePoint site.



Mega menu

When a communication site is associated with a hub site, site owners can quickly and easily customize the organization and navigation of a SharePoint site. Learn what you need to know about mega menus in Create a mega menu in hub sites.



Selecting **Edit** on the top menu opens a three-level outline list. The example site uses only two of three possible levels on its mega menu: the main menu and a sub menu.

- Select the ... control on the right of the item name to set the item's link and outline level.

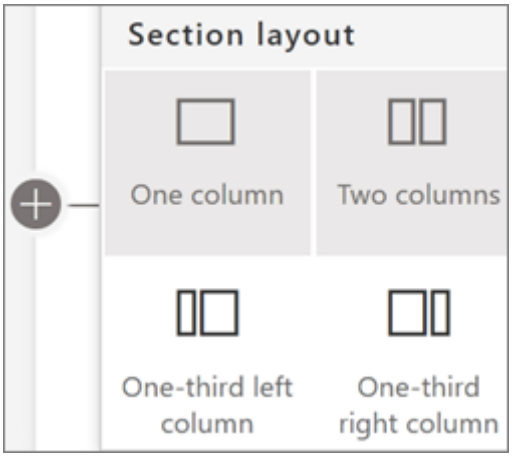
Back to top

Manage sections and web parts

Start editing by clicking **Edit** on the top right of the page.

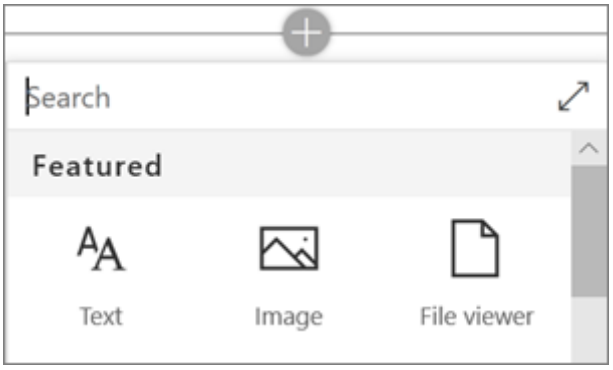
When you are editing, on the left, below the header your drafts can be saved for later or discarded.

The + symbol before or after a section adds a section using one of several layouts.



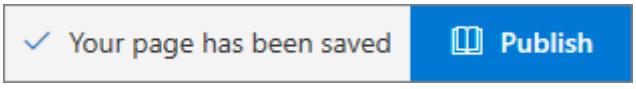
Sections make up your page, and are you place one or more web parts. While editing the page, each section shows controls to edit the layout, move, or delete the sections. For information on working with sections, see Add or remove sections and columns on a page.

Select the plus symbol in a section, which may appear before or after a web part in a section, to see the many types of web parts available. For more information on all web parts, see Using web parts on SharePoint pages.



Web parts may be edited, moved, or deleted within sections. The **Edit web part** icon opens detailed controls unique to each web part type.

When your page updates are ready, select **Publish** to make them visible to everyone in your organization who has permissions to view the content.



> **Tip**
>
> To manage all of your pages on the site, click **Pages** on the top menu.

For more information on using pages, see Create and use modern pages on a SharePoint site.

Back to top

Add formatted text with the Text web part

For more information on using the Text web part, see Add text and tables to your page with the Text web part.

Enhance the message

The example site creates a balance of text and imagery using several different web parts. At its core, the site is designed to inspire visitors to adopt branding guidelines and provide the tools needed to follow through.

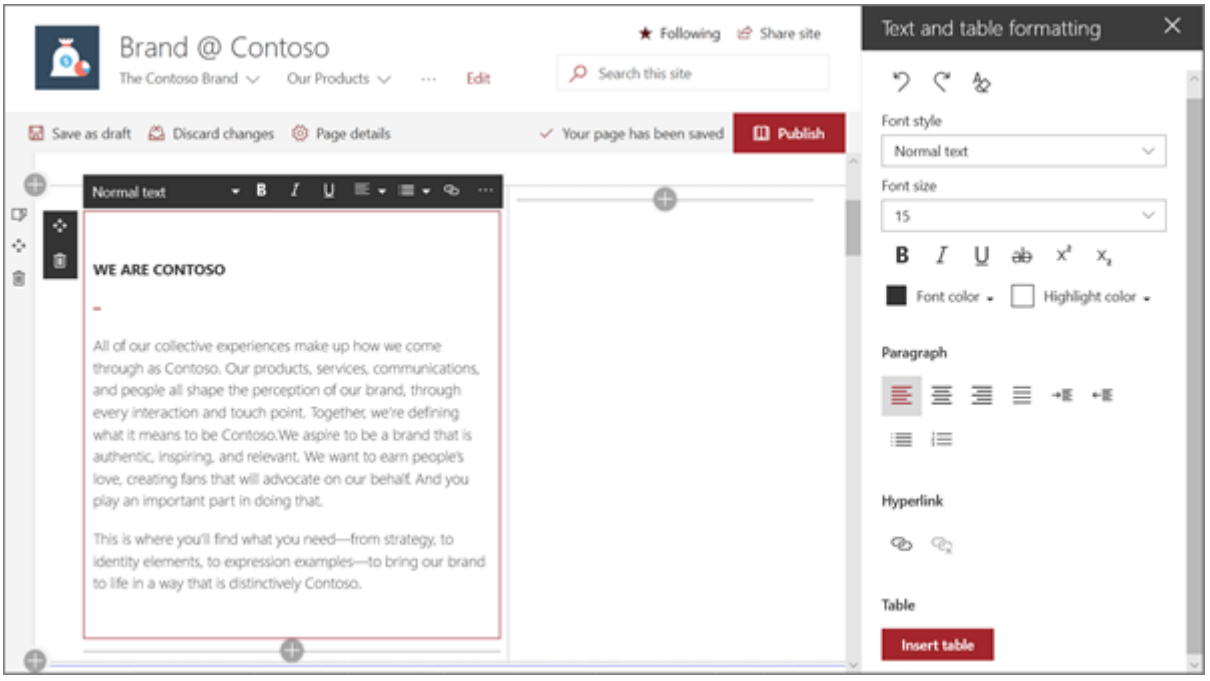
Layout matters

The first section of the page uses the section layout tools with a Text web part to create impact by enforcing white space to the right of the mission statement.

Refined typography

The Text web part builds on style of the built-in site template. The Text web part is using the **Normal** text style. Clicking the **...** control at the right end of the formatting toolbar offers more options to the right of the web part.

In this example, the web part is in a two-column section.



Back to top

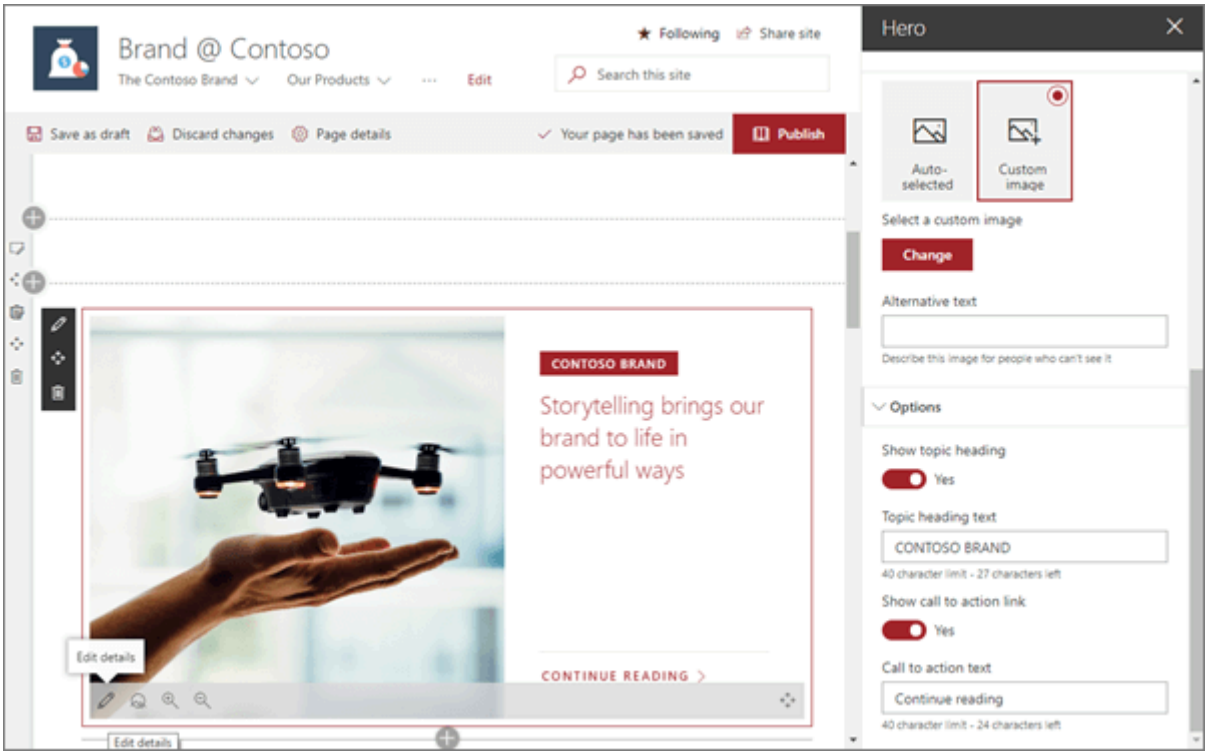
Focus on priorities with the Hero web part

Let your team know what's most important with high-impact hero images, company branding, and important news. The initial impact of the site home page is created by large and eye-catching images of the Hero web part. The page uses the Hero web part in its **Layers** option.

Hero layout

Editing the web part presents layout options. The **Layers** option, such as the one shown above, sets each image as a layer with the image next to the title. Up to five layers are possible, so that you can use the web part to fill the entire page.

In this example, the Hero web part uses one layer and is in a full-width section.



Customize each layer

Options for adding a heading and a linked call to action allow each layer to be a starting point for a deeper message.

It's possible to create an entire visual homepage with just the Hero web part using **Layers**.

For more information on using the Hero web part, see Use the Hero web part.

Back to top

Add important news with the News web part

Automatically collect news and timely content

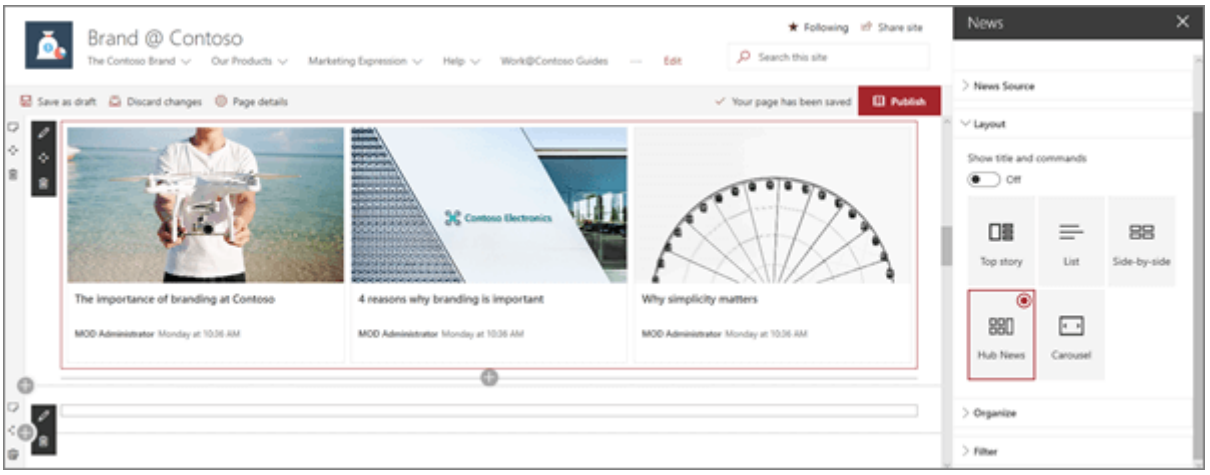
The News web part provides controls to choose the **News Source** and **Layout**, and to **Organize** and **Filter** the content to keep the content topical.

For more information on using the News web part, see Use the News web part on a SharePoint page.

Refine impact with news layouts

Changing the layout changes impact a news feed has. Under **Layout**, there are five options to adjust how news items are presented. In this example, news stories are using the **Hub News** layout. The stories are presented side-by-side with three equal-sized images because only three news stories on the site are published.

In this example, the web part is in a one-column section.



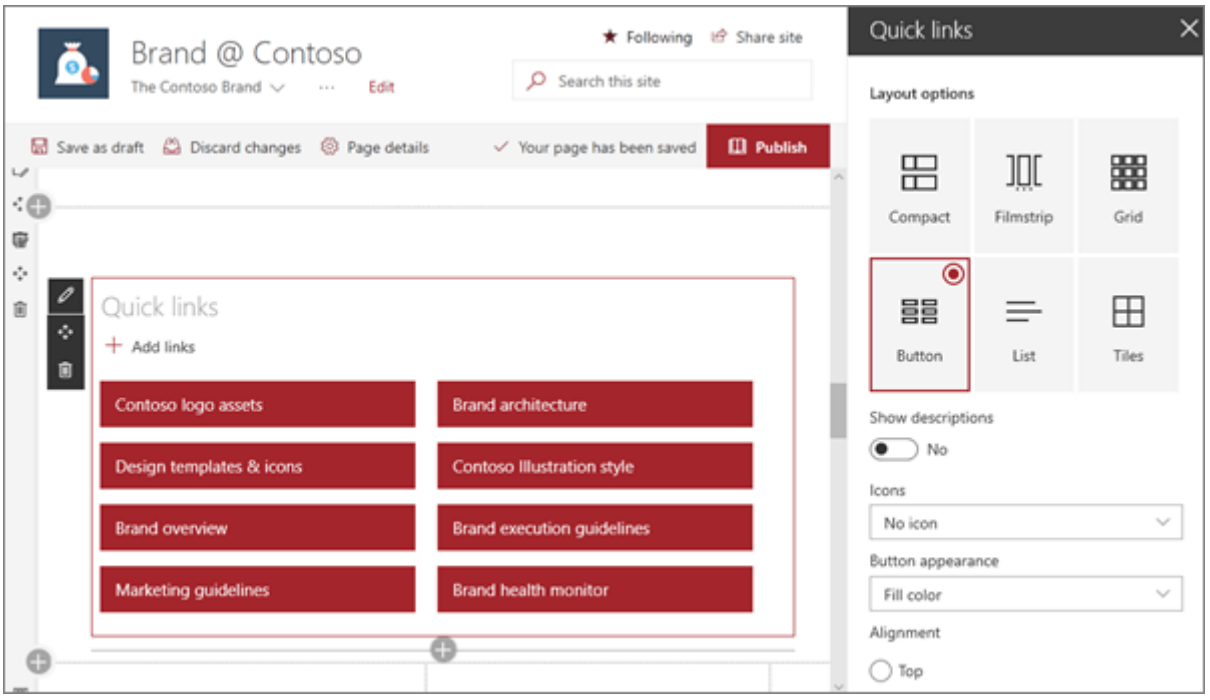
Back to top

Use color and icons with the Quick Links web part

The Quick links web part provides dozens of professional styles for links created from a few easy-to-use options.

Start with the six base layouts, then adjust by color and alignment. Optionally, you can add icons or text descriptions to increase the menu impact. In this site example, this web part uses the Button layout.

For more information on using the Quick Links web part, see Use the Quick Links web part.

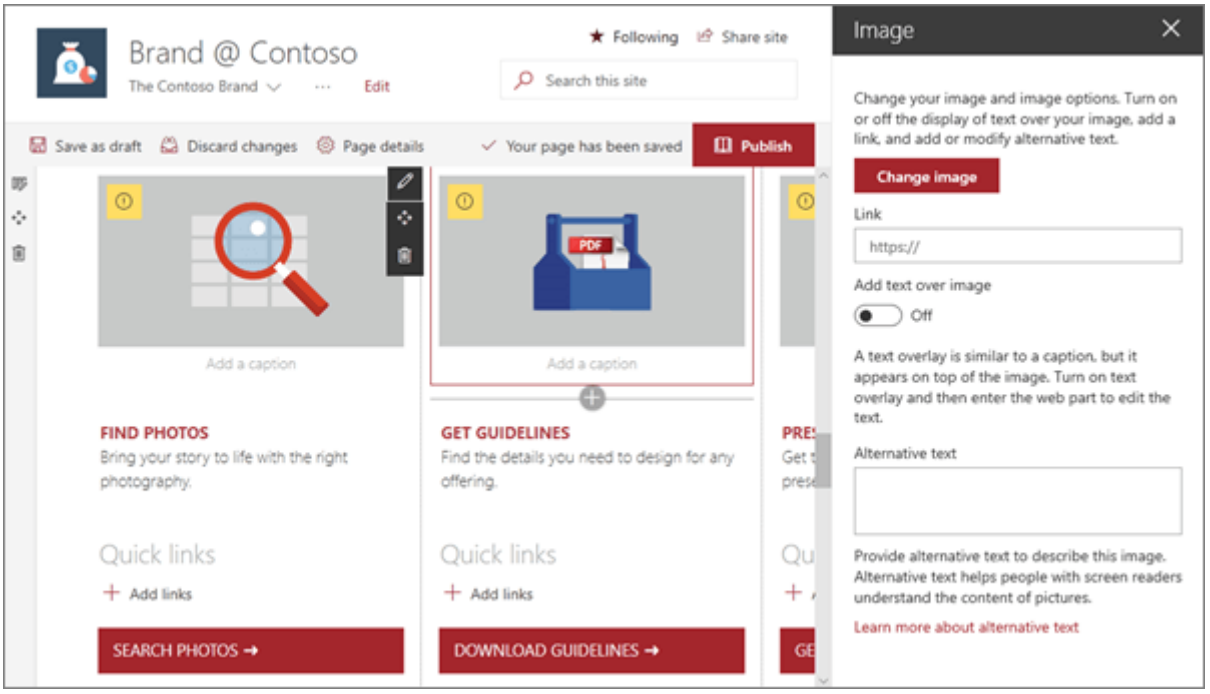


Back to top

Create call-to-action elements

The example site uses images to enhance the page look. It combines the Image web part with the Text and Quick links web parts to create a high visibility call-to-actions menu guiding visitors to key branding actions.

In the following example, the web parts are in the second column of a three-column section. For more information on using the Image web part, see Use the Image web part.



Back to top

Want more?

Get inspired with more examples in the SharePoint Look Book.

Last updated on 06/24/2026

Guided walkthrough: Creating a Team site

In this article, we show you elements of an example SharePoint Team site to inspire you, and help you learn how to create similar sites for your own organization.

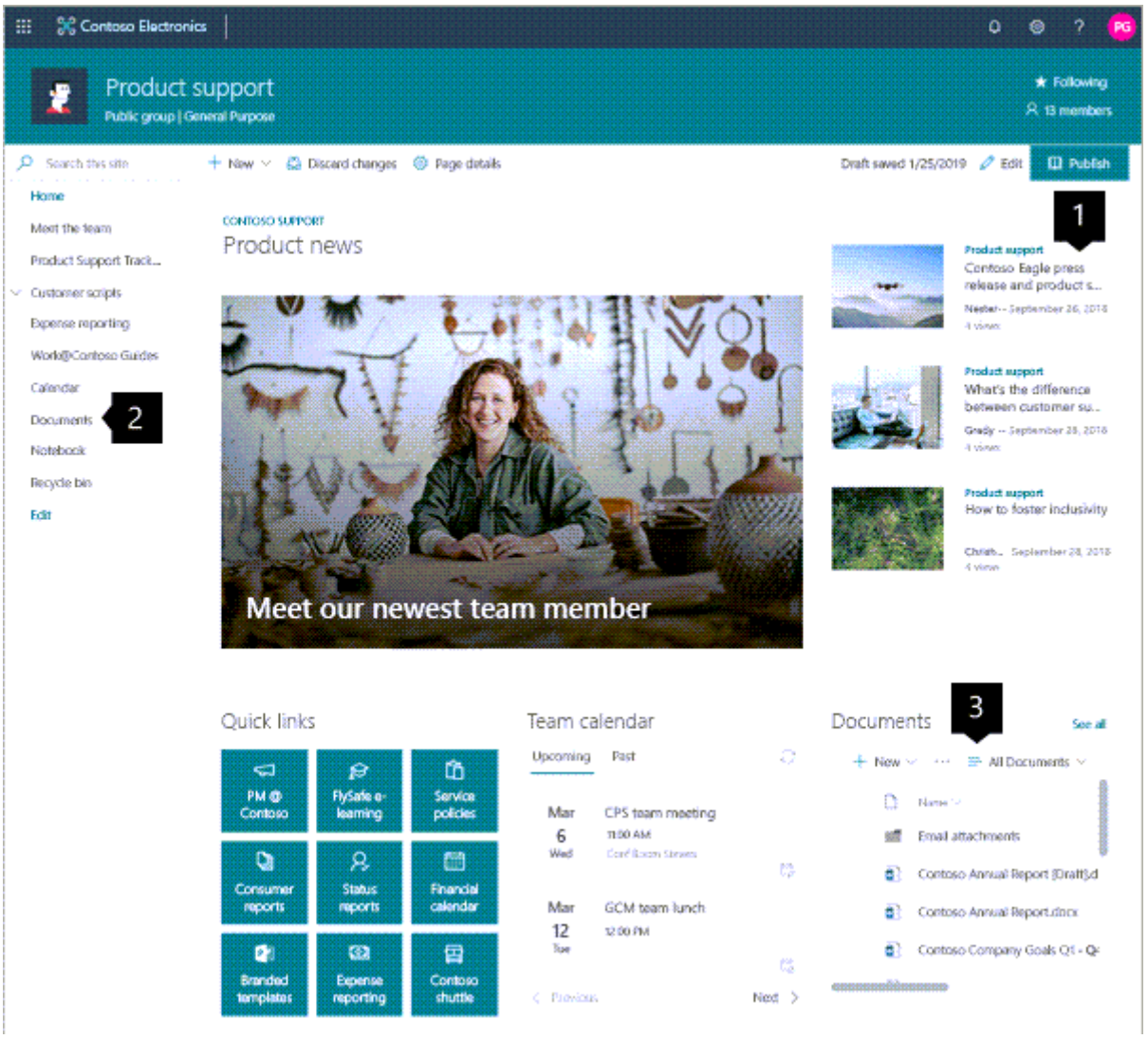
Use a team site when you want to collaborate with other members of your team or with others on a specific project. With a team site, typically all or most members can contribute content to the site and the information is limited to only the members of the team or project and specific stakeholders. Additionally, team sites are connected to groups and a Teams channel. This makes it easy for your team to have group permissions, and a Teams space to chat, meet, and share files.

First, if you haven't already created a Team site, check out Create a team site in SharePoint.

If you need to learn how to edit and publish the page on your site, check out the section Manage sections and web parts in this article.

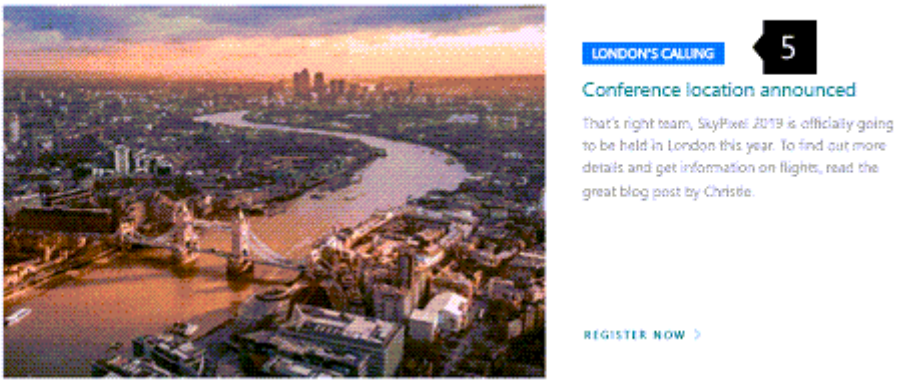
Once you've created your site and know how to edit pages, you can use the following guidance to add the elements shown.

Example Team site

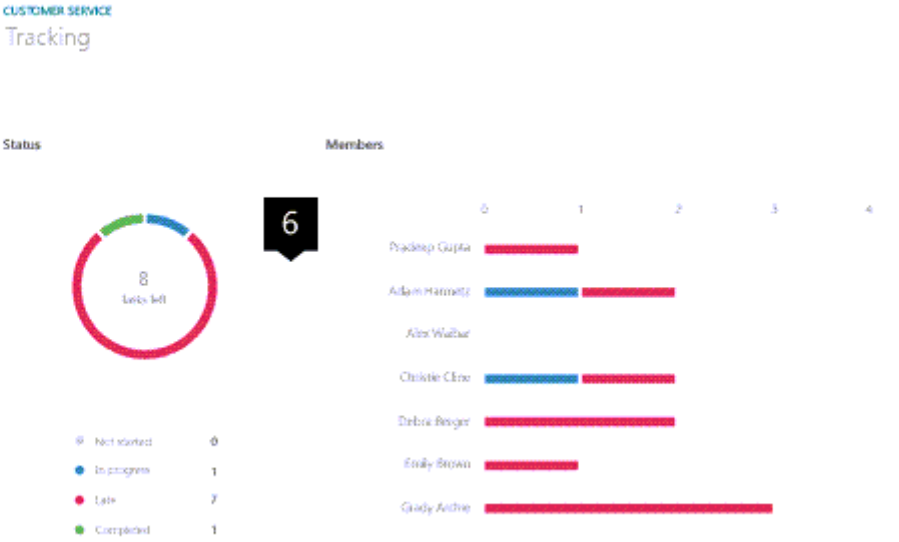


1. **Team highlights and news** Get visual while sharing information. Learn how
2. **Quick launch** Add links to more content around the site. Learn how
3. **Inform the team** Offer links, events, and content related to team work. Learn how

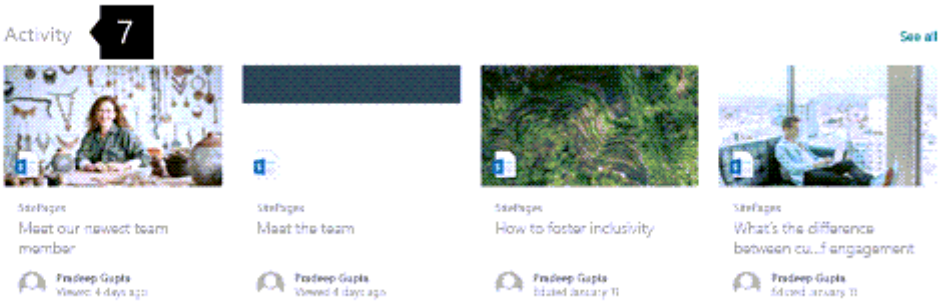
4. **Share news about the team** Offer news items of interest to the team. Learn how



5. **Highlight important information** Increase visibility of key information with the Hero web part. Learn how



6. **Display project status** Use the Planner web part to show team progress on projects. Learn how



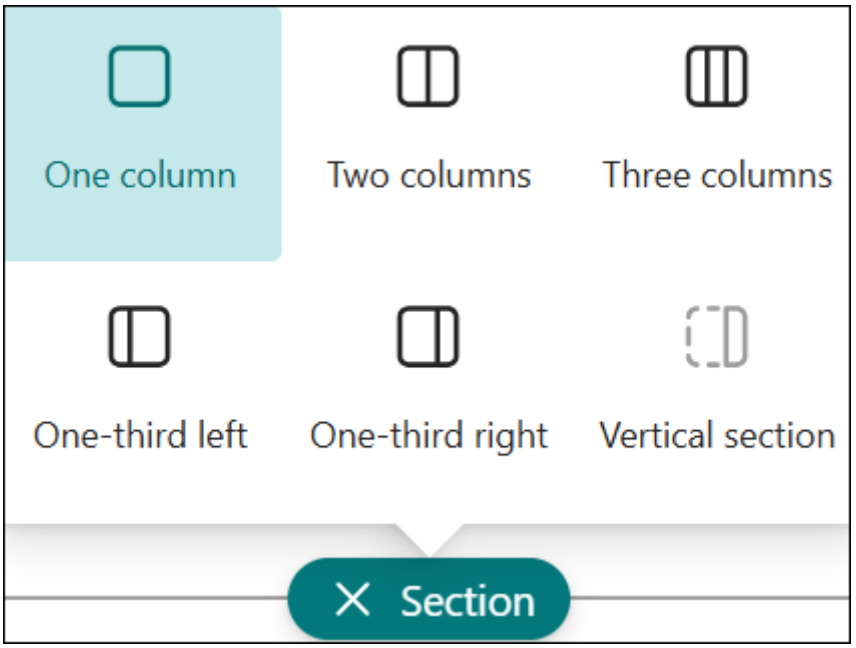
7. **Display recent activity** Automatically show the most recent updates to team site content. Learn how

Manage sections and web parts

Sections make up your page, and are where you place one or more web parts. When you edit the page, each section shows controls to edit the layout, move, or delete the sections.

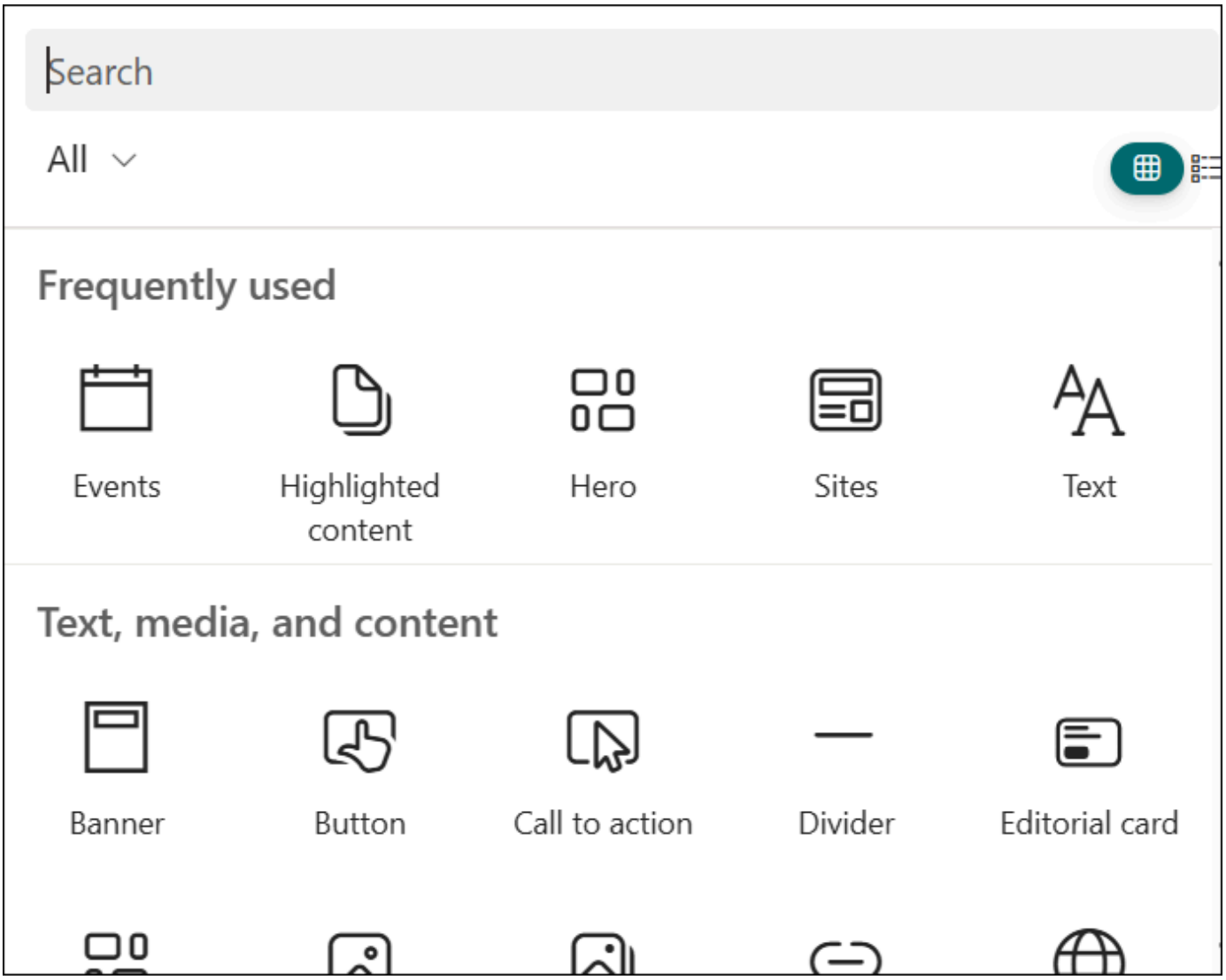
Start editing by selecting **Edit** on the top right of the page.

The + symbol before or after a section adds a section using one of several layouts.



For information on working with sections, see Add or remove sections and columns on a page.

To add web parts to sections, select the plus symbol in a section, which may appear before or after a web part in a section. Then select a web part to use. For more information on all web parts, see Using web parts on SharePoint pages.



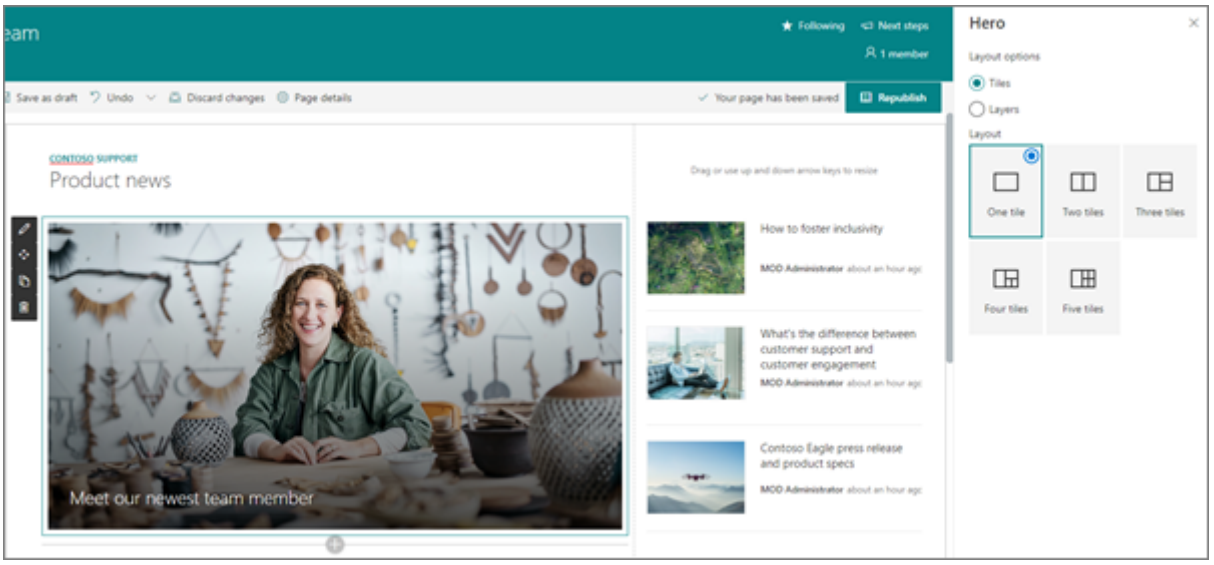
Web parts may be edited, moved, or deleted within sections. The **Edit properties** icon opens detailed controls unique to each web part type.

Back to top

Team highlights and news

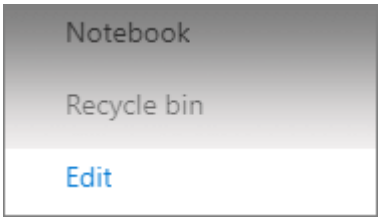
The first section of this example page uses a two-column layout. In the first column is a Hero web part that uses a one-tile layout to link to information introducing a new team member. Above that is a Text web part with a title. In the second column is a News web part that uses a list layout. Above that is a Spacer web part to help align the two web parts.

Learn how to use the Hero web part and the News web part.

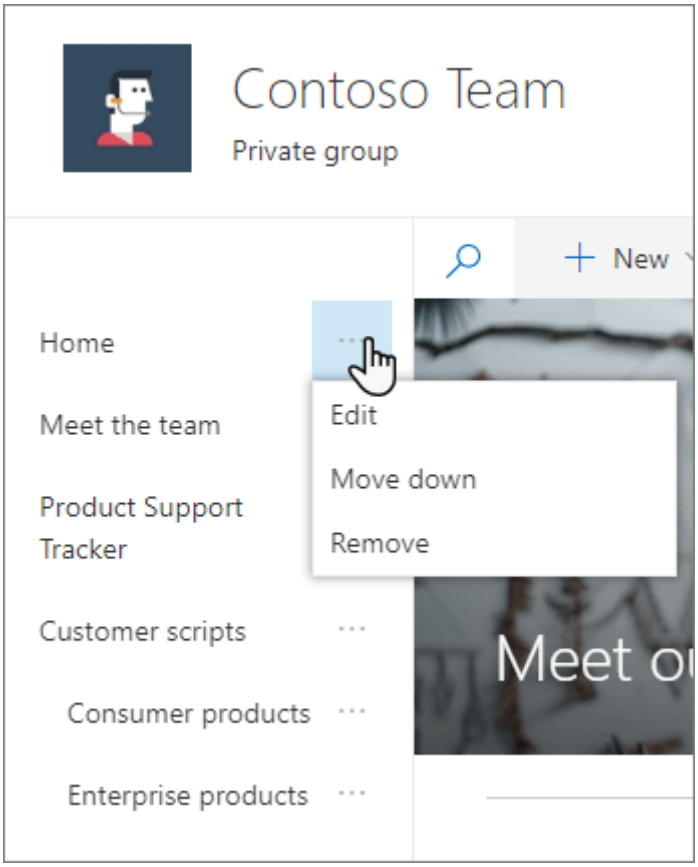


Quick launch

You can quickly and easily customize the organization and navigation of your SharePoint site. Edit the Quick launch menu by selecting **Edit** at the bottom of the menu.



Select the **...** on the right side of each menu item to **Edit**, **Move**, or **Remove** an item.

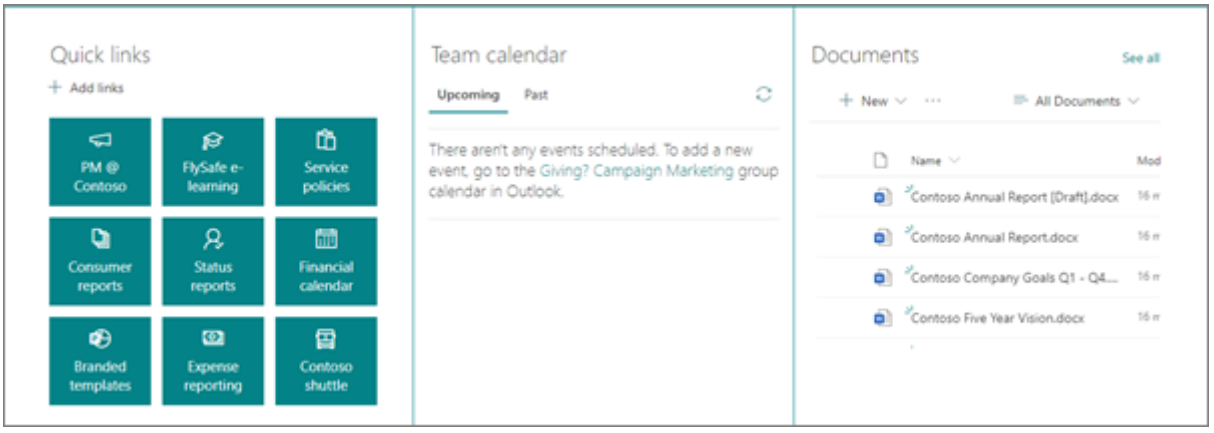


While you're editing, your drafts can either be saved for later or discarded. When your page updates are ready, select **Publish** to make them visible to site viewers.

Back to top

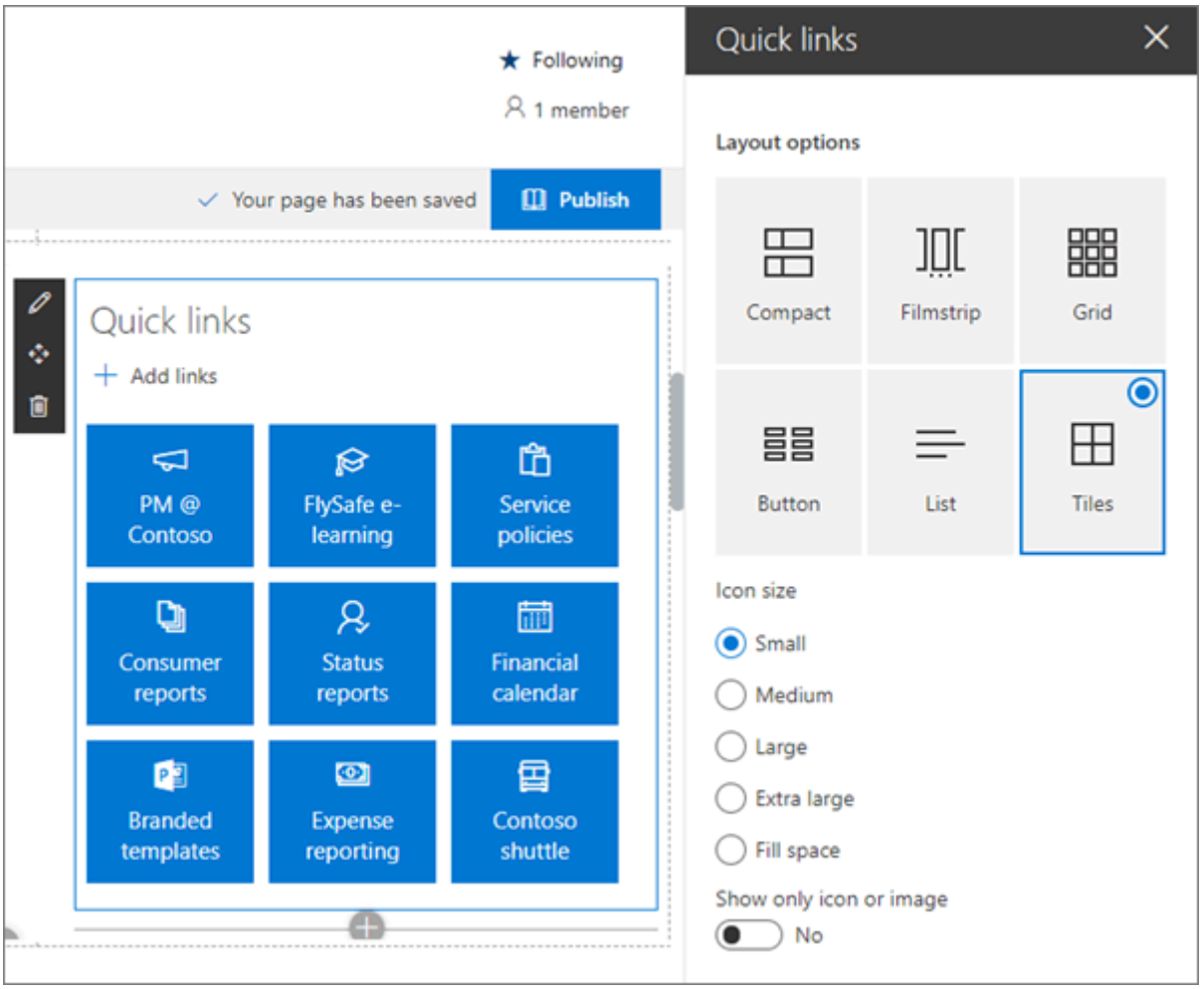
Inform the team

The second section in this example is in a three-column layout and includes the Quick links web part, the Group calendar web part, and the Document library web part.



Quick links

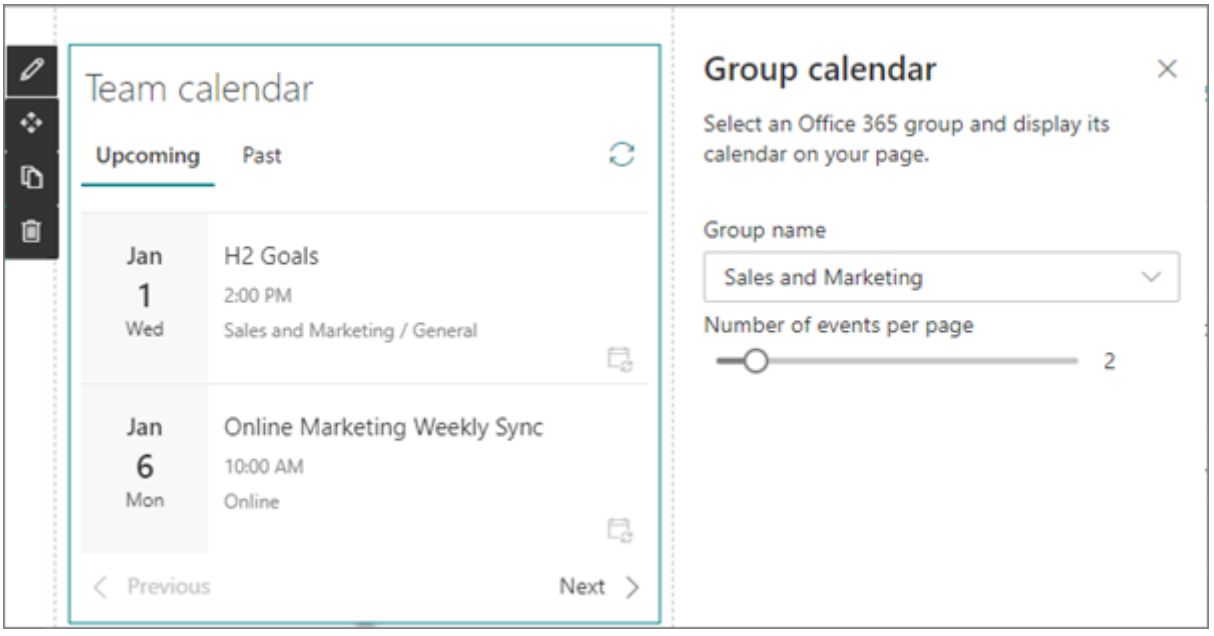
The Quick links web part offers several easy-to-use menu formats for listing links to other pages or sites. In this Team site example, this web part uses the **Tiles** layout with small icons for quick and easy reference.



For more information on using the Quick links web part, see Use the Quick links web part.

Group calendar

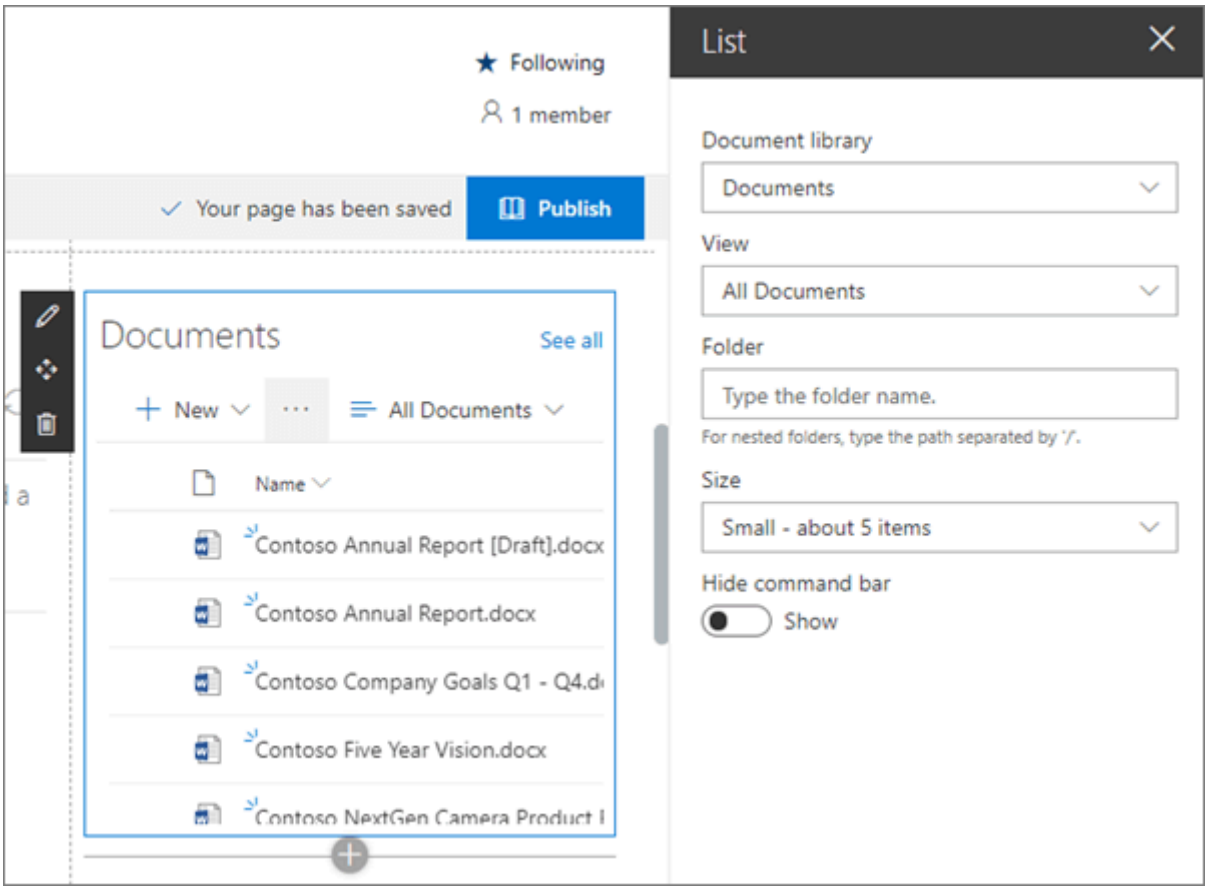
The Group calendar web part automatically shows meetings and appointments that are on your Office 365 group calendar. Office 365 groups and their associated calendars are created automatically when you create a team site.



For more information on the Group calendar web part, see Use the Group calendar web part.

List web part

Display site content including documents where the team can easily find it. You can use lists either as a document library or to track information.

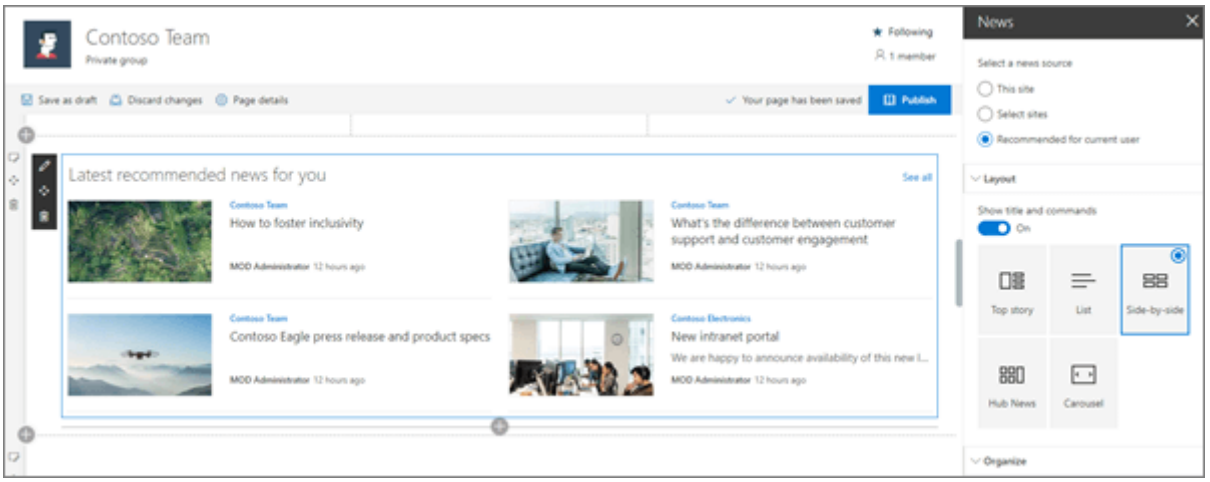


For more information on using the List web part, see Using the List web part.

Back to top

Add important news with the News web part

Team sites allow you to show news for the entire team or filter news tailored to the interests of specific users. In this example, the News web part uses **Recommended for current user** as the source and a **Side-by-side** layout in a one-column section with a background.



For more information on using the News web part, see Use the News web part on a SharePoint page.

Back to top

Highlight important information

Let your team know what's most important with high-impact hero images, company branding, and important news. The Hero web part allows you to use large and eye-catching images to draw immediate attention to the most important information on your site. The layout used in this example is **Two tiles**.

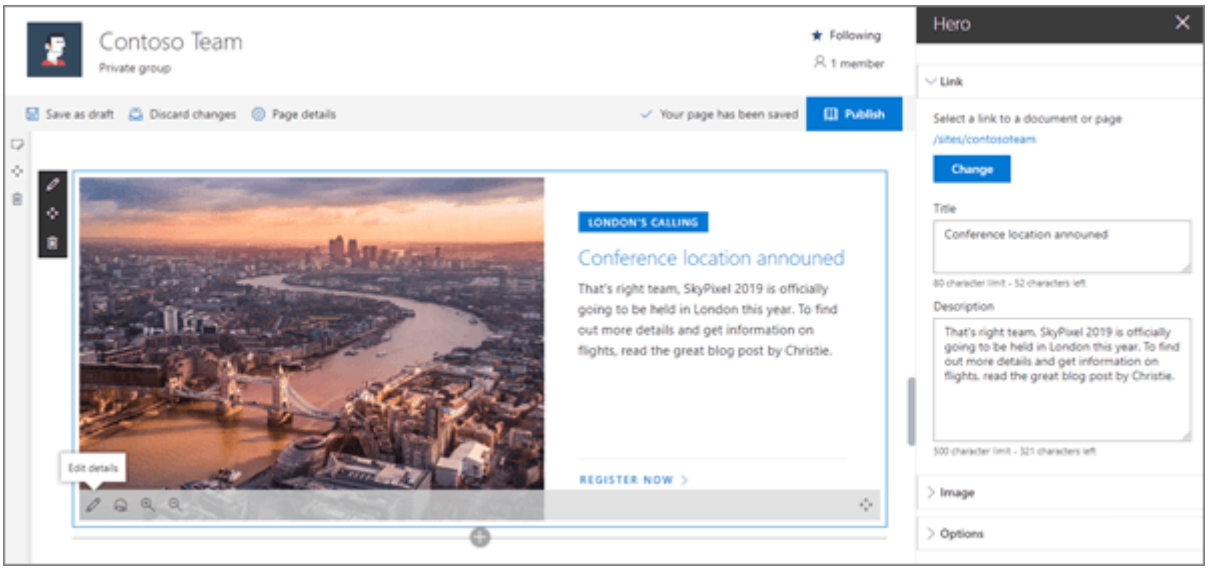
The power of tiles

Tiles can include images, topic headings, titles, descriptions, and a call to action link. Other adjustments include image scaling and setting the focus for the image zoom animation.

Each tile can be edited

Use the **Move item** control on the left to rearrange the tiles within the Hero web part. Controls on the right allow you to **Edit details** to adjust the text and image, **Set focal point** for the hover animation, and **Zoom in** and **Zoom out** of the image.

In this example, the Hero web part is in a full-width section.



For more information on using the Hero web part, see Use the Hero web part.

Back to top

Show project status

If you use Microsoft Planner to manage your projects, and have a plan created, you can use the Planner web part to show status for that plan on your SharePoint site.

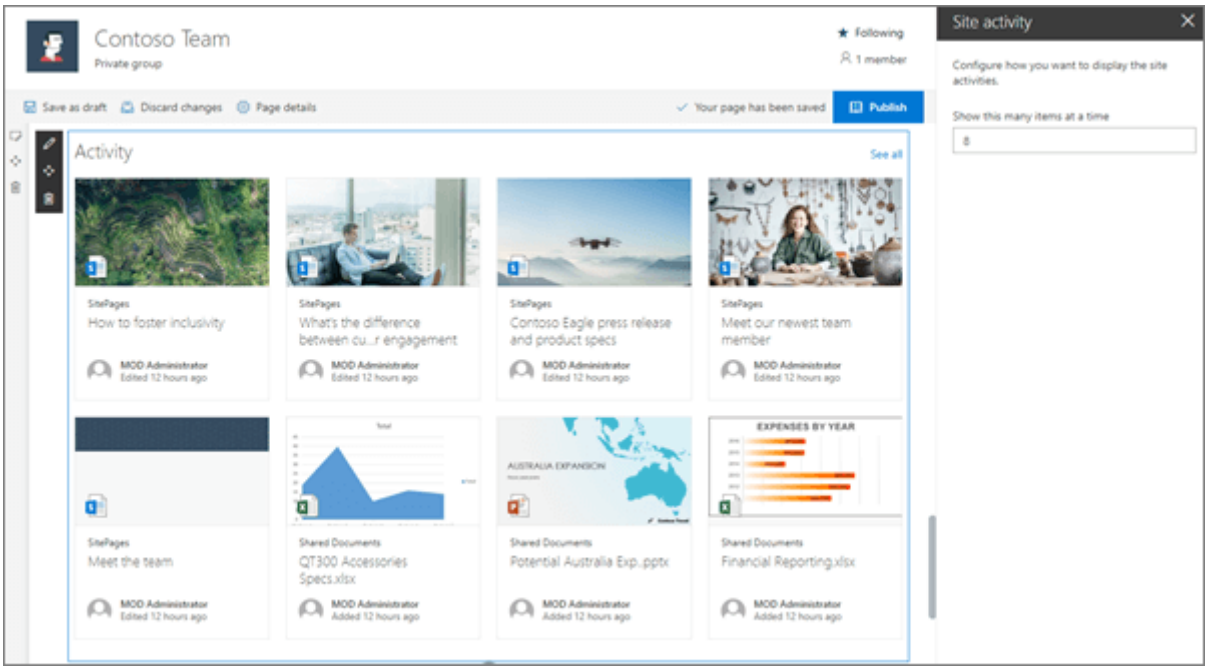
For more information on using the Planner web part, see Use the planner web part.

Back to top

Show team activity with the Site activity web part

The activity web part has only one setting - how many items to show. Activity shown by the web part includes page updates and all documents stored on the team site.

In this example, the web part is in a one-column section.



For more information on using the Site activity web part, see Use the site activity web part.

Back to top

Want more?

Get inspired with more examples in the SharePoint Look Book.

See other guided walkthroughs for creating sties for your organization.

Last updated on 06/24/2026

Guided walkthrough: Create a giving site for your organization

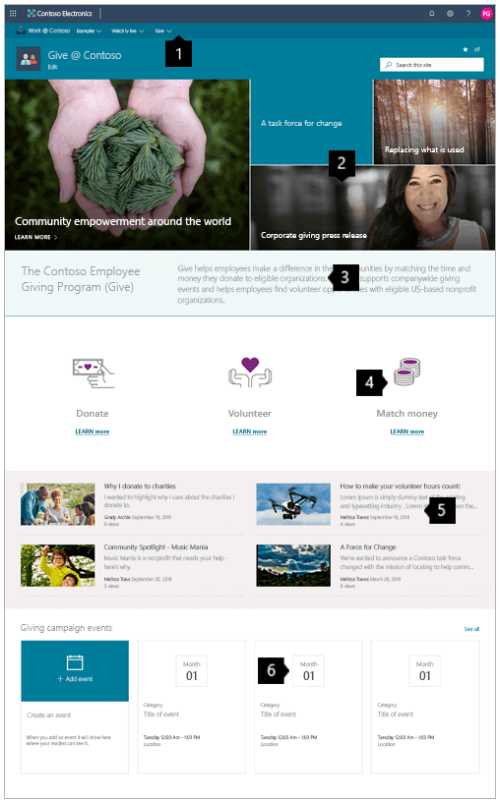
In this article, we show you elements of an example Giving site to inspire you, and help you learn how to create similar sites for your own organization. In this example, the Giving site provides an example of how a page with thoughtful design and messaging can inspire your organization. This example page is also deployed as part of a Human Resources Hub site.

First, if you haven't already created a Communication site, check out the Create your site section in this article.

Once you have your created your site and know how to edit pages, you can use the steps below to add the elements shown.

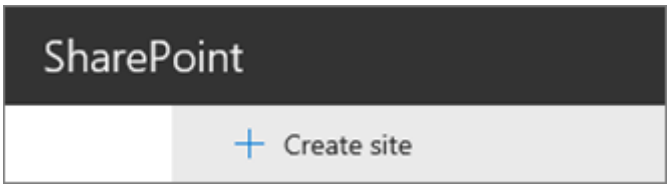
Example Giving Site

Expand table

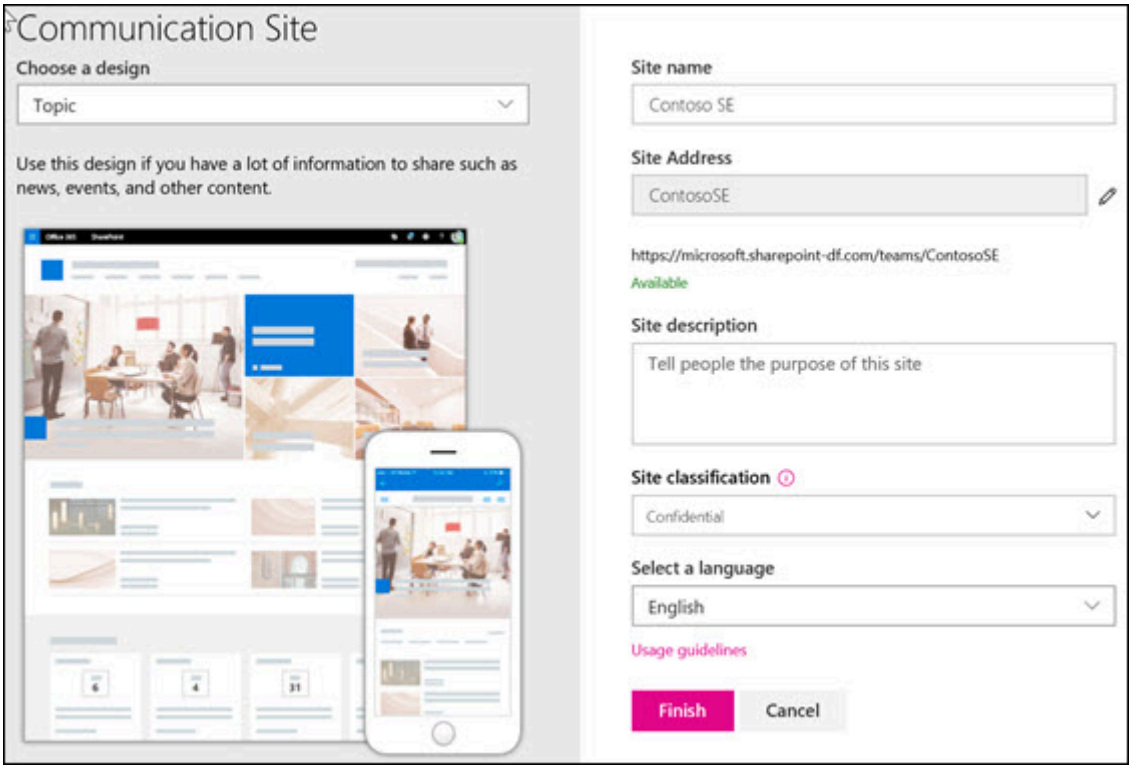
Image of the homepage	Customization instructions
	**1. Make your site easy to get around** Customize navigation to make it easy for people to discover important content on your site. *Learn how* **2. Inspire with imagery and information** Use eye-catching and inspiring images that link to content at the top of the page. *Learn how* **3. Make a statement** Create professional, consistent text with multiple formatting choices. *Learn how* **Call to action** Make it easy for people to take action right away. *Learn how* **4. Spread the news** Share ideas and stories that enhance your message. *Learn how* **5. Get events on the calendar** Add an event calendar to keep people up to date on related events. *Learn how*

Create your site

To make a site like the one shown here, you'll create a Communication site. To do this, select **Create site** from the SharePoint start page (or, if you're going to associate this site with an existing Hub site, navigate to the hub site and select **Create site** there so that the communication site is automatically associated with that hub site).



Next, choose **Communication site**, and then the **Topic** layout. Fill out your site name, description, and other information, and select *Finish*. Then you'll get a template with the same type of layout as the example in this article.

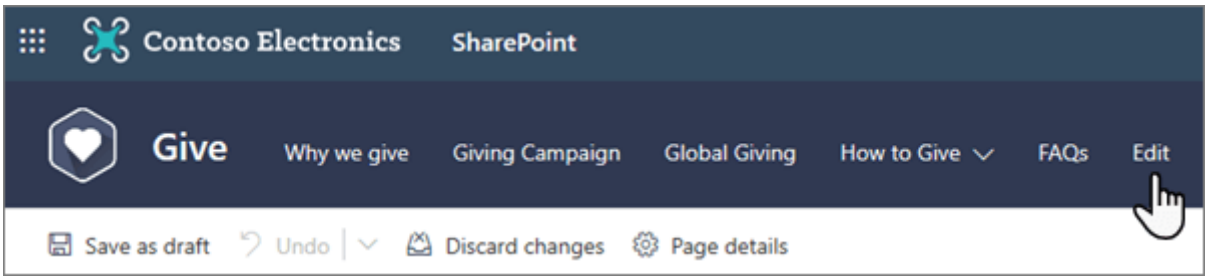


For more information, see Create a communication site in SharePoint Online.

Back to top

Make your site easy to get around

You can quickly and easily customize the organization and navigation of your SharePoint site to make it easy for your visitors to navigate the site and find the information they need.



- **Add and edit the main menu** Easily edit the top menu to link the page to other SharePoint pages or on the Internet.
- **Mega menus** When a site is deployed as part of a hub site, you can create powerful mega menus.

For more detailed information on working with navigation, see Customize the navigation on your SharePoint site.

Back to top

Inspire with imagery and information

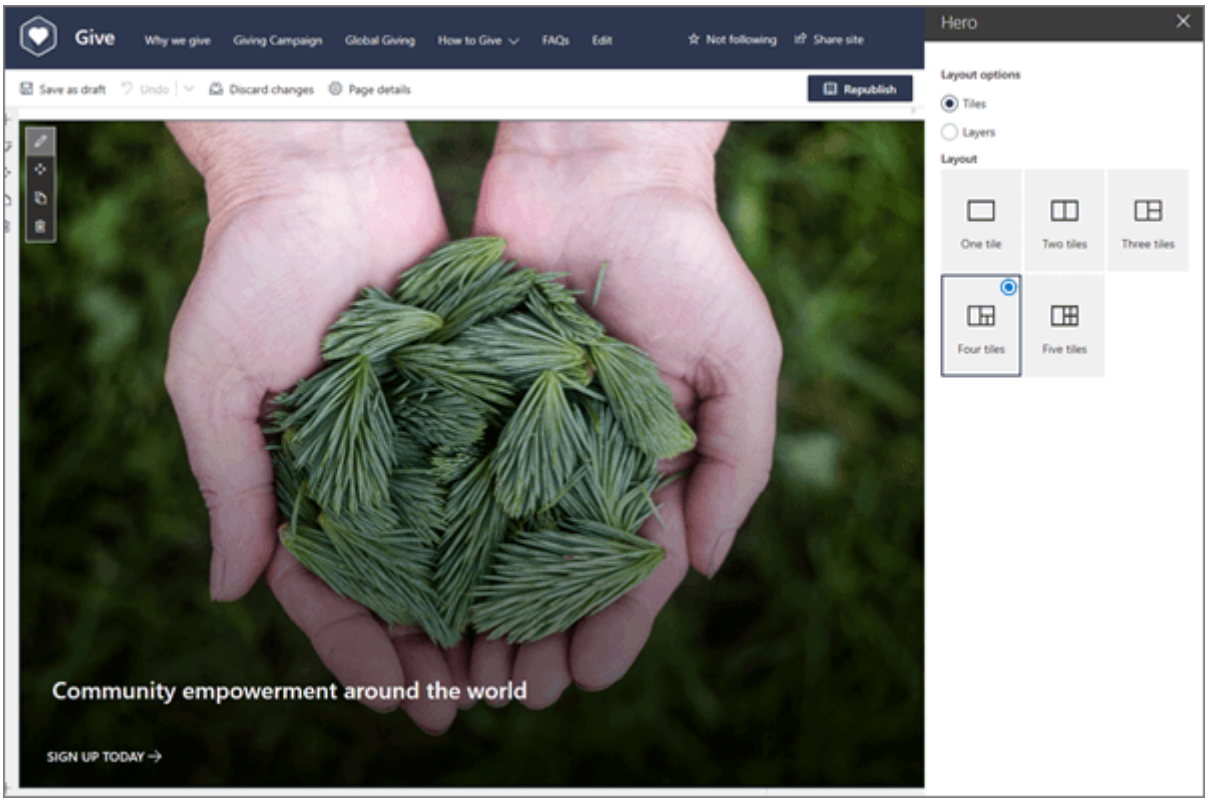
Let your team know what's most important with high-impact hero images, company branding, and important news. The initial impact of the Giving site home page is created by large and eye-catching images of the Hero web part. The layout used in this example is **Four tiles**.

Hero layout

Editing the web part presents layout options. The **Tiles** option, such as the one shown above, presents layouts for between one and five tiles. The **Layers** option sets each image as a layer with the image next to the title. Up to five layers are possible, so that you can use the web part to fill the entire page.

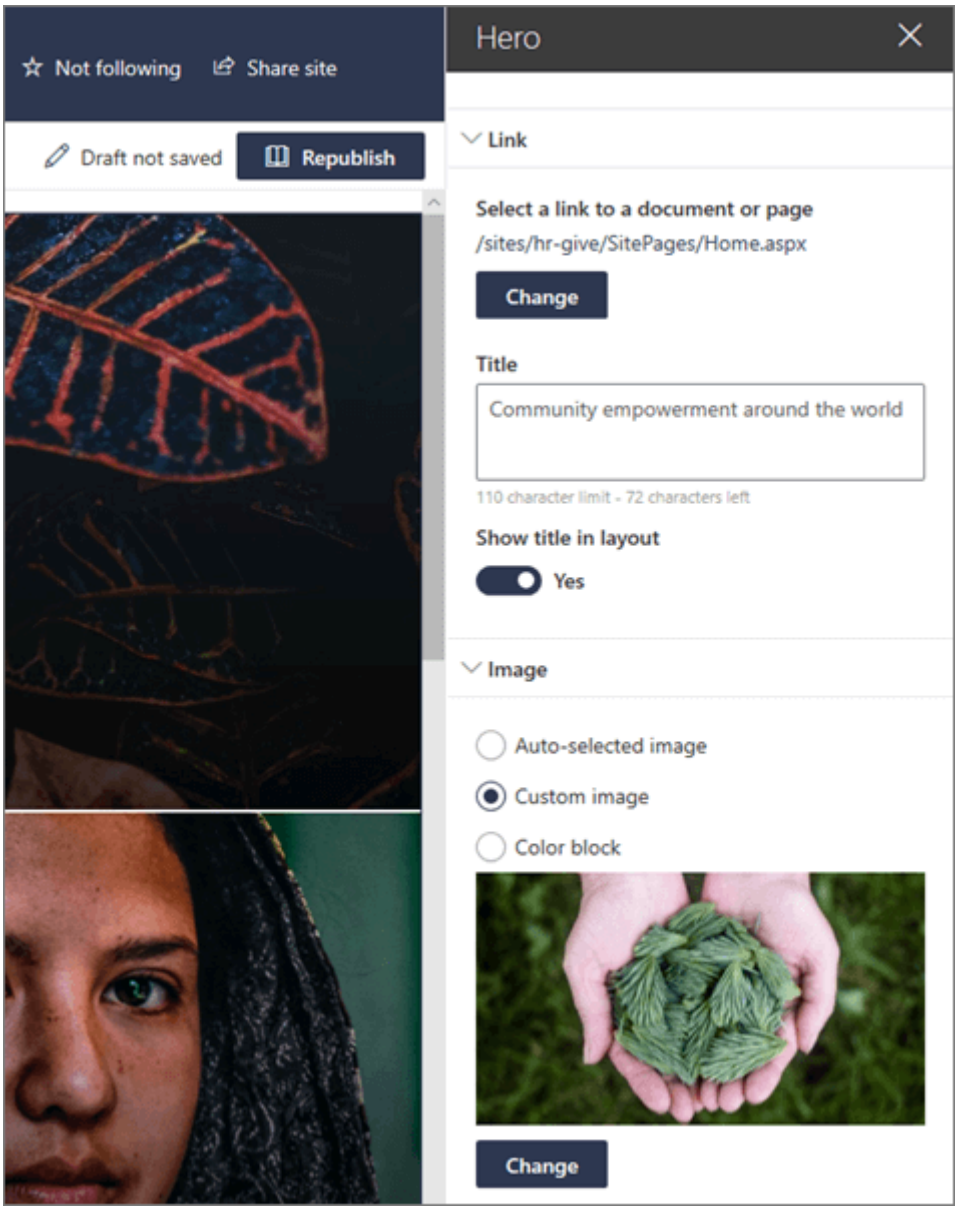
In this example, the Hero web part is in a full-width section.

Use the **Move item** Move web part button on the left to rearrange the tiles within the Hero web part.



Customize each tile

When you select a tile, you'll see a toolbar at the bottom of the tile where you can select **Edit details** where you can change the link and image used. With the larger tile, you can also set call to action text and link. On the same toolbar, you can set focal point for the hover animation, plus zoom in and zoom out of the image.



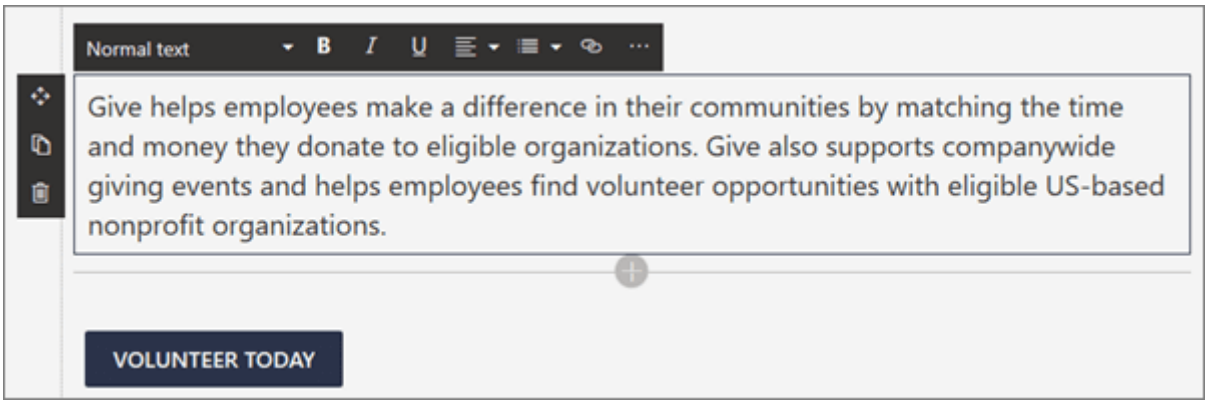
For more details on using the Hero web part, see Use the Hero web part.

Back to top

Make a statement with the text web part

Uniform, professional-looking typography is a feature of this site, and the Text web part provides tools to refine the impact of text used in several locations on this page. In this example, the Text web part is using the **Normal text** style. Selecting the ellipses (...) at the right end of the formatting toolbar offers additional options.

In this Giving site example shown below, the web part is in a one-column section.

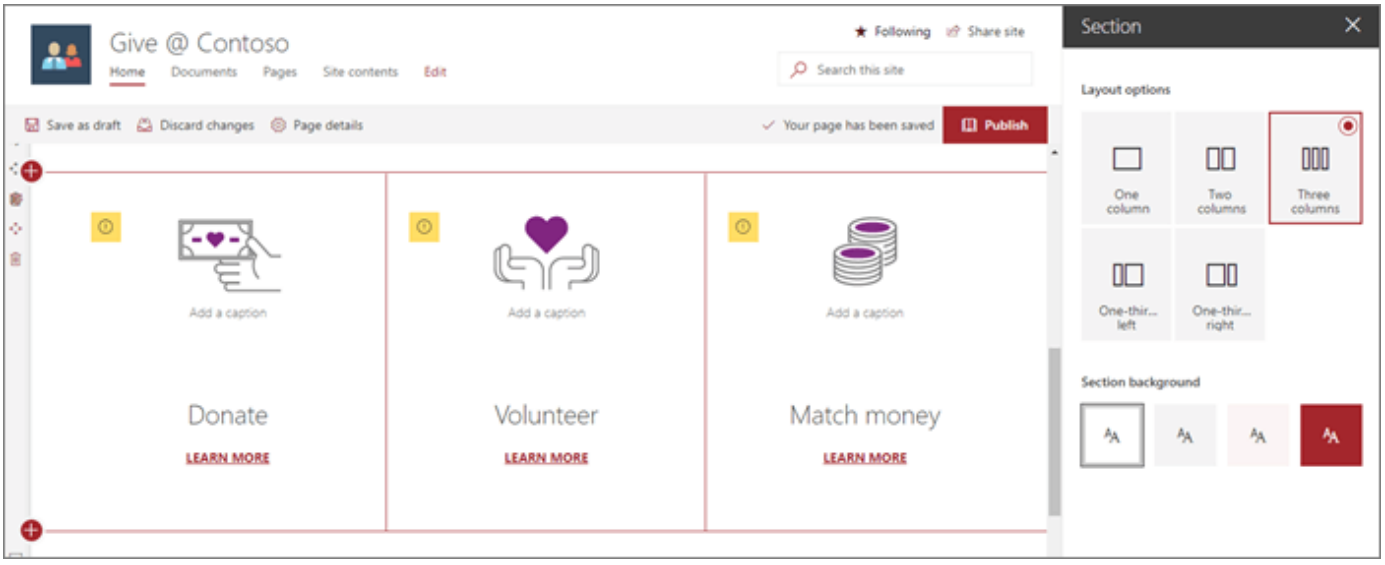


For more details on using the Text web part, see Add text and tables to your page with the Text web part

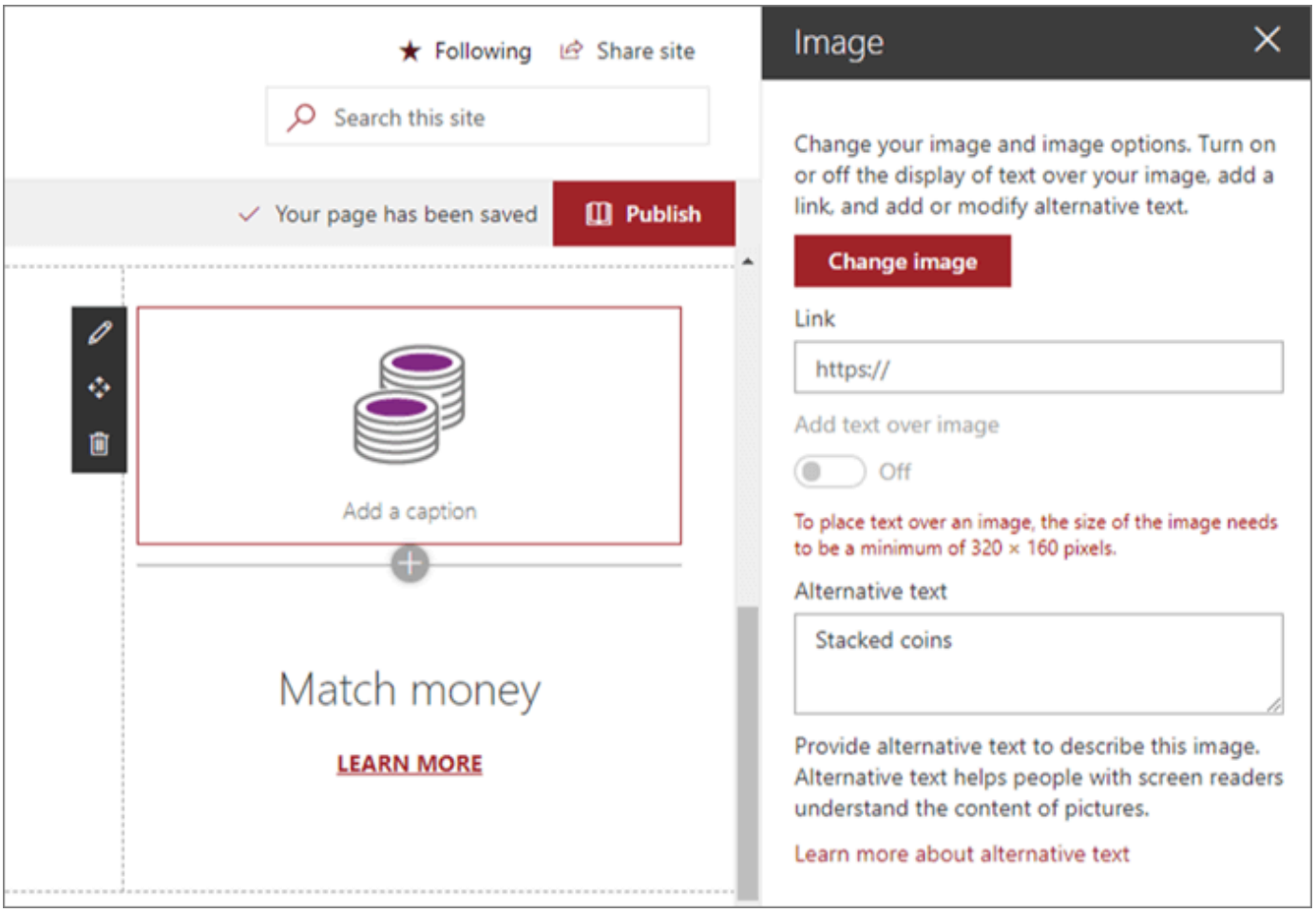
Back to top

Call to action

In this example, the Giving site has a section using a three-column layout with images and links within the section.



Here, the Image web part is paired with a text web part to create a call to action.

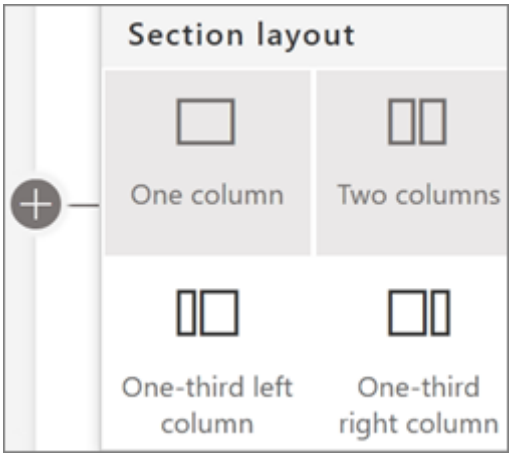


For more details on using the Image web part, see Use the Image web part.

Working with sections

To create sections, start editing by clicking **Edit** on the top right of the page.

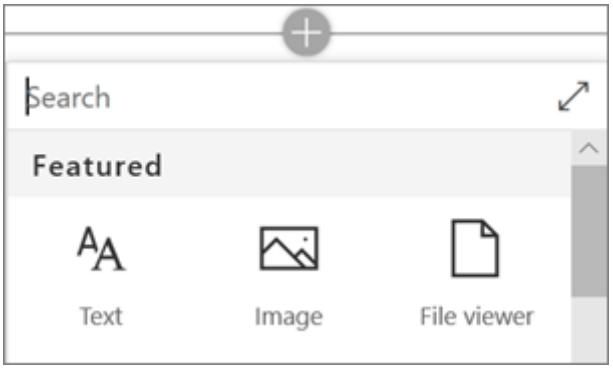
The + symbol before or after a section will add a section using one of several layouts.



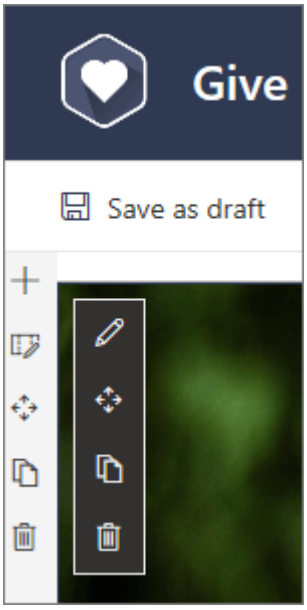
Sections make up your page, and are you place one or more web parts. While editing the page, each section will show controls to edit the layout, move, or delete the sections. For information on working with sections, see Add or remove sections and columns on a page.

Working with web parts

Select the plus symbol in a section, which may appear before or after a web part in a section, to see the many types of web parts available. For more information on all web parts, see Using web parts on SharePoint pages.



Web parts may be edited, moved or deleted within sections. The **Edit web part** icon opens detailed controls unique to each web part type.



When your page updates are ready, Selecting **Publish** to make them visible to your audience.

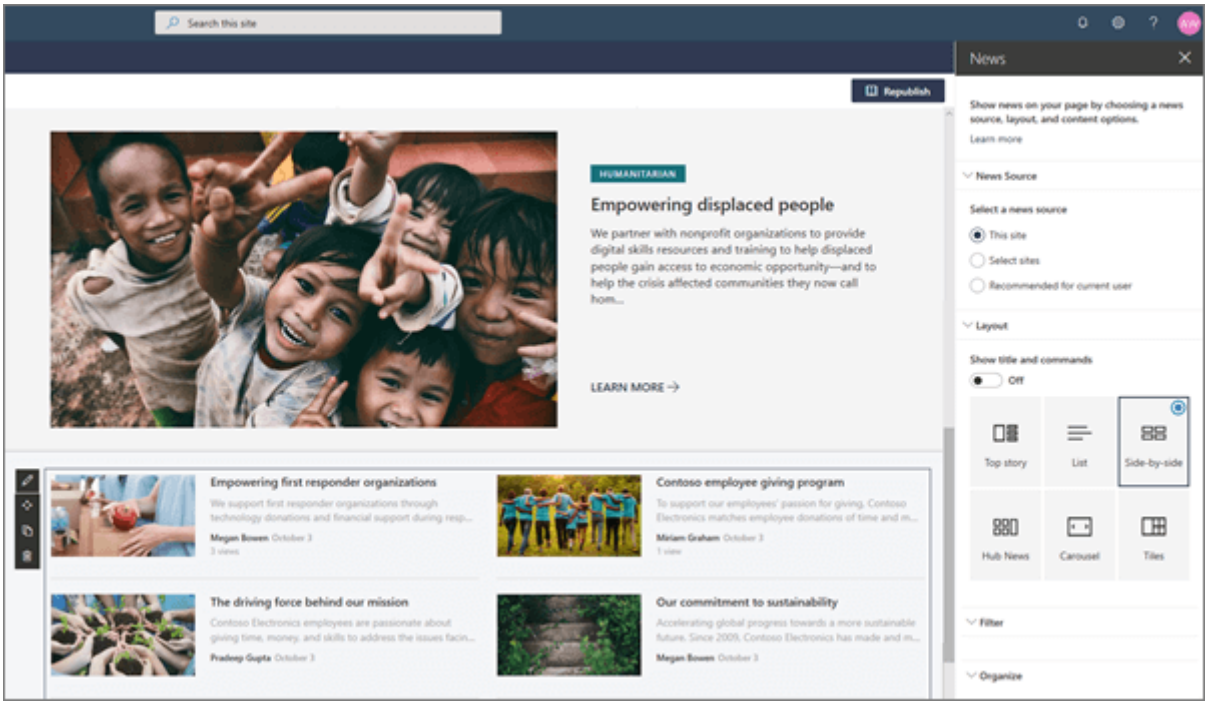
> **Tip**
>
> To manage all of your pages on the site, click **Pages** on the top menu. For more details on using pages, see Create and use modern pages on a SharePoint site.

Back to top

Spread the news with the News web part

The News web part provides controls to choose the **News Source** and **Layout**, and to **Organize** and **Filter** the content. Under **Layout**, there are five options to adjust how news items are presented. In this example, news stories are using the site as the source, and the **Top story** layout. The stories are presented side-by-side with one large image and two smaller images because only three news stories on the site are published.

In this example, the web part is in a one-column section.



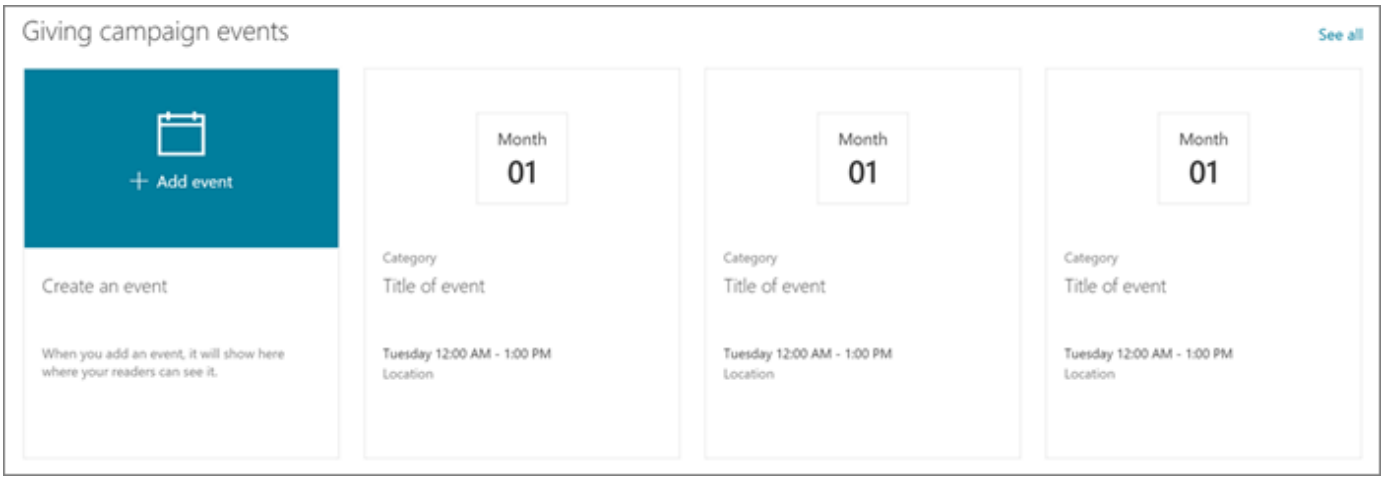
For more details on using the News web part, see Use the News web part on a SharePoint page.

Back to top

Add a calendar of events with the Events web part

The Events web part allows you to easily display upcoming events on your Giving page. You can use this web part to draw attention to Giving-related events, ranging from planning sessions to the actual events, and viewers can easily select the event to add it to their calendars.

In this Giving site example, this web part uses the Filmstrip layout.



For more details on using the Events web part, see Use the Events web part.

Back to top

Want more?

Get inspired with more examples and the ability to add an example Giving site with the SharePoint Look Book.

Last updated on 06/24/2026

Guided walkthrough: Creating a leadership site for your organization

In this article, we show you elements of an example leadership site to inspire you, and help you learn how to create similar sites for your own organization. In this example, the leadership site provides your organization insight into the goals and priorities of the leadership team. Watch this video to see how to build it, or read the following article.

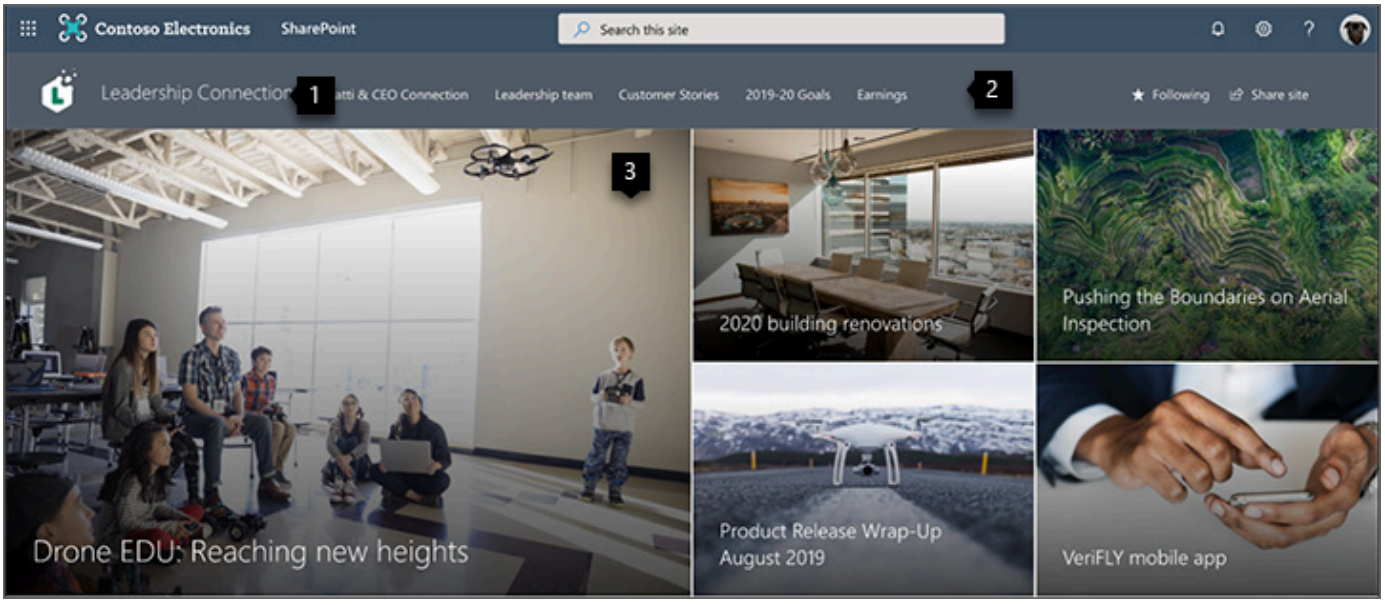
https://learn-video.azurefd.net/vod/player?id=4b95af84-58c9-47f4-ae5c-96022b364684&locale=en-us&embedUrl=%2FSharePoint%2Fguided-walkthrough-creating-leadership-site

Let's get started

First, if you haven't already created a Communication site, check out the Create your site section in this article. If you need to learn how to add sections and web parts, check out the section Add sections and web parts in this article.

Once you have your created your site and know how to edit pages, you can use the following steps to add the elements shown.

Example leadership site

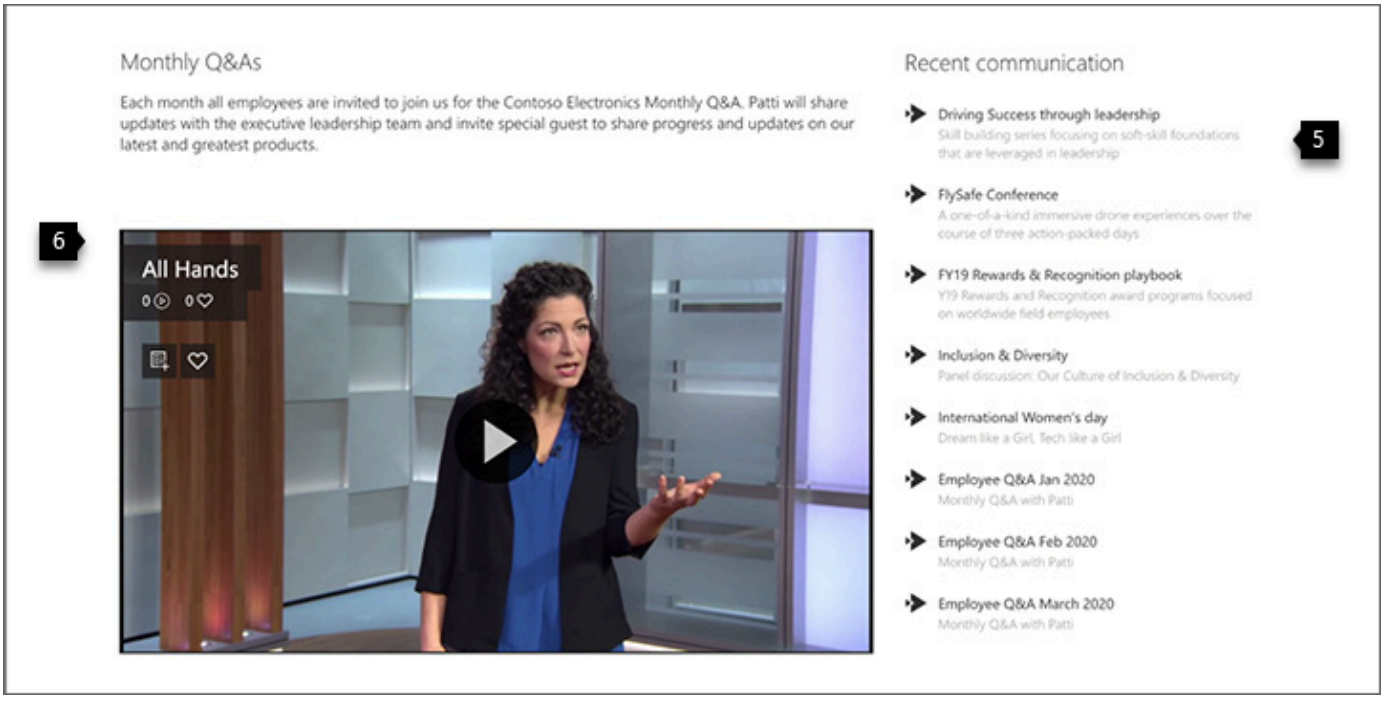


1. Showcase your company branding Make it yours with a logo and theme. Learn how

2. Make your site easy to get around Customize navigation to make it easy for people to discover important content on your site. Learn how

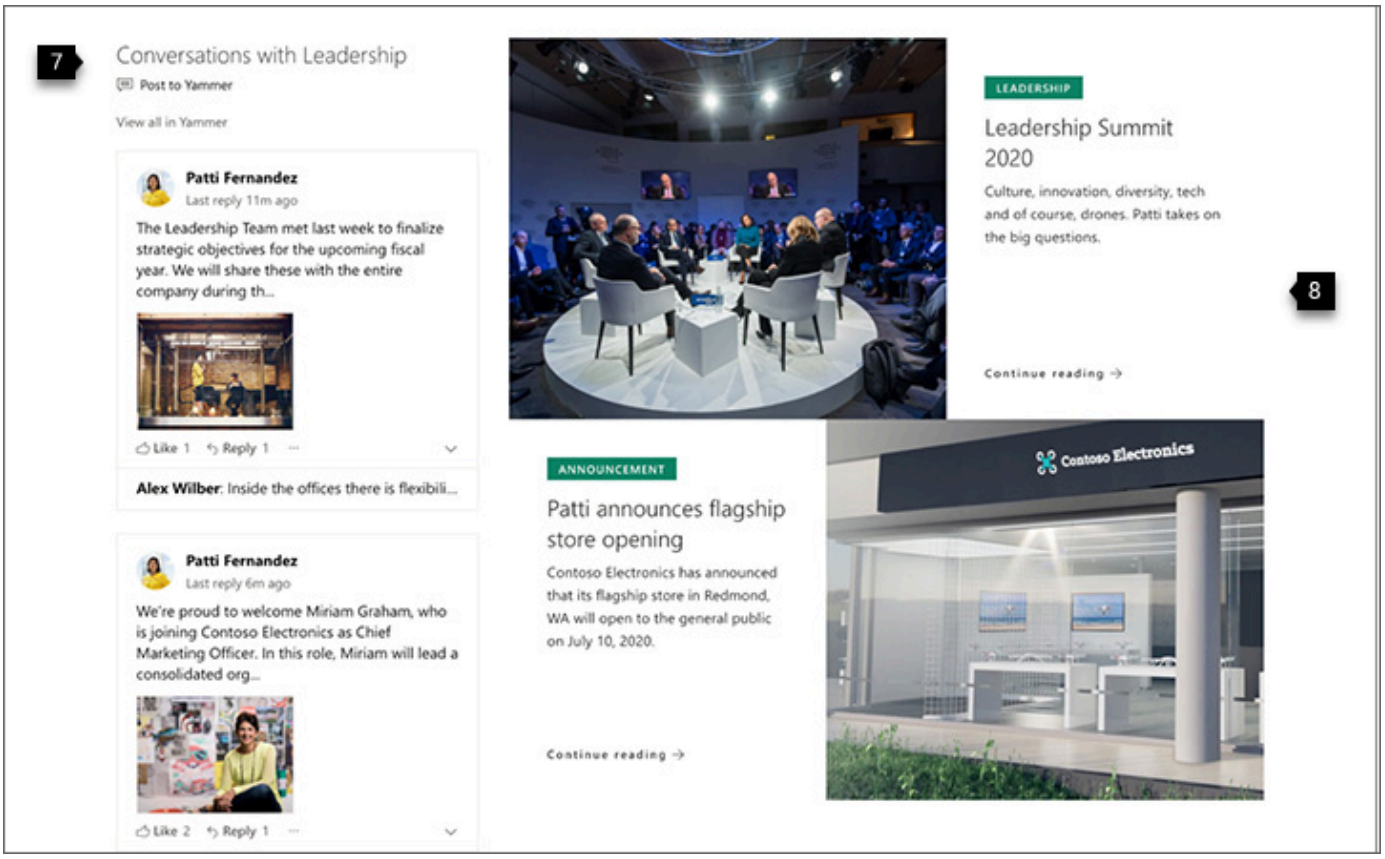
3. Focus on priorities Feature curated content that's a priority for the organization. Learn how

4. Share timely news Share the most recent news, like vision statements and blog postings. Learn how



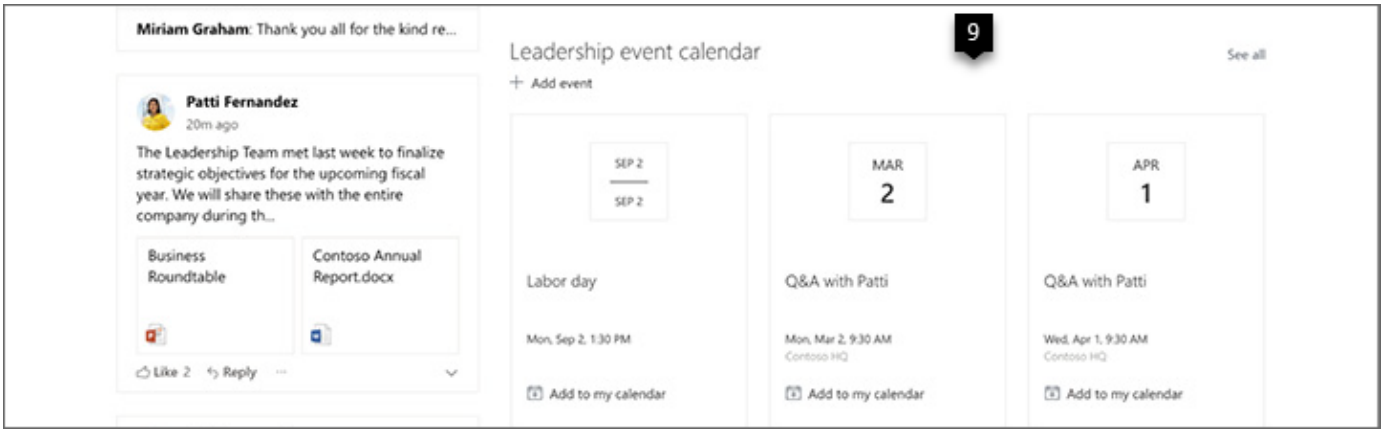
5. Connect to important resources Link to pages and sites that cover key topics. Learn how

6. Engage with video Add video to keep people updated on the latest talks, updates, and more. Learn how

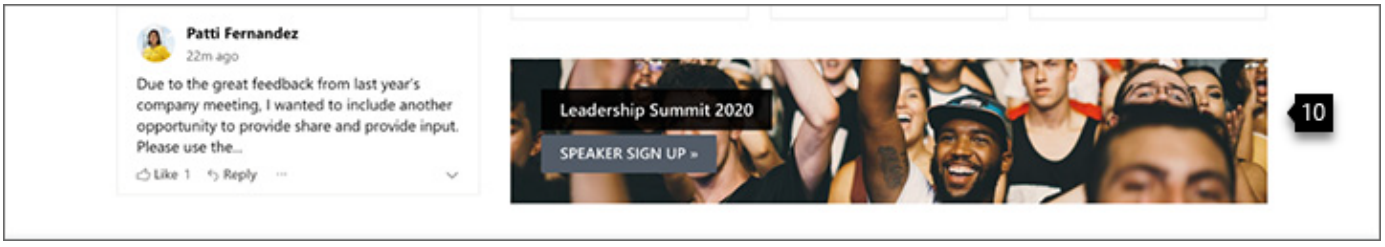


7. Keep communication fresh Share recent conversations and comments from your organization. Learn how

8. Showcase images Add more images with text and links to make your page look great and engage users. Learn how



9. Keep everyone up-to-date Show a calendar of the latest events. Learn how

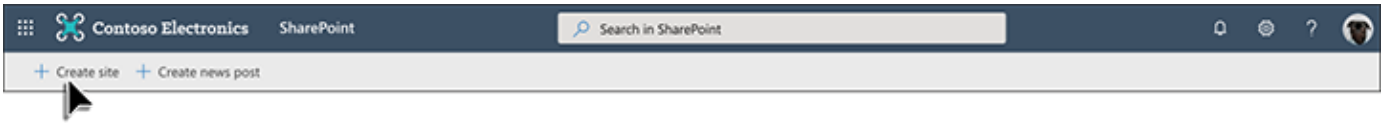


10. Create a call to action Create a call to action for sign-ups, surveys, or other important actions. Learn how

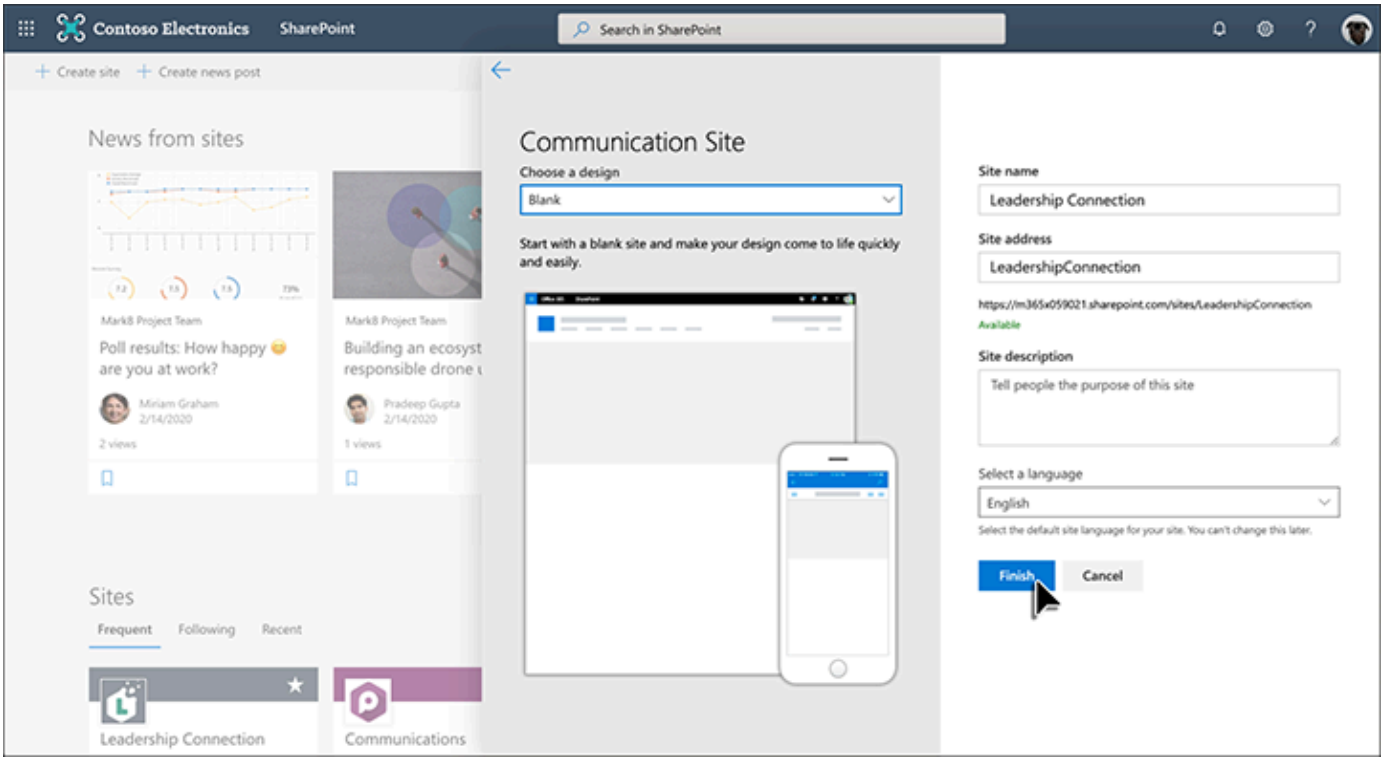
11. Use text Use the Text web part to add a quote or share a message. Learn how

Create your site

To make a site like the one shown here, you'll create a Communication site. To do this, select **Create site** from the SharePoint start page (or, if you're going to associate this site with a Hub site, navigate to the hub site and select Create site there so that the communication site is automatically associated with that hub site).



Next, choose **Communication site**, and then the **Blank** layout. Fill out your site name, description, and other information, and select **Finish**.



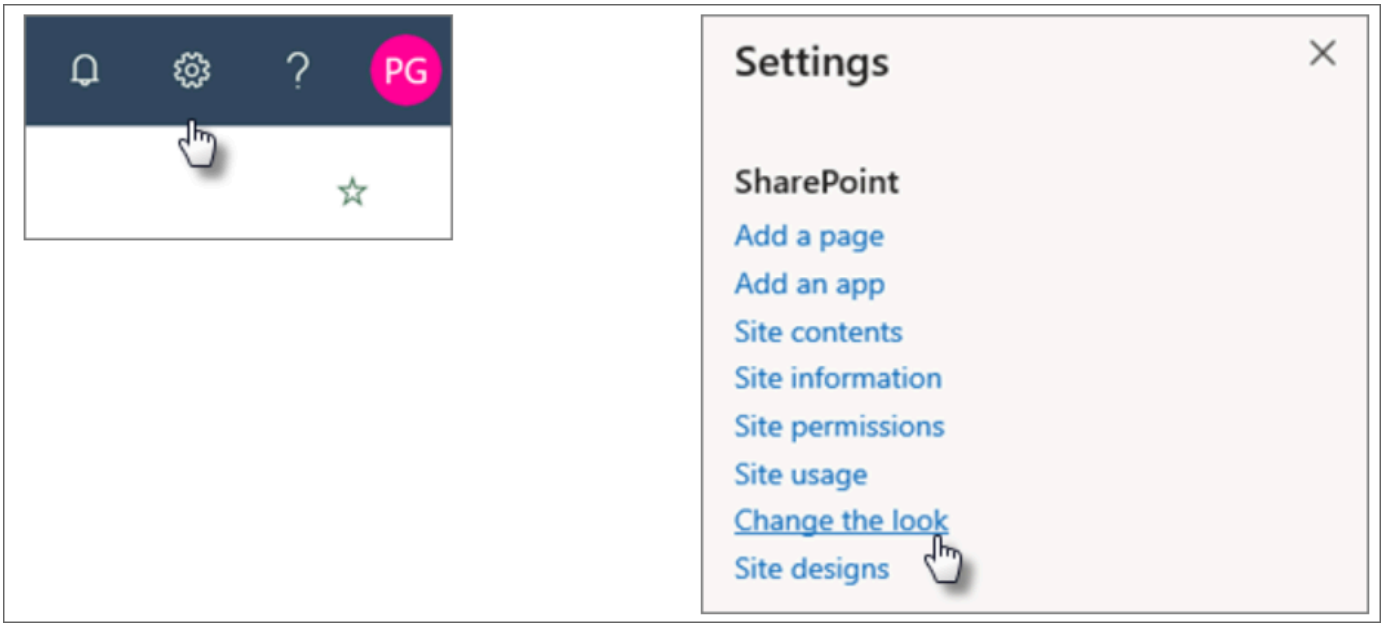
For more information, see Create a communication site in SharePoint Online.

Back to top

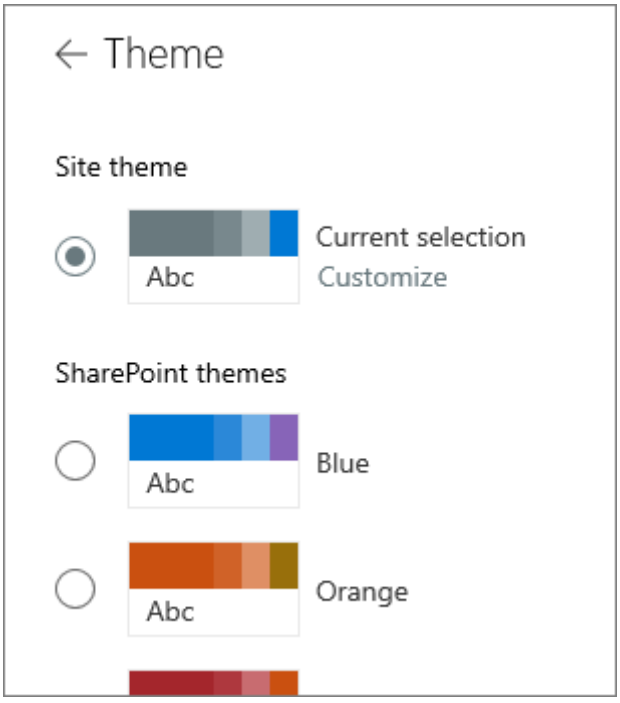
Showcase your company branding

You can quickly and easily customize the look of your SharePoint site to reflect your professional style and brand.

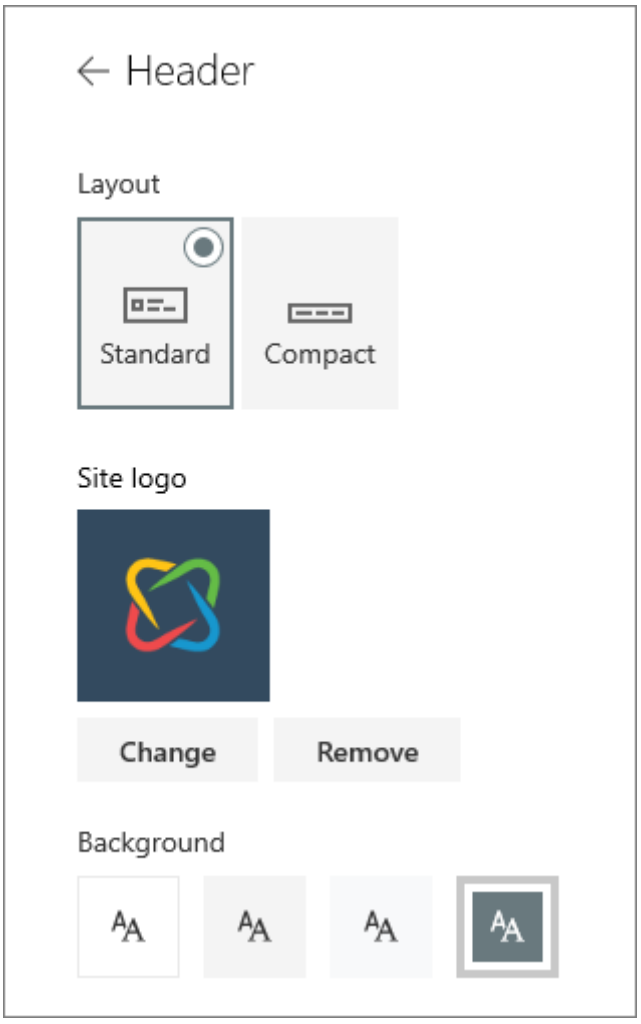
Change the look settings are located under **Settings** in the top right corner of your SharePoint site.



You can select the site theme you want, and even customize it.



You can change your header layout and logo when you select **Header** under **Change the look**.

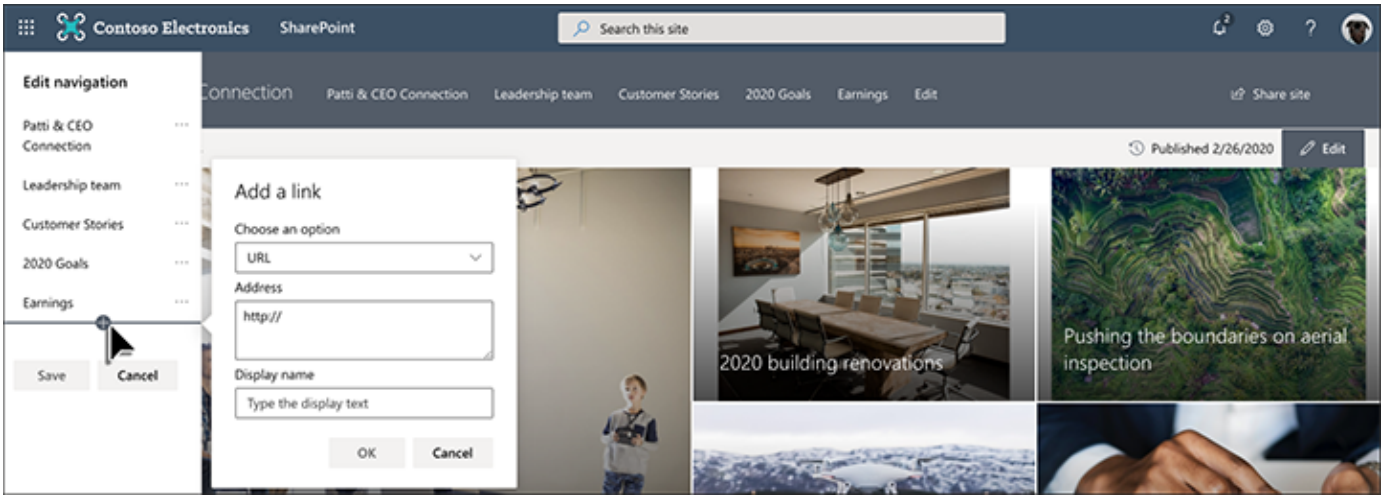


Under Change the look, you can also find options for navigation (cascade or mega menu) and footer options. For more information on changing the look of your site, see Change the look of your SharePoint site.

Back to top

Make your site easy to get around

Easily edit the left and top menus to link the page to other SharePoint pages or on the Internet.



Select **Edit** on the bottom of the left navigation to manage links there, or on the top menu to manage links there. Hover over the location in the menu where you want to add a link, and select +. Then add the type of link you want to add, your website address, and name to display in the navigation bar in the **Add a link** dialog box. Want to reorder your navigation links? Just drag them into the position you want.

For more detailed information on navigation, see Customize the navigation on your SharePoint site.

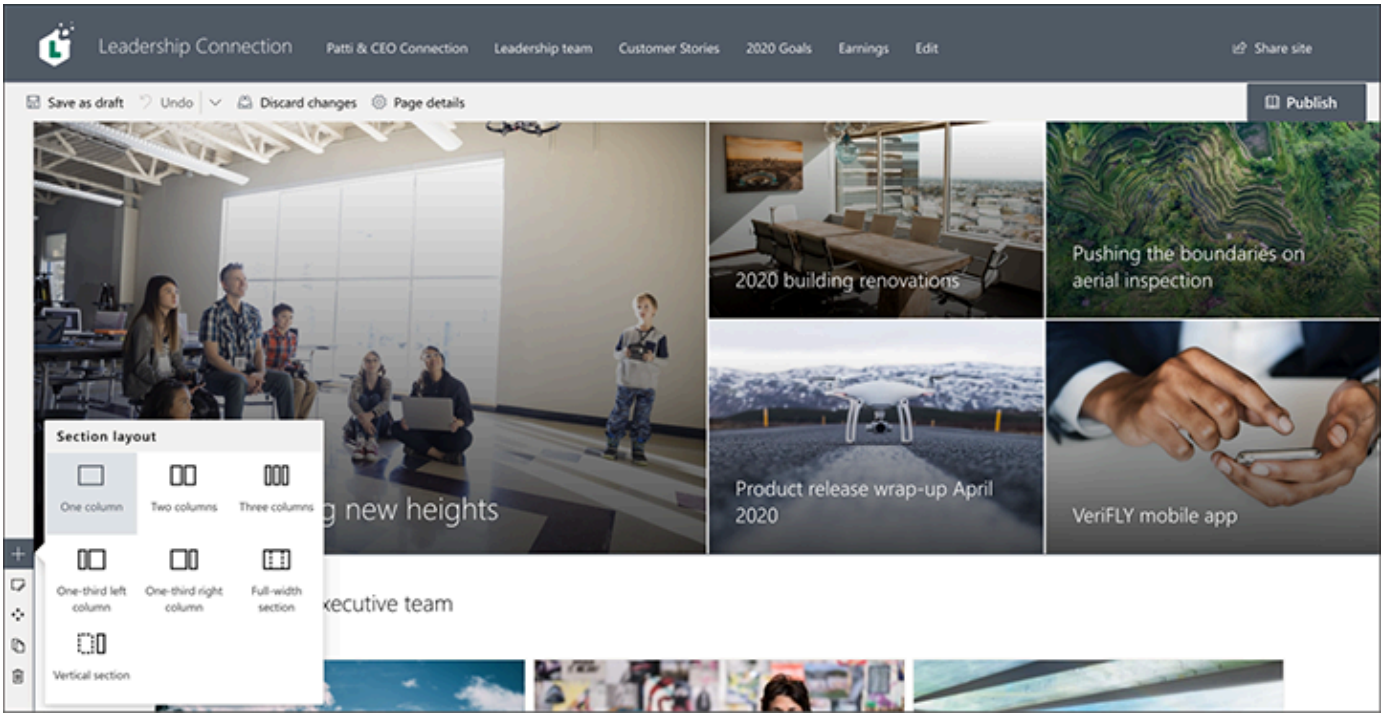
Back to top

Add sections and web parts

Sections make up your page, and are where you place one or more web parts. While editing the page, each section will show controls to edit the layout, move, or delete the sections.

Start editing by clicking **Edit** on the top right of the page.

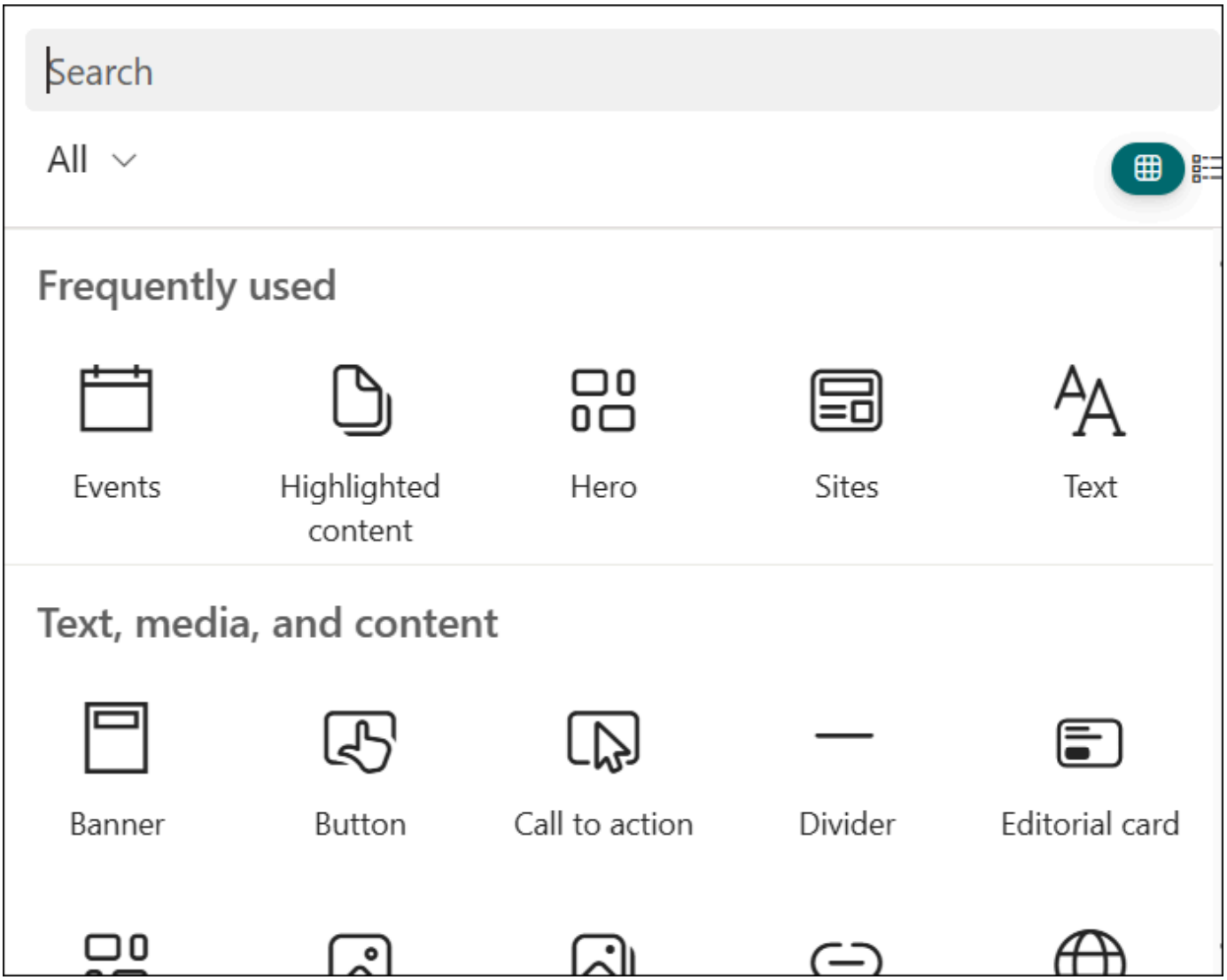
The + symbol before or after a section adds a section using one of several layouts.



For information on working with sections, see Add or remove sections and columns on a page.

To add web parts to sections, select the plus symbol in a section, which may appear before or after a web part in a section. Then select a web part to use. For more information on all web

parts, see Using web parts on SharePoint pages.



Web parts may be edited, moved, or deleted within sections. The **Edit web part** icon opens detailed controls unique to each web part type.

Back to top

Focus on priorities with the Hero web part

Let your team know what's most important with high-impact hero images, company branding, and important news. The initial impact of the Leadership site home page is created by large and eye-catching images of the Hero web part. The layout used in this example is **Three tiles**.

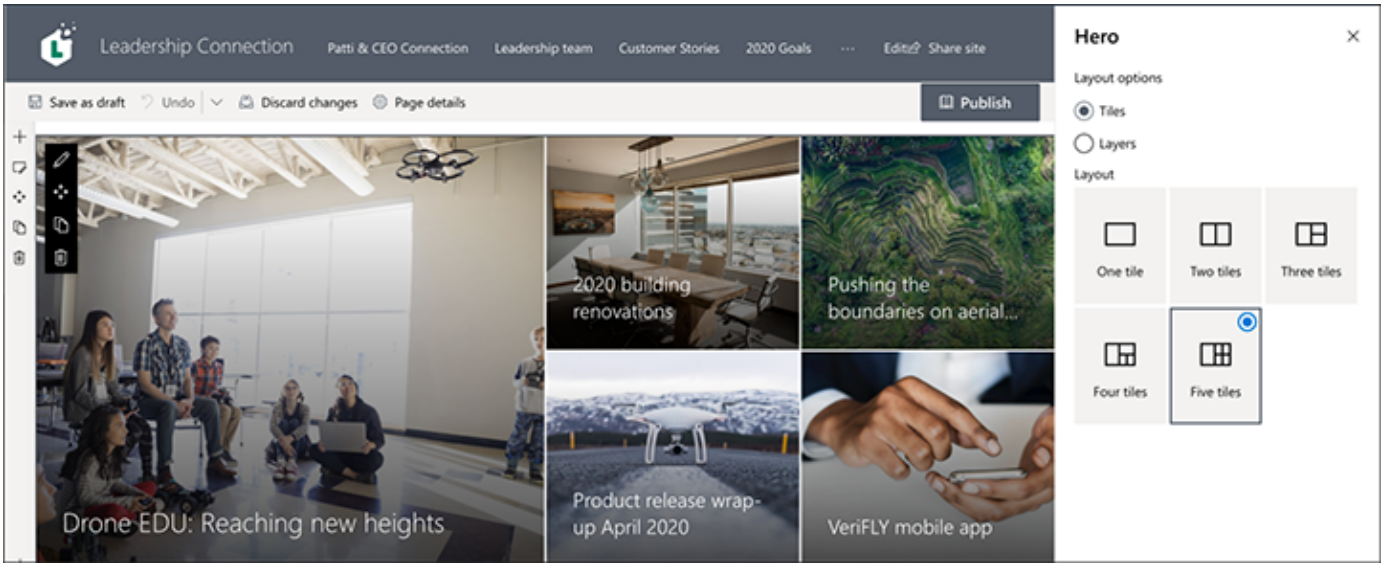
Hero layout

Editing the web part presents layout options. The **Tiles** option, such as the one shown below, presents layouts for between one and five tiles. The **Layers** option sets each image as a layer with

the image next to the title. Up to five layers are possible, so that you can use the web part to fill the entire page.

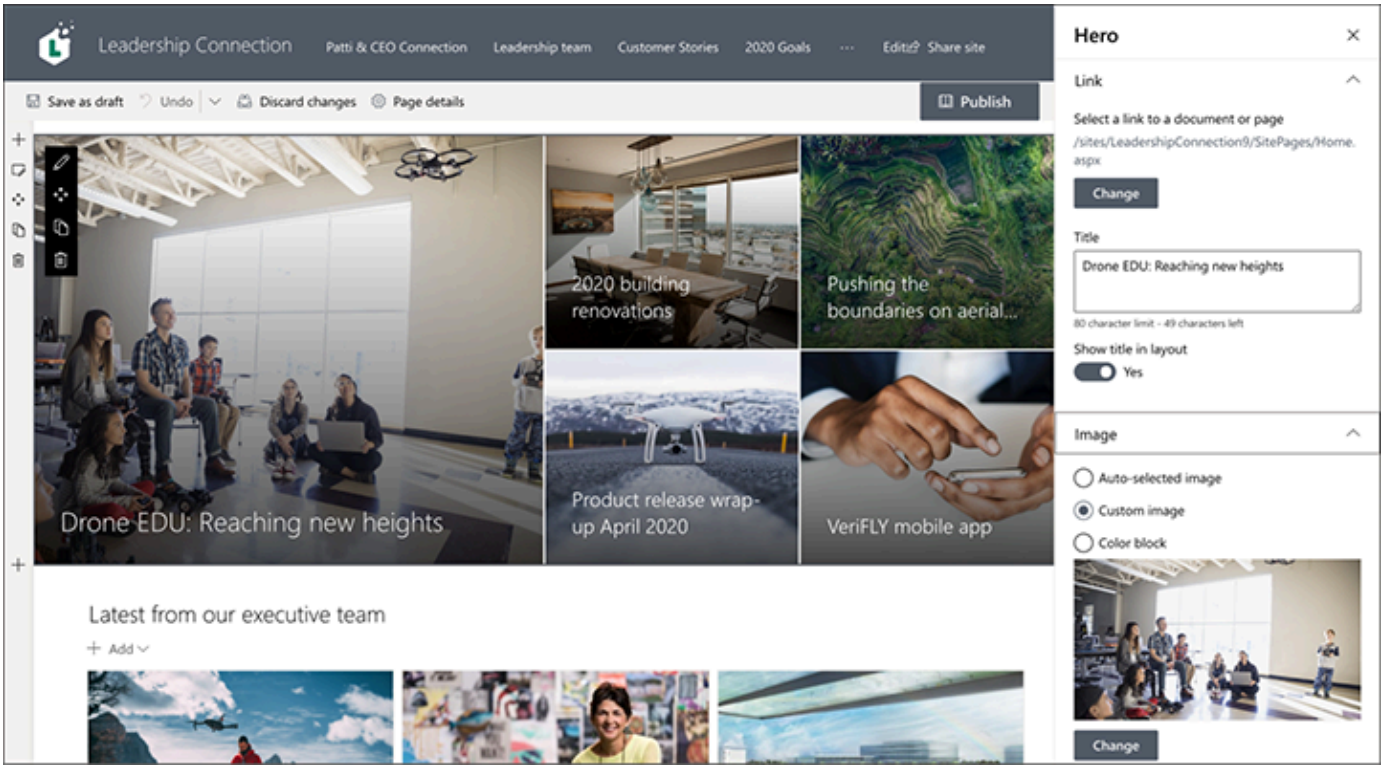
In this example, the Hero web part is in a full-width section.

Use the **Move item** button on the left to rearrange the tiles within the Hero web part.



Customize each tile

When you select a tile, you'll see a toolbar at the bottom of the tile where you can select **Edit details** where you can change the link and image used. With the larger tile, you can also set call to action text and link. On the same toolbar, you can set focal point for the hover animation, plus zoom in and zoom out of the image.



For more details on using the Hero web part, see Use the Hero web part.

Back to top

Share timely news with the News web part

The News web part provides controls to choose the **News Source** and **Layout**, and to **Organize** and **Filter** the content. Under **Layout**, there are five options to adjust now news items are presented. In this example, news stories are coming the site as the source, and the **Top story** layout. The stories are presented side by side with large images because only two news stories on the site are published.

In this example, the web part is in a one-column section.

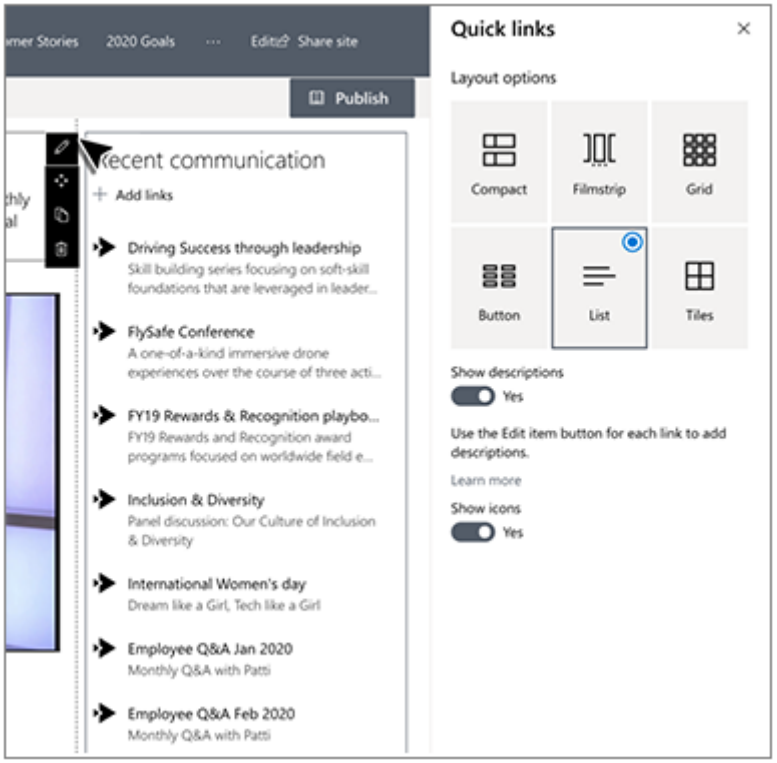
For more details on using the News web part, see Use the News web part on a SharePoint page.

Back to top

Connect to important resources with the Quick Links web part

With the Quick links web part, you have the ability to easily create professional, on-page menus for listing links to other pages or sites. In this example, the web part is using the **Compact** layout, but other layouts, like Button and Filmstrip, are available.

In this Leadership site example shown above, this web part is in the second column of a two-column section.



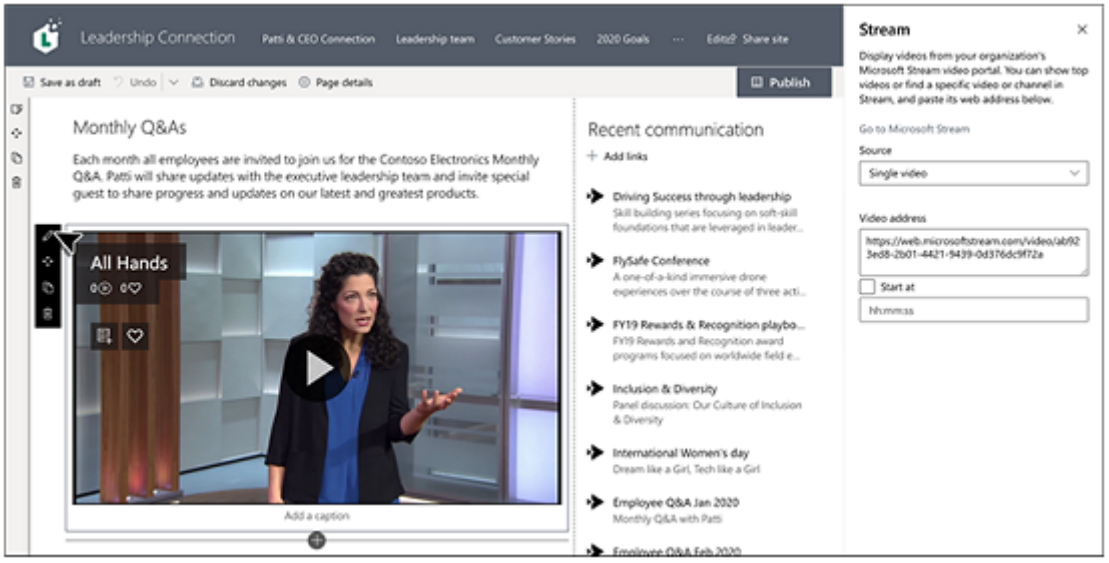
For more details on using the Quick links web part, see Use the Quick Links web part.

Back to top

Add video with the Stream web part

Using the Microsoft Stream service, you can add Stream videos to your page for enhanced visuals and higher user engagement.

In this Leadership site example shown above, this web part is in the first column of a two-column section.



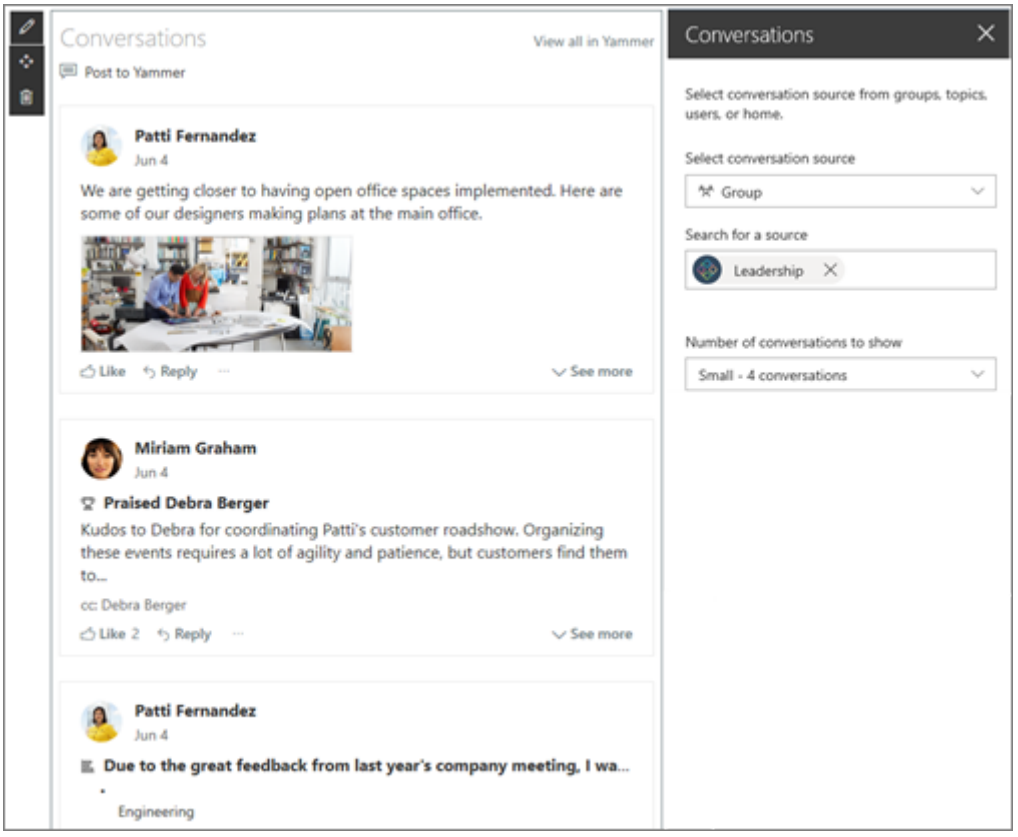
For more details on using the Stream web part, see Use the Stream web part.

Back to top

Keep communication fresh with the Viva Engage web part

With Viva Engage, you can have organization-wide conversations. Now you can have those conversations right on your page with the Viva Engage **Conversations** web part. In this example, the conversation is being pulled from a Viva Engage group called Leadership.

In this Leadership site example shown above, this web part is in the first column of a two-column section.

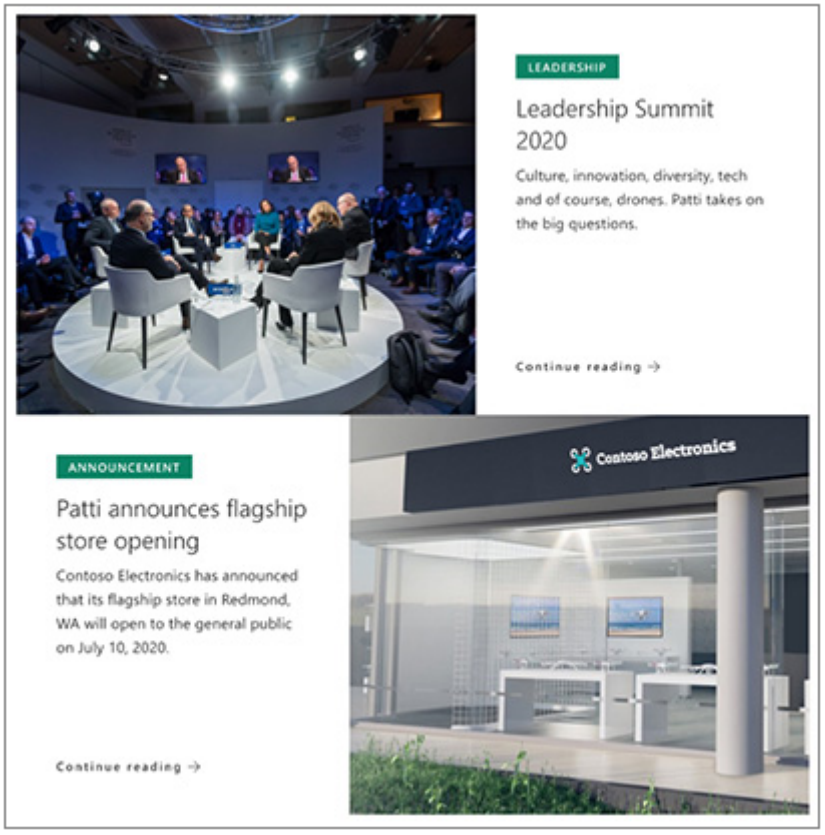


For more details on using the Viva Engage web part, see Use a Viva Engage web part in SharePoint Online.

Back to top

Engage users with a second Hero web part

The Hero web part doesn't have to be for the top of the page only. In this example, a second hero web part further down the page uses the **Layers** layout with two rows to display larger images.



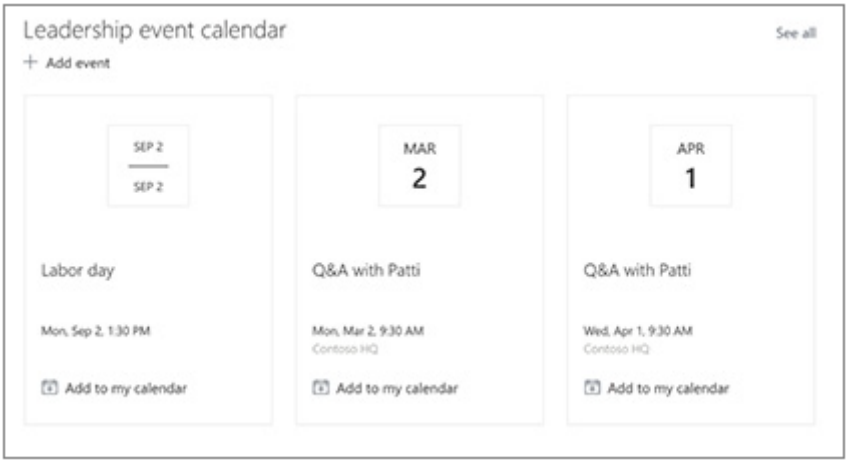
Learn more about the Hero web part.

Back to top

Keep everyone up to date with the Events web part

The Events web part allows you to easily display upcoming events on your page. In this example, leadership events are highlighted.

In this Leadership site example, the web part is in the second column of a two-column section.



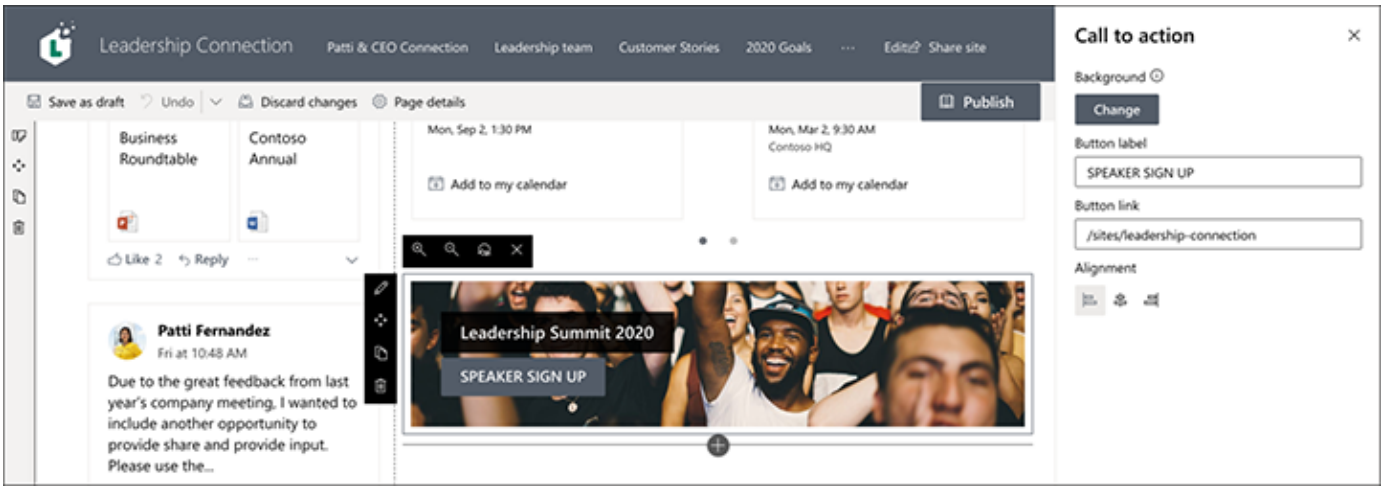
Learn more about the Events web part in Use the Events web part.

Back to top

Add a Call to action web part

The Call to action web part allows you to create a button with a call to action for users. In this example, it's used to encourage and direct employees to sign up for a speaker session.

In this Leadership site example, the web part is in the second column of a two-column section.



For more details on how to use this web part, see Use the Call to action web part.

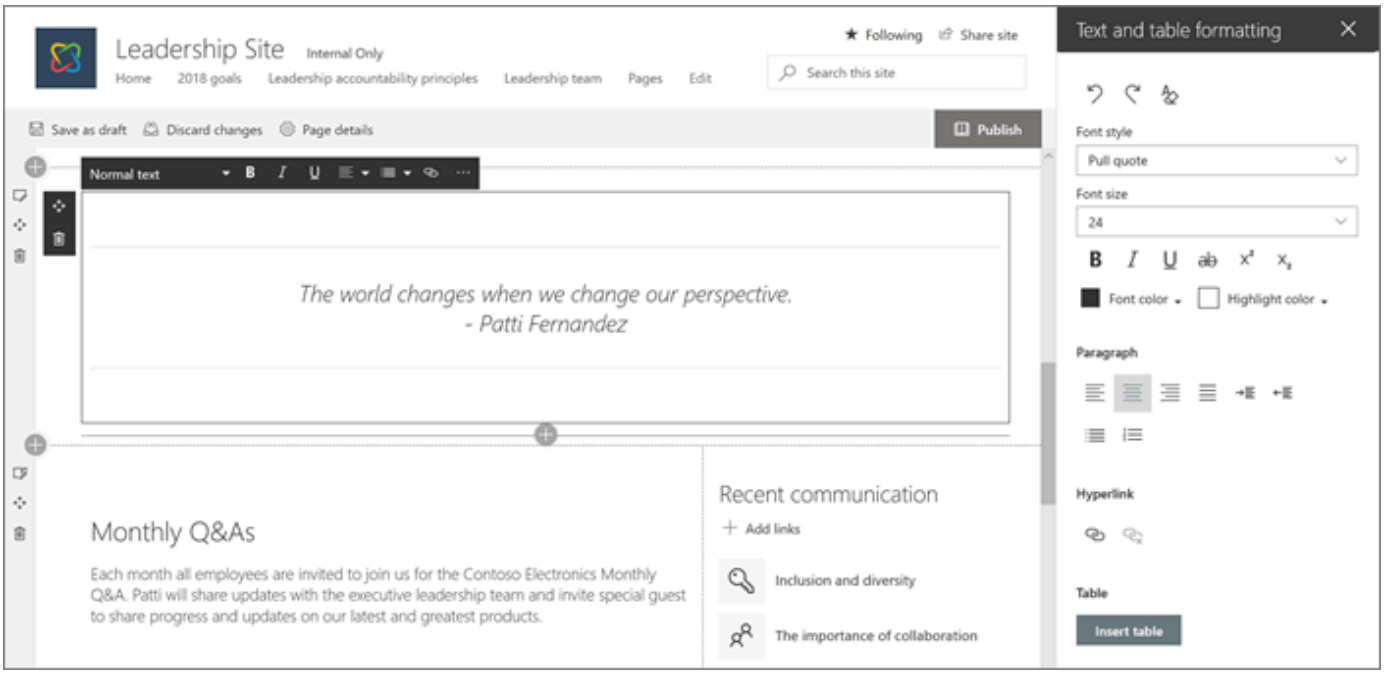
Back to top

Make words matter using the Text web part

Enhance the message

The leadership quote uses the Text web part. This web part allows basic text formatting, including styles and tables, for creating fixed sections of formatted text. In this example, the Text web part is using the **Pull quote** style. Clicking the **...** control at the right end of the formatting toolbar offers more options to the right of the web part.

In this Leadership site example shown above, the web part is in a one-column section.



For more details on using the Text web part, see Add text and tables to your page with the Text web part.

Back to top

Want more?

Get inspired with more examples in the SharePoint look book.

See other guided walkthroughs for creating sties for your organization.

Last updated on 06/24/2026

Guided walkthrough: Creating a Training site for your organization

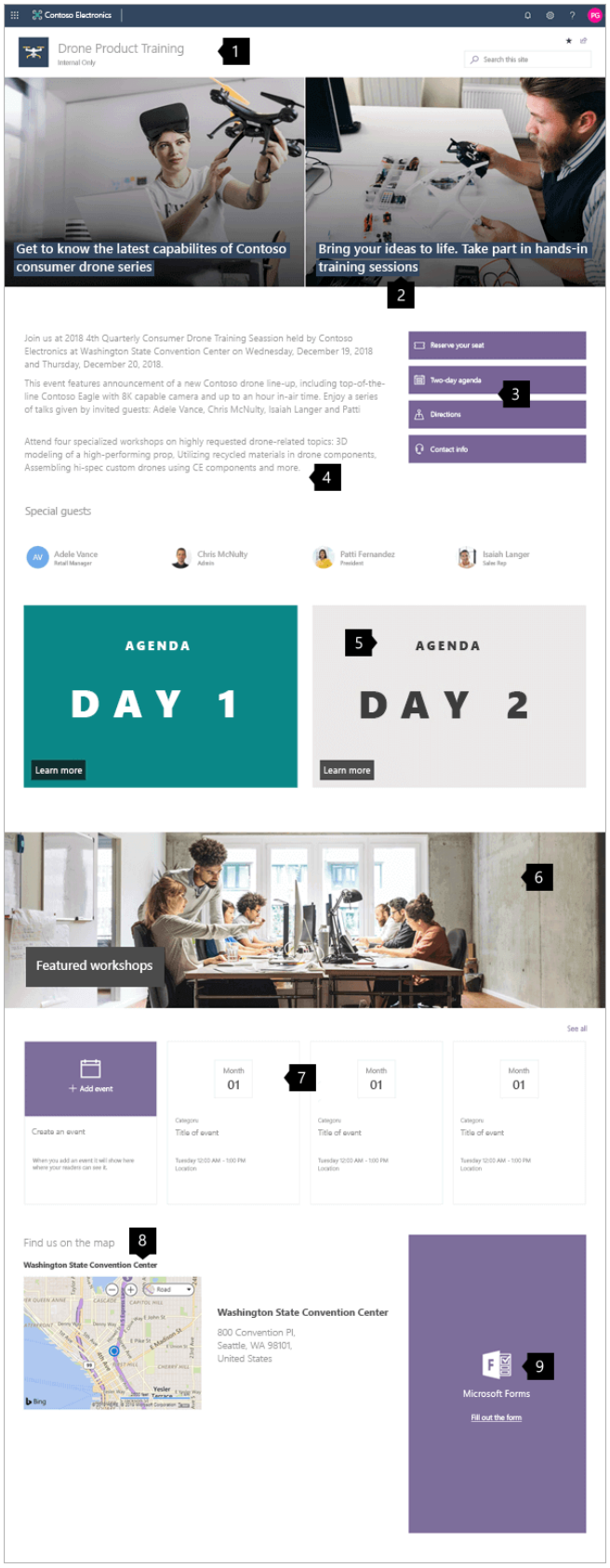
In this article, we show you elements of an example Training site to inspire you, and help you learn how to create similar sites for your own organization. This example site provides info about a specific event and guides the user toward learning and registration. It relies on visuals to engage and motivate the visitor.

First, if you haven't already created a Communication site, check out the Create your site section in this article. If you need to learn how to edit and publish the page on your site, check out the section Edit, work with sections and web parts, and publish in this article.

Once you have your created your site and know how to edit pages, you can use the following guidance to add the elements shown.

Example Training site

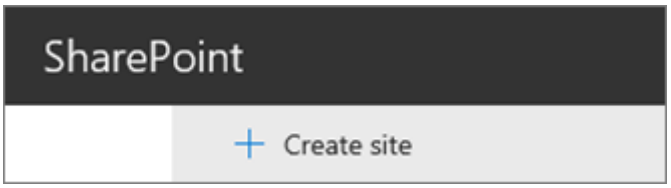
Expand table

Image of the homepage	Customization instructions
	**1. Logo and site classification** Customize your logo and classify your site. *Learn how* **2. Create impact** Use the hero web part to visually communicate your value. *Learn how* **3. Guide users to key action** Lead visitors to register or discover more. *Learn how* **4. Describe the event** Use text to describe the "what" and "why" of the event. *Learn how* **5. Use images with links** Increase visibility and link to detailed agenda pages. *Learn how* **6. Highlight detailed information** Images can define areas of important information. *Learn how* **7. Show event dates** Provide an event calendar so users can plan their schedules. *Learn how* **8. Add a map** Use a map to help users get to where they need to be. *Learn how* **9. Provide on-page registration** Add a form for easy registration. *Learn how*

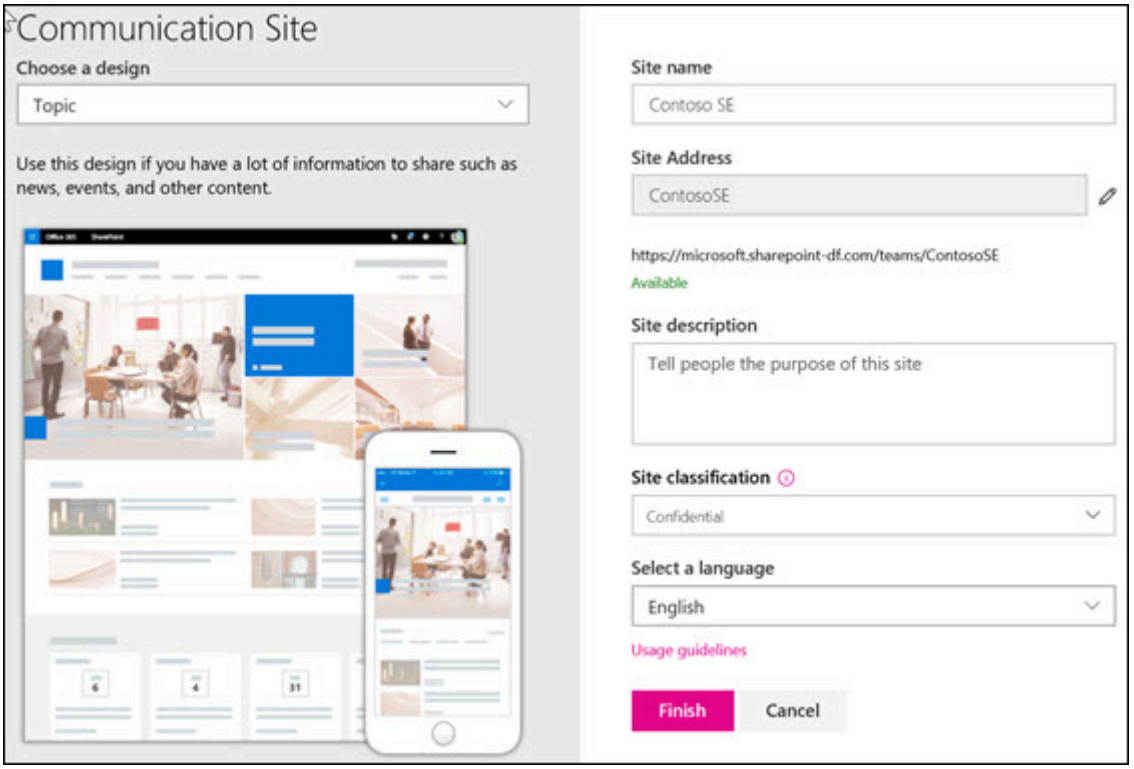
Create your site

To make a site like the one shown here, you create a Communication site. To do this, select **Create site** from the SharePoint start page (or, if you're going to associate this site with a Hub

site, navigate to the hub site and select **Create site** there so that the communication site is automatically associated with that hub site).



Next, choose **Communication site**, and then the **Topic** layout. Fill out your site name, description, and other information, and select **Finish**. Then you get a template with the same type of layout as the example in this article.

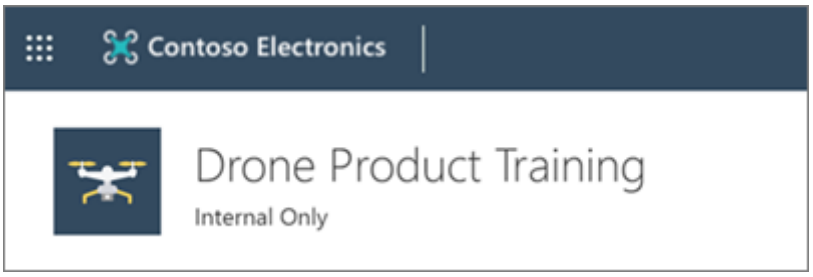


For more information, see Create a communication site in SharePoint Online.

Back to top

Logo and site classification

In this example, the header area doesn't contain any navigation because it's a "stand-alone" page. However, the header area does contain a custom logo, and shows a label indicating that the site is classified as "Internal Only." Site classification uses values such as internal, confidential, high business impact, low business impact, and so on. These values can pertain to sensitivity of information or to the life cycle of information.



To learn how to change the logo and classify your site, see Manage your SharePoint site settings.

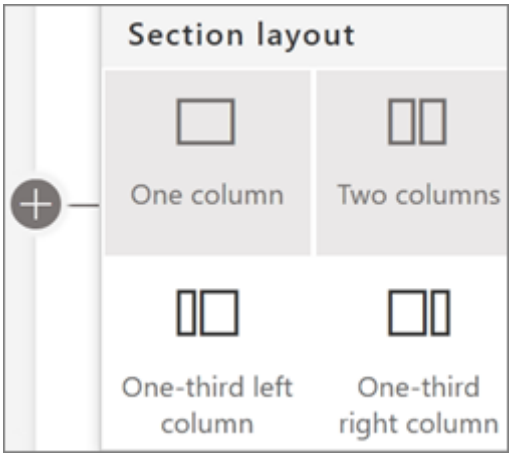
Back to top

Manage sections and web parts

Start editing by clicking **Edit** on the top right of the page.

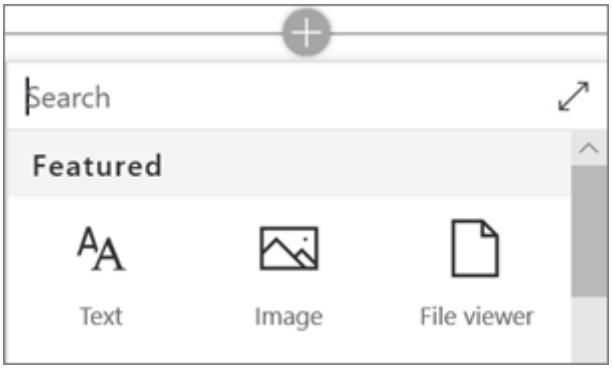
While editing, on the left, below the header your drafts can be saved for later or discarded.

The + symbol before or after a section will add a section using one of several layouts.



Sections make up your page, and are you place one or more web parts. When you edit the page, each section shows controls to edit the layout, move, or delete the sections. For information on working with sections, see Add or remove sections and columns on a page.

Select the plus symbol in a section, which may appear before or after a web part in a section, to see the many types of web parts available. For more information on all web parts, see Using web parts on SharePoint pages.



Web parts may be edited, moved, or deleted within sections. The **Edit web part** icon opens detailed controls unique to each web part type.

When your page updates are ready, select **Publish** to make them visible to your entire organization.

> **Tip**
>
> To manage all of your pages on the site, select **Pages** on the top menu.

For more information on using pages, see Create and use modern pages on a SharePoint site.

Back to top

Create impact with the Hero web part

Let your visitors know the focus of your Workshop with the Hero web part. The layout used in this example is **Two tiles**.

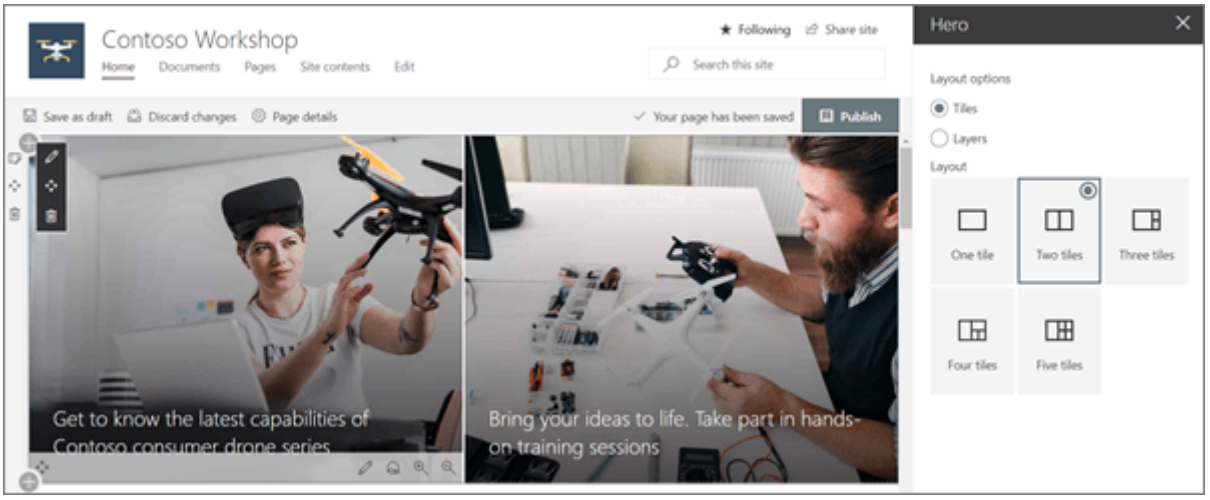
Hero layout: Tiles or Layers:

Editing the web part presents layout options. The **Tiles** option presents layouts for between one and five tiles. The **Layers** option sets each image as a layer with the image next to the title. Up to five layers are possible allowing one web part to create an entire page.

Each tile can be edited:

Use the **Move item** control on the left to rearrange the tiles within the Hero web part. Controls on the right allow you to **Edit details** adjusting the text and image used, **Set focal point** for the hover animation, plus **Zoom in** and **Zoom out** of the image.

In this example, the Hero web part is in a full-width section.



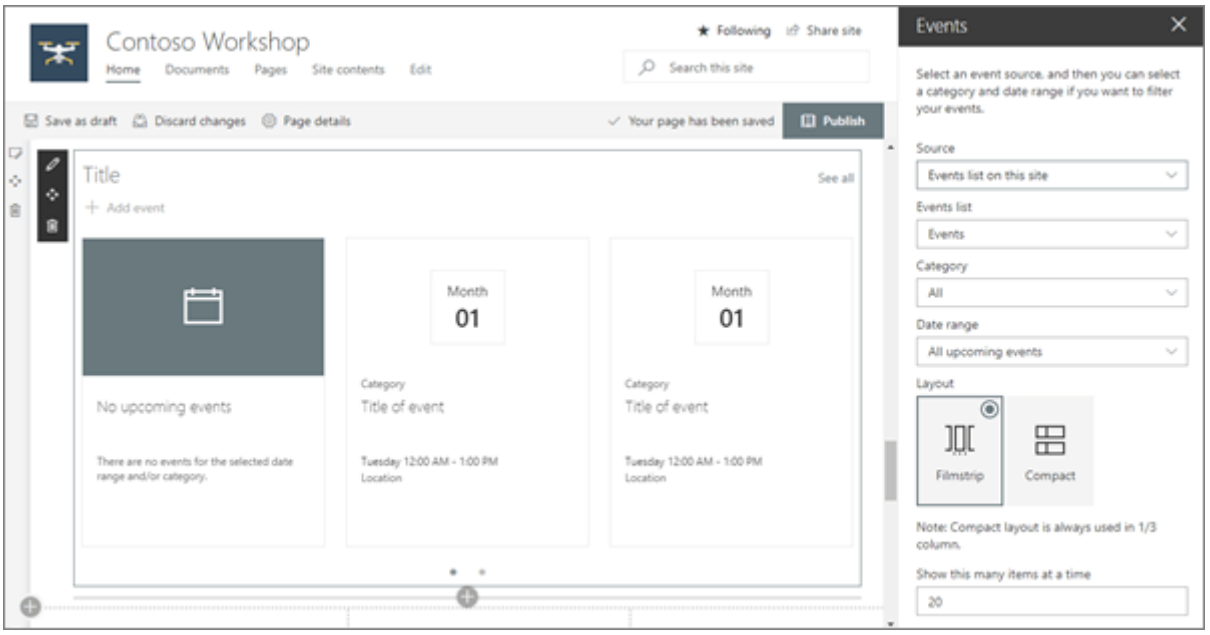
For more information on using the Hero web part, see Use the Hero web part.

Back to top

Show event dates

The Events web part automatically displays event information. The events shown are controlled by filters for **Source**, **Event list**, **Category**, and **Date range**. Events can be shown with detailed summaries in **Filmstrip** view or in a **Compact** view.

In this Workshop site example, this web part uses the **Filmstrip** layout.



For more information on using the Events web part, see Use the Events web part.

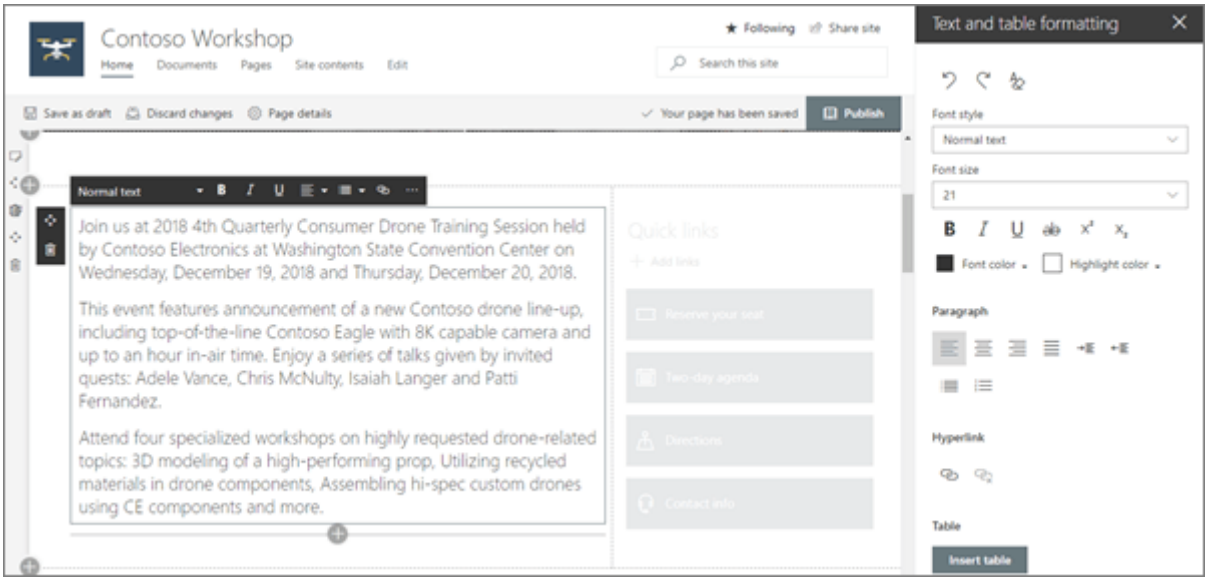
Back to top

Describe the event with the Text web part

The leadership drop quote and the Monthly Q&A descriptions use the Text web part. This web part allows basic text formatting for creating fixed sections of formatted text.

When editing text, this web part offers basic formatting tools to set styles and add enhancements like **bold** and *italics*. Selecting the ... control at the right end of the formatting toolbar offers more options to the right of the web part.

In this Workshop site example shown before, the web part is in a one-column section.



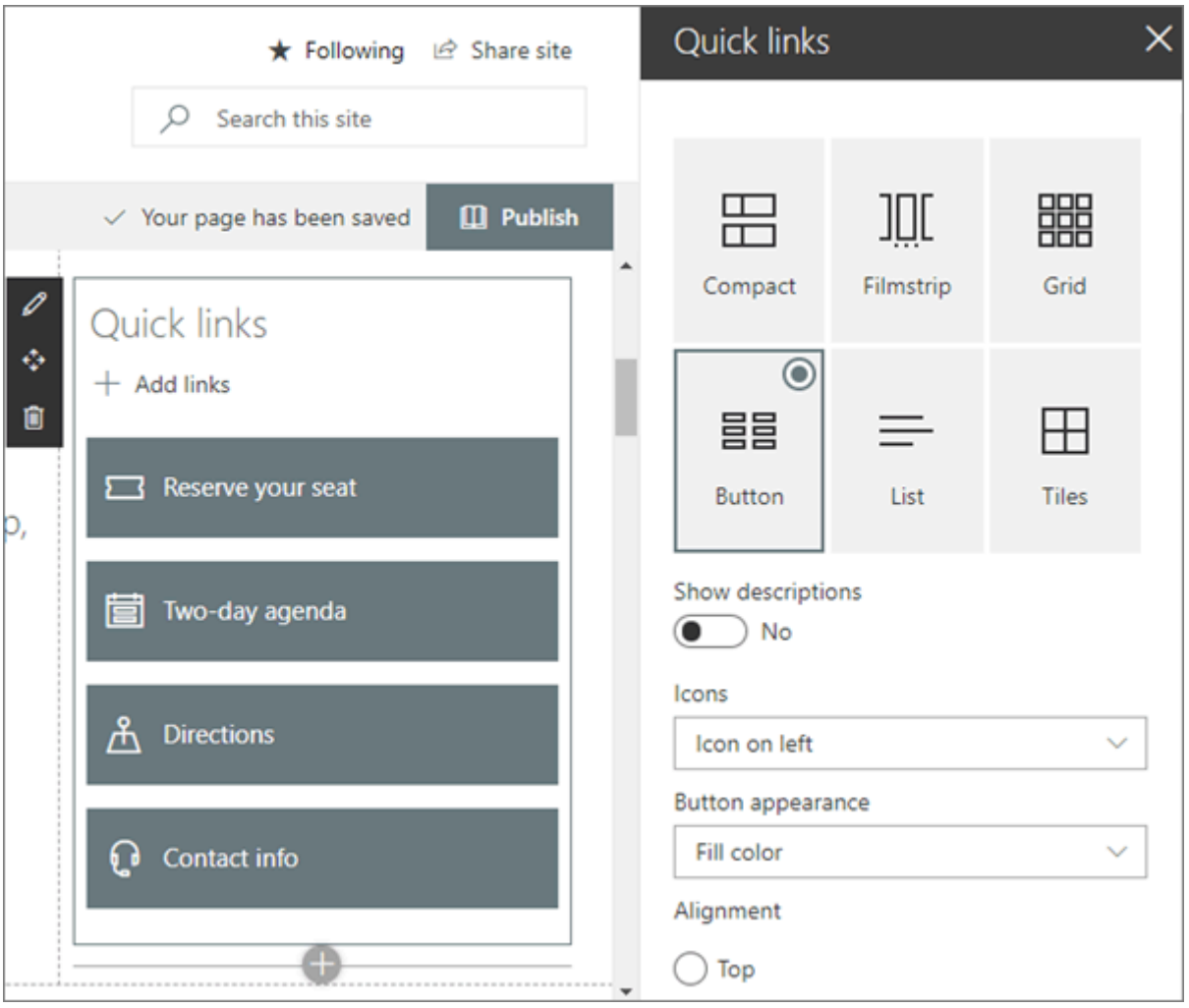
For more information on using the Text web part, see Add text and tables to your page with the Text web part.

Back to top

Guide users to key actions with Quick links

The Quick links web part offers several easy to use menu formats for listing links to other pages or sites.

In this site example, the web part uses the **Button** layout for quick and easy reference.

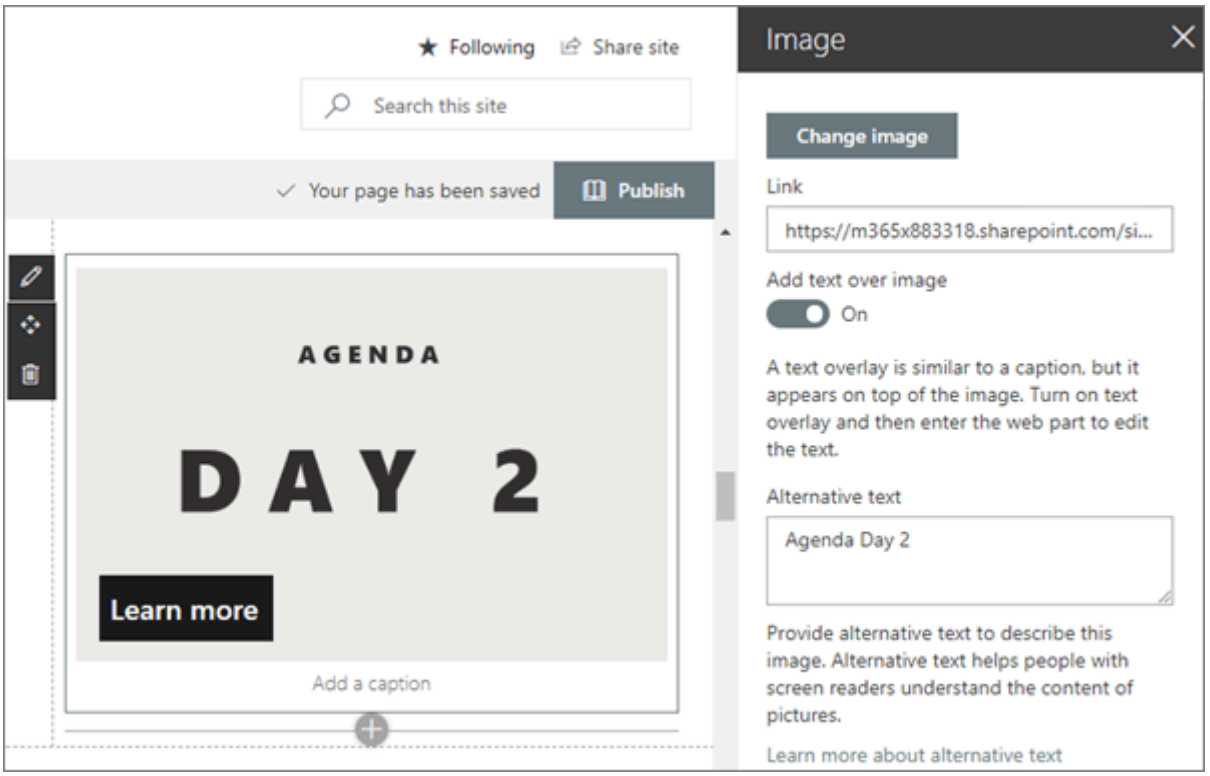


For more information on using the Quick Links web part, see Use the Quick Links web part.

Back to top

Use images with links

The Image web part places a fixed image on the page. Images can be photographs, diagrams, or even used to bring emphasis to text. Captions and alt-text keep images accessible.

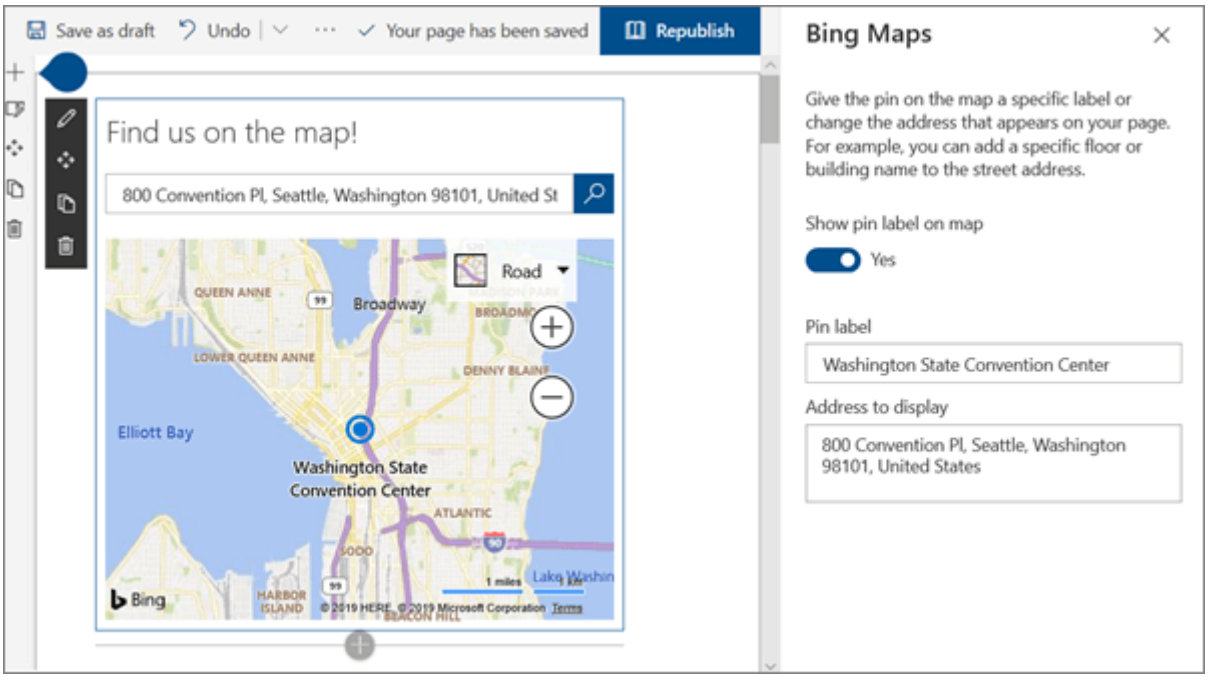


For more information on using the Image web part, see Use the Image web part.

Back to top

Add maps with the Bing Maps web part

The Bing Maps web part offers an easy visual map reference and quick link to allow visitors to plan their route to your workshop.

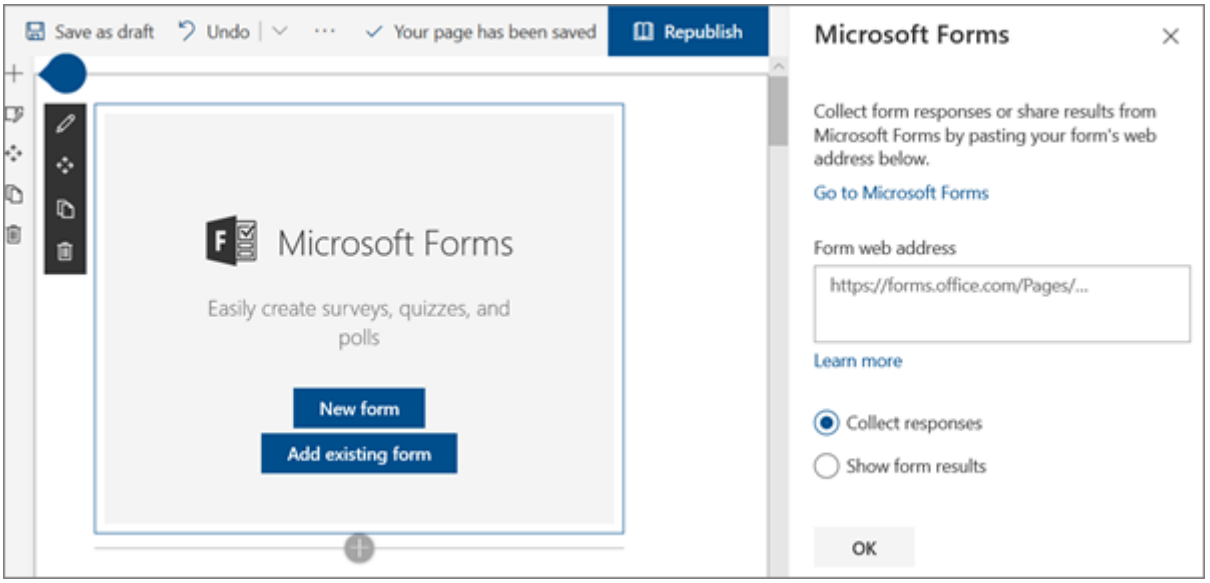


For more information on using the Bing Maps web part, see Use the Bing Maps web part.

Back to top

Add forms for registration

If you created a form for registration using Microsoft Forms, you can place that form directly on the page with the Microsoft Forms web part. It's an easy way for attendees to fill out their information, and an easy way for you to collect it.



For more information on using the Microsoft Forms web part, see Use the Microsoft Forms web part.

Back to top

Want more?

Get inspired with more examples in the SharePoint Look Book.

Last updated on 06/24/2026

Guided walkthrough: Creating an organization site

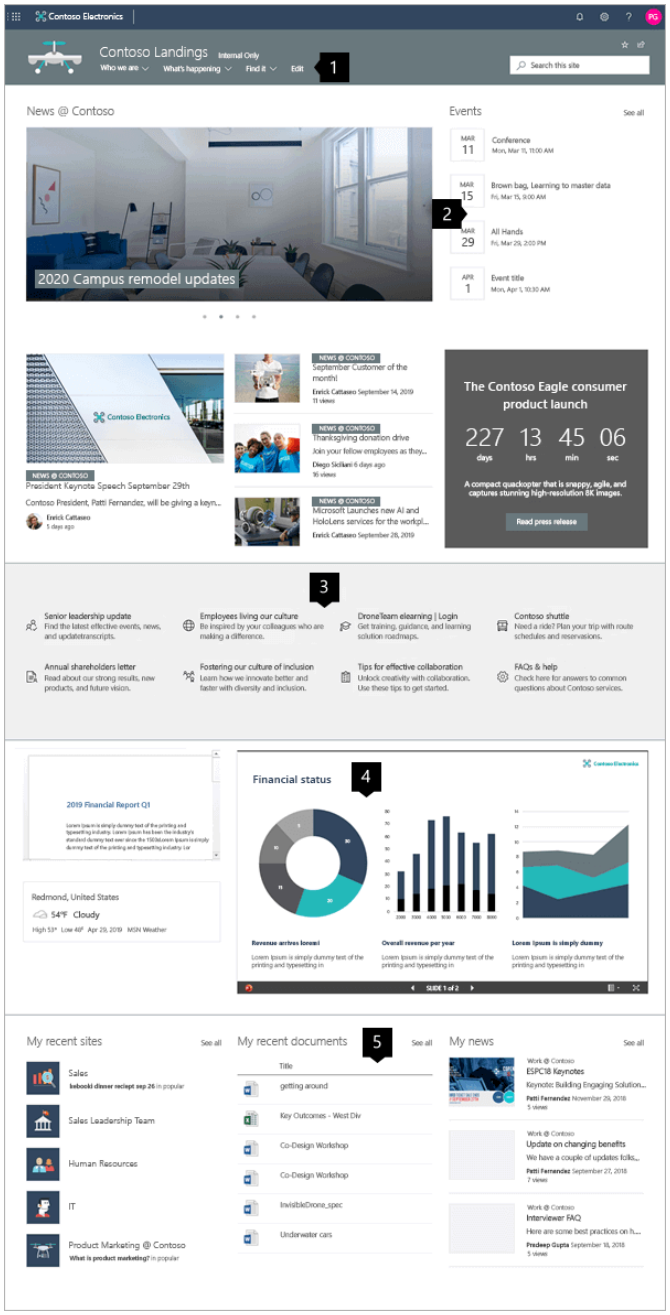
In this article, we show you elements of an example SharePoint enterprise landing site to inspire you and help you learn how to create similar sites for your own organization. In this example, the site emphasizes news, resources, and personalized content. You'll see which web parts on used in different sections, along with links for more information on each web part.

First, if you haven't already created a Communication site, check out the Create your site section in this article.

Once you have your created your site and know how to edit pages, you can use the steps below to add the elements shown.

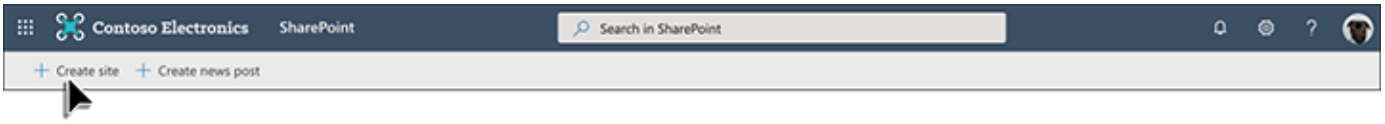
Example SharePoint enterprise landing site

Expand table

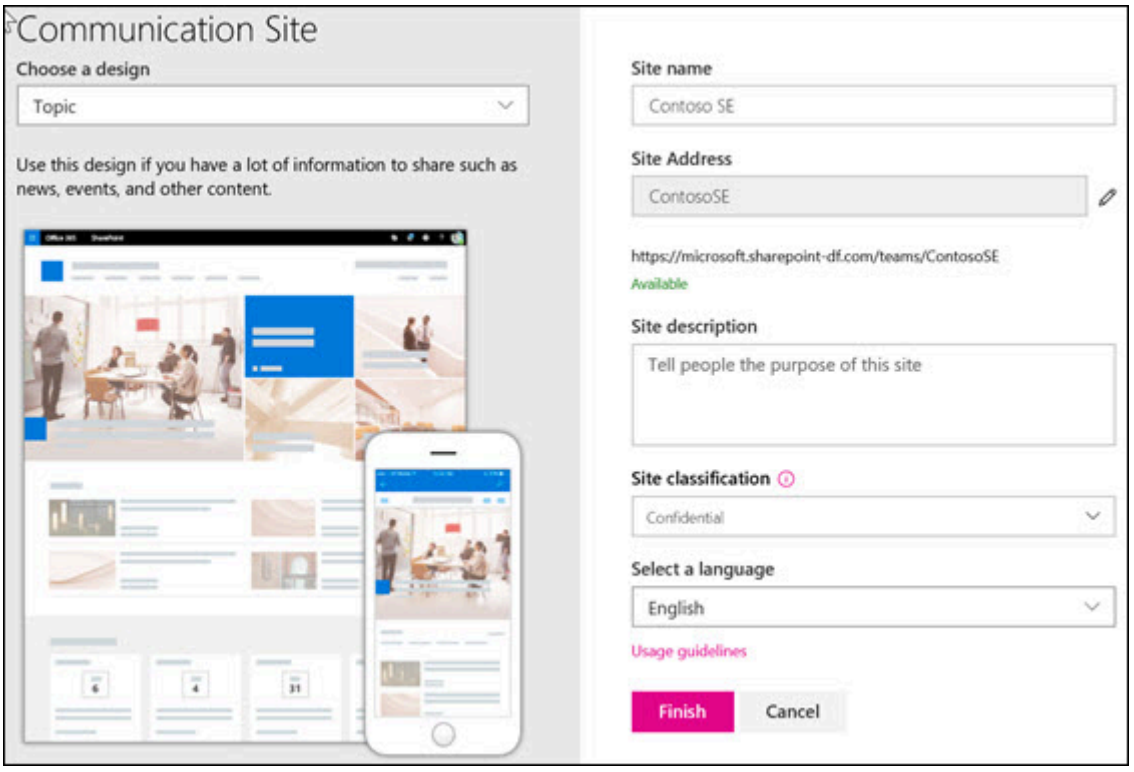
Web part	Description
	**1 Navigation** Quickly guide visitors to the information they're looking for with site navigation. Learn how **2 News and events** Keep everyone up to date on the latest happenings. Learn how **3 Quick links** Format the Quick links web part with icons, images, and descriptions. Learn how **4 Important information** Display important documents and files. Learn how **5 Personalization** Use web parts designed to dynamically provide personalized information for the user. Learn how

Create your site

To make a site like the one shown here, you need to create a Communication site. To do this, select **Create site** from the SharePoint start page (or, if you're going to associate this site with a Hub site, navigate to the hub site and select **Create site** there so that the communication site is automatically associated with that hub site).



Next, choose **Communication site**, and then the **Topic** layout. Fill out your site name, description, and other information, and select **Finish**. Then you get a template with the same type of layout as the example in this article.



For more information, see Create a communication site in SharePoint online.

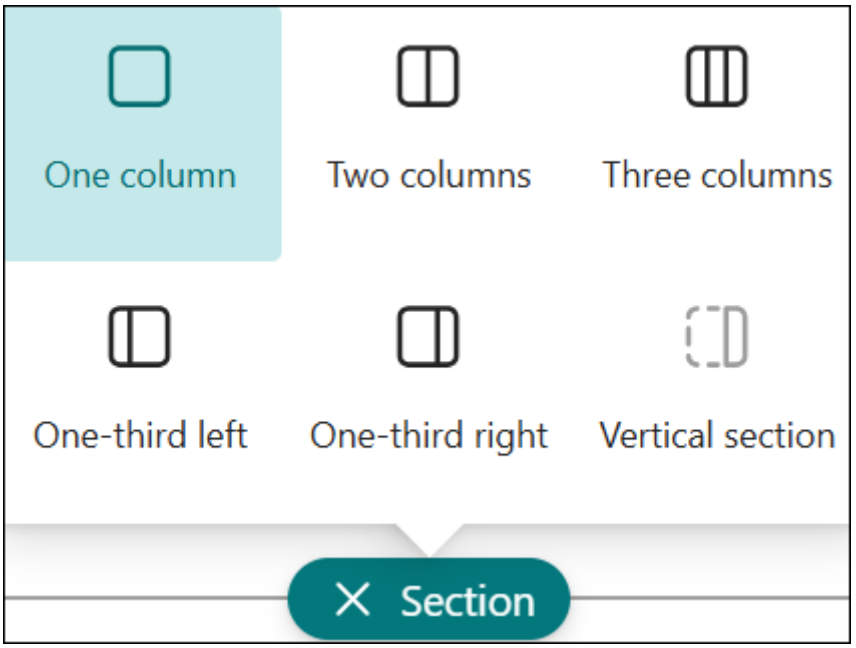
Back to top

Manage sections and web parts

Sections make up your page, and are where you place one or more web parts. While editing the page, each section shows controls to edit the layout, move, or delete the sections.

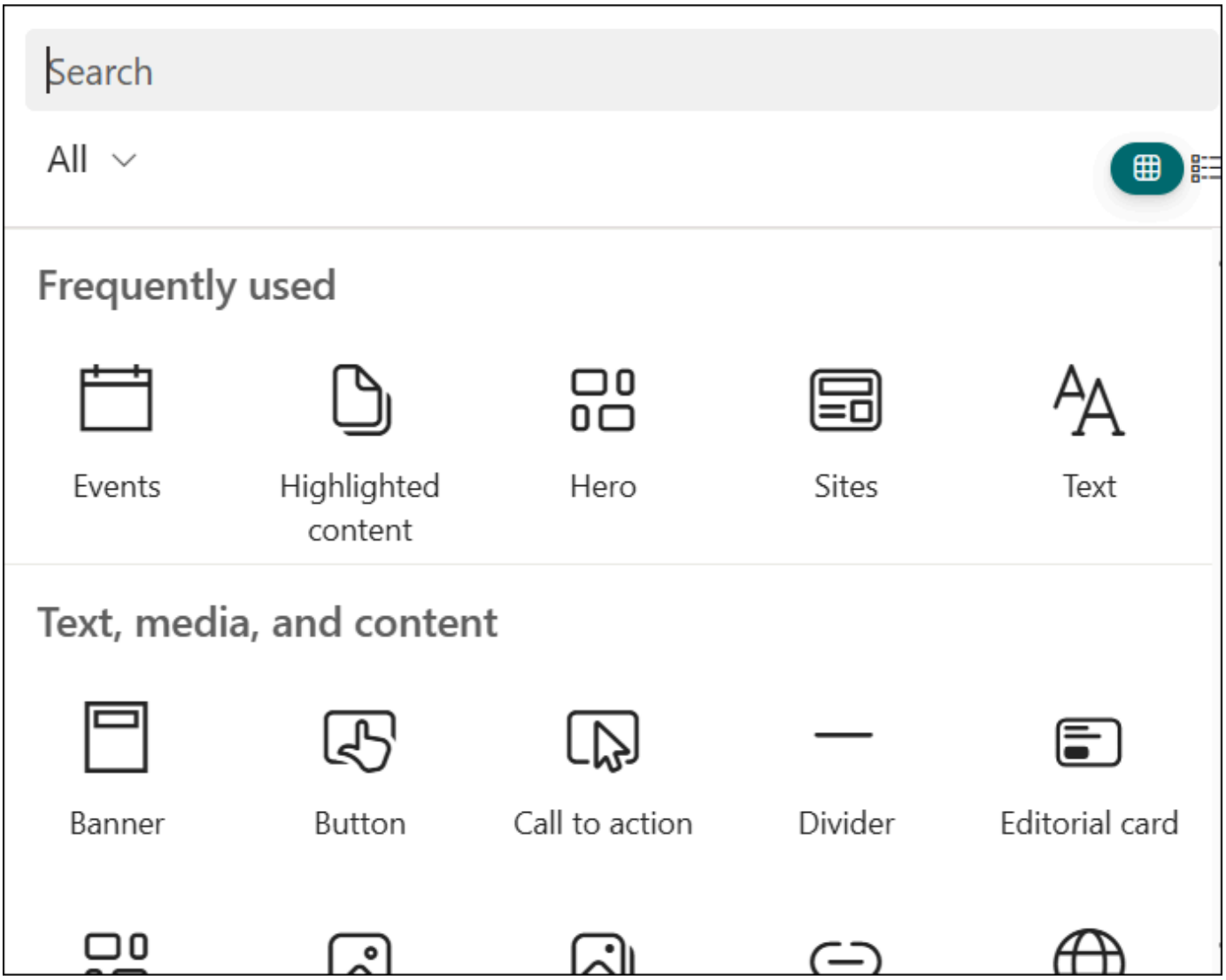
If your page isn't already in edit mode, select **Edit** on the top right of the page.

The + symbol before or after a section will add a section using one of several layouts.



For more information on working with sections, see Add or remove sections and columns on a page.

To add a web part to a section, select the plus symbol , which may appear before or after a web part in a section. For more information on all web parts, see Using web parts on SharePoint pages.

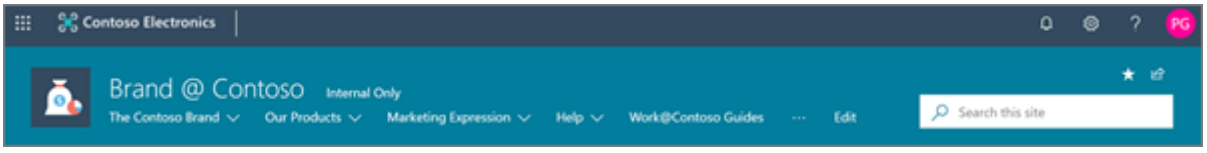


Web parts may be edited, moved, or deleted within sections. The **Edit web part** icon opens detailed controls unique to each web part type.

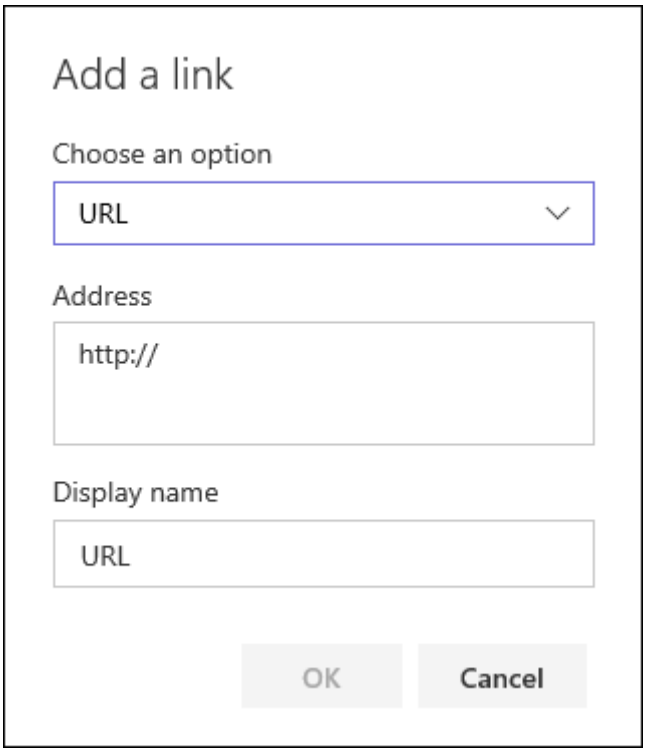
Back to top

Navigation

You can quickly and easily customize the organization and navigation of your SharePoint site.



Select **Edit** on the top menu to add and arrange links.

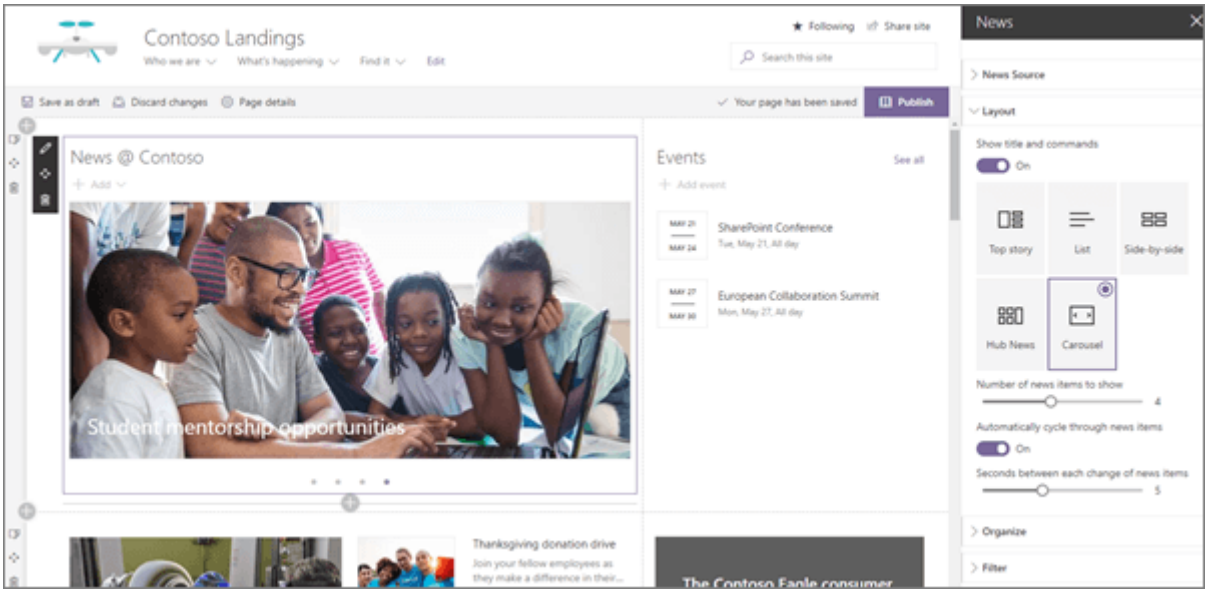


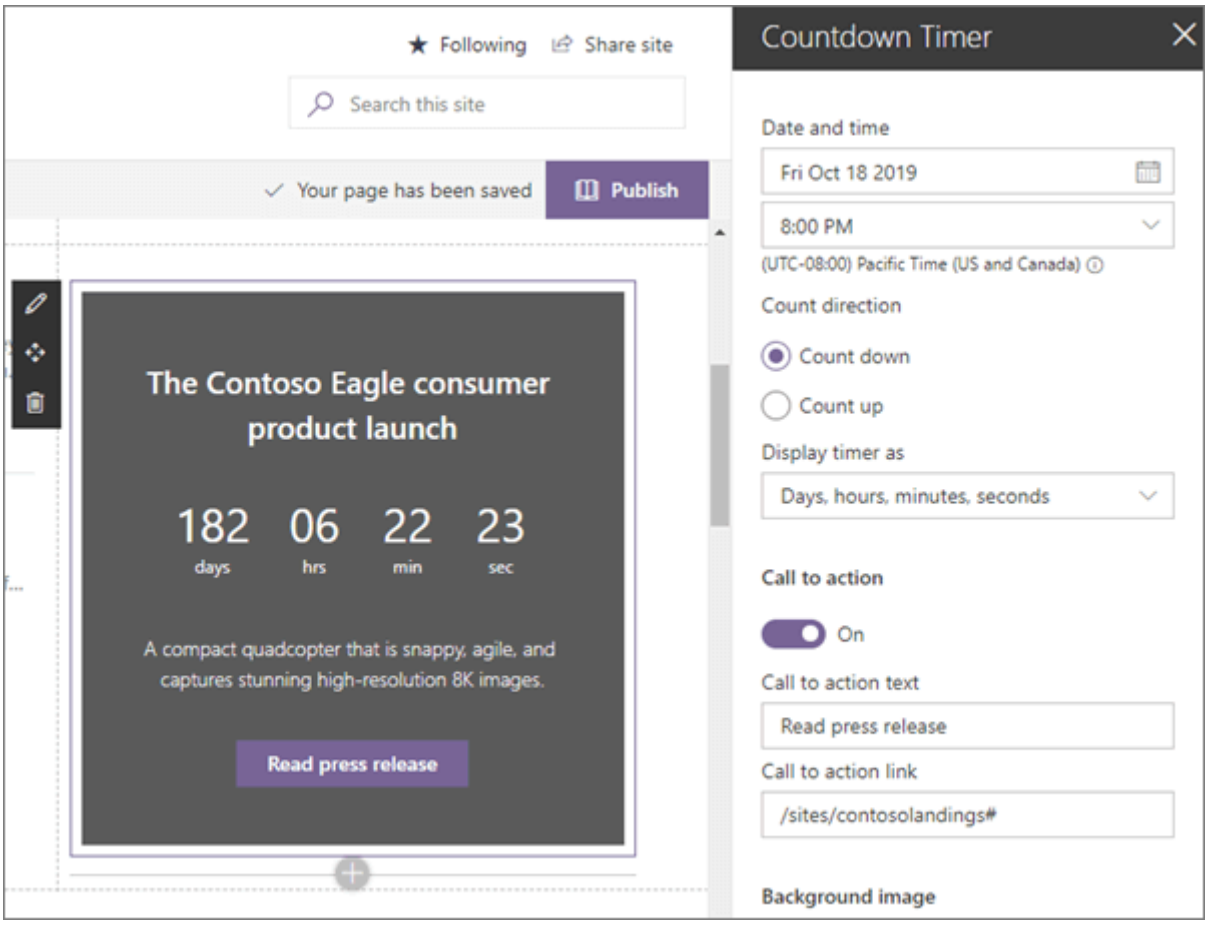
Learn more about customizing the navigation on your SharePoint site.

Back to top

Keep everyone up to date

The Enterprise Landing page uses two different News web parts. One uses the **Carousel** layout, and the other uses the **Top story** layout. In the example at the beginning of the article, these layouts are both in the first column of two-column sections on the page. The second column contains an Events web part that you can use to display upcoming events and activities. The second example photo below includes the Countdown timer web part to generate excitement for things like an upcoming event, activity, or launch.





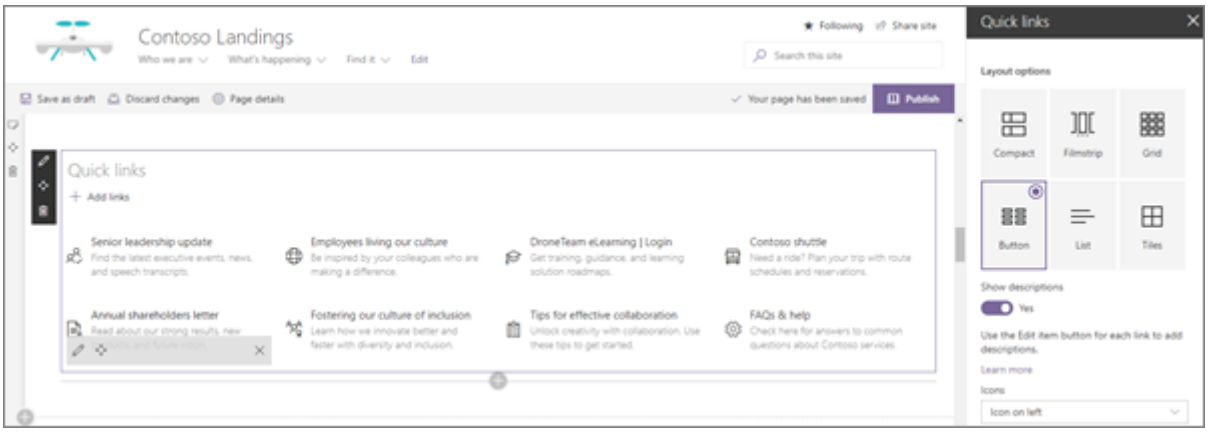
Back to top

Quick links

You can use buttons, icons, and descriptions to turn simple links into engaging guidance to help visitors find the sites they need.

In the example below, the Quick links web part is in a separate, one-column section.

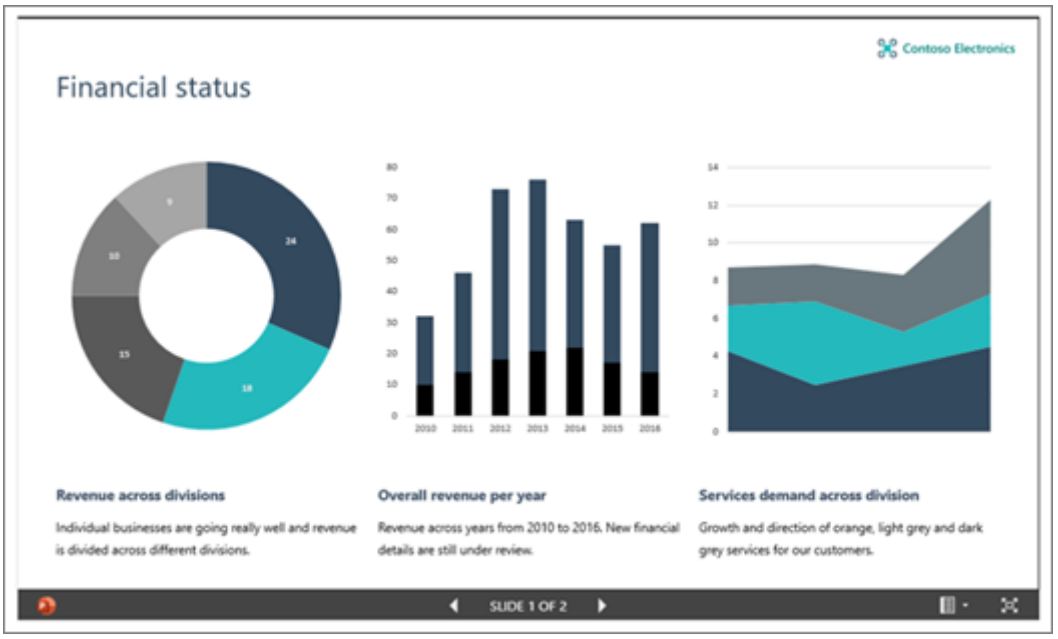
In this Enterprise landing site example at the beginning of the article, this web part uses the List layout with icons and descriptions added. To get this look, choose **Show descriptions** when you choose the **List** layout for the Quick Links web part. Then, use the Edit pencil under each individual link where you can add your own description. Then, use the **Edit** pencil icon under each individual link to add your own description.



Back to top

Documents and files

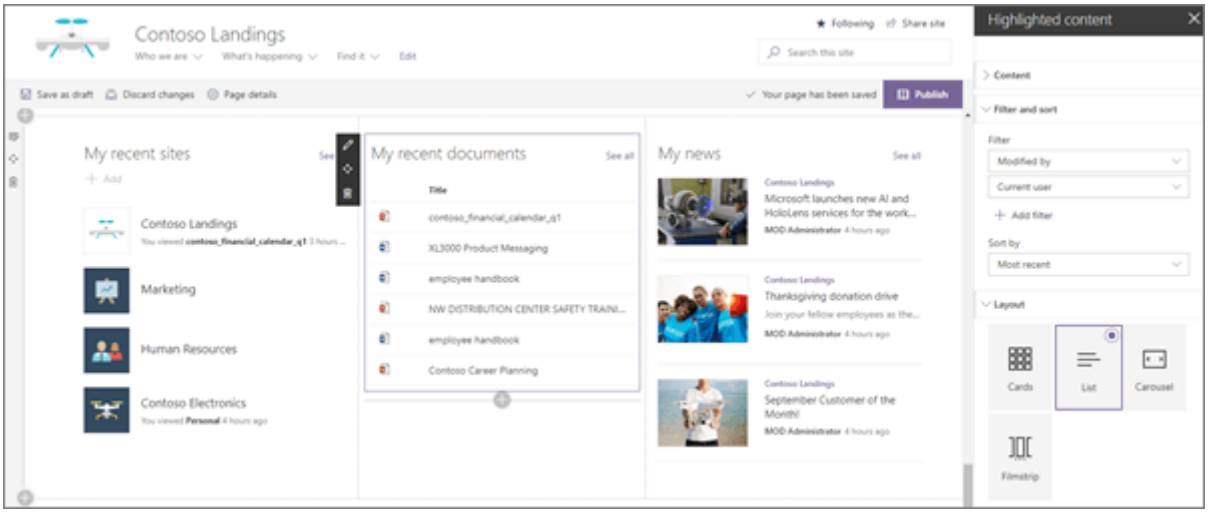
Display a file on the page with the File viewer web part. You can display Word, PowerPoint, Excel, PDF, and 3D model files, and many more types. In the example, two File viewer web parts are shown in two columns. One displays a Word document, and one displays a PowerPoint presentation.



Back to top

Personalized web parts

Recent sites (left column), Highlighted content (middle column), and News (right column) web parts are in a separate, three-column section. Each can filter content based on the current viewer of the site. These kinds of web parts used in this way can help draw viewers back to the page to see their latest visited sites, content, and news.



For more information on using these web parts, see Use the Sites web part, Use the Highlighted content web part, and Use the News web part on a SharePoint page.

Back to top

Want more?

Get inspired with more examples in the SharePoint Look Book.

See other guided walkthroughs for creating sites for your organization.

Last updated on 06/24/2026

Guided walkthrough: Create a hub site for your organization

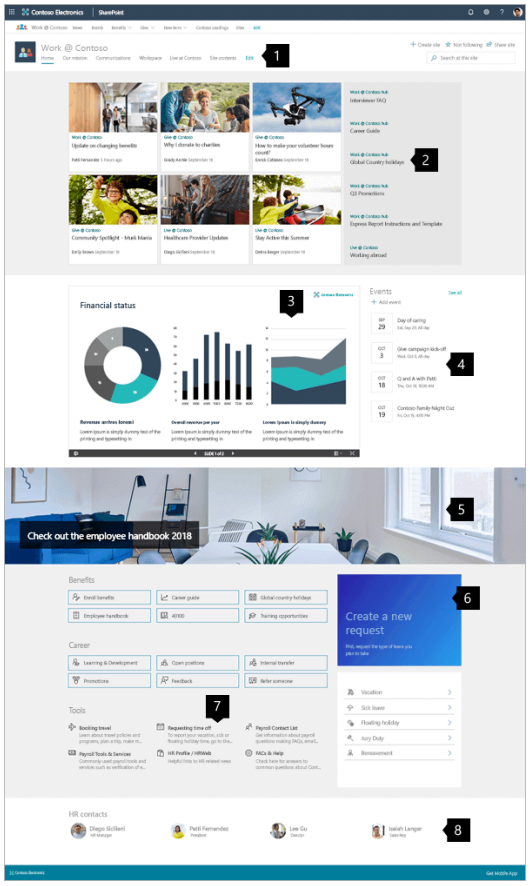
In this article, we show you elements of an example Hub site to inspire you, and help you learn how to create similar sites for your own organization. Hub sites empower visitors to find information and resources fast. This example Hub site offers news, links to key resources, events, and contacts. This example of a Human Resources hub site also suggests a custom app for employee time-off requests

First, if you haven't already created a Communication site, check out the Create your site section in this article. If you need to learn how to edit and publish the page on your site, check out the section Edit, work with sections and web parts, and publish in this article.

Once you have your created your site and know how to edit pages, you can use the steps below to add the elements shown.

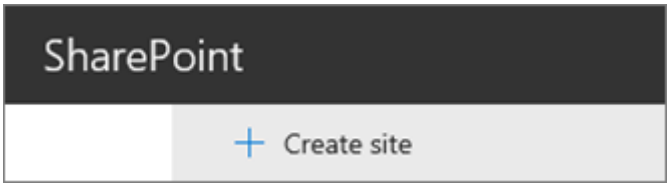
Example Hub Site

Expand table

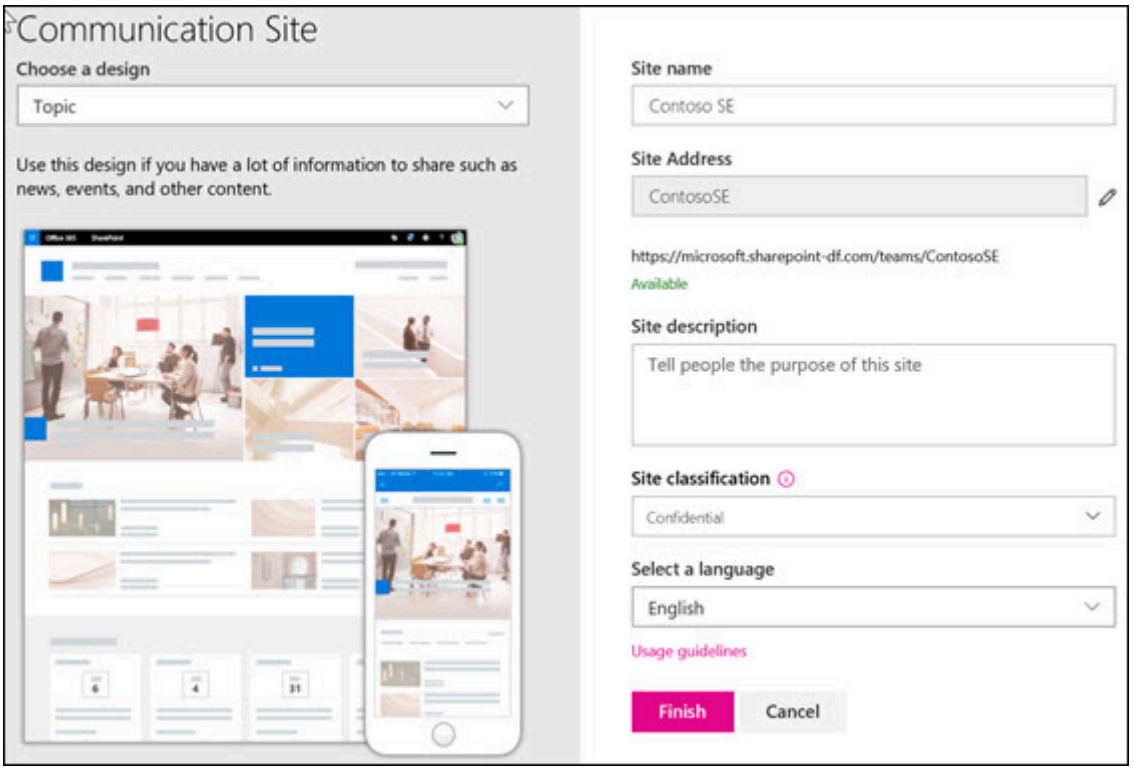
Image of the homepage	Customization instructions
	**1. Mega menus and edit controls** Quickly guide visitors to the information they seek. This area also provides admins access to editing tools. *Learn how* **2. Share news** Collect important news relevant to the site's area of focus. *Learn how* **3. Feature important content** Easily share financial presentations, charts, and reports. *Learn how* **4. Keep up-to-date on events** Offer quick access to information on upcoming events. *Learn how* **5. Create visual impact** Add visual impact with banner images. *Learn how* **6. Guide visitors to tools** Add custom tools to streamline process like requesting time off. *Learn how* **7. Provide a clear path** Guide users to the correct information and tools with icons and text summaries. *Learn how* **8. Feature the experts** Guide visitors to the experts who can help them resolve issues effectively. *Learn how*

Create your site

To make a site like the one shown here, you'll create a Communication site. To do this, select **Create site** from the SharePoint start page (or, if you're going to associate this site with an existing Hub site, navigate to the hub site and select **Create site** there so that the communication site is automatically associated with that hub site).



Next, choose **Communication site**, and then the **Topic** layout. Fill out your site name, description, and other information, and select *Finish*. Then you'll get a template with the same type of layout as the example in this article.

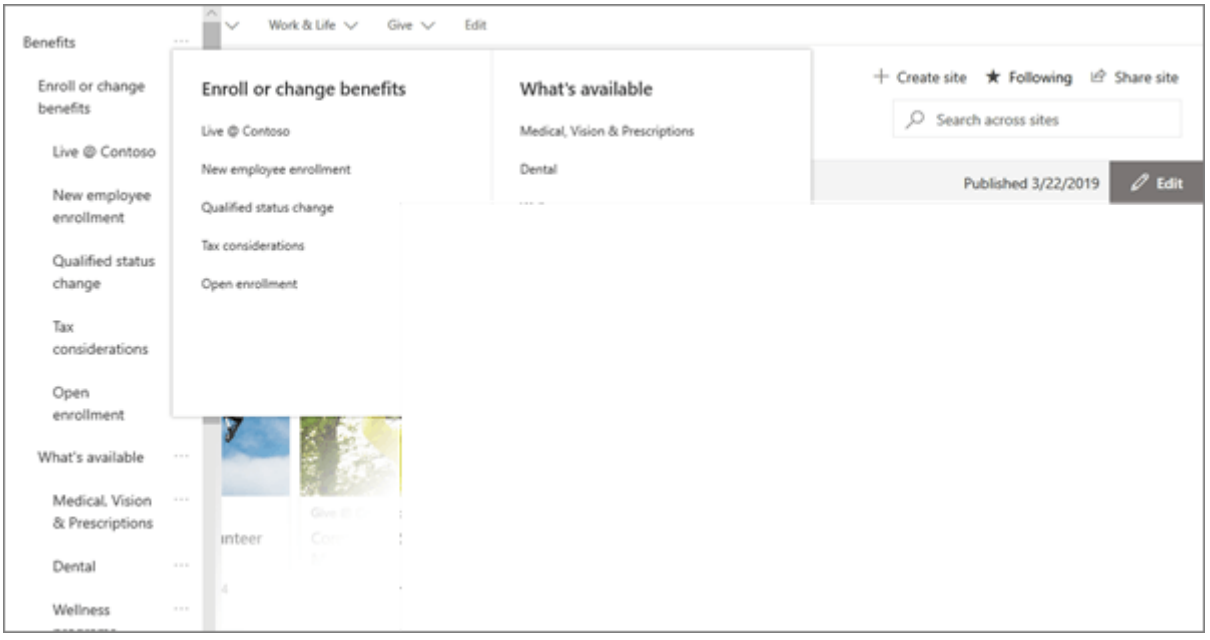


For more information, see Create a communication site in SharePoint Online.

Back to top

Managing the Mega Menu

The Hub site is optimized to organize and present links to other locations effectively.



Clicking **Edit** on the top menu opens a simple three-level outline list on the left. The outline level equates to the menu parts: Main menu, Header item, or Menu item.

- Select the **...** control on the right of the item name to set the items link and outline level.

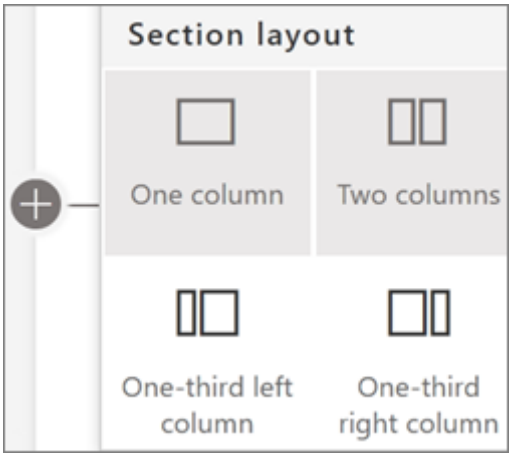
On the right, below the header, select **Edit** to begin editing your page. While editing, your drafts can either be saved for later or discarded. When your page updates are ready, select **Publish** to reveal them to your entire organization.

Back to top

Manage sections and web parts

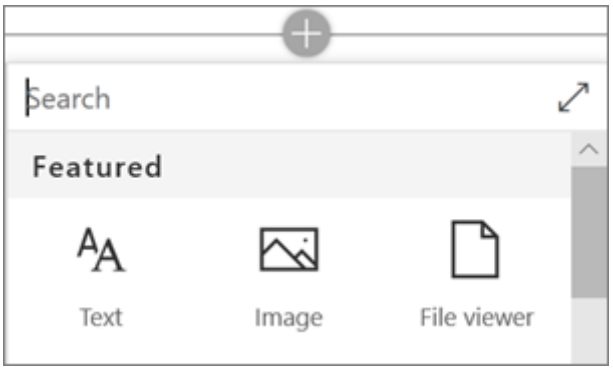
To create sections, start editing by clicking **Edit** on the top right of the page.

The + symbol before or after a section will add a section using one of several layouts.



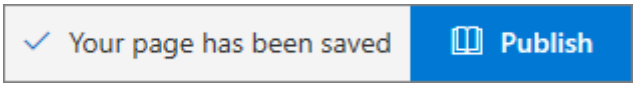
Sections make up your page, and are you place one or more web parts. While editing the page, each section will show controls to edit the layout, move, or delete the sections. For information on working with sections, see Add or remove sections and columns on a page.

Select the plus symbol in a section, which may appear before or after a web part in a section, to see the many types of web parts available. For more information on all web parts, see Using web parts on SharePoint pages.



Web parts may be edited, moved or deleted within sections. The **Edit web part** icon opens detailed controls unique to each web part type.

When your page updates are ready, select **Publish** to make them visible to your audience.



> **Tip**
>
> To manage all of your pages on the site, click **Pages** on the top menu.

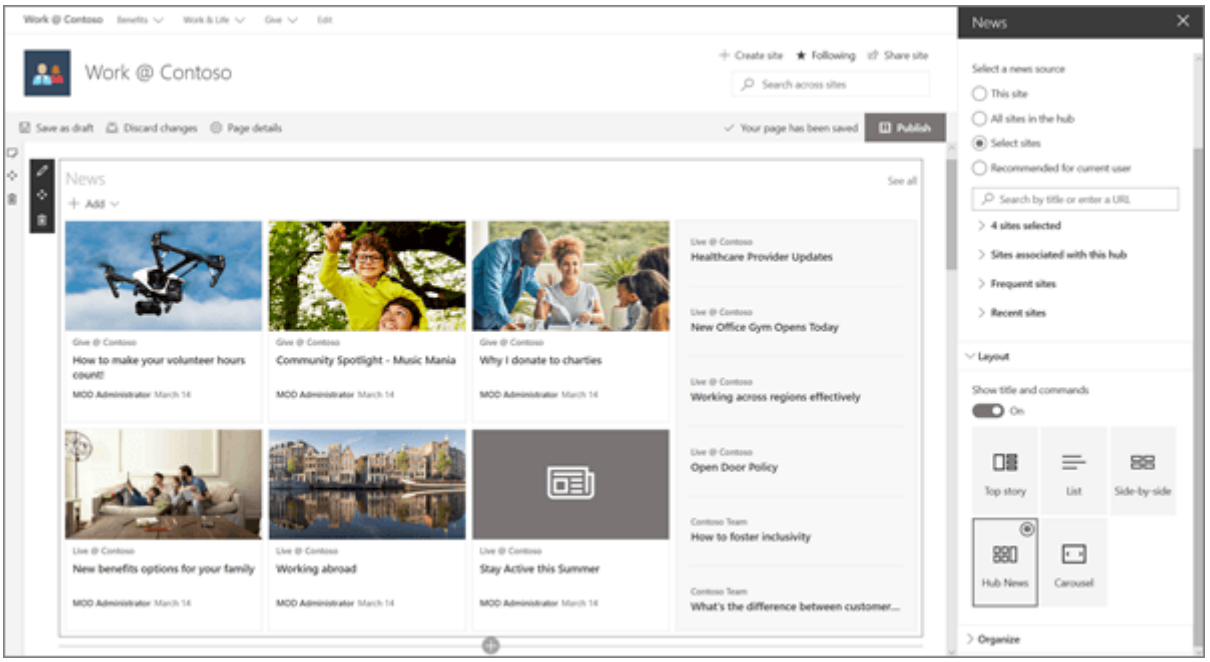
For more details on using pages, see Create and use modern pages on a SharePoint site.

Back to top

Add important news with the News web part

The News web part provides controls to choose the **News Source** and **Layout**, and to **Organize** and **Filter** the content. Hub sites bring information and resources together so visitors can find what they need and move forward in completing tasks efficiently. This site uses the **Hub News** layout, which is one of five options. Once a layout is chosen, explore the **Organize** tools to refine priorities in how the news is displayed.

In this example, the web part is in a one-column section.



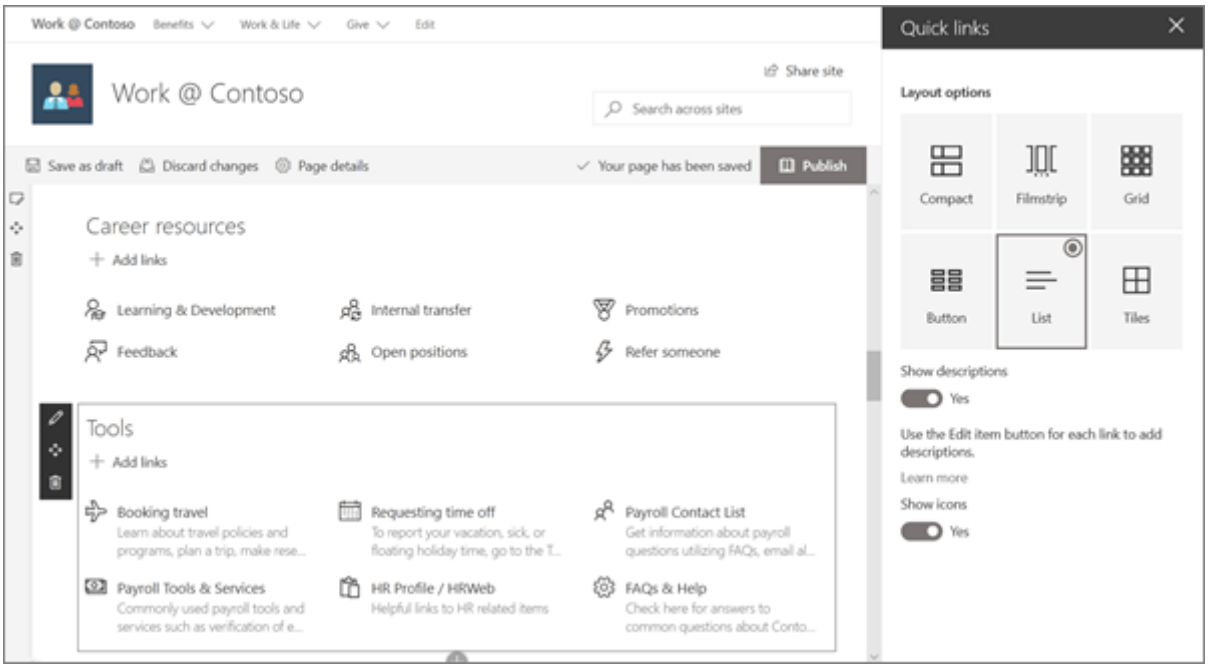
For more details on using the News web part, see Use the News web part on a SharePoint page.

Back to top

Style links to match the page with the Quick Links web part

The Hub site features the Quick links web part, and while it's lower on the Hub page, it is a key feature of the page. The Quick links web part provides several Layout options that use icons and text to help visitors locate the link they need.

In this site example, the **Compact** layout is used for Career resources, and the **List** layout is used for Tools, which allows short text summaries for each link.



For more details on using the Quick Links web part, see Use the Quick Links web part.

Back to top

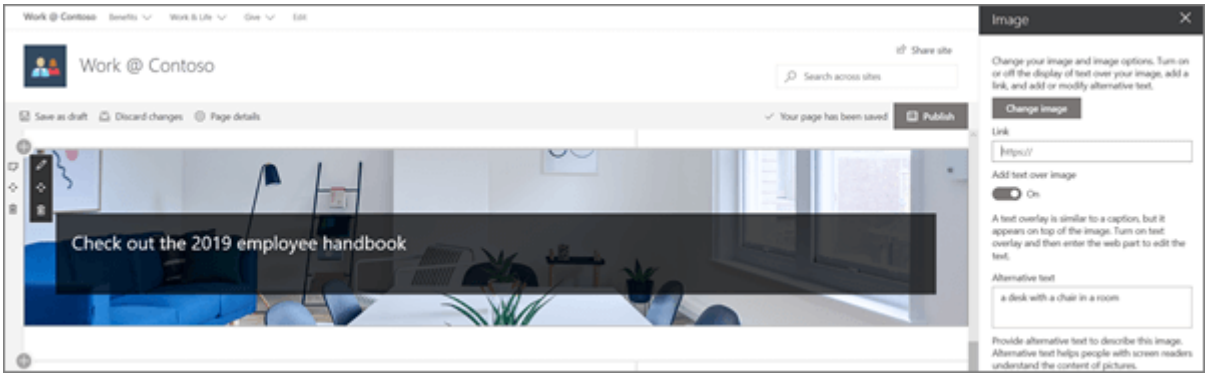
Add graphics with the image web part

Use images to create impact:

On this hub, an image with text guides visitor eyes to important links, information, and tools. This site also uses an image to suggest implementing a tool for employee time off requests.

Flexible controls:

The image can come from a location on the site, the cloud, or uploaded. Text options enhance communication and accessibility.



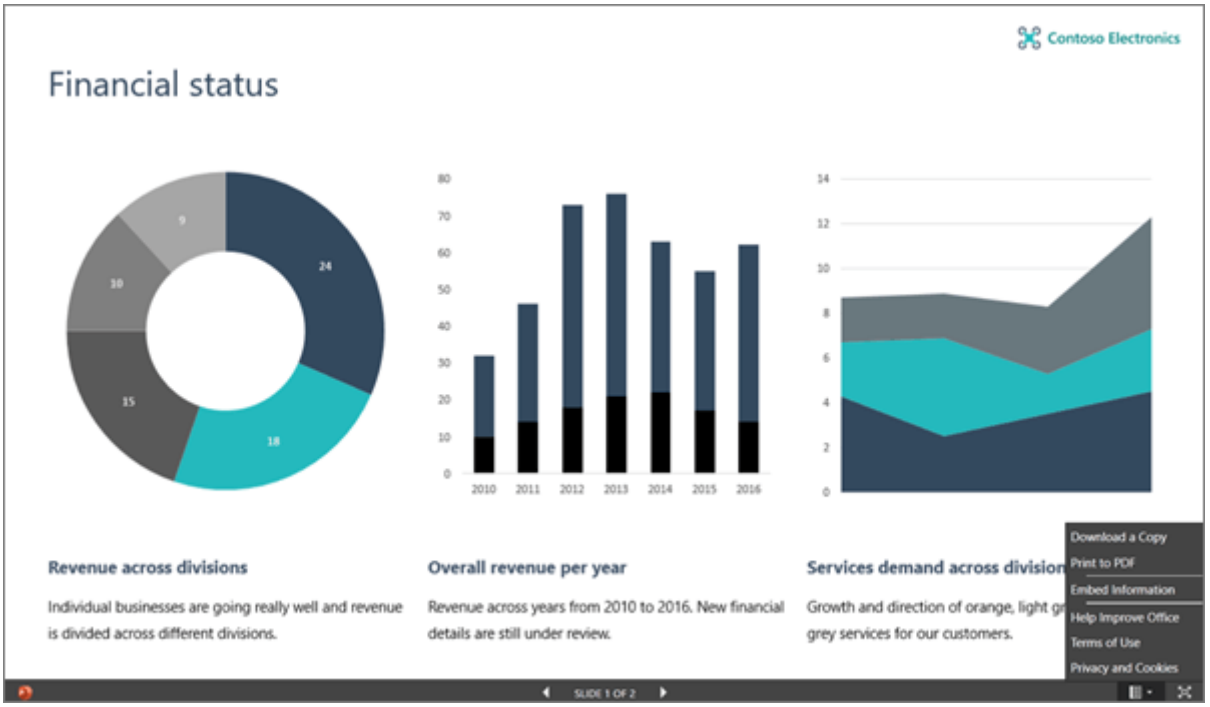
For more details on using the Image web part, see Use the Image web part.

Back to top

Share files interactively with the File Viewer web part

The File viewer web part allows important files in many formats to be posted to the page. The viewer allows visitors the choice to view and interact with the files using several methods. Visitors may:

- Download full copies
- Print to PDF
- View the files full screen in the browser

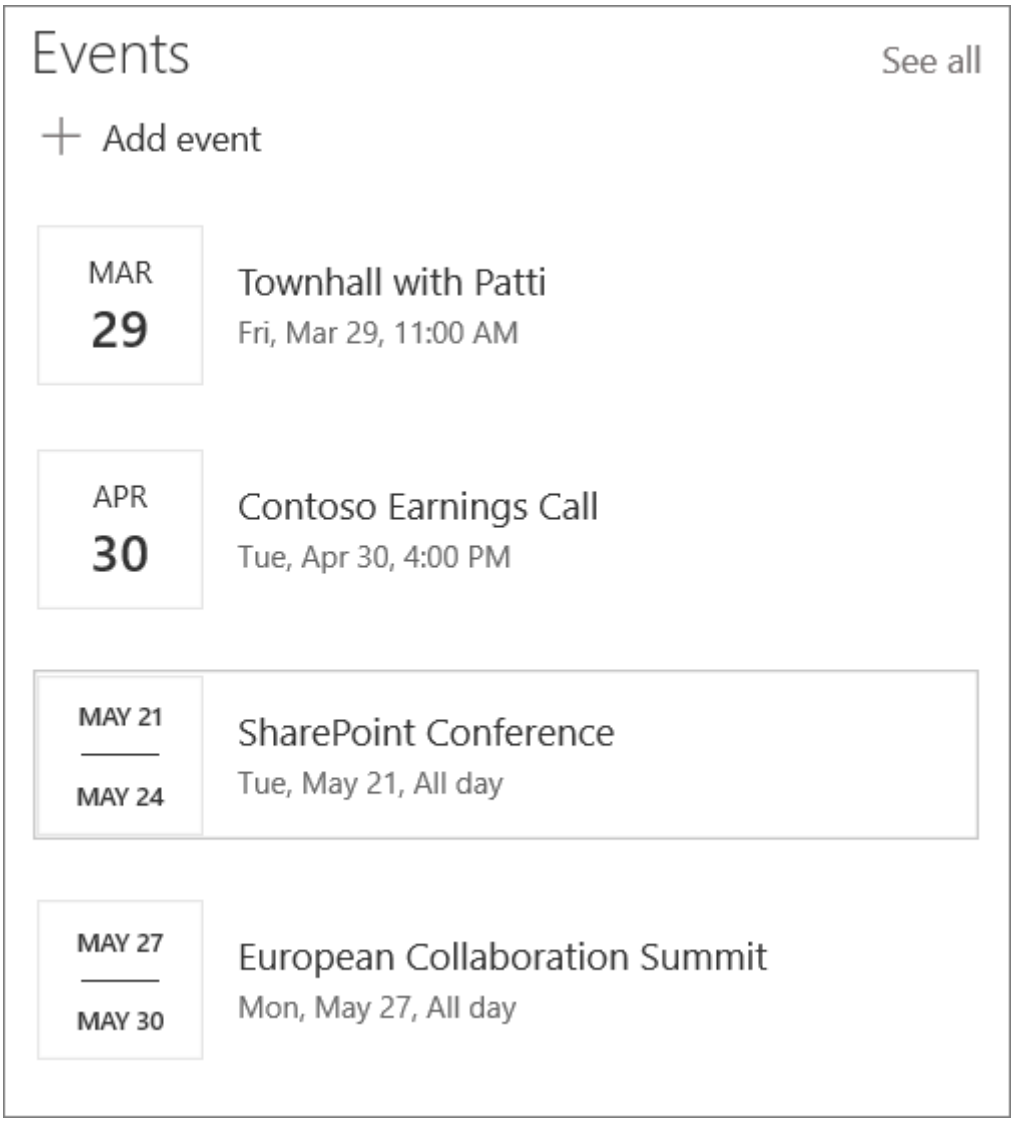


For more details on using the File viewer web part, see Use the File viewer web part. Back to top

Add a calendar of events with the Events web part

Inform visitors of important events. The Events web part can summarize events from all over the organization or from a specific list or calendar, and viewers can easily click the event to add it to their calendars.

In this Hub site example, this web part uses the Compact layout.

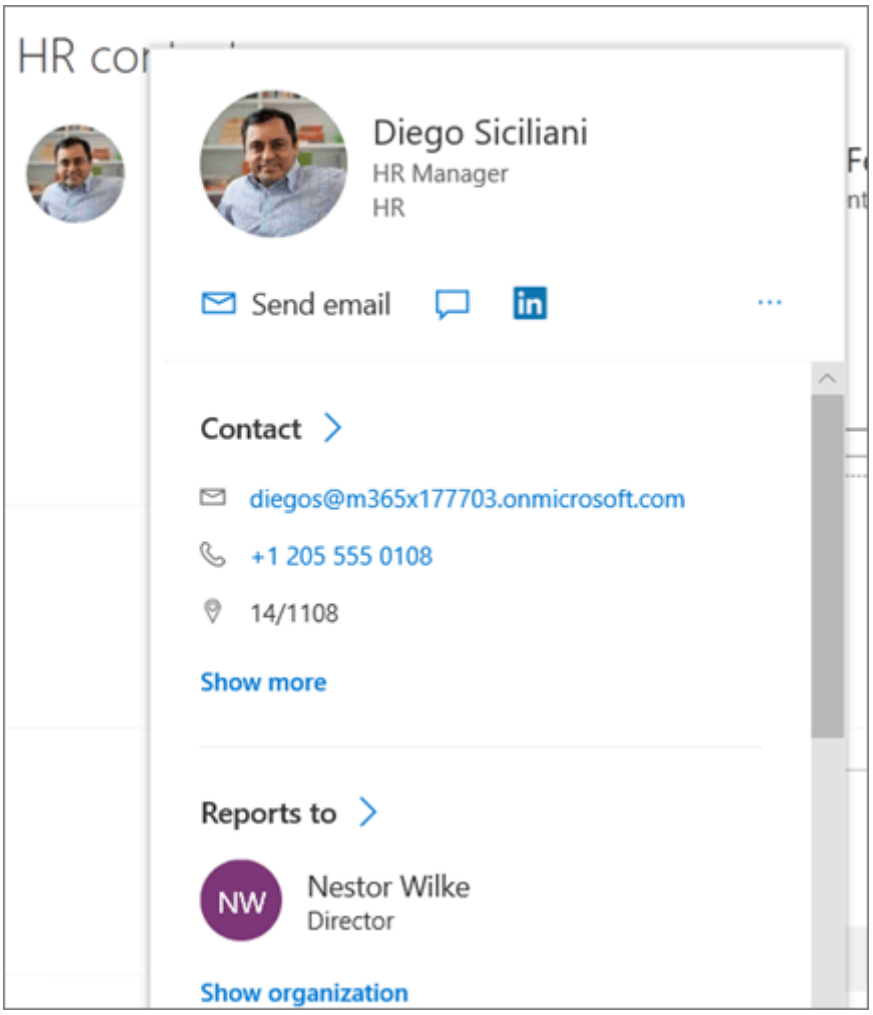


For more details on using the Events web part, see Use the Events web part .

Back to top

Feature people with the People web part

When visitors need to find stakeholders or expertise, make it easy by featuring them on the site. People tiles can be simple or provide extra detail, and one click brings up key details from their profile.



For more details on using the People web part, see Show people profiles on your page with the People web part.

Back to top

Want more?

Get inspired with more examples and the ability to add an example Giving site with the SharePoint Look Book.

Last updated on 06/24/2026

Guided walkthrough: Setting up news for your organization using a hub site

With SharePoint, you can share news content across your organization in a meaningful and discoverable way. By default, SharePoint news is shown on the SharePoint start page, on team sites, communication sites, hub sites, and on the mobile app according to how relevant the news is for the user. For example, if an important news story is posted by someone in your close sphere of work or posted to a site where you're active, it will be shown to the user.

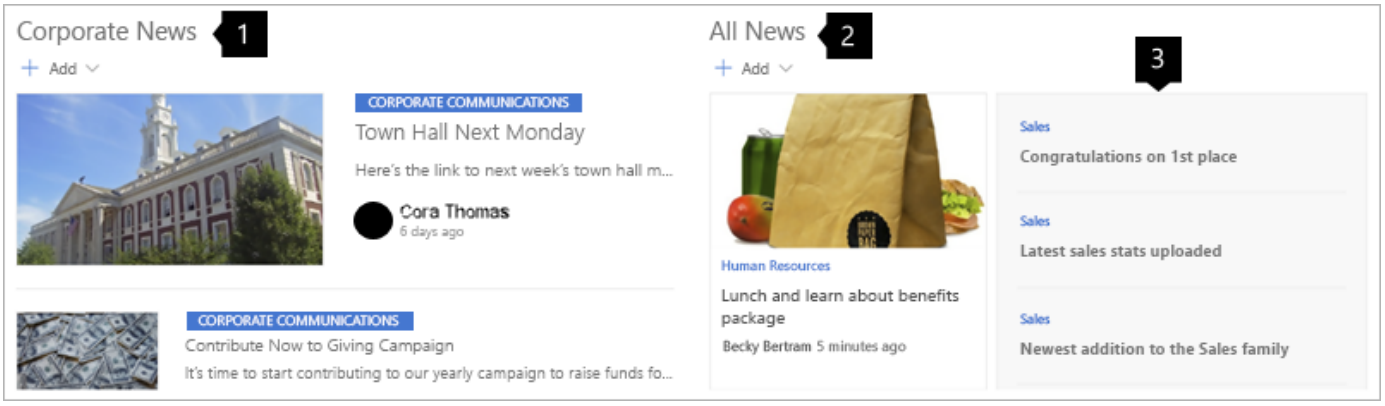
Organizations have many options as to the kind of news shown, where it's shown, who can author posts, and more.

In this article, we'll show you how to implement a comprehensive strategy for setting up news at all levels of your organization.

The strategy

In this walkthrough, we'll do more than just set up News web parts on various sites. We'll show you a comprehensive strategy that includes setting up an "official" news site for news that is visually distinguished as organization news; setting up categories for different types of news; and even setting up an approval process for news posts. We'll display news on an intranet hub site that comes from a corporate communication site, a department communication site, and a department team site.

The hub site homepage displays all approved news stories for any site associated with the hub. That means users see all news posts created in the Corporate News site, all news posts created in departmental communication sites, and news stories for just their department's team site.



1. News from an official corporate communication site that's part of the hub site

2. News from a department communication site that's part of the hub site
3. News from a department team site that's part of the hub site

Content is displayed in the following way on the sites in the hub:

- Each departmental communication site displays news posts for just that department.
- Each departmental team site displays news posts created in that team site and posts created in the Corporate News site.

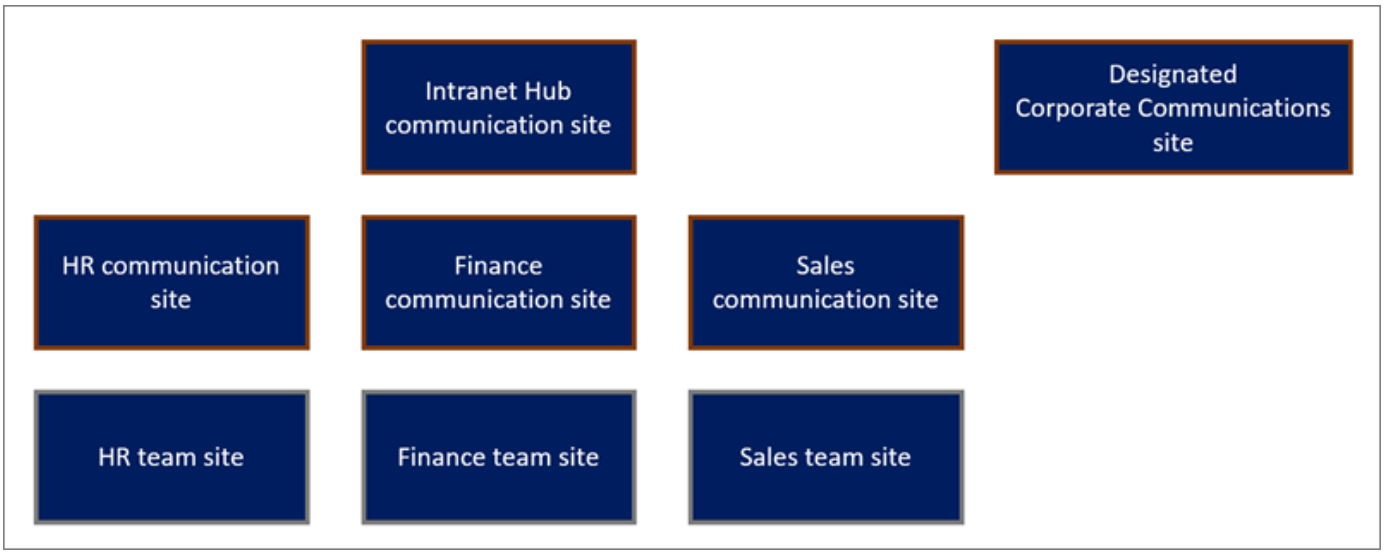
Here's how the news flow works:

- All employees have permission to create news on their team sites. Posts can be tagged as being a "milestone" or simply "departmental."
- Each department has one or more employees assigned the task of creating news posts in their department's communication site.
- All news stories created in departmental communication sites go through a page approval flow in which a designated person from the Corporate Communications department approves posts.
- Official news posts from the Corporate Communications department are created in a special site called Corporate News, which is not associated with the hub site. This site is designated as "official" news.
- On a monthly basis, a newsletter containing selected news stories from Corporate Communications is emailed to all employees.

The hub site structure

All team and communication sites, except for the Corporate communication site, are associated with a single hub site.

Each department has a communication site to share information with the rest of the organization, and a team site for internal communication among department employees.



Implementing the strategy

In this section, you'll walk through the process of setting up your SharePoint environment to meet the requirements of this news strategy. This process involves setting up the News web part and creating a Page approval process in a Pages library, creating categories for news, and designating one site as "official news."

In this example, the assumption is that each of the communication and team sites is already associated with a hub site (except for Corporate Communications) and there are already several news posts in the Corporate Communications site. If you need to know how to set up these types of sites, see Set up your SharePoint hub site, Create a communication site in SharePoint Online, and Create a team site in SharePoint.

Set up your corporate communications site for official organization news

Setting up your corporate communication site for "official" organization news allows news stories from Corporate Communications to appear with emphasis so your users know immediately that this is official company news, like in this example:

To enable this feature and specify the site for organization news, a SharePoint Administrator must use the SharePoint Online PowerShell commands:

Get-SPOOrgNewsSite

Set-SPOOrgNewsSite

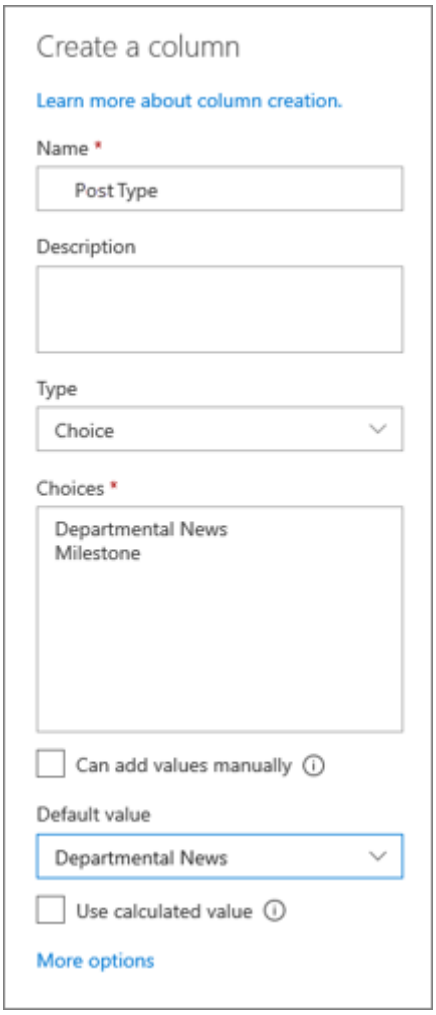
Set up news on a department team site

In your department team site, you'll add the News web part to the page three times. Each web part will display different news information based on news source and categories. To create the categories, add a column to the Pages library to allow authors to tag their pages with the appropriate category.

Create columns for categories

1. On your department team site, select the **Pages** link in the site navigation to go to the pages library.

2. Select + **Add column** or the + to the right ot the last column name at the top of the pages.



3. In the **Name** field, enter the name **Post Type**.

4. In the dropdown menu, choose **Choice** as the type of column.

5. Provide two choices: "Department News" and "Milestone."

6. Select **Save**.

Next, we'll add News web parts to the department team site home page to show department news, milestone news, and news from your organization's website.

Add Department news

1. Add a one-third right section to the home page.
2. In the first column, add the **News** web part, and title it “Department News.”
3. Select **Edit** in the web part toolbar.
4. Set the following options in the web part property pane:

    - **News source**: This site
    - **Show title and commands**: On

- **Layout**: Top story
- **Filter**: Page properties
- **Property name**: Post type **Equals** Department News

5. Select **Apply** to save your changes.

Add Milestone news

1. In the same column, beneath the web part you just added, add the **News** web part again, and title it "Milestones."
2. Select **Edit** in the web part toolbar.
3. Set the following options in the web part property pane:

    - **News source**: This site
    - **Show title and commands**: On
    - **Layout**: Side-by-side
    - **Filter**: Page properties
    - **Property name**: Post type **Equals** Milestones

4. Select **Apply** to save your changes.

Add Corporate news

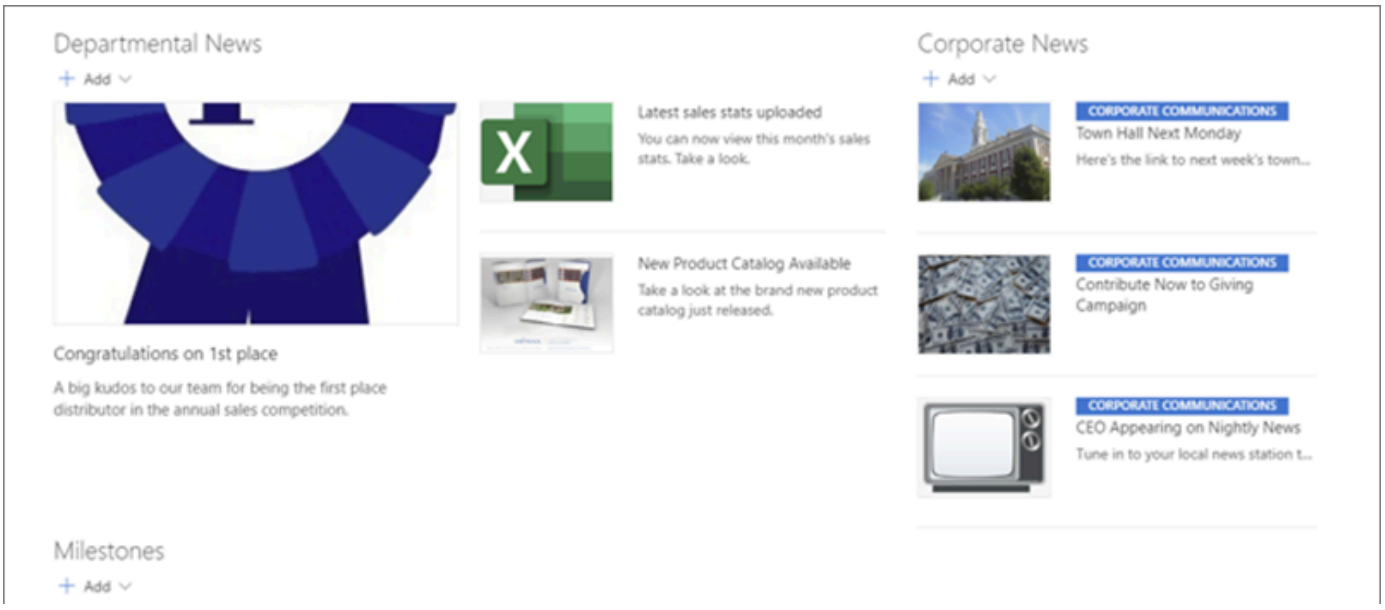
1. In the second (right) column, add the **News** web part again, and title it "Corporate news."
2. Select **Edit** in the web part toolbar.
3. Set the following options in the web part property pane:

    - **News source**: Choose **Select sites**, and then select your corporate news site.
    - **Show title and commands**: On
    - **Layout**: Side-by-side
    - **Filter**: Page properties
    - **Property name**: Post type **Equals** Milestones

4. Select **Apply** to save your changes.

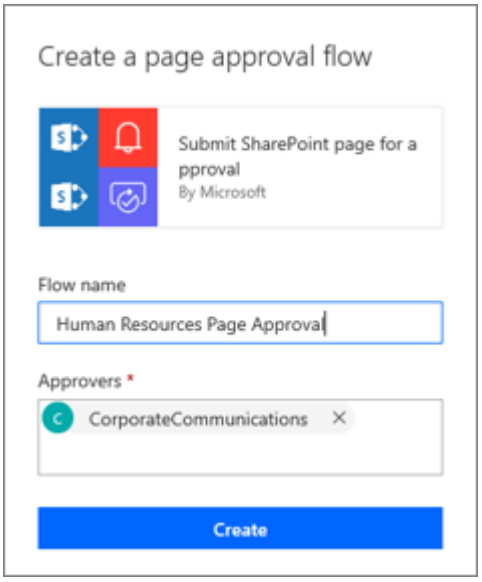
To test what you've done so far, create several news posts in the department site. Set the page properties on your news story pages so that in some the Post Type is set to Department News, and in others, set the Post Type to Milestone. For a refresher on setting properties for pages, see View, edit, and add page details.

This is what the department homepage looks like after it's complete:



Set up your department communication site

In this example, news posts created in the communication site must be approved. You can set up page approval using Power Automate. Give the Flow a name that includes the site name such as "Human Resources Page Approval" and set the approver to an employee in the Corporate Communications department.



Next, set up the site home page to display news stories from this site.

1. On the home page of your department communication site, add a **News** web part.
2. Select **Edit** in the web part toolbar.
3. Set the following options in the web part property pane:

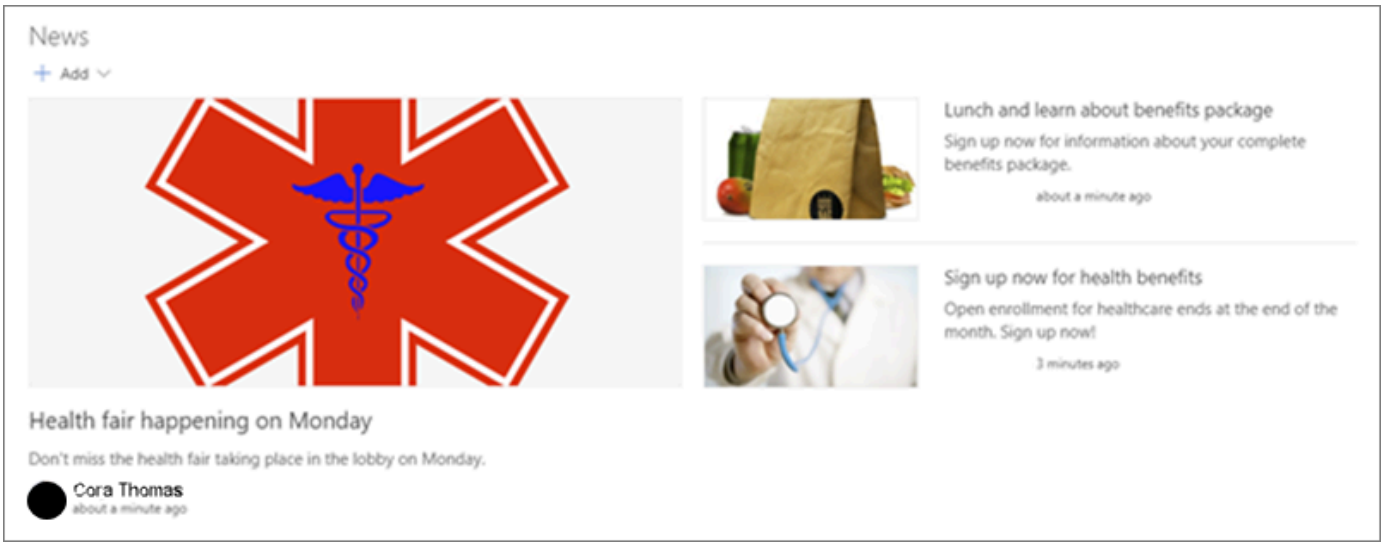
- **News source**: This site
- **Layout** Top story

4. Create a news post you'd like to display on your home page. When you're done, submit the page for approval by selecting **Submit for approval** at the top right of the page.

The employee designated as an approver when you set up the Flow will receive an email that the page is waiting for approval. Once they approve the page, it will appear in the News web part on your department communication site.

Go ahead and create several news posts in this site. Ensure that each page is submitted for approval and then approved.

In this example, you can see the kind of news displayed on departmental communication site for the Human Resources department:



Set up the Intranet hub site homepage

1. Add a two-column section to your hub site home page.
2. In the left column, add the **News** web part.
3. Select **Edit** in the web part toolbar.
4. Set the following options in the web part property pane:

    - **News source**: Choose **Select sites**, and then choose **Corporate Communications site**.
    - **Layout**: Top story

5. In the right column, add the **News** web part again.
6. Set the following options in the web part property pane:

    - **News source**: All sites in the hub

- **Layout**: Hub news

When you're done, you should see just the news posts from Corporate Communications on the left side of the page, and news posts from every site associated with the hub in the web part on the right.

Developing your own news strategy

Now that you've seen how to put one specific strategy to work, you can think about your own strategy. Here are some questions to ask yourself, and your organization, to help you prepare:

- How is news currently communicated? How can you use the same people or processes that you already have in place when utilizing the new approach?
- What kind of news content do you want to share?
- Who will be authoring content?
- Does news need to be approved? If so, what should the approval process be?
- How is news currently communicated?

Organization- and department-wide communications

In many organizations, there's already a formal means of communicating information to employees organization-wide. Additionally, in many cases, employees within a department communicate with one another in a less formal way. It’s important to think through these processes because, in some cases, you can continue to utilize the same people or processes within SharePoint.

When thinking about communication organization-wide, ask yourself the following kinds of questions:

- Does someone at your organization create and send newsletters?
- Are they emailed? If so, what's the current process for letting that person know which news needs to be included? How often are the newsletters sent out?
- What's the process for determining which news gets included and which doesn't? Who makes that decision?
- What's the process for editing the content?
- What's the process for deciding which images get included in stories?

At the departmental level, ask yourself these kinds of questions:

- Is there someone whose job responsibility includes sharing information with the rest of the department?
- Do employees share information informally with each other using tools such as email or messaging one another?
- What content is being shared?

Types of content and its relevance

The next step in building your news strategy is to evaluate the kind of news content being produced by your organization. Types of news stories might include:

- "In the news" stories that notify employees that your company or organization got public press, such as appearing in a trade publication or on a news program
- Company announcements or milestones, such as releasing a new product or starting a new initiative
- Employee milestones, such as when an employee gets married, has a child, or retires
- Information that requires employees to take action, such as signing up for benefits or attending training

As you think about this content, it's important to think about relevance and importance for various groups within your organization. For example:

- Everyone in your organization needs to know when they can sign up for benefits. This is important and relevant for everyone.
- People in the Finance department need to know about new laws that relate to their accounting practices. This is relevant and important to them. However, it's not relevant or important for anyone else in the organization.
- The Sales department is having a cooking competition in the break room on Friday. This might be relevant to those in the Sales department, but it doesn't qualify as important, and

no one else in the organization would consider it relevant or important.

The purpose of thinking through your content is to make a note of which content needs to be surfaced in a more predominant way, a secondary way, or not at all. How you answer this question may depend on factors such as the size of your company. If you're a small company, you may decide that employee milestones should be displayed company-wide, while a larger company may only show this to employees in a particular department.

Who's doing what

Who's authoring news content?

In some organizations, news content is created and managed by a central person or group of people, such as the Corporate Communications department. This centralized approach creates a simple approach to authoring and managing news content, ensuring that only important and relevant content is published for employees company-wide. However, this approach reduces the amount of news content typically generated because it requires the intensive time of one individual or one group of people. By opening up the publication process to others in your organization, you're empowering others to author news content. News content created by users in their own departments will be newer and more focused on their department activities, increasing the content's relevance.

Who's approving news content?

Once you allow others to create news content, it's possible that content will be created that doesn't fit your criteria for quality content. That may include content that has spelling and grammatical errors, uses inappropriate language, or is irrelevant. You may decide to implement an approval process to ensure that content meets the criteria necessary for publication.

How will users consume news using SharePoint?

Traditionally, intranet sites were built with the assumption that users would navigate to the intranet homepage and consume news there. In this scenario, important company news would be presented on the homepage, with an additional news feed of stories that were aggregated from departmental sites. This is a "pull" scenario, where "official" content (often important and relevant to all employees) is displayed and aggregated content is "pulled" from other departmental sites. In many cases, however, users don't navigate to the intranet homepage anymore. Users may simply navigate directly to their departmental site homepage, since that site contains most of the information they find relevant. In some cases, organizations may choose to implement a "push"

scenario, where official information is “pushed” down to their departmental site and is displayed alongside news stories that were created just in their department.

If your organization is using hub sites, you can aggregate news content at the hub level. If your organization has implemented multiple hubs, it’s important to think about how these hubs play into your overall news strategy. It’s common practice to create both an internal and external department site. The internal departmental site is typically a group-connected SharePoint team site. That site is only intended for members of that department. However, there's also a public SharePoint communication site, which is used to communicate information from that department outward to the whole organization.

Using this model, all users will see all news posts created in departmental communication sites, but users will only see news posts created in team sites to which they belong.

It’s also important to think about the other places where users might consume news content. Users can read news stories using the SharePoint app on their mobile device and on the SharePoint page in Office 365. Additionally, a site owner can create a newsletter of recent news stories, which can be sent to users. Also, users can post news stories from a group-connected SharePoint site to a Microsoft Teams channel.

Want more?

Get inspired with more examples in the SharePoint Look Book.

See other guided walkthroughs for creating sites for your organization.

Last updated on 06/24/2026

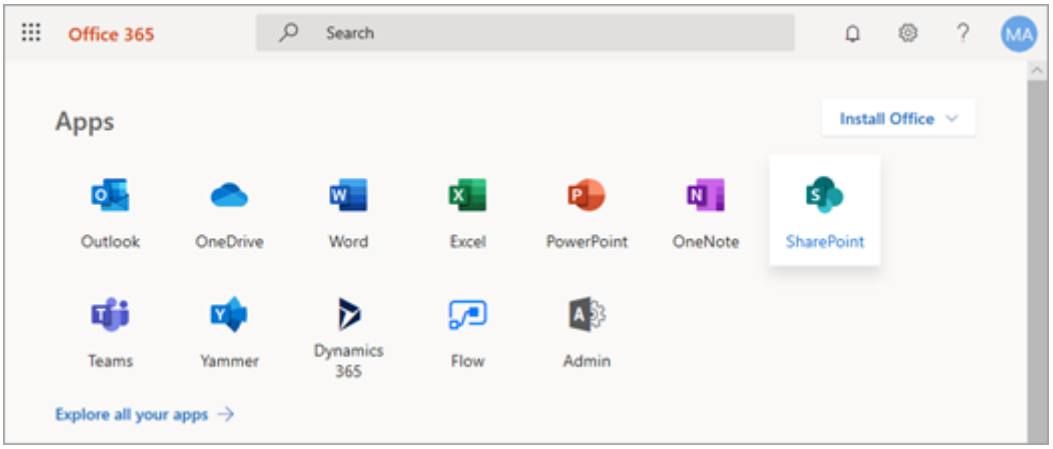
Add featured links to the SharePoint start page

As at least a SharePoint Administrator in Microsoft 365, you can feature the sites and content you want on the SharePoint start page by changing the **Featured links** list in the left pane. To add links to a SharePoint Server page, see Video: Add a link to a page.

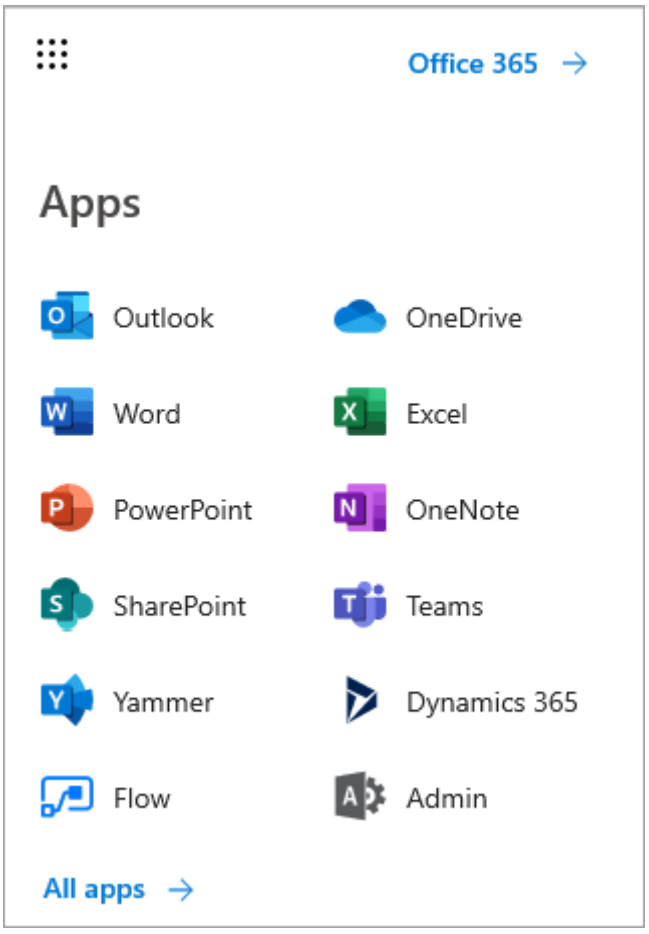
> **Note**
>
> To learn more about the SharePoint start page, see Find news, sites, and portals in Microsoft 365.

To view the SharePoint start page:

1. Sign in with your work or school account at https://www.office.com/signin.
2. Select SharePoint from the list of apps.

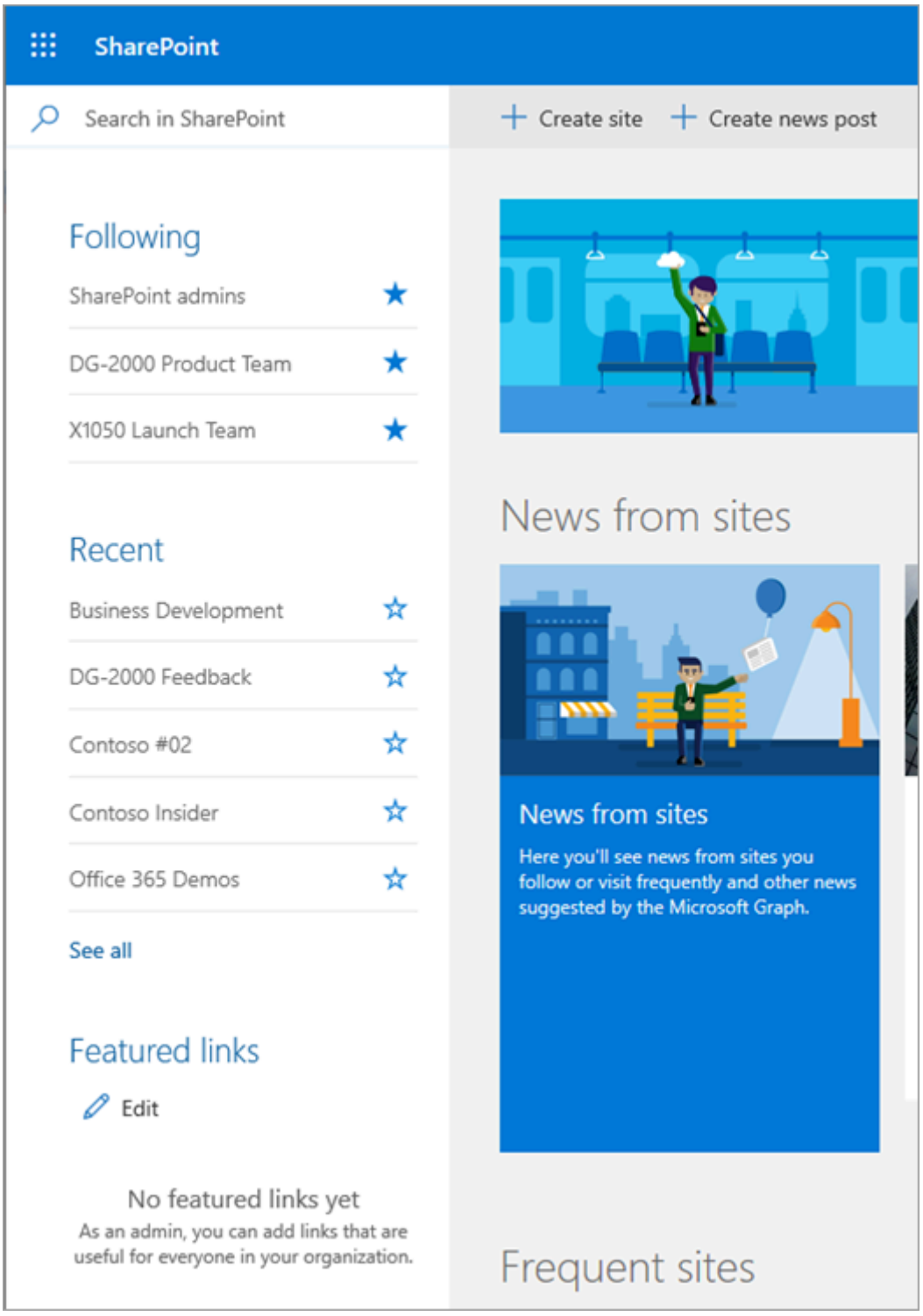


If you don't see the list of apps, select the app launcher icon in the top-left corner of the page, and then select **SharePoint**.



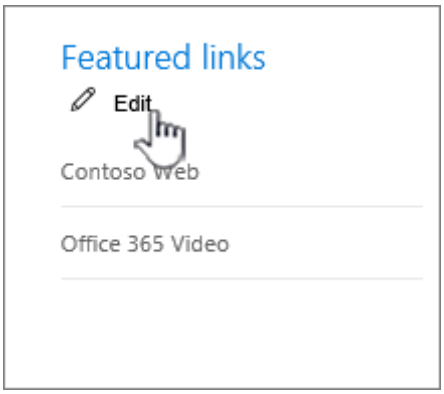
Can't find the app you're looking for? From the app launcher, to see an alphabetical list of all the available Microsoft 365 apps, select **All apps**. From there, search for a specific app.

On the left side of the page, a **Featured links** list appears.



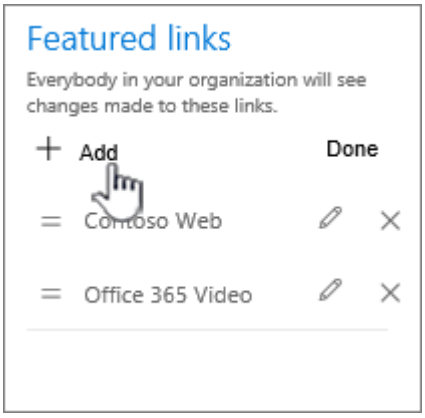
Add a link

1. Select **Edit**.

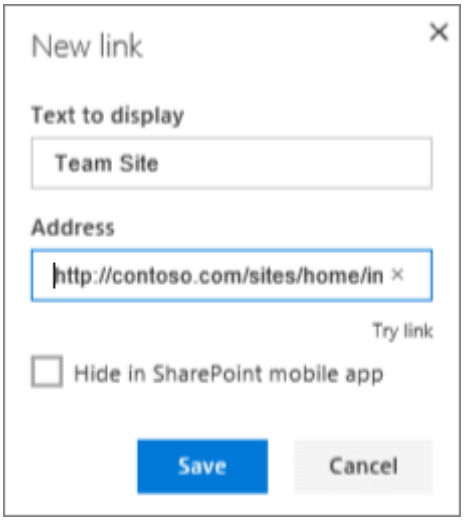


> **Note**
>
> If you don't see **Edit**, you don't have permission to change the Featured links list. Contact your administrator.

2. To add a link, choose **+ Add**.



3. Fill in the **Text to display** and **Address** in the **New link** dialog.



4. Select **Try link** to check the link.

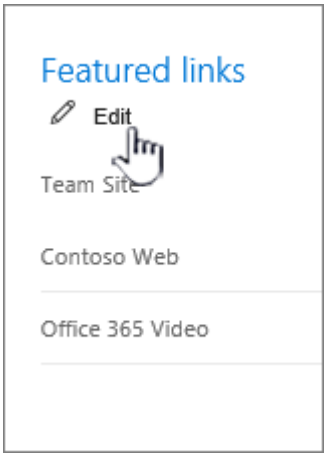
5. Select **Save**.

The new link will appear at the top of the list. To change where the link appears, you can drag and drop it within the list.

6. To leave edit mode, select **Done** when you're finished.

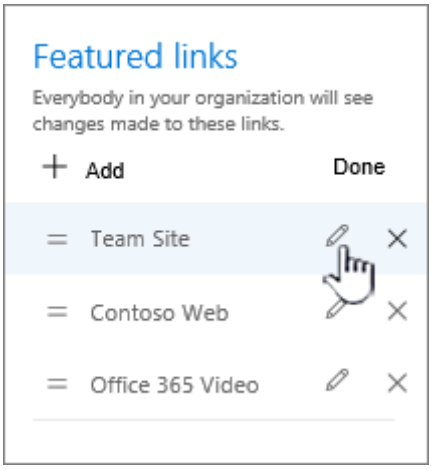
Edit a link

1. Select **Edit** at the top of the list.

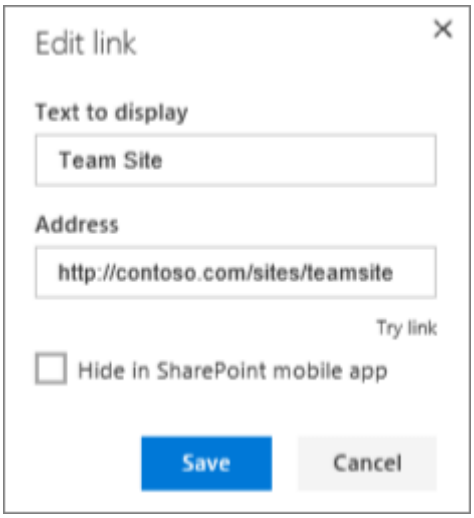


> **Note**
>
> If you don't see **Edit**, you don't have permission to change the Featured links list. Contact your administrator.

2. Select the link you want to change.



3. Fill in the **Text to display** and **Address** in the **Edit link** dialog.



4. Select **Try link** to check the link.

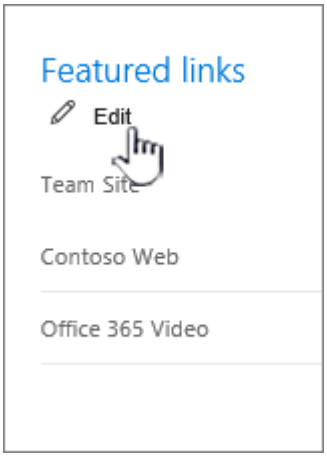
5. Select **Save**.

6. To leave edit mode, select **Done** when you're finished.

   To change where the link appears, you can drag and drop it within the list.

Change the order of links

1. Select **Edit** at the top of the list.



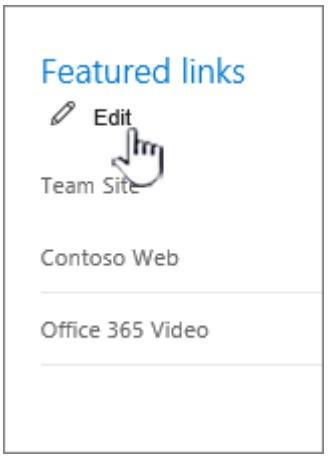
> **Note**
>
> If you do not see **Edit**, you don't have permissions to change the Featured links list. Contact your administrator.

2. Drag each link to the place you want within the list.

3. To leave edit mode, select **Done** when you're finished.

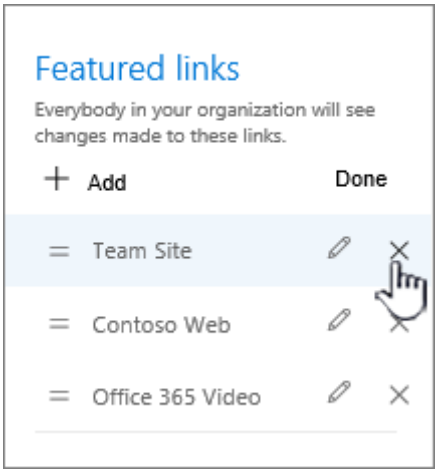
Delete a link

1. Select **Edit** at the top of the list.



> **Note**
>
> If you don't see **Edit**, you don't have permission to change the Featured links list. Contact your administrator.

2. Select **X**.



3. Select **Delete** in the confirmation dialog.

4. To leave edit mode, select **Done** when you're finished.

> **Note**
>
> If you had custom promoted sites in classic view of the SharePoint Sites page, the Featured links section of the SharePoint start page is pre-populated with those sites. The pre-population of promoted sites in the Featured links list happens only once when the first user

visits the new SharePoint start page. If you go back to classic view and change the promoted sites, the changes will not be reflected in the Featured links list on the SharePoint start page.

Last updated on 06/24/2026

Roll out SharePoint and OneDrive

Article • 02/21/2023

Be sure you've reviewed these SharePoint and OneDrive deployment resources before you start your rollout.

- Plan for SharePoint and OneDrive in Microsoft 365
- Identify business requirements for SharePoint and OneDrive
- Create a compliant SharePoint and OneDrive environment
- Plan sharing and collaboration options in SharePoint and OneDrive
- Plan file sync for SharePoint and OneDrive in Microsoft 365
- Training and change management for rolling out SharePoint and OneDrive

Also, make sure your migration plans are in place as you roll out.

We highly recommend rolling SharePoint and OneDrive out to a pilot group before rolling them out to your entire organization. A pilot program can help you test your business processes and determine if there's further change management or training needed to help your users succeed with SharePoint and OneDrive.

Pilot rollout of SharePoint and OneDrive

We recommend that you start with a small pilot and then increase in scope and speed of rollout as you review feedback from the pilot group and make changes where needed.

For each phase of the pilot, you'll need to train the users in your pilot group, and then give them access to SharePoint and OneDrive. This may include migrating content for them (or allowing them to do so themselves) or setting up SharePoint Server hybrid.

Create success criteria so you'll know when it's time to expand the pilot and when to roll out SharePoint and OneDrive more broadly.

Be sure there's a process to collect information from pilot users and allow them to report issues. If your help desk or support personnel are involved in the pilot process, they may be able to manage this with existing processes.

Do a small initial pilot

For the initial pilot phase, consider the following:

- Depending on how technical your users are, you may want to do the initial pilot with highly technical users, such as people in your IT department.

- Exclude users who need to interact with your customers regularly. Pilot users will be using new processes for the first time. To give your customers the best service, you may want to leave customer-facing people out of the initial pilot.

Use this initial pilot phase to validate some core business processes and workflows and to train your support or help desk personnel.

Expand the pilot

Once the initial pilot users are successfully using SharePoint and OneDrive, extend the pilot to a wider variety of users. We recommend that you create a group of knowledgeable stakeholders across departments and disciplines to specifically test the core use cases you've identified for SharePoint and OneDrive.

Monitor the pilot as it proceeds. When the people involved are able to easily accomplish the expected tasks, consider rolling the pilot out to a larger group.

Once the people in your pilot group are able to validate the expected use cases and the number of issues reported is low, consider scheduling the remaining rollout for the rest of the organization.

Rolling out SharePoint and OneDrive broadly

Once your pilot program has concluded successfully, you can roll SharePoint and OneDrive out to the rest of your organization.

Feedback

Was this page helpful? Yes No

Provide product feedback

Set up SharePoint and OneDrive in Microsoft 365 with a step-by-step guide

Article • 06/26/2023

The Microsoft SharePoint setup guide is a step-by-step guide in the Microsoft 365 admin center that provides instructions for setting up and configuring SharePoint to meet specific organizational needs. The setup guide incorporates Microsoft's best practices for SharePoint and recommendations on how to optimize SharePoint for performance, security, and user experience.

The setup guide covers a wide range of topics related to SharePoint, including:

- Site creation and document libraries
- Managing user permissions and search/share settings
- Workflow setup
- Data migration
- App protection policies to protect company data on mobile devices
- Data loss prevention (DLP) capabilities to protect sensitive information
- Information rights management (IRM) to encrypt and assign usage restrictions on files
- Microsoft 365 network connectivity test to see results related to SharePoint

You must be a Microsoft 365 global administrator to run the setup guide.

Run the SharePoint setup guide

Related topics

Plan for SharePoint and OneDrive in Microsoft 365

Roll out SharePoint and OneDrive

Feedback

Was this page helpful? Yes No

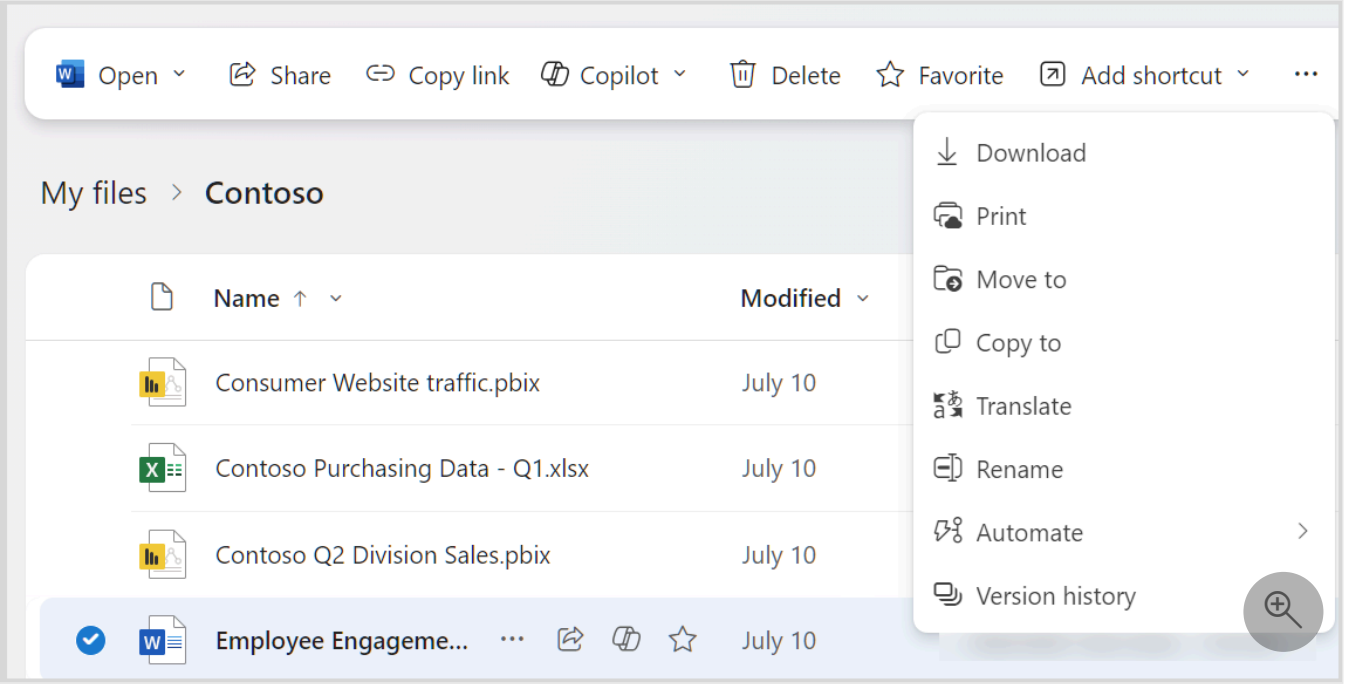
Provide product feedback

Translate documents in OneDrive

08/05/2025

> **Note**
>
> Through December 2025, you can try out document translation and other selected services at no cost if you have pay-as-you-go billing set up.
>
> For details on how to get started and the limitations, see Try out pay-as-you-go services.

OneDrive, with the document translation service, allows you to manually translate documents while preserving the original format and structure. With this feature, you can create a translated copy of a single file or a set of files. The translation feature is available for all supported languages and dialects, and supports up to 10 languages per translation request.



Key features

- **Multiple points of access**: OneDrive document translation can be accessed via **My files** in OneDrive or using the viewer after opening the document. If you want to access the document translation feature for SharePoint Online libraries, you can also access that feature through OneDrive's **Quick access** section. For more information about document translation for SharePoint Online, see Overview of document translation.
- **Request multiple languages per translation**: You can select up to 10 languages per document translation.

- **Translation of different file types**: Translate various file types. Supported file types include .docx, .pdf, .pptx, and more.
- **Video transcripts and captions**: The translation feature also supports translating video transcripts and closed caption files. For more information, see Transcript translations in Stream for SharePoint.

Prerequisites

To enable document translation for your tenant, you must:

- Link an Azure subscription to pay-as-you-go billing.
- Be a SharePoint Administrator or have credentials to access the Microsoft 365 admin center.

Enable document translation for your tenant

> **Note**
>
> Once an Azure subscription is linked to pay-as-you-go billing, the translation feature is automatically set up and turned on for all SharePoint and OneDrive sites.

Manage document translation for OneDrive

Even though OneDrive document translation is enabled by default, you can also turn off the feature.

To disable document translation for OneDrive:

1. Sign in to the Microsoft 365 admin center and select **Setup**.
2. Expand **Files and content** and select **Automate content processes with Syntex**.
3. On the **Automate content processes with Syntex** page, select **Go to Syntex settings**.
4. On the Syntex page, in the **Document & image services** section, select **Document translation**.
5. In the OneDrive section, select **Edit**. On the **Where can document translation be used?** panel, clear the **Available in OneDrive** checkbox.

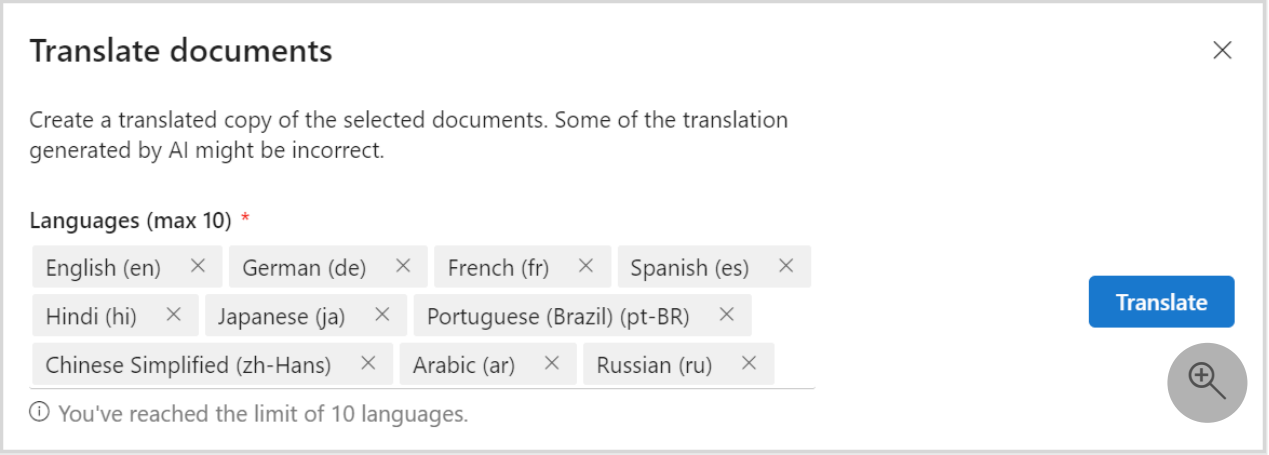
For more information about managing document translation for SharePoint sites, see Set up and manage document translation.

Translate a document

Sign in to OneDrive with your Microsoft account credentials.

1. Select **My files**.
2. Select the file you want to translate and select the **More commands (...)** button in the ribbon.

   Alternatively, you can get to this feature by selecting **More Actions (...)** beside the file name or opening the document in the viewer.
3. Select **Translate**.
4. Choose up to 10 languages and select **Translate**.



The translated file is saved in the same location as the file you selected to translate.

> **Note**
>
> It might take up to several hours to generate the translated files.

Requirements and limitations

Supported file types

Document translation is available for the following file types:

- `.csv`, `.docx`, `.htm`, `.html`, `.markdown`, `.md`, `.msg`, `.pdf`, `.pptx`, `.txt`, `.xlsx`

For legacy file formats, the translated copy is created in the modern equivalent:

- `.doc` → `.docx`
- `.xls` → `.xlsx`
- `.ppt` → `.pptx`

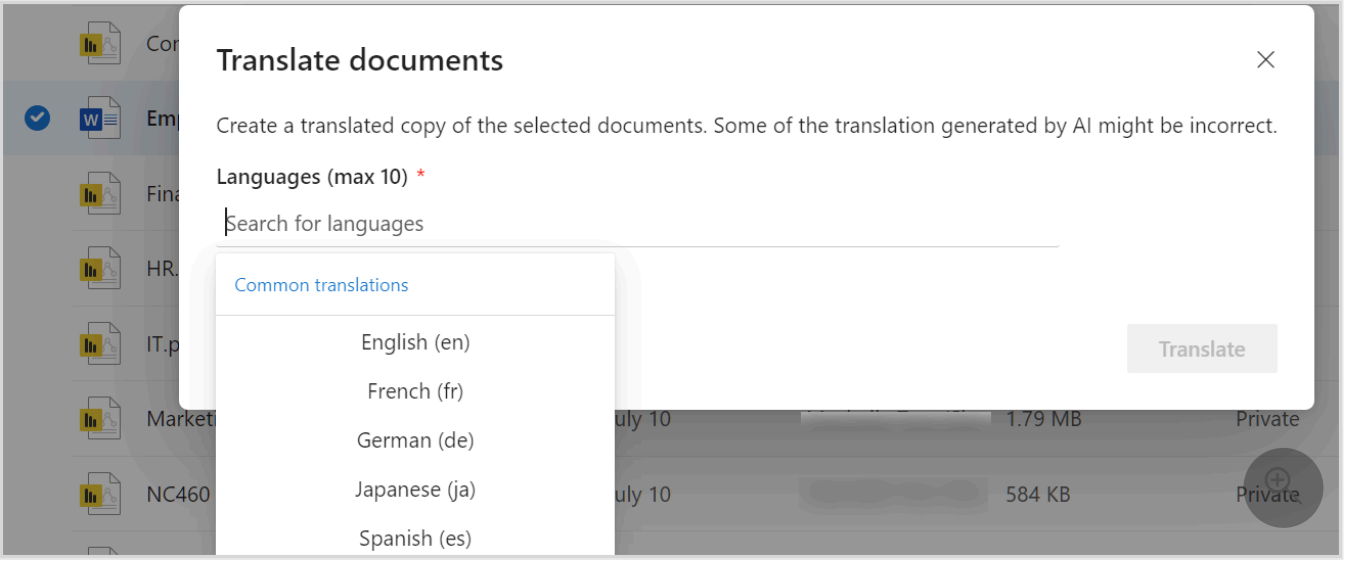
> **Note**
>
> SharePoint site pages aren't supported for translation at this time.

Supported file size

The maximum file size for translation is 40 MB.

Supported languages

Translation for the service is available for all supported languages and dialects.



Current limitations

- **Images**: Text embedded in images within documents isn't translated.
- **Encrypted files**: Encrypted files can't be translated.
- **Password-protected files**: Password-protected files aren't eligible for translation.

Frequently asked questions

For more information, see the following resources:

- Document Translation: FAQ
- How does Translator count characters?

Related topics

- Overview of document translation
- Set up and manage document translation
- Translate a document
- Configure pay-as-you-go billing

Copilot skills in the SharePoint admin center

Copilot in the SharePoint admin center uses generative AI to make you more productive by simplifying administration of SharePoint and OneDrive. It helps you focus on more strategic priorities. Copilot skills in the SharePoint admin center provide natural language interactions, contextual guidance, and proactive suggestions.

You can use Copilot to help manage your organization and focus on what's important. Try using the prepopulated prompt options in the Copilot pane for the best results. Or, try using Voice input controls to dictate your question.

The following sections describe what you can do with Copilot in the SharePoint admin center.

> **Note**
>
> To maintain your security and privacy, Copilot doesn't make any configuration changes on your behalf.

Prerequisites

You must have a Microsoft 365 subscription that includes SharePoint and a license for Microsoft 365 Copilot (see License options for Microsoft 365 Copilot).

For more information, see Prerequisites for SharePoint Advanced Management.

Get started with Copilot in the SharePoint admin center

To use Copilot in the SharePoint admin center, follow these steps:

1. Sign in to the SharePoint admin center.
2. Select the **Copilot** button in the upper right shell to launch Copilot in the SharePoint admin center.

Get step-by-step guidance with Copilot

Copilot can walk you through the exact steps required to complete common admin tasks. For example, you can ask questions like "How can I find sites that are potentially over-permissioned?"

Copilot recommends clear, sequential instructions to guide you from start to finish. It first runs the site permissions report for your organization, then runs activity-based reports, and finally initiates site access reviews for site owners to review and remediate their sites.

How can I find sites that are potentially over-permissioned?

Copilot AI-generated content may be incorrect

To find sites that are potentially over-permissioned in SharePoint or Microsoft 365, you can use the following approach:

1. **Run the "site permissions for the organization" report** in the SharePoint Admin Center:
   - This report scans all SharePoint and OneDrive sites and shows how many users have access to each site, including details about content shared with all users, guest access, and broad sharing links.
   - The report highlights the top 100 sites with the highest number of users, making them priority candidates for review.
   - You can download the report as a CSV for offline analysis.
2. **Use activity-based reports** to monitor ongoing sharing:
   - These reports help you track sharing activities, especially where content is shared with "Everyone Except External Users," "People in your organization," or "Anyone"—all indicators of potential oversharing.
   - You can sort, filter, or download these reports to identify and prioritize sites for further review.
   - The "Get AI insights" feature can provide recommendations and flag overshared sites.
3. **Review and remediate**:
   - Once you've identified sites with potential over-permissioning, initiate a Site Access Review for site owners to confirm and remediate oversharing as needed.

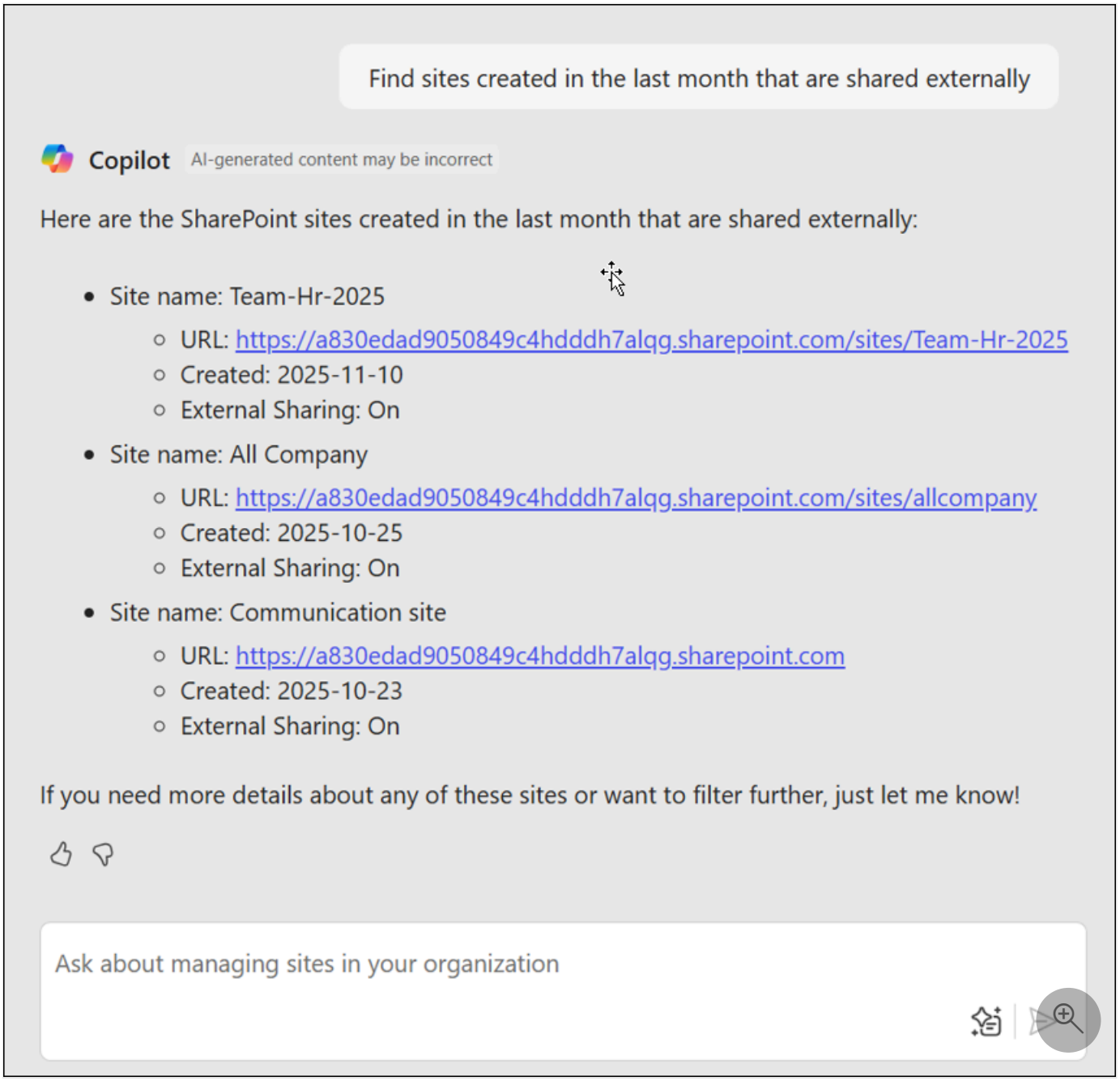
Would you like step-by-step guidance on running these reports, or help interpreting the results?

Ask about managing sites in your organization

Multi-criteria site search

Copilot can help you find sites by querying on multiple conditions at once. For example, you can type a query like "Find sites created in the last month that are shared externally."

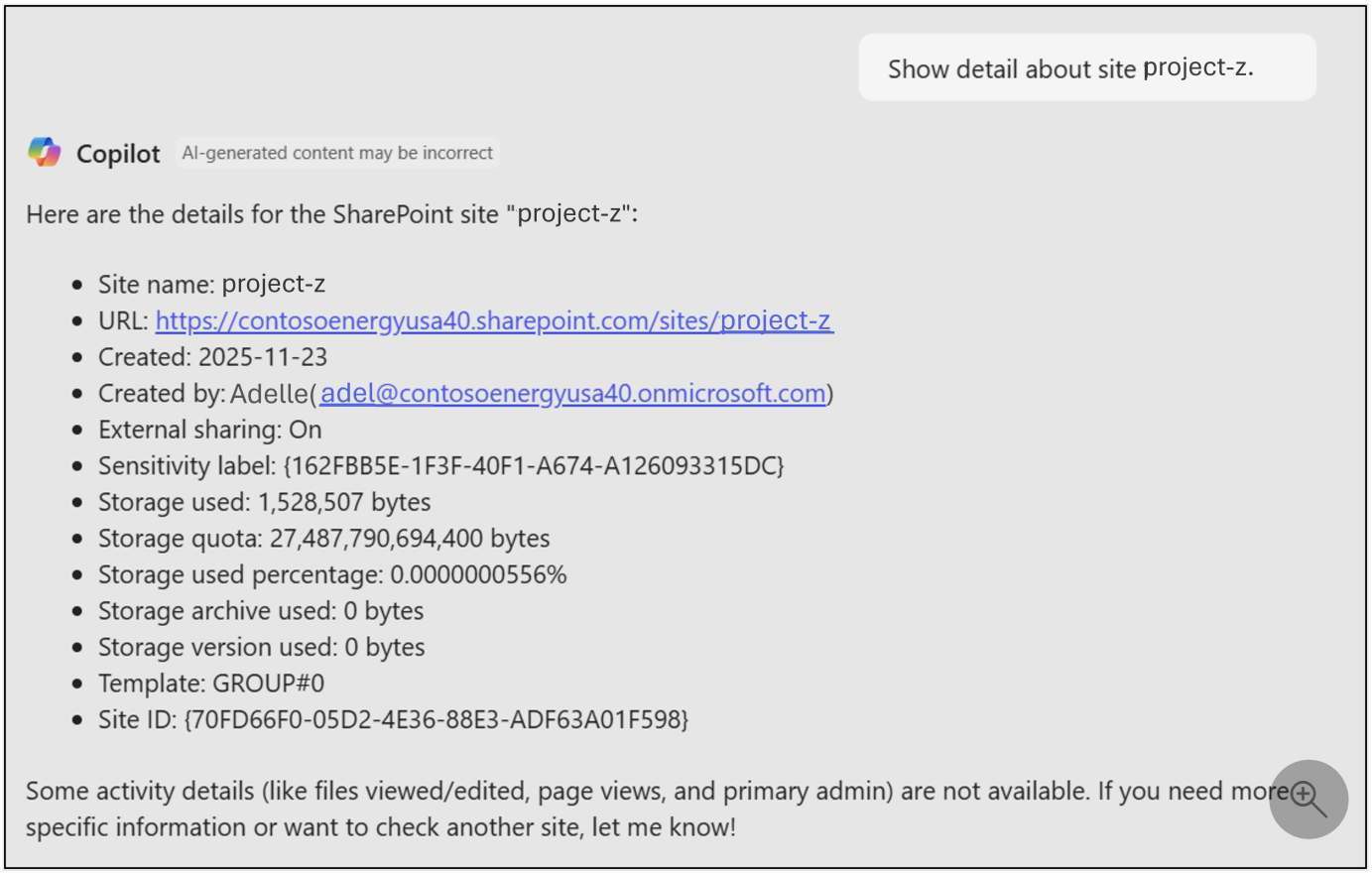
Copilot generates a filtered list of sites based on your criteria. In this case, the list includes sites that were created last month and that are shared externally. You can then ask for more details or apply more filters to refine your results.



Getting details about a specific site

You can ask Copilot to show you details about a specific site right in the chat. For example, you can type a query like "Show details about the site `site_name`."

Copilot returns details about the specific site, including site name, URL, creation date, creator, external sharing status, sensitivity labels, storage status, template, and site ID.

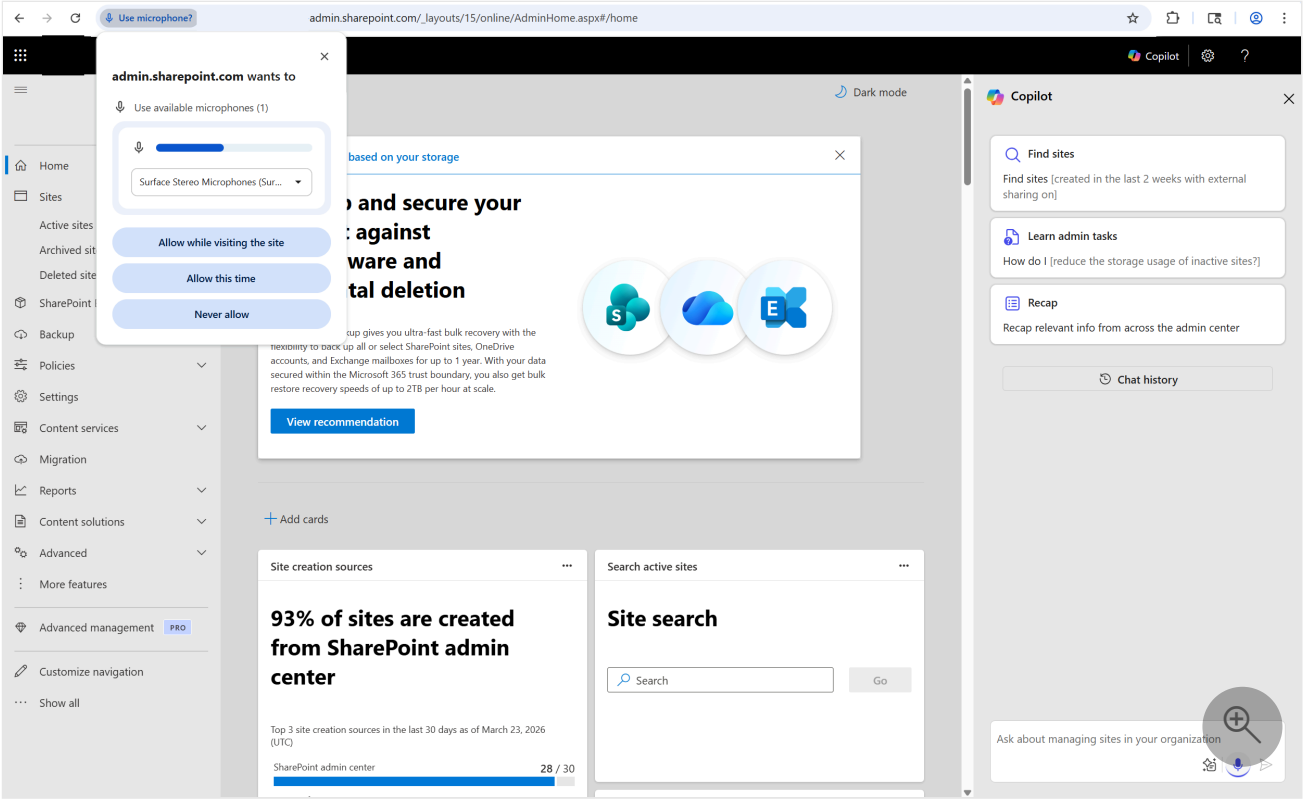


Voice input controls for Copilot in the SharePoint admin center

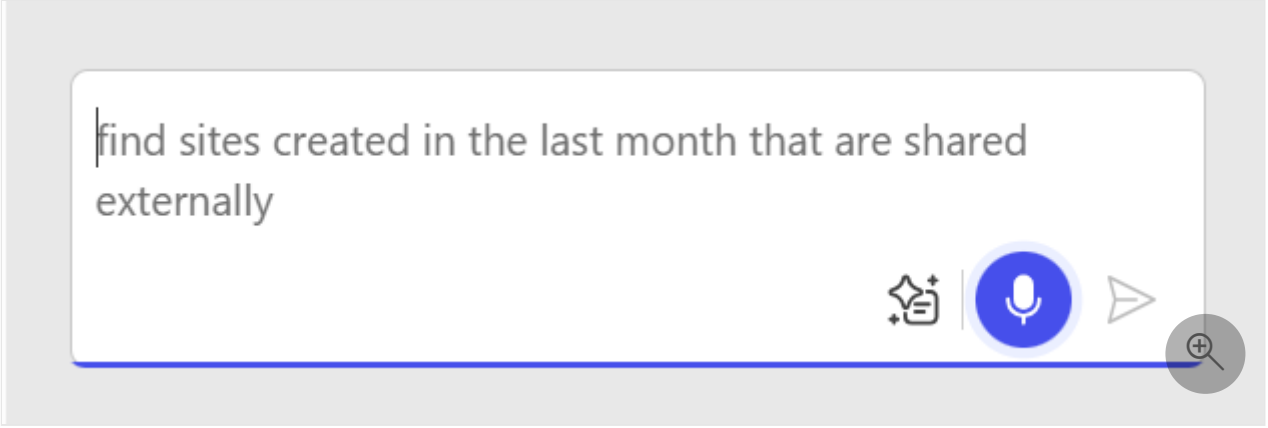
Voice input enables you to dictate queries into Copilot, improving accessibility and ease of use. When you use voice input with Copilot, the transcribed text appears in the Copilot chat box in real time, where you can review and edit it before submitting to Copilot.

How to use the voice input feature

1. In the SharePoint admin center, with Copilot open, select the microphone in your chat window. The first time, you're prompted to grant permission in your browser window.



2. With the microphone on, speak your query and see the transcription in the Copilot chat experience. You can modify the text during and after audio capture, and then submit your query when you're ready.



Copilot automatically stops transcribing if no audio is detected.

Frequently asked questions

How do I enable Copilot in the SharePoint admin center?

Copilot is automatically enabled for customers whose subscriptions include SharePoint and Microsoft 365 Copilot.

How do I disable Copilot in the SharePoint admin center?

To disable Copilot in the SharePoint admin center, set up a custom security group called `CopilotForM365AdminExclude`, and then add the administrators you don't want to have the Copilot experience. Once the group is configured, the Copilot experience is automatically disabled for those users.

Which admin roles can use Copilot in the SharePoint admin center?

The feature is available to SharePoint administrators. Copilot in the SharePoint admin center respects role-based access controls and only shows information and controls that the user has access to. Copilot doesn't make any configuration changes on your behalf.

Does Copilot in the SharePoint admin center support audit logging?

Yes. Copilot in the SharePoint admin center aligns with Microsoft's commitment to providing enterprise-grade compliance capabilities for all Copilot products. These capabilities include features such as auditing, eDiscovery, legal hold, and data retention controls.

How much does Copilot in the SharePoint admin center cost?

This feature is included with a Microsoft 365 Copilot license. When you purchase and assign Microsoft 365 Copilot licenses for your tenant, admin users who have a Copilot license can use Copilot in the SharePoint admin center.

Last updated on 06/25/2026

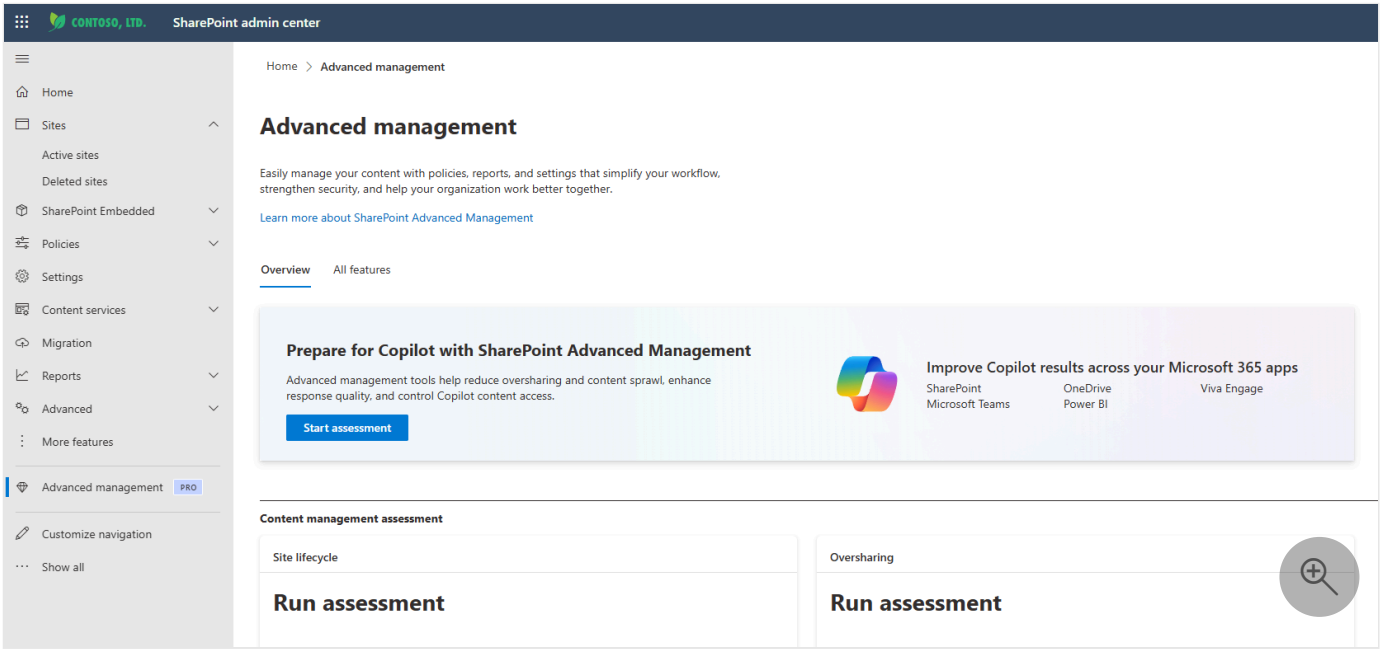
Get ready for Microsoft 365 Copilot and agents with SharePoint Advanced Management

Microsoft 365 Copilot and agents work best for your organization when your content is up to date and well governed. Copilot and agents retrieve data from Microsoft Graph and respect existing permissions, sharing settings, and policies.

This article describes how to prepare your environment for Copilot and agent usage by using capabilities in SharePoint Advanced Management.

Step 1: Use Content Management Assessment

The Content Management Assessment hub provides administrators with actionable insights and recommendations. It runs a suite of essential reports that surface key findings and categorize sites that might require attention.



The Content Management Assessment provides a simple, guided process for administrators to:

- Identify potentially overshared content
- Find issues or risks (such as inactive or ownerless sites)
- Define Copilot readiness for the organization
- Ensure compliance and maintain data integrity

- Receive actionable recommendations for remediation
- Track progress over time with recurring assessments

This hub helps make content governance accessible and actionable, even for administrators who might not have deep technical expertise yet.

Access the Content Management Assessment hub

1. In the SharePoint admin center, in the navigation pane, select **Advanced Management**.

2. Select **Start assessment**.

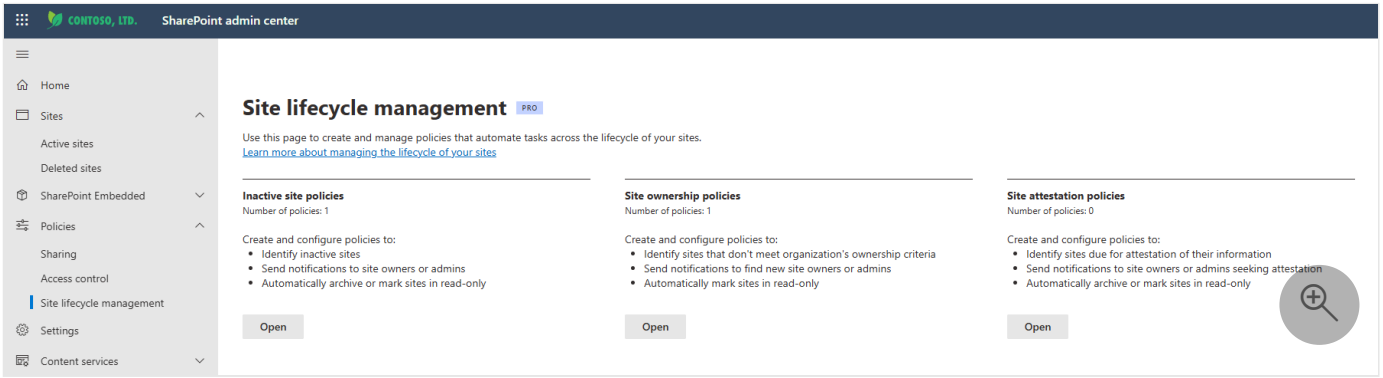
After the assessment runs, review the findings, and take appropriate actions. Rerun the assessment every 30 days to track your progress and address any new issues.

Step 2: Employ site lifecycle management and archiving

Site lifecycle management policies and archiving help ensure that your sites are up to date, compliant, and use storage efficiently. These capabilities help ensure Copilot and agentic experiences reference current content and can reduce storage costs.

Site lifecycle management

Site lifecycle management policies help reduce content sprawl by automating the process of ensuring that your organization's SharePoint sites are well governed.



When you set up your site lifecycle management policies, the system automatically identifies potential problems. You can configure enforcement actions and email notifications that ask site owners or administrators to take action.

View or create site lifecycle management policies

1. In the SharePoint admin center, in the navigation pane, select **Site lifecycle management**.

2. Under a category, such as **Inactive site policies**, **Site ownership policies**, or **Site attestation policies**, select **Open**.

Site lifecycle management policies

Site lifecycle management policies include the following:

- Site ownership policies that support effective site management and reduce the risk of ownerless sites. You can set minimum owner or administrator counts and automate notifications when sites don't meet the criteria.
- Inactive site policies that automatically detect inactive sites and notify site owners by email.
- Site attestation policies that ask site owners or site administrators to check and confirm the accuracy of site information, including site necessity, owners, members, permissions, and sharing settings.

Microsoft 365 Archive

Use Microsoft 365 Archive to retain inactive content, such as ownerless or inactive sites. This approach helps reduce your storage consumption and improves Copilot optimization. When you archive a site:

- The site moves to a Microsoft 365 Archive storage tier.
- The site no longer consumes active SharePoint storage quota.
- Content, permissions, and metadata are preserved.
- Users can't access the site until it's reactivated.
- Copilot isn't trained on archived content.

You can manage archived sites on the **Archived sites** page.

Set up and use Microsoft 365 Archive

See the following resources:

- Set up Microsoft 365 Archive
- Manage Microsoft 365 Archive
- End-user experience in Microsoft 365 Archive

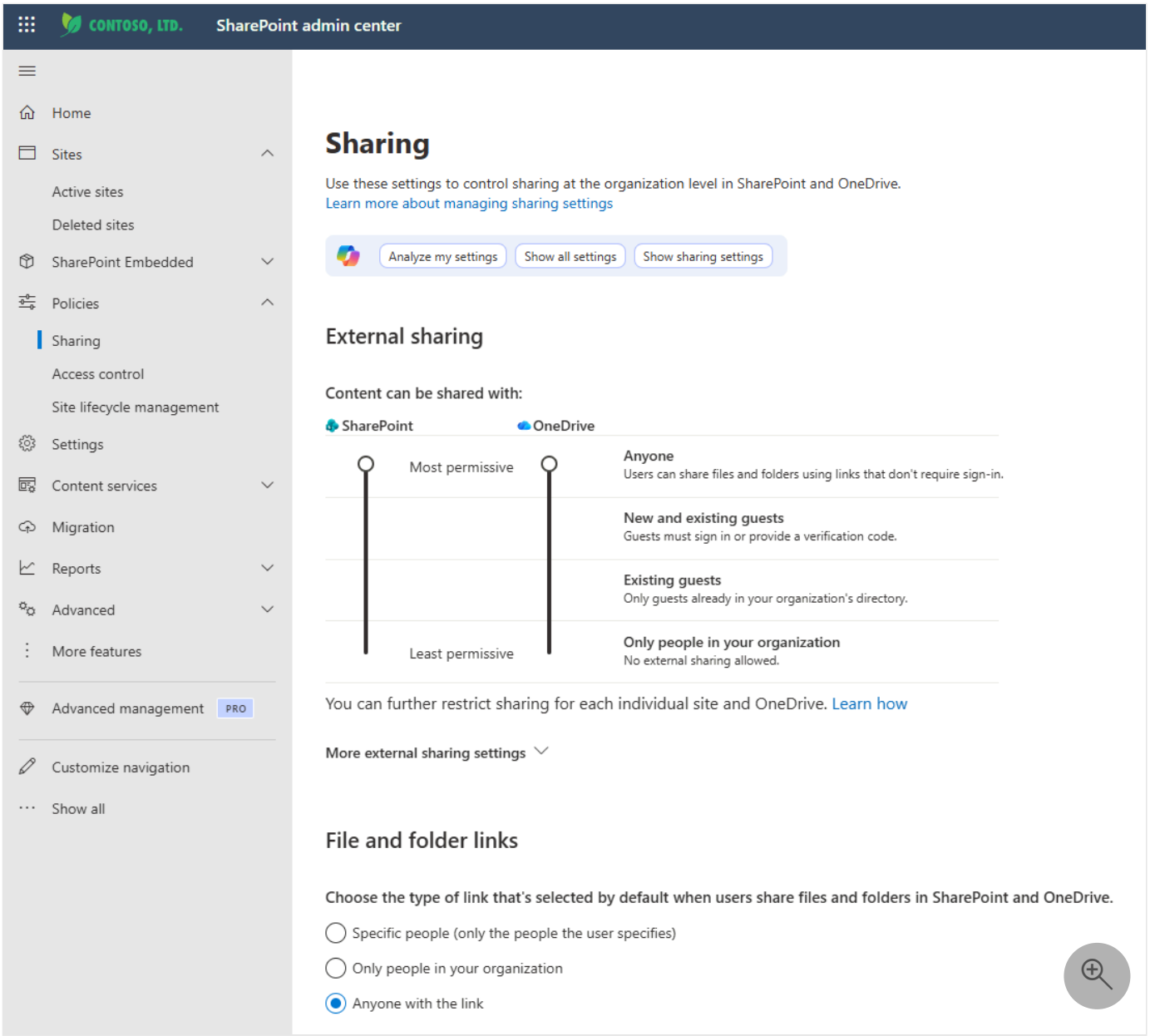
Step 3: Prevent accidental oversharing

To help prevent accidental oversharing in Copilot and agentic experiences, adjust sharing settings for SharePoint and OneDrive. Use data access governance reports and insights to identify and

prioritize oversharing risks. Restrict access to sensitive content.

Adjust sharing settings for SharePoint and OneDrive

By default, SharePoint sets sharing settings to the most permissive option. You can set sharing settings for SharePoint, OneDrive, and links to files or folders.



You can also specify expiration and permission options for links.

Adjust sharing settings

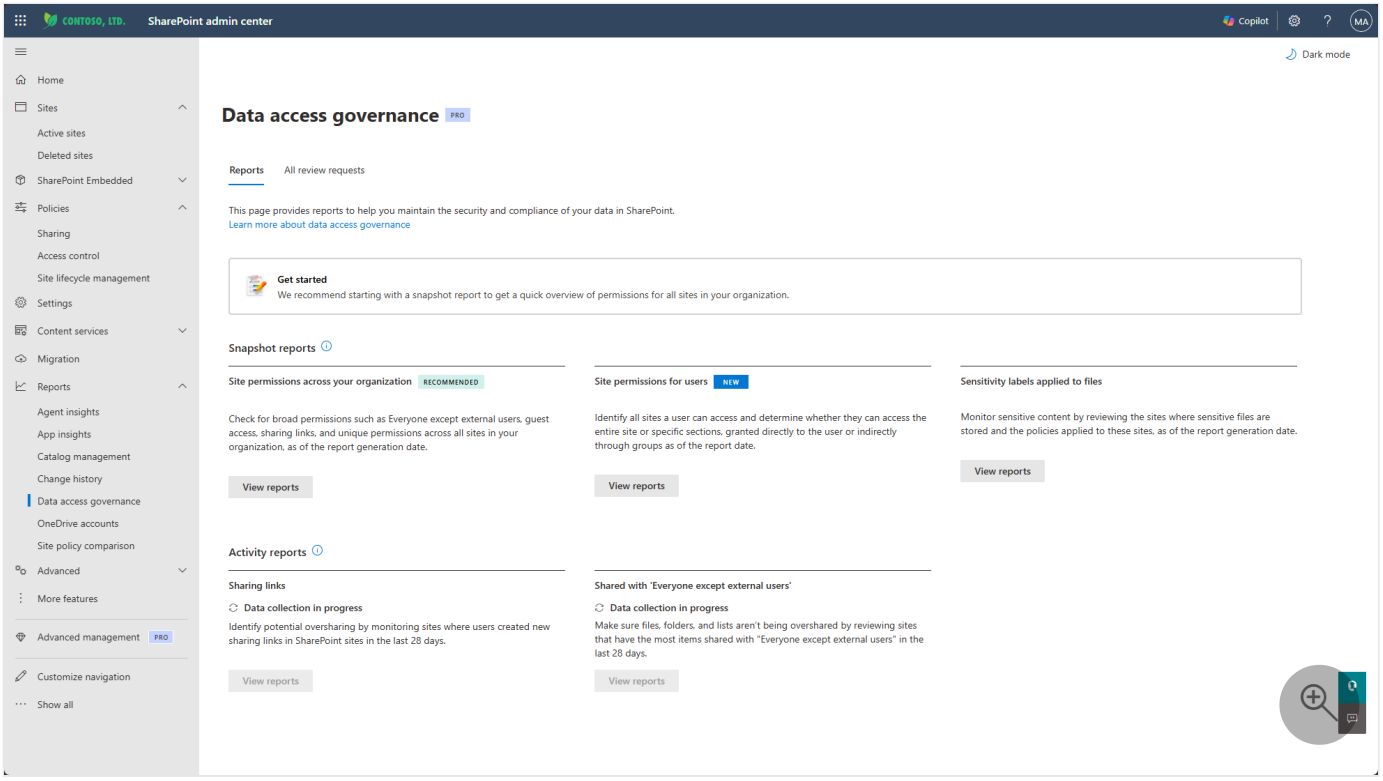
1. In the SharePoint admin center, in the navigation pane, expand **Policies**, and then select **Sharing**.

2. Starting at the top, specify your settings, and then select **Save**.

To get help with this task, see Manage sharing settings for SharePoint and OneDrive.

Use data access governance reports to identify oversharing risks

Data access governance reports help you identify sites that contain potentially overshared or sensitive content.



Several reports are available, including snapshot reports and activity reports.

Access data access governance reports

1. In the SharePoint admin center, expand **Reports**, and then select **Data access governance**.
2. Under a category, select **View reports**.

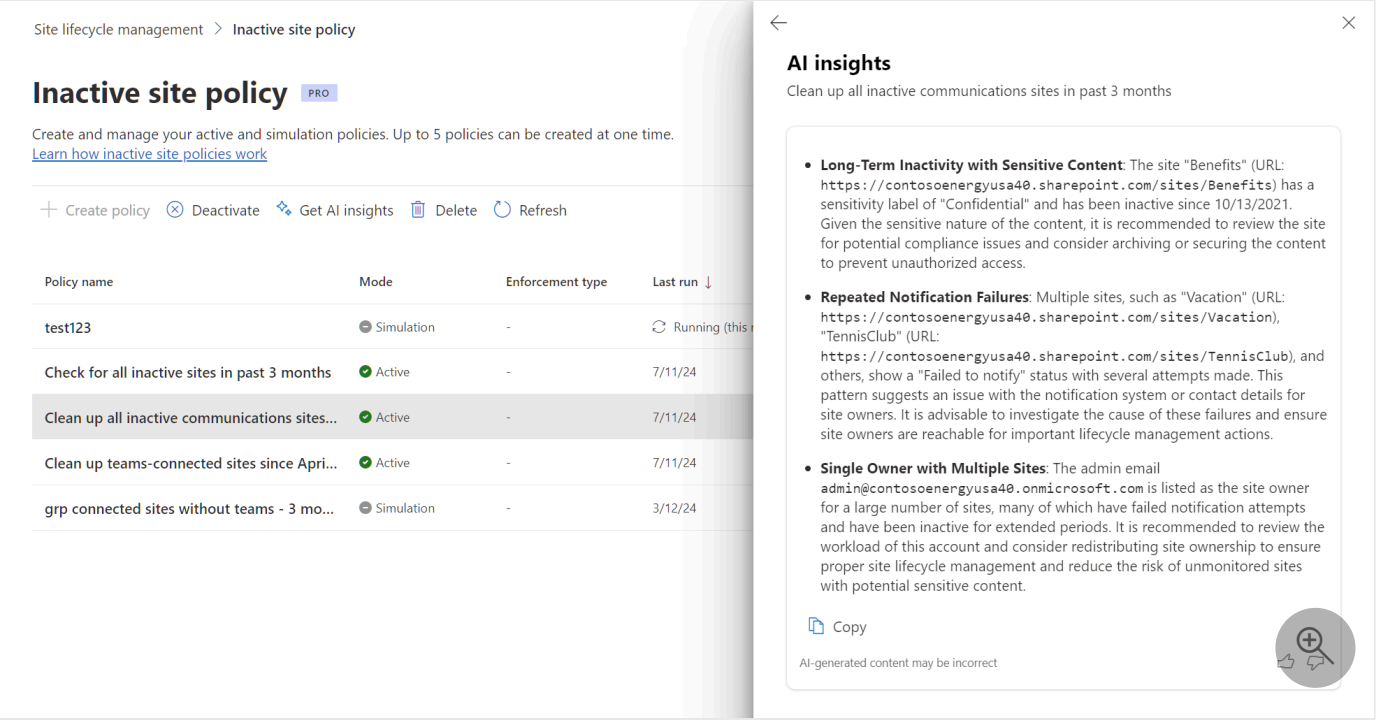
Start with these reports

- The site permissions baseline report helps you understand your organization's overall access exposure. This report provides you with a snapshot that shows your current permission structure across SharePoint and OneDrive sites, and enables you to identify sites that need immediate attention.
- The site permissions for users report lists all the sites a given user can access so you can determine whether permissions need to be adjusted.
- Activity-based reports:

- The Everyone except external users (EEEU) report helps you identify the top 100 sites where content was shared with your entire organization in the past 28 days, and security policies applied to those sites.
- The sharing links activity reports help you identify sites where users created the most sharing links within the last 28 days. You can see a list of sites with the highest number of "Anyone" links, "People in the organization" links, and "Specific people" links.

Use AI insights to interpret report findings

The AI insights feature reduces the manual effort required to review reports and helps mitigate content governance problems. It uses a language model to identify patterns and potential problems from reporting and provides actionable recommendations to solve problems.



Where available, use AI-generated insights to help interpret report findings and identify recommended actions.

The AI insights feature is available for these reports:

- Sharing links activity reports
- Sensitivity label snapshot report
- Inactive site policy, which helps identify inactive sites. After the policy runs, you can download a report in CSV format.
- Change history reports which show site actions or organization setting changes made within the last 180 days

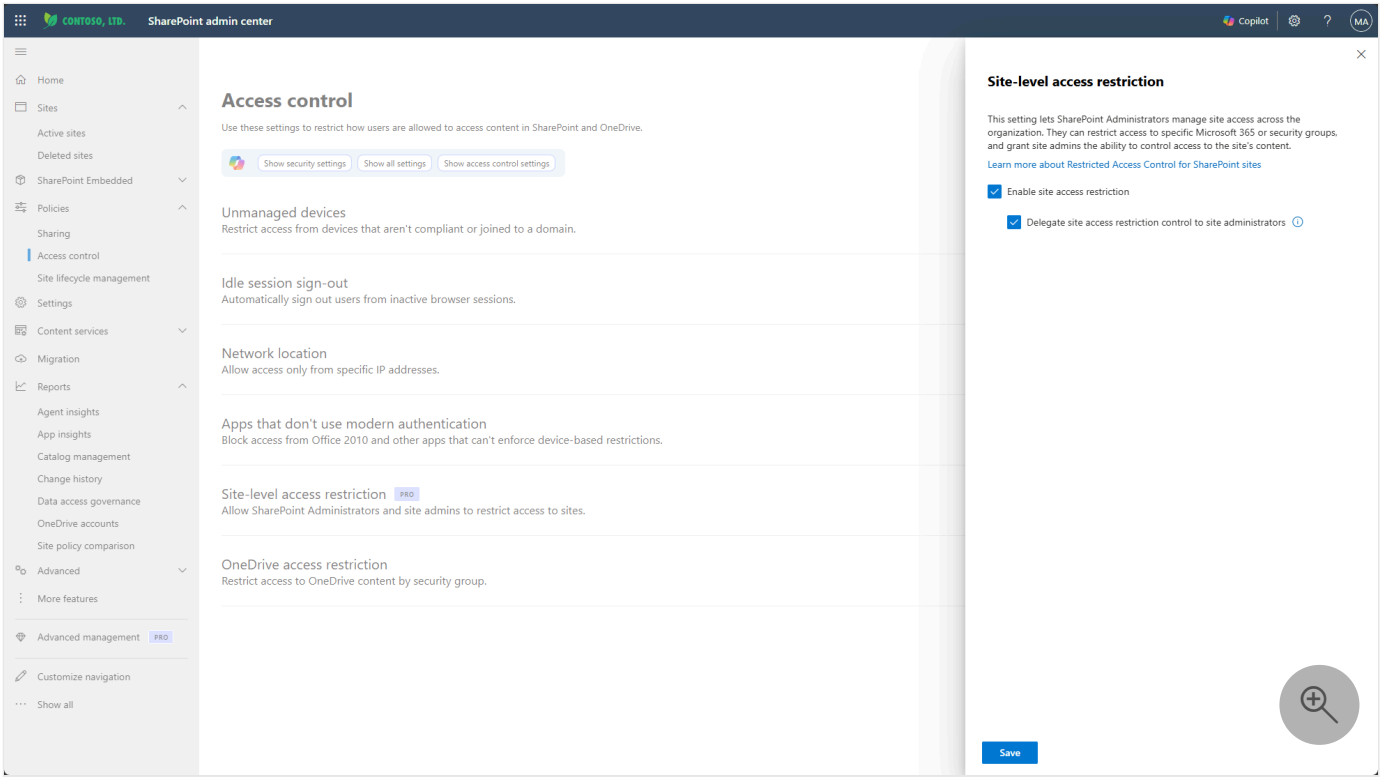
Generate AI insights

1. In the SharePoint admin center, in the navigation pane, expand **Reports**, and select an option, such as **Data access governance** or **Change history**.

2. Select a report, look for the **Get AI insights** button, and then select it to generate AI insights.

Restrict access to sensitive content

If necessary, restrict site access by using Restricted Access Control to help prevent oversharing. By using Restricted Access Control, you grant access to SharePoint sites by using groups, such as Microsoft Entra security groups or Microsoft 365 groups. Users who aren't part of the specified group can't access the site or its contents, even if they had prior access through permissions or a link.



Use your Restricted Access Control policy to:

- Limit site access to a defined group of users
- Prevent broad or unintended access
- Ensure that only authorized users can access content and see it in Copilot

Restrict site access

1. Set up or identify a security group in Microsoft Entra or a Microsoft 365 group (see Microsoft Entra: Group types).

2. In the SharePoint admin center, in the navigation pane, expand **Policies**, and then select **Access control**.

3. Select the **Enable site access restriction** option.

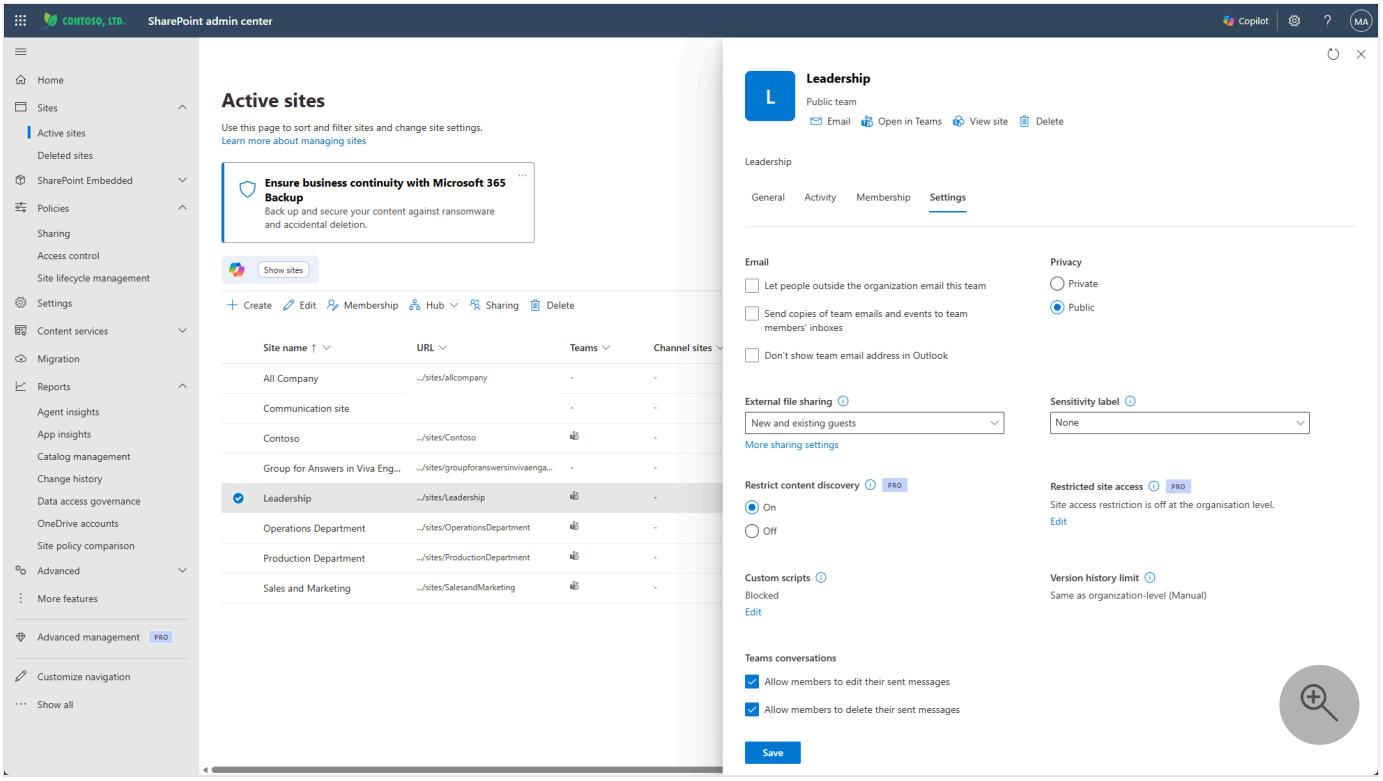
   To enable site administrators to control who can access their sites, select **Delegate site access restriction control to site administrators**.

4. Select **Save**.

For more information, see Restrict access to a SharePoint site.

Control content discovery of high-risk sites

If you have high-risk sites that you want to prevent accidental discovery in Copilot or agentic experiences, use Restricted Content Discovery for those sites.



Restricted Content Discovery helps to:

- Prevent content from appearing in Copilot or agentic experiences and in organization-wide search queries
- Reduce accidental exposure while leaving site permissions unchanged

Restricted Content Discovery is useful for content that must remain accessible, but shouldn't be broadly discoverable.

Identify high-risk sites

1. Use your tools and reports, such as the SharePoint Admin Agent and data access governance reports, to see these risk signals:

   - Broad sharing through "Anyone," "Everyone," and organization-wide links
   - Large audiences with excessive permissions
   - Broken permission inheritance and complex access models
   - Sensitive content with weak protection
   - Unlabeled or public sites
   - Governance gaps with ownerless, inactive, or unreviewed sites

   Sites where multiple risk signals overlap are considered high risk. Examples include:

   - Sites that contain sensitive data and that have "Anyone" sharing links
   - Public sites with no owner
   - Large audiences with broken permission inheritance

2. Use SharePoint Advanced Management tools and reports to highlight sites with oversharing or exposure risk.

   - Data access governance reports, such as site permissions reports and sharing link activity reports
   - AI insights
   - SharePoint Admin Agent

3. Create a list of high-risk sites that you want to restrict from content discovery.

Restrict content discovery

1. In the SharePoint admin center, expand **Sites**, and then select **Active sites**.

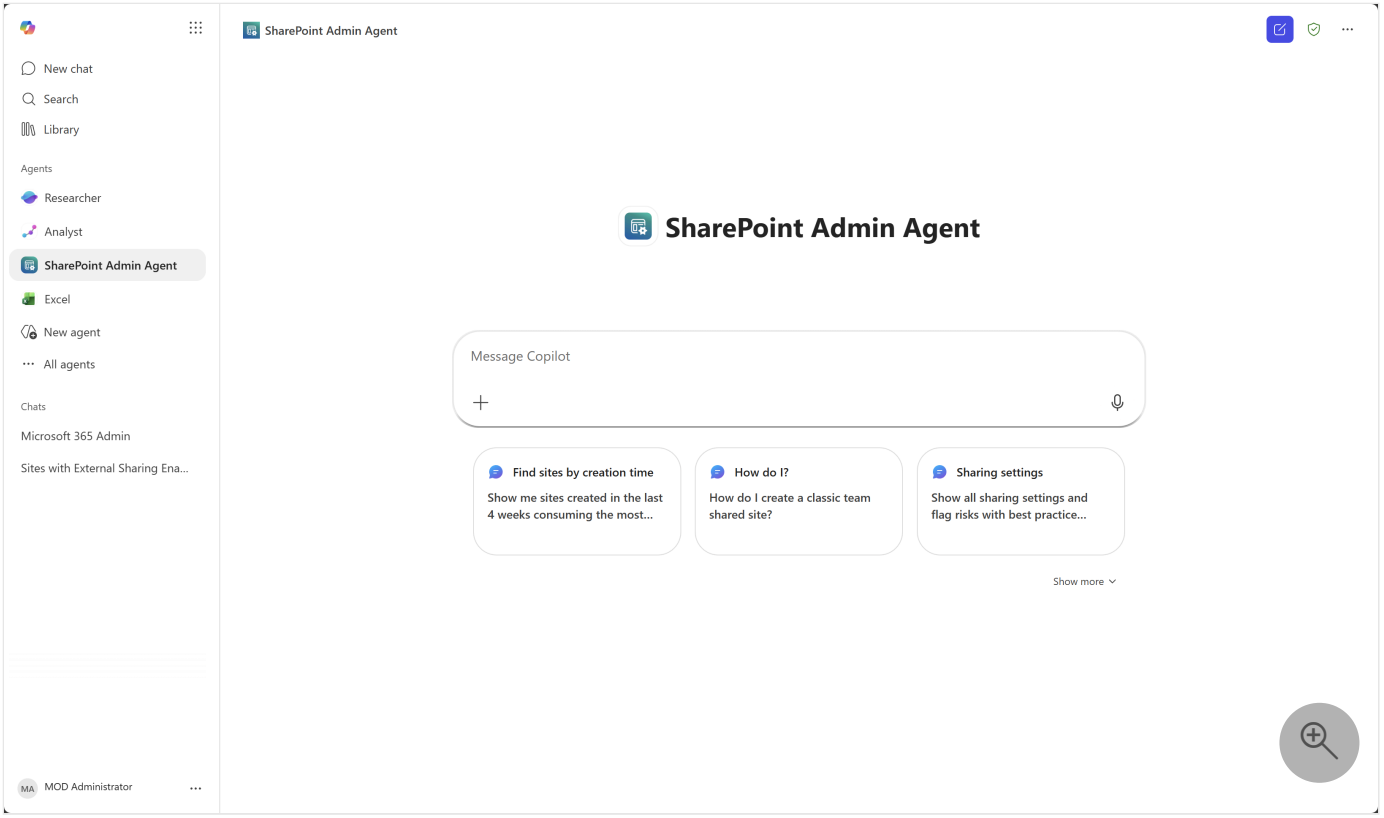
2. Select a site to open its flyout. On the flyout, select the **Settings** tab.

3. Under **Restrict content discovery**, select **On**. Then select **Save**.

For more information, see Restrict discovery of SharePoint sites and content.

Step 4: Use the SharePoint Admin Agent

The SharePoint Admin Agent responds to your questions by gathering the relevant data and reports, offering analysis and recommendations, and suggesting other prompts. Ask a question, such as "Show me how my content is distributed across my tenant," and get useful information with suggested prompts and next steps.



Open the SharePoint Admin Agent

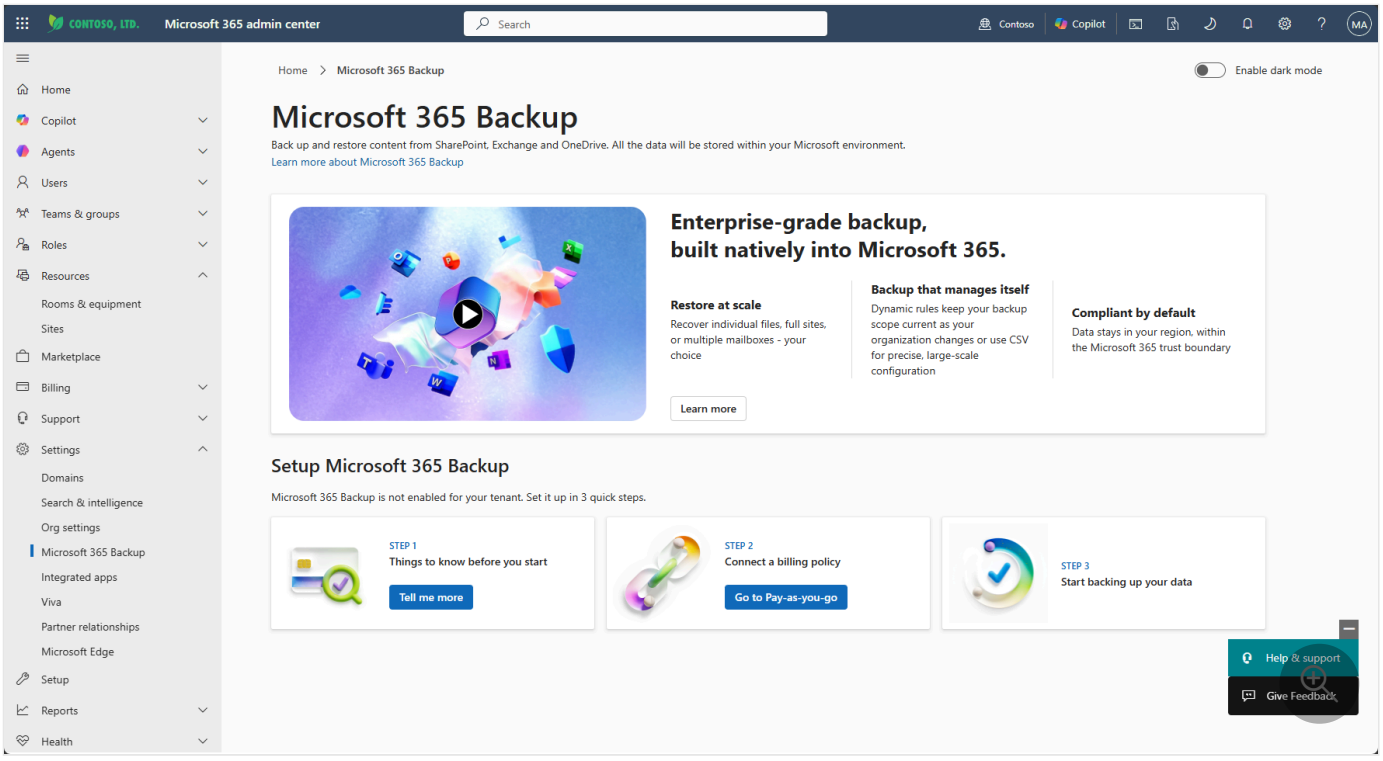
Take one of the following steps:

- In the Microsoft 365 Copilot app, expand **Agents**, and search for *SharePoint Admin Agent*.
- In the SharePoint admin center, select the **Copilot** button, and then select the **View prompts** button in the lower corner of the Copilot pane.
- In Microsoft Teams, select **Apps**, and then search for *SharePoint Admin Agent*.

For more information, see SharePoint Admin Agent.

Step 5: Implement backup and restore procedures

Business continuity requires a backup and restore solution, such as Microsoft 365 Backup. In the event of an accidental or malicious data deletion or overwriting, it's important for your data to be protected and easily recoverable.



With Microsoft 365 Backup:

- Data never leaves the Microsoft 365 data trust boundary and honors the geographic locations of your current data residency.
- Backups are immutable unless the backup tool administrator expressly deletes them.
- OneDrive, SharePoint, and Exchange have multiple physically redundant copies of your data to mitigate the impact of physical disasters.

Get started with Microsoft 365 Backup

1. In the Microsoft 365 admin center, in the navigation pane, expand **Settings**, and then select **Microsoft 365 Backup**.

2. Review the information on the page to learn more and get started.

To learn more about Microsoft 365 Backup, see the following resources:

- Overview of Microsoft 365 Backup
- Set up Microsoft 365 Backup
- Create, view, and edit backup policies in Microsoft 365 Backup
- Restore data in Microsoft 365 Backup

ⓘ**Note:** The author created this article with assistance from AI. Learn more

---

Last updated on 07/16/2026

SharePoint authoritative sites in Copilot Search

Authoritative sites help administrators identify official, organization-managed SharePoint sources. When you mark a site as authoritative, Copilot Search experiences recognize its content as trusted.

For users, this recognition improves confidence in search results. Visual signals, such as the **From your organization** label, make trusted items easier to identify.

> **Important**
>
> In the current release, configure authoritative sites through PowerShell and CSOM APIs. The configuration supports site-level designation but doesn't support personal sites.

Prerequisites

See Prerequisites for SharePoint Advanced Management.

Why use authoritative sites

Use authoritative sites to:

- Improve trust in Copilot Search by promoting verified organizational sources.
- Help users quickly identify official content.
- Reduce time spent validating whether content is reliable.
- Maintain centralized admin control over authoritative source designation.

Configure authoritative sites with SharePoint Online Management Shell

Use SharePoint Online Management Shell when you want a straightforward admin workflow.

1. Install and import the module.
2. Connect to your SharePoint admin center.
3. Mark the site as authoritative.

PowerShell

```
Install-Module -Name Microsoft.Online.SharePoint.PowerShell -Force
Import-Module -Name Microsoft.Online.SharePoint.PowerShell

Connect-SPOService -Url "https://<tenant>-admin.sharepoint.com"
Set-SPOSite -Identity "https://<tenant>.sharepoint.com/sites/<siteName>" -
IsAuthoritative $true
```

Configure authoritative sites with CSOM (advanced)

Use CSOM when you need automation or bulk operations.

> ⓘ **Note**
>
> CSOM version 16.1.26914.12004 or later is required.

Step 1: Install PnP PowerShell

PowerShell

```
Install-Module PnP.PowerShell -Scope CurrentUser -Force
```

Step 2: Register a Microsoft Entra ID app

Register an app for interactive authentication and copy the client ID from the output.

PowerShell

```
$tenant = "<TenantName>.onmicrosoft.com"
Register-PnPEntraIDAppForInteractiveLogin -ApplicationName "PnP Interactive (SPO
Admin)" -Tenant $tenant -SharePointDelegatePermissions "AllSites.FullControl" -
SharePointApplicationPermissions "Sites.FullControl.All" -GraphDelegatePermissions
"Sites.FullControl.All" -GraphApplicationPermissions "Sites.FullControl.All" -
Interactive
$clientId = "<FROM ABOVE OUTPUT>"
```

Step 3: Install SharePoint Online CSOM

PowerShell

```
Install-Package Microsoft.SharePointOnline.CSOM -Source nuget.org -Scope CurrentUser
```

Step 4: Load CSOM assemblies

PowerShell

```
$dllPath = "C:\Users\
<USER_NAME>\AppData\Local\PackageManagement\NuGet\Packages\Microsoft.SharePointOnline.
CSOM.<VERSION>\lib\netstandard2.0"
Add-Type -Path "$dllPath\Microsoft.SharePoint.Client.dll"
Add-Type -Path "$dllPath\Microsoft.SharePoint.Client.Runtime.dll"
Add-Type -Path "$dllPath\Microsoft.Online.SharePoint.Client.Tenant.dll"
```

Step 5: Connect to SharePoint Online

PowerShell

```
$tenantDomain = "<TenantName>.onmicrosoft.com"
Connect-PnPOnline -Url "https://<TenantName>-admin.sharepoint.com" -ClientId $clientId
-Tenant $tenantDomain -Interactive
```

Step 6: Initialize tenant object and verify API availability

PowerShell

```
$ctx = Get-PnPContext
$tenant = New-Object Microsoft.Online.SharePoint.TenantAdministration.Tenant($ctx)
$ctx.ExecuteQuery()

$tenant.GetType().GetMethod("GetAuthoritativeResources")
```

CSOM operations

Get authoritative sites

PowerShell

```
$authResources = $tenant.GetAuthoritativeResources()
$ctx.ExecuteQuery()
```

Mark a site as authoritative

PowerShell

```
$siteId = [Guid]"<SiteId>"
$result = $tenant.SetResourceAsAuthoritative($siteId)
```

```
$ctx.ExecuteQuery()
$result.Value
```

Remove a site from authoritative sites

PowerShell

```
$siteId = [Guid]"<SiteId>"
$result = $tenant.RemoveResourceAsAuthoritative($siteId)
$ctx.ExecuteQuery()
```

If the site is removed successfully, the response is empty. If the operation fails, PowerShell returns an exception.

Bulk mark sites as authoritative

PowerShell

```
[System.Guid[]]$siteIds = @([Guid]"<SiteId1>", [Guid]"<SiteId2>", [Guid]"<SiteId3>")
$results = $tenant.BulkSetResourceAsAuthoritative($siteIds)
$ctx.ExecuteQuery()
$results
```

Bulk remove authoritative sites

PowerShell

```
[System.Guid[]]$siteIds = @([Guid]"<SiteId1>", [Guid]"<SiteId2>", [Guid]"<SiteId3>")
$results = $tenant.BulkRemoveResourceAsAuthoritative($siteIds)
$ctx.Load($results)
$ctx.ExecuteQuery()
$results
```

Lifecycle and maintenance

Maintain authoritative sites as a living set of trusted sources:

- Review the list regularly and remove outdated or no-longer-official sites.
- Validate behavior after site deletion or restore events.
- Plan for propagation time after updates.

Limitations

- You can mark up to 100 sites as authoritative.

- Changes can take up to 72 hours to appear in supported experiences.
- Designation is currently site-level only.
- Multi-geo tenants manage authoritative site data per geo.
- Personal sites can't be marked as authoritative.

Troubleshooting

If changes don't appear as expected, check the following items:

- **Licensing**: A Microsoft Copilot license is required. (See Prerequisites for SharePoint Advanced Management.)
- **Feature availability**: Make sure the feature is enabled in your tenant.
- **Site eligibility**: Make sure the URL is valid and references a supported SharePoint site.
- **Timing**: Allow enough time for propagation (up to 72 hours).

Last updated on 08/26/2026

Get started with agents in SharePoint

> **Important**
>
> Microsoft is upgrading the agent experience (.agent files) in SharePoint to better align with the Microsoft Copilot extensibility ecosystem. By using the new agent experience, agents in SharePoint can be part of the Copilot app home experience and the Microsoft plugin registry.
>
> To learn more, see Upgrade agents in SharePoint and OneDrive.

Agents in SharePoint, powered by AI, help users quickly find information and insights on SharePoint sites, pages, and document libraries. These agents access your organization's data the same way Copilot in other Microsoft 365 apps does, responding to users based on their access permissions to the data. This article discusses how admins can get started with agents in SharePoint, including setting up pay-as-you-go billing and managing Azure resources for agents.

Understand who can set up and use agents

Agents in SharePoint don't require activation. Once a user is assigned a Copilot license, or if your organization uses pay-as-you-go billing, these agents automatically become available to the user on eligible sites where they have permissions.

Expand table

Action	Requirements for the user
Create an agent	- Assigned with a Copilot license. - Ability to add new files to a SharePoint site.
Configure and interact with an agent	- Assigned with a Copilot license or your organization has the pay-as-you-go billing set up for you.

> **Important**
>
> If your organization hasn't adopted Microsoft Copilot, review the requirements and learn how to adopt it for your organization. Learn more.

Use agents with Copilot licenses

Users can use agents in SharePoint after being assigned a Copilot license. Use the Microsoft Copilot setup guide in the Microsoft 365 admin center to assign the required licenses to users. For more information, see Assign licenses to users in the Microsoft 365 admin center and Microsoft Copilot requirements. To learn more, see controlling user access through licensing.

Use agents with pay-as-you-go billing

To use agents with pay-as-you-go billing, first set up SharePoint agents as a resource in Azure. Whenever a user without a Microsoft Copilot license uses an agent in SharePoint, their usage uses that resource. For more information, see Use agents with pay-as-you-go billing.

Comparison of Copilot licenses and pay-as-you-go billing

What does the user get with pay-as-you-go billing and a Copilot license? Here's a comparison:

Expand table

Licensed for Microsoft Copilot	Pay-as-you-go Enabled	What does the user get?
No	No	Cannot create or use agents.
No	Yes	All unlicensed users can use agents and are billed per pay-as-you-go billing.
Yes	No	- Licensed users can create and use agents. - Unlicensed users can't create or use agents.

Monitor agent usage

Users with at least site visitor permissions can check the agent's file statistics, use search to find all agents for bulk actions, and see site usage. SharePoint admins can use the SharePoint Online Management Shell, Microsoft Purview audit log, Microsoft Cost Management, and SharePoint Advanced Management to monitor agent usage at the organization level. For more information, see Monitor agent usage in SharePoint.

Last updated on 10/16/2026

Upgrade agents in SharePoint and OneDrive

Learn how to upgrade your agent experiences in SharePoint and OneDrive. Upgrading allows your agents to leverage Copilot in SharePoint and all the functionality of the Microsoft Copilot extensibility ecosystem.

What is changing?

Microsoft is upgrading the agent experience in SharePoint and OneDrive. Upgrading better aligns your agents with the Microsoft Copilot extensibility ecosystem, ensuring your agents are part of the Microsoft Copilot app Home experience and the Microsoft plugin registry, the shared catalog for discovering, publishing, and governing organization-approved and custom-built plugins across Microsoft Copilot experiences, Microsoft 365 apps, OneDrive and SharePoint.

Existing agents in the .agent file format will continue to work across SharePoint, Microsoft Teams, and the Copilot app until the end of March 2027. You can start upgrading or moving each experience to a supported path that best fits its purpose now. After March 2027, .agent files will stop responding and you will have to upgrade to continue using them.

The right upgrade path depends on what each agent helps users accomplish today:

Expand table

Agent role	Recommended path
Primarily answers questions about content on the current SharePoint site	Use Copilot in SharePoint directly
Performs a repeatable action, workflow, or task within the SharePoint site	Convert the agent to a skill
Provides a customized Q&A, retrieval, or analysis experience	Upgrade the agent with Microsoft Copilot Agent Builder
Is a custom engine agent built in Copilot Studio and published to SharePoint	Publish the existing Copilot Studio agent to Microsoft Copilot app

Starting in mid-November 2026, you'll use Microsoft Copilot Agent Builder to create agents for SharePoint and OneDrive. You can still select SharePoint and OneDrive content as knowledge sources and use a provided prompt to start building a conversational agent. However, creating

an agent no longer saves a .agent file in SharePoint or OneDrive. You can edit, share, and monitor your agents through the Copilot app and manage them through Agent 365.

Are agents in SharePoint and OneDrive being retired?

No, only the .agent file format is being retired. You can continue to deliver named conversational experiences and focused site tasks grounded in SharePoint content through Copilot in SharePoint and Microsoft Copilot Agent Builder.

How these agents are incorporated back into SharePoint will change with the Agent Chat web part (coming soon) as the primary experience. Agents saved as .agent files will stop working after March 2027.

Why is Microsoft making this change?

Copilot in SharePoint and the Copilot extensibility ecosystem provide a consistent foundation for creating, discovering, sharing, governing, monitoring, and managing agents and plugins. Upgraded agents can continue to use SharePoint and OneDrive content, with more customization options, broader distribution, and centralized administration through Agent 365. Skills add focused, reusable capabilities directly to Copilot in SharePoint.

Which agents are affected?

This change applies to agents stored as .agent files in SharePoint or OneDrive. You might currently use these agents in the SharePoint chat pane, through the Agent Link web part, in the agent immersive viewer, in a Microsoft Teams chat or channel, or in the Copilot app.

You don't need to recreate Copilot Studio agents published to SharePoint because of this change. Review their publishing configuration and publish them to Microsoft Copilot app to make them available to the Agent Chat web part for display.

Do I need to take action immediately?

No. Existing .agent files will continue to work until the end of March 2027. However, you should start planning your upgrade to take full advantage of Copilot in SharePoint, Copilot extensibility updates, and the governance and analytics of Agent 365.

What happens after March 2027?

Agents in .agent file format stop responding to prompts:

1. .agent files that you added to a Teams chat or channel stop responding.
2. .agent files that you used in Microsoft Copilot app stop responding.
3. In SharePoint and OneDrive:
    - Accessing a .agent file (directly or through a share link) displays a message that indicates an upgrade is required.
    - The agent no longer opens in the immersive viewer, Copilot app, or SharePoint side chat pane.
    - The agents icon on the SharePoint navigation no longer appears.
    - The only main agent available on a SharePoint site is Copilot, so this setting is no longer needed and will be removed.

Upgrade paths

You can choose from different Copilot capabilities to upgrade to based on what your existing agent does and where people need to use it.

As you upgrade an existing SharePoint or OneDrive agent, consider the outcome it provides today and choose the upgrade path that best preserves that outcome. Also consider reviewing agents with no recent use or no clear owner for archival or deletion, instead of upgrading them.

Agents

If your existing .agent file provides a named Q&A, retrieval, or analysis experience that users need to access beyond the current SharePoint site, consider creating an agent with Microsoft Copilot Agent Builder.

Agents created through Microsoft Copilot Agent Builder can be used across supported Microsoft 365 experiences, including Copilot app, Teams, and SharePoint. Users can monitor agents in this builder, and administrators can govern, analyze, and manage agents through Microsoft Agent 365.

In SharePoint, site owners can bring agents directly to their audience by adding them to the pages where people need them using the Agent Chat web part. Site owners control where these agents appear as part of the overall site experience. Usage by unlicensed users is consolidated under Copilot app pay-as-you-go (PAYG).

Upgrade the agent with Microsoft Copilot Agent Builder

The agent is a customized Q&A, retrieval, or analysis experience with an identity, description, starter prompts, and instructions.

Some examples:

- A named subject matter expert that users recognize and revisit to get information
- Used across SharePoint, Microsoft Copilot, and Teams
- Agents grounded in SharePoint and OneDrive content for question-and-answer using Retrieval-Augmented Generation (Q&A/RAG) scenarios

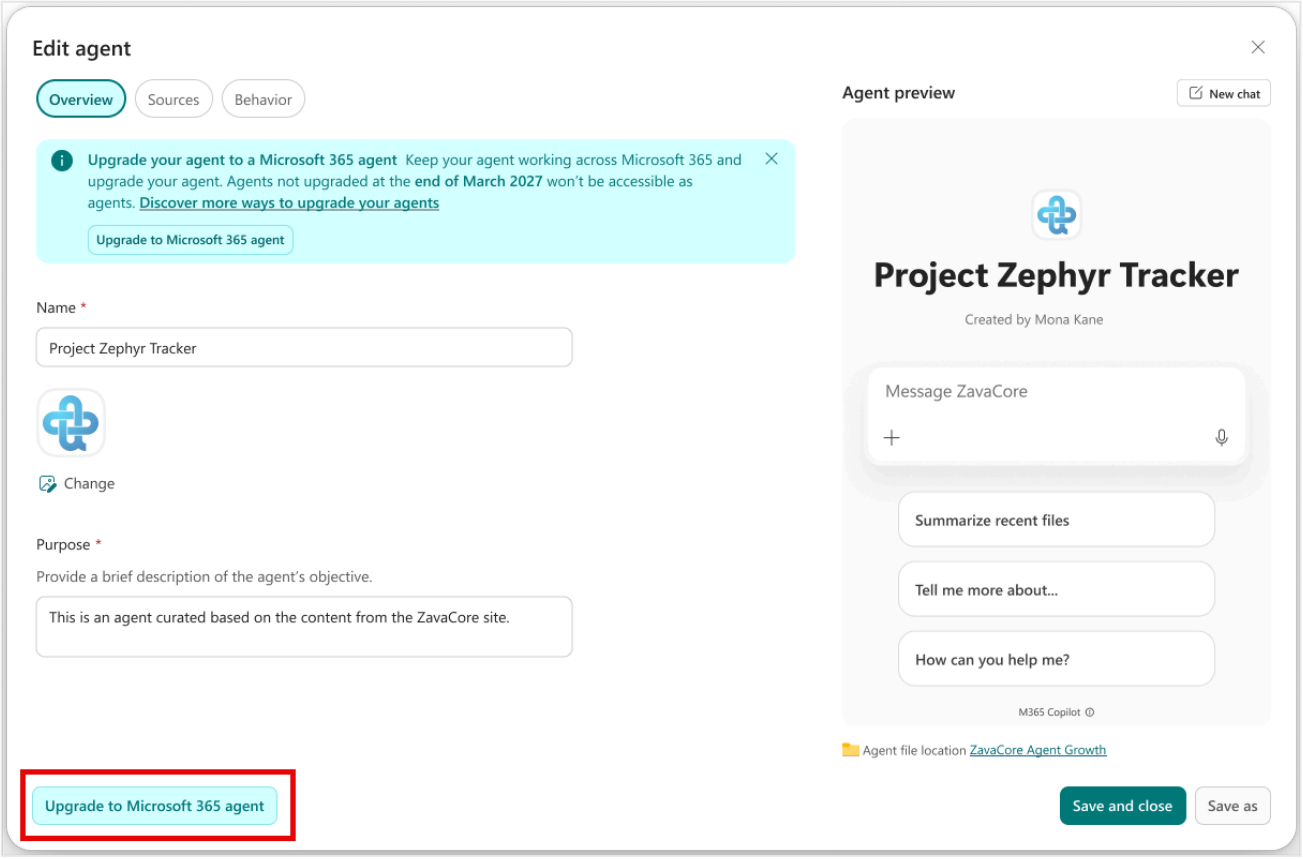
Before you start, confirm you have the following access:

- Edit permissions to the .agent file
- Ability to share that agent
- Permission to edit pages so an Agent chat web part can be added to the page

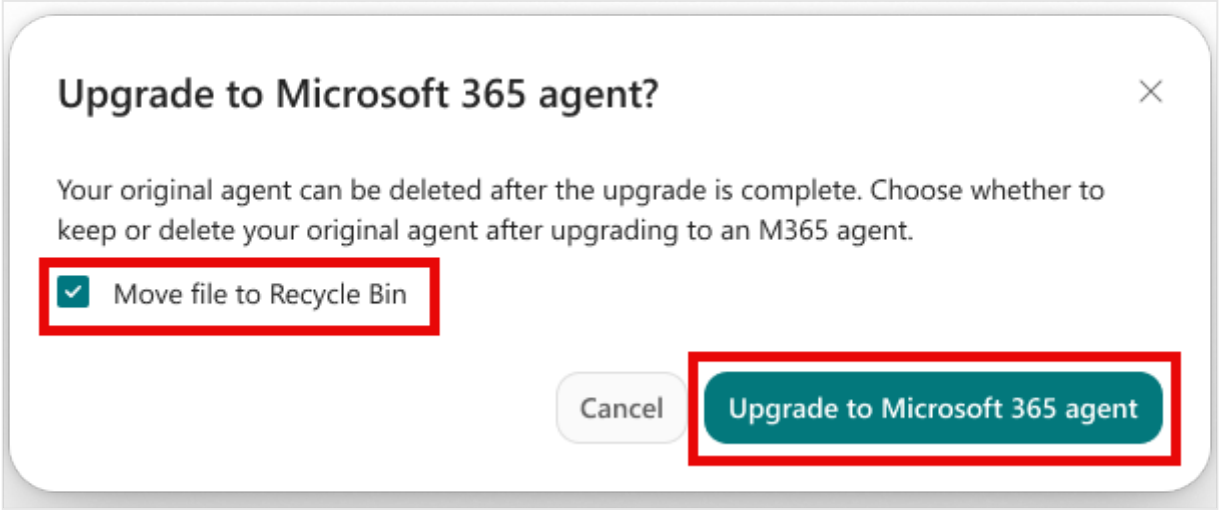
To upgrade:

> **Note**
>
> The upgrade experience described here will be available starting mid-November 2026.

1. Take note of who has access to the agent and where the agent is used.
2. Edit the .agent file.



3. Select **Upgrade to Microsoft 365 agent**. A confirmation dialog appears.



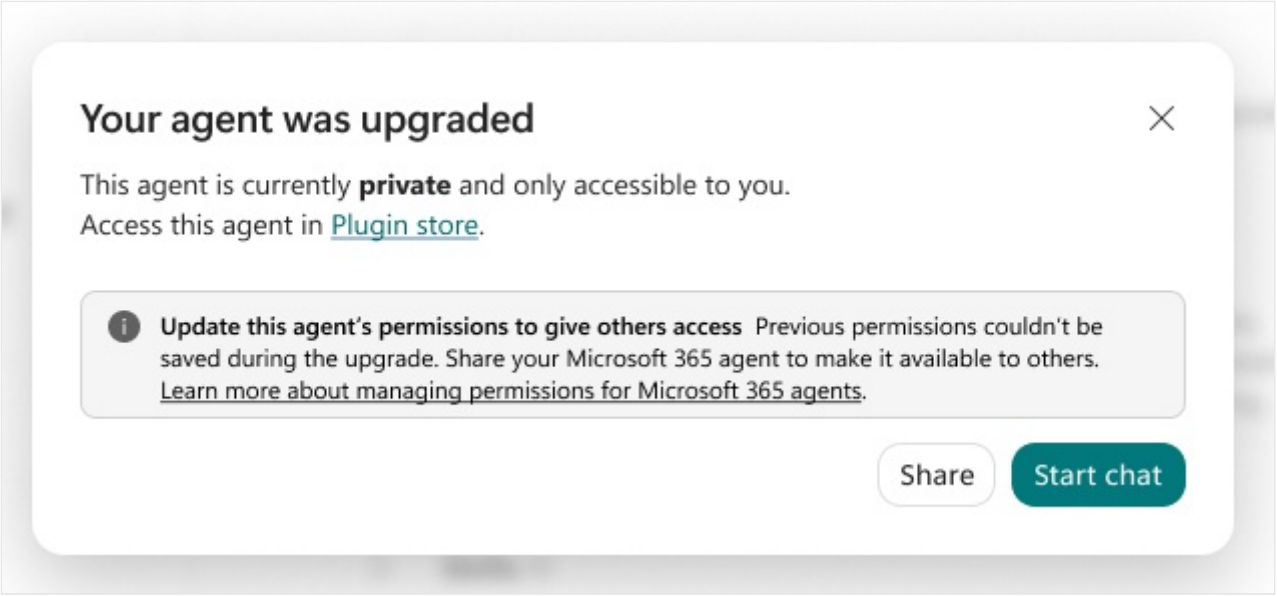
1. Select **Upgrade to Microsoft 365 agent** to confirm. Teams and Copilot app will automatically use the upgraded agent.

    - If you plan to add the agent to a page Agent Chat web part, select **Move file to Recycle bin**.

    - If you want to continue using the .agent file configuration as the main agent for the site until March 2027, through an Agent Link web part open in the SharePoint chat pane, don't select **Move file to Recycle bin**.

2. On a successful upgrade, the agent uses Microsoft Copilot Agent Builder for all future updates. You can no longer edit the original .agent file and it won't be changed by Microsoft Copilot Agent Builder.

3. If the original agent was shared with everyone in the organization, this access continues in the upgraded agent. Otherwise, the agent is private to you and you can share it to the necessary Microsoft 365 groups. Verify that users who need the agent can access both the agent and the selected knowledge sources.



1. The agent is now available through the plugin store in the Copilot app according to sharing and administrative policies. Not every upgraded agent is automatically published broadly.

You control the agent your audience uses during the transition period:

1. If you don't delete the original .agent file, you can open it in the SharePoint chat pane. If you link to it from the Agent Link web part, set it as the main agent, or open the file directly in the side pane, the original configuration loads and users can interact with it.

   To direct users to the upgraded agent instead:

- If the original agent is on a SharePoint page through a link or the Agent Link web part, update the page to use Agent Chat web part, instead.

- Upgraded agents can't be used in the site's chat pane, so you won't be able to set one as the main agent for the site. Instead, add the Agent Chat web part to a page, so it's prominent on the site and set the main agent as **Copilot**.

1. In the Copilot app, the upgraded agent automatically loads when requested.

2. In a Teams chat or channel, the agent is upgraded but needs to be re-added to the chat or channel. Remove the agent that's in the chat or channel now, then add the agent again by copying the sharing link and posting it to the chat or channel.

Here are some important differences between the .agent file and the Microsoft 365 agent:

- You don't manage Microsoft 365 agent permissions through SharePoint site permissions. Set share access through Microsoft Copilot Agent Builder. If you shared the .agent file with everyone in the organization, you can carry that organization-wide access over during the upgrade. Otherwise, the upgraded agent is private and the creator needs to share it with the people, groups, and email addresses that need to access it from the SharePoint site.
- Usage data starts collecting for the upgraded agent.

Custom engine agents

If you have a .agent file that resulted from publishing a custom engine agent created in Copilot Studio to the SharePoint channel, you don't need to rebuild it as a Microsoft Copilot Agent Builder agent.

To add these agents to the Agent Chat web part, you need to make them available to the Microsoft Copilot app and Teams channel. For more information about publishing, see Key concepts - Publish and deploy your agent - Microsoft Copilot Studio.

You can delete the .agent file after you add it to a SharePoint page by using the Agent Chat web part.

Copilot in SharePoint

Copilot in SharePoint helps people work directly with content on a SharePoint site.

If your .agent file primarily helps people ask questions about or understand content from the current site, you might not need to maintain a separate named agent. You can use Copilot in SharePoint directly.

Copilot in SharePoint answers questions about content on the current SharePoint site. It doesn't include special instructions beyond answering authoritatively.

Some examples:

- Catch me up on the most recent changes

- Tell me more about this [topic] on this site

Users need a Microsoft Copilot license to use Copilot in SharePoint. Verify that Copilot is available on the site.

To ensure that users discover Copilot in SharePoint, set Copilot as the Main agent for the site through the site's AI Settings. When you complete this step, you can delete the .agent file.

Skills for Copilot in SharePoint

> **Note**
>
> The `convert-agent-file-to-skill` skill will be available mid-November 2026.

Skills customize what Copilot in SharePoint can do for specific business outcomes.

A .agent file might be a good candidate for a skill if it performs a repeatable action, workflow, or task within the context of a SharePoint site instead of primarily providing a Q&A experience. The skill should run only in this site context and should be discoverable and executable through interactions with Copilot in SharePoint.

A simple way to distinguish between the two is:

- **Use a skill** when Copilot should perform a focused, repeatable task or multistep workflow within the SharePoint site.
- **Use an agent** when users need a customized Copilot experience for Q&A, retrieval, analysis, or other scenarios.

Some examples:

- Drafting a document from SharePoint content on this site.
- Reviewing a document to recommend updates.
- Organizing files for a business outcome.
- Applying focused instructions or guardrails to a narrow task.

Convert the agent to a skill

Before you start, confirm you have the following:

- Confirm the intended users have a Microsoft Copilot license. Only Microsoft Copilot licensed users can access Copilot in SharePoint and its services.
- Confirm Copilot in SharePoint is available on the site.
- Confirm the actions of this agent don't need to be accessible in the Copilot app or Teams.

To convert the agent to a skill:

1. Prompt to use the skill, `convert-agent-file-to-skill`, with the .agent or .copilot agent file. You will have the option to create a site or personal skill.
2. To help users discover a site skill, add a Button web part to the page to open Copilot in SharePoint to run a prompt with the skill. This step is optional.
3. You can delete the .agent file after the conversion.

Upgrade guidance

Who can upgrade an agent?

The agent owner, creator, or site owner is best suited to decide the upgrade path for the agent. They can make the decision based on how users discover and engage with the agent.

To upgrade the agent, you need:

- Edit permissions to the .agent file
- Ability to share that agent
- Permission to edit pages so the Agent chat web part can be added to the page

To convert to a skill, you need Copilot in SharePoint available on the site.

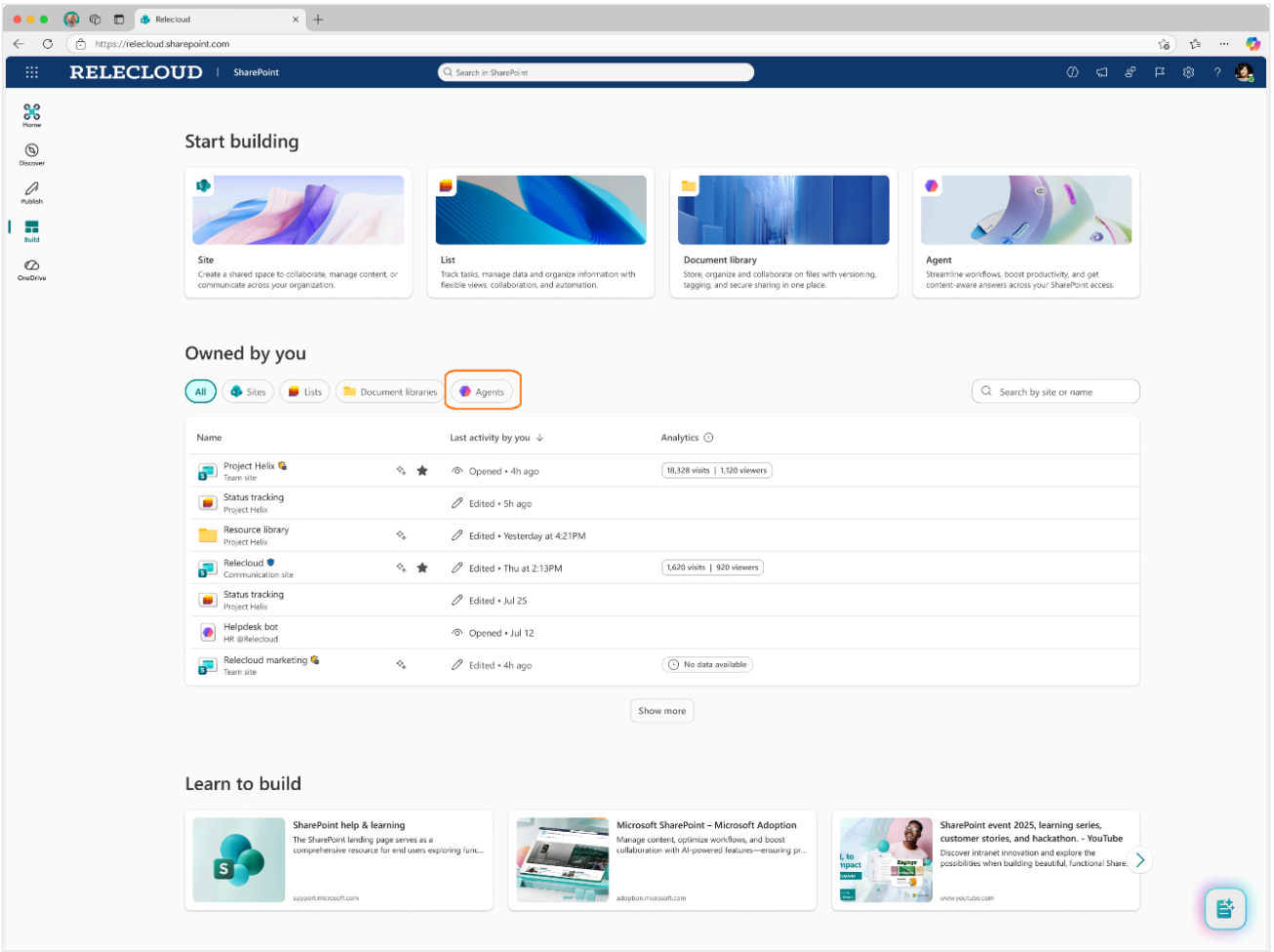
How do I find agents that need to be upgraded?

Individuals with OneDrive agents can prioritize those that they use most frequently. On SharePoint sites, prioritize agents with high usage, broad audiences, business-critical scenarios, custom instructions, pay-as-you-go dependencies, Teams distribution, or prominent SharePoint placement.

In OneDrive, you can find your agents through the filters on Home, Shared, or Favorites folders and the save location **My Files** > **Documents** > **Agents**.

In SharePoint, you have a few options for finding your agents:

- As the agent owner, visit the **Owned by you Agents** section of Build in SharePoint to see agents you own and are candidates for upgrade.



- Use the agent reports on SharePoint Advanced Management to inventory agents.
- Use the agent registry to see "SharePoint" agents.
- Use search to find your agents on the site.

What should I do if I use an agent that someone else created?

Contact the agent owner or the SharePoint site owner and ask whether a replacement is planned. Permission to use an agent doesn't necessarily provide the edit and creation permissions needed to upgrade it. Confirm that you can access and use the replacement before the .agent experience stops working.

Permissions, sharing, and data

Do existing permissions and sharing automatically transfer?

No. Sharing a Microsoft Copilot Agent Builder agent is separate from sharing files on a SharePoint site.

A .agent file uses SharePoint file permissions and might inherit access from its site or library. After the upgrade, the Microsoft Copilot Agent Builder agent uses agent-level sharing to share with people, groups, and email addresses, but not to SharePoint groups. If you shared the .agent file with everyone in the organization, that organization-wide access can carry over during the upgrade. Otherwise, the upgraded agent is private until the owner shares it.

Creators and owners should review and share the upgraded or new agent with the people and groups that will see the agent on the SharePoint site.

Access to an agent doesn't grant access to its underlying SharePoint or OneDrive content. Users must have permission to both the agent and the knowledge sources it uses.

What happens to existing usage history and analytics?

Existing .agent usage history doesn't transfer to the replacement. Analytics for the upgraded skill or agent begin as a new experience. Capture any legacy reporting needed for records or adoption analysis before completing the transition.

What happens to existing links and placements?

In SharePoint, update the page to use Agent Chat web part. Note that the upgraded agent can't be used in the site's chat pane, so you won't be able to set it as the Main agent for the site. Set the Main agent to be **Copilot** after adding the upgraded agent to a page.

In Copilot app, the upgraded agent automatically loads when requested. OneDrive users should use Copilot app to use their agents.

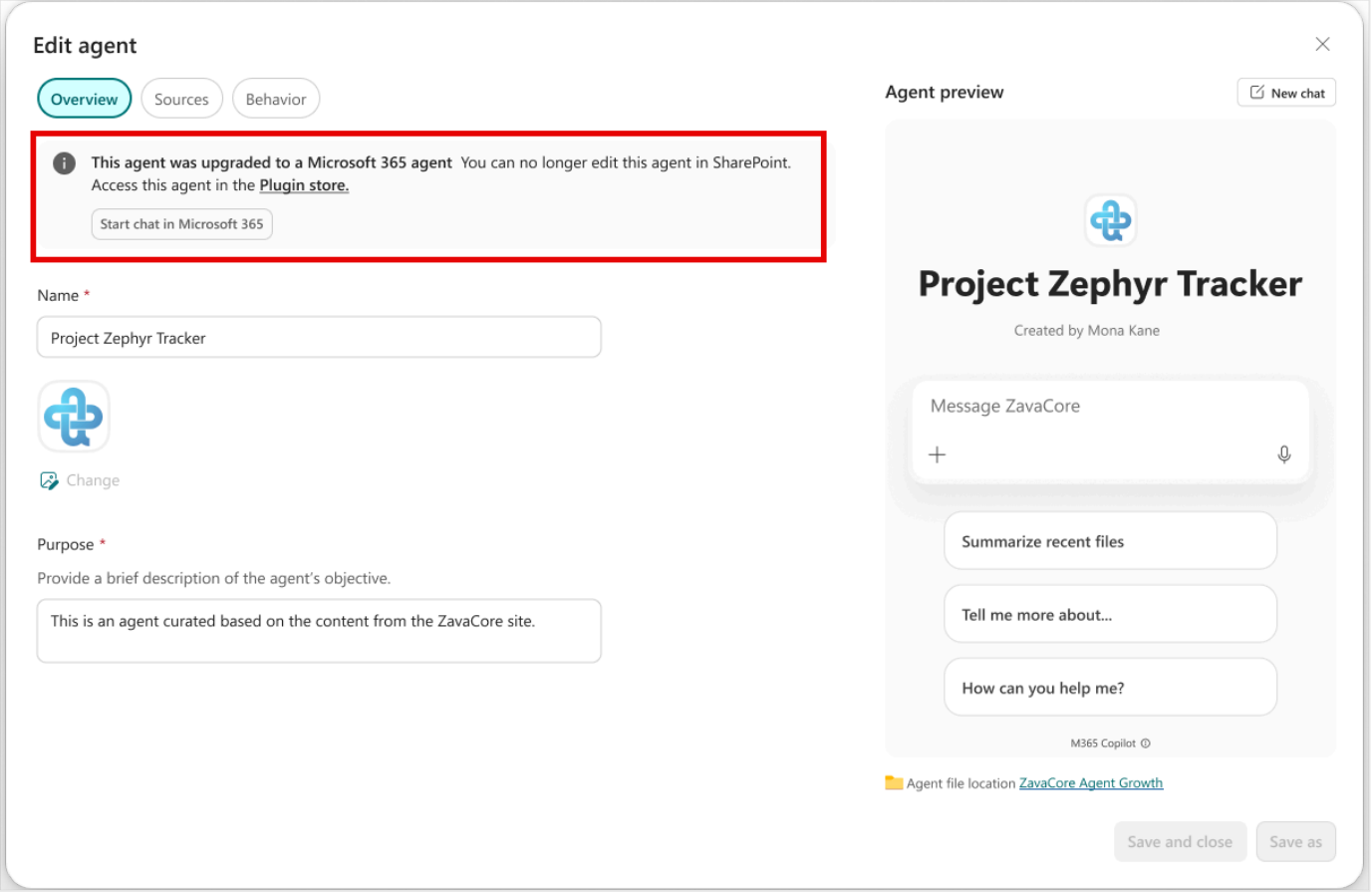
In a Teams chat or channel, the agent is upgraded but needs to be re-added to the chat or channel. Remove the agent that's in the chat or channel now, then add the upgraded agent by grabbing a link to it and adding it to a message to the chat or channel.

How do I know an agent is upgraded?

Deleting the .agent file after you choose an upgrade path is the easiest way to track which agents remain to upgrade.

If the agent was converted to a skill for the SharePoint site, there's no indication on the .agent file that a conversion happened, but the file moves to the skill location as a backup.

If the .agent file was upgraded to a Microsoft Copilot Agent Builder declarative agent, the SharePoint agent builder shows a banner indicating that the agent is upgraded and no longer editable.



Timing and preparation

Is my existing agent already gone?

No. You can use existing .agent files during the transition. The announcement provides time to inventory, evaluate, upgrade, and test experiences before .agent files stop responding to prompts after March 2027.

When will the experience change?

Expect the following changes starting mid-November 2026:

1. When you create an agent from SharePoint or OneDrive, you use Microsoft Copilot Agent Builder, and no longer create .agent files.
2. The **Upgrade to Microsoft 365 Agent** button appears in the builder.
3. The **convert-agent-file-to-skill** skill becomes available in Copilot in SharePoint.

When will existing .agent files stop working?

Existing .agent files will stop responding to prompts after March 2027. After that time, they will no longer respond in the SharePoint chat side pane, Teams, or the Copilot app. The Agent Link web part and the current immersive viewer will also no longer provide access to these agents.

Do I need to take action now?

You don't need to take any action now, but you should begin preparing. Start with the agents that are business-critical, actively used, broadly shared, embedded on SharePoint pages, added to Teams, or dependent on pay-as-you-go consumption.

1. Inventory .agent files in SharePoint and OneDrive.
2. Identify each agent's owner, audience, purpose, knowledge sources, and current access points.
3. Choose the best-fit upgrade path.
4. Upgrade or re-create the experience, then configure sharing and placement.
5. Test with representative users and familiar prompts before switching.
6. Archive or delete the original .agent file after validating the replacement.

Will Microsoft automatically upgrade my agents?

No. There's no automatic upgrade. An agent owner or site owner should review .agent files and choose the appropriate upgrade paths. This approach ensures that a named chat experience isn't converted into a skill, or a focused site task into a broader agent without considering the original business outcome. In some cases, the best thing to do is delete the .agent file because it's no longer used. Deleted files appear in the recycle bin.

Are these changes available in Microsoft Government Cloud?

All these upcoming changes apply to Microsoft Government Cloud.

Copilot extensibility is available in Microsoft Government Cloud, so upgrading to Microsoft Copilot Agent Builder declarative agents preserves your agents' capabilities.

Converting to a skill in Copilot in SharePoint will be available when Copilot in SharePoint is available in Microsoft Government Cloud (coming soon).

Administrator guidance

How should administrators prepare?

Learn about Microsoft Agent 365.

1. Ensure your agent creators can share that agent.
2. Identify active and business-critical .agent files.
3. Engage site owners and agent creators to assign ownership and choose an upgrade path.
4. Confirm licensing and consumption configuration for each destination.
5. Update internal guidance, support processes, training, and communications before the creation experience changes.
6. Allow time to test sharing, content access, Teams placement, SharePoint placement, and representative prompts.

Where will users find upgraded agents?

Users can discover declarative agents and Copilot Studio agents through supported Microsoft 365 experiences, including the plugin store, Microsoft Copilot app, and Teams.

SharePoint site owners can place relevant agents directly on pages through the Agent Chat web part (coming soon).

Users discover and use skills through Copilot in SharePoint and can highlight them with Quick Steps, Button web part, or other site entry points.

What is happening with SharePoint Agents pay-as-you-go?

SharePoint Agents pay-as-you-go only applies to .agent files. The upgraded agents follow the capabilities and licensing model for agents in Microsoft Copilot app.

SharePoint Agents pay-as-you-go doesn't apply to Copilot in SharePoint.

Last updated on 10/16/2026

Manage access to agents in SharePoint

Agents in SharePoint, powered by AI, help users quickly find information and insights on SharePoint sites, pages, and document libraries. Agents in SharePoint access your organization's data the same way Copilot in other Microsoft 365 apps does, responding to users based on their access permissions to the data. As a SharePoint admin, you can manage users' access to an agent in multiple ways by managing:

- Who can access the agents
- What information the user can access through the agent
- Where agents are available

Manage who can access the agents

Agents in SharePoint don't require activation. You can manage who can access agents through Copilot license assignment. Or, if your organization has the pay-as-you-go billing set up, you can control who can access agents through the security groups assigned to the billing policy. Learn more about setting up pay-as-you-go billing for agents in SharePoint.

Control user access through licensing

Currently, users with a Microsoft Copilot license can use the agents. You can use the Microsoft Copilot setup guide in the Microsoft 365 admin center to assign the required licenses to users. For more information, see Assign licenses to users in the Microsoft 365 admin center and Microsoft Copilot requirements.

Admins can choose to edit the service plans under the Copilot license to specifically allow or block users from using Copilot experiences on SharePoint. Under the license details page for Microsoft Copilot on the Microsoft 365 admin center, admins can turn '*Microsoft Copilot for SharePoint*' on or off on a per-user basis. For example, a user could be allowed to use Microsoft Copilot on Teams but not use any agents on SharePoint alone. However, this change also disables Copilot in OneDrive and on the SharePoint page authoring Copilot for that user.

Control user access through pay-as-you-go billing

For users who aren't assigned with a Microsoft Copilot license, you can control user access to agents through pay-as-you-go billing. To do so, you need to first set up SharePoint agents as a resource in Azure. Then, you set up a pay-as-you-go policy that is assigned to a security group.

You can link that policy to the agent resource in SharePoint. Only users in the security group assigned to the billing policy have access to agents. For more information, see Use agents with pay-as-you-go billing.

Use file permissions on a specific agent file

Agents in SharePoint are represented as .agent files. The permissions on the `.agent` file determine who can access or edit the agent. Only users who can create or access files on a SharePoint site can create or access agents.

> **Note**
>
> For users who access and use an agent in SharePoint, the agent's responses depend on each user's permissions to the agent's data sources. For instance, if a user has access to the agent but not to the site or document library it references, the agent's responses for this user don't include content from those restricted sources.

Manage what information a user can access through the agents

Use built-in SharePoint features

Agents in SharePoint use SharePoint sites, pages, and document libraries as knowledge sources to respond to the user. You can control a user's access to the information when they use an agent by controlling their access to the site. SharePoint provides many tools to control access to a site:

- Control access to a site that is associated with a Microsoft 365 Group by setting the site as private (team sites only) and controlling group membership.
- Control access to a site that isn't associated with a group by using site permissions.
- Control access by using access governance policies available in the SharePoint admin center and PowerShell.

Use SharePoint Advanced Management

Currently, to restrict access to a site by Microsoft Copilot, the SharePoint admin can set up a restricted access control policy. As a result, all access to the site is restricted to only the group of users specified in the policy. Accordingly, the content from the site is visible in Microsoft Copilot only for this restricted group of users. You can restrict access to individual sites or OneDrive. To

learn more about features to prevent oversharing, control access, and enhance your content governance, see Get ready for Microsoft Copilot with SharePoint Advanced Management.

With Microsoft Purview Data Loss Prevention (DLP)

To prevent selected files from being used by agents, use sensitivity labels along with Microsoft Purview Data Loss Prevention (DLP). By creating a DLP custom policy with the **Content contains** > **Sensitivity labels** condition, you can prevent sharing of sensitive content with external users and exclude items from being processed. The citations in the response include identified items, but the content of the item isn't used in the response. You can't yet add a sensitivity label directly to the .agent file. If you want to govern your `.agent` file by using DLP, use conditions based on the `.agent` extension instead of using sensitivity labels as the condition.

Manage where agents are available

Site owner controls in SharePoint

Agents that you create in SharePoint don't automatically appear in any list or published location. Users can manually go to *.agent* files to use them, just like how they discover or use Word or Excel files. Site owners can choose one main agent for their site. This agent opens when users select the Agent icon in the global header. For more information, see Manage agents in SharePoint.

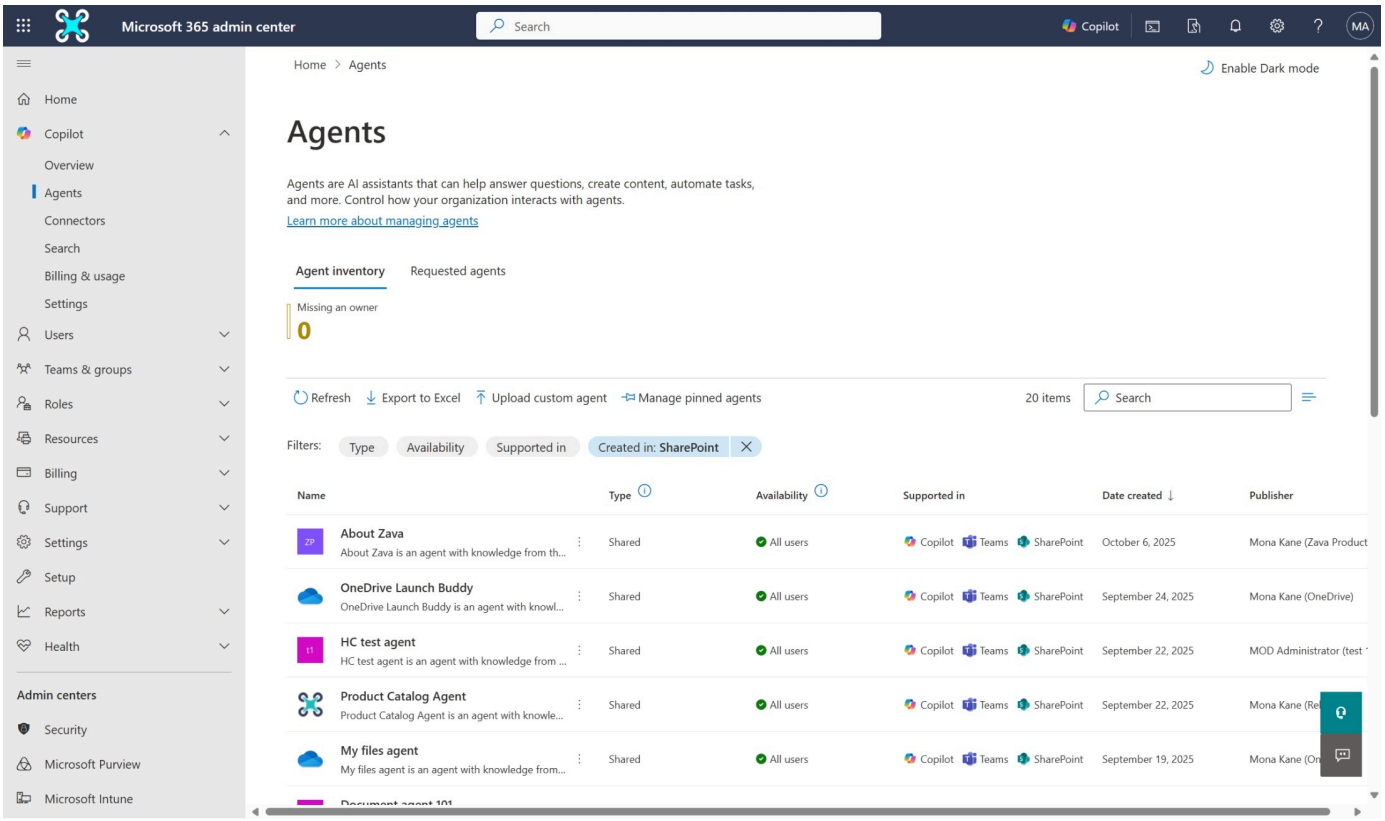
Turn off agents on sites with restricted content discovery

As a SharePoint admin, you can turn off all agent-related features on individual sites by using the restricted content discovery feature. Once you flag a site with restricted content discovery, users can't see the Agent icon on the global header of the site. Therefore, they don't have access to use the ready-made agent, create new agents, or add content from that site to any other agents. The restricted content discovery policy leaves site access unchanged but prevents the site's content from being surfaced in Microsoft Copilot or organization-wide search for all users.

Block agents from being used in Copilot Chat

Tenant admins and AI admins can manage actively used agents in SharePoint in the Microsoft 365 admin center, under the **Agents** section of the Copilot Control System (formerly known as integrated apps). This experience gives administrators a clear overview of all agents ever used in Copilot Chat, with the ability to view details and block or unblock any agent for use in Microsoft

Copilot, all from one place. For more information, see Manage Copilot agents in the Microsoft 365 admin center.



> **Note**
>
> Currently, blocking an agent only affects its availability in Copilot Chat. It doesn't yet apply to OneDrive, SharePoint, or Teams.

Related articles

- SharePoint site roles and permissions
- Permission levels in SharePoint
- Get ready for Microsoft Copilot with SharePoint Advanced Management
- Learn about data loss prevention

Last updated on 09/24/2026

Use agents with pay-as-you-go billing

> **Important**
>
> Microsoft is upgrading the agent experience (.agent files) in SharePoint to better align with the Microsoft Copilot extensibility ecosystem. By using the new agent experience, agents in SharePoint can be part of the Copilot app home experience and the Microsoft plugin registry.
>
> To learn more, see Upgrade agents in SharePoint and OneDrive.

Set up SharePoint agents as an Azure resource

To use pay-as-you-go billing, you need to first set up SharePoint agents as a resource in Azure. That resource is used whenever a user without a Microsoft Copilot license uses a SharePoint agent.

Prerequisites to set up SharePoint agents as a resource in Azure

To set up SharePoint agents as a resource in Azure, you need to have at least the following permissions as:

- A SharePoint administrator
- Owner or Contributor Azure roles to an Azure subscription
- Owner or Contributor Azure roles to an Azure resource group linked to the same Azure subscription

> **Note**
>
> - You only need the Owner or Contributor Azure roles during the billing setup process.
> - To assign an Owner or Contributor Azure role, see Assign Azure roles using the portal.

To set up SharePoint agents as an Azure resource, you need to do the following if you haven't already:

1. Create an Azure subscription.
2. Create an Azure resource group for SharePoint agents.

Set up pay-as-you-go billing for SharePoint agents

After setting up an Azure resource group for SharePoint agents, you can set up pay-as-you-go billing for SharePoint agents in the Microsoft 365 admin center. Here are the steps:

Step 1: Set up a pay-as-you-go billing policy To set up a pay-as-you-go billing policy for SharePoint agents, go to the Microsoft 365 admin center and follow the steps outlined in Set up or disconnect pay-as-you-go billing in the Copilot node of the Microsoft 365 admin center.

Step 2: Connect the billing policy to the SharePoint agent service

- After creating the billing policy, select **Connect a service** for the policy, on the **Billing & usage** page. The **Pay-as-you-go services** tab opens.
- Choose **SharePoint agents** from the list of apps and services. The **Manage billing policy connections** pane appears.
- Select the billing policy to connect it to the SharePoint agent service.
- Select **Save**, then **Done**. Your billing policy is now connected to the SharePoint agent service.

Migrate from previous pay-as-you-go policies

If you currently have a pay-as-you-go policy for SharePoint agents set up under **Org settings** and would like to take advantage of the new billing policy updates, you will need to first disconnect your existing policy before linking SharePoint agent to a new policy. By doing so, you benefit from the updated pay-as-you-go billing policies:

- You can assign one policy per security group and monitor cost for each group separately.
- Only users in the security group assigned to the billing policy have access to SharePoint agents.

> **Note**
>
> - Each billing policy can currently have one security group. Support for multiple security groups will be available soon.
> - You can create up to 10 policies, with each policy assigned a security group.

To disconnect your existing SharePoint agents pay-as-you-go billing policy:

1. Sign in to the Microsoft 365 admin center, select **Org settings** > **Pay-as-you-go services**.

2. Select SharePoint agents. The **Manage billing for SharePoint agents** page appears with a notification message at the top: "We've updated how pay-as-you-go billing works with SharePoint agents. With the new billing policies, you can divide charges across multiple Azure subscriptions. Learn about using SharePoint agents with pay-as-you-go billing. To manage pay-as-you-go billing for SharePoint agents, go to *Copilot Billing & usage*."
3. Select **Copilot Billing & usage** to open the **Billing & usage** page.
4. Select **SharePoint agents** under **Pay-as-you-go services**.
5. Select **Disconnect previous billing**.

Your previous billing is now disconnected. You can now set up a new billing policy and connect it to SharePoint agents.

Billing rates

The following table illustrates the differences in the subscription models for the cost of SharePoint agent usage.

Expand table

SharePoint agent feature	Billing rate	Use in Microsoft Copilot scenarios[1]	Autonomous use
Generative answer	2 messages	No charge	2 messages
Tenant graph grounding for messages	10 messages	No charge	10 messages

[1] Interactive use of generative answers, tenant graph grounding and agent actions by authenticated Microsoft Copilot users, in Microsoft 365 apps and services, are included at no extra cost.

- Generative answers: These events are dynamically generated using AI models, such as Generative Pretrained Transformers (GPTs). They can adapt and change based on the context and the knowledge sources they're connected to. They're useful for handling a wide range of topics and providing more flexible and natural interactions.

- Tenant graph grounding for messages: These events provide higher quality grounding for your agents using retrieval-augmented generation (RAG) over your tenant-wide Microsoft Graph, including external data synced into Microsoft Graph through connectors. This results in more relevant and improved responses and ensures that the grounding information is up-to-date. This capability is optional, and you can turn it on or off for each agent.

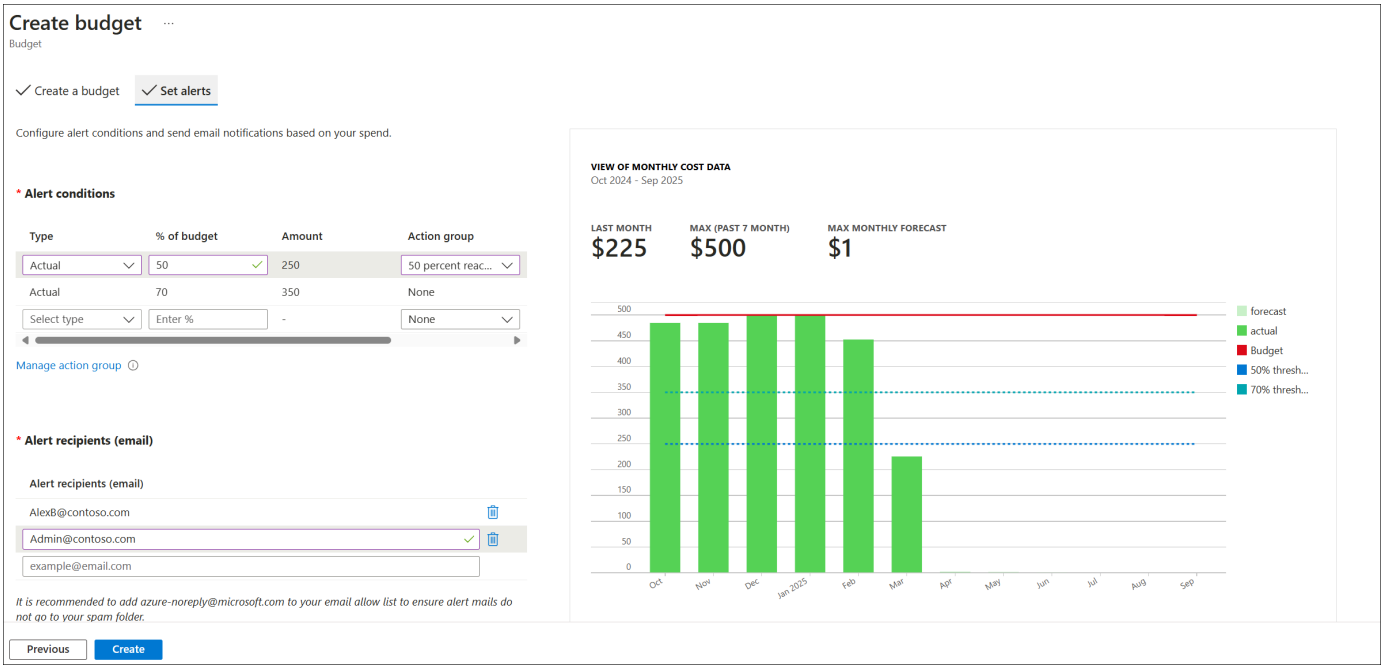
> **Note**
>
> - SharePoint agents are grounded in the tenant graph, so each interaction with a SharePoint agent uses 12 messages (10 messages for tenant graph grounding, and 2 messages for generative answers) to respond to a single complex prompt from the user.
> - Charges of SharePoint agent usage appear under the Copilot Studio meter in your invoice. However, in Microsoft cost management, you can see a detailed breakdown by feature, including SharePoint agents.

Monitor consumption in Microsoft Cost Management

You can monitor your organization's consumption of SharePoint agents with the pay-as-you-go with Microsoft Cost Management. If needed, change the scope to select the subscription that is being used for agents in SharePoint.

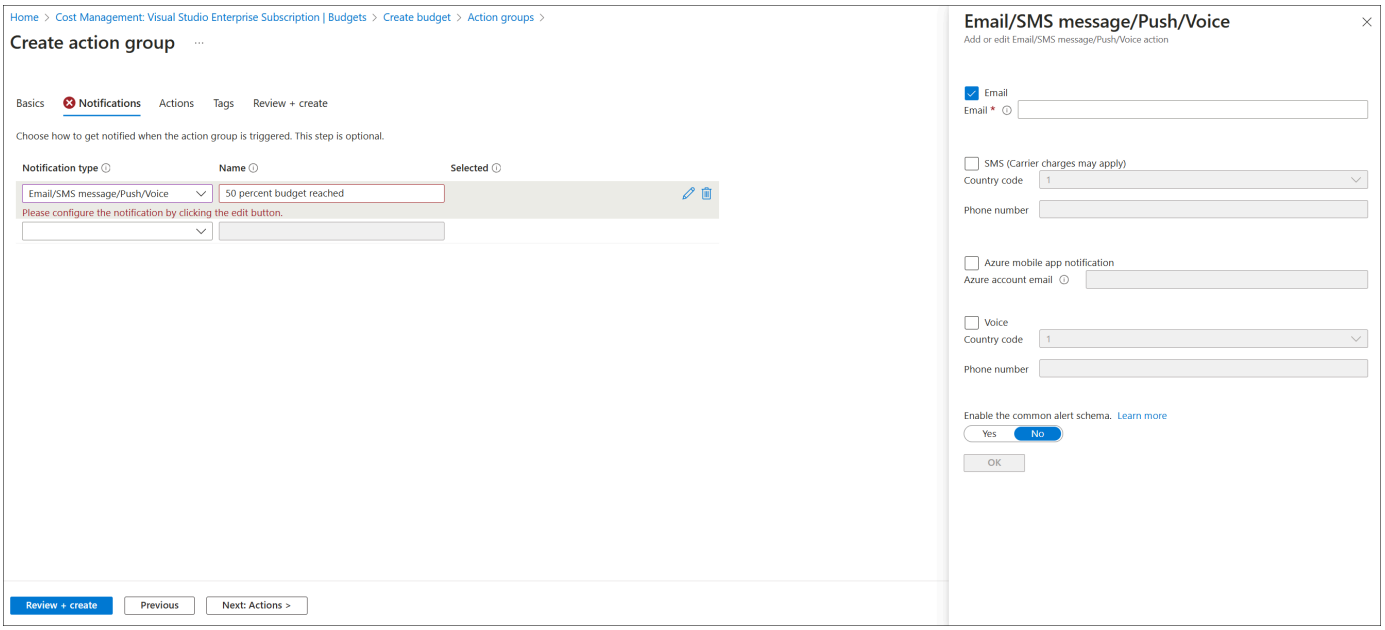
Select **Reporting + analytics**, then select **Cost analysis** to review and analyze your consumption. Choose to use **Smart views** to quickly view your consumption by Services, Resources, and Resources groups. You can also create custom views to analyze your consumption by different dimensions.

You can quickly create a budget under **Monitoring** > **Budgets** for your selected scope.



Select Alert conditions to set up the budget alert conditions. You can set up alerts for when your actual spending or the forecast reaches a certain percentage of your budget. Select **Manage**

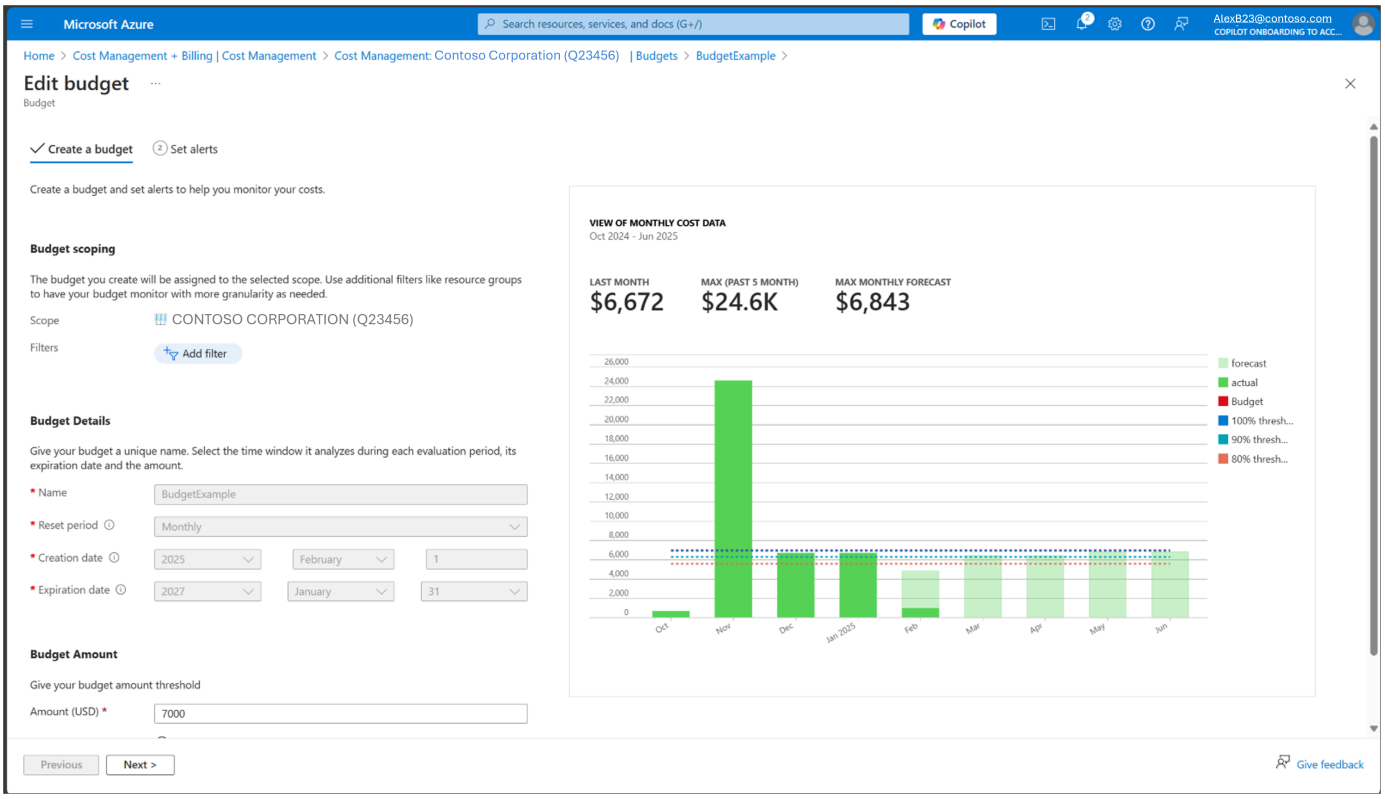
action group to set up the action group for the alert. You can choose to send an email, SMS, or push notification to the action group when the alert is triggered.



You can also create a budget in Microsoft Cost Management with Bicep and ARM template.

Budget helps you inform others about their spending to proactively manage costs and monitor how spending progresses over time. When you can also set up various types of cost alerts to monitor the consumption.

You can view your invoices under **Billing** > **Invoices**. Use text search to filter for the invoices you want. You can also filter by **Status** and **Timespan**. You can also download the invoice in CSV format.



Adjusting consumption

Using pay-as-you-go billing means that each user is responsible for their own consumption. Work with people in your organization to ensure the efficient use of agents in SharePoint. For example, restrict access to SharePoint sites with agents to only those who need to use them.

Paying your invoice

Your organization receives an invoice for all Azure services used at the end of each month. You can pay these invoices under the Invoices section in the subscription that you use for agents in SharePoint.

Disconnect agents from pay-as-you-go billing

To disconnect agents from pay-as-you-go billing, follow these steps:

1. In the Microsoft 365 admin center, select **Copilot** > **Billing and usage**.
2. On the **Pay-as-you-go services** page, select the SharePoint agent policy.
3. The **Manage billing policy connections** panel opens up. All policies including the ones that are connected to agents are displayed.
4. Select the checkbox next to the SharePoint agent policy you would like to disconnect.
5. View confirmation that your Azure Subscription has been disconnected.
6. Pay-as-you-go services will discontinue for this Azure Subscription.

7. If multiple services are connected to a single policy, each service can be disconnected by going through the above steps.

Last updated on 10/16/2026

Monitor agent usage in SharePoint

You can monitor agent usage in SharePoint through various tools and methods. Each tool and method suits the needs of specific user roles within the organization. This article outlines the options available for users with at least site visitor permissions and SharePoint admins. These two role groups have different ways to monitor and analyze the performance and usage of agents in their respective areas.

> **Note**
>
> To ensure that security and privacy settings are always honored, some of these tools are restricted to specific user roles.

The following tools and techniques are available for monitoring agent usage in SharePoint, categorized based on user roles and permissions:

- For **users with at least site visitor permissions** (site admins, site owners, site members, and site visitors):
  - **File statistics**: Select an individual `.agent` file and use the Details pane to view its file statistics.
  - **Search**: Use **Search** to find all agents on a site for bulk actions.
  - **Site usage**: Use **Site usage** to see the most popular files and agents on their sites.
- For **SharePoint admins**:
  - **SharePoint Online Management Shell**: SharePoint admins can use SharePoint Online Management Shell to get an inventory of the agents created across sites at the organization level in a specified time period.
  - **Microsoft Purview audit log**: SharePoint admins with Compliance admin permissions can use the Microsoft Purview audit log to monitor agent creation and usage details across the organization.
  - **Microsoft Cost Management**: SharePoint admins can use Microsoft Cost Management to monitor the cost of agent usage at the organization level.
  - **SharePoint Advanced Management**: Coming soon, SharePoint admins can use SharePoint Advanced Management to obtain detailed insights on agent usage across sites. The report lists the number of agents that are created, along with details on policies

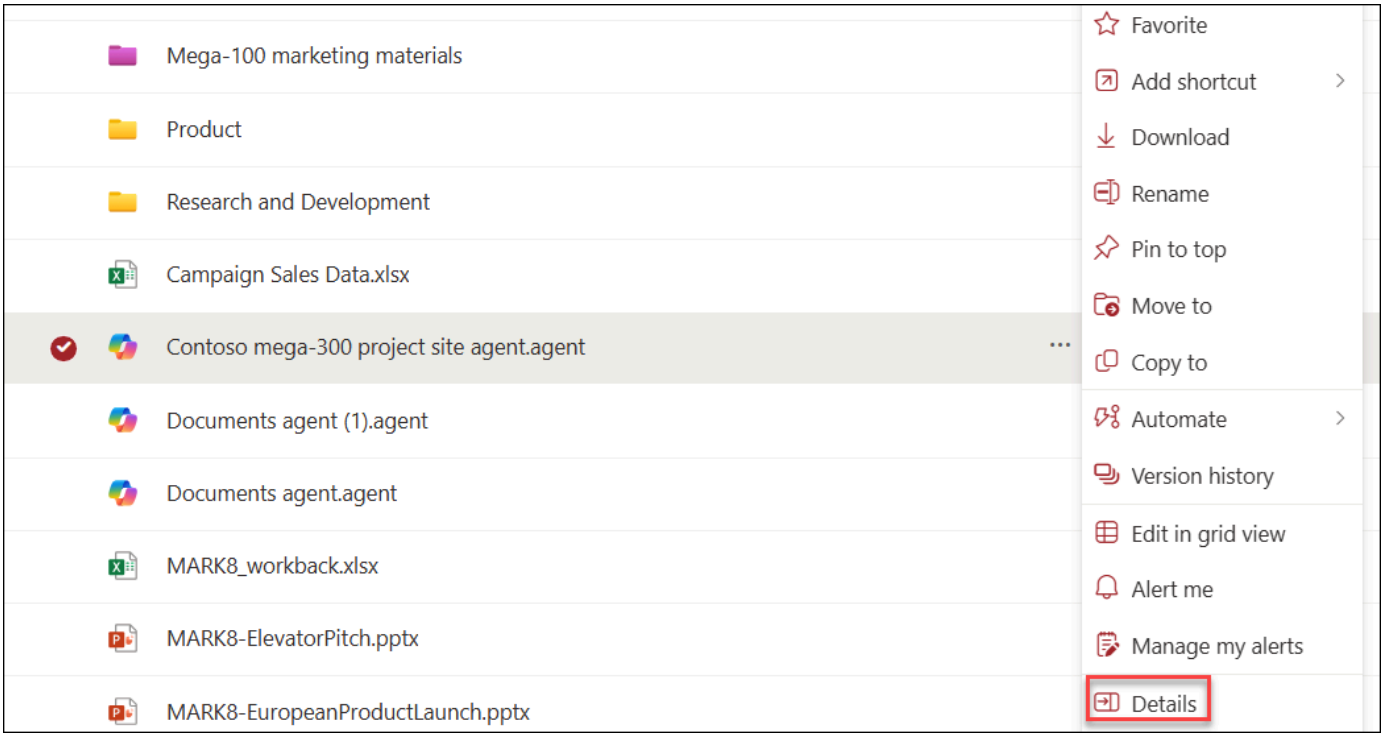
such as Restricted Content Discovery and Restricted Access Control associated with a particular site.

These tools align with user roles and permissions, enabling monitoring and management of agent activities in SharePoint. The following section provides additional details on how each tool functions and how you can use them effectively.

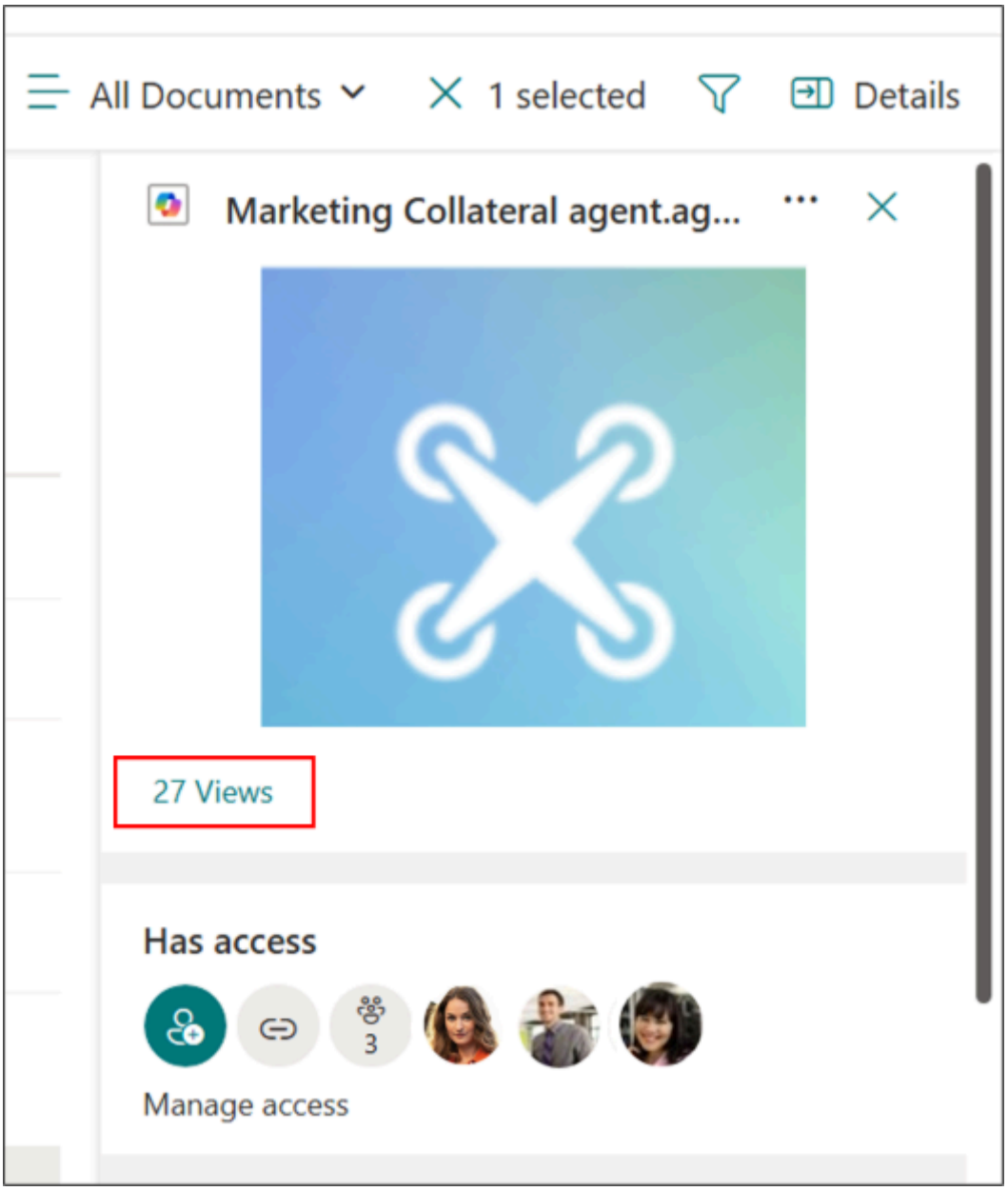
Monitor agent usage with at least site visitor permissions

Check individual agent file usage with File Statistics

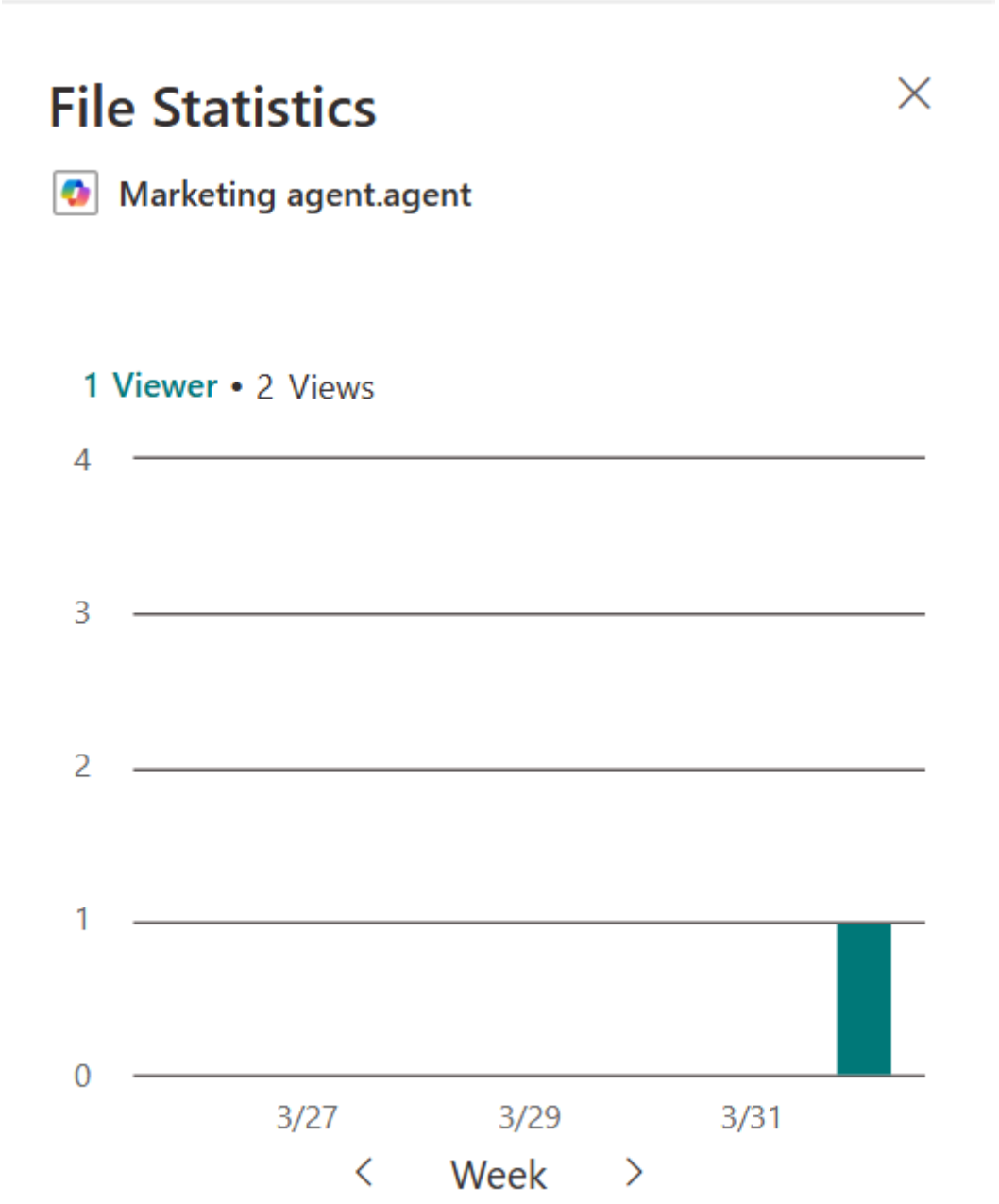
Every agent you create in SharePoint is a `.agent` file saved in the location where you create it. Users with view permission to the file can check the `.agent` file's usage by using File Statistics. File Statistics is one of the file insights available from the file card or details/info pane. To check the `.agent` file's file statistics, select the `.agent` file, and then select **Details** to see the number of views and unique viewers.



In the Details pane, select the view count to review comprehensive information about the usage of the `.agent` file.

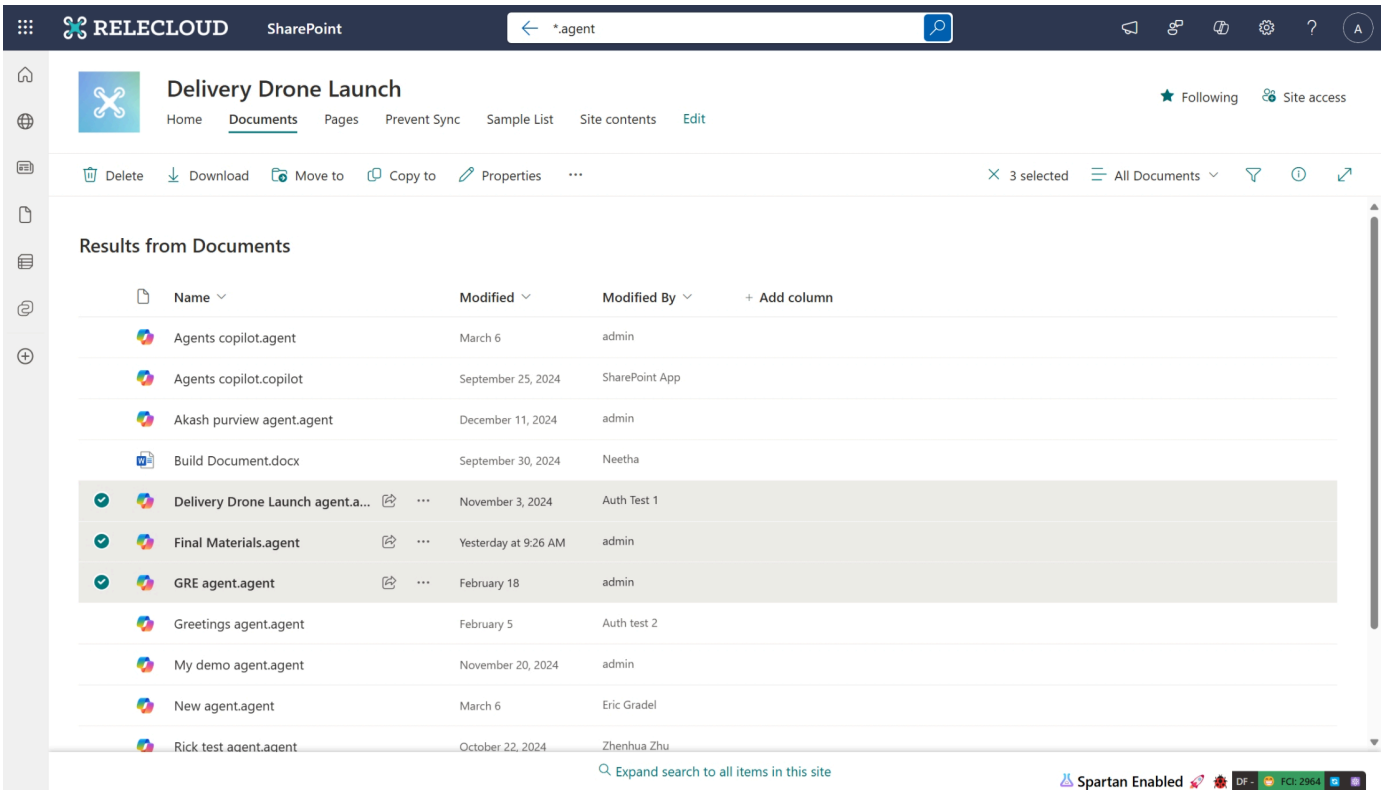


You can check the agent file's usage by weekly **Viewers** or **Views**:



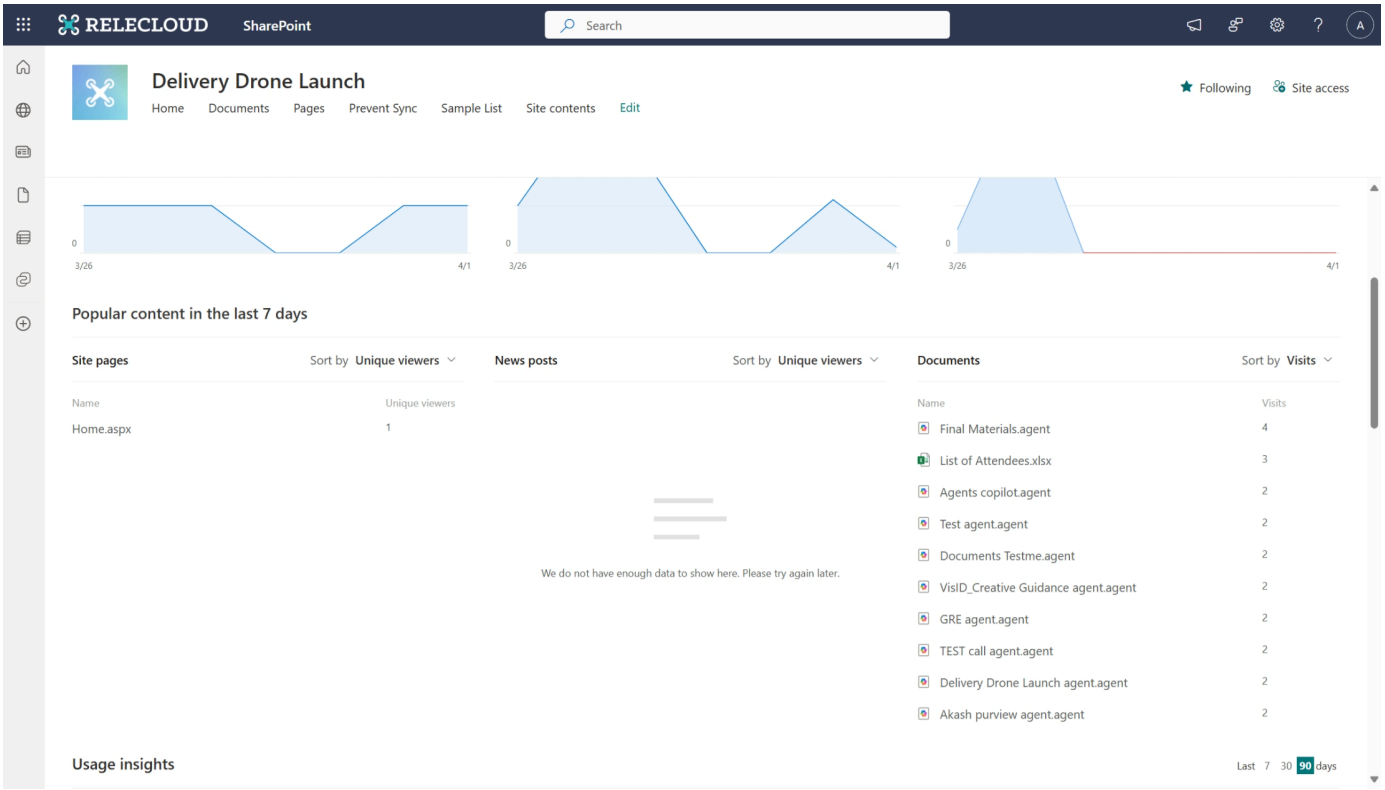
Use Search to find all agents for bulk actions

SharePoint users can locate all agents in a specific container, like a document library, site, or even across the entire organization, by searching for files with the `.agent` extension. By searching for `*.agent`, you find all agent files within the selected scope. The results only include agent files that you have permission to access. For site owners and members, this method is a convenient way to find agents and take bulk actions as needed.



See the list of the most popular agents with Site usage

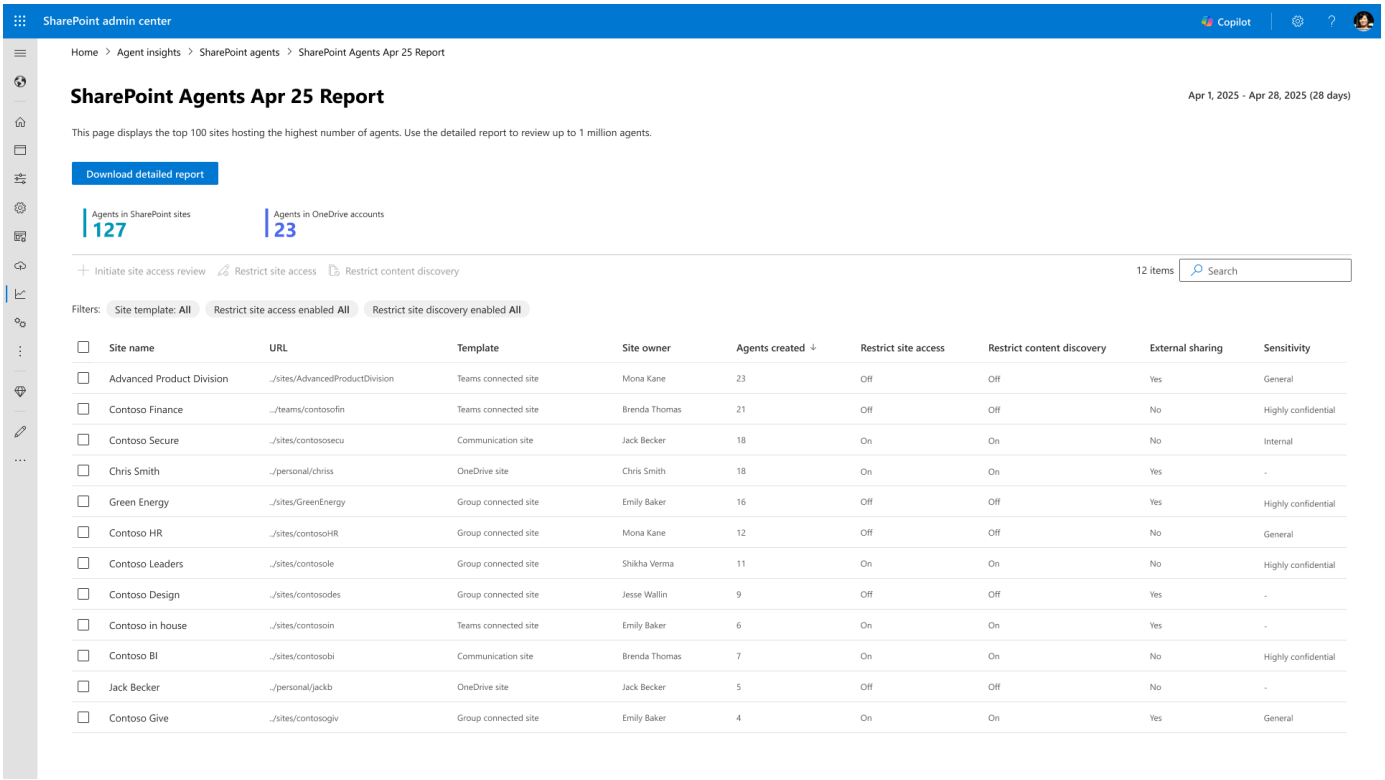
Site admins, owners, members, and visitors can view site usage data, which includes a list of popular files on the sites. Popular content in the last seven days includes `.agent` files along with other content. You can sort the list of popular files and agents by visits or unique visitors. To view usage data for your site, select the settings gear and then select **Site usage**. Based on your site navigation settings, you might also access the **Site contents** option from the left-hand menu. Then select the **Site usage** option in the top navigation bar.



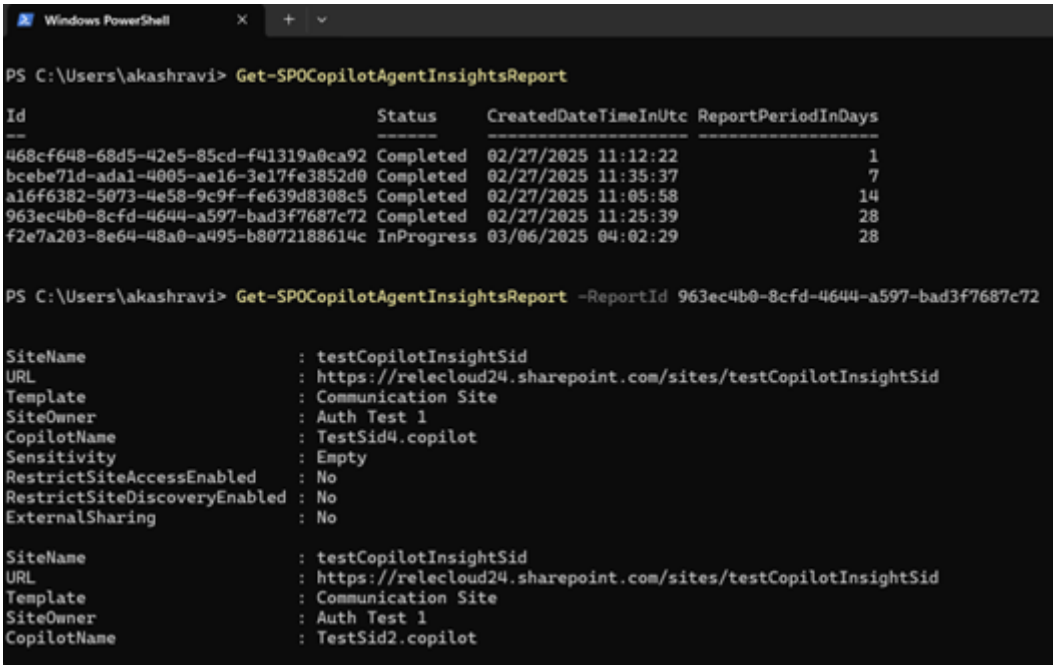
Monitor agent usage as SharePoint admins

Use agent reports on SharePoint Advanced Management

The Agent Insights report gives SharePoint admins detailed visibility into newly created agents across all SharePoint and OneDrive sites within their organization. This report helps you identify which sites have the highest number of agents, so you can better oversee and manage the content these agents use as grounding data, ensuring content integrity and governance. You can generate these reports from the SharePoint Admin Center or use PowerShell cmdlets.



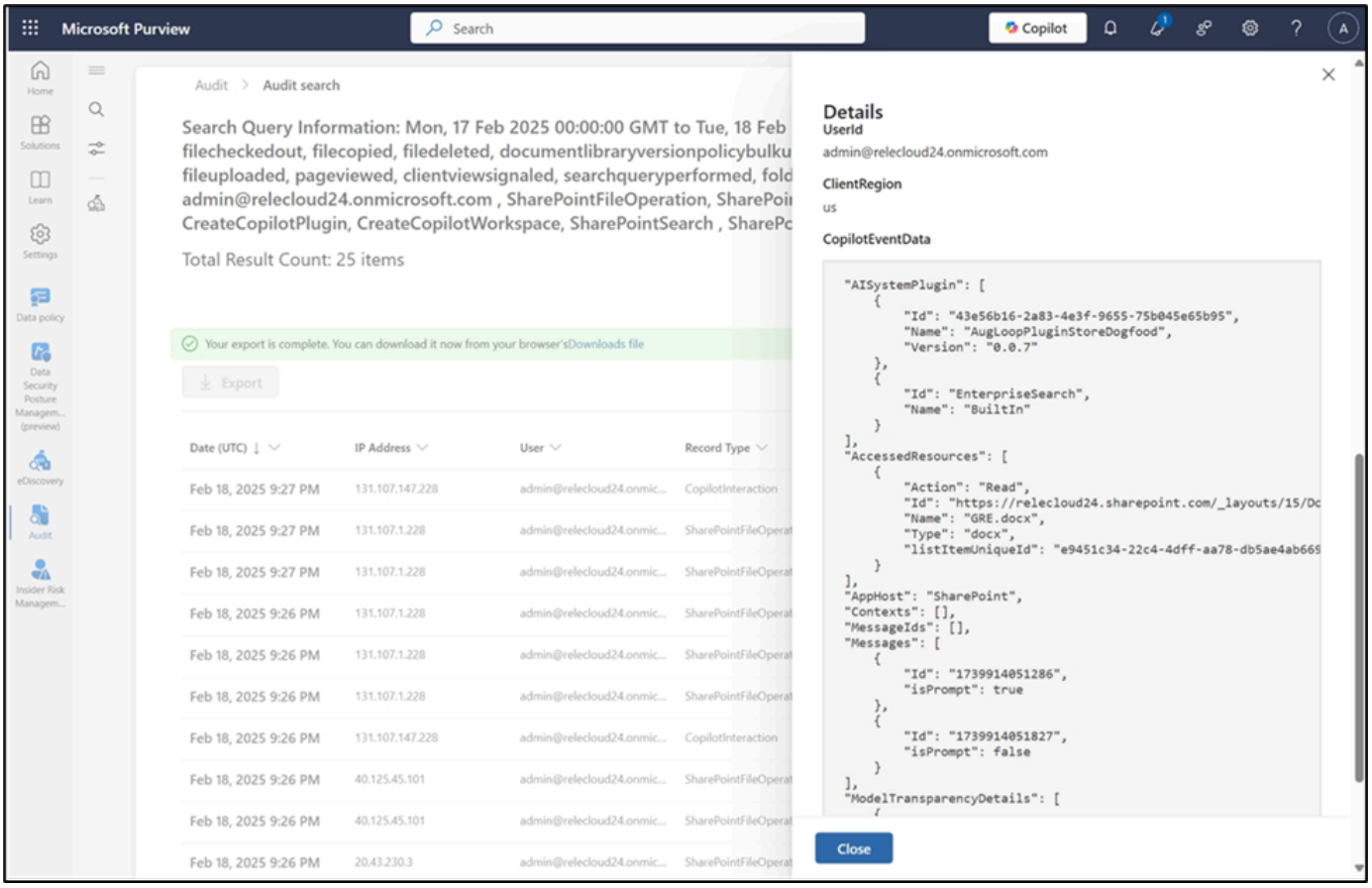
Site name	URL	Template	Site owner	Agents created	Restrict site access	Restrict content discovery	External sharing	Sensitivity
Advanced Product Division	../sites/AdvancedProductDivision	Teams connected site	Mona Kane	23	Off	Off	Yes	General
Contoso Finance	.../teams/contosofin	Teams connected site	Brenda Thomas	21	Off	Off	No	Highly confidential
Contoso Secure	../sites/contososecu	Communication site	Jack Becker	18	On	On	No	Internal
Chris Smith	../personal/chriss	OneDrive site	Chris Smith	18	On	On	Yes	-
Green Energy	../sites/GreenEnergy	Group connected site	Emily Baker	16	Off	Off	Yes	Highly confidential
Contoso HR	../sites/contosoHR	Group connected site	Mona Kane	12	Off	Off	No	General
Contoso Leaders	../sites/contosole	Group connected site	Shikha Verma	11	On	On	No	Highly confidential
Contoso Design	../sites/contosodes	Group connected site	Jesse Wallin	9	Off	Off	Yes	-
Contoso in house	../sites/contosoin	Teams connected site	Emily Baker	6	On	On	Yes	-
Contoso BI	../sites/contosobi	Communication site	Brenda Thomas	7	On	On	No	Highly confidential
Jack Becker	../personal/jackb	OneDrive site	Jack Becker	5	Off	Off	No	-
Contoso Give	../sites/contosogiv	Group connected site	Emily Baker	4	On	On	Yes	General



Unless you grant explicit roles, regular site owners can't run these reports. The output report might include agent files that the site owners and site admins don't have access to. From the list, admins can go to the site, search for the agent file, and take actions as needed. They might need to grant access to themselves.

Use Microsoft Purview audit log to monitor agent creation and usage details

Users with at least Compliance admin permissions with access to Purview can track agent creation and usage details. In addition to all file operation audits, the logs include which users interacted with the agent, and where and when the interaction took place. Audit records also include references to files, sites, or other resources Copilot and AI applications accessed to generate responses to users' instruction.



Microsoft is prioritizing delivering even richer analytics across Copilot Analytics dashboard, Microsoft 365 Admin Center, SharePoint Advanced Management, and SharePoint Online in the coming months.

Use Microsoft Cost Management to monitor the cost of agent usage

SharePoint admins can use Microsoft Cost Management to monitor the cost of agent usage at the organization level. To monitor your organization's consumption of agents by using the pay-as-you-go model, create a budget in Microsoft Cost Management by using Bicep and ARM template. A budget helps you inform others about their spending to proactively manage costs and monitor how spending progresses over time. You can also set up various types of cost alerts to monitor the consumption. Furthermore, you can view your organization's consumption by:

1. Going to Microsoft Cost Management.
2. If needed, changing the scope to select the subscription that is being used for agents in SharePoint.

Last updated on 07/29/2026

Get started with Copilot in SharePoint

Copilot in SharePoint brings agentic capabilities into SharePoint so teams can ask questions, run workflows, and create sites, pages, interactive reports, and Office files from their SharePoint content using natural language. Videos, prompt guides and other getting started materials are available here.

Copilot in SharePoint is currently in public preview. General availability begins rolling out on September 30, 2026. Capabilities may appear in your tenant after that date as rollout progresses.

> **Important**
>
> Two things change at general availability:
>
> - **Availability controls.** The PowerShell cmdlets used to opt tenants and sites in or out during preview are being retired. Existing settings are honored until November 1, 2026. Learn how to manage availability here.
> - **Advanced work with Copilot Credits** New agentic capabilities and the ability to work at greater scale than was possible in preview are being added to Copilot in SharePoint. These are called advanced work and use Copilot Credits through usage-based billing.

The everyday Copilot in SharePoint capabilities that have been in public preview stay included with the Microsoft 365 Copilot license.

Prerequisites

To use Copilot in SharePoint:

- **Microsoft 365 Copilot license.** Users must have an active Microsoft 365 Copilot license. Everyday Copilot in SharePoint capabilities are included with this license at no extra cost, and no opt-in step is required.

To use advanced work in Copilot in SharePoint:

- **Enable usage-based billing.** To use advanced capabilities or to work at greater scale, users need usage-based billing enabled through a spending policy in the Microsoft 365 admin center and available Copilot Credits.

- **Set up site-level enablement for site-wide real-time Autofill.** For site-wide, real-time metadata autofill, usage-based billing must also be enabled for the SharePoint site.

Licensing and Copilot Credits

Copilot in SharePoint uses a hybrid business model. Everyday individual productivity is included with the Microsoft 365 Copilot license. Advanced work requires usage-based billing and consumes Copilot Credits.

For most users, the experience is unchanged from preview. Users with Copilot credits are asked to confirm before moving into advanced work that spends Copilot credits.

Expand table

	Included with the Microsoft 365 Copilot license	Requires Copilot Credits
Value	Understand, create, and organize content	Automate and operate content at scale
When to use it	Understand and create content across files, pages, lists, and libraries. Copilot in SharePoint works with your content—answering questions, drafting what's next, and organizing as you go.	Automation across large sets of content and content estates. Hand the job to Copilot when it spans more content than you can work through yourself, needs to run on its own, or has to keep pace as content arrives.
Capabilities	• Ask questions, find content, and catch up • Create HTML, Word, Excel, or PowerPoint files • Create and edit pages, libraries, or lists • Create simple rules, approvals, and deterministic workflows • Rename and share individual files • Create and manage skills • Use Autofill metadata	• Work across large or unbounded content sets, including large-scale synthesis and document review • Create entire sites and solutions • Create and edit files, pages, libraries, and lists at scale • Build multistep, complex AI workflows, such as skills in scheduled AI automations • Use real-time Autofill metadata • Generate new images in document libraries and pages, and edit existing ones • Get analytics on how sites, pages, news, and documents are performing

Copilot Credit consumption varies based on the type and complexity of the task and nature and volume of the content involved. For examples of credit scenarios, see the Copilot Credits Guide.

Set up usage-based billing

Copilot in SharePoint uses the same Copilot Credits cost-management experience as other advanced AI workloads. It doesn't introduce a separate administration model. Details on usage-based billing and cost management are here.

For most organizations, an admin action is required before anyone can use advanced capabilities.

1. In the Microsoft 365 admin center, go to **Copilot** > **Cost management**.
2. Select **Add spending policy** and give the policy a name.
3. Under **Access scope**, choose whether the policy applies to all users or to specific security groups.
4. Under **Agents and services**, select **Advanced work in SharePoint**.
5. Set **Limits and alerts** for the policy, choose a **Billing method**, then review and add the policy.

Notes:

- Admins who are new to Copilot Credits need to create a cost management policy.
- Existing cost management policies might automatically include newly available services if the **Allow new agents and services as they become available** option is turned on for the policy. Review your existing policies to check this setting.

Decide who needs Copilot Credits

You don't need to enable usage-based capabilities for every SharePoint user. Prioritize people who manage sites and content at scale:

- **Content managers**—prioritize for credits. Examples include knowledge managers, records managers, paralegals, compliance analysts, and library services coordinators who curate, classify, and process content across large collections or on an ongoing basis.
- **Site managers**—prioritize for credits. Examples include SharePoint administrators, digital workplace managers, intranet managers, and collaboration platform leads who create or update sites at scale and enable site-wide processing.
- **Content creators**—assign based on need. Everyday content creation is included, but high-volume or repeatable creation might require advanced capabilities.
- **All other SharePoint users**—likely do not need credits. Everyday individual productivity scenarios remain included with the Microsoft 365 Copilot license.

What users see

- **For most users, the experience is unchanged from preview.** Copilot Credits aren't required for everyday productivity tasks.
- **Users with credits are asked to confirm.** When a prompt requires an advanced capability, or crosses the threshold of working at scale, Copilot asks the user to approve credit use before continuing. The UI then indicates that credits are being spent for that session.
- **Users can check credit usage.** Prompting `/cost` shows how many credits a task used and how much of the monthly limit remains, including when the limit resets.
- **Users are warned before running out.** When 20% of the monthly credit limit remains, Copilot notifies the user that usage-based features pause until the next month when the limit is reached. Users can request more credits from that prompt.
- **Users without credits see a graceful stop.** If a prompt requires an advanced capability and the user doesn't have Copilot Credits, Copilot explains what it can't complete. If a task crosses the working-at-scale threshold, Copilot completes what it can, then asks the user to start a new chat session.

Language support

Copilot in SharePoint supports only languages that appear in **both** the SharePoint Online supported language list and the Microsoft Copilot supported language list.

- Languages supported by SharePoint
- Languages supported by Microsoft Copilot

> **Note**
>
> For best results, use a supported language for your prompts. Copilot in SharePoint isn't tested or validated for languages outside the supported list, and results might vary.

Models

Copilot in SharePoint currently runs on a Microsoft-managed reasoning model from OpenAI. Microsoft selects and manages the model, and the specific model might change over time as the service adopts newer models. You don't need to configure a model to use Copilot in SharePoint.

Usage limits

The weekly limits that applied during public preview are removed at general availability.

In rare cases, daily service protection limits may still apply for Copilot licensed users to help ensure fair access for everyone. If a user reaches a service protection limit, Copilot features in SharePoint are temporarily unavailable until the limit resets.

Manage Availability of Copilot in SharePoint

Site AI settings

The **Site AI settings** panel lets site owners manage how users interact with AI on their site, including Copilot in SharePoint. Owners can:

- Choose which agent opens from the agent icon on the global header—either Copilot in SharePoint or a custom agent.
- Hide the Copilot button on site pages for site visitors only.
- Enable advanced document processing for the site.

To open the panel, go to **Settings** > **Site AI**.

Restricted Content Discovery

Restricted Content Discovery is an existing setting that's respected. If it's enabled on a site, Copilot in SharePoint and AI actions don't appear on that site. This rule applies regardless of your other availability settings.

Retirement of the preview PowerShell controls

PowerShell controls were previously used to manage availability of Copilot in SharePoint. With the transition from public preview to general availability, Copilot in SharePoint is retiring the PowerShell commands used to opt tenants and sites in or out during preview—`KnowledgeAgentScope`, `KnowledgeAgentSelectedSitesList`, and `KnowledgeAgentSelectedSitesListOperation`.

- Existing PowerShell settings continue to be honored until **November 1, 2026**.
- After November 1, 2026, manage availability using Site AI settings and Restricted Content Discovery.

Powershell controls details

Use the existing `KnowledgeAgent` parameters in `Set-SPOTenant` to manage availability across all sites, selectively include sites, or selectively exclude sites.

For multigeo tenants, run the PowerShell script in each geo. Note that the underlying PowerShell parameter names, such as `KnowledgeAgentScope`, retain the preview naming for compatibility. Although the feature is now described as Copilot in SharePoint, the parameter names remain unchanged.

Use the SharePoint Online Management Shell version 16.0.26615.12013 or later to manage access to Copilot in SharePoint for users with Copilot licenses. For setup instructions, see Get started with SharePoint Online Management Shell.

If you already have the SharePoint Online Management Shell installed, make sure you're running the latest version by running the following command in administrative mode: `Update-Module -Name Microsoft.Online.SharePoint.PowerShell`.

To resolve versioning errors

If you get the following error, it might indicate that you have multiple or conflicting versions of the SharePoint Online Management Shell installed:

```
Set-SPOTenant : A parameter cannot be found that matches parameter name 'KnowledgeAgentScope'
```

To resolve the issue, follow these steps:

1. Remove the conflicting SharePoint modules. Open **Add or remove programs**, and search for *SharePoint*. Uninstall any SharePoint admin modules you find.

2. Check the installed modules by running the following command:

   ```
   Get-Module -Name *SharePoint* -ListAvailable
   ```

   If multiple versions are listed, remove them by running:

   ```
   Uninstall-Module -Name <ModuleName>
   ```

3. Manually delete the remaining modules. If you encounter exceptions during uninstall, use this command to locate the module path:

   ```
   (Get-Module -Name *SharePoint* -ListAvailable).Path
   ```

   Go to the parent folder and manually delete it.

4. Restart PowerShell. Close the terminal and reopen it to clear any modules loaded in memory.

5. Repeat cleanup. Repeat steps 2 and 3 until no SharePoint Online PowerShell modules remain.

6. To install the latest SharePoint Online PowerShell module, run:

   `Install-Module -Name Microsoft.Online.SharePoint.PowerShell`

   > **Note**
   >
   > To verify the installed version, use the following command:
   >
   > `(Get-Module -Name Microsoft.Online.SharePoint.PowerShell -ListAvailable).Version`
   >
   > If multiple versions appear, repeat the previous cleanup steps.

Manage availability for specific sites

KnowledgeAgentScope

- **Description**: Administrators use KnowledgeAgentScope to control which SharePoint sites have access to Copilot in SharePoint.

- **Valid values**:
  - `AllSites`: Copilot in SharePoint is available on all sites.
  - `IncludeSelectedSites`: Copilot in SharePoint is available only on sites specified in KnowledgeAgentSelectedSitesList.
  - `ExcludeSelectedSites`: Copilot in SharePoint is available on all sites except those specified in KnowledgeAgentSelectedSitesList.
  - `NoSites`: Copilot in SharePoint isn't available on any sites. (This is the default value.)

- **Note**: Requires Microsoft Copilot license.

KnowledgeAgentSelectedSitesList

- **Description**: Administrators use KnowledgeAgentSelectedSitesList to pass a list of SharePoint site URLs to include or exclude from Copilot in SharePoint.

- When `KnowledgeAgentScope` = **ExcludeSelectedSites**: the list is treated as sites to **EXCLUDE** (site opt-out list).
  - When `KnowledgeAgentScope` = **IncludeSelectedSites**: the list is treated as sites to **INCLUDE** (site opt-in list).

- By default, this list overwrites any existing list.
- You can only call this parameter when `KnowledgeAgentScope` is set to `IncludeSelectedSites` or `ExcludeSelectedSites`.
- The list of site URLs can't exceed 100 items.
- **Note**: Requires Microsoft Copilot license.

KnowledgeAgentSelectedSitesListOperation

- **Description**: KnowledgeAgentSelectedSitesListOperation specifies the operation to perform on the current sites list.
- **Valid values**:
  - `Overwrite`: Overwrite the existing sites list (default).
  - `Append`: Append the input list of sites to the existing sites list.
  - `Remove`: Remove the input list of sites from the existing sites list.
- **Note**: Calling this parameter without `KnowledgeAgentSelectedSitesList` has no effect.

Examples

Make Copilot in SharePoint available on all sites

PowerShell

```
# Connect to SharePoint Online admin center
Connect-SPOService https://yourtenant-admin.sharepoint.com

# Make Copilot in SharePoint available for all sites in the tenant
Set-SPOTenant -KnowledgeAgentScope AllSites

# Verify the configuration
Get-SPOTenant | Select-Object KnowledgeAgentScope
```

Make Copilot in SharePoint available on specified sites only

PowerShell

```
# Connect to SharePoint Online admin center
Connect-SPOService https://yourtenant-admin.sharepoint.com

# Make available only on the included sites
Set-SPOTenant -KnowledgeAgentScope IncludeSelectedSites
```

```
# Specify sites to include (initial inclusion list)
Set-SPOTenant -KnowledgeAgentSelectedSitesList
@("https://yourtenant.sharepoint.com/sites/site5",
"https://yourtenant.sharepoint.com/sites/site7")

# Add additional sites to the existing inclusion list (if needed)
Set-SPOTenant -KnowledgeAgentSelectedSitesList
@("https://yourtenant.sharepoint.com/sites/site3") -
KnowledgeAgentSelectedSitesListOperation Append

# Verify the inclusion configuration
Get-SPOTenant | Select-Object KnowledgeAgentScope, KnowledgeAgentSelectedSitesList
```

Opt out specific sites (available on all sites except those listed)

PowerShell

```
# Connect to SharePoint Online admin center
Connect-SPOService https://yourtenant-admin.sharepoint.com

# Make available on all sites except selected sites
Set-SPOTenant -KnowledgeAgentScope ExcludeSelectedSites

# Specify sites to exclude (initial exclusion list)
Set-SPOTenant -KnowledgeAgentSelectedSitesList
@("https://yourtenant.sharepoint.com/sites/site1",
"https://yourtenant.sharepoint.com/sites/site2")

# Add additional sites to the existing exclusion list (if needed)
Set-SPOTenant -KnowledgeAgentSelectedSitesList
@("https://yourtenant.sharepoint.com/sites/site3") -
KnowledgeAgentSelectedSitesListOperation Append

# Verify the exclusion configuration
Get-SPOTenant | Select-Object KnowledgeAgentScope, KnowledgeAgentSelectedSitesList
```

Turn off Copilot in SharePoint for the tenant

PowerShell

```
# Connect to SharePoint Online admin center
Connect-SPOService https://yourtenant-admin.sharepoint.com

# Turn off Copilot in SharePoint for all sites
Set-SPOTenant -KnowledgeAgentScope NoSites

# Verify it is turned off
Get-SPOTenant | Select-Object KnowledgeAgentScope
```

> **Note**
>
> Microsoft 365 Government—GCC, GCC High, DoD, Office 365 air-gapped cloud environments, and Microsoft 365 operated by 21Vianet don't currently support Copilot in SharePoint.

Last updated on 09/25/2026

Create document library with AI

By using Copilot in SharePoint to create a document library, you can go from a simple description to a well configured, metadata-rich document library. Instead of manually creating a library, defining columns, and setting up tagging rules, describe what the library is for and optionally provide a sample file. Copilot in SharePoint then generates the library name, description, and a complete metadata schema - with columns that automatically tag new documents as they're added.

This feature is useful for organizations that need to quickly create well-organized document libraries, such as:

- **Finance and accounting:** Invoice repositories, expense report libraries, financial statement archives.
- **Legal and compliance:** Contract libraries, regulatory filing repositories, policy document collections.
- **Project management:** Project deliverable libraries, product specs, milestone documentation.
- **Human resources:** Employee records libraries, benefits documentation, training material collections.

How AI-powered library creation works

The library creation process uses AI to handle the setup that would otherwise require manual configuration by a site owner or content manager.

1. **You describe the purpose:** Provide a natural language description of what the library is for, for example, "I need a library for vendor invoices."
2. **You provide a sample file (recommended):** Upload an example or seed file that represents the type of content to store. AI uses this file to better understand the document structure and suggest relevant metadata fields. If you don't provide a sample file, AI generates the library configuration from your description alone.
3. **AI generates the configuration:** Based on your description and sample file, AI proposes a library name, description, and a metadata schema with columns tailored to your type of document.
4. **AI creates and configures the library:** The library is created, your sample file is copied to the library if you provided one, and AI-powered columns are configured. These columns use prompts to extract metadata from supported files added to the library.

Prerequisites

1. Users must have a Microsoft Copilot license assigned.
2. Copilot in SharePoint is on by default for licensed users; no opt-in step is required. To control availability, see Get started with Copilot in SharePoint.
3. Users must have permissions to create document libraries on the SharePoint site.

Steps for creating a library with AI

1. From the site home page or site contents page, select **+ New** > **Document library**.
2. Select the AI-assisted creation process.
3. Describe the purpose of the library in the text field. For example:

    - "I need a library to store and organize vendor invoices."
    - "A library for marketing campaign assets and deliverables."
    - "Repository for employee onboarding documents."

4. Optionally, upload a sample file to help AI understand the structure of your documents. You can select a file from:

    - The current SharePoint site
    - A OneDrive location
    - Your local device

5. Review the AI-generated library configuration:

    - **Library name:** A descriptive name based on your input.
    - **Library description:** A summary of the library's purpose.

6. Select **Create** to confirm. AI creates the library, copies over your sample file, and configures the metadata columns.

AI-powered columns

When you create the library, it includes AI-powered columns based on the metadata schema generated from your description and sample file. These columns use prompts to extract and populate metadata from supported files.

- **Automatic tagging:** When you upload or drop documents into the library, AI reads the content and automatically populates the column values. You can review and update values as needed.

- **User control:** You can review the schema and the underlying prompts during creation and anytime after that.

Supported file types

AI-powered library creation uses the same underlying Autofill feature that reads document content and populates metadata values. This feature means the same file type compatibility applies to both the initial sample file you provide during library creation and to any documents you add to the library afterward.

Last updated on 09/25/2026

Create sites with AI

Copilot in SharePoint makes it faster and easier to create SharePoint sites and solutions using natural-language description. Copilot in SharePoint streamlines the process of building sites and solutions with natural language. Describe what you need, and AI will recommend a structure—including pages, lists, libraries, and more. You can review and adjust the AI-generated plan through chat before anything is created. Once you approve the plan, your site is set up in minutes, complete with sample data.

> **Important**
>
> **Create sites with AI** is still under preview.

> **Note**
>
> The site creation can take up to 15 minutes. Please don't close the browser while creation is progressing.

Prerequisites

Before you start, confirm the following:

1. **Enable Copilot in SharePoint (preview):** A SharePoint Administrator or Global Administrator must enable the preview for your tenant. Your tenant must have opted into the preview using the All Sites or Exclude Selected Sites config. If you have opted in with the Selected Sites or No Sites config, users in your organization won't be able to use this feature. For enablement steps and prerequisites, see Get started with Copilot in SharePoint.

2. Microsoft Copilot license. Users need an active Copilot license to use Create site with AI.

3. Users must be allowed to create SharePoint sites in your organization. To enable users create new sites, admins must enable self-service site creation.

> **Note**

If users aren't enabled for self-service site creation, SharePoint administrators can create sites with AI on behalf of users.

Key benefits

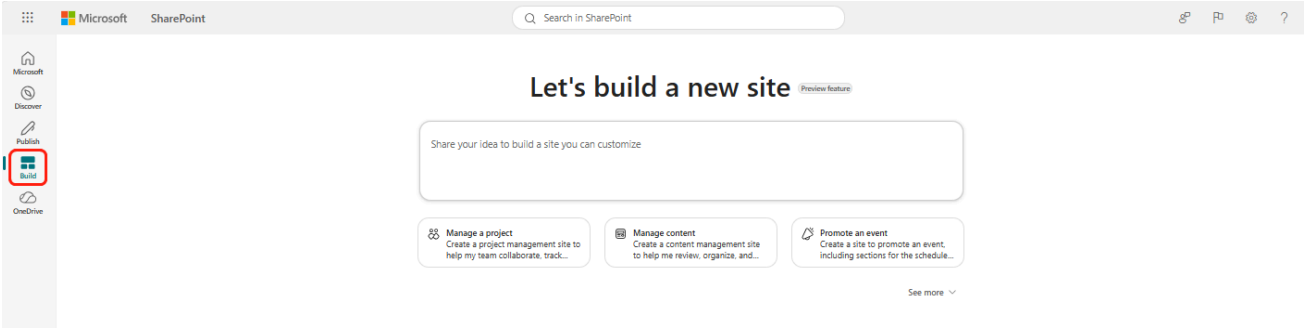
- **Plan with AI:** Describe what you need and get a proposed build plan (no SharePoint expertise required).
- **Review before you build:** Edit the outline (pages, lists, libraries) before anything is created.
- **Fast execution:** After approval, Copilot in SharePoint creates the site and configures content based on the build plan.
- **Ongoing refinement:** After the site is created, continue to use Copilot in SharePoint to improve pages, organize content, and get answers.

How to create sites with AI

The easiest way is to send prompts that include **create new site** keywords to Copilot in SharePoint. Copilot uses the prompts to build the site.

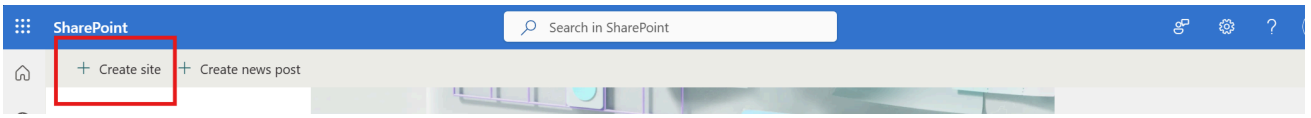
If your users have the new SharePoint experience (preview), follow these steps:

1. Select **Build** in the left navigation.
2. Then describe what you would like to build in the prompt box or select one of the suggested prompts.

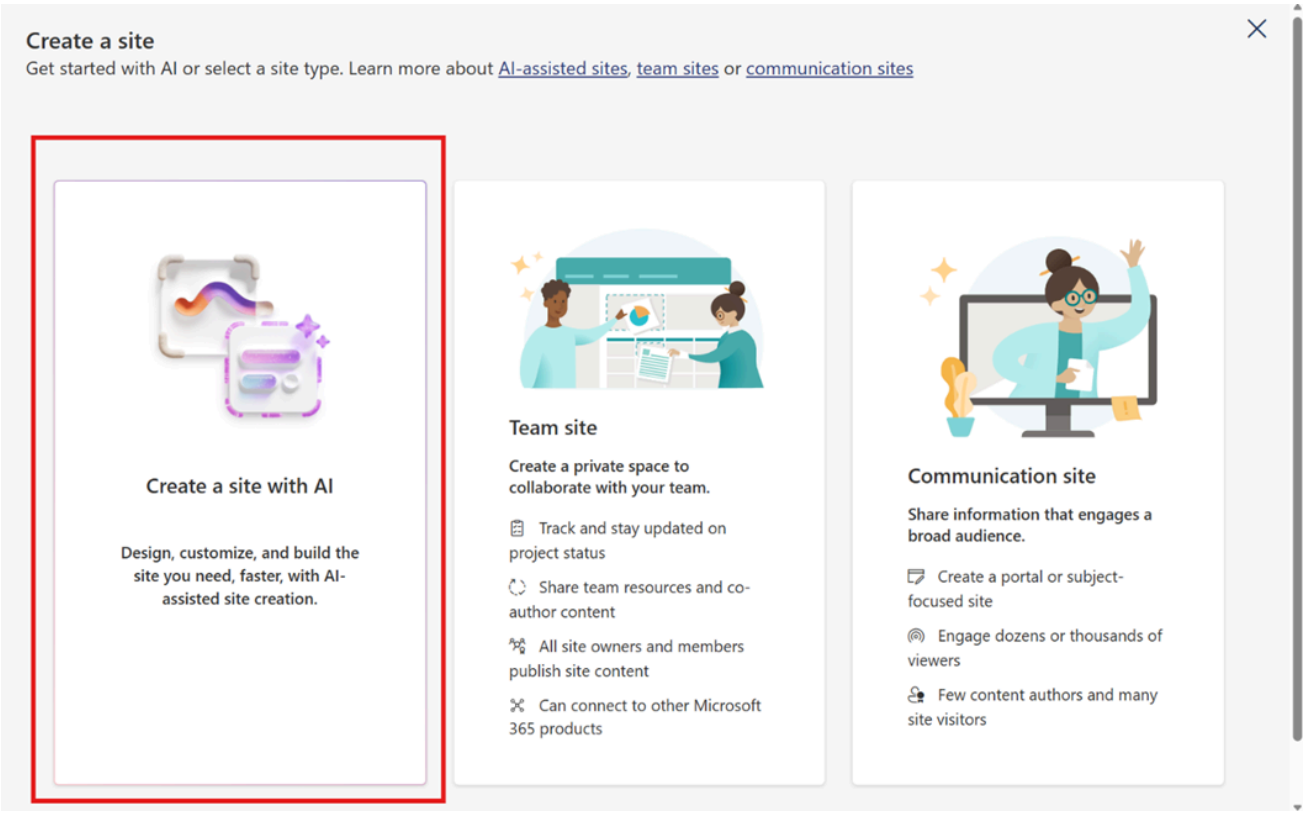


You can also start from the SharePoint start page.

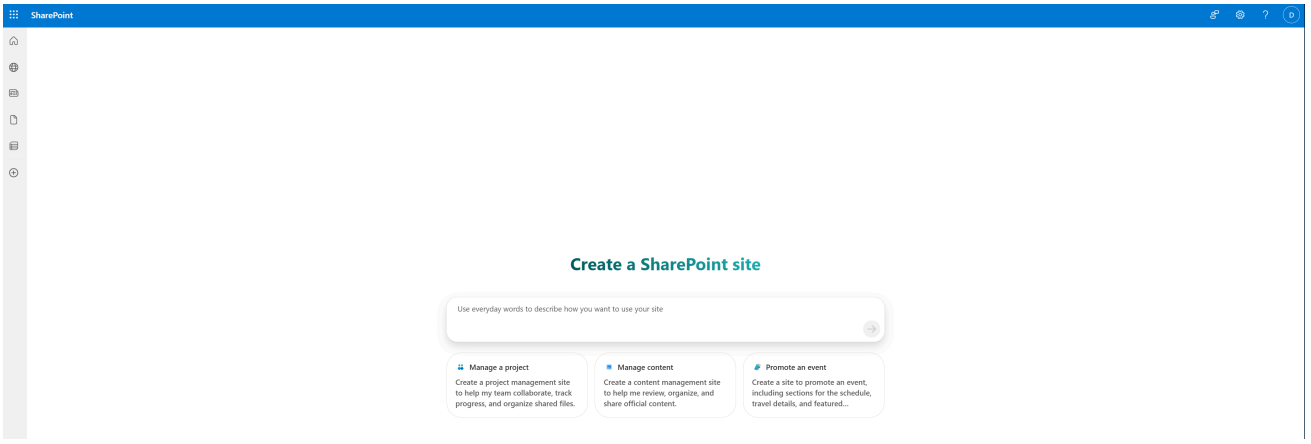
1. Navigate to the SharePoint start page to launch the experience.
2. From the SharePoint start page, follow these steps:
3. Select **Create site**.



4. In the **Create a site** dialog, select **Create a site with AI**.



5. Then describe what you would like to build in the prompt box or select one of the suggested prompts.



How it works

Create site with AI uses a planning mode that you can use to review the proposed build plan and the visual outline of pages, lists, and libraries before execution begins. The process doesn't create any assets until you formally approve the plan. The AI site-building process includes the following steps:

Step 1: Provide a natural language description

In the prompt box, enter a comprehensive description of the site you want to create. AI may ask follow-up questions to confirm details.

Example: "Create a site to help my team collaborate and track project progress."

You may be asked a few clarifying questions if more information is needed. In our example, the AI might ask follow-up questions, such as

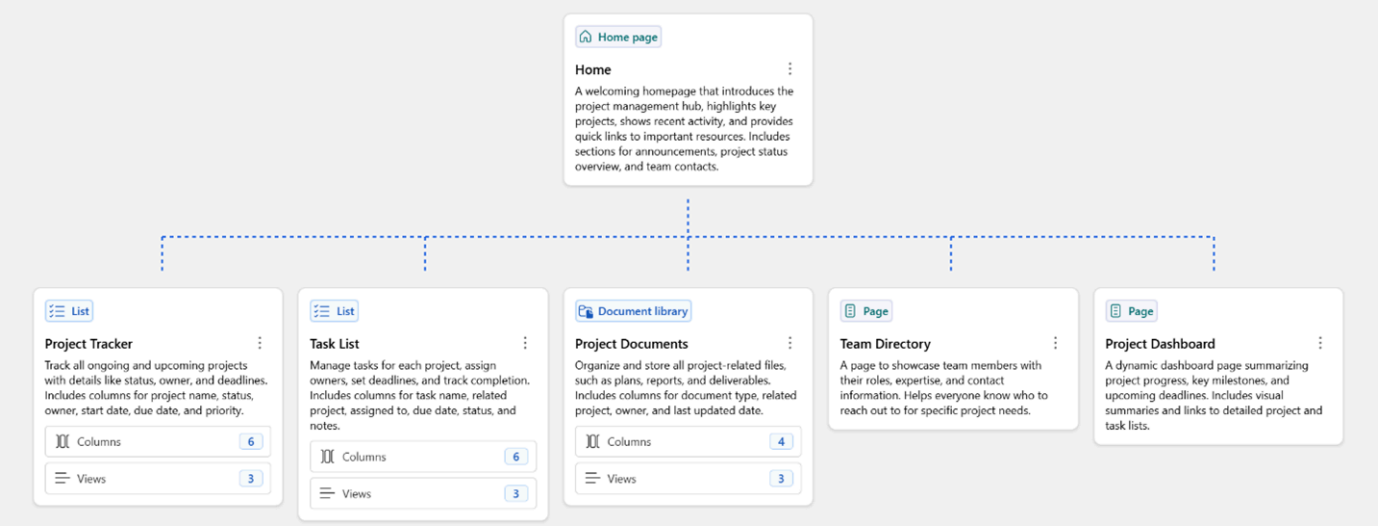
"*What kind of projects does your team work on? (e.g., marketing campaigns, software development, event planning, etc.)?"*

"Do you need to track tasks with deadlines and assignments, or is it more about tracking overall project status?"

Based on your description and answers to the clarifying questions, Copilot in SharePoint proposes an outline as well as a plan that can include pages, lists, libraries, columns, and views. These clarifying questions are necessary because they help the AI understand the purpose of your site and your specific requirements.

Step 2: Review the proposed plan and outline

Review the proposed plan and outline presented in the previous step to make sure it meets your needs. The visual outline shows the structure and description of each of proposed site component. The screenshot below shows an example of the visual outline.



You can reopen the preview by directly asking Copilot to reopen the preview in natural language.

Step 3: Refine the build plan through chat

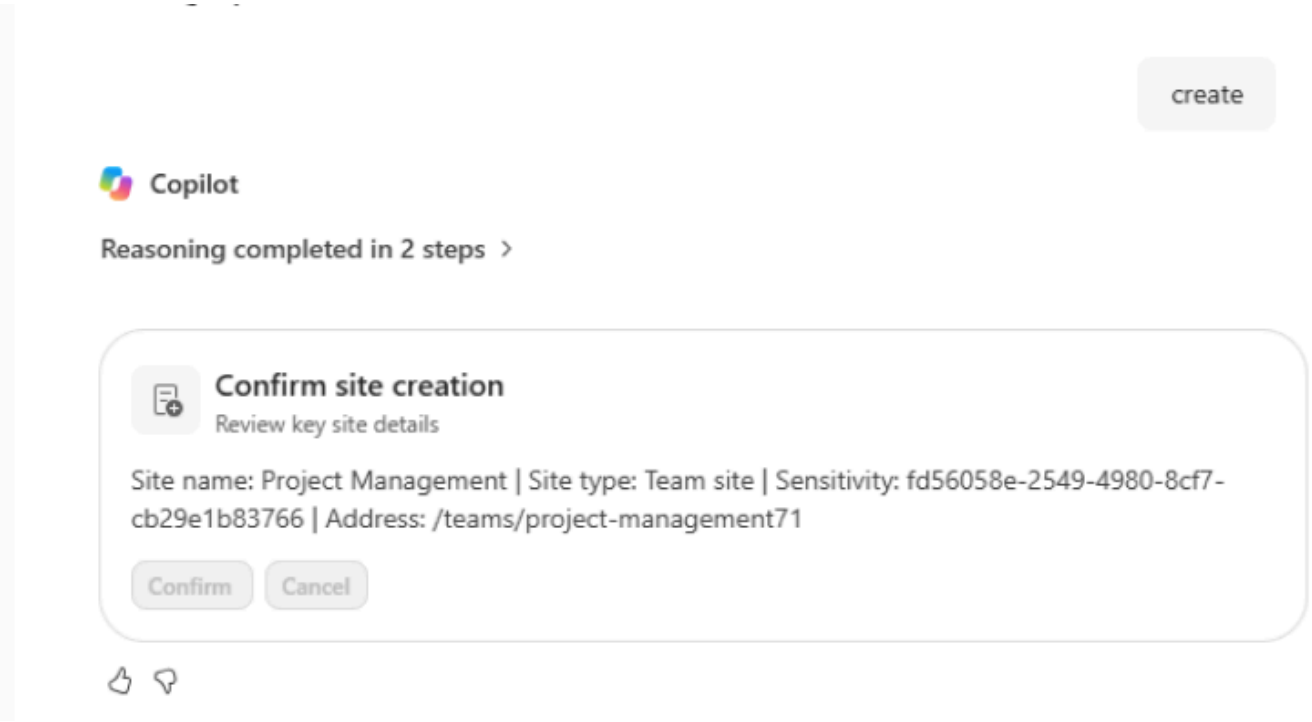
Use chat to answer clarifying questions and refine the plan. Refine the plan by adding or removing components, renaming pages, or updating list and library columns etc. Some examples of how to refine your plans include:

- *"Add a column for time estimate on the Tasks list."*
- *"Remove the Team overview page."*

The plan, including the visual outline, updates as you make changes. However, the process doesn't create anything until you send a **create** request and select the **Confirm** button in confirmation card. Copilot in SharePoint also surfaces recommendations to strengthen and enhance your solution, drawing on its understanding of common scenarios and what's typically needed to support them. If the plan is missing a component, rephrase your request or add it by using natural language.

Step 4: Create the site

When you're ready, send a **create** request in chat and select **Confirm**.



During execution, Copilot in SharePoint will follow the plan to:

1. Create the site.
2. Configure navigation and settings.
3. Create lists and libraries (columns, views, metadata).

4. Create pages with sample content.
5. Add sample documents and list items.

Execution can take up to 15 minutes to complete, depending on how many components are in your site. When execution completes, you'll see a confirmation and a link to navigate to your new site.

Step 5: Explore the new site and provided content

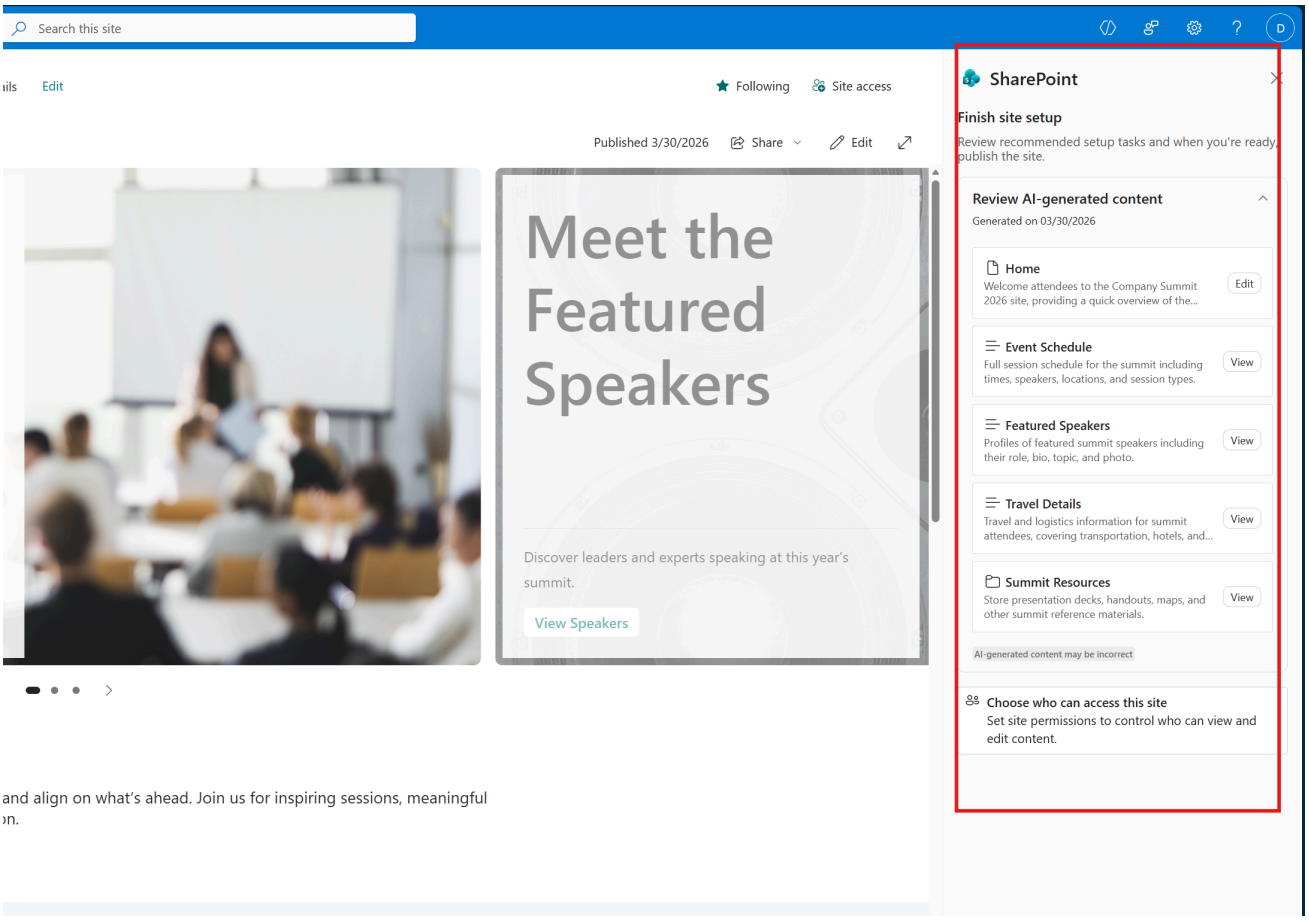
The new site includes sample content and structure, such as:

- **Pages** with sample content based on your scenario.
- **Libraries** with relevant names and columns and sample files.
- **Lists** with sample items so teams can understand the structure quickly.

Step 6: Post-creation refinement

After your site is created, Copilot in SharePoint remains available to help you continue refining, iterating, and configuring the site. When you land on the site homepage, a **Finish site setup** panel will appear. The panel:

- Provides a summary of what was created (pages, lists, libraries).
- Offers quick links to key site components.
- Recommends next steps such as sharing your site with others.



Learn more:

- Get started with Copilot in SharePoint

Unsupported Scenarios

During the preview, some SharePoint features and integrations aren't available. If you ask Copilot in SharePoint for something that isn't supported, you'll likely get a response during the planning phase that it can't automatically complete the task and may suggest to complete it manually after the site is created. A few unsupported features include complex Power Automate flows, permission and sharing set up, column and row formatting, advanced web parts, and third-party integrations.

Last updated on 09/28/2026

Create autofill columns

Copilot in SharePoint helps you automatically generate metadata for your document libraries using autofill columns.

The Create autofill columns capability analyzes files in the library and suggests metadata columns and extraction prompts. These columns automatically populate metadata from file content, helping organize libraries, improve discovery, and support automation scenarios.

Get suggested columns and metadata

To get suggested columns and metadata based on the first 20 files in your document library, follow these steps.

1. Launch the quick action.
2. Use a suggested prompt or enter a custom prompt.
3. Save your changes.

Launch the quick action

1. Select the Copilot in SharePoint icon in the lower-right corner of your document library.

2. From the quick actions menu, select **Create autofill columns**.

3. The chat panel opens and displays a list of suggested prompts related to the creation of columns.

   > **Note**
   >
   > If this is the first time using Copilot in SharePoint in the library, it will automatically suggest up to three columns based on the available files.

4. You can also request your own column in the chat panel.

Use a suggested prompt

1. From the chat panel, select an action. For this example, we use create autofill columns or add autofill columns.

2. In the chat box, review the instruction provided. If needed, you can modify the text to better suit your intent. Once you're ready, select **Send** to submit your action.

3. AI analyzes up to 20 recent files in the document library to generate column suggestions. These files are selected across supported file types (such as Office documents and PDF files) to provide representative analysis.

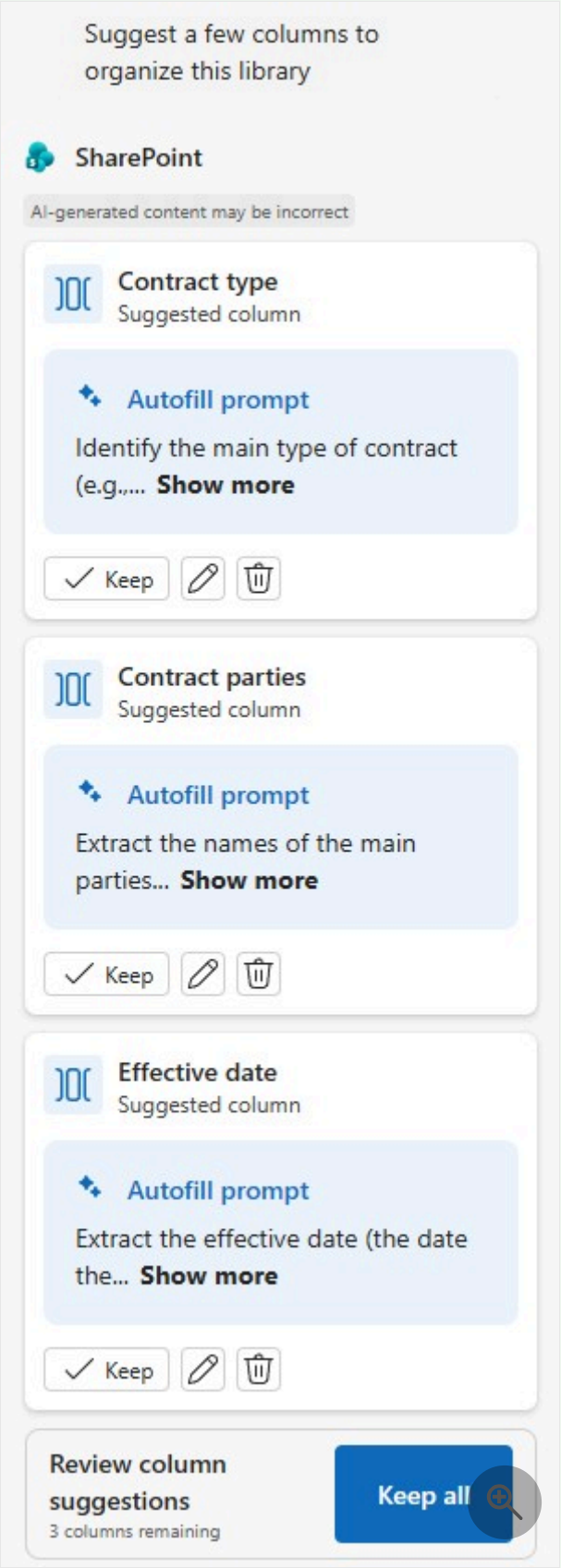
   If you select specific files before running Autofill, AI analyzes only the selected files.

   The suggested columns appear highlighted and marked as AI-generated. This might take a few moments.

Name	Contract type	Contract parties	Effective date
contracts_T1_F2.docx	Master services agreement	InfraBuild Holdings, Inc.; Nexus Enterprises, LLC	2024-06-14 00:00
contracts_T3_F2.docx	Employment agreement	InfraBuild Holdings; Ms. Isabella Chen	2025-08-06 00:00
contracts_T5_F2.docx	Partnership agreement	Axiom BioPharma; Catalyst Dynamics	Not found
contracts_T7_F2.docx	Lease agreement	Dr. Anya Petrova, CEO, BioInnovate; InfraBuild Holdings	Not found
contracts_T9_F2.docx	Supply agreement	InfraBuild Holdings; Industrial Raw Materials SA	Not found

Tip

The suggested column information is summarized in the chat panel.



4. Review the suggested columns and the associated metadata to make sure they're appropriate for your content.

5. To remove a suggested column:

- From the document library page, select the column name, and then select **Remove column**.
- From the chat panel, on the column card, select **Remove**.

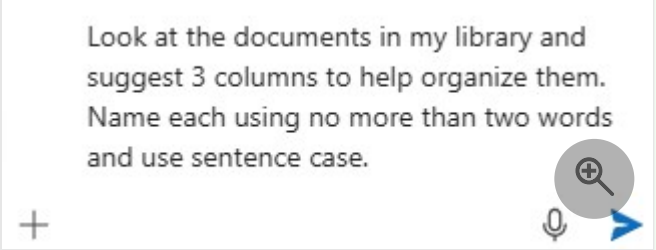
6. To rename the column or to refine the metadata in a suggested column:

   - From the document library page, select the column name, and then select **Edit column**.
   - From the chat panel, on the column card, select **Edit**.

7. On the **Edit column** panel, you can change the column name or modify the instruction that generates the metadata. After you edit the instruction, test it on up to 10 files to make sure it gives you the information you want. When you're done making changes for that column, select **Save**.

Enter a custom prompt

1. In the chat panel's text box, enter your own instruction.

   > **Tip**
   >
   > When requesting a column, be sure to specify a clear name and what type of information you would like to capture (for example, reason for document creation or project rationale), as well as any specifics around format and length. This helps ensure the column meets your needs.
   >
   > 
   >

2. Select **Send** to submit your action.

Save your changes

1. When you're ready to save all of the column changes, select **Save changes**.

2. On the **Save and apply your changes?** confirmation screen, verify that you want to update the current library view or save as a new view, and then select **Apply changes**.

   > **Tip**

> If you create a new view, it will be the name of the library appended with a numerical value. The naming experience will be improved in future updates, but for now you can rename the view from the library command bar.

3. You're returned to the updated library, and processing begins for up to the first 20 files in the library. You can verify and monitor the progress in the activity panel.

4. After these prompts are saved on a column, any new files uploaded to the library are automatically processed, and the extracted information is saved to the corresponding columns.

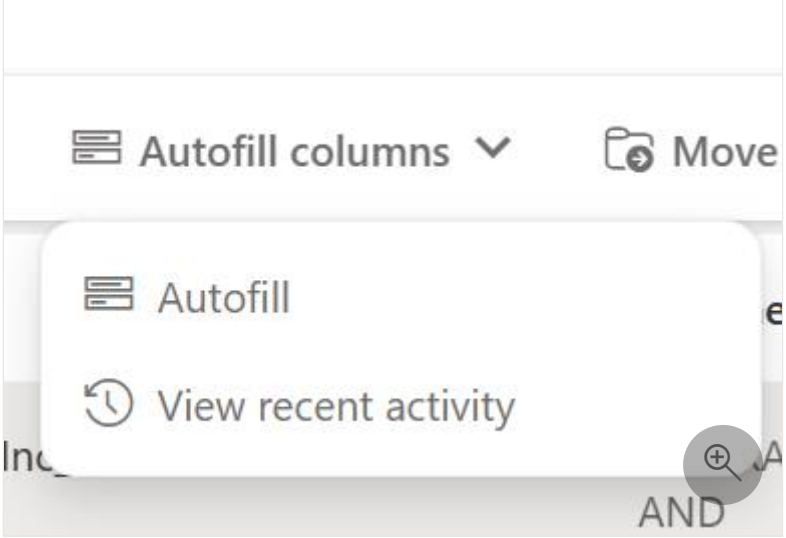
Newly uploaded files

After you save the changes and create autofill metadata columns for a library, all newly uploaded files are automatically processed with metadata. This applies regardless of whether the uploader has a Copilot license. Any new file added to the library will have metadata applied automatically.

All newly added files are also included as part of your Copilot benefits. Even if the library is connected to a pay-as-you-go meter, new files in this library are not charged at a pay-as-you-go rate and are instead covered by the Copilot license.

Apply changes to existing files

You can apply the same metadata logic to existing files in the library by selecting the files you want to process. Once selected, select the **Autofill** button to get documents processed and updated with metadata.



Advanced Autofill

Advanced Autofill uses Copilot Credits to process documents faster when you need additional processing capacity. It's available only to organizations that have turned on usage-based billing for Copilot in SharePoint.

Site admins can turn on Advanced Autofill for all site members by sharing their Copilot Credits with the site. Once turned on, Autofill uses advanced processing whenever it runs on the site.

If Copilot Credits are unavailable, Autofill uses the processing capacity included with each user's Microsoft 365 Copilot license until credits are available again.

Set up Advanced Autofill

Only site admins can change the Advanced Autofill setting.

To turn on Advanced Autofill on a SharePoint site:

1. On the SharePoint site, select **Settings**.
2. Open the **Site AI** panel.
3. Under **Advanced Autofill columns**, turn on **Share credits for advanced autofill columns**.

> **Note**
>
> Site admins can only share Copilot Credits from their own account.

Requirements and limitations

- **Supported file types:** .csv, .docx, .pdf, .xlsx, and other Microsoft 365-compatible formats.
- **Supported languages:** All languages supported through Microsoft Copilot for text-based prompts and responses, but can only process files in English.
- **Supported column types:** Text, Multiple lines of text, Number, Yes/No, Date and time, Choice, Hyperlink, Currency, and Managed metadata.
- **Limitations:**
  - Person or Group, Location, Image, and Lookup column types are currently unsupported.
  - For optimal performance, we recommend adding no more than 10 columns per library and processing files no larger than 65 pages.
  - Copilot in SharePoint can process files only, not folders. If files within a folder are used to configure the library, the configuration applies to the entire library.
  - Copilot in SharePoint processes up to 20 files during initial column configuration. To extract information from additional files, select the files and choose **Autofill columns** >

Autofill from the command bar. You can monitor progress by selecting **Autofill columns** > **View autofill activity**.

- If a managed metadata column type is used, it can only use the first 100 terms of a mapped term set. If a preferred term or synonym matches, the preferred term is saved to the column.
- Encrypted files cannot be analyzed, and their metadata is not included in the results. If encrypted files are present, they may appear as not processed.
- Copilot in SharePoint can configure document libraries only. The following library types aren't supported: FormServerTemplates, SitePages, Style Library, and SiteAssets.
- This service is available only for SharePoint sites — including hub sites, sites associated to a hub site, and the primary site of a site collection. Subsites aren't supported.

Last updated on 09/25/2026

Automate workflows in a SharePoint document library

Copilot in SharePoint enables you to set up automations in your document library by describing what you want to happen using natural language. You don't need to know technical terms or navigate complex menus. Simply describe your intent and an appropriate workflow rule is suggested and configured.

Launch the quick action

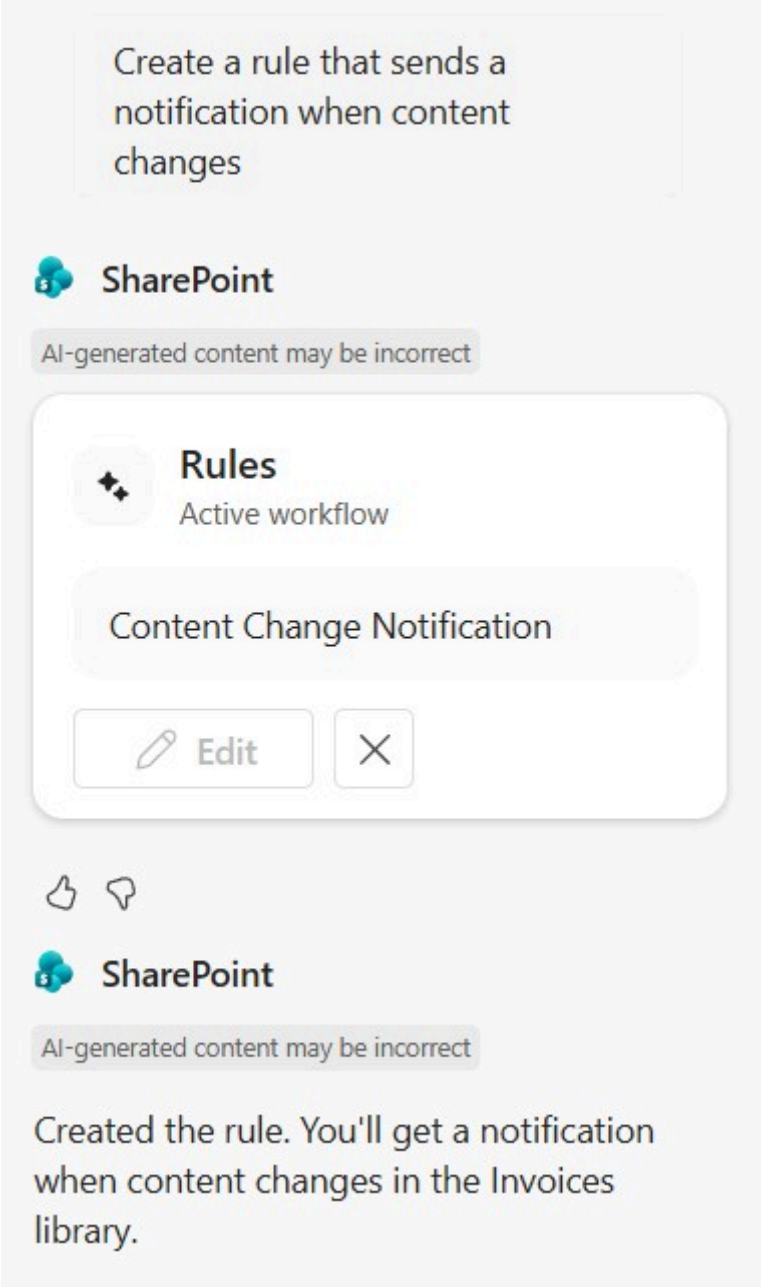
1. In the lower-right corner of your document library, select the Copilot in SharePoint icon.
2. From the **quick actions** menu, select **Set up rules**.
3. The chat panel opens and displays a list of suggested actions related to the creation of rules.

> **Note**
>
> If this is the first time using Copilot in SharePoint in the library, the system automatically generates up to three suggested columns based on the available files. These columns are auto-populated with metadata and can be useful when creating rules.

Use a suggested prompt

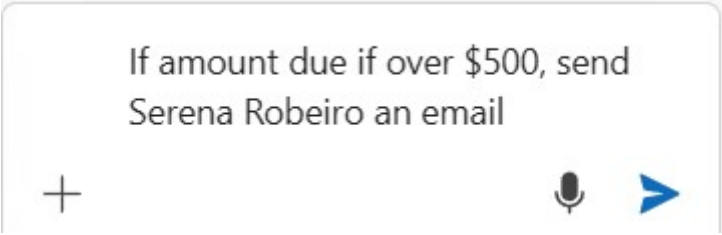
1. From the chat panel, select an action. For this example, use **Send notification**.
2. In the chat box, review the instruction provided. If needed, modify the text to better suit your intent. When ready, select **Send** (▷) to submit your action.
3. Based on your prompt, the system generates a rule. Review the rule and select **Create** to set up the rule.

4. The chat panel summarizes the rule conditions.



Enter a custom prompt

1. In the chat panel's text box, enter your own automation instruction. When requesting a rule, specify the condition in which it should run and the action that should happen. This condition ensures the rule meets your needs.



> **Tip**

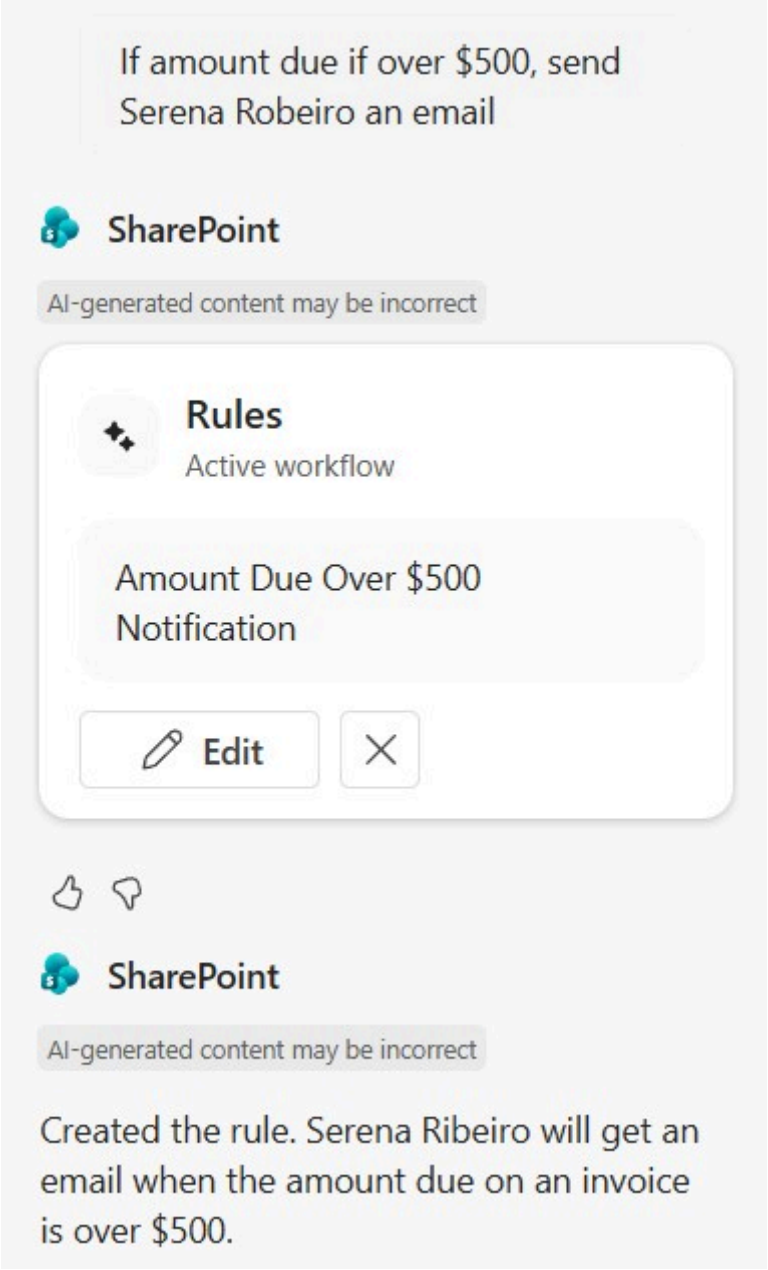
You can use Copilot in SharePoint to perform four actions: email, move, copy, and set value. Here are some sample prompts:

- Send an email (for example, "Email me when a contract is approved" or "Notify me when new files are added and the release date is in 2025")
- Move a file (for example, "Move reviewed invoices to the Verified Expenses folder")
- Copy a file (for example, "Copy all Northwind Traders invoices to the Northwind folder")

2. Select **Send** (▷) to submit your prompt.

3. Based on your prompt, a rule is generated. Review the rule created and select **Create** to set up the rule.

4. The chat panel summarizes the rule conditions.



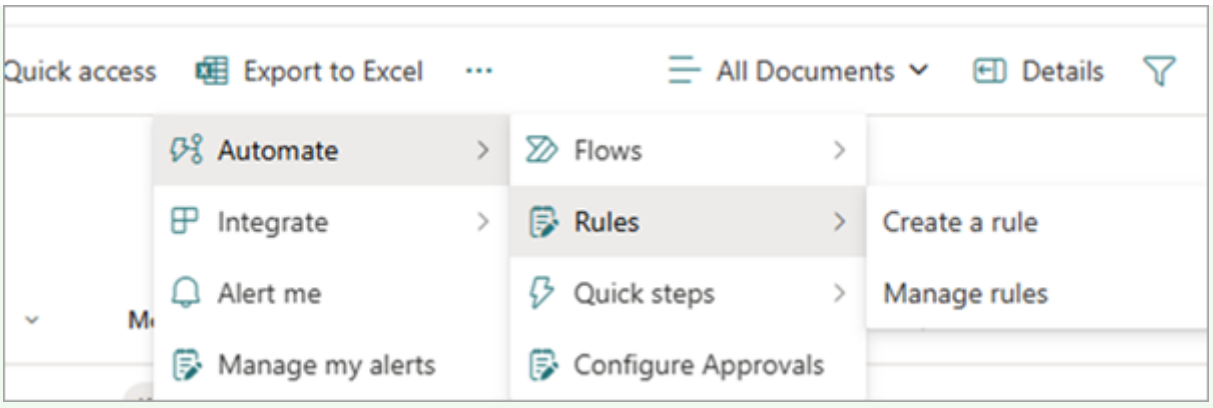
Save your changes

1. When you're ready to save the rule you created and any other changes you made, select **Save changes**.

2. On **Save changes to library?**, confirm the changes and then select **Apply changes**.

3. You're returned to the updated library, and the rule runs automatically whenever the defined conditions are met.

> **Tip**
>
> If you want to see all of the rules in your document library, from the header select **Automate** > **Rules** > **Manage rules**.



Requirements and limitations

- **Supported rule triggers**: A new item is created, an item is modified, or an item is deleted.
- **Supported rule actions**: Email, move, copy, and set value.
- **Supported languages**: All languages supported through Microsoft Copilot for text-based prompts and responses, but it can only process files in English.
- **Limitations**:
  - Encrypted files can't be analyzed to run rules.
  - The "date approaches" trigger for rules isn't yet supported by Copilot in SharePoint.
  - The translate and delete rule actions aren't yet supported by Copilot in SharePoint. Organizations with pay-as-you-go billing set up can translate files using AI capabilities, but they incur costs on their pay-as-you-go meter.
  - Multi-step prompts to create new columns and configure a rule in one step don't yet work for the set value action.
  - You can create up to 15 rules per list or library.
  - You can't apply rules to multi-line text columns.
    - Rules don't support email-enabled security groups for notifications.
- **Notifications**: Copilot sends emails from *no-reply@sharepointonline.com* to specified individuals.

Last updated on 09/24/2026

Create views in a SharePoint document library

Copilot in SharePoint helps you create custom views of your document libraries. By showing and hiding columns, sorting, and filtering, these capabilities can configure your library to highlight what's most important to you.

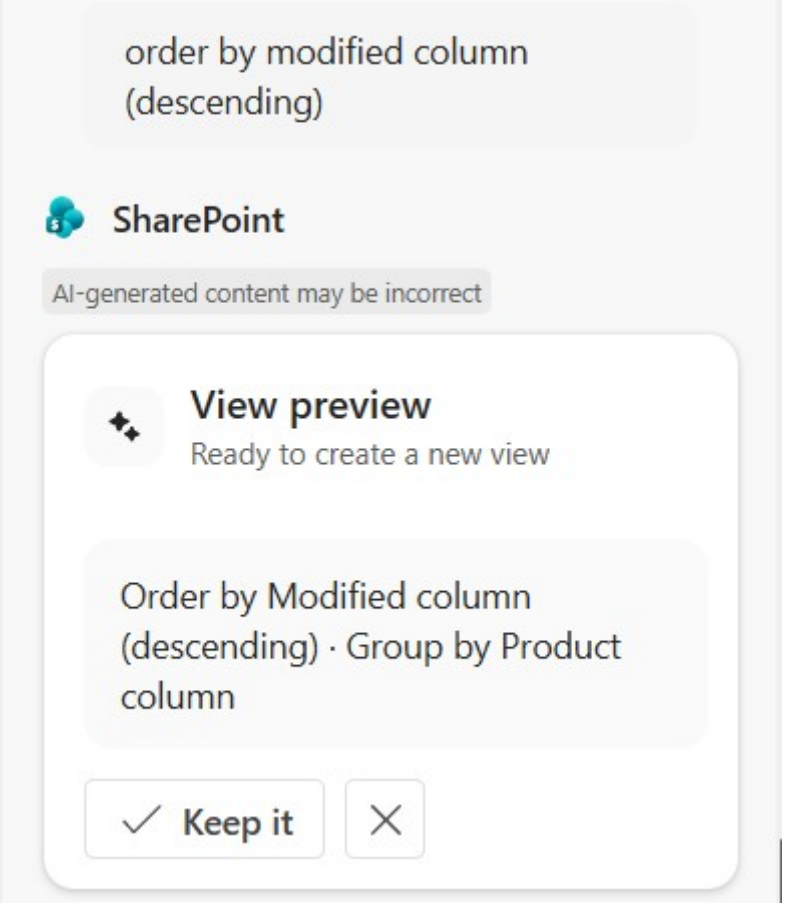
Launch the quick action

1. In the lower-right corner of your document library, select the Copilot in SharePoint icon.
2. From the **quick actions** menu, select **Create new view**.
3. The chat panel opens and displays a list of suggested actions related to custom views.

> ⓘ **Note**
>
> If this is the first time using Copilot in SharePoint in the library, it automatically generates up to three suggested columns based on the available files. These columns are auto-populated with metadata about your files and can be useful when creating views.

Use a suggested prompt

1. From the chat panel, select an action. For this example, use **Show recently updated files first**.
2. In the chat box, review the instruction provided. If needed, modify the text to better suit your intent. When ready, select **Send** (▷) to submit your action.
3. Based on your prompt, a view is generated. The view parameters are summarized in the chat panel.



Enter a custom prompt

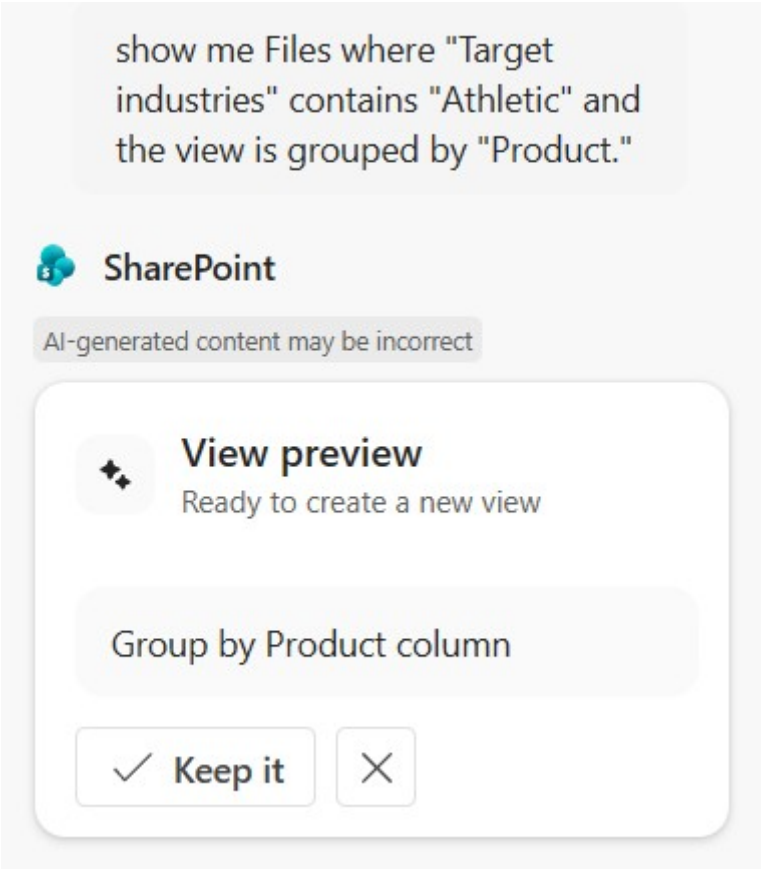
1. In the chat panel's text box, enter your own custom view instruction. When describing a view, consider what you want to see (filters) and how you want it grouped or sorted. This consideration helps ensure the view meets your needs.

> **Tip**
>
> You can use Copilot in SharePoint to show and hide columns, sort, filter, and group. Here are some sample prompts that you can use on libraries containing different document types:
>
> - **Invoices**: Show me past due invoices, grouped by vendor and sorted by amount due.

- **Product specs**: Show me products with a release date in 2020 and sort by market positioning.
- **HR policy documents**: Display HR policies by category showing only those that are already in effect.
- **Project plans**: I want to see project plans grouped by phase and sorted by start date. Show the owner column and hide the location column.

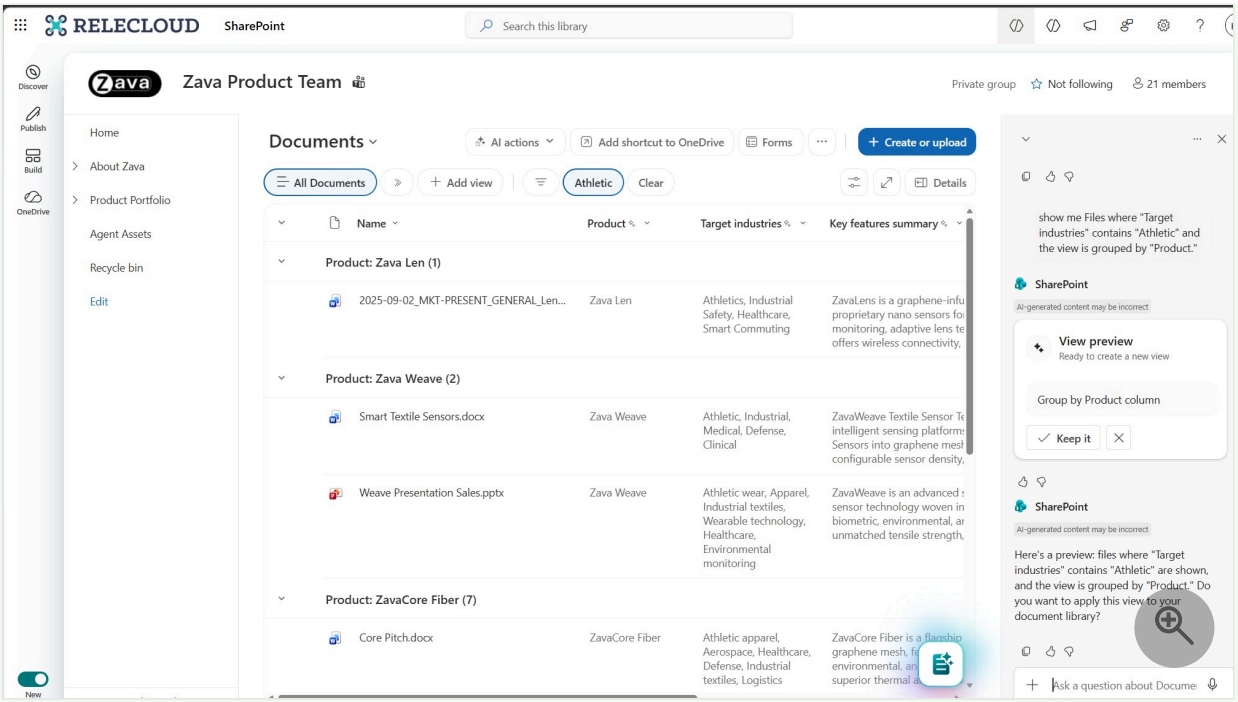
2. Select **Send** (▷) to submit your action.

3. Based on your prompt, a view is created and summarized in the chat panel.



Tip

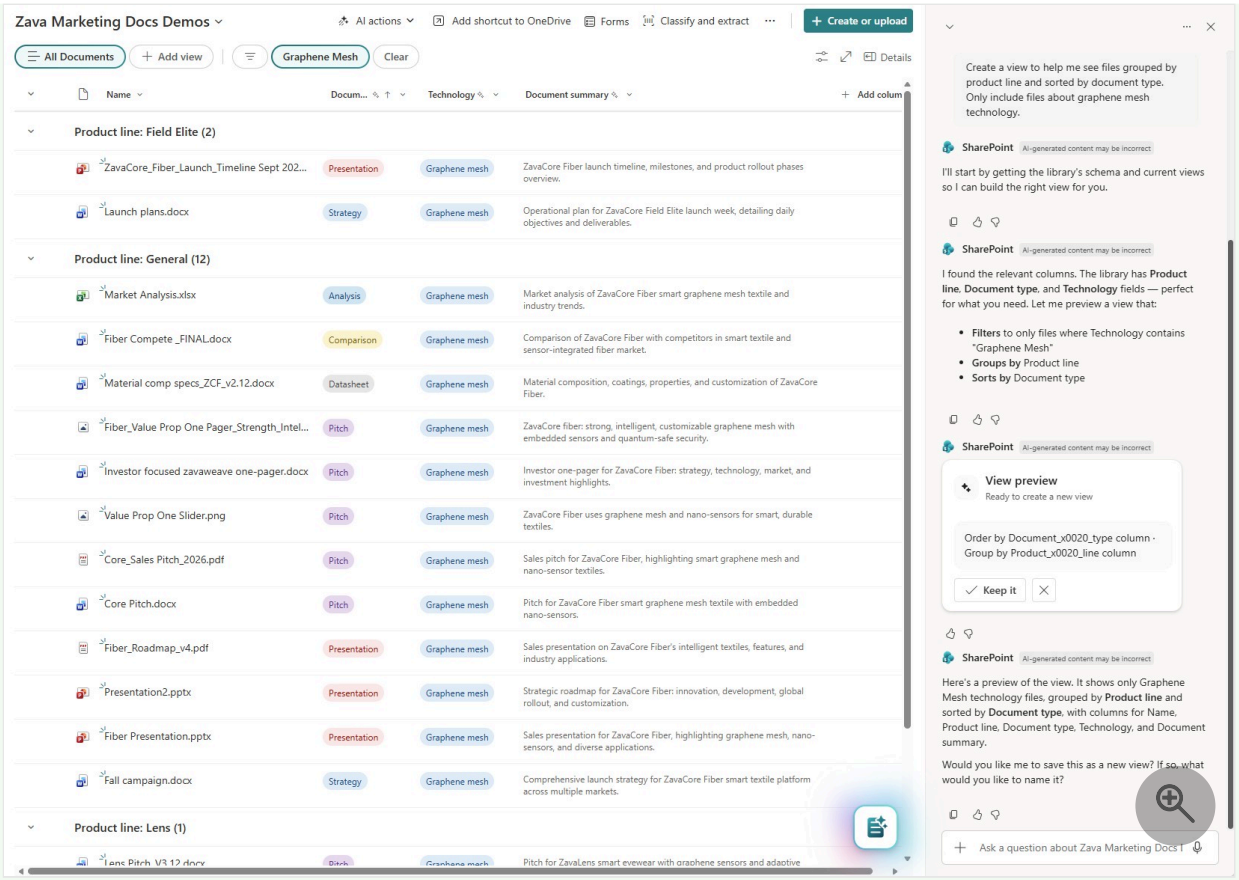
In the chat panel, you can see a full description of the view created. The view is also reflected in the document library.



The generated view might also apply visual cues to help highlight important information in the library. For example, filtered results or grouped items might appear together, making it easier to quickly identify relevant files. These visual changes are part of the view configuration and reflect filters, grouping, and sorting defined by the prompt.

Tip

Copilot in SharePoint can generate views from library metadata. In this example, it groups files by product line, sorts by document type, and filters to display only graphene mesh content.



Save your changes

1. When you're ready to save the view you created and any other changes you made, select **Save changes**.

2. On the **Save changes to library?** confirmation screen, verify that you want to update the **current library view** or save as a **new view**, and then select **Apply changes**.

> **Tip**
>
> If you create a new view, the name of the library is appended with a numerical value. Future updates will improve the naming experience, but for now you can rename the view from the library command bar.

3. You're returned to the updated library and the view you created. Views created by using Copilot in SharePoint are public views and are visible to everyone who uses the document library.

Requirements and limitations

- **Supported view actions**: Show column, Hide column, Sort, Filter, and Group-By.

- **Supported column types for filtering**: Choice, Number, Text, DateTime, Boolean, Currency, and MMD.
- **Supported column types for column creation**: Choice, Number, Text, DateTime, Boolean, Note, Currency, URL, and MMD.
- **Supported languages**: All languages supported through Microsoft Copilot for text-based prompts and responses, but it can only process files in English.
- **Limitations**:
  - Encrypted files can't be analyzed to generate metadata for views.
  - Copilot in SharePoint doesn't yet support column ordering, column width changes, or conditional formatting of views.
  - Personal views aren't currently supported. Views created by using Copilot in SharePoint are public views that are visible to everyone who uses the document library.

Last updated on 09/24/2026

Monitor file processing status

You can monitor real-time updates on files processed in a SharePoint library. This feature lets you:

- See when a file is being processed.
- Check the status of the file: **In progress**, **Completed**, or **Failed**.
- Understand what worked, what didn't, and why.

You can view the processing status for a file that is being processed, for a selected file or for all files in a document library.

Prerequisites

To use this feature, you need:

- Microsoft Copilot license
- Copilot in SharePoint

Monitor the status of a file being processed

When you submit an on-demand request to process a file:

1. A message bar appears at the top of the library, indicating the action is in progress.
2. On the right side of the message bar, select **View status** to open the activity panel.
3. The activity panel shows the current action being processed.

Monitor the status of any file

To view the processing status of one or more files:

1. In a SharePoint document library, select the files.
2. From the **More options** (...) menu next to the file name or on the command bar, select the service, and then select **View recent activity**.
3. The activity panel shows the current action being processed.

Monitor the status of all files

To view the processing status of all files in the library:

1. In a SharePoint document library, on the command bar, select **More options** (...), select the service, and then select **View recent activity**.

2. The activity panel shows the current actions being processed.

View the activity panel

The activity panel displays a list of file processing events, including:

- File name
- Summary of the action that was performed, or information about why it failed
- Processing status: **In progress**, **Completed**, or **Failed**
- Date and time of the event

> **Note**
>
> If you select no files or more than 30 files, the activity pane displays the processing status for the entire library, rather than for individual files.

Filter activity options

By default, the panel shows activity for the last 60 days.

- To filter by date, select **Filter** > **Date range**.

- To show only failed files, select **Filter** > **Failed status**.

Status definitions

Expand table

Status	Description
In progress	The service starts processing the file. A timestamp is displayed.
Completed	The service finishes processing successfully. A description of the completed actions is provided.
Failed	The service encounters an error. A description of the cause of the failure is provided.

Last updated on 09/25/2026

Generate structured documents in a SharePoint document library

> **Note**
>
> This article applies to the preview version of Copilot in SharePoint (previously referred to as AI in SharePoint).

Structured document generation lets you turn Word document templates into intelligent, AI-powered forms. When a user submits a form, the system automatically generates a new document from the template with the submitted values merged into the appropriate fields. This process creates consistent, governed documents every time - without requiring manual edits to the template.

This feature is useful for organizations that regularly produce standardized documents, such as:

- **Legal and compliance** - Contracts, NDAs, statements of work, settlement agreements, vendor agreements.
- **Procurement and finance** - Purchase orders, invoices, payment authorizations.
- **Human resources** - Employment verification letters, offer letters, travel and visa support letters.
- **Sales and operations** - Proposals, bid documents, statements of compliance, customer letters.

How structured document generation works

The document generation process involves two roles and a handoff between them.

Content manager (template creator) - Creates and governs templates and forms. They define the document structure, required fields, and conditional rules to ensure that every generated document is consistent and compliant.

Content consumer (form submitter) - Submits forms to generate documents. They fill out the form with the requested information, and the system generates a new document that preserves the approved layout and language - only the field values change.

Prerequisites

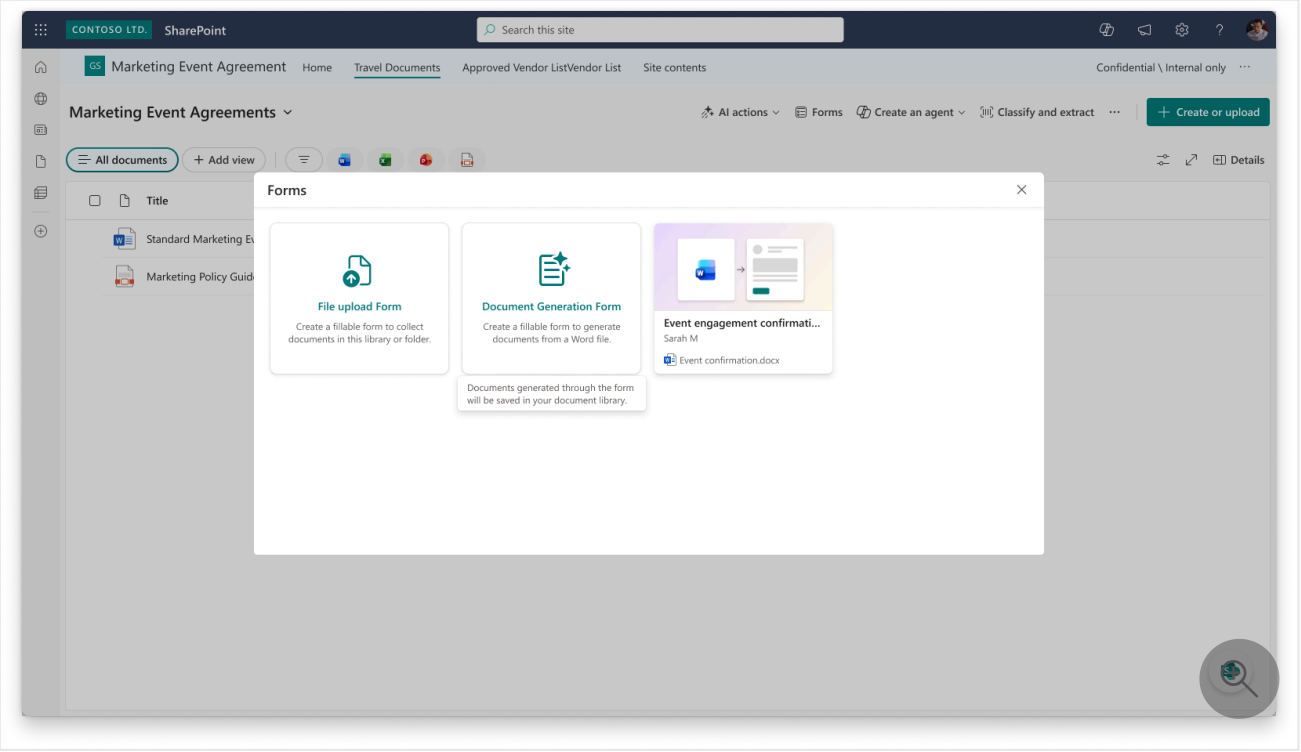
- Content managers, or users who create and configure forms, must have a Microsoft Copilot license assigned.
- To create a form, users must have **Edit** permissions on the document library.
- The source document must be a Microsoft Word document (.docx format).

Create a form from a document

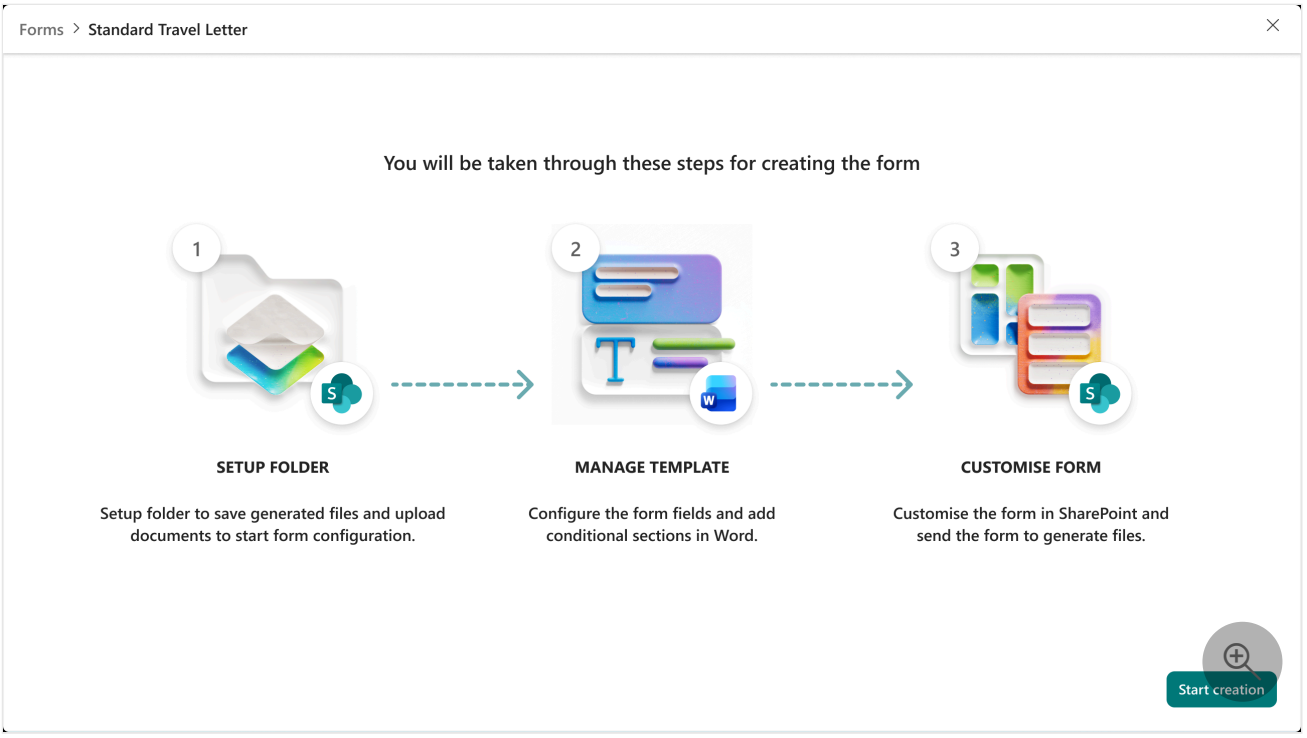
You can create a form from any Word document stored in a SharePoint document library.

1. In a SharePoint document library, select **Forms** from the command bar.

2. Select **Document generation form** to start the form creation process.



3. You get a high-level step pane that highlights how you go about the flow, so you know what to expect at each stage of form creation.

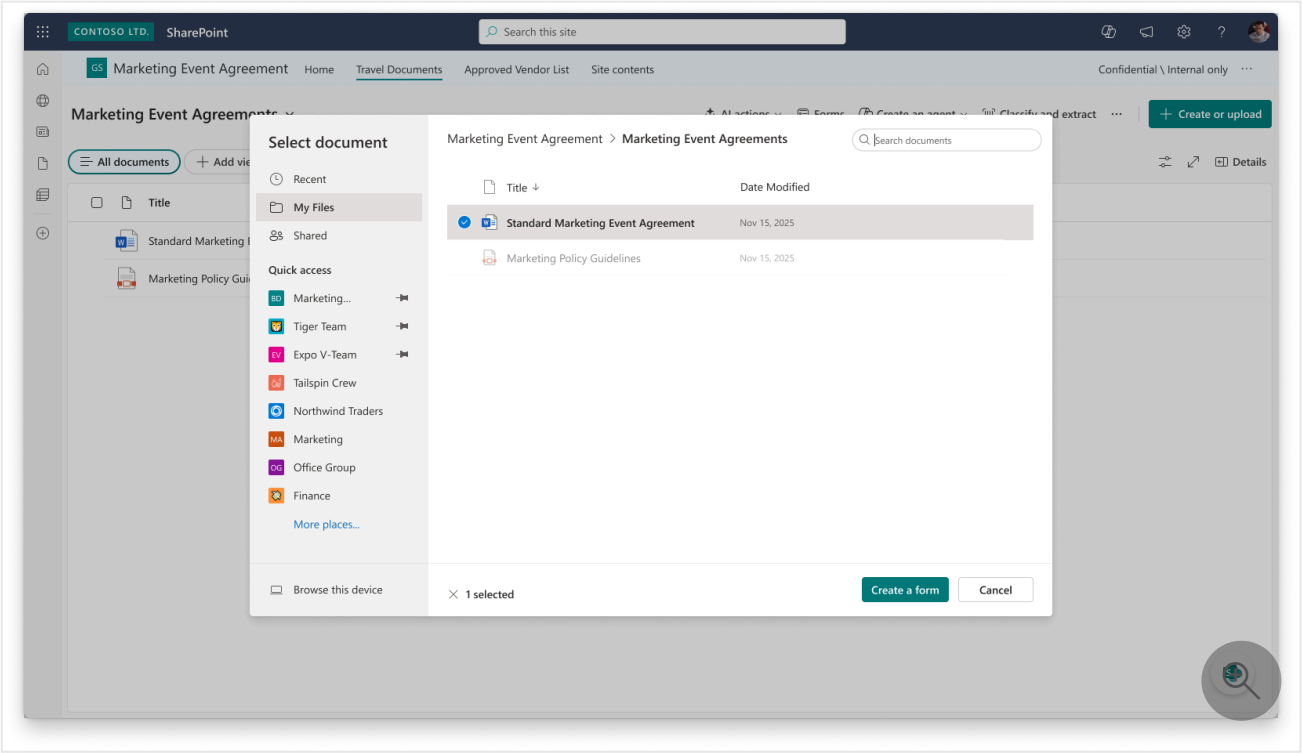


4. If you're on the document library home page, you're prompted to create a target folder. Each document generated from the form is saved into this folder.

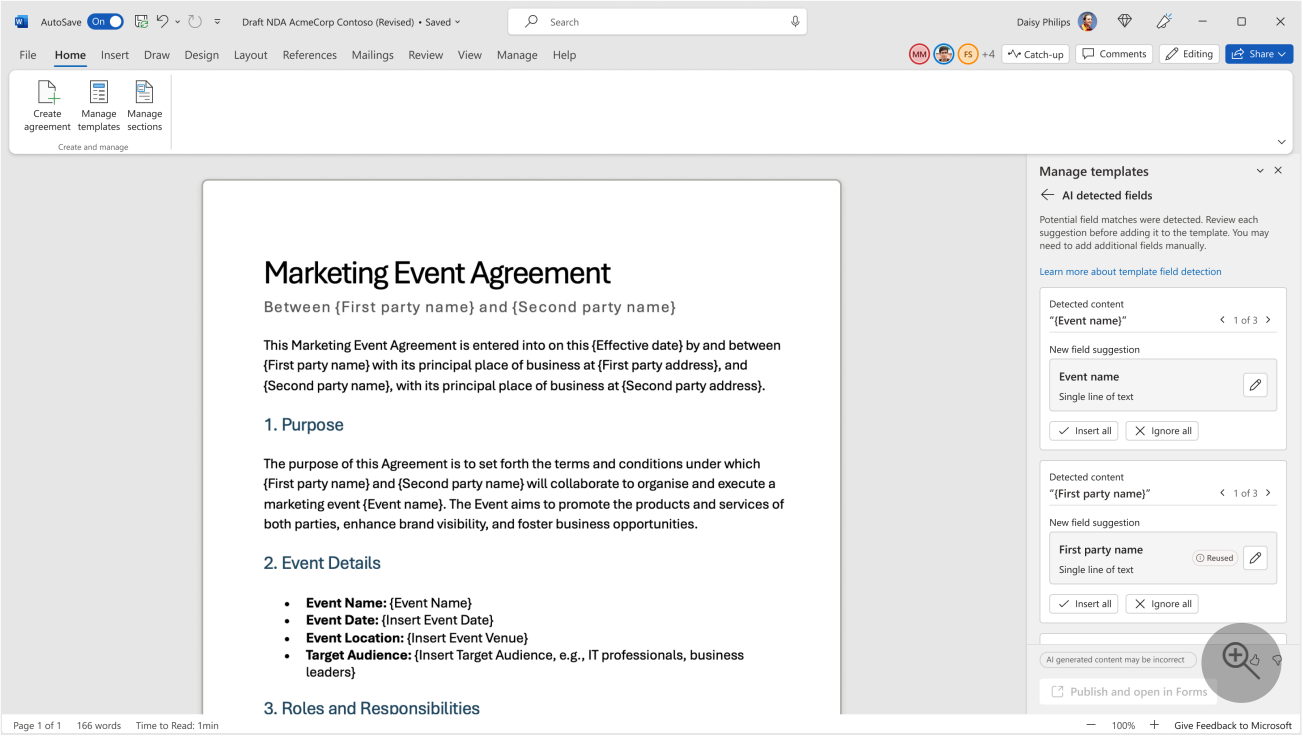
5. Upload the Word document you want to use as a template. You can select a document from:

    - The current SharePoint document library
    - A OneDrive location
    - Your local device

> **Tip**
>
> For best results, upload a Word document with annotated placeholders such as {} or [].



6. Copilot in SharePoint analyzes the structure of the document and automatically suggests fields—such as names, dates, addresses, and responsibilities—so you don't have to do manual setup.



Note

If you have other forms in the document library, you might see a reused indicator that calls out that this field "Matches an existing column in this site. Saving this field reuses that column instead of creating a new one." More on this.

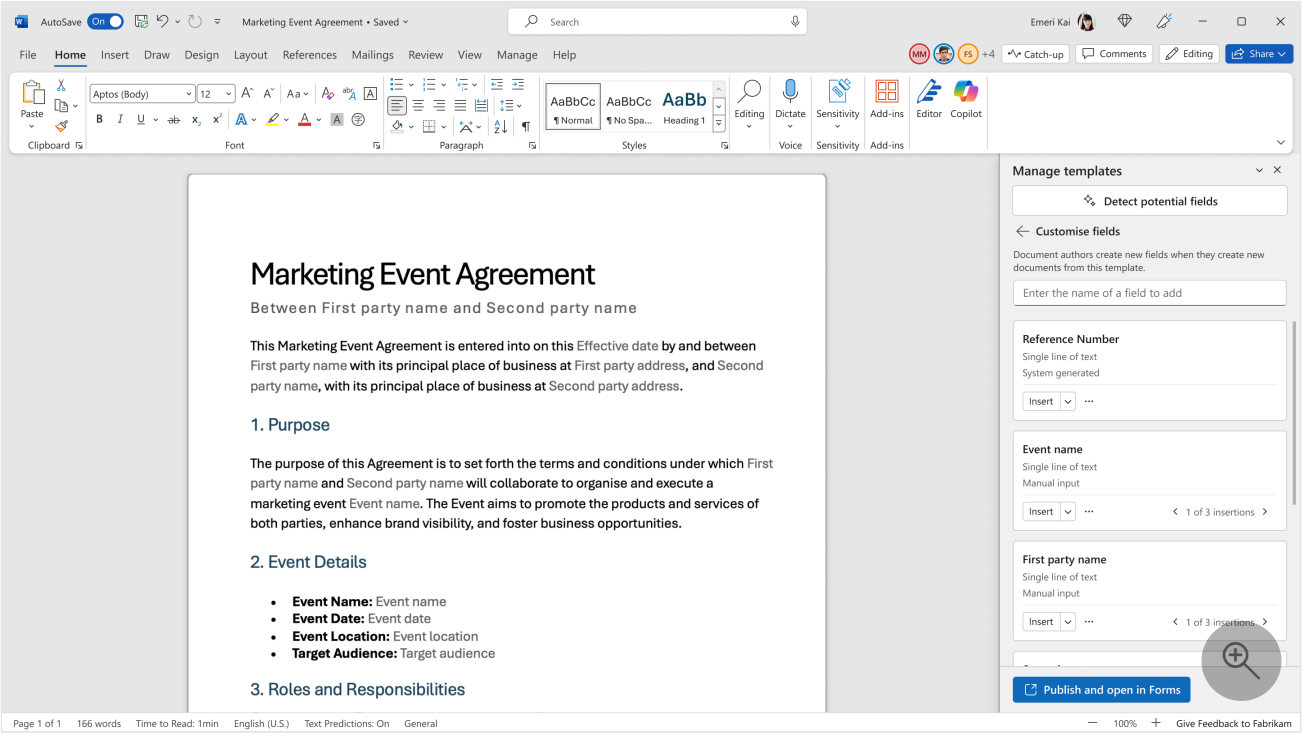
7. Review the suggested fields. You can:

    - Confirm which fields are required.
    - Refine field names to match your organization's terminology.
    - See how each field maps back to locations in the document.

Customize fields section

In the **Customize fields** section, you can:

- Use the search pane to look for existing columns to reuse, or add new fields.
- Select **Detect potential fields** to run AI detection on the document content.
- Use the **Insert** dropdown on each field to map it to specific locations in the document.
- Select the **...** (more options) menu on a field to rename it, change help text, or delete it.



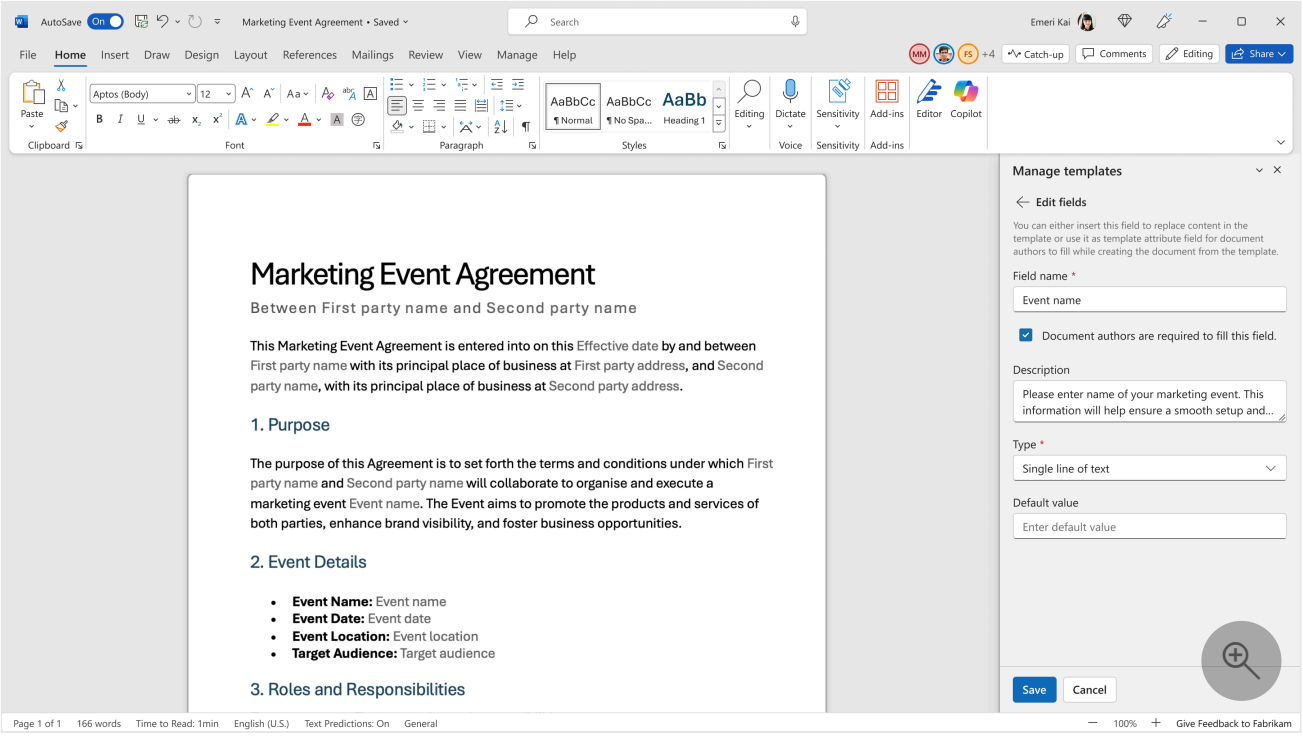
> **Note**

Each field shows the number of insertions in the document (for example, "1 of 3 insertions"), so you can see exactly where values appear in the generated document.

Configure field details

When you create or edit a field, configure the following details:

- **Field name** — Enter a descriptive name for the field.
- **Description** — A free-form text field for summaries or explanatory notes that give additional context about the field.
- **Required** — Select the **Document authors are required to fill this field** checkbox to make the field mandatory.
- **Type** — Select the data type for the field from the **Type** dropdown.
- **Default value** — Enter a value that pre-fills the field on the form, so submitters can accept it as-is or change it before submitting.



Reuse fields across forms

If other forms already exist in the same document library, you can reuse an existing field instead of creating a duplicate one. When adding a field, use the search bar to find matching columns in the library—you'll see each match along with its data type—and choose whether to reuse an existing column or create a new one.

Reusing a field means multiple forms share the same underlying library column, so it appears only once in the library view. This feature eliminates duplicate columns (such as several "Contractor Name" fields), keeps your library schema clean, and ensures consistent metadata across every form.

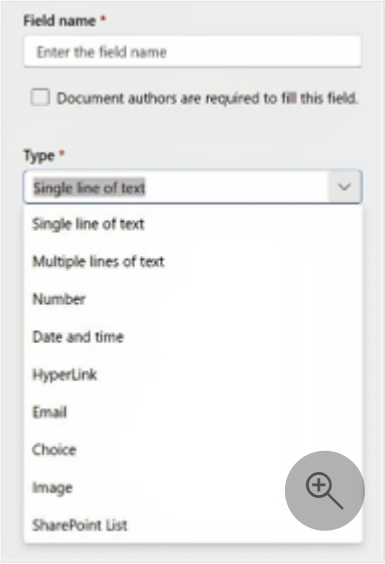
When a column is shared by more than one form, its **name and data type are locked** and can only be changed through SharePoint column settings, not from the form. Form-specific properties such as help text and the required checkbox remain editable per form. If you need a different data type for a shared field, the system warns you and, if you proceed, creates a new "forked" column—leaving the original unchanged for other forms. Deleting a shared field removes it only from the current form; once just one form uses it, the field becomes fully editable again.

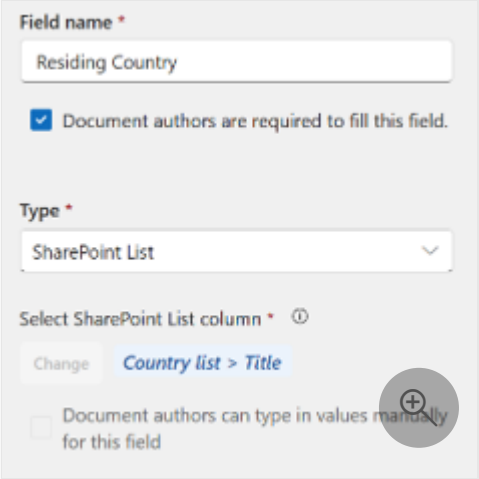
Supported field types

The following field data types are supported:

- **Single line of text** — A short text input for names, titles, or brief descriptions.
- **Multiple lines of text** — A longer text input for detailed content such as responsibilities or clauses.
- **Number** — A numeric input for quantities, amounts, or identifiers.
- **Currency** — Stores monetary values with currency formatting and precision for financial calculations.
- **Date and time** — A date picker for selecting dates or date and time values.
- **Hyperlink** — A URL input for linking to external resources or references.
- **Email** — An email address input field.
- **Choice** — A dropdown selection from predefined options.
- **Image** — An image field for inserting logos, signatures, or other visual content into the document.
- **Managed metadata** — A field that references terms from a managed term set, so submitters select standardized, governed values instead of typing free text.
- **SharePoint List** — A lookup field that references values from a column in a SharePoint list.

When you select **SharePoint List** as the field type, you're prompted to select the SharePoint list column to associate with the field. You can also select the **Document authors can type in values manually for this field** option to allow form submitters to enter values directly in addition to selecting from the list.





Set up conditional sections

You can define business rules as conditional logic and map them to multiple sections in the document. Conditional sections let you control which parts of the generated document are included based on the values that form submitters enter.

For example, a legal agreement might include country-specific clauses that only appear when the submitter selects a particular country.

To set up a conditional section:

1. Open the template document. In the **Manage templates** pane, go to **Conditional sections** and select **+ New**.

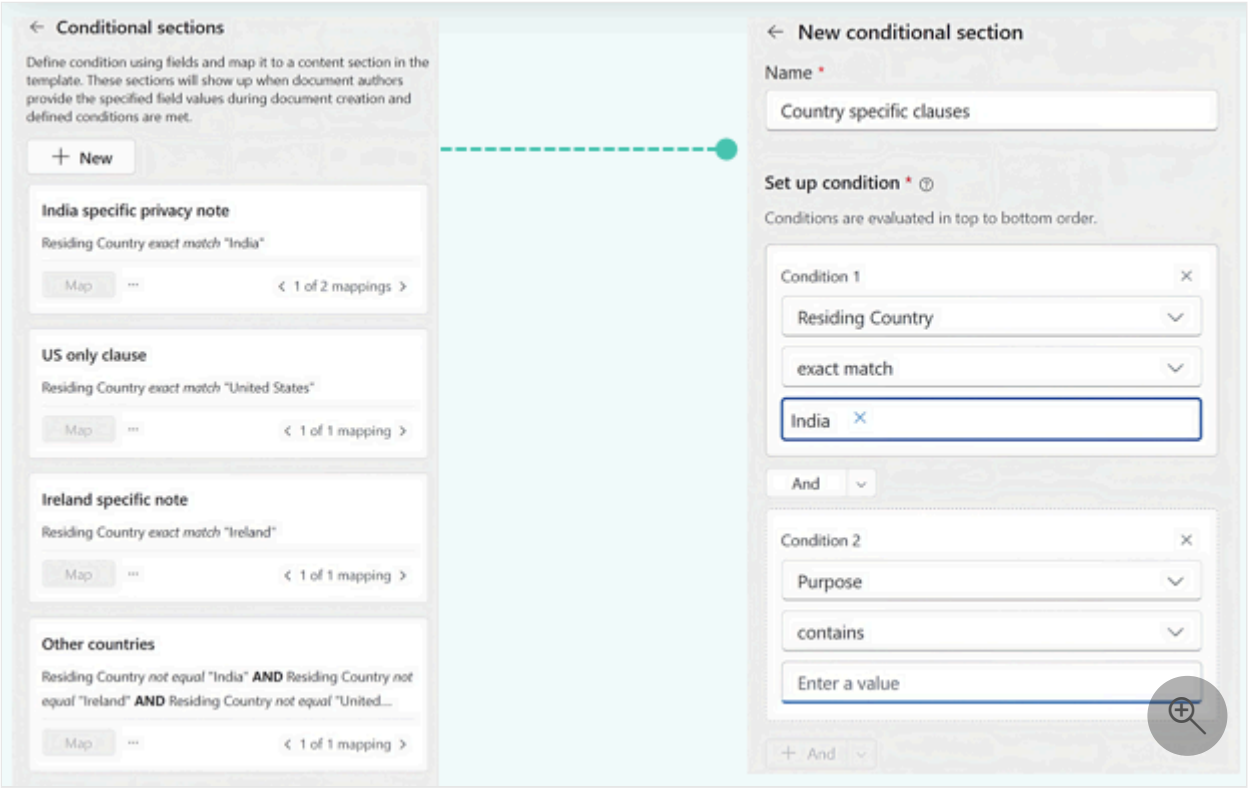
2. Enter a **Name** for the conditional section, such as "Country specific clauses".

3. Under **Set up condition**, configure one or more conditions. The system evaluates conditions in top-to-bottom order. For each condition:

- Select the field to evaluate, such as "Residing Country".
- Select the matching rule, such as **exact match** or **contains**.
- Enter the value to match against.

4. To add multiple conditions, select **And** or **Or** to combine them.

5. Select **Map** to associate the conditional section with one or more sections in the document content.



> **Note**
>
> You can create multiple conditional sections, each with different rules. For example, you might have separate conditions for "India specific privacy note," "US only clause," and "Other countries," each mapped to different sections of the document.

> **Important**
>
> Conditional sections are evaluated when the document is generated from the form. In a generated document opened in **Word for the web**, conditional sections don't update when you change a field value after generation—the hidden and shown sections stay as they were at generation time. This is a platform limitation of Word for the web, which supports a subset of the functionality available in Word for Windows (desktop), and there's currently no reliable workaround. To re-evaluate conditional sections against new field values, submit the

form again to generate a new document, or open the generated document in Word for Windows (desktop).

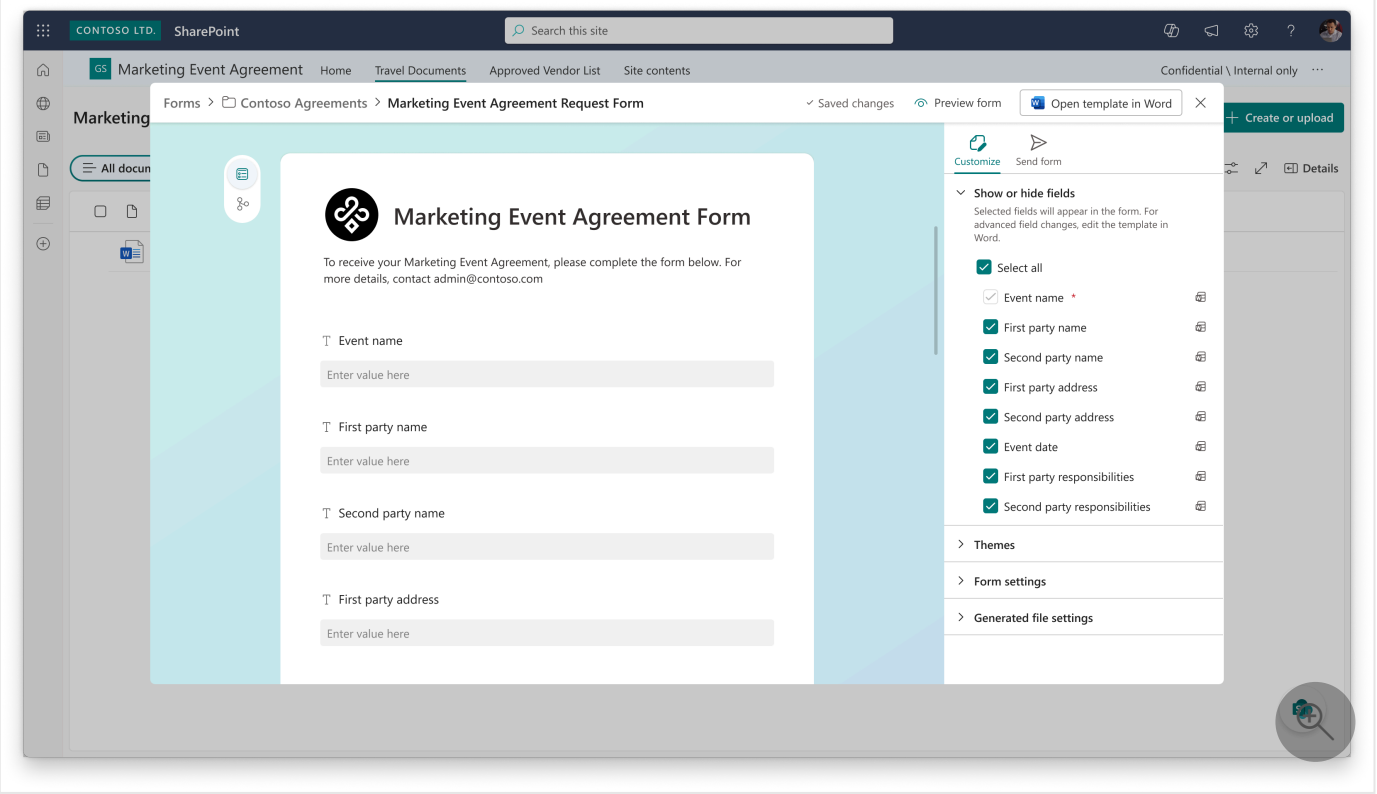
When you finish configuring fields and conditional sections, select **Publish and open in Forms** at the bottom of the pane. Word closes the template and transitions to the form view in SharePoint. A loading indicator shows "Closing template and opening form" during the transition.

Customize the form

After you publish the template, the form opens in SharePoint with a customization pane on the right side. The pane has two tabs: **Customize** and **Send form**.

Show or hide fields

On the **Customize** tab, the **Show or hide fields** section lists all fields from the template with a checkbox for each one. Selected fields appear in the form. Clear the checkbox for any field you don't want to show to form submitters.



> **Note**
>
> For advanced field changes, edit the template in Word. The **Show or hide fields** section controls field visibility only.

Set up conditional field visibility

While **Show or hide fields** controls which fields appear for everyone, *conditional field visibility* shows or hides an individual field dynamically—based on the answers a submitter provides to other fields. This keeps forms short and relevant, so submitters only see the questions that apply to them.

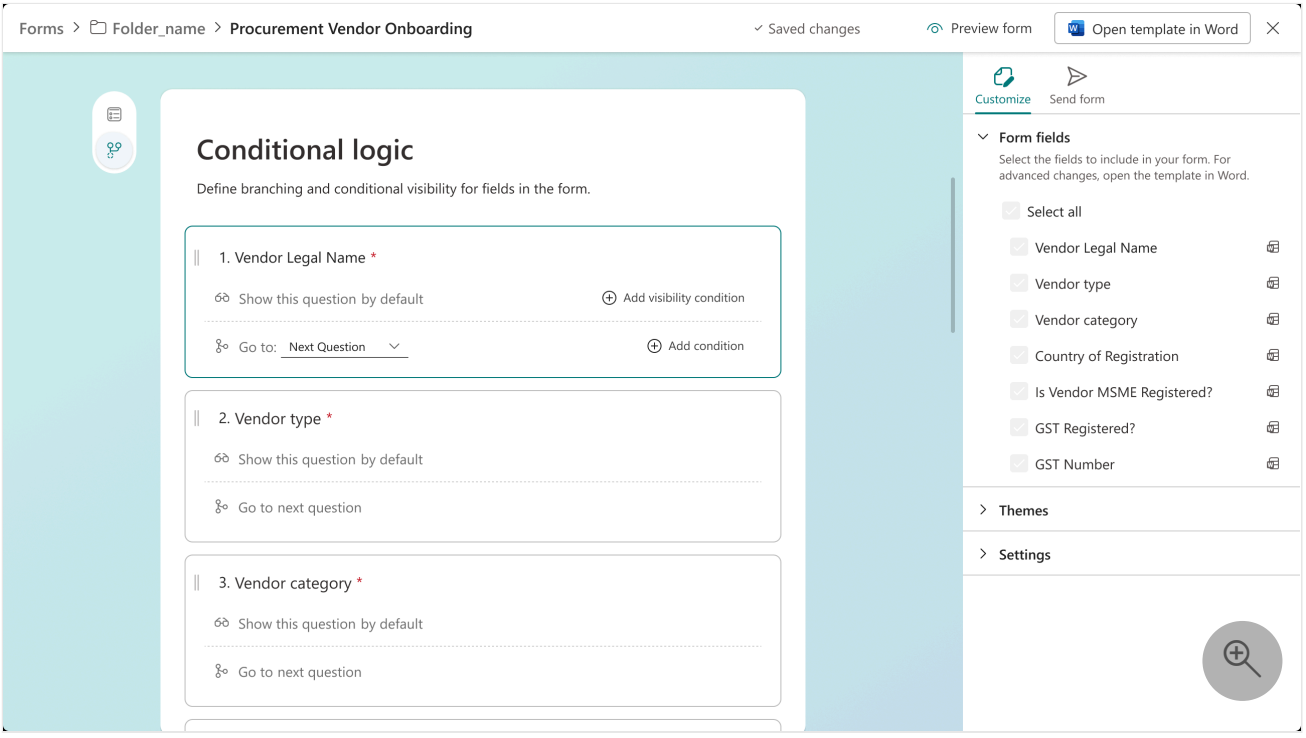
For example, on a vendor onboarding form you can hide the **Hardware Certification ID** field until the submitter selects **Hardware** in a **Vendor Category** choice field. If the submitter selects multiple categories—such as **Hardware** and **Professional Services**—every matching field appears automatically, while fields for unselected categories stay hidden.

A field that has a visibility rule is hidden by default and appears only when its condition evaluates to true.

> **Note**
>
> Conditional field visibility is also available for List forms and File upload forms, not just document generation forms.

To configure conditional visibility for a field:

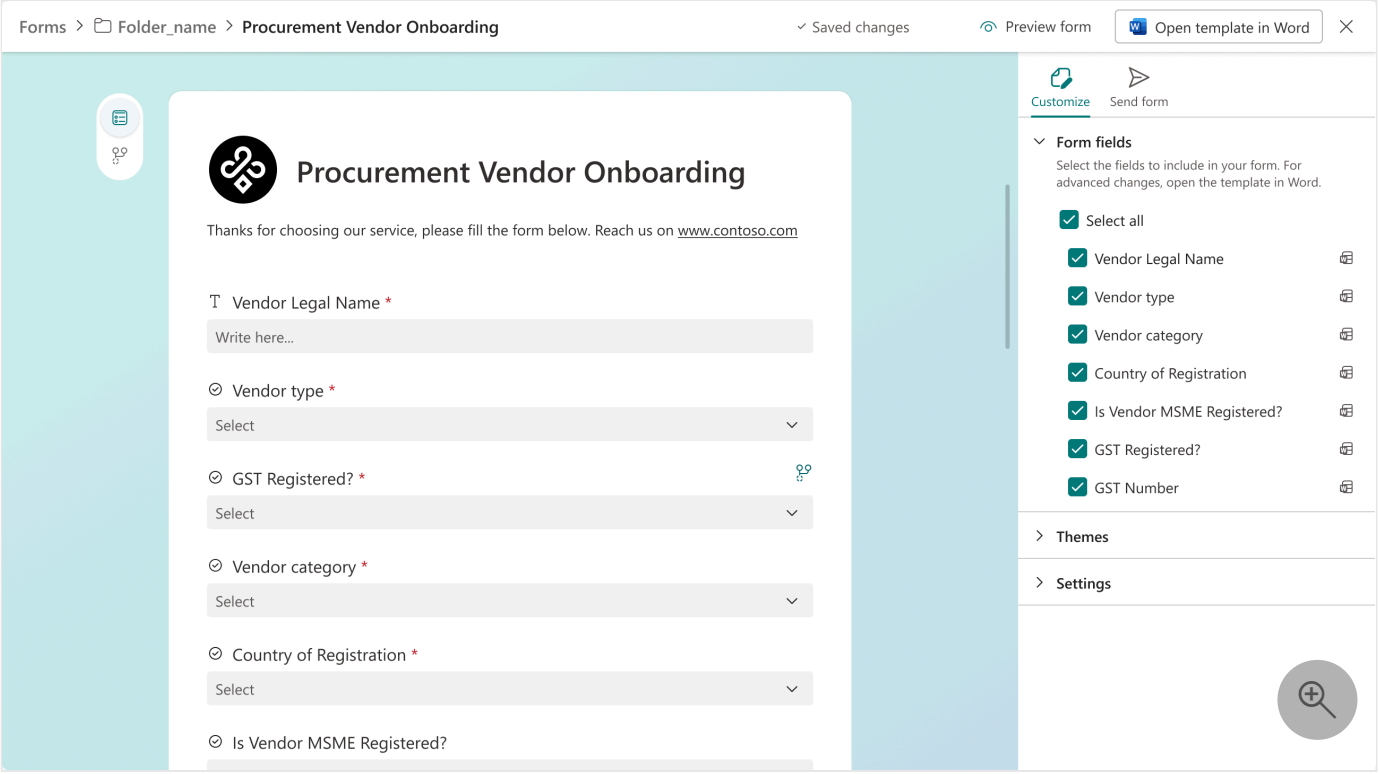
1. On the **Customize** tab, select the **Conditional logic** pivot.



2. Select the field you want to show or hide conditionally, and then select **Add visibility condition**.

3. Set the behavior to **Show this field when** the condition is met, then define a condition:
    - Select the **master field** whose answer the rule evaluates.
    - Select an **operator** for the comparison.
    - Enter or select the **value** to compare against.
4. To combine conditions in the same rule, add another condition and choose **AND** (every condition must be true) or **OR** (any one can be true). Conditions are evaluated top to bottom.
5. The field now stays hidden until a submitter's answers satisfy the condition.

Once a rule is set, each field that has conditional visibility shows an indicator in the form editor—select it to jump straight to that field's condition and edit it.



> **Note**
>
> If a field's visibility comes from a conditional section defined in the Word template, that condition is generated automatically and appears in the **Conditional logic** pivot as read-only. To change it, edit the conditional section in the Word template.

> **Note**

Conditional visibility and branching work at different levels. Branching jumps the submitter to a specific *field* based on an answer, while conditional visibility controls whether an *individual field* appears. When you use both, branching decides which field comes next, then conditional visibility determines whether the fields along the way are shown. A rule built on a field the submitter never reaches—because it's hidden or skipped by branching—can never be satisfied, so its target field stays hidden.

Supported field types and operators

You can build conditions on the following field types. The operators and input control depend on the field type.

Expand table

Field type	Operators	Input control
Single line of text, Multiple lines of text	Exact match, Not equal, Contains, Does not contain, Is empty, Is not empty	Text input
Choice (single or multiple), SharePoint List	Exact match, Not equal, Contains, Does not contain, Is empty, Is not empty	Choice selector
Number, Currency	Equal, Not equal, Greater than, Less than, Is empty, Is not empty	Number input
Date and time	Exact match, Not equal, Before, After, Is empty, Is not empty	Date picker
All other types	Is empty, Is not empty	No input control

For the **Is empty** and **Is not empty** operators, no value input is required.

> **Note**
>
> Date and time as master fields aren't available yet. The operators are listed above for reference, but conditions built on a Date and time field aren't supported in this release—support is coming soon.

Validation and required fields

- If a rule references a field that you deleted or removed from the form, the system shows a warning so you can fix the rule. It doesn't block you from publishing.

- A required field that is hidden by its visibility rule doesn't block submission. The form validates a required field only when it's visible and left empty, so submitters are never blocked by a required field they can't see.

> **Important**
>
> Conditional field visibility affects what a submitter sees while filling out the form—it's a form-filling experience, not a way to control the data itself. Because of this, **Power Automate doesn't apply conditional visibility**: if you generate documents through a Power Automate flow, the flow doesn't hide or show fields the way the form does, so a required field that your form hides will still be visible in the document.

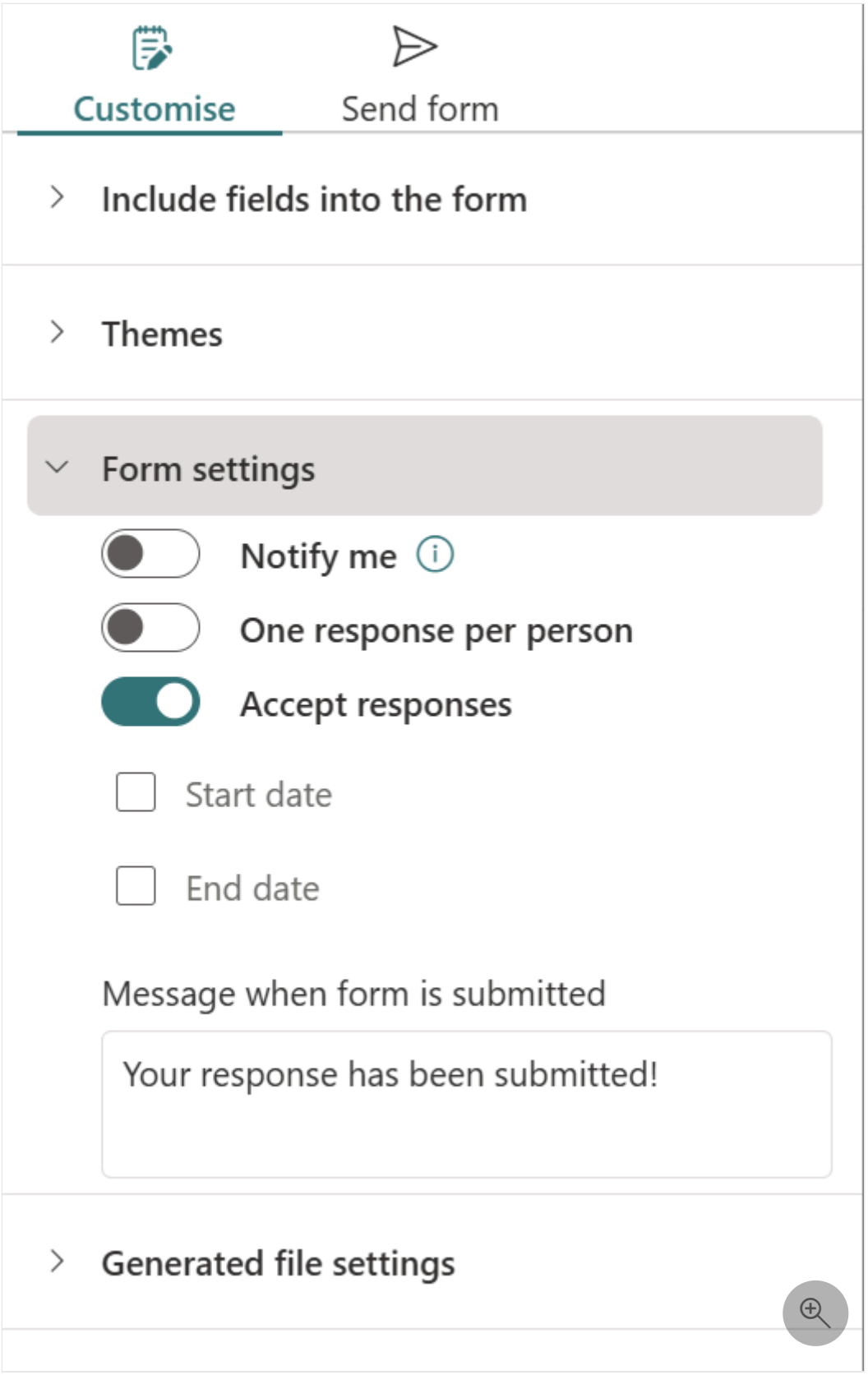
> **Tip**
>
> When you use a form with Power Automate, make any field you'd normally hide an optional field so it doesn't block the intended flow.

Themes and settings

Expand the **Themes** section to change the visual appearance of the form.

Expand the **Settings** section to configure form-level options:

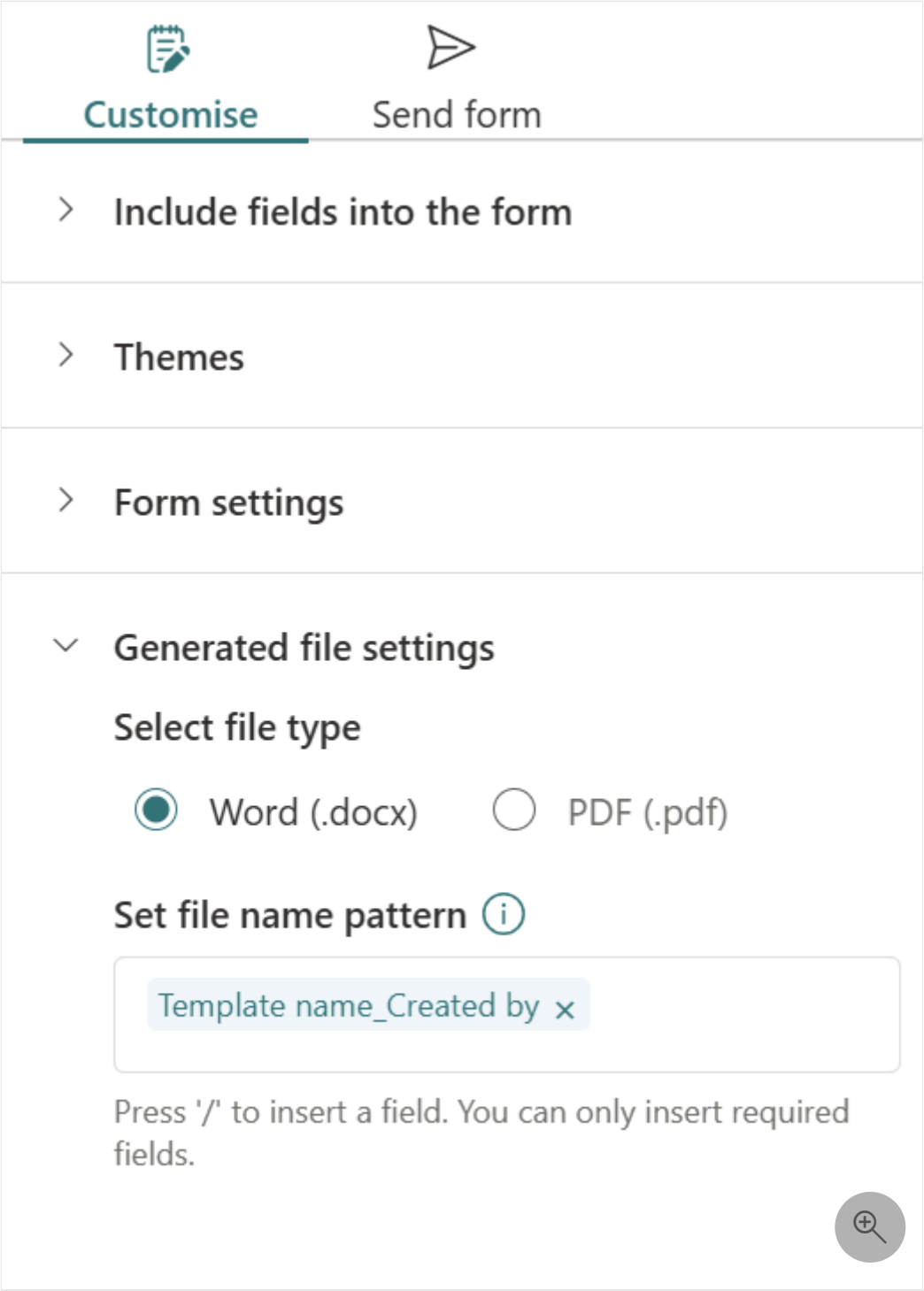
- **Notify me** — Toggle to receive a notification when a form is submitted.
- **One response per person** — Toggle to limit each user to a single form submission.
- **Accept responses** — Toggle to start or stop accepting form submissions.
- **Message when form is closed** — Customize the message displayed to users when the form is no longer accepting responses (default: "We're not accepting responses at the moment.").



Expand the **Generated file settings** section to control the output format and naming of the documents the form produces.

- **Select file type** — Choose the format for the generated document: **Word (.docx)** or **PDF (.pdf)**.

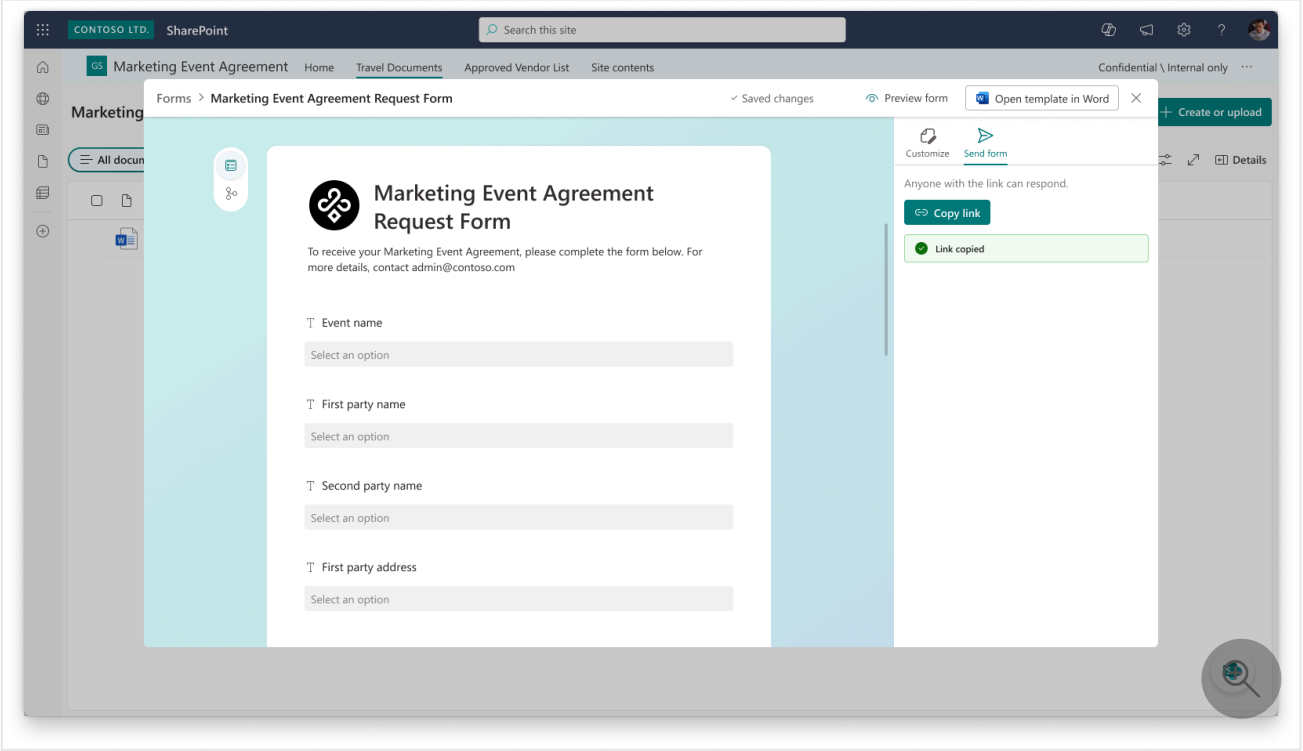
- **Set file name pattern** — Define how generated files are named by combining fields and text (for example, "Template name_Created by"). Press **/** to insert a field; only required fields can be inserted.



Share the form link

After you publish the form, share the form link so users in your organization can submit forms and generate documents.

1. Select the **Send form** tab in the customization pane to access the form link.



2. Copy the form link and distribute it through any collaboration channel:

    - Microsoft Teams
    - Outlook
    - SharePoint agents
    - SharePoint site pages

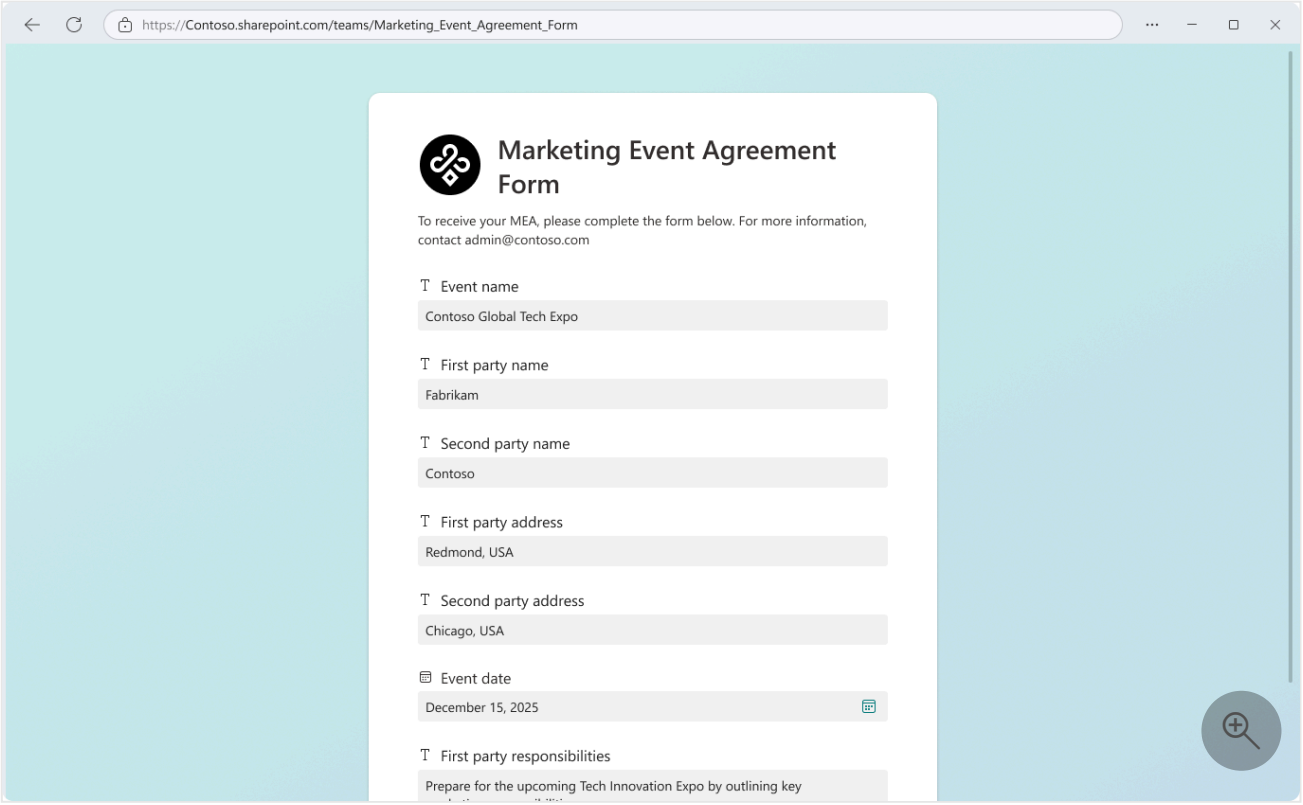
> **Tip**
>
> You can embed the form link directly on a SharePoint site page so that users can find and access it alongside other resources on your internal sites.

The form link is persistent—it stays the same URL even when you update and republish the template. Form submitters always see the latest published version.

Fill out and submit a form

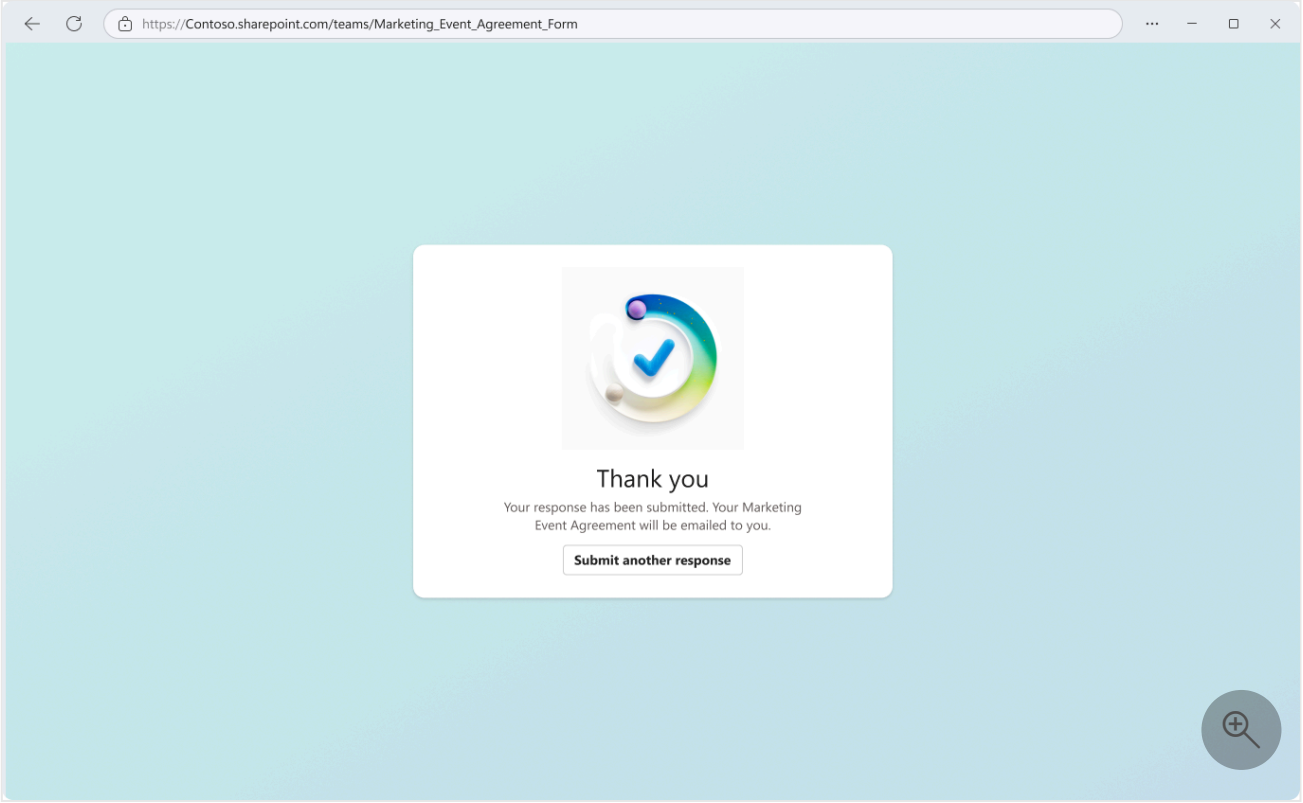
Content consumers use the shared form link to generate documents.

1. Open the form link from the location where you shared it—for example, a SharePoint site page, a Teams message, or an email. A simple form opens in the browser.

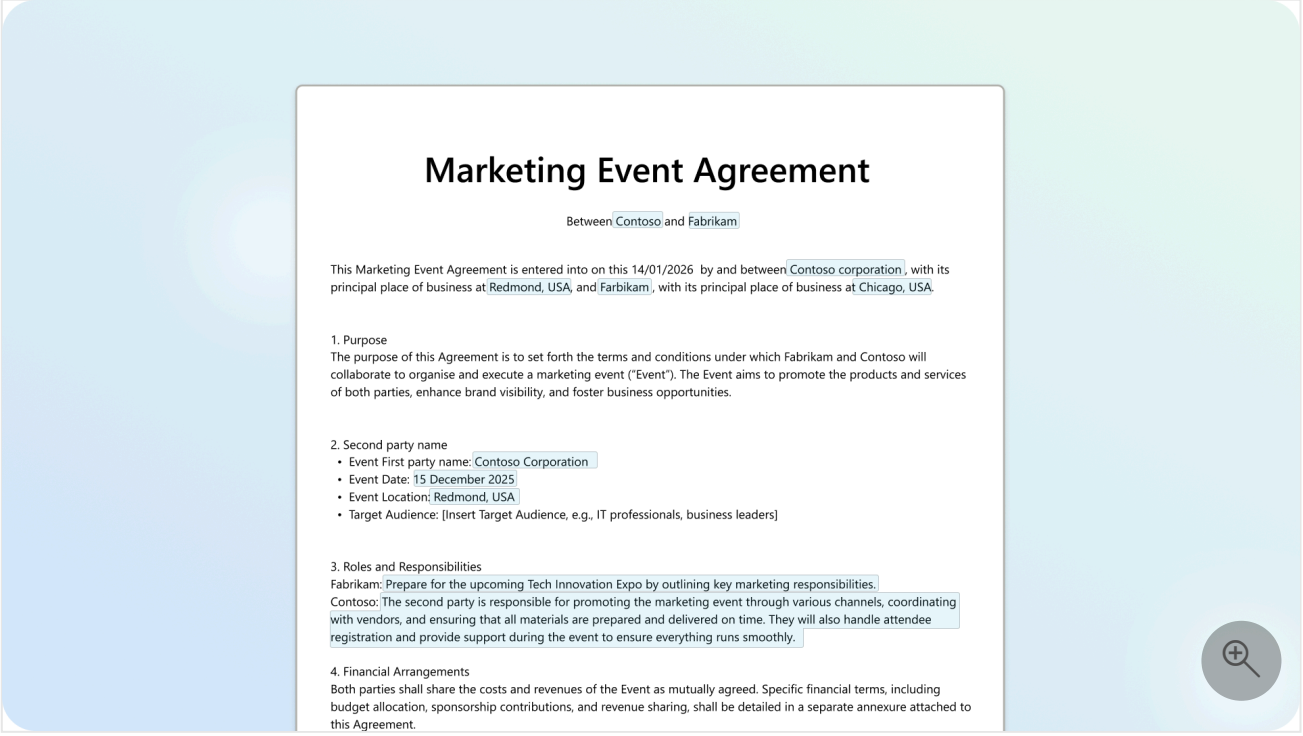


2. Fill in the requested fields, such as event details, vendor information, roles, responsibilities, and key dates. Each field shows its data type with an icon. Required fields are clearly indicated.

3. Select **Submit** to generate the document.



4. The system generates a professionally formatted document using the approved template. The field placeholders in the template are replaced with the values you entered—no copying, no manual edits.



Marketing Event Agreement

Between Contoso and Fabrikam

This Marketing Event Agreement is entered into on this 14/01/2026 by and between Contoso corporation, with its principal place of business at Redmond, USA, and Farbikam, with its principal place of business at Chicago, USA.

1. Purpose
The purpose of this Agreement is to set forth the terms and conditions under which Fabrikam and Contoso will collaborate to organise and execute a marketing event ("Event"). The Event aims to promote the products and services of both parties, enhance brand visibility, and foster business opportunities.

2. Second party name
- Event First party name: Contoso Corporation
- Event Date: 15 December 2025
- Event Location: Redmond, USA
- Target Audience: [Insert Target Audience, e.g., IT professionals, business leaders]

3. Roles and Responsibilities
Fabrikam: Prepare for the upcoming Tech Innovation Expo by outlining key marketing responsibilities.
Contoso: The second party is responsible for promoting the marketing event through various channels, coordinating with vendors, and ensuring that all materials are prepared and delivered on time. They will also handle attendee registration and provide support during the event to ensure everything runs smoothly.

4. Financial Arrangements
Both parties shall share the costs and revenues of the Event as mutually agreed. Specific financial terms, including budget allocation, sponsorship contributions, and revenue sharing, shall be detailed in a separate annexure attached to this Agreement.

Behind the scenes, the generated document lands in the governed SharePoint library configured by the form creator, with metadata automatically captured from the form submission.

> **Note**
>
> You don't need access to the destination document library to submit the form. You only need access to view the generated document afterward.

Manage generated documents

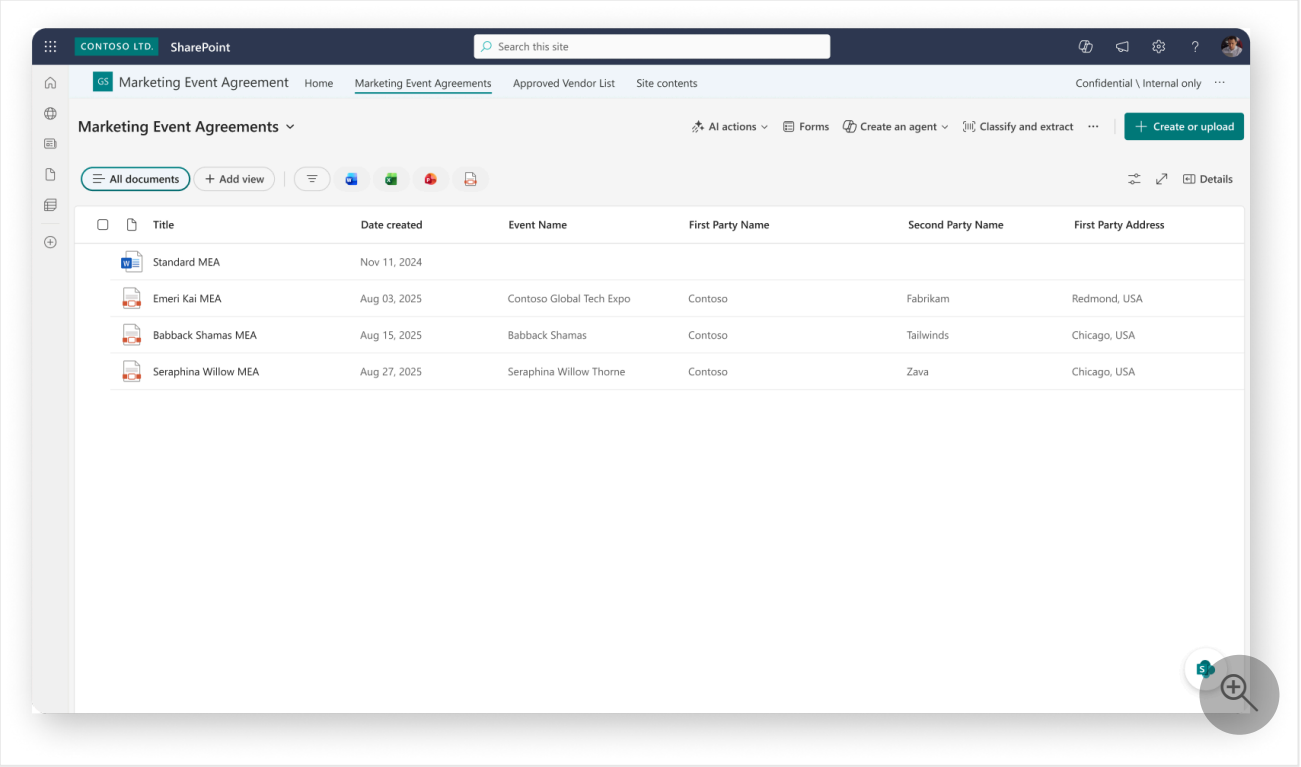
Each form submission generates a new document that's stored in the SharePoint library where you configure the form. To view generated documents:

1. Go to the SharePoint document library where you set up the form.

2. Open the folder that's linked with the form. Each generated document is stored here with the submitted values merged into the template.

3. Review the document metadata. Because the form captures rich, structured metadata from each submission, the library columns automatically populate with the field values - such as

names, dates, and other details - making it easy to sort, filter, and search across generated documents.



> **Note**
>
> Every generated document automatically receives a **reference number**—a unique identifier that stays with the document for its entire life, independent of its file name, location, or format. Each reference number is created once, never reused, and is unique across the site. The reference number becomes a usable field that you can insert into the document template just like any other field, and it stays the same when documents are copied or moved. If a document is regenerated, it gets a new reference number.
>
> Content managers can decide how it appears by adding a prefix and suffix around an automatic, system-controlled running number that's at least four digits. The prefix and suffix can include text or contextual details—such as a fiscal year, department, or vendor name—letting you build a readable format, for example `MEA-2026-0001`.

Set up downstream automation

The rich metadata captured from form submissions makes it straightforward to configure downstream automation workflows. For example, you can:

- **Set up notifications** - Use SharePoint rules or Power Automate to notify stakeholders when a new document is generated.
- **Trigger approval workflows** - Route generated documents for review and approval based on metadata values.
- **Move or copy documents** - Automatically organize generated documents into specific folders based on field values.
- **Integrate with other systems** - Use Power Automate to send document details to external systems, CRM tools, or reporting dashboards.

> **Tip**
>
> Because each form submission creates a list item with structured metadata, you can use the full range of SharePoint list automation capabilities - including rules, Power Automate flows, and API integrations - to build end-to-end business processes around your generated documents.

Edit a published form

After you publish a form, the form fields are read-only in the SharePoint form view. To make structural changes to fields, edit the template in Word.

1. From the form view in SharePoint, select the option to open the template in Word.
2. In Word, select **Edit template** in the **Manage templates** pane. You can now add, update, or remove fields.
3. When you finish making changes, select **Publish and open in Forms** to republish the template and return to the form view.
4. The form link stays the same. Form submitters automatically see the updated fields after republishing.

> **Important**
>
> After you publish a form, make structural changes to fields (adding, deleting, or modifying field types) in Word. Make non-structural changes such as showing or hiding fields, changing themes, and updating settings directly in the SharePoint form view.

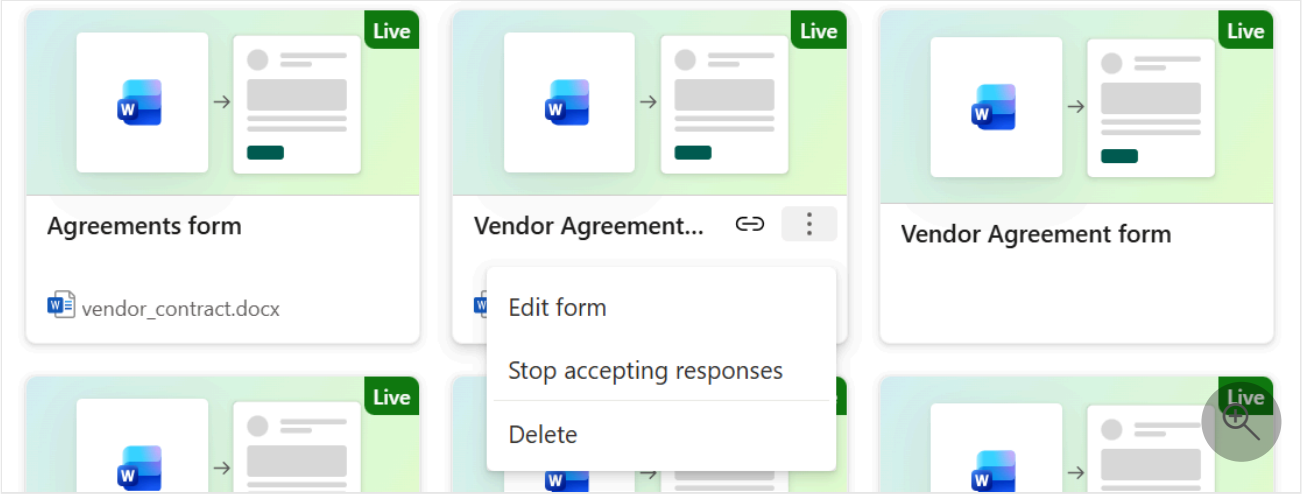
Manage forms

You can view and manage all forms associated with a document library from the **Forms** menu.

1. In the document library, select **Forms** from the command bar to see all created forms. Each form has a one-to-one mapping with a template.

2. From the forms list, you can:

    - **Edit form** — Open the form configuration to make changes.
    - **Delete form** — Remove the form. The underlying template is preserved.
    - **Start or stop accepting responses** — Toggle form availability.



Use Power Automate with structured document generation

Use Power Automate to automate document generation and build end-to-end workflows that use forms in SharePoint.

- **Form submitted (Preview)** triggers a flow when a form is submitted, so you can start workflows such as approvals or notifications.

- **Get form metadata (Preview)** retrieves the form structure, so you can map responses to fields without manual configuration.

- **Generate document from form (Preview)** creates documents by mapping input data to a document generation template and saves the output to a SharePoint library.

By using these capabilities, you can automate document creation as part of larger workflows, such as generating contracts or reports based on business events.

For more details on triggers and actions, see SharePoint connector actions and triggers.

Requirements and limitations

- **Supported file types** — Only Microsoft Word documents (.docx) support creating templates.
- **Permissions** — Form creators need Edit access on the document library. Form submitters need only the form link (Read access to the template is granted automatically).
- **Limitations**:
  - Forms are read-only once published. To make structural field changes, edit the template in Word and republish.
  - Form submitters don't automatically receive access to the destination document library. You must grant access to view the generated document separately, or the form creator can enable the receipt option.
  - PDF generation doesn't work if sensitivity labels are enabled for the site or library. Support for that feature is coming soon.

Last updated on 08/26/2026

Extend Copilot in SharePoint with skills

Skills extend Copilot in SharePoint by turning a repeatable, multistep workflow into a reusable asset. Skills can support an individual's way of working or a shared process on a SharePoint site.

You can ask Copilot to create a skill by using natural language. Copilot uses the built-in **Create skill** capability to help you define the workflow and choose between a personal skill and a site skill. You can review the draft before saving it and then reuse the skill in future prompts.

What you'll learn

- Understand the difference between personal and site skills.
- Choose the appropriate skill type for a workflow.
- Create and run personal and site skills from natural-language requests.
- Locate and manage both types of skills.

Choose a skill type

Choose the skill type based on who needs to use the workflow.

Expand table

Consideration	Personal skill	Site skill
Best fit	A workflow based on your individual preferences or way of working	A workflow that people on the same site should use consistently
Owner	The user	The site admin
Storage	The user's OneDrive	The site's **Agent Assets** library
Availability	Available to its owner across SharePoint sites	Available only on the associated site
Examples	Review documents with your own checklist; format content in your preferred style	Apply team review requirements; enforce shared document standards; update a shared list

Important

Portability doesn't grant access. A personal skill can act only on sites and content that the user already has permission to access.

What skills can do

Personal and site skills use the same built-in capabilities of Copilot in SharePoint and can chain those building blocks into a sequence of steps. Depending on what Copilot in SharePoint supports on a site, both skill types can understand and summarize content, organize files and folders, and interact with SharePoint content such as lists. Their main differences are ownership, storage, and availability.

> **Note**
>
> Skills can't connect to external systems or execute custom code. A skill can only perform actions the user already has permission to do and doesn't expand access or introduce new capabilities beyond what Copilot in SharePoint provides.

Where skills are stored

Personal skill storage

Personal skills are stored in the skill owner's OneDrive and are available to the owner across supported Copilot in SharePoint experiences.

Site skill storage

Site skills are stored as Markdown (.md) files in the site's **Agent Assets** library, under `/Agent Assets/Skills/<skill-name>/SKILL.md`. The site admin owns and manages them, while authorized site members can create or use them according to their SharePoint permissions.

You can create and manage site skills through chat. You can also review the underlying .md file directly if needed. If you edit the .md file directly, keep the format intact so Copilot in SharePoint can continue to interpret the skill correctly.

Governance and permissions

Skills are a native capability within Copilot in SharePoint. There are no separate admin controls to turn skills on or off. By default, skills are available only within the first-party Copilot in SharePoint

experience.

Neither personal nor site skills expand user permissions. A skill can act only on sites and content that the person running it already has permission to access.

Personal skill governance

Personal skills are owned by the user and stored in the user's OneDrive. They are subject to applicable OneDrive retention, sensitivity, auditing, and lifecycle policies.

Site skill governance

The site admin owns and manages site skills. The **Agent Assets** library is created and managed by the product and can't be deleted. You can, however, apply standard SharePoint file governance to site skill files (for example, permissions, retention, sensitivity labels, and auditing) the same way you would for other content stored in SharePoint.

By default, any user with **Edit** permissions on the site can create a site skill, and any user with **View** permissions can use it. If you need a different model, you can break permission inheritance on the **Agent Assets** library and apply more restrictive permissions.

Prerequisites

1. Access to a SharePoint site where Copilot in SharePoint is available.
2. Permissions to the site: **Edit** to create skills, **View** to run skills.

> **Note**
>
> You don't need to activate or configure Agent Assets before creating a site skill. Copilot automatically activates Agent Assets and creates the **Agent Assets** library when you create the first site skill.

Create a personal or site skill

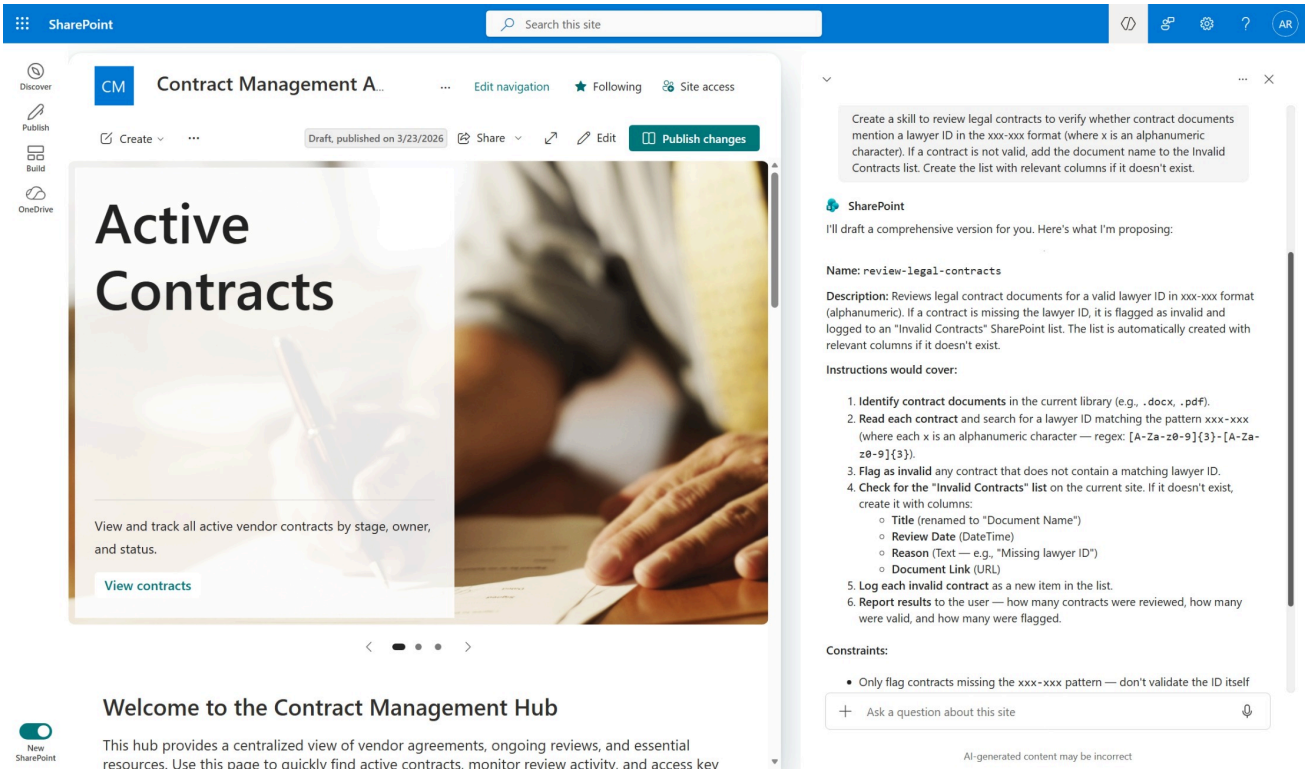
1. Open the Copilot in SharePoint chat panel from a site page or a document library. Make sure the page isn't in edit mode.
2. Ask Copilot to create a skill. Copilot uses the built-in **Create skill** capability to guide you through the process.

3. Describe the reusable workflow, including the steps, inputs, and expected outputs.

4. Specify whether the skill should be personal or site-specific. If you don't specify a type, Copilot can help you choose based on the workflow and where you want to use it.

> **Tip**
>
> **Personal skill example:** "Create a personal skill that reviews documents using my preferred structure, checks headings and terminology, and recommends consistent formatting."
>
> **Site skill example:** "Create a site skill to review legal contracts to verify whether contract documents mention a lawyer ID in the **xxx-xxx** format (where **x** is an alphanumeric character). If a contract is not valid, add the document name to the **Invalid Contracts** list. Create the list with relevant columns if it doesn't exist."

5. Review the draft skill definition that Copilot returns. If needed, ask Copilot to refine the steps, inputs, or outputs.



6. Confirm that you want to save the skill.

Run a skill

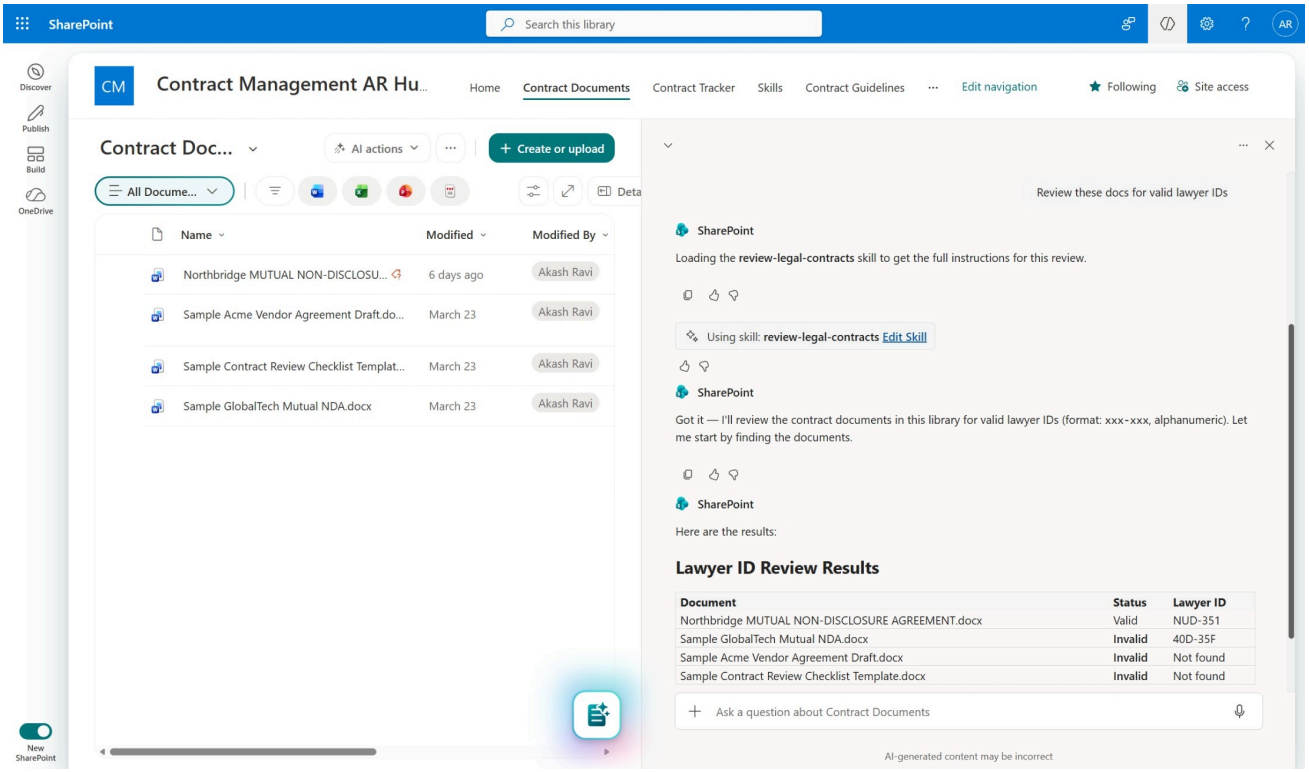
1. In the document library, select one or more files that you want the skill to work on. This step is optional but recommended for testing.

2. In chat, ask a question or give an instruction that matches the skill's purpose. Copilot in SharePoint automatically loads the right skills needed to execute the prompt.

   A personal skill can load for its owner across SharePoint sites. A site skill can load only on its associated site.

3. If needed, invoke the skill explicitly by name. For example, "Run *skill name* on the selected documents."

4. When Copilot runs your request, look for the skill indicator card in the chat UI to confirm that a skill was loaded. Provide any additional details Copilot asks for.



Built-in skills

Copilot in SharePoint includes built-in skills that are available by default. These skills help you manage the skill lifecycle, including creating, checking, and improving skills. Microsoft creates and maintains built-in skills as part of Copilot in SharePoint.

Built-in skills aren't personal or site skills, and they aren't stored in OneDrive or the **Agent Assets** library. Users can't edit them directly, but they can extend their functionality by creating their own skills. The built-in **Create skill** capability guides users through creating personal and site skills.

To view the built-in skills currently available, enter `/skills` in the Copilot in SharePoint chat and review the skills listed under **Built-in skills**.

Related articles

Get started with Copilot in SharePoint

Create autofill columns

Create a document library with AI

Automate workflows with Copilot in SharePoint

Last updated on 09/29/2026

Upcoming changes to classic publishing sites, classic pages, and custom scripting in SharePoint Online

Microsoft SharePoint continues to evolve to help organizations create and manage content more securely, easily and intelligently. As part of this evolution, new changes will be introduced to classic publishing sites, classic user-created pages, and custom scripting in SharePoint Online to reduce security and governance risks associated with legacy customization models, and help organizations move to more secure, manageable, and mobile-ready modern SharePoint experiences.

The change rollout begins on March 1, 2027, and continues on October 1, 2028. Start assessing your environment and planning modernization now.

> **Important**
>
> These changes don't delete or modify existing classic page content. Affected pages remain available for viewing but become read-only when the applicable phase takes effect.

Rollout timeline

Phase 1 — Beginning March 1, 2027

Changes for all tenants

- Creation of new classic publishing sites will be disabled for both site collections and subsites.
- Activation of classic publishing feature will be disabled for both site collections and subsites.
- The `AllowClassicPublishingSiteCreation` tenant setting will be enforced as `False` and cannot be changed.

Additional changes for new tenants created on or after March 1, 2027

- Users can no longer create new classic pages.
- The ability to add or update custom scripts will be disabled by default.
- The `DenyAddAndCustomizePages` site setting will be enforced as `True` and cannot be changed.

Phase 2 — Beginning October 1, 2028

The Phase 1 page and scripting restrictions will extend to all remaining existing tenants:

- Classic user-created pages become read-only. Users can no longer create or edit classic pages.
- The ability to add or update custom scripts will be disabled by default.
- The `DenyAddAndCustomizePages` site setting will be enforced as `True` and cannot be changed.

> **Important**
>
> Existing classic user-created pages will remain accessible for viewing in a read-only form after Phase 2.

Classic user-created pages in scope

The read-only change applies to:

- Wiki pages
- Web Part pages
- Blog pages
- Publishing pages
- Custom ASPX pages created by using SharePoint Designer or third-party solutions

Other classic experiences, including list and library views and list form pages, aren't in the current scope. However, custom scripts embedded in those experiences are subject to the changes to custom script creation and updates.

Cloud environments in scope

The changes to classic user-created pages apply across all Microsoft 365 environments, including:

- Microsoft 365 Government (GCC, GCC High, and DoD)
- Office 365 air-gapped cloud environments
- Microsoft 365 operated by 21Vianet

Why this change is happening

Classic pages and legacy customization models rely on server-side rendering and custom scripting. These technologies can increase security risk, administrative complexity, and

maintenance costs. They also limit the consistency, manageability, and pace of innovation available with modern experiences.

Modern SharePoint provides:

- More secure and well-governed collaboration environments
- A foundation for current and future AI-powered experiences
- Mobile-ready experiences
- Easier administration and long-term maintenance

What you should do now

Use a phased approach to reduce migration risk and give site owners time to validate modernized pages.

1. Discover and assess your classic environment

Identify active classic sites and pages across your tenant.

- Use the Microsoft Purview Audit `SharePoint Classic Activities` category and the `ClassicPageCreated`, `ClassicPageEdited`, and `ClassicPageViewed` events to understand current usage.
- Run the Microsoft 365 Assessment Tool to identify classic pages, Web Parts, customization patterns, and modernization feasibility.
- Review the requirements for the classic pages assessment before collecting usage data.

If your assessment finds no classic publishing sites, classic user-created pages, or affected custom scripts, no action is required for these changes.

2. Prioritize by business importance and usage

Start with frequently edited, high-traffic, or business-critical pages. Group pages by complexity and modernization pattern so you can migrate representative waves and reuse what you learn.

3. Transform pages to modern SharePoint experiences

Use the classic page transformation guidance and PnP PowerShell for deterministic page transformation. Validate each generated page before expanding to a larger wave.

For complex pages with custom HTML, script editor content, or layouts that need human judgment, evaluate the open-source SharePoint Page Migration Agent (preview). Preview and

community tools might not fully automate complex scenarios and don't have a Microsoft support SLA. Highly customized pages can require redesign or manual rebuilding.

4. Modernize in waves

Combine centralized planning and prioritization with execution by site owners. A wave-based migration makes it easier to validate content, links, permissions, Web Parts, and page layout before expanding the migration.

Frequently asked questions

What happens to my existing classic sites?

Existing classic sites remain available. These changes don't modify or delete classic page content. You can modernize many classic sites in place rather than rebuild them from scratch. For guidance, see Modernize your classic SharePoint sites.

What happens to classic pages that I don't modernize?

For tenants created on or after March 1, 2027, classic user-created pages are read-only by default beginning on that date. For all remaining existing tenants, classic user-created pages that haven't been modernized become read-only beginning October 1, 2028. Users can continue to open and view the pages, but they can't edit them or create new classic user-created pages. Modernize pages that must remain editable after the applicable date.

Can I create classic publishing sites in the future?

Beginning March 1, 2027, you can't create site collections or subsites that use the following publishing-related templates. Other classic templates aren't affected by this change.

Expand table

Template ID	Template
`BLANKINTERNETCONTAINER#0`	Publishing Portal Site
`CMSPUBLISHING#0`	Publishing Site
`BLANKINTERNET#0`	Publishing Site Blank
`ENTERWIKI#0`	Enterprise Wiki

Template ID	Template
`SRCHCEN#0`	Enterprise Search Center
`SPSSITES#0`	Site Directory
`SPSNHOME#0`	News Home Site
`PRODUCTCATALOG#0`	Product Catalog
`SPSREPORTCENTER#0`	Report Center
`SPSTOPIC#0`	Topic Area Template

Can I migrate classic sites and pages from SharePoint Server to SharePoint Online?

Beginning March 1, 2027, classic publishing sites can't be migrated as-is to a newly created classic publishing site in SharePoint Online because creation of those sites is disabled.

Classic user-created pages can still be migrated, but they become read-only in SharePoint Online when the applicable phase takes effect. Script-based page elements and other customizations might not be preserved. Plan to modernize these pages as part of the migration.

Are other classic pages affected?

No. The page read-only change applies only to the classic user-created page types listed in this article. List and library views, list form pages, and other classic experiences aren't in the current scope and might be addressed on a separate timeline. Custom scripts embedded in those experiences are still subject to the custom scripting changes.

Related resources

- Guide to the modern experience in SharePoint
- Allow or prevent custom scripts in SharePoint sites
- Modernize your classic SharePoint sites
- Transform classic SharePoint pages to modern pages
- Microsoft 365 Assessment Tool

Last updated on 08/28/2026

Moving from publishing sites to communication sites

Being able to communicate broadly using attractive sites and pages is a key feature of organization intranets. For example, you might have an HR department home page that serves up important communication to hundreds or thousands of employees.

In the modern SharePoint experience, communication sites fulfill the same purpose as traditional publishing sites: to communicate broadly to a large audience while maintaining a level of control on the creation side. Communication sites support most of the same scenarios as publishing sites, and more capabilities are coming soon. Best of all, communication sites are easier to build and maintain and include new features such as a modern authoring canvas. They allow you to share news, reports, statuses, and other information in a visually compelling format. To sum up: you can quickly create beautiful pages that look great on mobile devices and that are accessible by default - all without heavy developer investment. You can get inspired with some great examples in the SharePoint Look Book .

Traditionally, sites and pages like this have been designed and built using the publishing features of Microsoft SharePoint – either team sites with publishing enabled or fully structured publishing sites. You could specify page layouts, design pages, and set up content approval workflows. Publishing features allowed for a tight level of control by a small number of people while allowing broad communication to many people. But with traditional design and deployment of publishing sites, developer involvement is usually required for customization of site functionality, navigation elements, and included investment in master pages, CSS, JavaScript, and web parts. Additionally, traditional site types designed for a PC browser may not work well or look attractive on mobile devices, and design and development efforts are needed to provide proper interaction with tools like screen readers or high-contrast color schemes. With all this, it commonly takes more time and resourcing to build, test, and deploy when using the classic publishing infrastructure.

Classic publishing site features that are not supported in modern communication sites

- **Classic Publishing Feature** – Turning on the classic publishing feature for a modern communication site is not supported. Instead, modern versions of the publishing features

will be available outside of the publishing infrastructure. For more info, see Enable publishing features.

- **Community Site Feature** – The Community Site feature is not supported for modern communication sites.
- **Video Content Type** – Video content type features are not supported for a modern communication site. Use the Stream web part as the modern replacement.
- **Classic Web Parts** – Classic web part features are not supported on a modern communication site. This includes script editor and content editor web parts. For more info, see Using web parts on SharePoint pages.
- **Save Site as a template** – The save site as a template feature is not supported on a modern communication site. For more info, see Save, download, and upload a SharePoint site as a template.
- **Save List/Library as a template** – The save list as a template feature will only work when custom scripts are allowed. For more info, see Allow or prevent custom script.
- **Reset to Site Definition** – The reset to site definition feature is not supported on a modern communication site.
- **Classic Record Center** – The Record Center feature is not supported on a modern communication site. Instead, use the modern records management capabilities. For more info, see Microsoft Purview Records Management and Learn about Records.
- **SharePoint 2010 and 2013 Workflows** – SharePoint 2010 and 2013 Workflows are not supported with modern communication sites. Instead, use Microsoft Power Automate. For more info, see Microsoft Power Automate and SharePoint 2010 workflow retirement.
- **Subsites** – The subsite feature is not supported on modern communication sites but is supported on Teams sites. Creation of subsites is available but not recommended. Consider using the modern hub site feature instead. For more info, see What is a SharePoint hub site?.

Get started: Move from a publishing site to a modern communication site

So, how you do move from publishing sites to communication sites? First, know that you don't have to change all your site collections and sites at once. If you have a very large collection of publishing sites, you can gradually begin using modern sites, pages, and web parts. For example, you can start with creating one or more new communication sites as home pages for existing sites. If you have several departments in your organization, you can create modern sites and implement modern features one department at a time. You can choose a strategy that works best for the size and scale for your organization. To help with determining your strategy, you can use

the SharePoint Modernization scanner tool to find out which classic publishing features are used in your organization or in a subset of site collections. Find this tool and more information about it in Modernize classic publishing portals.

When you are ready to begin creating new communication sites and using modern features, here are some areas to consider:

- Structure and navigation
- Branding and site design
- Pages
- Web parts
- Sharing news
- Permissions and sharing
- Audience targeting
- Multilingual communication sites

Structure and navigation

Let's say your organization has a publishing site for Human Resources, with subsites for Benefits, Policies, Training, and Careers. It might be organized like this:

In this example, Human Resources is your site collection that includes four subsites for Benefits, Policies, Training, and Careers.

In the modern experience, you can use a hub to mimic the same structure while carrying design elements across related sites:

This structure is no longer hierarchical in the technical sense. Instead, it is a flat structure where each site is connected because they are part of the Human Resources hub. In this scenario, each site can be a communication site. But you can also include team sites for collaboration within the hub, while limiting their availability to the entire organization. With a hub, you can:

- Apply common navigation and branding across associated sites.
- Search across all associated sites.
- Easily aggregate news and other types of content across all sites.

The best part about hubs is that they are so flexible. As your organization changes, your intranet organization can change just as quickly, just by associating or disassociating a site.

To learn more about planning hubs, see Planning your SharePoint hubs. To create a hub, see Create a hub site. To learn more about navigation options and planning, see Planning navigation for modern SharePoint.

Branding and site design

In the modern SharePoint experience, it is easy to *change the look* and feel of your sites to match your company or organizational brand. You can customize the logo, colors, navigation, header, and footer – often without writing a single line of code. Branding can be applied at the site level, to a group of sites, or to all sites within your organization. SharePoint includes an updated set of default site themes and site designs (or templates) that are responsive and look great on any device. With site themes, you can customize your site's logo and colors to match your brand.

Coming soon are multiple options for headers and footers on communication sites, and options for navigation such as a mega menu. For these and other features that are in development, rolling out, or launched, check the Microsoft 365 Roadmap. To learn more about branding

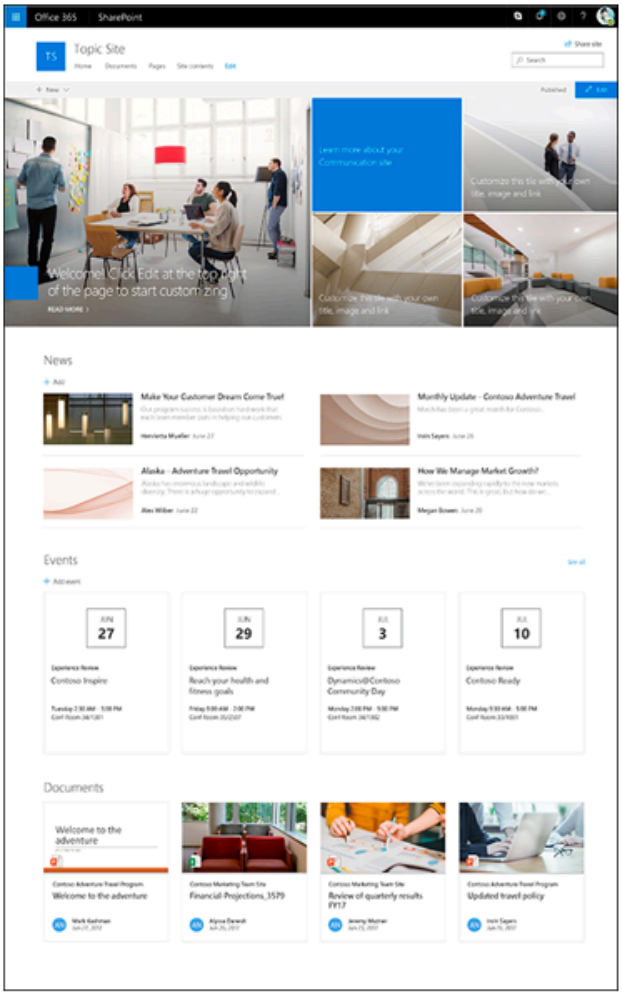
options, see Branding your SharePoint site. To learn more about planning navigation, see Planning navigation for modern SharePoint.

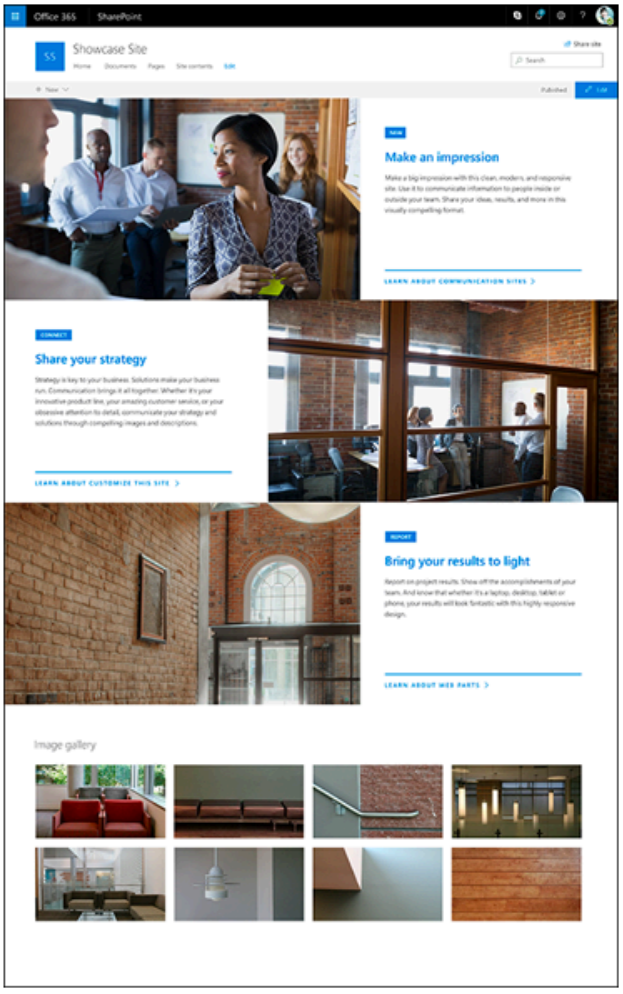
Classic site templates and modern site designs

SharePoint handles branding differently for classic site templates, like the publishing site. Instead of a site template, communication sites have three out-of-the-box layout designs: *Topic*, *Showcase*, and one open layout: *Blank*.

When you create a communication site in SharePoint, you can start with a blank site or choose one of the other site designs, each of which comes with a default set of web parts. The options available are:

- **Topic** to share information such as news, events, and other content. The home page includes a Hero web part, to highlight and link to important content; a News web part, to distribute announcements, reports, status, and more; an Events web part based on a calendar list; and a Highlighted content web part to dynamically show documents based on your criteria.
- **Showcase** to use photos or images to showcase a product, team, or event. This is a highly visual design that includes a Hero web part with large imagery in a layered layout, and an Image gallery that can be displayed in several different layouts, such as a tiled layout or carousel layout.
- **Blank** to create your own design.





If you want more customized branding and theming applied to each new site, you can use site designs with site scripts to provide custom configurations to apply when new sites are created. They can be used each time a new site is created to apply a consistent set of actions. Common site design actions typically affect the site itself, such as setting the theme or logo, creating lists, or configuring navigation. You can find more information on how to use site designs and scripts at SharePoint site design and site script overview.

Pages

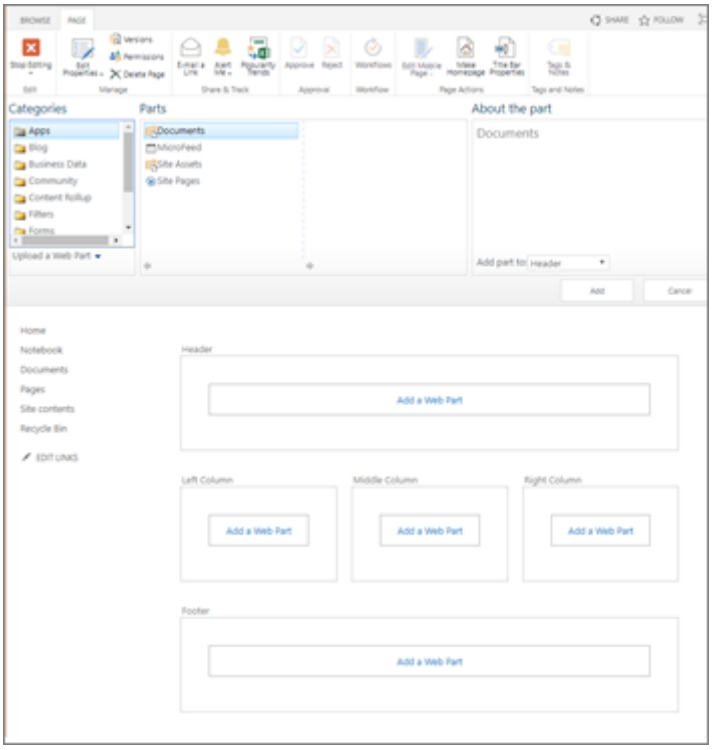
Master pages and page layouts are components of a publishing site. Page layouts and master pages work together to create the layout for a traditional SharePoint web page. Modern communication sites do not utilize master pages or page layouts, but do provide a greater level of flexibility for site owners and page authors.

In the classic experience, you may have created web part pages based on page layouts. Page layouts can be locked down to control what is authored on a page. However, they are inflexible in that pages based on page layouts are confined to the layout and options provided by the page layout.

> **Important**
>
> When customizing classic pages (for example, through master pages), avoid using or referencing internal or undocumented SharePoint components (such as non-public assemblies or APIs), as these are not supported and may change or be removed.
>
> Avoid customizations that rely on page markup or DOM structures, as they will not carry forward to modern experiences. Use supported options like [SharePoint Framework] and modern pages instead.

Modern pages provide a fast, easy way to build responsive pages using the functionality of modern web parts. Pages are similar to classic web part pages and publishing pages, but are less structured and easier to create. And, each page's layout is flexible in that it can be changed anytime to align to the content for the page and the experience you are trying to create for your readers.

Classic web part page:

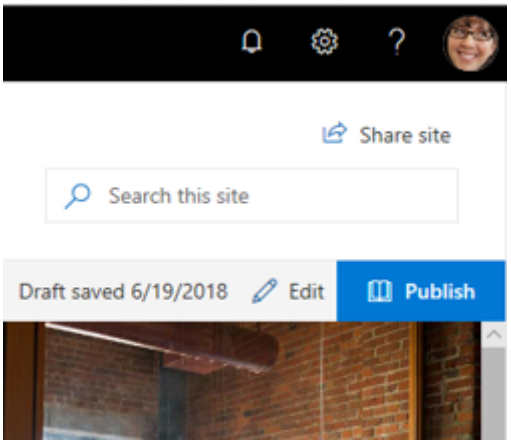


Modern web part page:

Pages are made up of a title area and sections. Sections can include a full-width column for full-bleed images or hero web parts or up to three regular columns. You can add a variety of web parts to the page, and easily move them around on the page to get the look you want. Check out this short video to see how to create, layout, and publish a page:

https://videoplayercdn.osi.office.net/hub/?csid=ux-cms-msoffice&uuid=RE2ZpSP&AutoPlayVideo=false

Publishing: On a classic publishing site, commands for Publish and Check in/Check out are available on the ribbon. In the modern experience, it is even easier for authors to discover how to edit and make their content visible with buttons to Edit, Save, and Publish right on the page. When a modern page is in edit mode, it is automatically checked out to the person who is editing. When a page is saved or published, it is automatically checked in. If someone has a page open for editing but hasn't made any changes to it for at least 5 minutes, it is automatically saved and taken out of Edit mode so that others can access and edit the page.



To learn more about how to create and edit pages, see Add a page to a site.

Content approval for pages

Content approval ensures that edits to pages meet company policies or standards. Classic publishing allows for content approval on pages using out-of-the-box workflows. Modern pages also provide for content approval and once it is enabled, users need only to press a Submit button on the page to start the approval flow. The recommended way to do this is to use the built-in Power Automate commands. Learn more at Page approval flow.

Scheduling

Scheduling content to "go live" at specific times is a feature of classic publishing sites and now a feature of modern pages. To learn more about modern page scheduling, see Schedule a SharePoint page or news post to go live at a specific time.

Moving from classic to modern pages: At this time, there is not a way to change a classic page into a modern page without using a multi-step code solution, which may work well for IT Admins and developers. If you are neither of those, we recommend you gradually start planning for and creating modern pages, as needed.

If you are using a classic publishing site, you should know that it is possible to create modern pages in a classic publishing site, but there is not an automated way to move from a publishing site to a communication site. To move to a communication site, we recommend you begin creating modern pages in a new communication site rather than in a classic publishing site.

There are several important advantages to moving to a new communication site. One of the most important advantages is that you can use the upgrade as an opportunity to re-think the "story" of your site and validate that the content is needed, up-to-date, and relevant to users. In addition, you can use the move as a time to look at the content that is no longer needed it and remove it. Cleaning up your unused content improves both user experiences and search outcomes – so consider the move as an opportunity to clean up legacy content and establish new governance practices to make sure that your content is kept up-to-date going forward.

Wiki pages

Wiki pages are a content type available in publishing sites, but they are not available in communication sites. However, you can create modern pages using either a Text web part or Markdown web part to cover many of the same scenarios as Wiki pages. Note that Wiki syntax

is not available in a Text web part, with the exception of adding a hyperlink with the use of brackets "[[".

Web parts

Modern pages use modern web parts. Modern web parts are designed to be easier to use, faster, and look great on all devices. It is important to note that for security reasons, modern out-of-the-box web parts do not allow for the insertion of custom code including JavaScript.

> **Important**
>
> Classic web parts cannot be used on modern pages and modern out-of-the-box web parts cannot be used on classic pages. Developers may create custom modern web parts that may work on both classic and modern pages. Additionally, there is not a 1:1 mapping of classic to modern web parts, but there are web parts that have similar purposes.

To learn about all of the modern web parts, see Using web parts on SharePoint pages. To learn about modern web parts that have similar purposes to classic web parts, see Classic and modern web part experiences.

For developers, the SharePoint Framework allows for the building of custom modern web parts that appear alongside out-of-the-box web parts in the web part toolbox. The SharePoint Framework also allows for custom extensions, the use of the Microsoft Graph API, as well as secure access to third-party solutions and APIs secured by Microsoft Entra ID. Developers are encouraged to consult the SharePoint starter kit, where you'll find a fully built sample solution that includes numerous web parts, extensions, and other components that you can use as an example and inspiration for your own customizations. Additionally, find design guidance and standards for web parts at Designing great SharePoint experiences.

Web parts unique to publishing sites

Publishing sites include a variety of web parts that enable authors to insert video, rich text, forms, and dynamic content onto a site page. Three web parts that have been unique to publishing sites are the *Content query* web part to show dynamic content, the *Summary links* web part, and the *Table of contents* web part to display links to important content. The following are a selection of modern web parts that help fulfill the same purposes as these web parts.

Content query: The Highlighted content web part serves a similar purpose as the Content Query web part. It dynamically displays content from a document library, a site, a site collection,

or multiple sites. With the Highlighted content web part, many of the advanced and confusing search/query options of the Content Query web part have been replaced with streamlined query options. However, unlike its classic counterparts, custom display templates are not allowed.

Summary links, Table of contents: There is not a 1:1 mapping of these web parts to modern web parts. However, there are several modern web parts that can fulfill the same purpose, which is to help your users navigate from a page level to important content. These are:

> Quick links
>
> With Quick links, you can add links to a page and set display options like a carousel format called filmstrip, list, or a smaller compact format. Each of the links in the compact format can be arranged and displayed with or without images. It is currently not possible to populate Quick links based on a SharePoint list.
>
> Link
>
> The Link web part shows one complete URL link and adds the ability to show or hide a preview pane with the link target.
>
> Hero
>
> The Hero web part is, by default, included on both the Topic and Showcase communication site templates. It is an attractive way to bring focus and visual interest to your page. You can display up to five items in the Hero web part and use compelling images, text, and links to draw attention to each. You can use the Hero web part at the top of a page or anywhere in the page as well. In general, you don't want to use more than one hero web part on the same page. And, if you have more than 5 critical items to emphasize, consider using a different method to feature this content, such as the Quick links web part in a grid view.
>
> Text
>
> In the Text web part, you can add links within your content using the toolbar. Additionally, with the Text web part you can create a link that opens in a new tab.

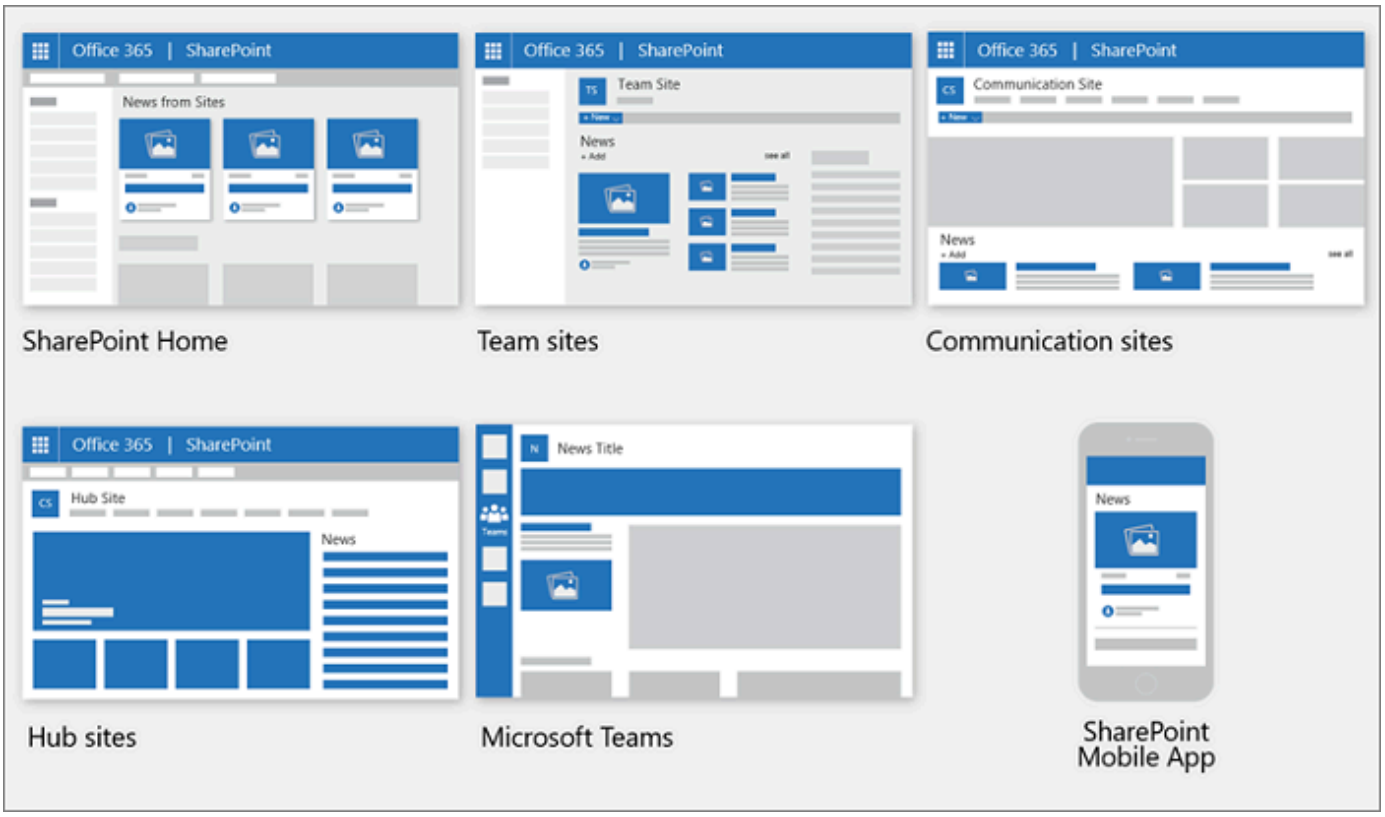
To learn more about modern web parts that have similar purposes to classic web parts, see Classic and modern web part experiences.

Sharing news

The News feature is an effective distribution system created to deliver relevant content across your organization.

Built on modern pages and web parts, you can tell stories with rich, attractive content that can be dynamically shown on the SharePoint start page, on team sites, communication sites, hubs, and even on the SharePoint mobile app. You can also choose to show News in a Teams channel.

Where news can be distributed



News posts can be created from the SharePoint start page, from a team site or communication site, and from pages that have the News web part on them already. You can customize sources and layouts of news, and you can also organize and order news posts as well as target specific audiences for news. To learn more about how to create and share News, see Create and share news on your SharePoint sites.

Users and permissions

You probably don't want a large group of people having the ability to make changes to your site that communicates information to a whole department or organization. Publishing portal sites included roles such as Approvers and Designers. Communication sites present a simplified experience, so not all these roles are present by default. While you could set up roles like these manually, we recommend that you use the new sharing interface, which also can provide you with needed controls.

To help you limit who has permissions to change the site, communication sites are not group-enabled like modern team sites. This means that a communication site is not automatically connected to a group of people with edit permissions. However, you can give specific people permission to make changes to your communication sites by selecting **Site permissions** under **Settings** and then **Share a site**. You can use Advanced permissions to give even more granular permissions if needed. For more in-depth information on the differences between classic and modern permissions, see Permissions and Sharing in the SharePoint modern experience.

You can also share a communication site externally if needed from the SharePoint admin center.

Audience targeting

In the classic experience, many types of content can be targeted to appear only to people who are members of a particular group or audience. This capability is available in the modern experience with modern Pages and documents, the News web part, the Highlighted content web parts, and navigation. For example, if you have two departments within your organization that have different policies, you can choose to show a News post about a policy to just the people in the department that the policy applies to. To learn how to enable audience targeting, see Target content to specific audiences.

Multilingual communication sites

If your organization spans a diverse population, you may want to make content in your intranet sites available in multiple languages. User interface elements like site navigation, site title, and site description can be shown in the user's preferred language. Additionally, you can provide pages and news posts on communication sites that you translate and that are shown in the user's preferred language.

To create pages on communications sites in different languages, you use the translation feature to make copies of pages created in your default language. The copies can then be manually translated. Published translation pages are automatically shown in the appropriate language site, including in the News and Highlighted content web parts for each language.

To learn how to set up and use the multilingual feature for communication sites, see Create multilingual communication sites, pages, and news.

> **Note**

At this time, the multilingual feature is available for communication sites only.

Last updated on 06/12/2026

Customizing SharePoint

In earlier versions of SharePoint, it was possible to make changes to a SharePoint environment by deploying custom code that would run in the physical SharePoint server environment. Changes made to SharePoint that didn't require the deployment of custom code were referred to as "customizations", because the changes were not fundamentally changing the product's functioning but were rather configuring the existing product in a unique way. Examples of customizing SharePoint Server have included deploying custom branding elements such as master pages and style sheets to a site collection; deploying pre-configured web parts to a web part gallery; creating custom workflows in SharePoint Designer; changing the look and feel of list forms using InfoPath; and more. Because of the shared nature of the SharePoint infrastructure, Microsoft does not allow the deployment of custom code to its environment. As a result, the concept of customizing SharePoint as opposed to deploying custom code is no longer a relevant paradigm. However, it's still helpful to think of ways that SharePoint can be customized, or configured uniquely, in a broader sense of the word.

The purpose of this document is to help you understand how you can customize your SharePoint environment using modern tools and techniques.

Branding

Modern SharePoint sites allow you to change the look of the site by modifying elements such as the site logo and the colors used throughout the site. Branding your SharePoint site can help you match a site to a brand as well as help users differentiate between multiple SharePoint sites. While several themes options are available by default, it's also possible to specify unique theme colors by supplying SharePoint with a custom configuration file. Older, "classic" SharePoint sites allow administrators to apply custom branding and page layouts to a SharePoint site by applying a custom master page, applying a custom theme to a site, deploying custom page layouts, and more. Because classic sites are not as fast and mobile-friendly as modern sites, Microsoft recommends using modern sites going forward.

Navigation

Navigation helps users find the information they need quickly by providing links to pertinent information in a persistent manner. Planning your navigational strategy in modern sites is a critical element in the usability of your SharePoint environment. Modern SharePoint sites provide

a streamlined model for adding navigational elements using the browser. The position of the navigation is determined by the kind of site being viewed, the size of a user's screen, and whether the megamenu option has been enabled for the site. Additionally, modern sites can take advantage of hub site navigation.

Note that earlier versions of SharePoint allowed navigational elements to be dynamically generated using the structured navigation and managed metadata navigation providers. These options are no longer available in modern sites. However, if you are using a classic site with modern pages, you can still use these providers and the modern pages will reflect the correct navigational links. In terms of layout, because modern sites do not allow you to customize the site's master page or style sheet, it's not possible to move the position of the navigation elements on the page as could be done in classic SharePoint sites.

Page content

Nearly every version of SharePoint has had a way of creating custom layouts for web pages, whether that was by selecting a web part page, a wiki page layout, or a publishing page layout. Modern sites also provide a similar functionality. However, rather than providing a static layout that provides a set number of editable regions on the page, modern pages provide the ability for page editors to "stack" column layouts on a row-by-row basis. Page editors can also choose various options related to how the title region of the page is displayed. Finally, the most fundamentally way to customize a modern page is to place custom content on the page. This can be done by adding modern web parts to the page. Note that web parts used in classic web sites will not work in modern sites. However, it is possible to create and deploy custom ("client-side") web parts that were created using the SharePoint Framework.

Workflows

We recommend using Power Automate for configuring and executing all workflows in your Microsoft 365 environment, including SharePoint. For example, it's possible to create unique approval workflows for content stored in SharePoint. Additionally, it's possible to use Power Automate as the default workflow engine for approving SharePoint page content, directly from the SharePoint user interface. Flows can be triggered by SharePoint actions (such as when an item is created in a list), or perform actions within SharePoint (such as update a list item). While SharePoint Designer workflows are still supported, new workflows should be created using Power Automate.

Forms

Power Apps can be used to create custom forms for use in modern SharePoint sites. There are several ways in which these Power Apps forms can be used in your SharePoint site:

- As a custom SharePoint list form
- As a custom SharePoint list view
- As a stand-alone app that uses a SharePoint as its data source

You can embed a Power App form in a modern page using the Power Apps web part.

Forms that were previously created using InfoPath and hosted in SharePoint using InfoPath Forms Services should be converted to Power Apps forms, as Microsoft has announced the deprecation of InfoPath.

Microsoft Forms can also be used for easily creating light-weight forms. Like Power Apps, it's possible to embed a Microsoft Form in a page using the Microsoft Forms web part.

Customize your SharePoint site programmatically

Legacy versions of SharePoint Server relied on solution packages to deploy content and make configuration changes to SharePoint sites. It's still possible to programmatically provision sites as well as customize team sites, lists and libraries, and site pages. There are various methods for making programmatic changes to your SharePoint environment, including using the Office Developer Patterns and Practices APIs, the Microsoft 365 CLI, the Microsoft Graph API, the SharePoint Framework, and more.

Use the SharePoint Framework (SPFx) to render custom web parts on a modern SharePoint page. Additionally, Extensions to the SPFx provide the ability to add scripts to pages, create modified views of data, and surface new commands in the SharePoint user interface. SPFx application packages can be deployed to SharePoint sites using the SharePoint App Catalog.

Use third-party apps and solutions

Not only can you deploy custom apps to your environment, but you can also get apps from the SharePoint Store. For more information, see Use the App site to make custom business apps available for your SharePoint environment and Add an app to a site.

If you want to change the settings for whether or not site users can acquire apps from the SharePoint Store, see Configure settings for the SharePoint Store.

If you are interested in exploring services or applications from Microsoft partners that are available for SharePoint, browse Microsoft 365 apps on Microsoft AppSource. There are also

many open-source solutions developed by the collective SharePoint community, including Microsoft, MVPs, Partners, and Customers on the Microsoft 365 Developer Patterns and Practices GitHub site.

Examples of modern customization approaches

The following table gives an example of older methods for customizing sites along with a current recommended approach:

Expand table

Legacy	Modern
Implement branding using custom master pages, page layouts, and themes	Use the "apply a look" option to customize branding elements like logo, header, footer and colors
Use custom navigation providers such as structured navigation or managed metadata navigation to dynamically generate navigational elements	Manually specify navigational links
Create a wiki page and choose a text layout option to modify the layout of the page	Create a modern page and add section layouts to the page to arrange web parts on the page.
Create a workflow using SharePoint Designer	Create a workflow using Power Automate
Customize a SharePoint form using InfoPath	Customize a SharePoint form using a Power App
Deploy a web part to a site using a sandbox solution	Use the SharePoint App Catalog to deploy a client-side web part to a site

Last updated on 06/24/2026

Change the default list and library experience

The new SharePoint list and library experience is faster, simpler, and responsive on mobile devices. It also supports many new capabilities that are not available in the classic experience, including Power Apps and Power Automate integration, the Filters pane, and column formatting. Many sites that have features or customizations that don't work in the new experience will automatically switch back to the classic experience. For more information about this behavior, see Differences between the new and classic experiences for lists and libraries. To detect lists that won't work well with the new experience, run the SharePoint Modernization scanner.

It's no longer possible to select the classic experience as the default for all sites in your organization. Instead, we recommend setting it for only the specific sites that need it. You can activate the site collection feature *SharePoint Lists and Libraries experience* to turn off the new list and library experience for a site collection. To learn how, see Enable or disable site collection features. For info about changing this setting using PowerShell, see Opting out of the modern list and library experience.

> **Note**
>
> Users can select the default experience for an individual list or library, overriding what you set. For info, see Switch the default experience for lists or document libraries from new or classic.

Last updated on 06/25/2026

Classic home page modernization

Modernizing the home page of a classic SharePoint team site makes the page look great on any device and makes it easier for users to customize the layout and see news and activity. This article covers all the details on how automatic modernization works and the controls you have as an administrator.

How it works

If a classic team site meets the following criteria for being updated, the home page will automatically modernize the next time a user visits. When users first experience the change, they'll see a walkthrough that highlights the new capabilities and includes a link to a help article with more details.

We encourage users to adopt the change in order to benefit from the power of modernized pages. However, if site admins or site owners want to revert to the classic home page, they can. Instructions are available in the support article.

Update criteria

- Classic team site (STS#0) only.
- Home page name in any language is 'Home.aspx'.
- Contains default web parts only: getting started (GettingStartedWebPart), Newsfeed (SiteFeedWebPart), and document library (XsltListViewWebPart).
- No text is present (wiki HTML isn't customized).
- DisplayFormTemplateName = "WikiEditForm".
- ModernizeHomepageOptOut feature isn't activated.
- No custom master pages are detected.
- The classic publishing feature is turned off.

> **Note**

All update criteria must be met for a team site home page to qualify for the automatic upgrade.

The technical details

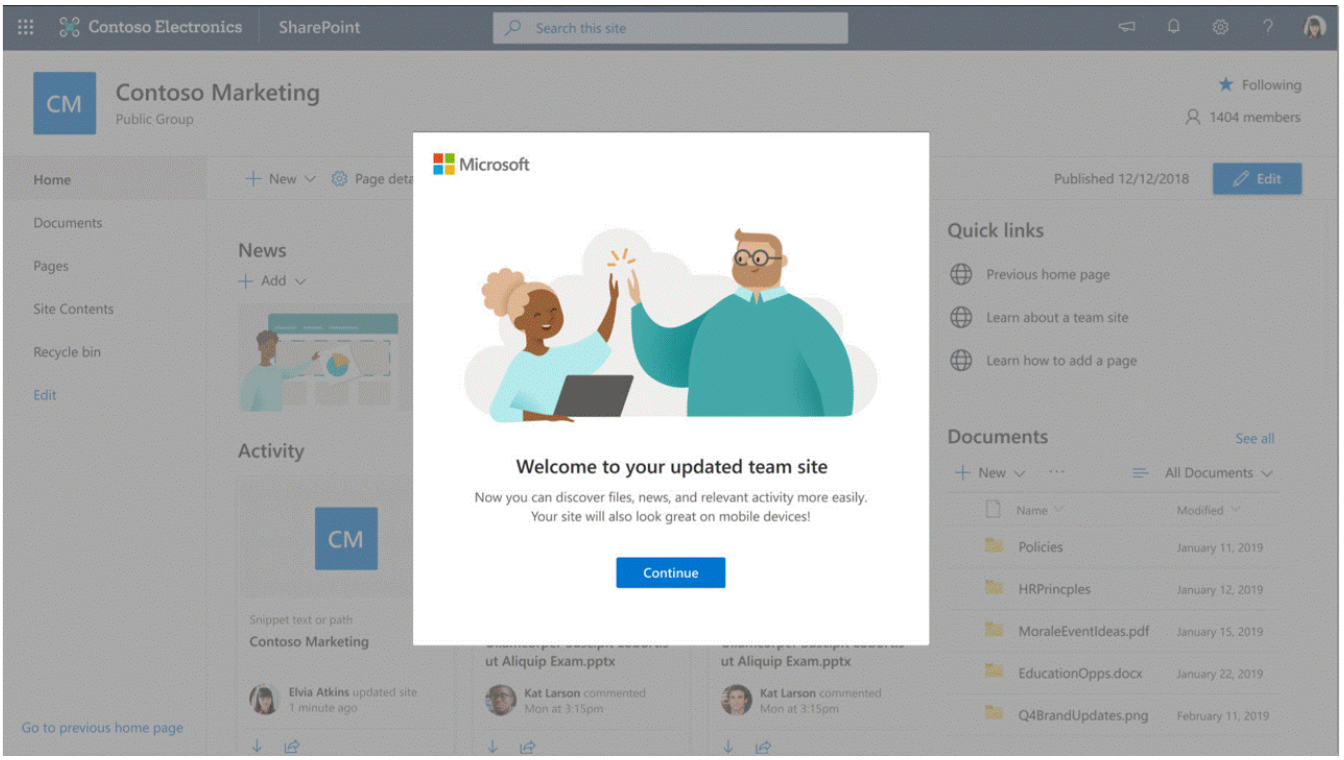
- Applies to both STS#0 site collections and all corresponding subsites.
- The update applies only to the home page. No other classic pages will be changed. We recommend using the SharePoint PnP modernization framework for all other site pages.
- The new modern home page is named 'Home.aspx' and the classic page gets renamed to 'Home(old).aspx'.
- This update doesn't create a Microsoft 365 Group for the team site.
- Classic site themes may not be identical once your page is updated to modern. Learn how to apply custom styles and color to your site.
- Only site admins can revert to the classic home page through the link appearing in the left navigation. Site owners can revert to the classic page by visiting site pages and marking the classic page as their home page.
- Update happens on demand based on next site access. If a subsite is accessed, it will trigger the update for its root site collection and its other subsites. Remember, the update only applies to the root site collection and subsites if the criteria are met.
- We don't check the state of custom actions, therefore they won't transfer to your new modern page.
- We don't check the state of modern SharePoint lists and libraries for classic sites.

Why update classic team site home pages to modern?

Over the years, SharePoint modern pages have become powerful tools for collaboration and productivity at work and we want more users to take advantage of these capabilities. Automatically modernizing team site home pages that aren't customized is the first step to helping classic site users get more out of SharePoint.

What to expect after a classic team site home page is updated to modern

When users first experience the change, they'll see a walkthrough that highlights the new capabilities and includes a link to a help article with more details like this:



For more training, download the classic to modern walkthrough.

How to prevent specific sites from being updated

To disable the update on specific sites, use one of the following options:

Option 1: Use PnP PowerShell to prevent a specific site from being upgraded by enabling a web scoped feature on each site and sub site that's being impacted.

Connect to the site using Connect-PnPOnline. For example,

```
Connect-PnPOnline -Url https://[tenant].sharepoint.com/sites/siteurl -Credentials $cred
```

To prevent modernization of an uncustomized home page, run:

```
Enable-PnPFeature -Identity F478D140-B148-4038-9CB0-84A8F1E4BE09 -Scope Web
```

If you later want to re-enable modernization of that page, run:

```
Disable-PnPFeature -Identity F478D140-B148-4038-9CB0-84A8F1E4BE09 -Scope Web
```

Option 2: Don't know what sites will be impacted by this change? You can use the SharePoint Modernization Scanner and run the scanner in "HomePageOnly" mode. The output of the modernization scanner run contains a file called SitesWithUncustomizedHomePages.csv. Use this

file to get a list of sites and sub sites that will get a modern homepage. This tool will enable you to message users impacted if desired. If needed, use the PowerShell cmdlet above, or the following sample script to opt multiple sites out of the update: https://github.com/SharePoint/sp-dev-modernization/tree/dev/Scripts/HomePageModernizationOptOut

Option 3: Add an out-of-the-box SharePoint web part, a custom web part, or text to your team site home page.

> **Note**
>
> It's highly recommended that you modernize home pages to benefit from the latest SharePoint features and to improve the viewing experience for users on desktop and mobile. Another option for modernizing classic sites is to enable the communication site experience on a specific classic site. For info, see **Enable the communication site experience on classic team sites**.

What about new classic team sites STS#0 created after this change?

Classic team sites (STS#0) created after **May 1, 2020** won't get updated.

Can I also modernize the other pages in my sites?

For a more consistent user experience, we recommend that you modernize all pages on classic team sites. This can be self-service done via the open-source SharePoint PnP Page Transformation solution.

Getting excited about modern?

For more help in transitioning to modern, refer to the following resources:

- Guide to modern experience in SharePoint
- SharePoint Look Book templates
- Modernizing your classic sites
- Transform classic pages to modern pages
- Enable the communication site experience on classic team sites

Last updated on 06/24/2026

Enable the communication site experience on classic team sites

A SharePoint communication site is a great tool for sharing information with others in your organization. Your users can share news, reports, statuses, and other information in a visually compelling format. Now, any classic team site can have this capability too. By running a PowerShell cmdlet, you can bring modern communication site features to your classic team sites.

Requirements

- The site must be a **classic team site that's not connected to a Microsoft 365 group** (the STS #0 (Team site classic experience) site template).
- The site must be the top-level site in the site collection. It can't be a subsite.
- The user who runs the PowerShell cmdlet must have full owner permission on the target site.
- The site must not have SharePoint Server Publishing Infrastructure enabled at the site collection level or SharePoint Server Publishing enabled at the site level. Learn how to enable and disable publishing features. If these features were previously enabled but are now deactivated, go to the site contents page and make sure it doesn't still contain a Pages library. Learn more about features enabled on a publishing site.

Effects of this change

- A new modern page is created in the site and set as the home page. To see the changes, open the site in a new tab .
- Any user that has access to the site sees the new home page with the default web parts and content immediately. Until you're ready to launch the new communication site experience, you can change the home page back to the former page.
- Full width pages with horizontal navigation are available. (The top navigation from classic view is hidden, but can be seen on classic pages like the site settings page.) You can now customize the navigation on this site.
- Custom script isn't allowed on the site.
- Minor versioning on the Site Pages library is enabled. Learn more about versioning
- Site Pages are the default content type in the Site Pages library
- No site permissions are changed.

- The SharePoint lists and libraries experience isn't changed.
- Any content types enabled in the site aren't changed.
- If the classic site collection had subsites, they aren't changed.
- If you plan to launch this site as a high traffic portal or share the site with a large number of users, make sure to follow the portal launch guidelines.

Run the PowerShell cmdlet

You can use either the SharePoint Online Management Shell **OR** SharePoint PnP PowerShell to enable the communication site experience on a classic team site. We recommend that you test the experience with a minimally used classic site before running it on popular classic sites in your organization.

> **Important**
>
> After you enable the communication site experience on a classic site, you can't undo the change.

SharePoint admin instructions

1. Download the latest SharePoint Online Management Shell. Version 20122.1200 or later is required.

   > **Note**
   >
   > If you installed a previous version of the SharePoint Online Management Shell, go to Add or remove programs and uninstall "SharePoint Online Management Shell."

2. Connect to SharePoint as a global admin or SharePoint admin in Microsoft 365. To learn how, see Getting started with SharePoint Online Management Shell.

3. Run the following command:

   PowerShell

   ```
   Enable-SPOCommSite -SiteUrl <URL of target site>
   ```

For more info about this cmdlet, see Enable-SPOCommSite.

Site admin instructions

1. Learn how to use SharePoint PnP PowerShell commands.

2. In Windows 10, run the following commands in PowerShell:

PowerShell

```
Install-Module SharePointPnPPowerShellOnline
Connect-PnPOnline -Url <Url of Targetsite> -Credentials (Get-Credential)
Enable-PnPCommSite
```

Frequently asked questions

Will this cmdlet change all my classic sites?

- No. The cmdlet can be run on one site at time.

Will this cmdlet change the site template?

- No. The cmdlet enables communication site features, but the site still has the STS#0 site template. The site continues to appear as "Team site (classic experience)" in the SharePoint admin center.

Why can't I use this cmdlet on publishing sites?

- The modern communication site experience isn't compatible with SharePoint Server publishing features.

Can I run this command on the root site in my organization?

- Yes, if you meet the requirements listed at the beginning of this article.

How can I get a list of all classic sites that have the communication site experience enabled?

PowerShell

```
function Get-CommsiteEnabledSites{

    $adminUrl = Read-Host "Enter the Admin URL of O365 (eg. https://<Tenant Name>-
admin.sharepoint.com)"
    $userName = Read-Host "Enter the username of O365 (eg.
admin@<tenantName>.onmicrosoft.com)"
    $password = Read-Host "Please enter the password for $($userName)" -AsSecureString

    # set credentials
```

```
    $credentials = New-Object -TypeName System.Management.Automation.PSCredential -
argumentlist $userName, $password
    $SPOCredentials = New-Object
Microsoft.SharePoint.Client.SharePointOnlineCredentials($userName, $password)

    #connect to to Office 365

    try{

        Connect-SPOService -Url $adminUrl -Credential $credentials
        write-host "Info: Connected succesfully to Office 365" -foregroundcolor green

    }

    catch{

        write-host "Error: Could not connect to Office 365" -foregroundcolor red
        Break connectToO365

    }
    get-siteCollections
}



function get-siteCollections{

    write-host "----- List of classic sites with comm site feature enabled  -------" -
foregroundcolor green

#Get all site collections
    $siteCollections = Get-SPOSite

    #loop through all site collections
    foreach ($siteCollection in $siteCollections){

        #set variable for a tab in the table
        $pixelsweb = 0
        $pixelslist = 0
        $enabledCommSite = Get-SPOIsCommSiteEnabled($siteCollection.url)
        $background = "white"
        if($enabledCommSite -ne ""){
            $background = "cyan"
        }
    }
}

function Get-SPOIsCommSiteEnabled($url){

    #fill metadata information to the client context variable
    $featureID = "f39dad74-ea79-46ef-9ef7-fe2370754f6f"
    $context = New-Object Microsoft.SharePoint.Client.ClientContext($url)
    $context.Credentials = $SPOcredentials
    $web = $context.Web
    $context.Load($web)
```

```
    $context.load($web.Features)

    try{

        $context.ExecuteQuery()
        $isCommSiteEnabled = $web.Features | Where {$_.DefinitionID -eq $featureID}
        $webTemplate = $web.WebTemplate

        if($webTemplate -ne "SITEPAGEPUBLISHING" -AND $isCommSiteEnabled){
            write-host "Found $($web.url)" -foregroundcolor green
            return "Enabled"

        }
    }
    catch{

        write-host "Could not find web" -foregroundcolor red

    }

    return ""
}

Get-CommsiteEnabledSites
```

See also

For info about automatically modernizing the home page on classic sites, see Classic home page modernization.

Last updated on 06/25/2026

Differences between the classic and modern search experiences in SharePoint

Article • 08/14/2024

SharePoint in Microsoft 365 has both a classic and a modern search experience. Microsoft Search in SharePoint is the modern search experience. Both search experiences use the same search index to find results.

As a search admin, you can't enable or disable either search experience, both are enabled by default. Users get the classic search experience on publishing sites, classic team sites, and in the Search Center. Users get the Microsoft Search experience on the SharePoint start page, hub sites, communication sites, and modern team sites. Learn about classic and modern sites

The most visible difference is that the Microsoft Search box is placed at the top of the SharePoint, in the header bar. Another difference is that Microsoft Search is personal. The results you see are different from what other people see, even when you search for the same words. You'll see results before you start typing in the search box, based on your previous activity and trending content in Microsoft 365, and the results update as you type. Learn more about the Microsoft Search experience for users .

Search admin can customize the *classic* search experience, but not the Microsoft Search experience. As a search admin you can *tailor* Microsoft Search to your organization so it's easy for your users to find often needed content in your organization.

For example, if your organization has Microsoft Search fully deployed, custom result sources at site collection or tenant level won't affect the search result. The search admin can use Microsoft search verticals instead. To learn more, see Manage search verticals.

You use the SharePoint admin center to manage classic search and the Microsoft 365 admin center to manage Microsoft Search. Certain aspects of the classic search settings also impact the modern search experience:

- The search schema determines how content is collected in and retrieved from the search index. Because both search experiences use the same search index to find search results, any changes you make to the search schema, apply to both experiences. The Microsoft Search experience doesn't support changing the sort order of results or building refiners based on metadata. Therefore, the following search schema settings don't affect the Microsoft Search experience:

  - Sortable
  - Refinable
  - Company name extraction (deprecated since November 15, 2019)

- In environments where vertical configuration is available the modern search experience only shows results from the standard result source (Local SharePoint Results). To learn more, see Manage search verticals.

- In environments where vertical configuration is not available the modern search experience only shows results from the default result source. If you change the default result source, both modern and classic search experiences are impacted.

- Depending on the search scenario, some Microsoft Search features might not work if the classic global Search Center URL is not set to point to the URL of the default classic Search Center. Depending on your tenant, this URL is "yourcompanyname.sharepoint.com/search" or "yourcompanyname.sharepoint.com/search/pages". Furthermore, ensure that the Search Center site collection exists and that all users have read access to it.

- If you temporarily remove a search result, the result is removed in both search experiences.

- The classic search experience lets admins define **promoted results** to help users find important content, while the Microsoft Search experience uses **bookmarks** to achieve the same. For clouds which support **bookmarks**, only **bookmarks** will show at the organization level on the **All** tab. For clouds without **bookmark** support, promoted results will show on the **All** tab if they searched across the whole organization. On site or hub site scope, promoted results defined at that site will show. In addition promoted results defined at the tenant level will show **All** tab.

  > **Tip**
  >
  > If you want the the same bookmark to appear for both the organization level and site levels, you must create both a tenant **bookmark** and a **promoted result** for the sites where you want the bookmark to appear.

Feedback

Was this page helpful? Yes No

Provide product feedback

About the SharePoint Administrator role in Microsoft 365

Article • 05/29/2025

Users assigned the SharePoint Administrator role have access to the SharePoint admin center and can create and manage sites, designate site admins, manage sharing settings, and manage Microsoft 365 groups, including creating, deleting, and restoring groups, and changing group owners.

Global Administrators in Microsoft 365 can assign users the SharePoint Administrator. The Global Administrator role already has all the permissions of the SharePoint Administrator role.

For info about assigning a user the SharePoint administrator role, see Assign admin roles in the Microsoft 365 admin center. If a user's role is changed so they gain or lose access to the SharePoint admin center, it takes about an hour for the change to take effect.

> **Important**
>
> Microsoft recommends that you use roles with the fewest permissions. Using lower permissioned accounts helps improve security for your organization. Global Administrator is a highly privileged role that should be limited to emergency scenarios when you can't use an existing role.

Site management

Global Administrators and SharePoint Administrators don't have automatic access to all sites and each user's OneDrive, but they can give themselves access to any site or OneDrive. They can also use Microsoft PowerShell to manage SharePoint and OneDrive. See more about this role's Key tasks of the SharePoint admin.

Site admins have permission to manage sites, but they don't need to have an admin role in Microsoft 365, and don't have access to the SharePoint admin center.

For info about adding or removing a site admin, see Manage site admins.

Term store administration

There's a separate role within SharePoint called the Term Store administrator. Users assigned to this role can add or change terms in the term store (a directory of common terms you want to use across your organization). To learn more, see Assign roles and permissions to manage term sets.

API access

To manage API access in the SharePoint admin center, you need at least a application administrator role. For more information, see Manage access to Microsoft Entra ID-secured APIs.

Key tasks of the SharePoint admin

Here are some of the key tasks users can do when they're assigned to the SharePoint Administrator role:

- Create sites
- Delete sites
- Manage sharing settings at the organization level
- Add and remove site admins
- Manage site storage limits

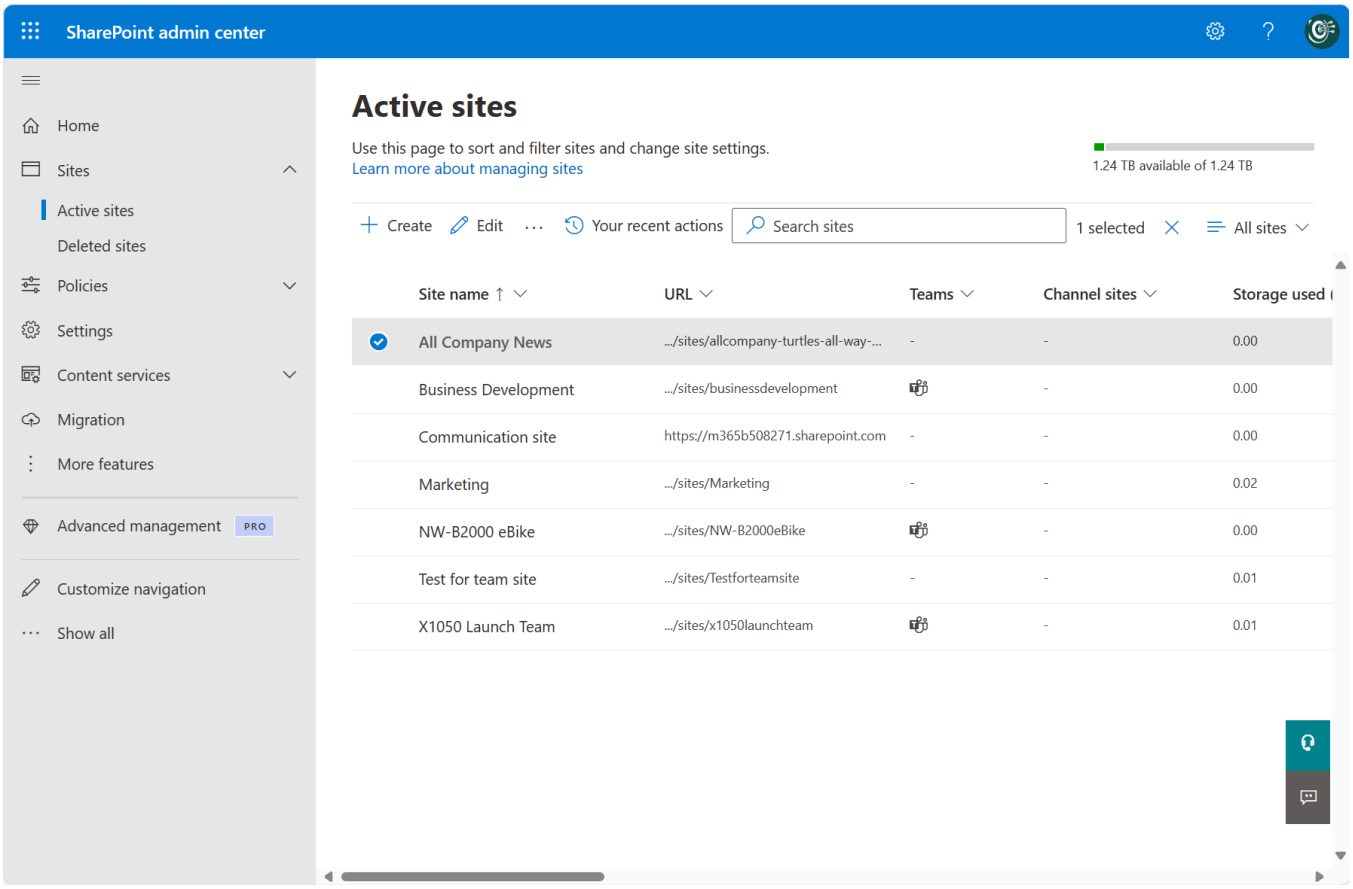
Related articles

About Microsoft 365 admin roles

Getting started with SharePoint Online Management Shell

Manage sites in the SharePoint admin center

The **Active sites** page of the SharePoint admin center lets you view the SharePoint sites in your organization, including communication sites, channel sites, and sites that belong to Microsoft 365 groups. It also lets you sort and filter sites, search for a site, and create new sites. The Active sites page lists the root website for each site collection.



> **Tip**
>
> As a companion to this article, see our **Microsoft Sharepoint setup guide** to review best practices and understand the deployment process from site creation to data migration. Features include protection labels, data loss prevention policies, and file activity auditing. For a customized experience based on your environment, you can access the **Set up SharePoint in Microsoft 365 guide** in the Microsoft 365 admin center.

- Sites with these URLs aren't included for the Active sites page:

Expand table

URL	Description
/sites/contentTypeHub	Content hub host
/sites/CompliancePolicyCenter	Policy center
/portal/hub	PointPublishing hub
/search	Search site
/personal/	OneDrive sites

- Sites with these templates aren't included for the Active sites page:

Expand table

ID	Name	Description
3	CENTRALADMIN#	Central admin site
16	TENANTADMIN#	Tenant admin site
21	SPSPERS#	SharePoint Portal Server personal space
54	SPSMSITEHOST#	My Site host
65	POINTPUBLISHINGHUB#	PointPublishing hub
66	POINTPUBLISHINGPERSONAL#0	Personal blog
67	POINTPUBLISHINGTOPIC#0	PointPublishing topic
69	TEAMCHANNEL#0	Microsoft Teams Channel Site
69	TEAMCHANNEL#1	Microsoft Teams Channel Site with feature optimization
70	CSPCONTAINER#	CSP container
301	REDIRECTSITE#	Redirect site
3500	POLICYCTR#	Compliance policy center
6000	REVIEWCTR#	Review center
10043	FunSite#	SharePoint tenant fundamental site
30003	TestSite#	Test site

Note that you may see differences between the sites in the active sites list and those listed in the SharePoint site usage report in the Microsoft 365 admin center because both the site templates and URLs listed above are included in the SharePoint site usage report.

For more info about tasks on the **Active sites** page, see:

- Create a site
- Register a site as a hub site and Unregister a site as a hub site
- Change sharing settings for a site
- Delete a site
- Manage site storage limits

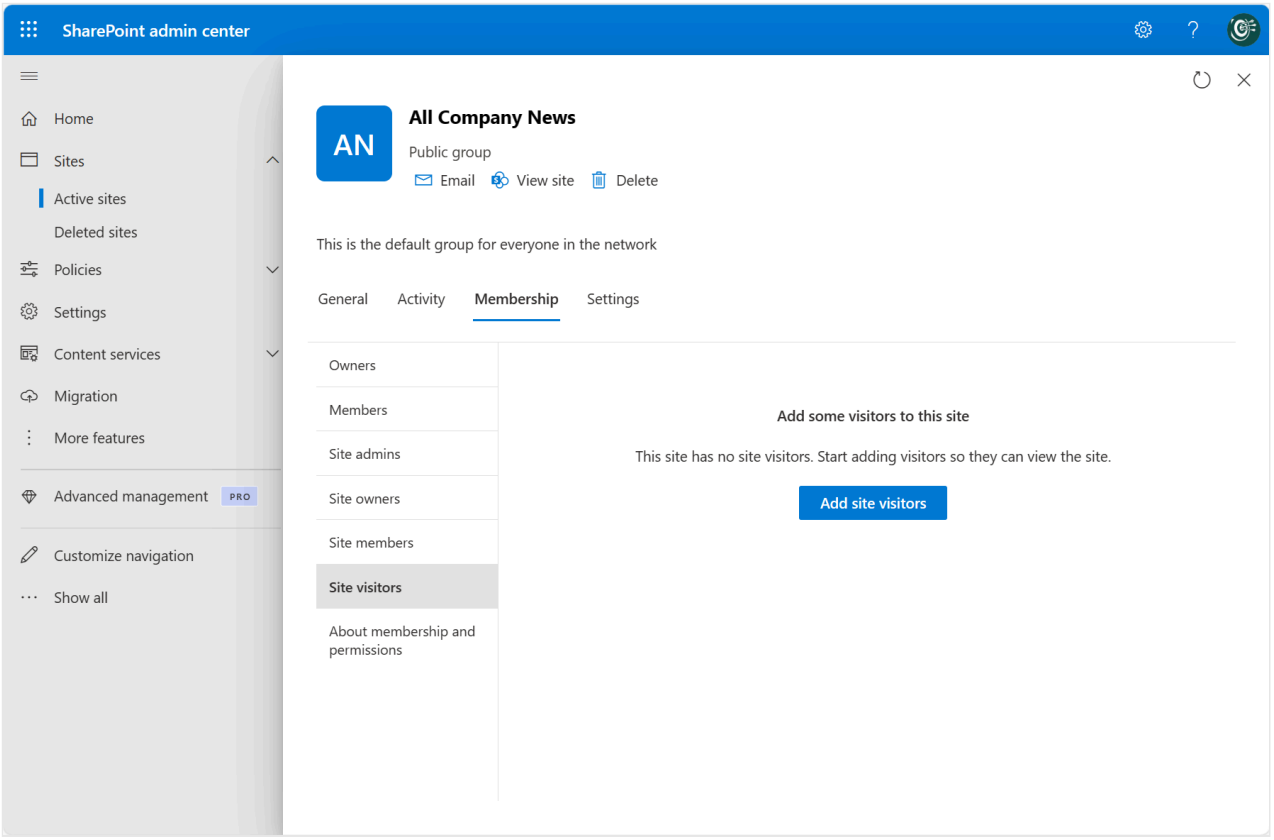
Add or remove site admins and group owners

For all site types except channel sites, you can add or remove site admins and change the primary admin. For group-connected team sites, you can also add and remove group owners. Note that if you remove a person as a primary admin, they will still be listed as an additional admin. For info about each role, see About site permissions.

1. In the SharePoint admin center, select **Sites** > **Active sites** or browse to the **Active sites page**.

2. In the left column, select a site.

3. Select **Membership** on the command bar to open the details panel to update the permissions of the members.



4. Add or remove people or change their role, and then select **Save**.

Change a site's hub association

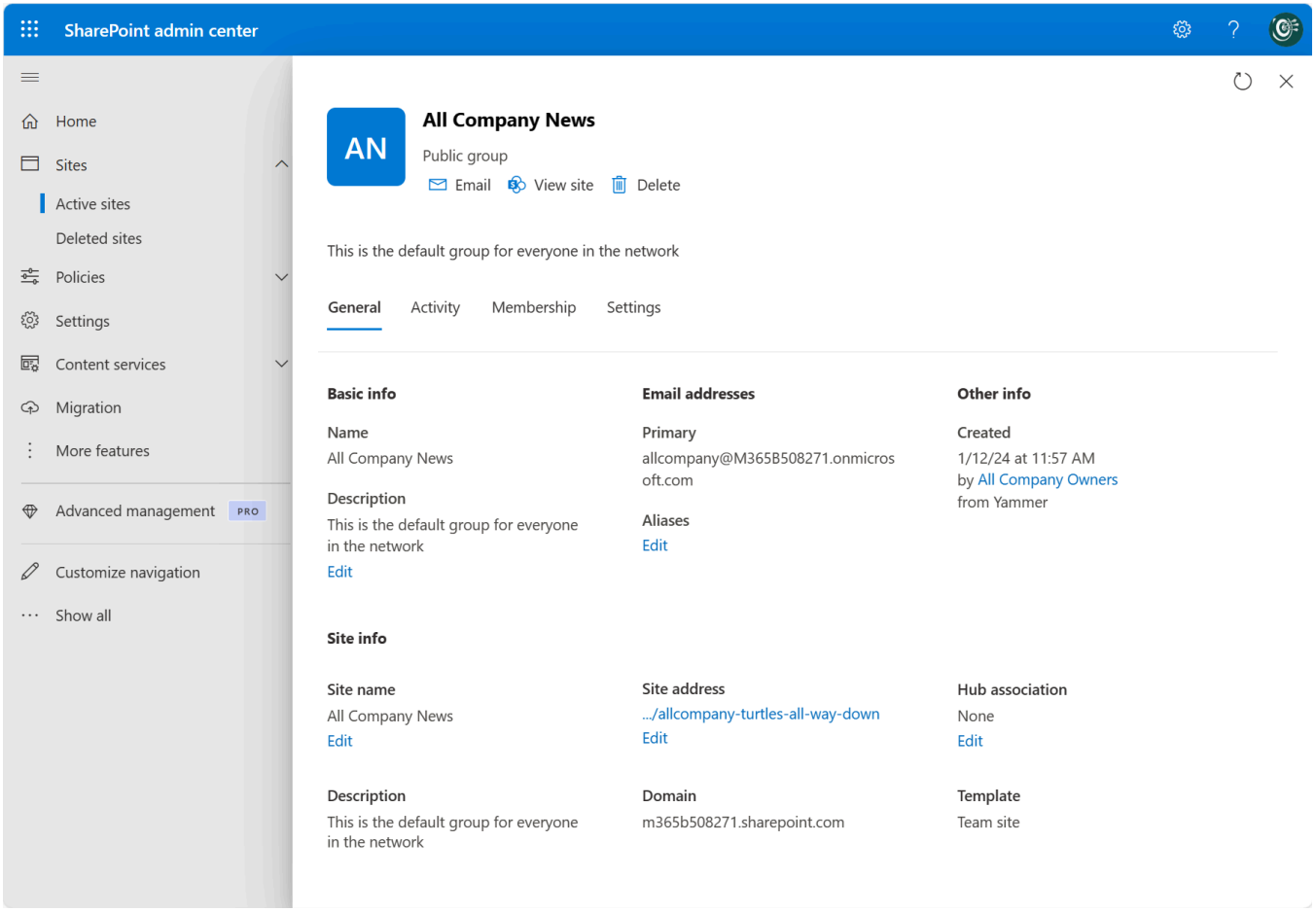
1. In the SharePoint admin center, select **Sites** > **Active sites** or browse to the **Active sites page**.

2. In the left column, select a site.

3. Select **Hub** on the command bar. The options that appear depend on whether the site you selected is registered as a hub site, or associated with a hub. The Hub menu lets you register a site as a hub site, associate it with a hub, change its hub association, and unregister it as a hub site. For more information, see More info about hubs.

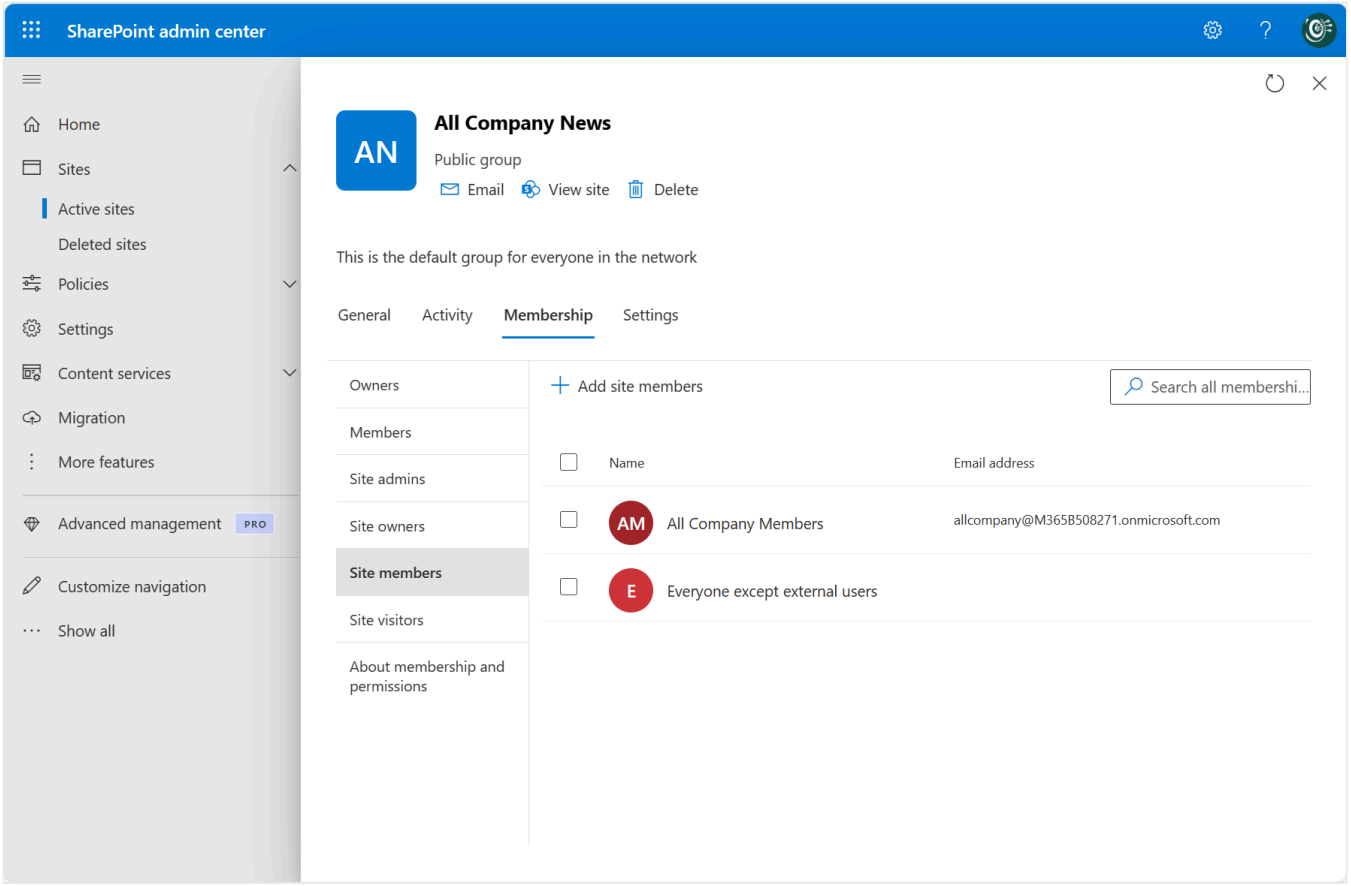
View site details

For more info about a site, select the site name or select anywhere on the site row except on the URL column to open the details panel. For channel sites, select the link in the **Channel sites** column and then select the site name.



To view site activity including the number of files stored and storage usage, select the **Activity** tab. Activity information is not available for US Government GCC High and DoD customers.

To view site admins, owners, members, and visitors, select the **Membership** tab.



For info about the roles in this panel, see About site permissions.

Related topics

Manage site storage limits

Last updated on 01/13/2026

Customize the SharePoint admin center site list

Article • 03/01/2023

The **Active sites** page in the SharePoint admin center lets you view the SharePoint sites in your organization. You sort and filter sites, search for sites, and customize the columns and views.

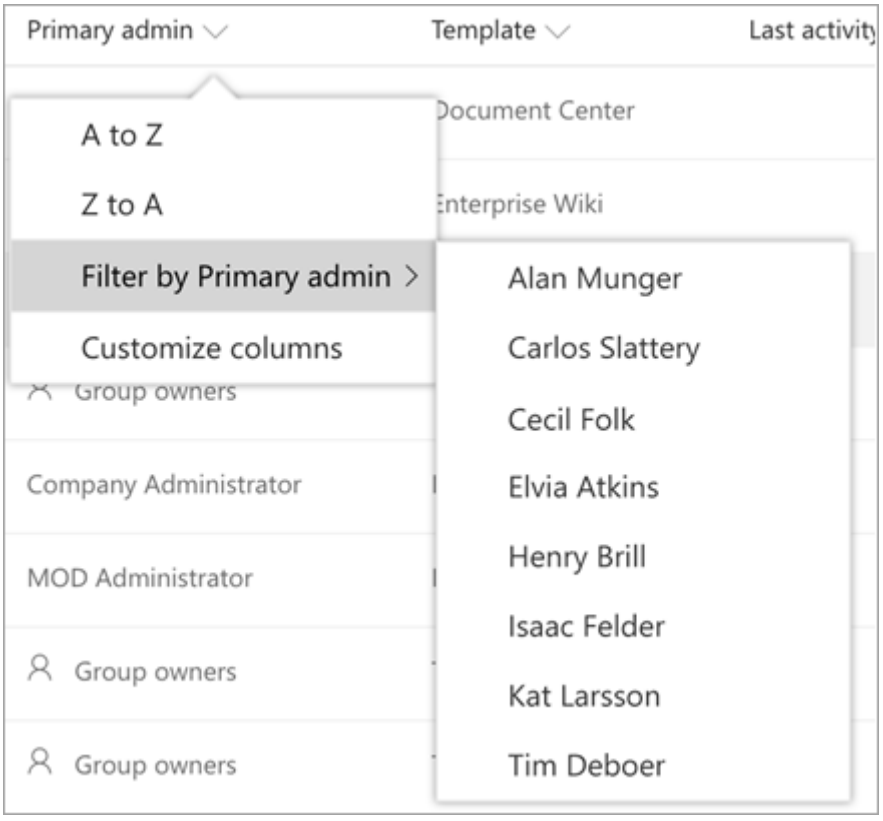
Sort and filter the site list

Sorting and filtering the site list is just like sorting and filtering other lists in SharePoint.

1. Select the arrow next to the column header.

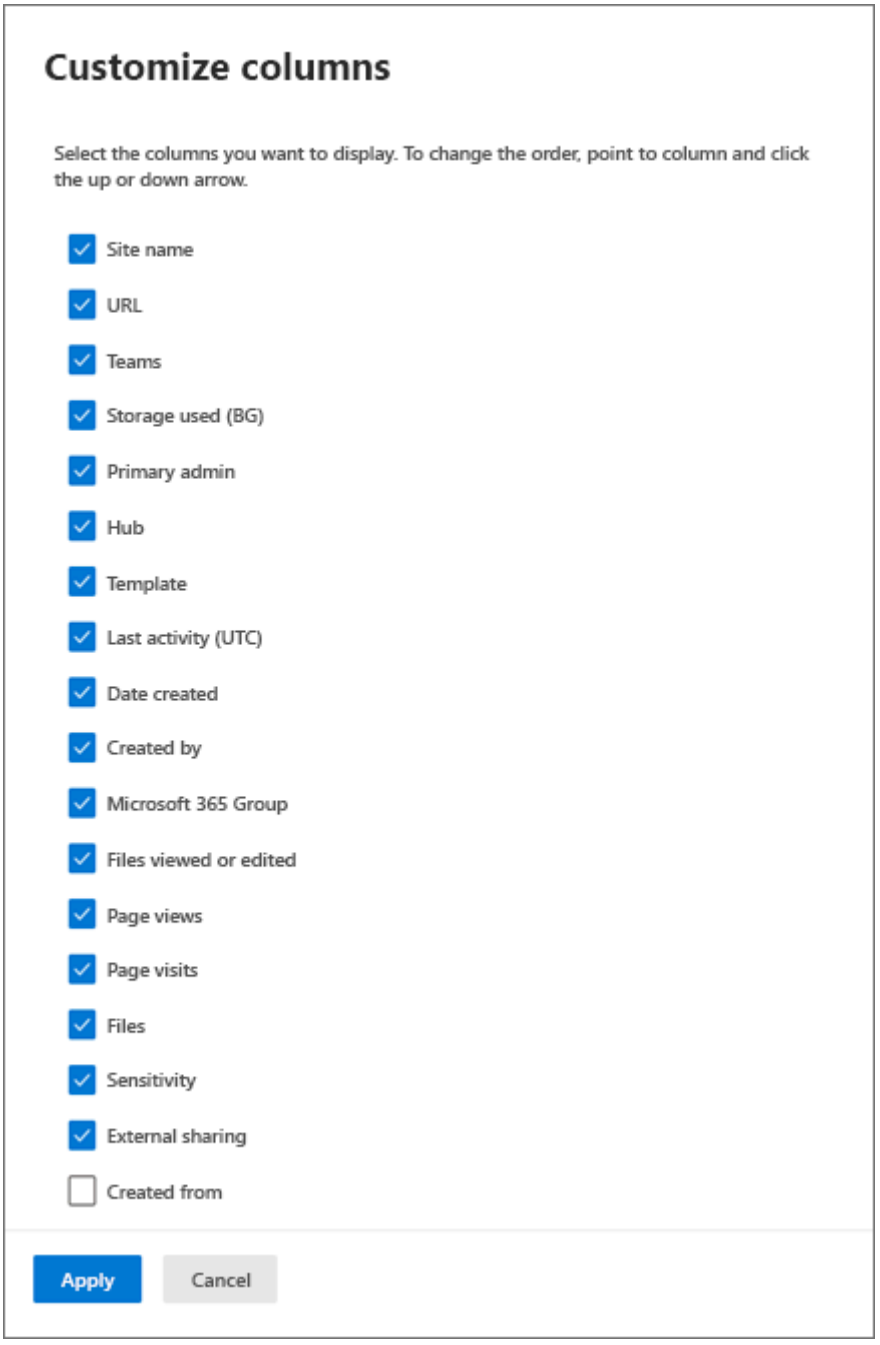
2. Select how you want to arrange the items. The options vary depending on the column. For example, you might have options to sort alphabetically, in numeric order, or chronologically.

   If the column allows filtering, a "Filter by" option appears. Select the value or values that you want to show. Your selections appear with a check mark beside them. To remove a selection, select that value again. To clear all filters on the column, select **Clear filters**.



Customize columns

1. Select the arrow next to any column header, and then select **Customize columns**.
2. To show and hide columns, select and clear check boxes.
3. To rearrange the columns, point to a column, and select the up or down arrow to move the column up or down.



> **Note**
>
> Data in the following columns is not available for US Government GCC High and DoD customers:
>
> - Last activity

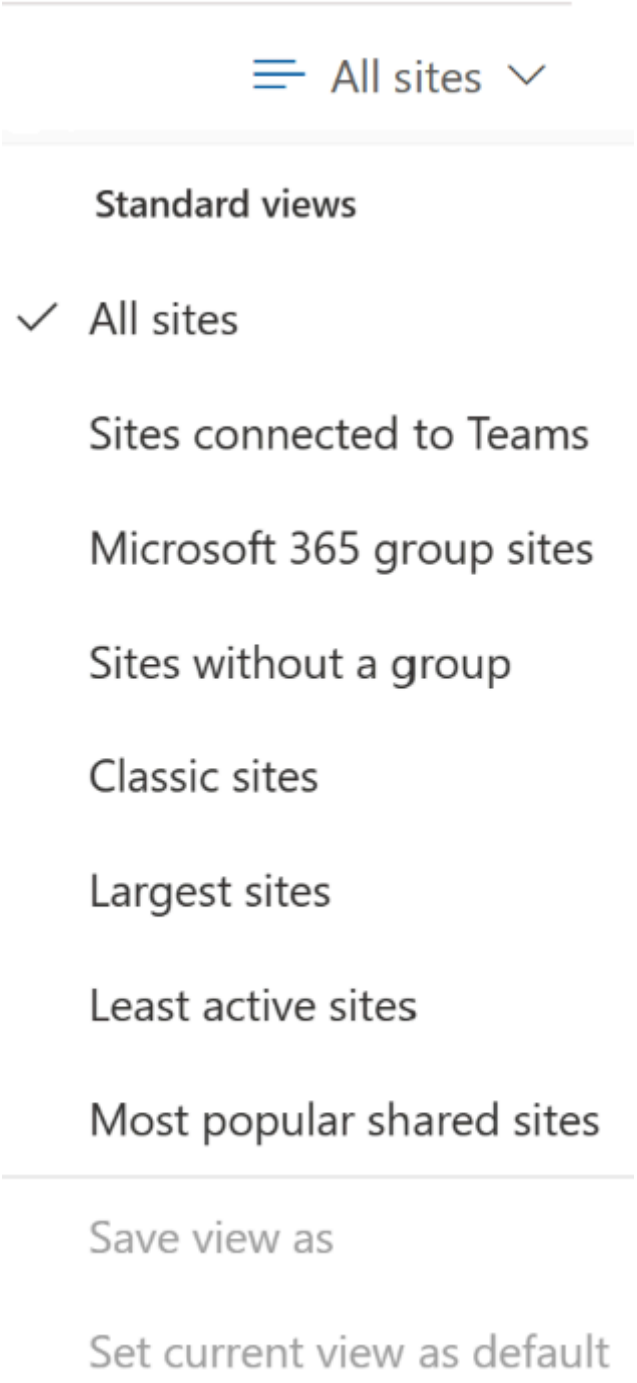
- File views or edited
- Page views
- Page visits
- Files
- Storage used

Switch views and create custom views

The SharePoint admin center comes with a few standard views: **All sites**, **Sites connected to Teams**, **Microsoft 365 Group sites**, **Sites without a group**, **Classic sites**, **Largest sites**, **Least active sites**, and **Most popular shared sites**.

To select a different view:

- On the far right of the command bar, select the **Change view** arrow next to the name of your current view, and then select a different view.



To create and save a custom view:

1. Customize columns, sort, and filter your view the way you want. (Views that are filtered through search can't be saved.)
2. On the far right of the command bar, select the **Change view** arrow next to the name of your current view.
3. Select **Save view as**.
4. In the **Save as** dialog box, enter a name for the view.

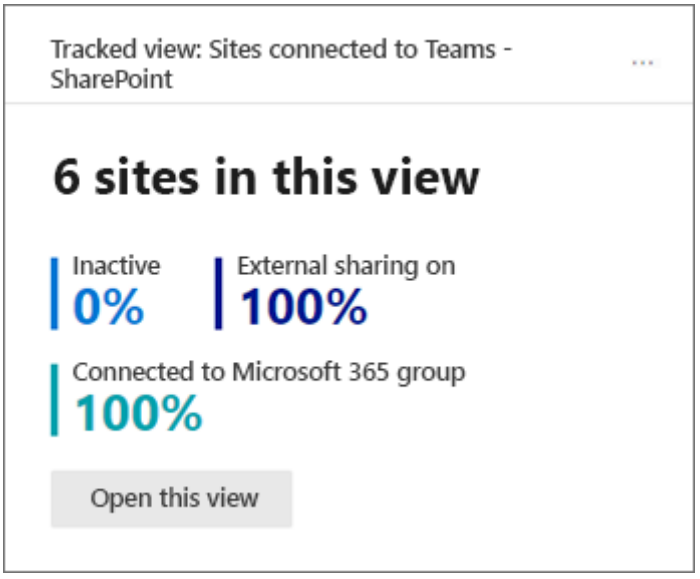
> **Note**

To set the view as default, in the list of views, select **Set current view as default**.

Track a view

When you select a built-in or custom view, you can add a card to your home page that shows the number of sites in the view and summarizes info about the set of sites.

1. Select the **Change view** arrow, and then select the view you want to track.
2. Select **Track view** on the command bar.
3. Select **Add card**.
4. Go to your home page to see the card for the tracked view.



> ⓘ **Note**
>
> If you remove a tracked view card from your home page, you can't add it back from the Add cards panel. You need to open the view on the Active sites page and select **Track view**.

Search for a site

You can search for a site by name, URL, primary admin, or template. To do this, enter keywords in the Search box, and press Enter.

> ⓘ **Note**

Search doesn't look in hub site display names for the keywords you enter.
All characters you enter are treated as part of the query. Search doesn't recognize operators or wildcards (*).

Export to CSV

To export the site list you're viewing as a .csv file that you can work with in Excel, go to **Active sites** page and select **Export** on the command bar.

> **Note**
>
> The .csv file lists the hub as a GUID and the template as an ID (for example, STS#0).

Feedback

Was this page helpful? Yes No

Provide product feedback

Guidance for retiring Delve in your organization

Article • 05/02/2025

In December 2024, Delve was retired. This change was first announced in an MC Post available in the Microsoft 365 Message Center. There's also an article you can refer to, Alternatives to Delve in Microsoft 365, that focuses on helping end users find alternatives for their tasks within Microsoft 365. The purpose of this article is to assist administrators with the Delve offboarding process.

What was retired?

Delve offers many features that are built on top of multiple Microsoft 365 services. When we say we're retiring Delve, it's important to note that we're not changing or retiring anything on the services side. Both documents and people data that are surfaced in Delve continue to be stored and managed as today.

There are a couple of exceptions regarding data storage. Delve stores a limited set of Delve-specific data, such as list of users recently viewed in Delve, Delve favorite documents, Delve favorite tags, and some Delve-specific settings. These are retired together with Delve. You can export this data before December 16, 2024, in Delve by going to **Select settings** > **Feature settings** > **Export data**.

Where can users view user properties currently surfaced in Delve?

Starting December 2024, properties currently surfaced in Delve, including custom user profile properties, are added to the profile cards available in search experiences on Microsoft365.com, Office.com, and in SharePoint. Eventually, these changes are enabled everywhere the profile card is available. However, for technical reasons, this change takes time. For December 2024, we recommend directing users to Microsoft365.com, Office.com, or SharePoint, which also offer a people search similar to what's offered in the Delve search.

Direct links to profile cards

The modern search experiences on Microsoft365.com, Office.com, and in SharePoint include profile pages built on the same data as profile cards. They have a unique link and can be used in documentation, email signatures, and other related resources. Starting December 16, we'll handle redirects from Delve profiles to these profile pages on Microsoft365.com. Although

there are three URLs that offer the same experience and continue to work for some time, we suggest you start using the new domain, m365.cloud.microsoft.

Example links

For m365.cloud.microsoft: `https://m365.cloud.microsoft/search/overview?pp=<User.aadObjectId@TenantId>|UPN`
`https://m365.cloud.microsoft/search/overview?pp=11111111-1111-4a21-acea-db38b244ac46%4022222222-2222-49c2-99e6-c5c0f6f8ead1%7CAdeleV%40M365x14029536.OnMicrosoft.com`

For Microsoft365.com:
`https://www.microsoft365.com/search/overview?pp=<User.aadObjectId@TenantId>|UPN`
`https://www.microsoft365.com/search/overview?pp=11111111-1111-4a21-acea-db38b244ac46%4022222222-2222-49c2-99e6-c5c0f6f8ead1%7CAdeleV%40M365x14029536.OnMicrosoft.com`

For Office.com:
`https://www.office.com/search/overview? pp=<User.aadObjectId@TenantId>|UPN`
`https://www.office.com/search/overview?pp=11111111-1111-4a21-acea-db38b244ac46%4022222222-2222-49c2-99e6-c5c0f6f8ead1%7CAdeleV%40M365x14029536.OnMicrosoft.com`

For SharePoint:
`https://<tenant>.sharepoint.com/_layouts/15/search.aspx/overview? pp=<User.aadObjectId@TenantId>|UPN`
`https://<tenantname>.sharepoint.com/_layouts/15/search.aspx/overview?pp=11111111-1111-4a21-acea-db38b244ac46%4022222222-2222-49c2-99e6-c5c0f6f8ead1%7CAdeleV%40M365x14029536.OnMicrosoft.com`

What happens to existing URLs pointing to Delve or SharePoint profiles?

Both Delve URLs and SharePoint profile URLs are redirected to the modern search profile pages on Microsoft365.com. For tenants not using Delve today, there are no change to URLs and their legacy profile experiences in SharePoint. However, they get the extended profile page in modern search and the extended profile cards across Microsoft 365, which include the properties that are visible in Delve.

Below are all the URLs that redirect to modern search profile pages on Microsoft365.com. If you are using a third-party solution with crafted Delve URLs or have internal documentation that for some reason is providing URLs not in this list, these need to be updated. One option is to remove the subdomain and just use the main domain (delve.office.com). Another is to update your solution to support the new profile URLs in modern search. Examples of these URLs can be found at another place on this page.

`https://delve.office.com`

`https://gcc.delve.office.com`

`https://delve-gcc.office.com`

`https://nam.delve.office.com`

`https://eur.delve.office.com`

`https://apc.delve.office.com`

`https://gbr.delve.office.com`

`https://can.delve.office.com`

`https://lam.delve.office.com`

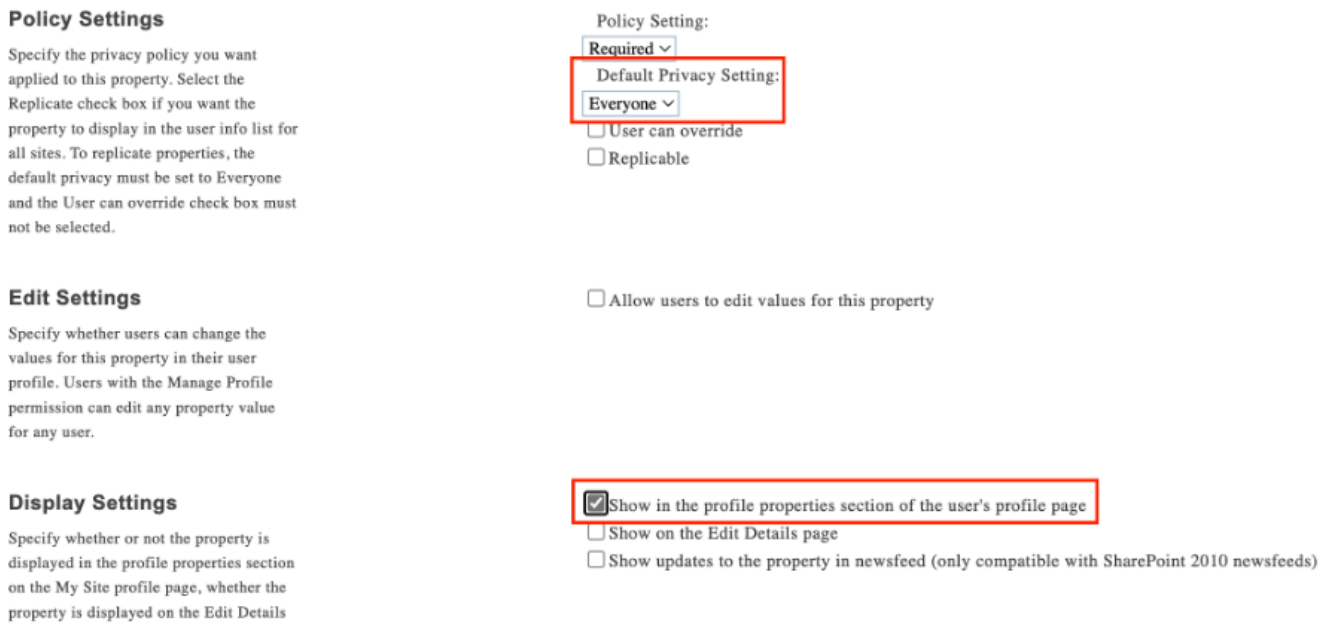
`https://sfeur.delve.office.com`

`https://sfnam.delve.office.com`

How can administrators control which custom user profile properties are visible on profile cards?

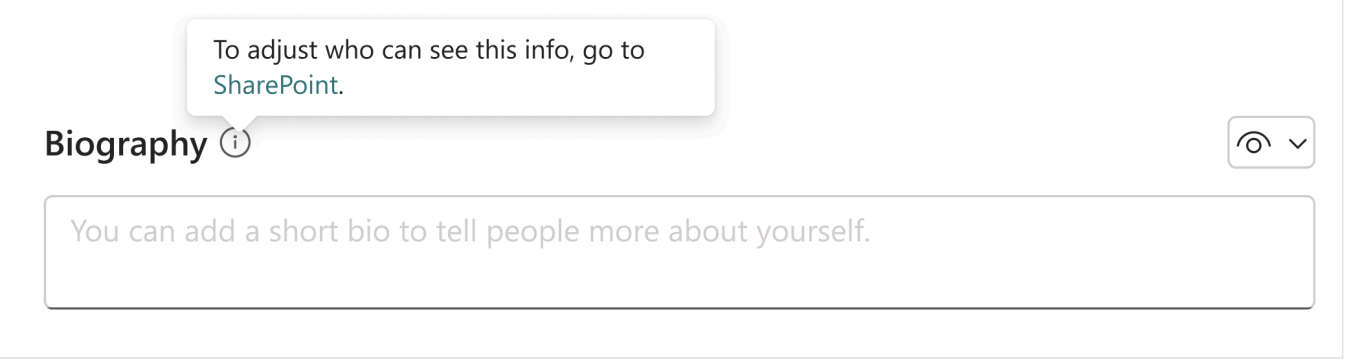
Administrators can control the visibility of custom user profile properties on the profile card by adjusting the Policy Setting and Display Setting for the specific custom user profile property in the SharePoint admin center. To show a property, ensure the Default Privacy Setting under Policy Setting is set to "Everyone" and select "Show in the profile properties section of the user's profile page" under Display Settings. To hide a property, make sure "Show in the profile properties section of the user's profile page" is not selected. For more details, refer to the

article Add and edit user profile properties in SharePoint.

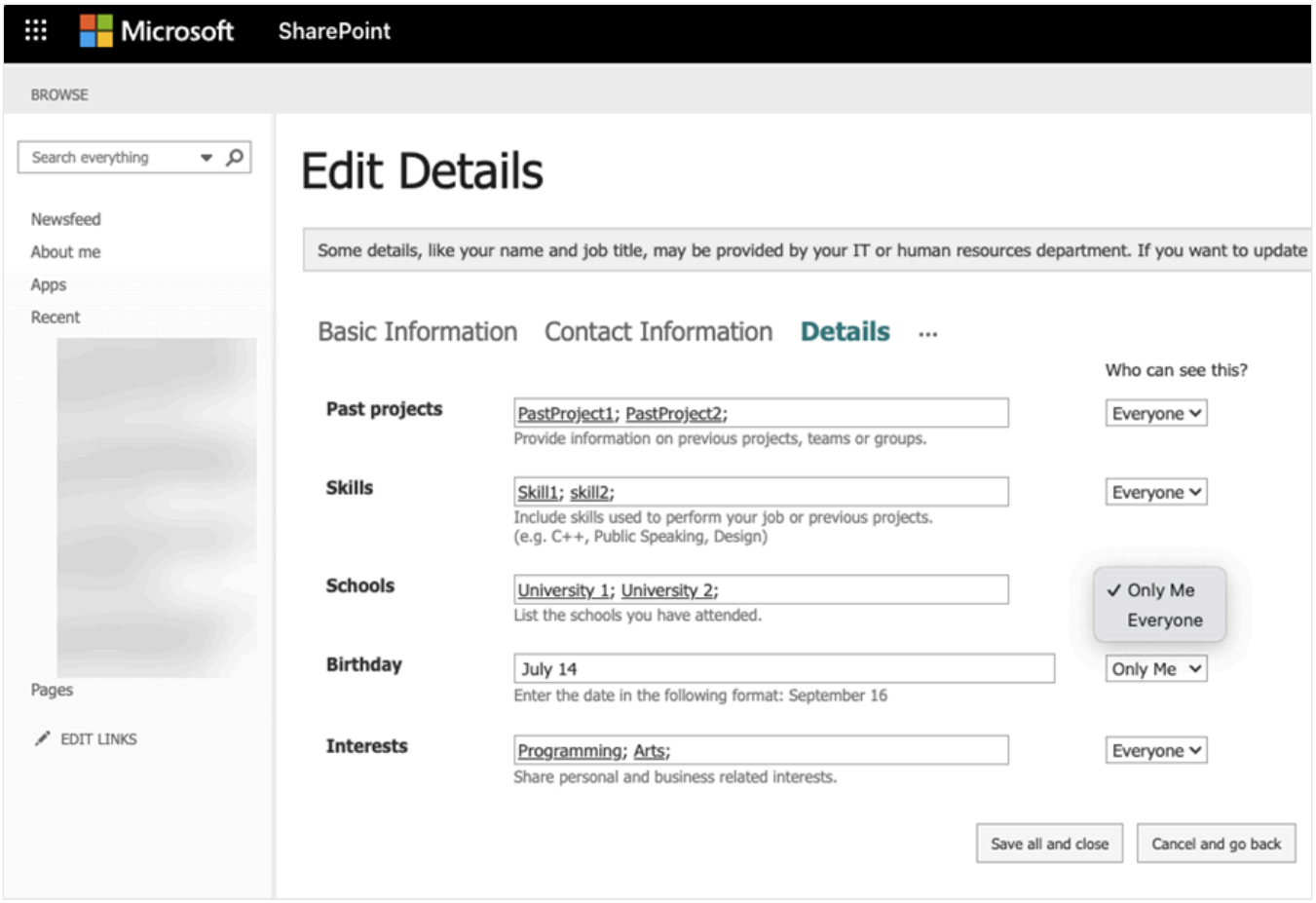


Where can users edit properties they used to edit in Delve?

A new edit profile experience, tightly coupled with the profile card, was released in December 2024. It allows users to easily edit their profiles across Microsoft 365. Only properties that were editable in Delve are editable in the new edit profile experience. For some properties, like custom user profile properties, user have to go to the SharePoint edit profile experience. To make this effortless, a link to the SharePoint edit profile experience is part of the new edit profile experience. For more information on the new edit profile experience, visit Profile editor in Microsoft 365 .



The link to the legacy SharePoint edit profile experience.

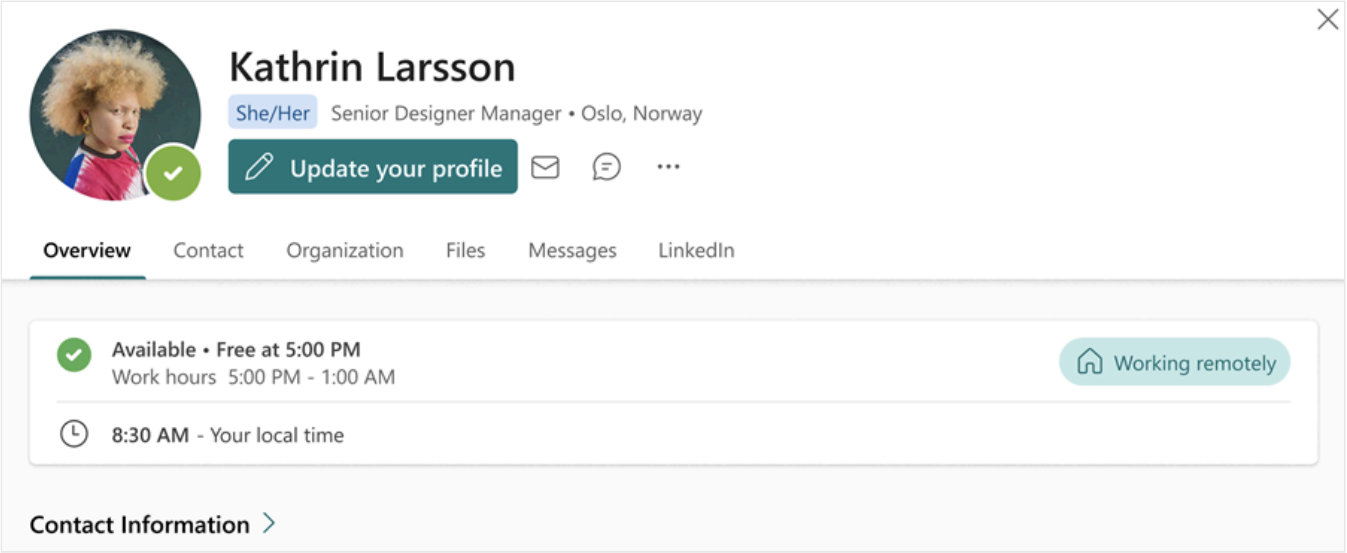


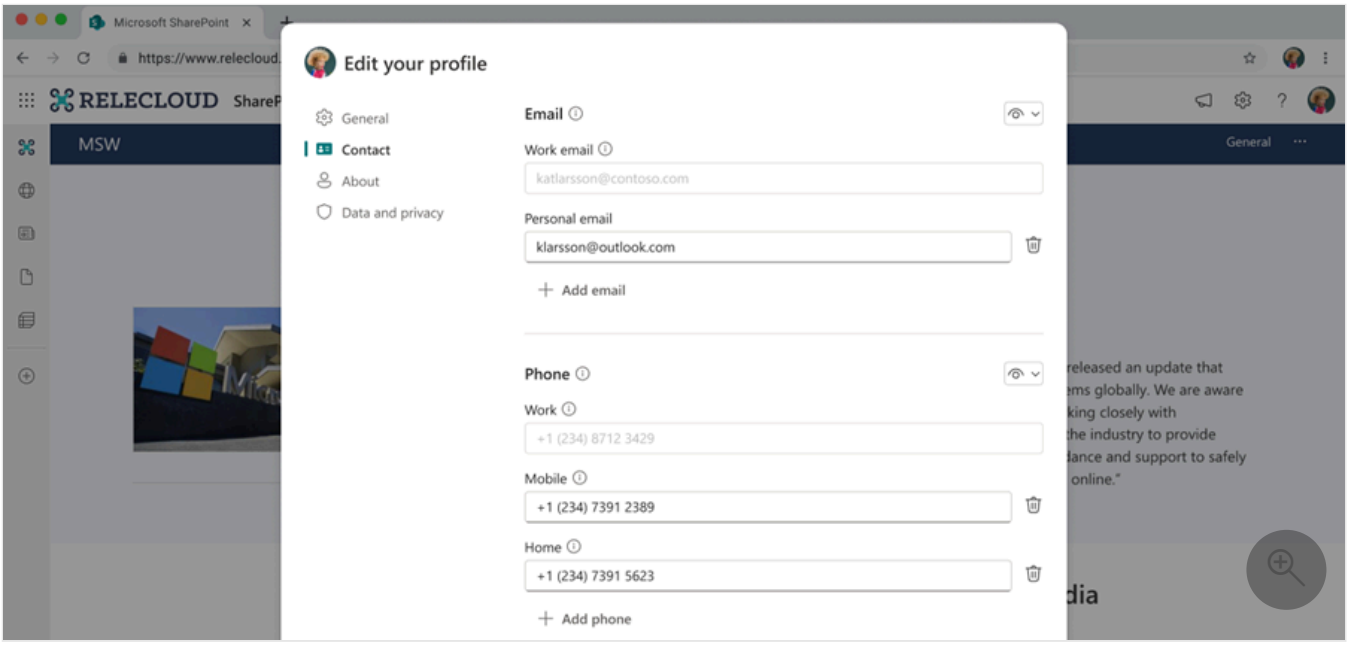
The SharePoint Edit Details dialog box.

What do the new edit experience in profile cards look like?

The new edit profile experience is built on top of Microsoft 365 profile cards, and it is presented in an overlay as profile cards are handled today. A most common user pattern is for the user to open their own profile card and select "edit profile." Instead of being redirected to Delve, the edit experience opens in the profile card. Below is an example of what this process looks like.

Please note that if the new edit profile experience isn't yet enabled in the experience where a user is, selecting "edit profile" redirects the user to the modern search profile page on Microsoft365.com.





Where can users search for people and user profile properties that are currently supported in Delve?

Users can search for people in the modern search experience in Microsoft365.com, Office.com, and SharePoint. Classic search continues to work as before and clicks on people results that today link to Delve redirects to the modern search profile page on Microsoft365.com.

Note that people are presented in multiple ways in modern search. Selecting a people result in the "all" vertical takes the user to the modern search profile experience. Selecting on people results in the people vertical opens the large profile card. Both experiences include properties that today are surfaced in Delve.

Custom people search solutions

If your tenant depends on custom solutions for people search it should continue to work as before. They're built on services powering Delve and not on the Delve experience itself. One common third-party solution in use is the PnP Modern Search app. This particular app allows administrators to create custom search-based experiences based on SharePoint web parts. It's easy to configure people results to support opening profile cards on hover and click. It's also possible to include links to Delve profiles and the legacy SharePoint profile (*person.aspx/personimmersive.aspx*). These links continue to work as users are redirected to the modern search profile page in Microsoft365.com.

Properties not supported by the new edit experience

In general, the new edit experience built on profile cards supports editing properties in the profile card, but there are exceptions. One exception is with properties hosted by Microsoft Entra ID and synced to UPA (SharePoint). By default, these aren't editable in Delve or in the legacy profile edit experience in SharePoint. However, administrators can override the default behavior to make them editable for the user. If administrators make this change, some properties can be edited in Delve, and some can be edited in the legacy edit profile experience in SharePoint.

The new edit profile experience built on profile cards won't support editing these properties. Users can still edit them if administrators have made the setting changes mentioned above, in the legacy edit profile experience, but by default they'll not be visible anywhere and only provide value if you have a custom solution. The following list contains these properties.

Properties synced from Microsoft Entra ID that aren't editable (by default) in Delve

- UserPrincipalName
- DisplayName
- GivenName
- Sn
- telephoneNumber
- proxyAddresses
- PhysicalDeliveryOfficeName
- Title
- Department
- WWWHomePage
- PreferredLanguage
- msExchHideFromAddressList

- Manager

When is Delve no longer be available?

Delve was retired on December 16, 2024. The extended profile card experience, the updated profile pages in modern search, and the new edit profile experience are available before Delve was retired. For a limited period, both Delve and the new experiences are available for users. Delve retires when the redirect of Delve URLs is activated.

What do we recommend administrators do?

- Educate your users about the upcoming changes by updating internal documentation and training material relevant for the Delve retirement.
- Once released, validate that your users can solve their Delve tasks in the new edit profile experience, updated profile pages in modern search, people search in Microsoft365.com, and in the extended profile cards.

More resources

Edit your profile in Microsoft 365

Alternatives to Delve in Microsoft 365

Add and edit user profile properties in SharePoint

Tips and tricks on how to search for organizational content more effectively

Profile cards in Microsoft 365

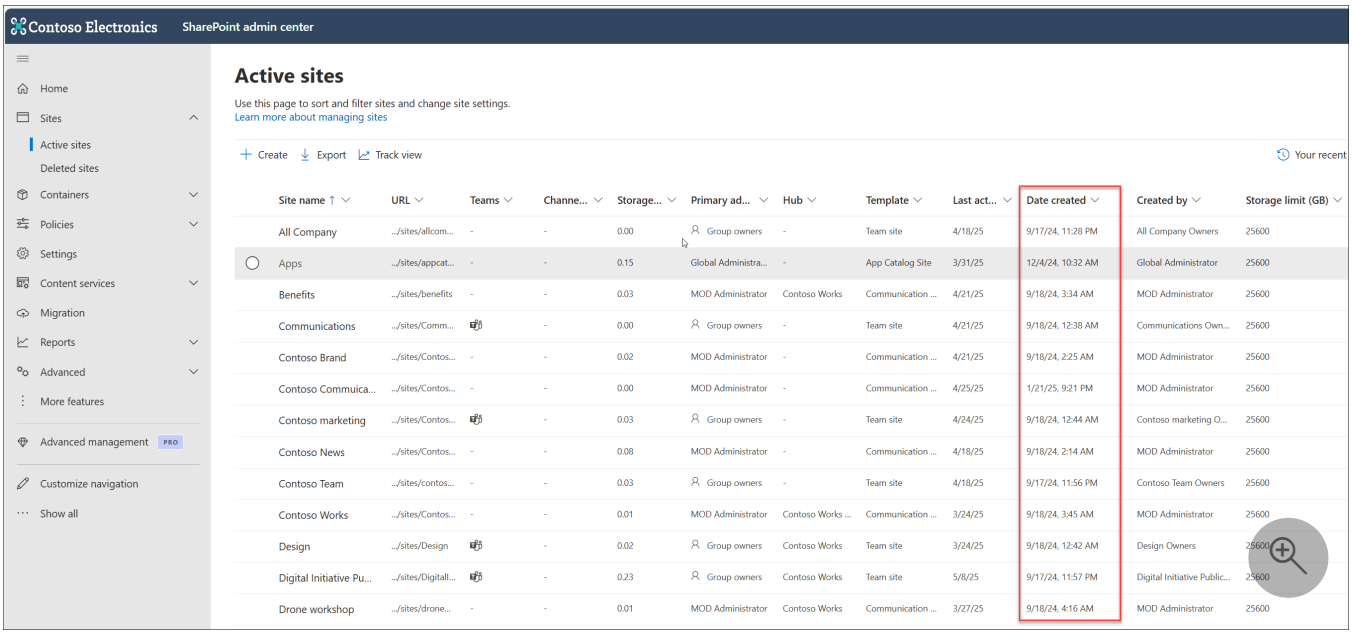
User profile synchronization

Unified cloud.microsoft domain for Microsoft 365 apps

Best practices for changing site creation time zone display in SharePoint admin center

10/23/2025

As a SharePoint admin, sometimes you may have the need to change the displayed creation time zone of the **Active sites** page in the SharePoint admin center. Instead of changing the time zone setting of the SharePoint admin center itself, we recommend using user-level settings for time zone and locale change.



What can happen when you change the time zone in SharePoint admin center

You can change the time zone for the SharePoint admin center by adding `"_layouts/15/regionalsetting.aspx"` to the end of your admin center URL. For example: `https://contoso-admin.sharepoint.com/_layouts/15/regionalsetting.aspx`.

By default, the SharePoint admin center uses Pacific Time (PST). When you create a new SharePoint site, it inherits the current time zone setting from the admin center. If you change the time zone of the SharePoint admin center after sites have already been created, new sites will use the updated time zone, but existing sites will keep their original time zone for creation dates. This can lead to confusion and reporting issues, as older sites may display creation timestamps based on the previous time zone, while newer sites reflect the new setting.

What we recommend: use user-level settings for Time Zone and Locale

To avoid time stamp misalignments on the **Active sites** page in SharePoint admin center, we recommend using user-level settings for time zone and locale instead of directly changing the SharePoint admin center's time zone settings. User-level time zone and locale settings affect how times are displayed in Outlook, SharePoint, and other Microsoft 365 services.

> **Note**
>
> If your organization enforces tenant-level time zone settings, personal changes may be overridden. Changes may take a few minutes to propagate across services.

Related content

- Change your personal language and region settings
- Change regional settings for a SharePoint site

What is SharePoint Advanced Management?

SharePoint Advanced Management (SAM) provides administrative governance controls for SharePoint and OneDrive that help organizations:

- **Manage content sprawl**;
- **Manage the content lifecycle**; and
- **Prevent oversharing**.

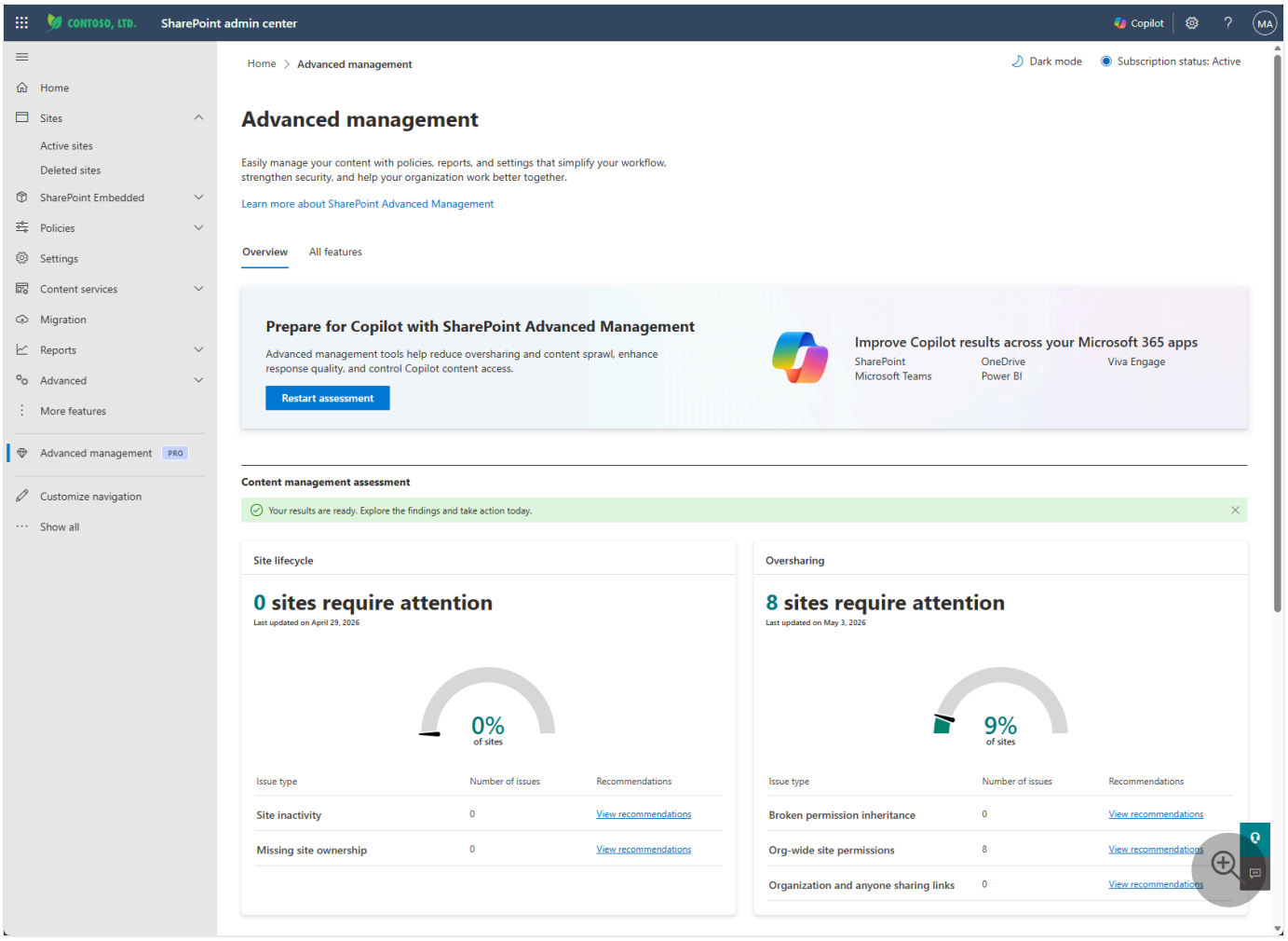
SAM capabilities are helpful as organizations prepare for Microsoft 365 Copilot and agents.

Video: SharePoint Advanced Management overview

Watch the following video to get an overview of SharePoint Advanced Management:

https://learn-video.azurefd.net/vod/player?id=2c7e1ddf-8415-4dff-a844-a8b6dc9d425b&locale=en-us&embedUrl=%2FSharePoint%2Fadvanced-management

Administrators primarily manage SAM through the SharePoint admin center. It's designed for SharePoint and Microsoft 365 administrators who are responsible for governance, risk reduction, and audit readiness. You can also use the SharePoint Admin Agent to make your SharePoint administration more productive and efficient.



Manage content sprawl

SAM helps administrators identify, assess, and reduce unnecessary or unmanaged SharePoint and OneDrive content to help strengthen your governance posture, improve storage utilization, and enhance the relevance of Copilot and Agentic responses.

- Create a site ownership policy: Define who should be responsible for each site, set minimum owner or admin counts, and automate notifications when sites don't meet your criteria.
- Manage inactive SharePoint sites: Detect inactive sites and notify site owners via email.
- Request site attestations: Request regular reviews by site owners or admins to check and confirm the accuracy of site information, including the site's necessity, its owners, members, permissions, and sharing settings.

Manage the content lifecycle

SAM provides administrators with auditability and traceability over SharePoint configuration changes, supporting compliance, operational reviews, and incident investigation.

- **Use catalog management to group SharePoint sites**: Organize and govern SharePoint sites by grouping them into logical categories based on regions, departments, users, information barriers, and custom properties.
- **Create change history reports**: Use history reports to track changes made to individual SharePoint sites or settings over the last 180 days.
- **Review recent changes to SharePoint site properties**: Review and monitor recent changes admins made to a SharePoint site's properties (such as renaming a site, deleting a site, or changing the storage quota) within the last 30 days.
- **Restrict site creation by apps**: Specify the non-Microsoft applications that can create SharePoint sites in your organization.

Prevent oversharing

SAM provides layered controls to manage permissions and access, and enforce least-privilege access across SharePoint and OneDrive. SAM capabilities help prevent oversharing by empowering your administrators with reports, insights, and policies that help protect your organization's sensitive information.

- **Use Conditional Access policies**: Use authentication contexts to connect a Microsoft Entra Conditional Access policy to a SharePoint site.
- **Use restricted access control (RAC)**: Restrict access to SharePoint or OneDrive sites to specific groups.
- **Use the content management assessment**: This hub provides a comprehensive set of tools for assessing and improving your organization's content management practices with actionable insights and recommendations.
- **Set up a "block download" policy**: Create and manage policies to block the ability to move or download files in SharePoint and OneDrive sites, and Teams meeting recordings.
- **Generate app insights**: Gain insights on the various non-Microsoft applications registered to your Microsoft Entra admin center and how they access your SharePoint content.
- **Get AI insights**: Use the **Get AI insights** button next to various reports in the SharePoint admin center. The AI insights feature extracts patterns from the report and offers a list of potential actions.
- **Get insights on agents in SharePoint**: Use this report to identify recently created agents across SharePoint and OneDrive sites, and identify sites with the highest number of agents created.
- **Use restricted content discovery (RCD)**: Prevent high-risk SharePoint sites and files from surfacing in Microsoft 365 Copilot and Agentic experiences.

- **Use data access governance (DAG) reports for SharePoint and OneDrive sites**: Identify sites that might contain overshared or sensitive content. AI insights can be generated from DAG reports to highlight access risk patterns and recommend next steps. You can also initiate site access reviews from a DAG report. DAG reports include:
  - **Permission state reports for sites, OneDrive sites, and files**: Use this report to get a snapshot of your organization's current permission structure across all SharePoint and OneDrive sites, helping you understand how broadly your data is exposed and identify potential oversharing risks.
  - **Site permissions for a given user report**: Use this report to get a list of all the sites a user can access and how access is granted.
  - **Sensitivity label snapshot report**: Use this report to get a snapshot of sensitivity label distribution across all SharePoint and OneDrive sites.
  - **Sharing links activity reports**: Use these reports to identify sites where users have created the most new sharing links within the last 28 days.
  - **Everyone except external users (EEEU) insights**: Identify the top items or groups shared with EEEU in the last 28 days and policies applied to those sites.
  - **DAG reports and PowerShell**: You can use the SharePoint Online PowerShell module to generate DAG reports.
- **Initiate site access reviews**: Initiate site access reviews to delegate the process of reviewing DAG reports to site owners of overshared sites.
- **Use site policy comparison reports**: Select one or more sites as your baseline, and then compare them to up to 10,000 target sites using AI.
- **Monitor agent access to SharePoint and OneDrive sites**: Use the agent access insights report to see how agents interact with SharePoint and OneDrive content.
- **Restrict access to OneDrive sites with security groups**: If necessary, you can restrict certain users from accessing or sharing OneDrive content by using security groups in Microsoft Entra ID.
- **Restrict access to a specific user's OneDrive site**: If necessary, you can restrict access to an individual's OneDrive site by using a security group in Microsoft Entra ID.
- **Restrict OneDrive and SharePoint site creation**: Using PowerShell, you can designate who can create OneDrive or SharePoint sites by using security groups in Microsoft Entra ID.

SAM prerequisites

To see the prerequisites for SAM, including the required licenses, roles, and PowerShell module, see SharePoint Advanced Management prerequisites.

Related articles

- SharePoint Admin Agent
- Get ready for Microsoft 365 Copilot and Agents with SharePoint Advanced Management
- Configure a secure and governed foundation for Microsoft 365 Copilot
- SharePoint Advanced Management features in Microsoft 365 Copilot licenses

ⓘ**Note:** The author created this article with assistance from AI. Learn more

---

Last updated on 06/29/2026

Prerequisites for SharePoint Advanced Management

To use SharePoint Advanced Management capabilities, make sure your organization meets specific licensing, role, and setup requirements. SharePoint Advanced Management helps your organization strengthen how you observe content and permissions, govern access and lifecycle policies, and secure your environment against risks like oversharing, especially in environments using Microsoft Copilot.

For a full list of features, see SharePoint Advanced Management service description.

This article outlines the foundational requirements, including supported base subscriptions, add-on licensing, required administrative roles, and PowerShell setup. These prerequisites ensure that your team has the appropriate access, tools, and permissions needed to manage governance features effectively and support these scenarios.

Microsoft 365 base subscription

Your organization must have one of the following base licenses:

- Office 365 E3, E5, or A5
- Microsoft 365 E1, E3, E5, or A5
- Microsoft 365 GCC, GCC-High, or DoD

Microsoft Copilot or the SharePoint Advanced Management Plan 1 add-on

You get SharePoint Advanced Management capabilities to support your Microsoft Copilot deployment when at least one of the following conditions is met:

- **At least one user in your organization is assigned a Microsoft Copilot license**. (The user doesn't need to be a SharePoint administrator.)

  --- or ---

- **Your subscription includes SharePoint K, P1, or P2, and your organization purchases the *SharePoint Advanced Management Plan 1* add-on**. (This add-on is sometimes referred to as *SharePoint Advanced Management standalone*.)

--- or ---

- **Your organization has Microsoft 365 E7**, also known as The Frontier Suite. It includes:
  - Microsoft 365 E5
  - Microsoft Copilot
  - Microsoft Entra Suite
  - Microsoft Agent 365

If your organization has at least one Microsoft Copilot license assigned to a user, your SharePoint administrators automatically receive access to SharePoint Advanced Management capabilities to support your Copilot deployment.

Some features, such as restricted site creation, require the SharePoint Advanced Management Plan 1 add-on. You can purchase this add-on through:

- The Microsoft 365 admin center
- A Cloud Solution Provider (CSP)
- Volume licensing enrollment

External users don't require a license.

For more information about Microsoft licensing, see Understand, choose, and manage your Microsoft licenses.

Role-based access control (RBAC) role assignments

To access the SharePoint admin center and use SharePoint Advanced Management capabilities, you must have an appropriate role assigned in Microsoft Entra ID. Assign these roles in either the Microsoft Entra admin center or the Microsoft 365 admin center.

- **SharePoint Administrator**: Provides full administrative control over the SharePoint Online service, including sites, policies, groups, and operational tasks, such as service health and support.

- **SharePoint Advanced Management Administrator**: Includes all SharePoint Administrator capabilities, plus advanced governance capabilities such as:
  - Viewing metadata (names, paths, URLs) across SharePoint content
  - Removing permissions from content at scale
  - Managing SharePoint Advanced Management features

SharePoint Online PowerShell module

The SharePoint Online Management Shell is a Windows PowerShell module that you can use to manage SharePoint settings at the organization and site level. To use SharePoint Online PowerShell commands, you need to install the SharePoint Online Management Shell module and connect it to the SharePoint Online service.

1. Always download the latest SharePoint Online Management Shell before running any of the commands.

2. In your PowerShell console, connect to SharePoint. To learn how, see Getting started with SharePoint Online Management Shell.

> **Note**
>
> If you installed a previous version of the SharePoint Online Management Shell, see SharePoint Online PowerShell command doesn't work correctly for instructions on removing older versions.

Related articles

- SharePoint Advanced Management features in Microsoft Copilot licenses
- What is SharePoint Advanced Management?

Last updated on 08/18/2026

SharePoint Advanced Management features in Microsoft Copilot licenses

If your organization assigns at least one Microsoft Copilot license to a user, SharePoint administrators get access to the SharePoint Advanced Management (SAM) features that support your Copilot deployment. This article summarizes those features and availability across business and government cloud environments.

SAM features in Copilot environments

The following table lists the SharePoint Advanced Management features that are included in Microsoft Copilot licenses for:

- Enterprise and business commercial customers, denoted as *Microsoft Copilot (WW)*
- Government Community Cloud customers, denoted as *Microsoft Copilot (GCC)*
- Government Community Cloud High customers, denoted as *Microsoft Copilot (GCC-H)*
- Department of Defense customers, denoted as *Microsoft Copilot (DoD)*

Expand table

Feature	Microsoft Copilot (WW)	Microsoft Copilot (GCC)	Microsoft Copilot (GCC-H)	Microsoft Copilot (DoD)
Compare SharePoint site policies: Easily identify sites with similar content but different security policies. This feature helps you review and adjust site policies and settings, ensuring consistent security across your organization.	Yes	Yes	Yes	Yes
Sprawl control				
Site ownership policy (simulation mode): Define who should be responsible for each site, set minimum owner or admin counts, and automate notifications when sites don't meet your criteria.	Yes	Yes	Yes	Yes
Site ownership policy (active mode)	Yes	Yes	Yes	Yes
Inactive SharePoint sites policy (simulation mode): Detect inactive sites and notify site	Yes	Yes	Yes	Yes

Feature	Microsoft Copilot (WW)	Microsoft Copilot (GCC)	Microsoft Copilot (GCC-H)	Microsoft Copilot (DoD)
owners via email.				
Inactive SharePoint sites policy (active mode)	Yes	Yes	Yes	Yes
Site attestation policy (simulation mode): Request regular reviews by site owners or admins to check and confirm the accuracy of site information, including the site's necessity, its owners, members, permissions, and sharing settings.	Yes	Yes	Yes	Yes
Site attestation policy (active mode)	Yes	Yes	Yes	Yes
Oversharing control				
Content management assessment: The hub for a comprehensive set of tools for assessing and improving your organization's content management practices with actionable insights and recommendations.	Yes	Yes	Yes	Yes
Block download policy: Create and manage block download policies to block downloads for: - Files in SharePoint and OneDrive sites - Teams meeting recording files specifically	Yes	Yes	Yes	Yes
Enterprise app insights: Gain insights on the various non-Microsoft applications registered to your Microsoft Entra admin center and how they access your SharePoint content.	Yes	Yes	Yes	Yes
SharePoint agent insights: Find the **Get AI insights** button next to various reports in the SharePoint admin center. Once selected, the AI insights feature extracts patterns from the report and offers a list of potential actions.	Yes	Yes	Yes	Yes
Conditional Access policies: Use authentication contexts to connect a Microsoft Entra Conditional Access policy to a SharePoint site.	Yes	Yes	Yes	Yes
Restricted access control (RAC): Restrict access to: - SharePoint sites by security groups - OneDrive sites by security groups - Specific OneDrive sites	Yes	Yes	Yes	Yes

Feature	Microsoft Copilot (WW)	Microsoft Copilot (GCC)	Microsoft Copilot (GCC-H)	Microsoft Copilot (DoD)
Restricted content discovery (RCD): Limit the ability of end users to search for files from specific SharePoint sites and prevent the sites from surfacing in Microsoft Copilot Business Chat, unless a user had a recent interaction.	Yes	Yes	Yes	Yes
Sharing links	Yes	Yes	Yes	Yes
Sensitivity labels (Requires E5 or G5)	Yes	Yes	Yes	Yes
Everyone except external users (EEEU) insights	Yes	Yes	Yes	Yes
Permission state reports for sites, OneDrive sites, and files	Yes	Yes	Yes	Yes
Site access review for all reports: Delegate the process of reviewing data access governance reports to site owners of overshared sites.	Yes	Yes	Yes	Yes
Content lifecycle control				
Catalog management: Organize and govern SharePoint sites by grouping them into logical categories based on regions, departments, users, information barriers, and custom properties.	Yes	Yes	Yes	Yes
Change history - site settings: Create change history reports to track changes made to: - Individual SharePoint sites - Organization settings in the SharePoint admin center	Yes	Yes	Yes	Yes
Recent admin actions: Review and monitor the last 30 changes you made to a SharePoint site's properties (such as renaming a site, deleting a site, changing storage quota) within the last 30 days in the SharePoint admin center.	Yes	Yes	Yes	Yes

> **Note**
>
> Restricted site creation by apps isn't included with your Microsoft Copilot license. This feature requires the SharePoint Advanced Management Plan 1 add-on. Restricted site creation enables you to specify the non-Microsoft applications that can create SharePoint sites in your organization.

Advanced tenant renaming is not available in GCC, GCC-High, or DoD tenants.

Advanced tenant renaming is available in enterprise and business tenants. If there are more than 10,000 sites in these environments, SharePoint Advanced Management is required.

Related articles

- Prerequisites for SharePoint Advanced Management
- What is SharePoint Advanced Management?
- SharePoint Advanced Management service description

Last updated on 08/18/2026

What is the SharePoint Admin Agent?

The SharePoint Admin Agent is an AI-powered governance experience that helps your administrators assess and remediate content-related risks across your SharePoint and OneDrive environments. Instead of running reports manually, use natural language queries to investigate tenant-level conditions and take guided remediation actions.

Video: Overview of the SharePoint Admin Agent

The following video provides an overview of the SharePoint Admin Agent:

https://learn-video.azurefd.net/vod/player?id=061be5d6-b8a6-4100-ac10-e145721653ec&locale=en-us&embedUrl=%2FSharePoint%2Fcontent-governance-agent

Microsoft Copilot (Copilot) and Agents work best when SharePoint and OneDrive content is well-governed, relevant, and securely accessible. The SharePoint Admin Agent helps by enabling your administrators to move quickly from assessment to action using a conversational interface. It analyzes data drawn from SharePoint and SharePoint Advanced Management (SAM) to provide contextual insights aligned to governance priorities, such as:

- Managing content sprawl
- Managing the content lifecycle
- Preventing oversharing in search and AI responses
- Managing permissions and access to content and sites

How the SharePoint Admin Agent helps with content governance

Use the SharePoint Admin Agent to get started with these important content governance tasks:

- **Assess whether your organization is ready for Copilot** with content management assessment capabilities
- **Control your content structure** with catalog management capabilities
- **Manage the content lifecycle** with site lifecycle management policies, such as the site ownership policy, inactive sites policy, and site attestations, and archive stale content using Microsoft 365 Archive
- **Prevent accidental oversharing** with data access governance reports and policies

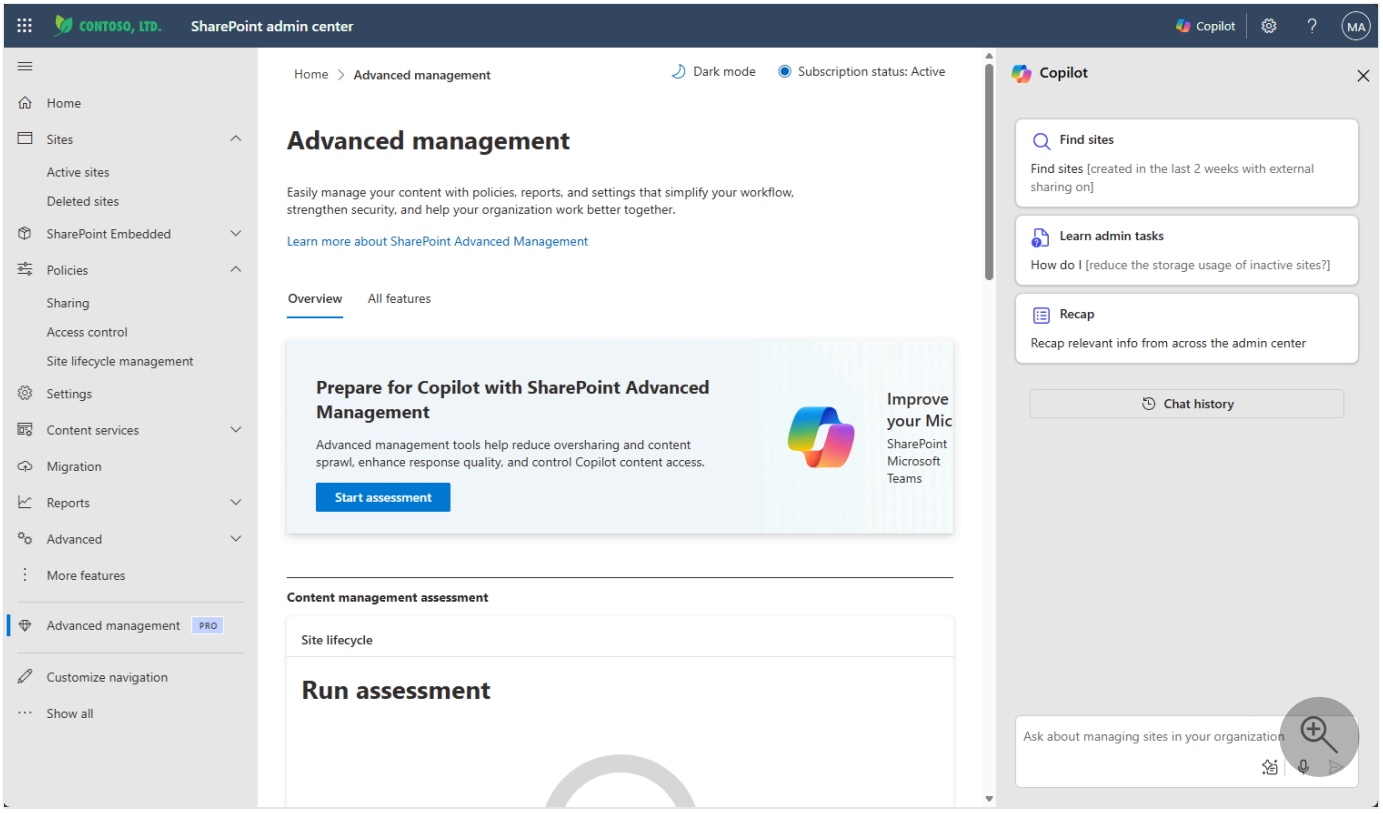
- **Control access to content** with reports, site access reviews, and policies like Conditional Access, restricted access control, and restricted content discovery
- **Implement content resilience** with Baseline Security Mode settings, Microsoft 365 Backup, and version history
- **Manage data residency compliance** with Multi-Geo capabilities, such as cross-geography content move status reports (*Preview*)

SharePoint Admin Agent prerequisites

Your organization must have SharePoint Advanced Management. See SharePoint Advanced Management prerequisites.

To use the SharePoint Admin Agent, you must have the SharePoint Advanced Management Administrator role assigned in Microsoft Entra ID.

Open the SharePoint Admin Agent

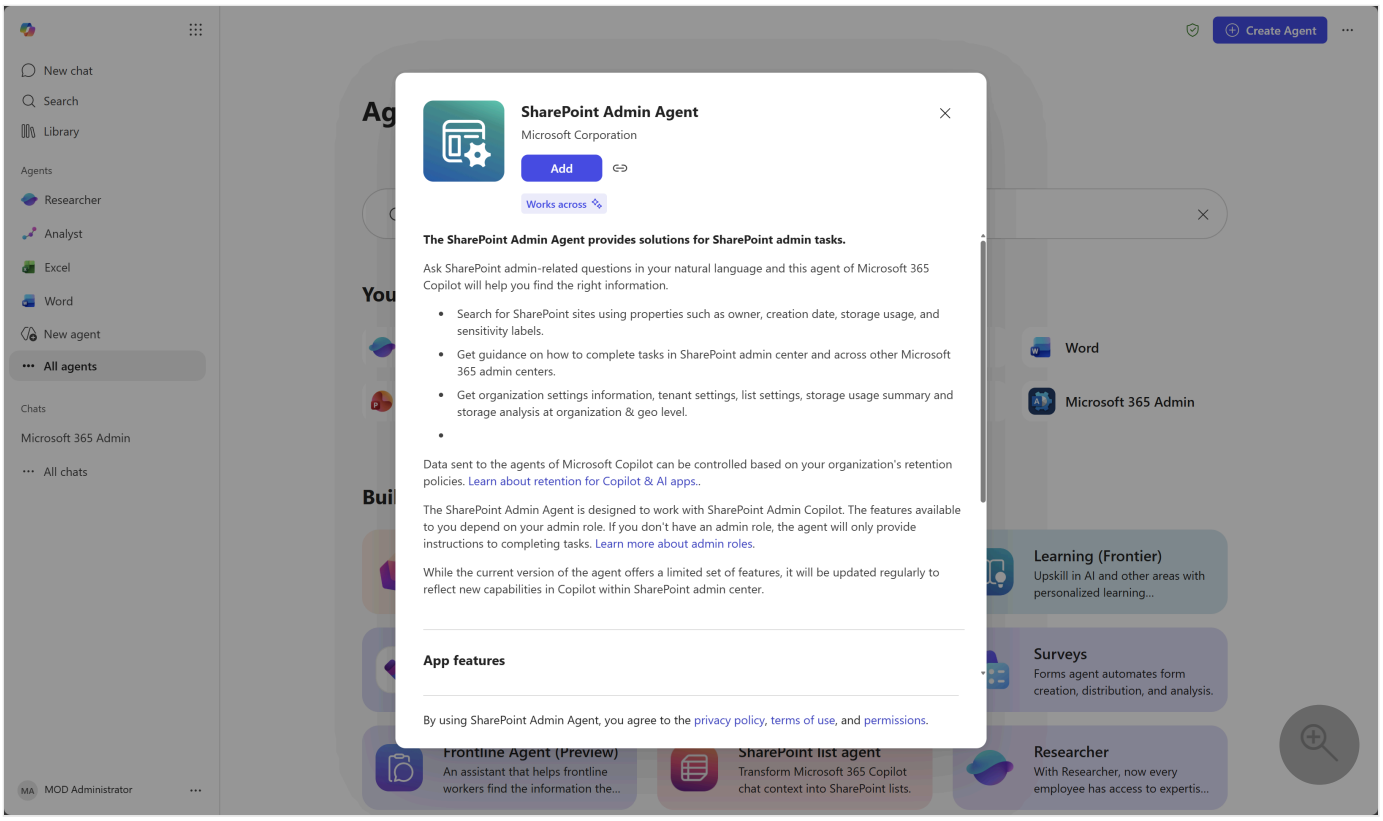


Open the SharePoint Admin Agent by using any of the following methods:

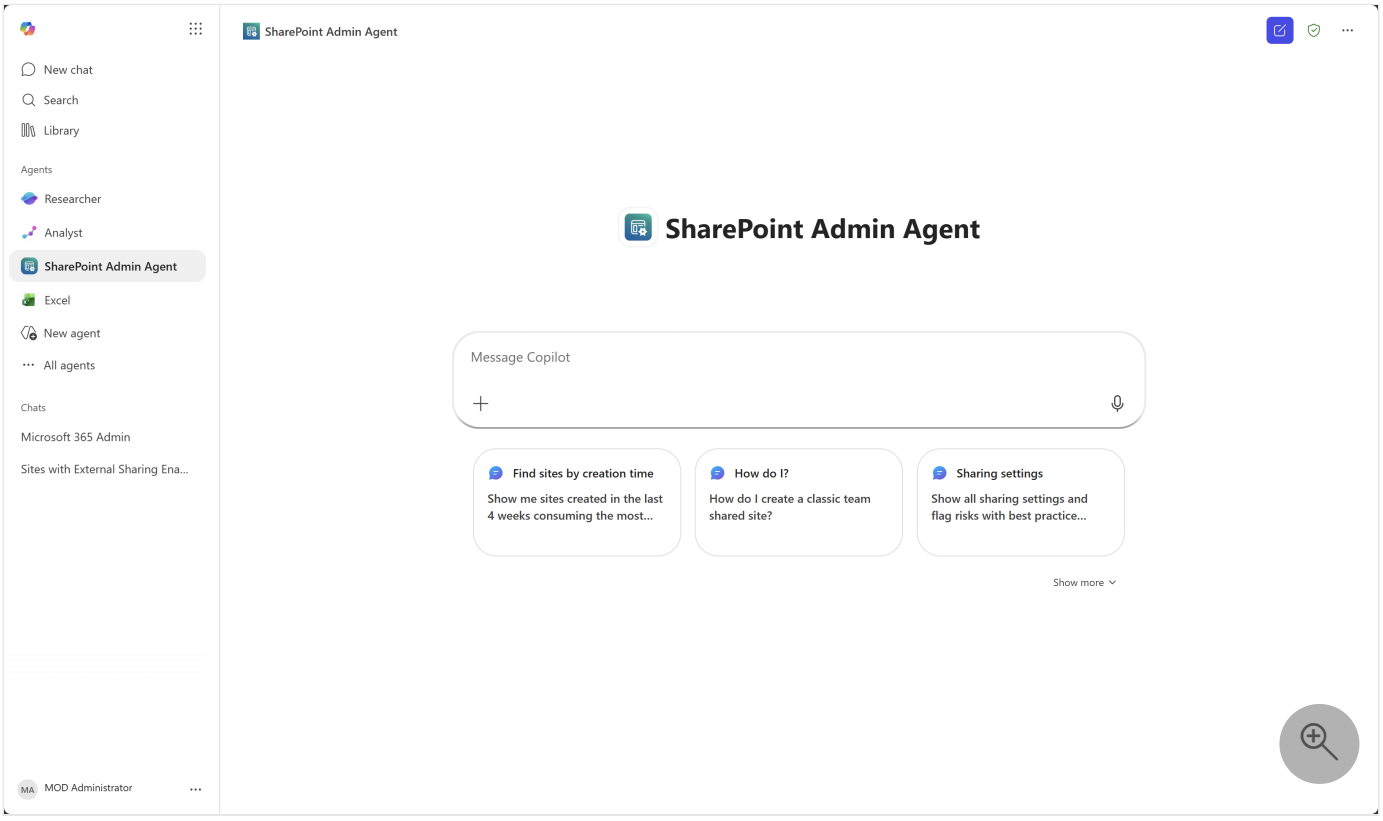
- Open the SharePoint Admin Agent in the Microsoft Copilot app
- Access content governance skills for Copilot in the SharePoint admin center
- Open the SharePoint Admin Agent in Microsoft Teams

Open the SharePoint Admin Agent in Microsoft Copilot

In the Microsoft Copilot app, expand **Agents**, and search for the SharePoint Admin Agent.

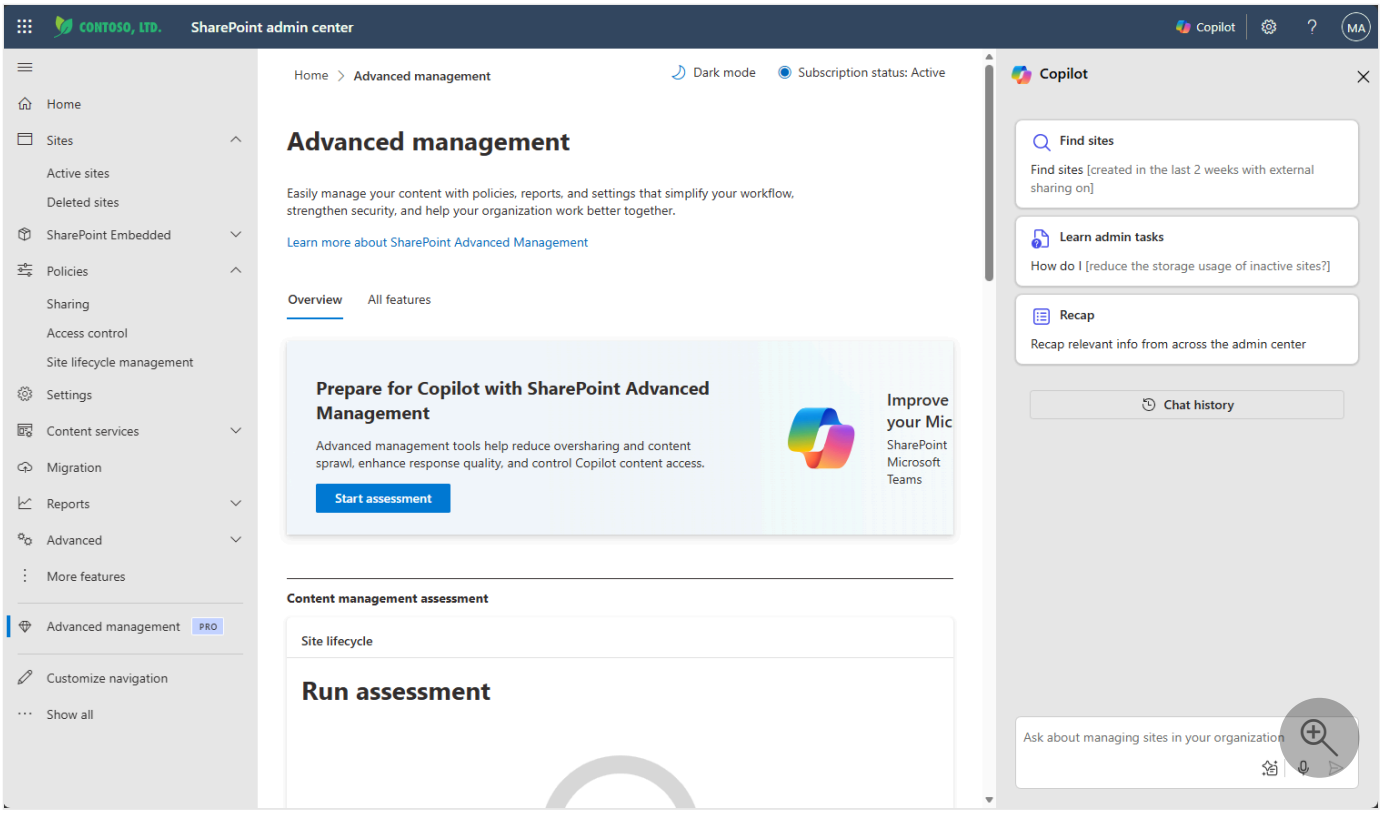


Use the agent in the Copilot app.

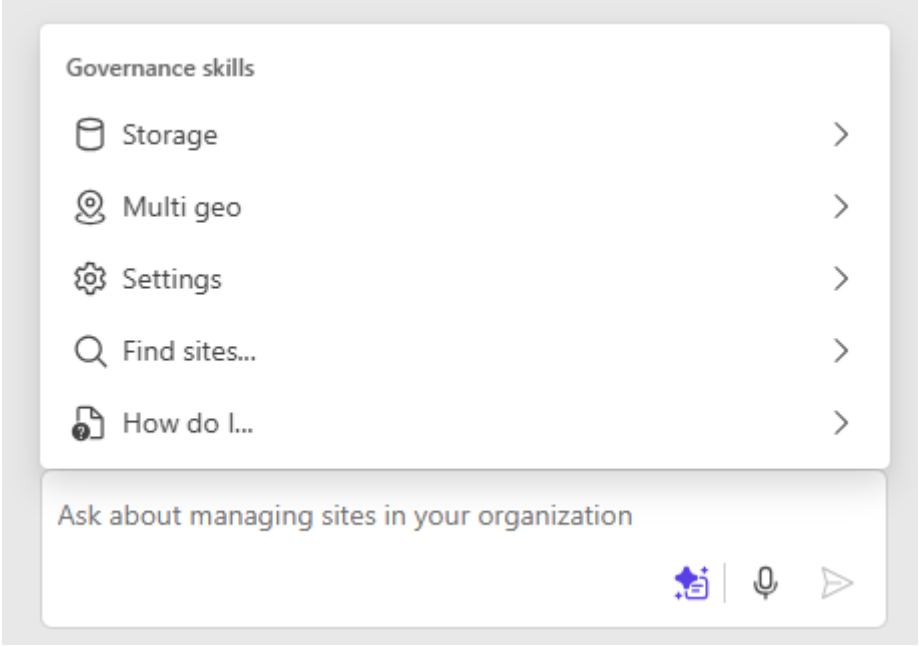


Access content governance skills in Copilot in the SharePoint admin center

Copilot in the SharePoint admin center includes content governance skills.

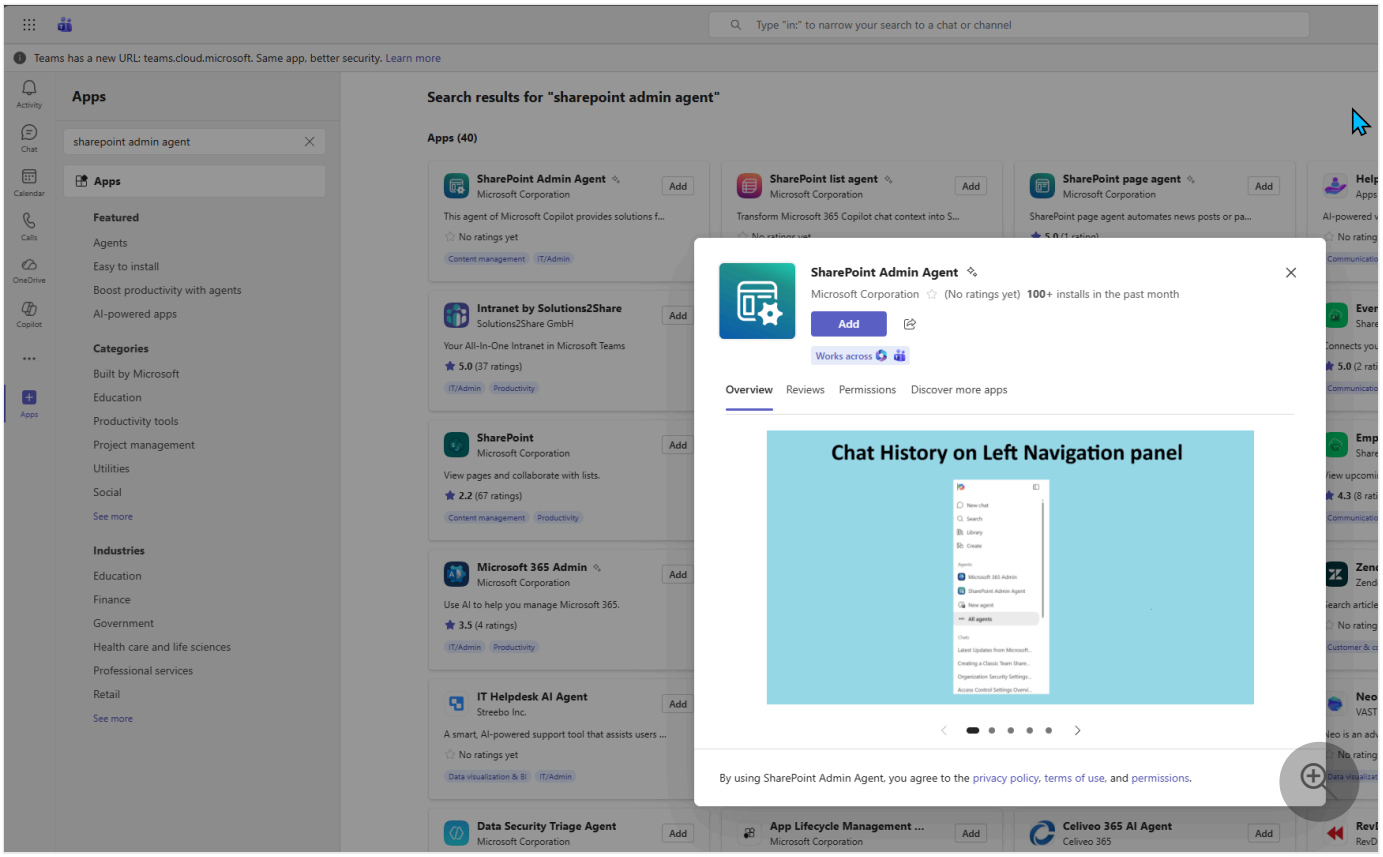


Select the **Copilot** button, and then select the **View prompts** button to view and use governance skills.



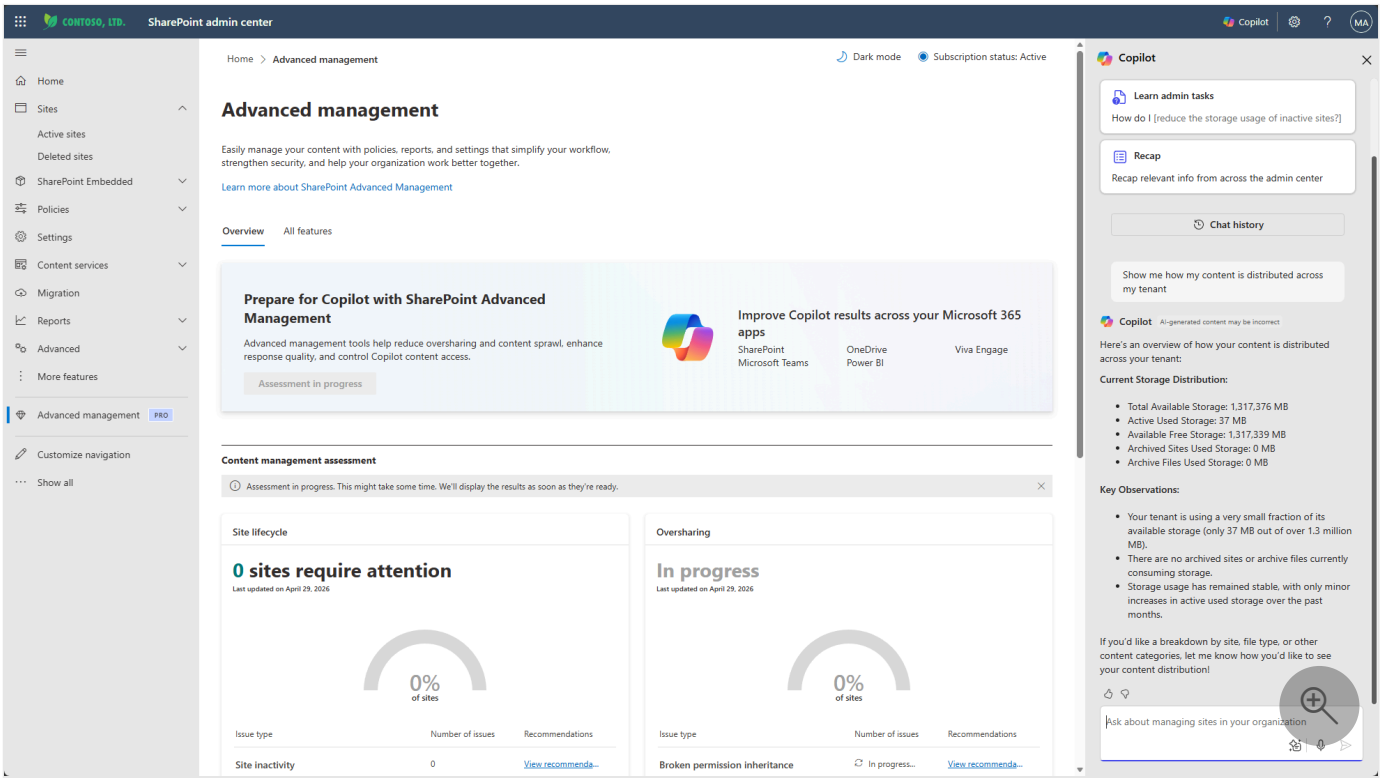
Open the SharePoint Admin Agent in Microsoft Teams

In Microsoft Teams, select **Apps**, and then search for *SharePoint Admin Agent*.



Get started with example prompts

To help you get started, the SharePoint Admin Agent suggests prompts that you can try in your environment.



As you submit a question, the SharePoint Admin Agent responds by gathering the relevant data and reports, offering analysis and recommendations, and suggesting other prompts. You can choose appropriate next steps from there.

The following sections include other example prompts to try.

Content distribution

Console

```
Show me how my content is distributed across my tenant
```

Storage information

Console

```
Show me storage information. Include my storage quota, storage used, and site counts
```

Sites with low activity

Console

```
Identify sites with low activity by department
```

Overshared sites and risk

Console

```
Which sites are overshared and what are the risk levels for these sites?
```

Overshared Teams-connected sites

Console

```
Give me details about Teams-connected sites that are overshared
```

Top 10 agents accessing content

Console

```
Show me a list of the top 10 agents that are accessing my SharePoint and OneDrive
```

```
content
```

Baseline security mode

Console

```
Is Baseline Security Mode enabled in my tenant?
```

Recovery options

Console

```
What recovery options are available for my SharePoint and OneDrive sites?
```

OneDrive libraries to move to another geo

(This feature is available for multi-geo organizations.)

Console

```
Show me users whose OneDrive libraries need to be moved to another location
```

Cross-geo moves that failed

(This feature is available for multi-geo organizations.)

Console

```
Show me cross geo moves that have failed
```

Status of cross-geo moves

(This feature is available for multi-geo organizations.)

Console

```
Show me the status of all cross geo moves initiated in past 7 days
```

Related articles

- What is SharePoint Advanced Management?

- Prerequisites for SharePoint Advanced Management

Last updated on 10/09/2026

SharePoint site lifecycle management

Site lifecycle management policies in Microsoft SharePoint Advanced Management help you maintain site governance at scale. These policies automate common governance tasks, so sites stay active, properly owned, and regularly reviewed throughout their lifecycle.

Video: Overview of SharePoint Advanced Management

The following video provides an overview of SharePoint site lifecycle management:

https://learn-video.azurefd.net/vod/player?id=bb46629d-2a00-4705-896f-a5a1268619e5&locale=en-us&embedUrl=%2FSharePoint%2Fsite-lifecycle-management

Site lifecycle management policies don't delete SharePoint sites directly. Instead, the policies notify site owners and administrators, and take actions based on how you configure the policies.

As your organization creates more SharePoint sites, Microsoft Teams-connected sites, and Microsoft 365 group-connected sites, it becomes increasingly difficult for your administrators to manually identify inactive sites, ownerless sites, or sites that no longer meet business requirements. Site lifecycle management policies help you automate these governance processes by monitoring sites, notifying responsible users, collecting responses, and taking enforcement actions when necessary.

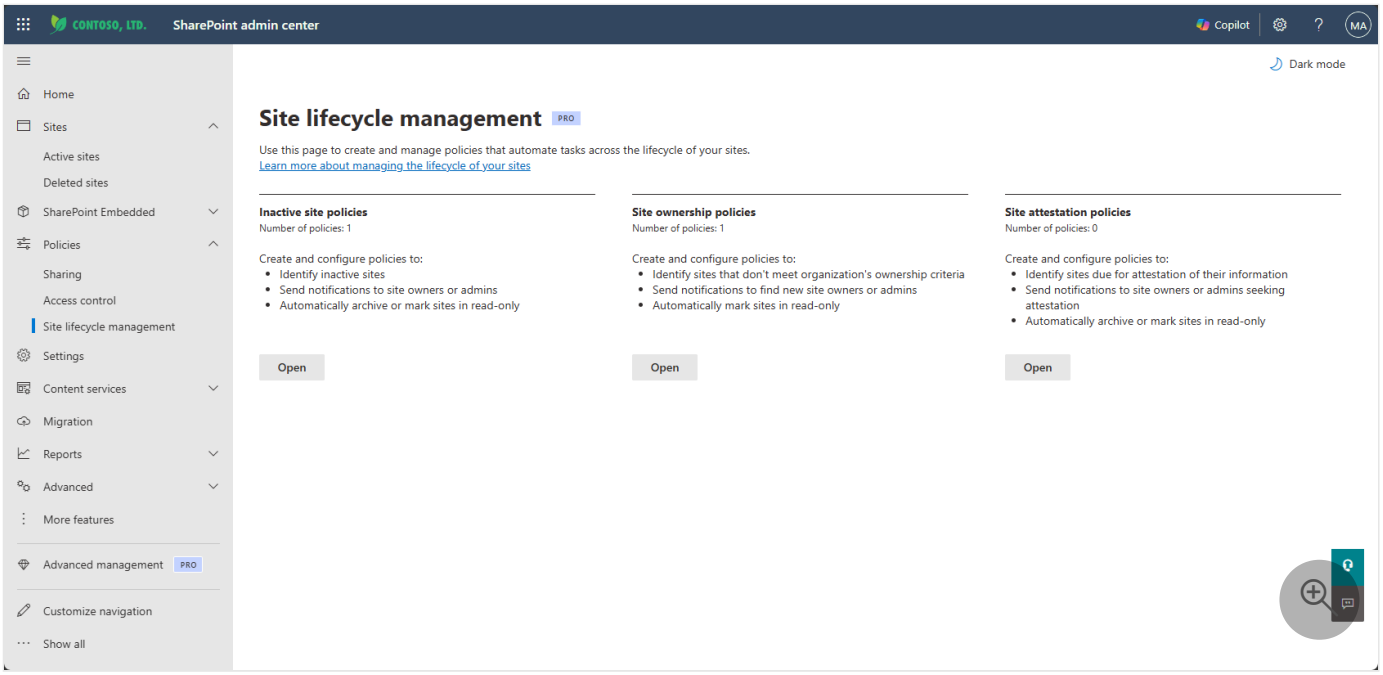
Benefits of site lifecycle management

Site lifecycle management policies help you:

- Reduce the number of inactive or abandoned sites.
- Identify and address sites that have insufficient ownership.
- Verify that sites continue to serve a valid business purpose.
- Improve compliance with organizational governance requirements.
- Automate notifications, reporting, and remediation workflows.
- Maintain a healthier and more manageable SharePoint environment.

Types of site lifecycle management policies

Site lifecycle management includes three policy types that address different governance scenarios.



Expand table

Policy type	Purpose
Site ownership policy	Helps ensure sites have the required number of owners or site administrators.
Inactive site policy	Identifies sites that aren't active for a specified period of time.
Site attestation policy	Requests periodic confirmation that a site is still needed and meets organizational requirements.

Use these policies independently or together to create a comprehensive site governance strategy.

Site ownership policies

Site ownership policies help ensure that every site has accountable individuals responsible for managing it. You can define ownership requirements, including:

- Whether ownership is based on site owners, site administrators, or both.
- The minimum number of owners or administrators required for a site.
- Which users receive notifications when ownership requirements aren't met.

For example, you can require all sites to have at least two site owners. If a site falls below that threshold, the policy can notify designated recipients and prompt corrective action.

Site ownership policies help reduce the risk of ownerless sites and improve administrative continuity when users change roles or leave the organization.

For more information, see Create a SharePoint site ownership policy.

Inactive site policies

Inactive site policies help identify sites that no longer show meaningful business activity. The policy evaluates activity across SharePoint and connected workloads, such as Microsoft Teams, Exchange, and Viva Engage, to determine whether a site remains active.

When a site exceeds the configured inactivity threshold, the policy can notify site owners or site administrators and request confirmation that the site is still in use. Use inactive site policies to:

- Reduce content sprawl.
- Identify abandoned collaboration spaces.
- Improve storage management.
- Support long-term governance objectives.

For more information, see Manage inactive sites using inactive site policies.

Site attestation policies

Site attestation policies help organizations periodically verify that sites remain necessary, business-relevant, and compliant with internal governance requirements. Unlike inactive site policies, which focus on detected activity, site attestation policies request an explicit review from designated site owners or site administrators.

Use attestation policies to:

- Confirm that a site is still required.
- Validate ownership and accountability.
- Review site purpose and business justification.
- Support governance and compliance programs.

For more information, see Request recurring site attestations for SharePoint sites.

Overlapping policies of same policy type

When more than one policy of the same policy type includes the same site, SharePoint helps reduce duplicate notifications by using stored site-level policy history.

If a notification was sent within the last 30 days from any policy of that type, and the site remains uncertified, no further notifications are sent and the policy execution report shows the site's

status as "Notified by another policy."

For example, if a site is covered by two different inactive site policies and receives a notification email from the first policy, the second policy doesn't send additional notifications within the next 30 days if the site remains uncertified.

We recommend that policies of the same type don't have overlapping scopes. If sites fall under multiple policies of the same type, notification schedules and enforcement actions can become difficult to predict.

Overlapping policies of different types

Policies of different types operate independently for notification purposes. Notification history is tracked separately for each policy type.

For example, if a site falls within the scope of both a Site Ownership policy and an Inactive site policy, site owners may receive notifications from both policies when the respective policy conditions are met.

Enforcement actions are evaluated independently by each policy. If a policy applies an enforcement action that changes the site's state, the site may no longer qualify for processing by other policies:

If a policy places the site in a read-only (locked) state, the site is no longer included in the scope of other policies.

If a policy archives the site, the site reaches a terminal state and is no longer considered for enforcement by other policies.

When multiple policy types target the same site, the enforcement action from the policy whose conditions are satisfied first is applied first.

Disabling or deleting a policy

Disabling or deleting a policy stops future activities from that policy, including notifications and enforcement actions. It doesn't automatically reverse previously applied actions.

Notification history is maintained at the site level separately for each policy type. As a result, disabling or deleting one policy doesn't affect notification history associated with other policy types that continue to target the site.

For policies of the same type, stored notification history (including notification count and last notification date) is retained even after a policy is disabled or deleted. This history naturally resets after the site has been absent from the scope of that policy type for 90 days.

If notification history needs to be reset sooner, contact Microsoft Support to determine whether the stored notification state can be cleared.

> **Important**
>
> To ensure predictable behavior, avoid creating overlapping policies of the same type that target the same sites. While SharePoint suppresses duplicate notifications where possible, overlapping policies can make notification timing and enforcement outcomes harder to interpret.

Policy execution and notifications

All site lifecycle management policies support two operating modes:

- **Simulation mode** – Runs the policy once and generates a report without ongoing enforcement.
- **Active mode** – Runs the policy on a recurring schedule, generates reports, and sends notifications to designated recipients.

Policy notifications use Outlook Actionable Messages, so recipients can complete governance actions directly from email. You can also configure messaging, guidance, and support resources.

Enforcement actions

After multiple notification attempts, site lifecycle management policies can take enforcement actions when no response is received. Depending on the policy type, available actions include:

- Take no action and continue reporting.
- Set sites to read-only mode.
- Archive sites after a configurable read-only period by using Microsoft 365 Archive.

These enforcement options help organizations balance user self-service with governance requirements.

Reporting and monitoring

Each policy execution generates reports that help administrators understand policy outcomes and identify sites that require attention. Reports can include information such as:

- Site ownership status.
- Site activity status.
- Notification history.
- Enforcement actions.
- Site metadata and configuration details.

Use these reports to monitor governance trends and prioritize remediation activities.

Recommended governance strategy

Many organizations achieve the best results by combining all three policy types:

- Use site ownership policies to ensure every site has accountable owners.
- Use inactive site policies to identify abandoned or unused sites.
- Use site attestation policies to periodically validate ongoing business need.

Together, these policies help maintain a secure, well-governed, and sustainable SharePoint environment.

Related articles

- Create a SharePoint site ownership policy
- Manage inactive sites using inactive site policies
- Request site attestations
- Overview of SharePoint Advanced Management

ⓘ**Note:** The author created this article with assistance from AI. Learn more

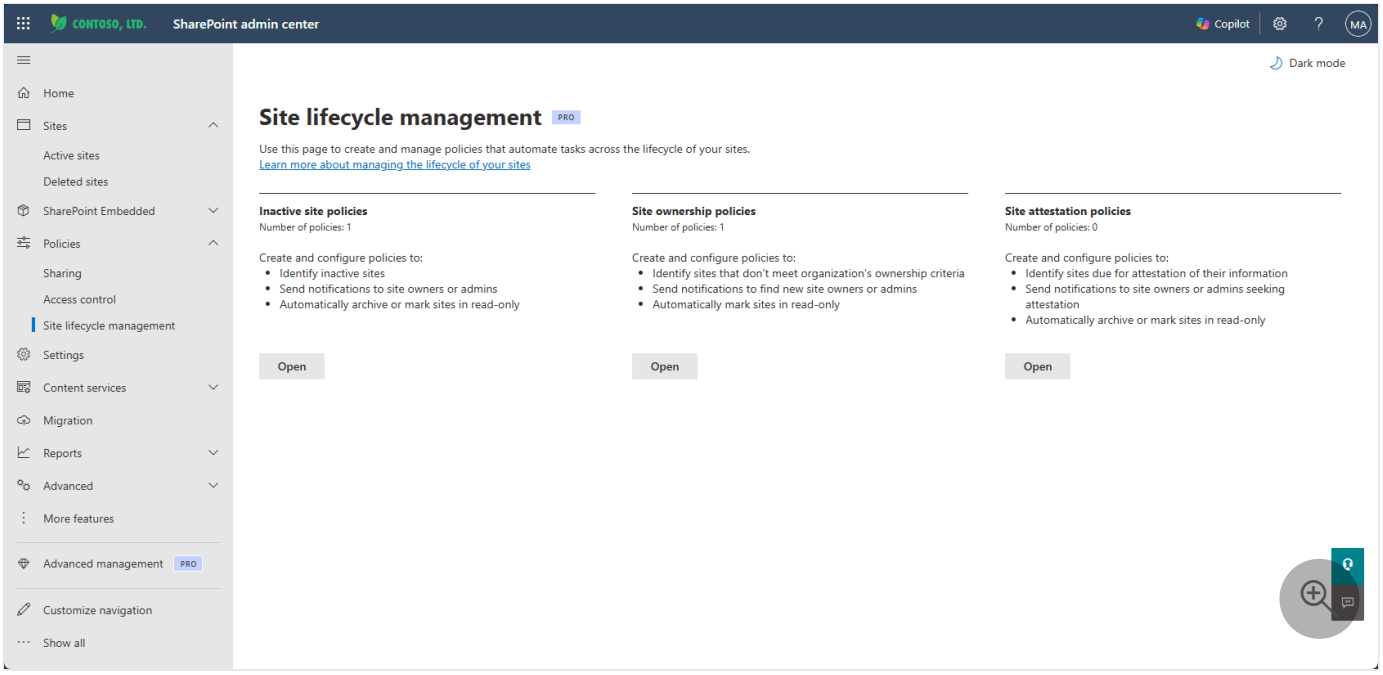
---

Last updated on 08/19/2026

Create a SharePoint site ownership policy

Site ownership policies help you identify sites that don't meet your organization's ownership requirements. Use these policies to define ownership criteria, notify responsible users when sites become noncompliant, and take enforcement actions when ownership issues aren't resolved.

For an overview of SharePoint site lifecycle management policies and how site ownership policies work alongside inactive site and site attestation policies, see Overview of SharePoint site lifecycle management.



This article describes how site ownership policies evaluate ownership requirements, how to create and configure a policy, and how to monitor policy execution.

Prerequisites

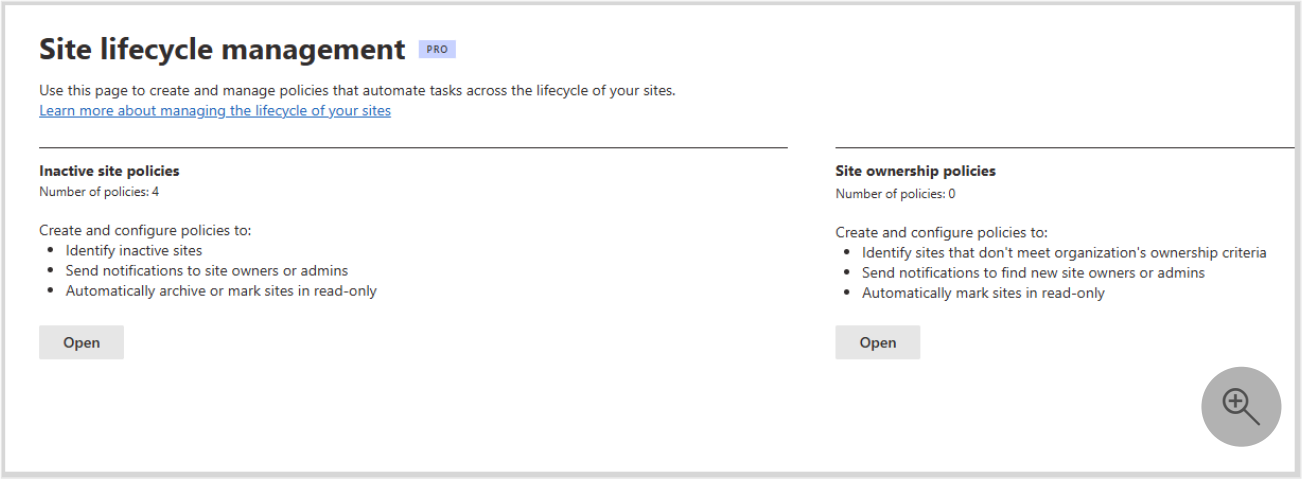
See SharePoint Advanced Management prerequisites.

Create a site ownership policy

To create a site ownership policy, follow these steps:

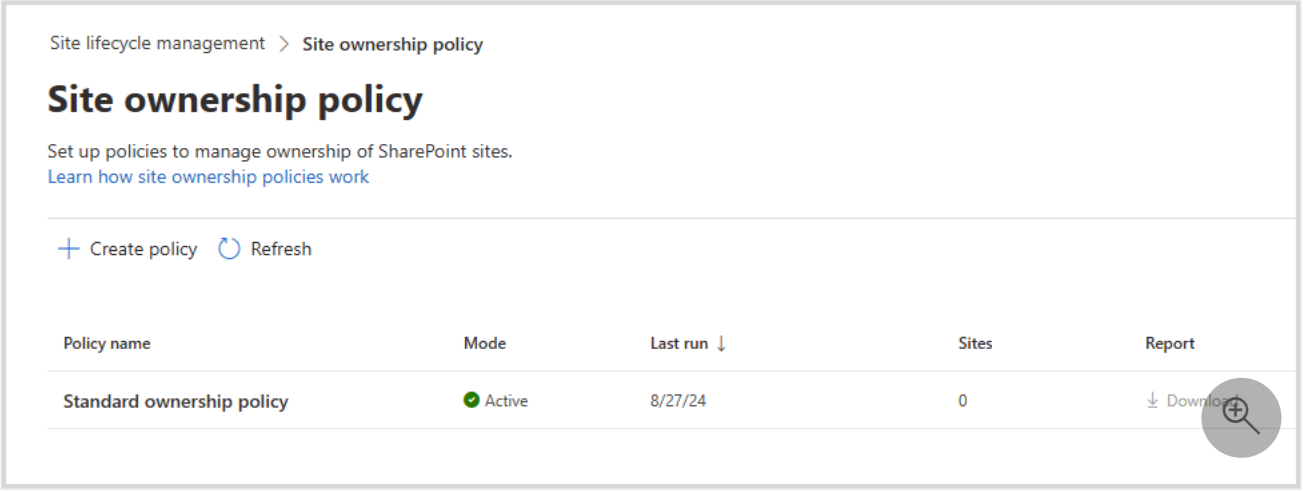
1. As a SharePoint administrator, go to the SharePoint admin center and sign in.

2. In the navigation pane, expand **Policies**, and then select **Site lifecycle management**.

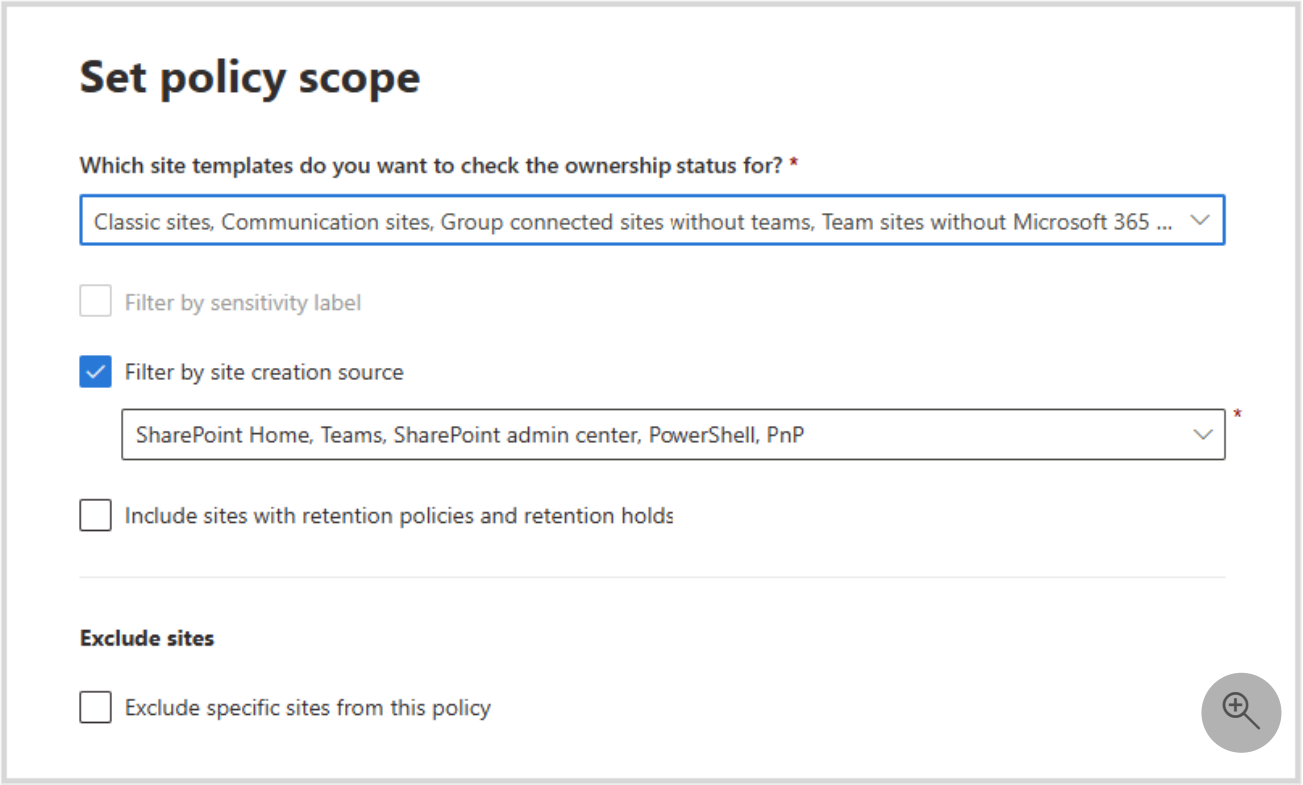


3. Under **Site ownership policies**, select **Open**. Then, select **+ Create policy**.

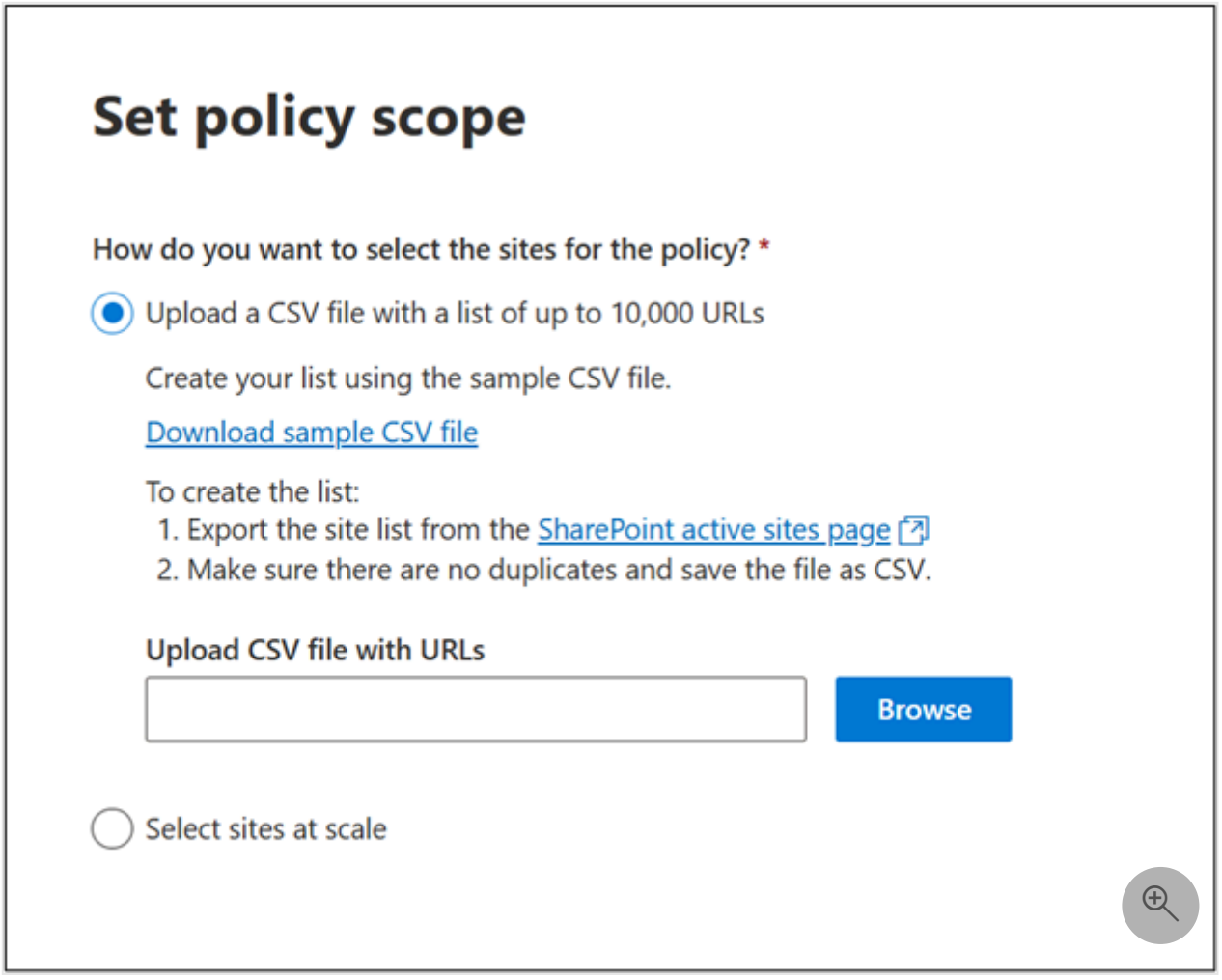
4. On **Manage ownership of sites**, review the information, and then select **Next**.



5. On **Set policy scope**, choose your policy scope parameters, and then select **Next**.

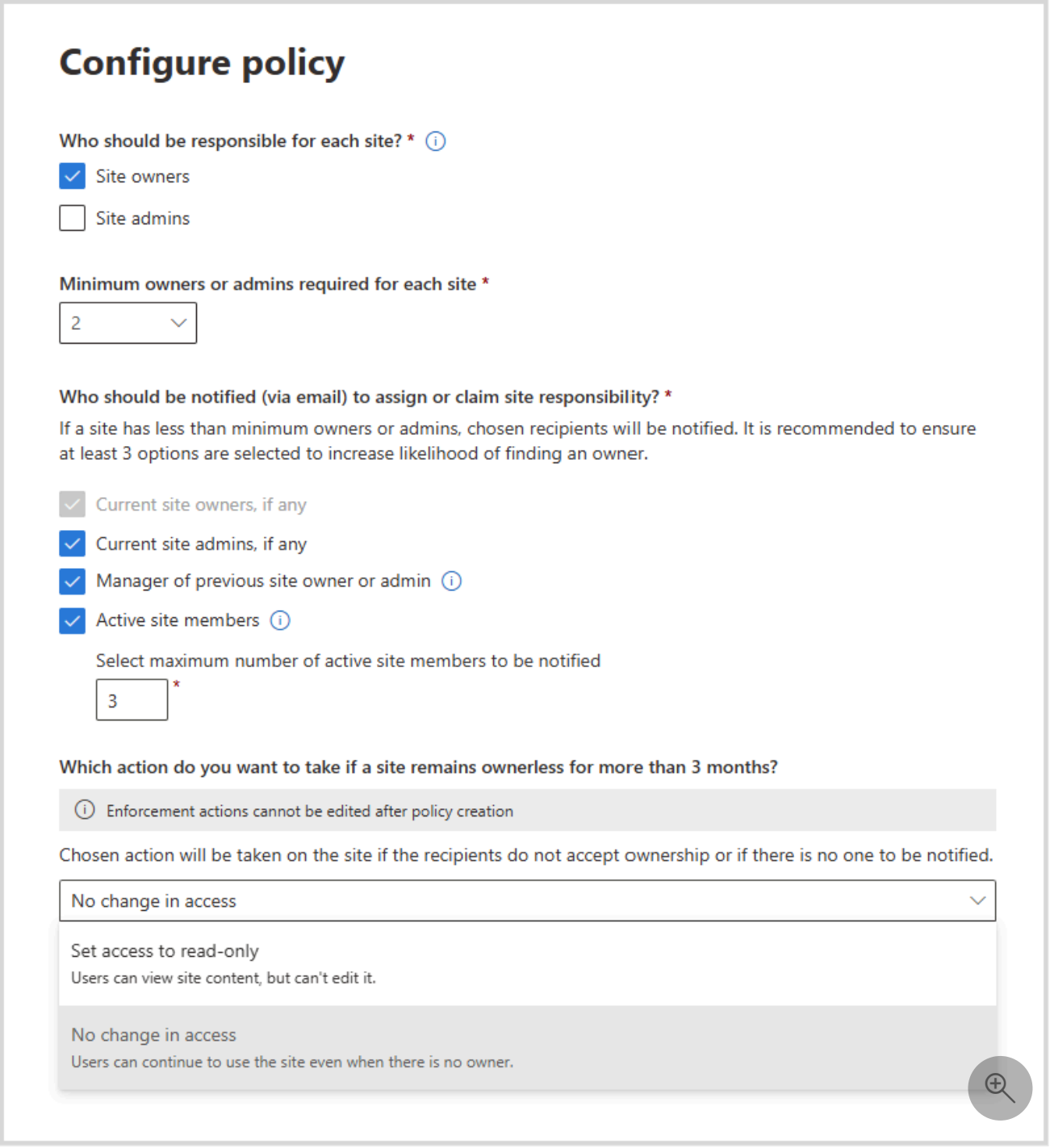


If you select **Upload a CSV file with a list of up to 10,000 URLs**, you can upload a list of site URLs of select sites for the policy.



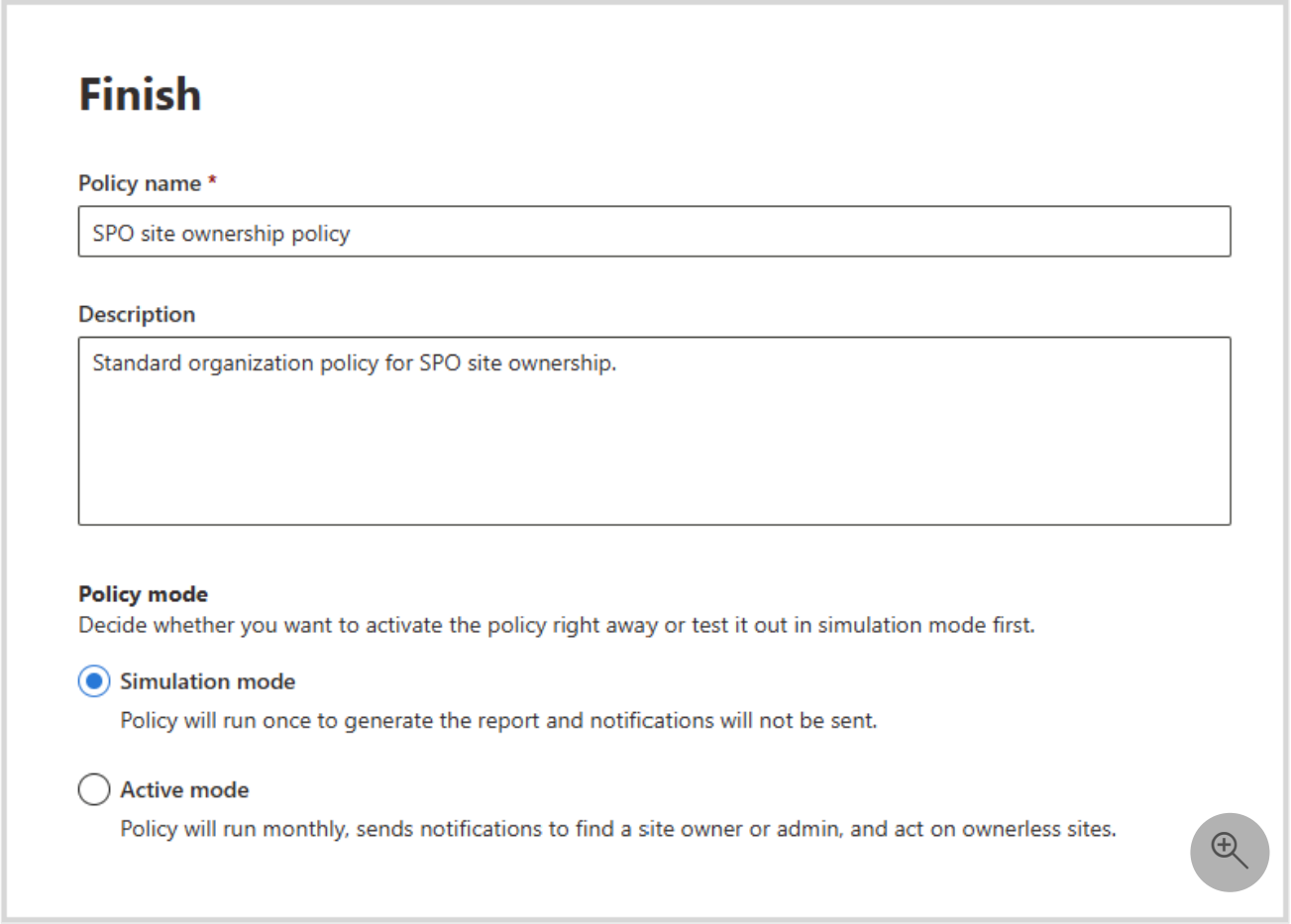
> **Tip**
>
> - You can export the site list from the SharePoint active sites page.
> - Ensure the CSV file uses the same format of the sample CSV file, that it has no duplicate URLs, and that the URLs are valid and complete.
> - Ensure the URLs listed in CSV file belong to your tenant's domain.

6. On **Configure policy**, specify criteria for your policy, and then select **Next**.



If you plan to exclude users or groups, see important information in the section, Excluding users or groups (in this article).

7. On **Finish**, specify a name and description for your policy, select a policy mode, and then select **Finish**.



   If you select **Active mode**, your policy runs monthly, generates a report, and notifies site owners or site administrator about potential issues, depending on policy configuration.

8. After your policy is created, select **Done**.

You can view and manage your policy by selecting **Site ownership policies** in the **Site lifecycle management** dashboard.

Define ownership criteria

When you create a site ownership policy, define the ownership criteria that sites must meet. You can determine:

- Whether ownership is determined by site owners, site administrators, or both.
- The minimum number of owners or administrators required for a site.

For example, setting the minimum owner count to `2` identifies sites that have only a single owner and require remediation.

When the policy runs, it identifies sites that don't meet the configured ownership requirements and generates a report. Active policies can also notify selected recipients.

Overlapping policies of same policy type

When more than one policy of the same policy type includes the same site, SharePoint helps reduce duplicate notifications by using stored site-level policy history.

If a notification was sent within the last 30 days from any policy of that type, and the site remains uncertified, no further notifications are sent and the policy execution report shows the site's status as "Notified by another policy."

For example, if a site is covered by two different inactive site policies and receives a notification email from the first policy, the second policy doesn't send additional notifications within the next 30 days if the site remains uncertified.

We recommend that policies of the same type don't have overlapping scopes. If sites fall under multiple policies of the same type, notification schedules and enforcement actions can become difficult to predict.

Overlapping policies of different types

Policies of different types operate independently for notification purposes. Notification history is tracked separately for each policy type.

For example, if a site falls within the scope of both a Site Ownership policy and an Inactive site policy, site owners may receive notifications from both policies when the respective policy conditions are met.

Enforcement actions are evaluated independently by each policy. If a policy applies an enforcement action that changes the site's state, the site may no longer qualify for processing by other policies:

- If a policy places the site in a read-only (locked) state, the site is no longer included in the scope of other policies.
- If a policy archives the site, the site reaches a terminal state and is no longer considered for enforcement by other policies.

When multiple policy types target the same site, the enforcement action from the policy whose conditions are satisfied first is applied first.

Disabling or deleting a policy

Disabling or deleting a policy stops future activities from that policy, including notifications and enforcement actions. It doesn't automatically reverse previously applied actions.

Notification history is maintained at the site level separately for each policy type. As a result, disabling or deleting one policy doesn't affect notification history associated with other policy types that continue to target the site.

For policies of the same type, stored notification history (including notification count and last notification date) is retained even after a policy is disabled or deleted. This history naturally resets after the site has been absent from the scope of that policy type for 90 days.

If notification history needs to be reset sooner, contact Microsoft Support to determine whether the stored notification state can be cleared.

> **Important**
>
> To ensure predictable behavior, avoid creating overlapping policies of the same type that target the same sites. While SharePoint suppresses duplicate notifications where possible, overlapping policies can make notification timing and enforcement outcomes harder to interpret.

Policy modes

Site ownership policies support two operating modes:

- **Simulation mode** – Runs the policy once and generates a report without ongoing enforcement.
- **Active mode** – Runs monthly, generates reports, sends notifications, and can apply enforcement actions based on policy configuration.

> **Note**
>
> Site lifecycle policies in simulation mode are now available in GCCH and DoD environments as of November 17, 2025.

For more information about policy modes across site lifecycle management policies, see Overview of SharePoint site lifecycle management.

Policy scope

You can create different site ownership policies for different groups of sites across your organization. When configuring scope, select sites based on:

- Site templates
- Site creation sources
- Sensitivity labels
- Retention policies
- Retention holds

You can also exclude up to 100 specific site URLs.

> **Note**
>
> The following sites are excluded from site ownership policies:
>
> - OneDrive sites
> - Sites created by system users
> - App catalog sites
> - Root sites
> - Home sites
> - Tenant admin sites

Resolve user ID mismatches before running a policy

Before you run a site ownership policy, resolve any user ID mismatches to help ensure accurate ownership evaluation. User ID mismatches can occur when you delete and later recreate a user account, which leaves site ownership references associated with an obsolete identifier.

See Fix site user ID mismatch in SharePoint or OneDrive.

Configure ownership notifications

During policy configuration, choose who should receive notifications when ownership requirements aren't met. The configured recipient categories are cumulative eligible recipient sets, not an ordered fallback chain. You can notify:

- **Current site owners:** If you set the minimum owner or admin count to two and the site has an existing site owner, the owner receives an email notification asking them to add another owner.
- **Current site admins:** If you set the minimum owner or admin count to two and the site has an existing site administrator, the administrator receives an email notification asking them to add another owner.
- **Managers of previous owners or admins:** If an owner or administrator of a site leaves the organization, their managers are informed that the site needs an owner for effective management. If managers are members of a site, they can accept ownership. If they're visitors or don't have access to the site, they can coordinate with SharePoint administrators to find the next best owner.
  - As a user's details are deleted from the system 30 days after leaving the organization, managers might get only one notification about the site.
  - If the policy runs after 30 days of a user's leaving the organization, manager information isn't available, and notifications can't be sent.
  - For a Teams site, the "manager of the previous site owner" notification works only for users added directly to the SharePoint site owner. If the user was added from a Microsoft 365 Group, the notification isn't sent. This limitation exists because of how user information is retained after an account is deleted. To improve the chances of successfully sending notifications, select at least three options.
- **Active site members:** Based on policy configuration, the policy sends emails to the most recent active members of a site to accept ownership.
  - To ensure relevance and recency, read or write activity performed by a site member on a site in the last 180 days is considered as an activity.
  - Any user with last activity beyond 180 days isn't considered for these notifications.
  - External and guest users aren't considered for these notifications to accept ownership.

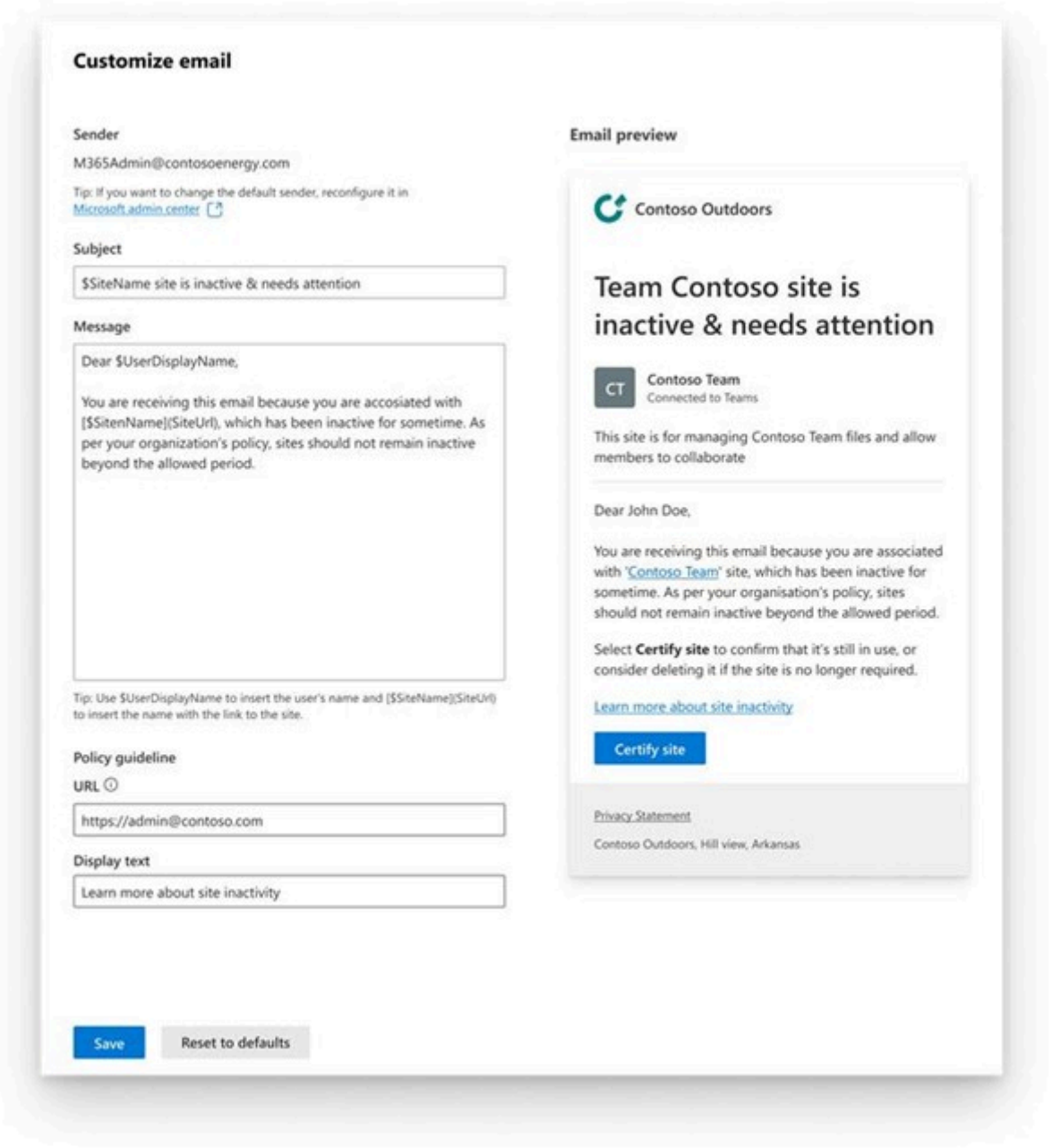
> **Note**
>
> If a site has no one to notify as per the email recipients provided during policy configuration, the count is provided in the summary. You can triage the sites and determine the next course of action.

Customize email notifications

Administrators can customize the email messages that site lifecycle management policies send when site issues require attention.

Customizing email content helps improve the read-through rate of the emails, which effectively improves response efficiency and contributes to better governance across the tenant.

You can customize emails in the configure step. When you select **Customize email to be sent**, the customization window opens as shown in the following screenshot:



The following table describes the sections you can customize:

Expand table

Customizable section	Description
Sender	You must configure a custom domain in the Microsoft 365 admin center before you can use the email customization feature. For more information, see Choose which domain to use for your email.
Subject (up to 100 characters)	Use `$UserDisplayName` to insert the user's name and `$SiteName` to insert the name of the site.
Message (up to 500 characters)	Use `$UserDisplayName` to insert the user's name, `$SiteName` to insert the name of the site, and `$SiteUrl` to insert the URL of the site.
Policy guideline URL	Only valid HTTP links are allowed.
Policy guideline description text	The default value is the placeholder text.

To customize emails for existing policies, follow these steps:

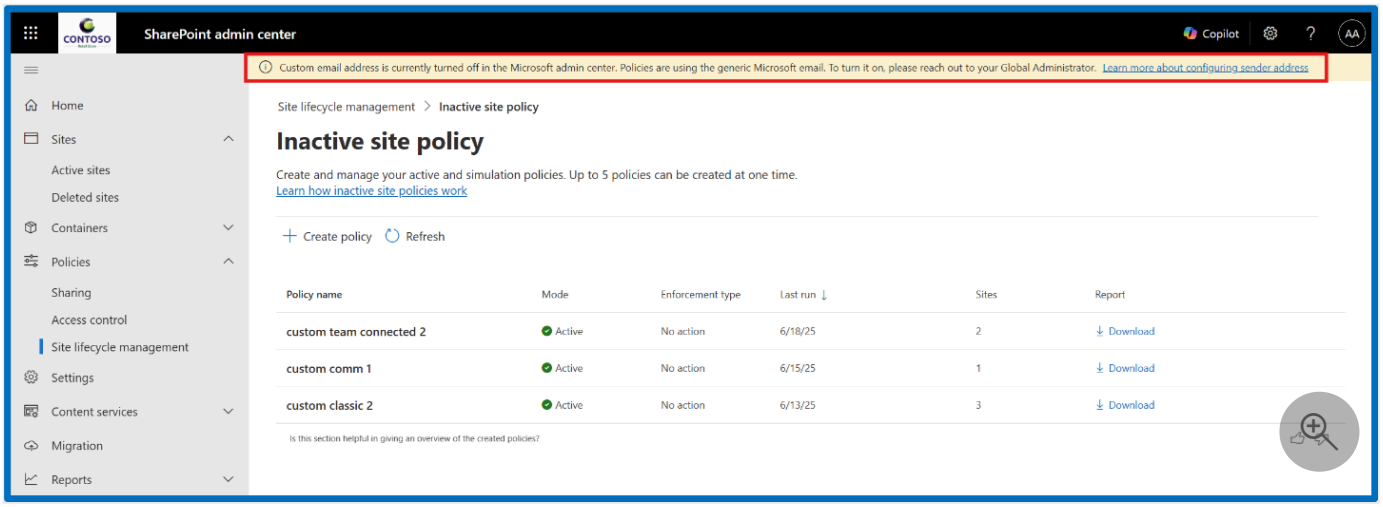
1. Select an existing policy.
2. Select **Edit configuration**.
3. Find the email customization option.

> **Note**
>
> If you don't configure email customization for a policy, the system continues to send default emails from `noreply@sharepoint.com`.

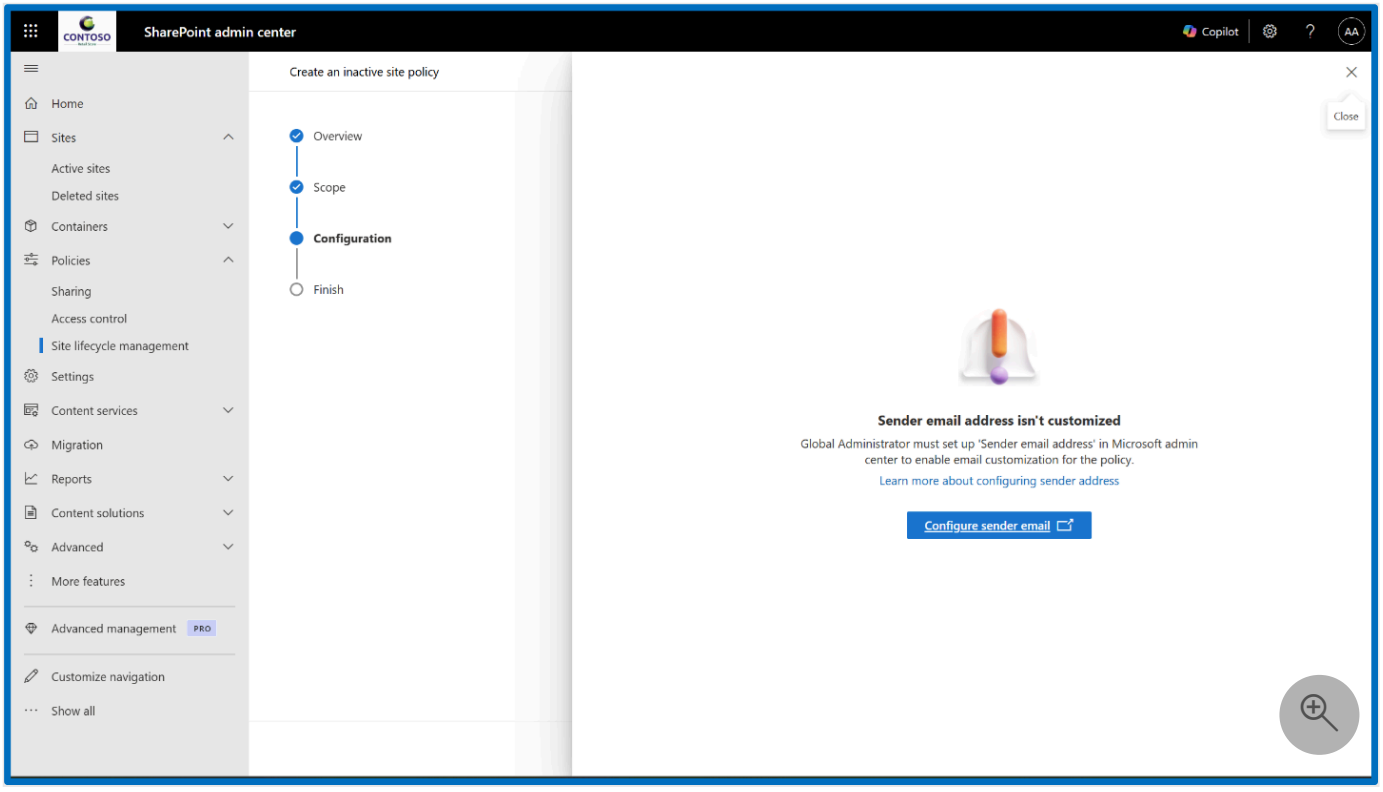
What to do if you can't customize email messages

You can't customize emails if the custom domain setting isn't configured or is turned off.

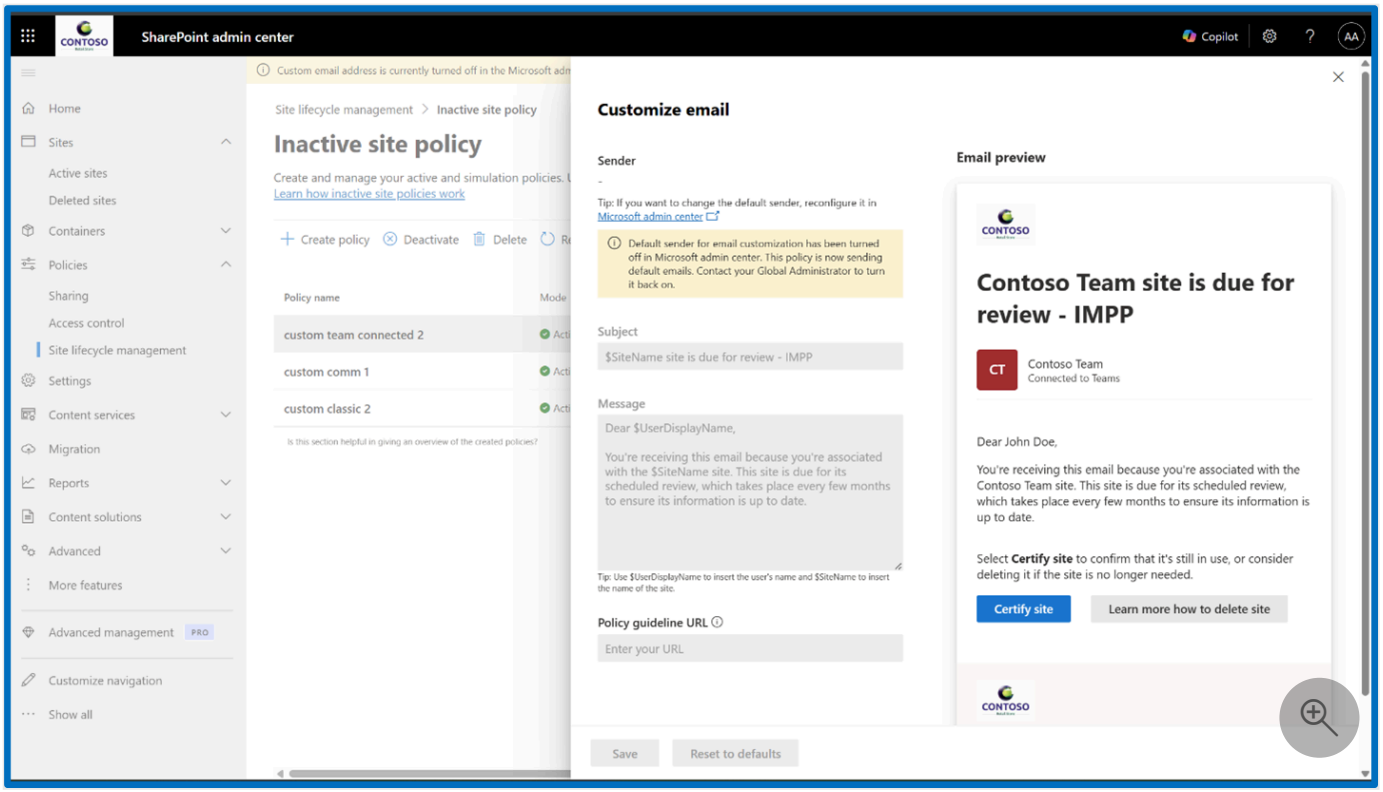
You must configure the **Send email notifications from your domain** setting in the Microsoft 365 admin center before you can customize emails. If you don't configure this setting, you see a warning message at the top of the policy list, as shown in the following image:



You might also see the warning message during the configuration step, as shown in the following screenshot:



If you previously customized emails in one or more policies, but later turn off the **Send email notifications from your domain** setting in the Microsoft 365 admin center, you see the message bar in the policy list, and a warning message in the email customization window, as shown in the following screenshot:



> **Note**
>
> Only someone who has the Global Administrator role can configure domain settings in the Microsoft 365 admin center.

Review ownership notifications

The active policy sends ownership policy notifications when it detects sites that don't meet ownership requirements. Recipients can take actions directly from the email to help resolve ownership issues.

> **Important**
>
> Site lifecycle management policies use Outlook Actionable Messages to enable recipients to take actions directly from email.
>
> - Ensure required Outlook versions are deployed.
> - US Government cloud customers must complete additional actionable message configuration.
> - For troubleshooting guidance, see the Outlook Actionable Messages documentation.

Excluding users or groups

You can exclude specific users, Microsoft 365 Groups, or security groups from receiving site lifecycle management requests and notifications, even if they're site owners or site admins for sites that are included in a policy.

Key behaviors:

- Exclusions are used only to determine notification recipients.
- Excluding a user or group doesn't change site permissions or ownership, and doesn't exclude the site from lifecycle policy evaluation
- Sites continue to be evaluated by the policy as usual.

Limits:

- You can add up to 100 entries to the exclusion list.
- Each entry can be an individual user, a Microsoft 365 Group, or a security group
- The 100-entry limit applies to the number of entries, not the number of users within a group. For example, a group with more than 100 members counts as one entry.

Group exclusion behavior (important):

- When a group is added to the exclusion list for a policy, that group is excluded from notifications only when the group is directly added to the site or is a nested group within other groups that are directly added to the site.
- A member of an excluded group might still receive a notification if they're directly added to the site or are part of some other group that is directly added to the site.

Enforcement actions

> **Note**
>
> Hard enforcement actions, such as locking a site or setting it to read-only, apply only to ownerless (zero owner) sites, where there's no accountable party and the governance risk is highest. Applying such enforcements to sites with an active owner can be disruptive and could unintentionally impact business workflows. As a result, this policy is designed to nudge rather than disrupt. Single owner sites receive notifications and reports that encourage restoration of the minimum owner count, without blocking access. If the site owner takes no action in such cases (nonownerless, but still in violation sites), after the third notification, there's a three-month cool-off period after which notifications resume.

The following table summarizes how the site ownership policy behaves, based on the selected enforcement action:

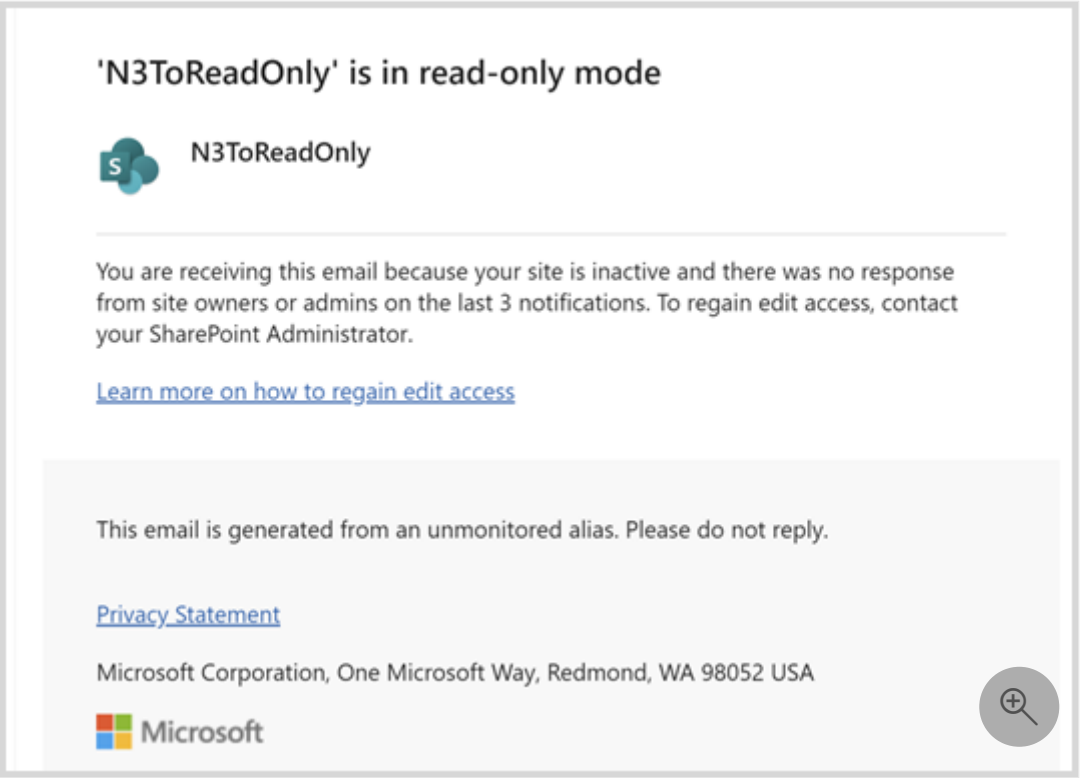
Expand table

Enforcement action	Policy behavior
Do nothing	The specified recipients receive monthly notifications for three months. After this period, the policy sends no notifications for the next three months. If the site remains in violation of ownership criteria after six months, monthly notifications resume. The policy execution report lists sites in violation as unactioned. You can download this report and filter out sites marked as unactioned.
Read-only access	The specified recipients receive monthly notifications for three months. - If the notification recipients don't address site ownership during this period and the site continues to be ownerless, it goes into read-only mode. - If the notification recipients don't address site ownership during this period but the site has at least one owner, after the third notification, there's a three-month cool-off period, after which notifications resume.
Archive sites after mandatory read-only period	The specified recipients receive monthly notifications for three months. - If the notification recipients don't address site ownership during this period, and the site continues to be ownerless, the site goes into a read-only mode for the configured number of months. After the configured number of months, the site gets archived through Microsoft 365 Archive. Archival must be enabled for the tenant in the Microsoft 365 admin center. - If the notification recipients don't address site ownership during this period but the site has at least one owner, after the third notification, there's a three-month cool-off period, after which notifications resume.

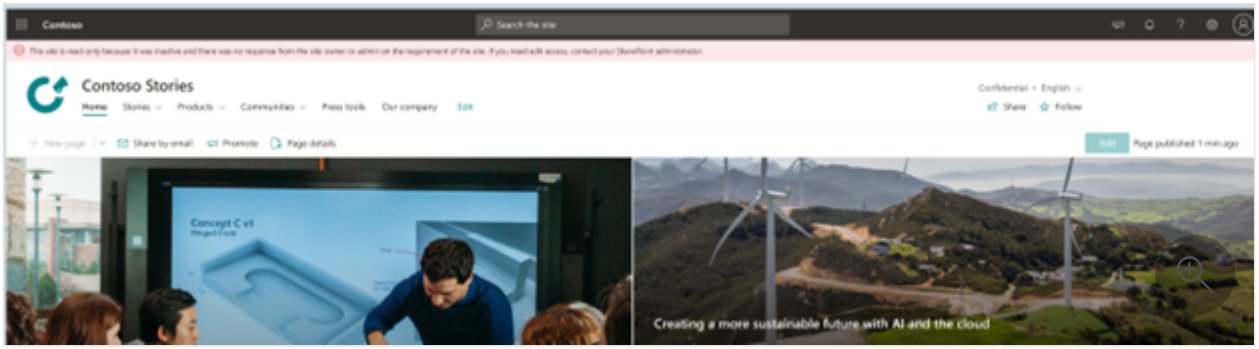
Read-only mode

A site ownership policy that you configure with the read-only enforcement action sends extra notifications to inform the specified recipients when there's no response.

When a site goes into read-only mode, a notification is sent.



If a site is in read-only mode, the following banner is added to the site:



Important points about read-only or locked sites

For sites that are in a read-only or locked state, the following behaviors are expected.

- **Unlocked sites**: Always included in policy scope
- **Read-only sites locked by the same policy type**:
  - Included in scope
  - Report indicates the site was previously actioned by this policy
- **Read-only sites locked by a different policy type**:
  - Excluded from policy scope
  - Another policy already owns and governs this site

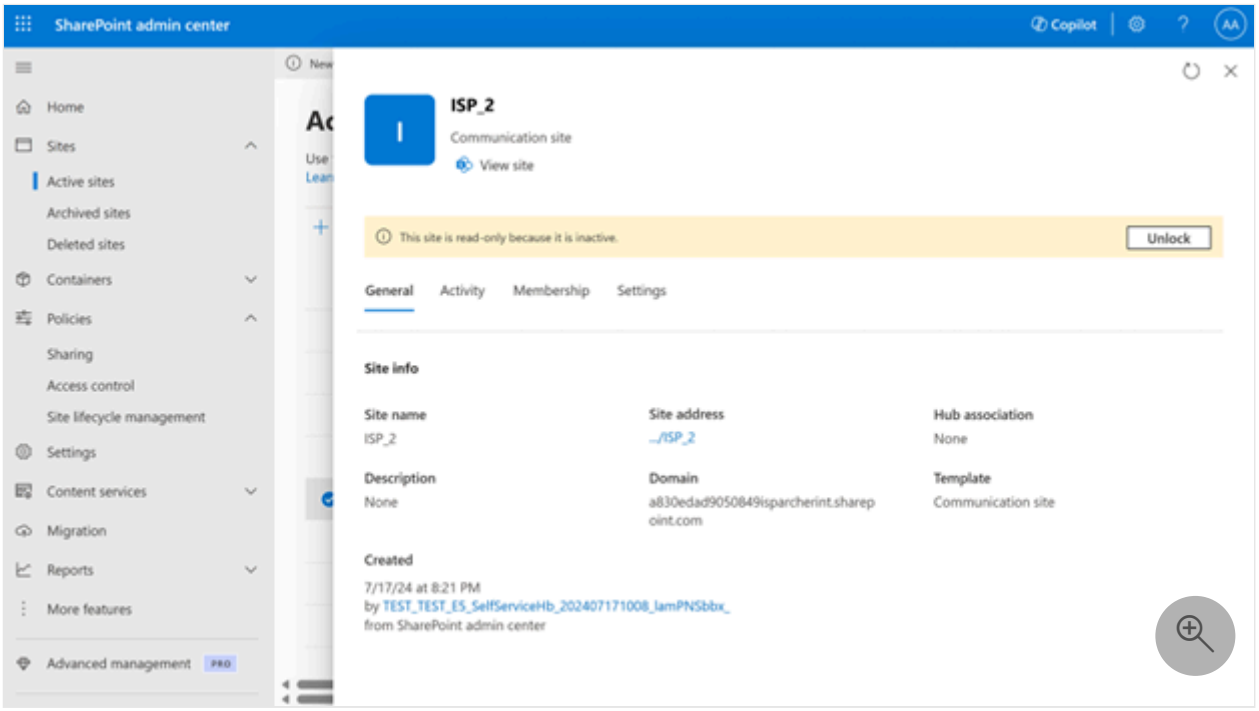
- **Read-only sites externally locked** (locked because of reasons other than site lifecycle management):
  - Included in scope
  - External locks do not prevent the site from being evaluated by the policy
- **No-access (fully locked) sites**:
  - Included in scope, but no enforcement action is taken
  - The policy skips action because the site is already in a no access locked state

These are default behaviors that can't be modified through policy configurations.

Remove a site from read-only mode

To remove a site from read-only mode in SharePoint admin center, go to the **Active sites** page, select the site, and then select **Unlock** from the site page panel.

Site owners can't remove a site from read-only mode and must contact the tenant admin to remove read-only mode.



Unarchive a site

To unarchive a site in SharePoint admin center, expand **Sites** and select **Archived sites**. Select the site you want to unarchive and select **Reactivate**.

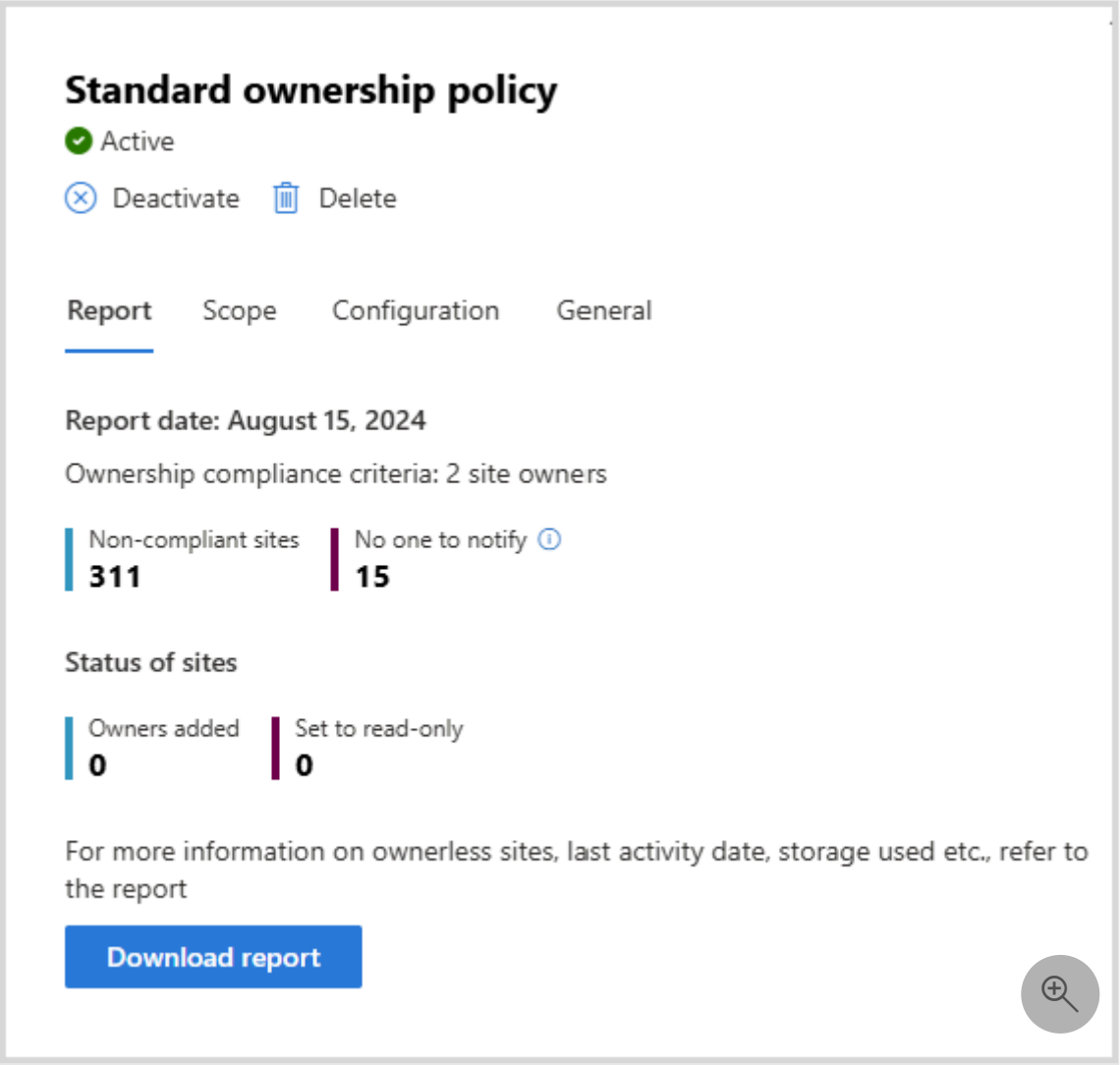
> **Note**

Only tenant admins can reactivate an archived site.

Reporting

Each policy run generates a report that shows sites that don't meet the configured ownership requirements. The report summarizes:

- Ownership compliance status
- Notification history
- Enforcement actions
- Ownership configuration details
- Site metadata



Select **Download report** to download the detailed report in a .csv format. The following table describes the information included in the policy execution report:

Expand table

Column	Description
Site name	Name of the site
URL	URL of the site
Template	Template of the site
Sensitivity label	Sensitivity label of the site
Retention policy	Indicates if any retention policy is applied to the site
Site lock state	State of site access **before** the policy runs (Unlock/Read-Only/No access)
Minimum owners or admins configured	Minimum owner or admin count you configured while creating the policy
Number of site owners	Total count of site owners for the site
Email address of site owners	Email addresses of all site owners
Number of site admins	Total count of site administrators for the site
Email address of site admins	Email addresses of all site administrators
Managers of previous owners or admins	Email addresses of the managers of previous owners or admins (if this option was configured during policy set-up)
Active members	Email addresses of the active site members (if this option was configured during policy set-up)
Total notifications count	Total notifications sent so far by any policy under the same policy template
Action status	Status of the site [First/second/third notification sent, Site in read-only mode, Site archived, Action taken by another policy]
Action taken on (UTC)	Date on which the enforcement action was taken (date when site was archived or put in read-only mode)
Last activity date (UTC)	Date of last activity detected across SharePoint site and connected workloads
Site creation date (UTC)	Date when the site was created
Storage used (GB)	Storage consumed by the site
Duration in read-only (days)	Number of days the site is in the enforced read-only state

Set up actionable emails for SLM policies in US Government cloud environments

In US Government Cloud (GCC High and DoD) environments, a tenant administrator must complete an extra, one-time setup for SharePoint site lifecycle management (SLM) policies to use actionable messages. This step helps ensure that policy notification emails display and function correctly. For example, site admins and site owners can take actions directly from email.

Unlike other commercial cloud environments, GCC High and DoD tenants require explicit administrator approval of the actionable message provider before it can send interactive email messages. Without this approval, SLM policy emails are delivered, but action buttons don't function as expected.

> **Important**
>
> You must be a Global Administrator or Exchange Administrator in the tenant to set up actionable messages.

Approve the SLM actionable message provider

1. Go to the Outlook Actionable Messages – Connectors admin portal for GCCH or DoD and sign in.
2. In the **Provider Status** filter, select **Approved by Microsoft – Pending Your Approval**.
3. Locate the provider named `InactiveSiteOAMProviderGCCH`.
4. Select the provider, and then select **Approve**.

After you approve the provider, the SLM policy notifications send actionable messages.

> **Note**
>
> This approval applies only to SLM policy notifications. Other applications or services that use actionable messages might require separate approval.

Ensure actionable messages are enabled for the tenant

Site lifecycle management policies use Outlook actionable messages to enable site owners or site administrators to take necessary actions by using links within email messages.

- For notifications to render properly, make sure your organization meets the Outlook version requirements.
- To troubleshoot rendering problems, see frequently asked questions.

Troubleshooting actionable messages

If actionable messages don't work as expected, try these steps:

- Make sure that the `InactiveSiteOAMProviderGCCH` provider is in an approved state.
- Allow sufficient time. It can take up to 24 hours for changes to propagate.

Related articles

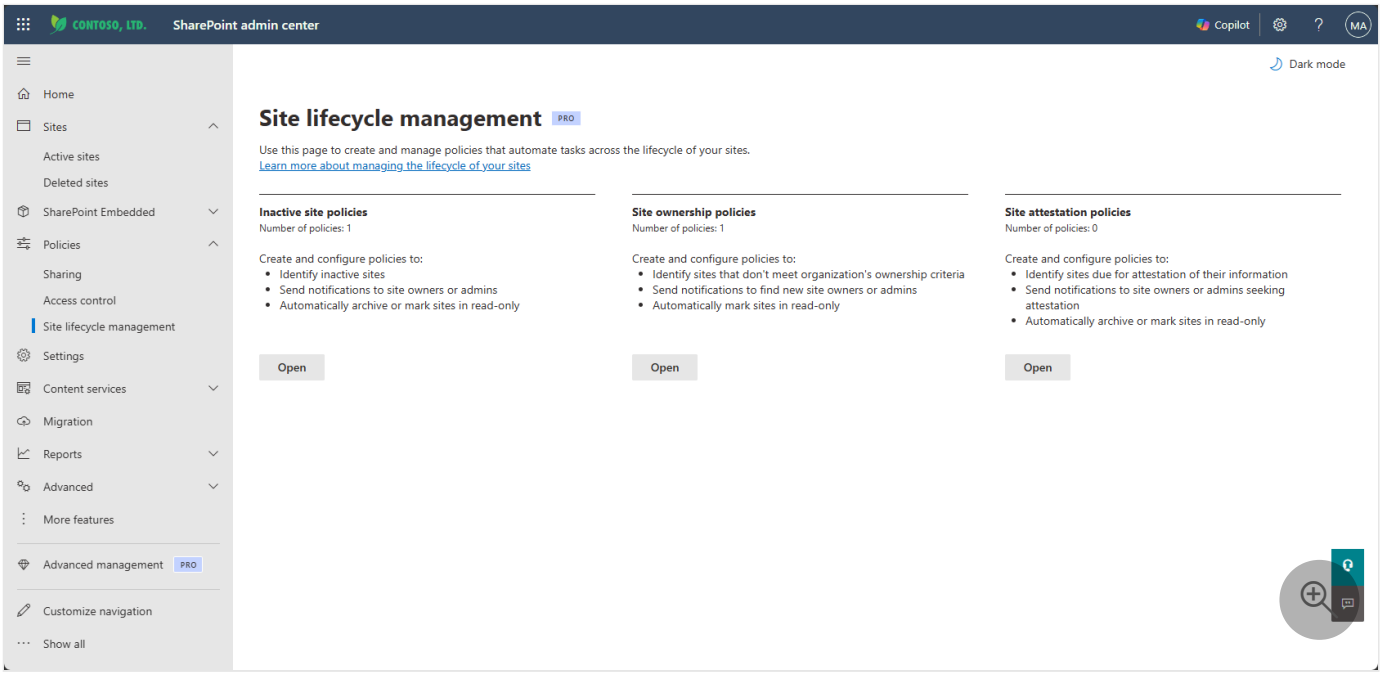
- SharePoint site lifecycle management
- Manage inactive sites by using inactive site policies
- Request recurring site attestations for SharePoint sites
- What is SharePoint Advanced Management?

Last updated on 08/19/2026

Manage inactive sites by using inactive site policies

Inactive site policies help you identify SharePoint sites that aren't active for a specified period of time. Use these policies to notify site owners or site administrators, request confirmation that a site is still needed, and take enforcement actions when no response is received. You can configure an inactive sites policy in the SharePoint admin center.

For an overview of SharePoint site lifecycle management and the available policy types, see Overview of SharePoint site lifecycle management policies.



This article describes how to set up an inactive site policy with notifications and enforcement actions.

Prerequisites for an inactive site policy

See SharePoint Advanced Management prerequisites.

How inactive site policies determine site activity

Inactive site policies evaluate activity across SharePoint and connected Microsoft 365 workloads to determine when a site was last active.

In-scope site activities

Inactive site policies analyze activity across SharePoint and connected platforms like Teams, Viva Engage (formerly Yammer), and Exchange to detect a site's last activity.

Expand table

Platform type	Activities
SharePoint	Viewed files, edited files, shared files internally and externally, synced files, viewed pages, visited pages
Viva Engage (formerly Yammer)	Posted messages, read conversations, liked messages
Teams	Posted channel messages in a team across standard channels, posted messages in Teams and standard channels, replied to messages, mentioned in messages, reacted to messages, sent urgent messages, conducted meetings (recurring, ad hoc, one-time)
Exchange	Received emails in the Exchange mailbox

Scope of app activities

Inactive site policies don't consider app activity through an app token. They consider app activity through a user token only when a user agent is involved and meets the following criteria.

Expand table

Activity source	Condition when activity is considered
PnP PowerShell activity via user token	Is not considered
SharePoint Online PowerShell activity via user token	Is considered only when UserAgent parameter value is passed
CSOM scripting activity via user token	Is considered when script explicitly sets UserAgent value
Any other app activity via user token	Is considered when UserAgent exists, except in the following scenarios when - UserAgent starts with "client-request=id"/"ACTIVEMONITORING"/"SPORUNNERS" **OR** - UserAgent ends with "MSDEMO"/"MSDPLATFORM"/"SystemUsage" **OR** - UserAgent contains "GomezAgent"/"bingbot.htm"/"ms search 6.0 robot"/"http://www.monitis.com"/"ISV"
App activity via app token	Is not considered

In-scope site templates

Site lifecycle management reviews the activity of communication sites, classic sites, Teams-connected sites, and group-connected sites with the following site template types:

Expand table

Site type	Template type
Communication site	SitePagePublishing#0
Classic sites	STS#0, STS#1, STS#2, WIKI#0, BLOG#0, SGS#0, SPS#0, SPSNEWS#0, ENTERWIKI#0, COMMUNITY#0, DEV#0, EXPRESS#0, EHS#1, EHS#2
Teams-connected site	STS#3 or Group#0
Group-connected site	STS#3 or Group#0

Out-of-scope sites

The following sites are out of scope and excluded from site activity detection:

- OneDrive sites
- Sites created by system users
- App catalog sites
- Root sites
- Home sites
- Tenant admin sites
- Sites associated with Shared and Private Teams channels

Policy modes

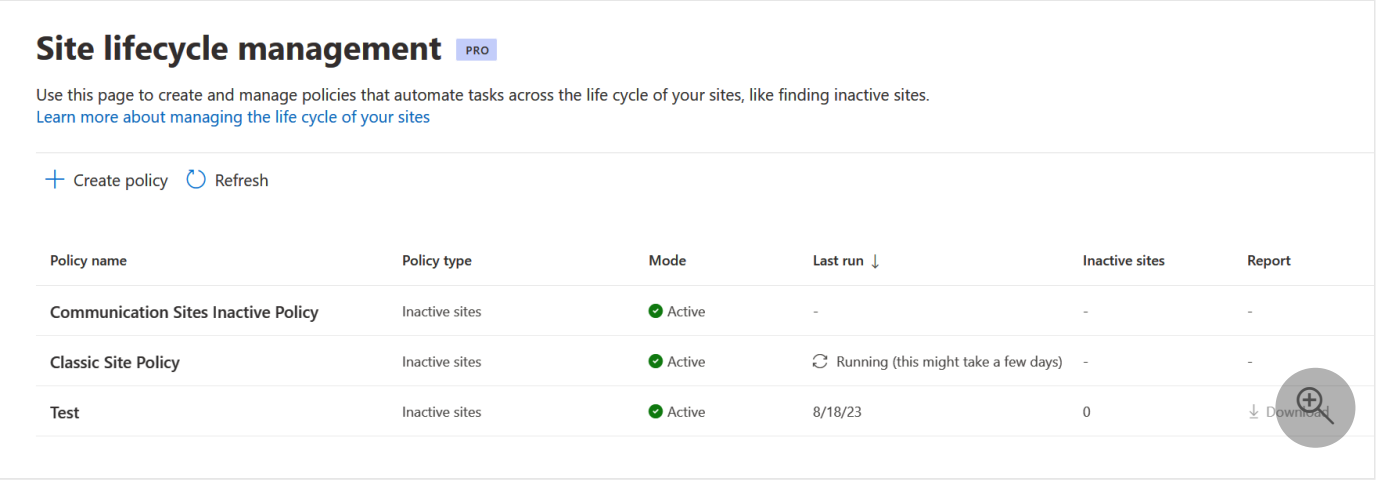
Site ownership policies support two operating modes:

- **Simulation mode** – Runs the policy once and generates a report without ongoing enforcement.
- **Active mode** – Runs monthly, generates reports, sends notifications, and can apply enforcement actions based on policy configuration.

> **Note**

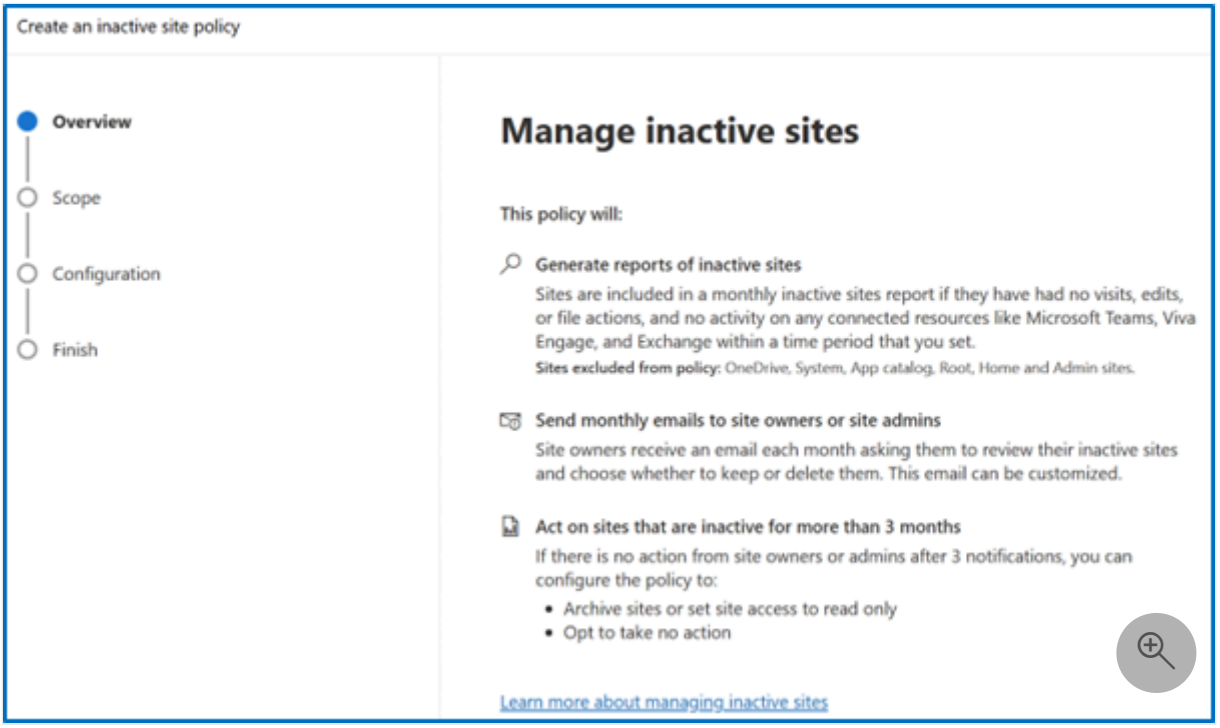
Site lifecycle policies in simulation mode are now available in GCCH and DoD environments as of November 17, 2025.

For more information about policy modes across site lifecycle management policies, see Overview of SharePoint site lifecycle management.

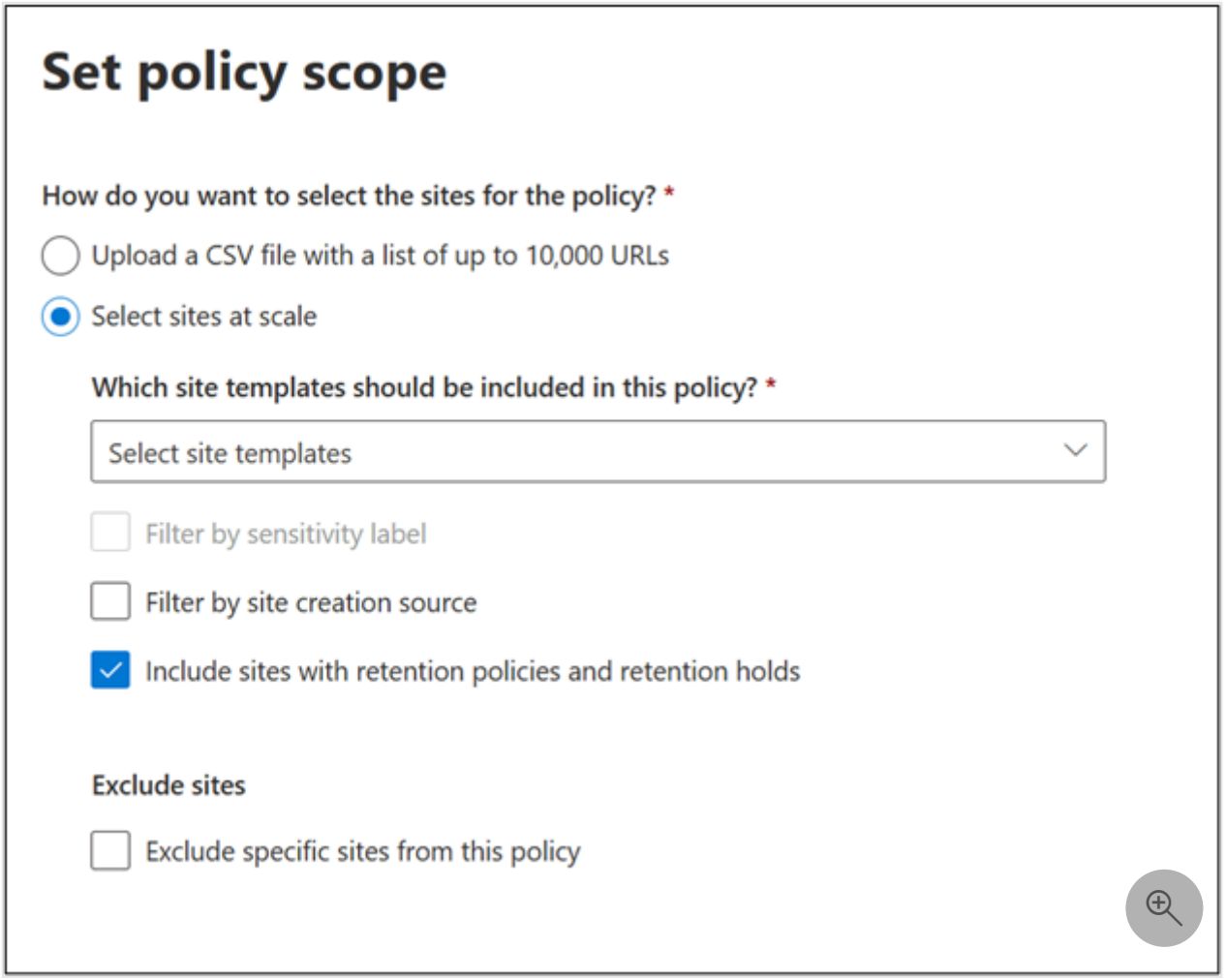


Create an inactive site policy

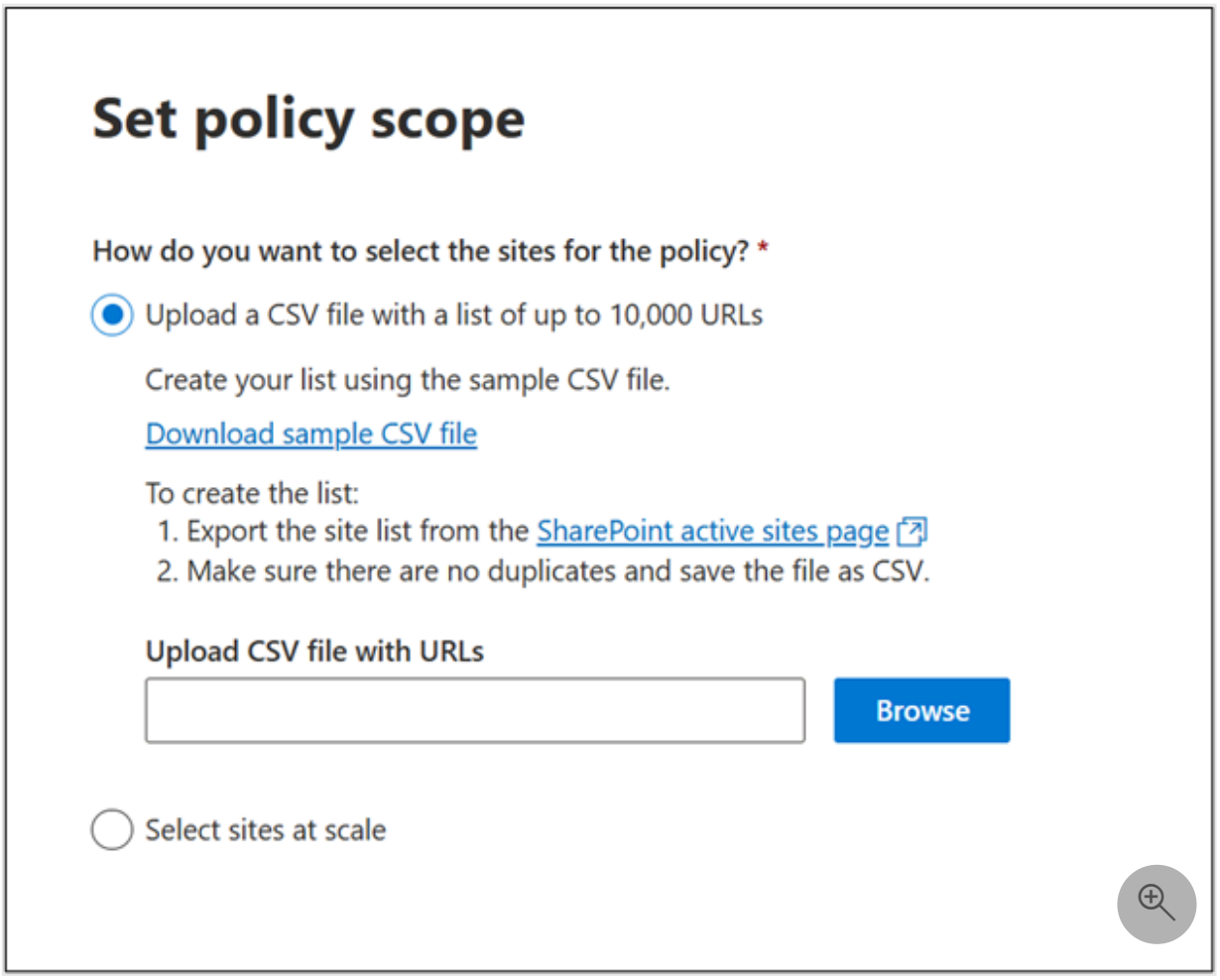
1. As a SharePoint administrator, go to the SharePoint admin center and sign in.
2. In the navigation pane, expand **Policies**, and then select **Site lifecycle management**.
3. Under **Inactive site policies**, select **Open**.
4. Select + **Create policy**. Review the **Manage inactive sites** information, and then select **Next**.



5. On the **Set policy scope** step, choose your policy scope option, and then select **Next**.



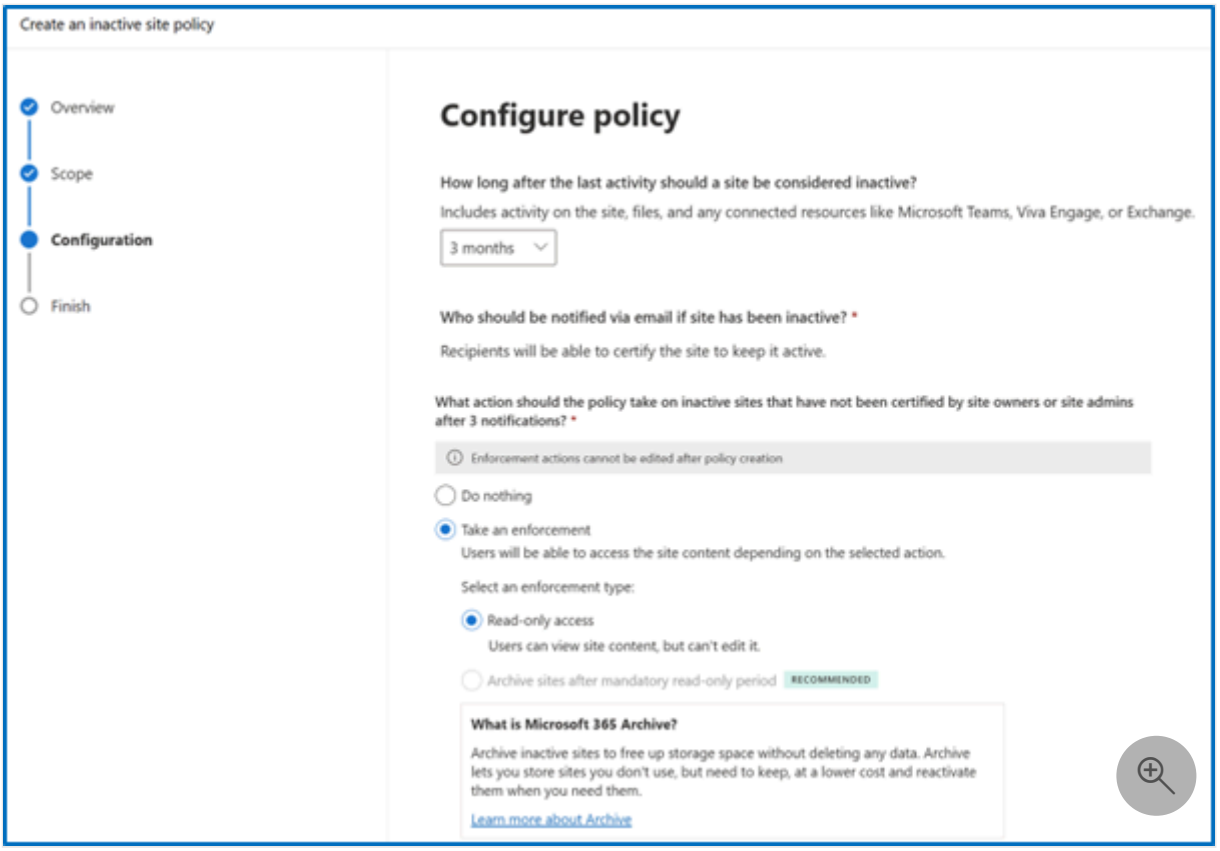
- If you select **Upload a CSV file with a list of up to 10,000 URLs**, you can upload a list of site URLs of select sites for the policy.



> **Tip**
> - You can export the site list from the SharePoint active sites page.
> - Ensure the CSV file uses the same format of the sample CSV file, that it has no duplicate URLs, and that the URLs are valid and complete.
> - Ensure the URLs listed in CSV file belong to your tenant's domain.

- If you chose **Include sites with retention policies and retention holds**, this option applies only to sites that are governed by Microsoft Purview retention policies and labels. This setting doesn't affect the inclusion or exclusion of sites that are in a read-only or locked state.

6. On the **Configure policy** step, specify an inactivity period, who to notify, and what actions you want to take after three notifications. Then select **Next**.



- Choose to send emails to site owners or site admins, or both.
- If you plan to exclude users or groups, see the section Exclude users or groups from a policy(in this article).
- Customize the email content to provide more context and instructions to the email recipients.
- Choose enforcement actions if there's no response from site owners or admins after three notifications.

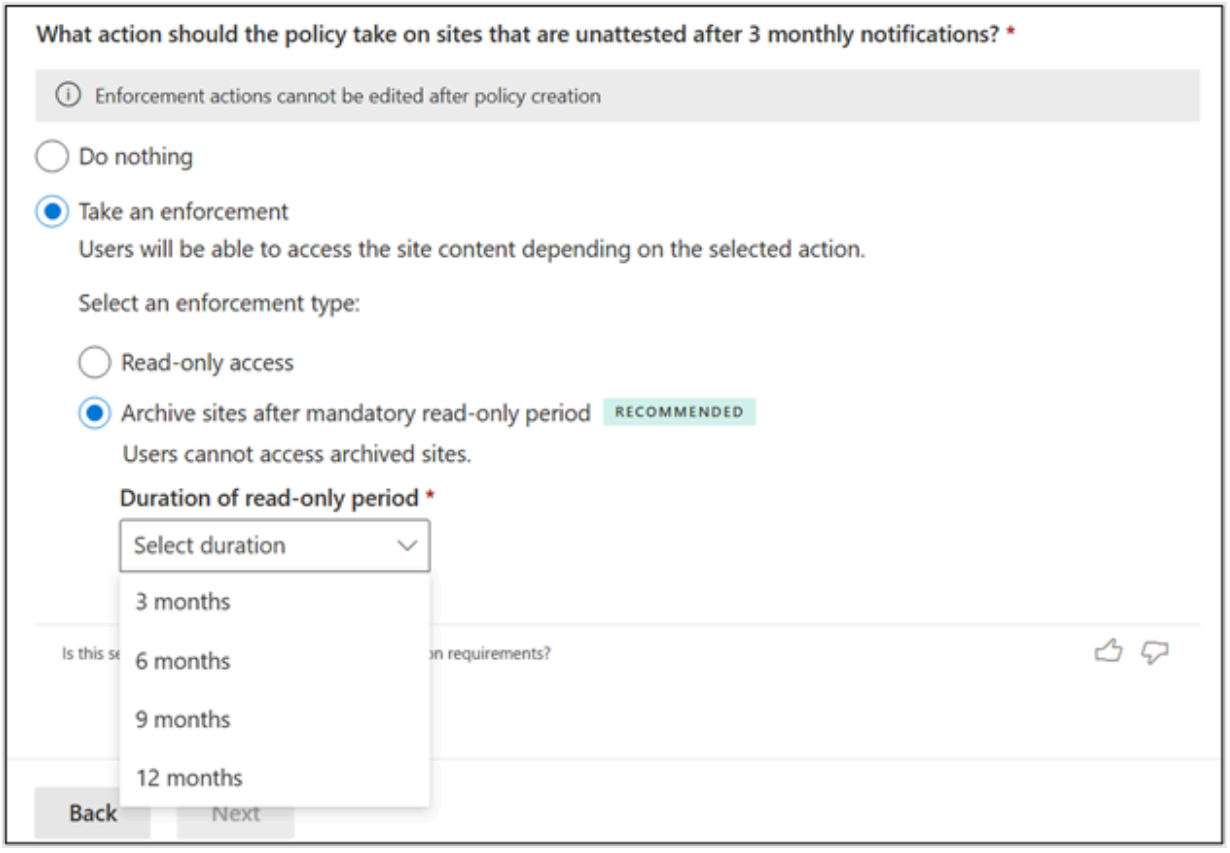
  With any of the SharePoint site lifecycle management policies, for sites that aren't certified or attested after three monthly notifications, you can take one of the following enforcement actions described in the following table:

Expand table

Enforcement action	Policy behavior
Do nothing	Site owners or site admins receive monthly notifications for three months. After this period, no notifications are sent for the next three months. If the site remains unattested after six months, monthly notifications resume. The policy execution report lists unattested sites as unactioned by the site

Enforcement action	Policy behavior
	owner. You can download this report and filter out sites marked as unactioned.
Read-only access	Site owners or site admins receive monthly notifications for three months. If the notification recipients don't mark the site as attested during this period, the site goes into read-only mode.
Archive sites after mandatory read-only period	Site owners or site admins receive monthly notifications for three months. If the notification recipients don't mark the site as attested during this period, then the site goes into a read-only mode for a configurable duration (3, 6, 9, or 12 months). After the configured number of months, the site gets archived through Microsoft 365 Archive. Archival is subject to the tenant enabling Microsoft 365 Archive in the Microsoft 365 admin center.

The following screenshot shows an example of configuring enforcement actions for a site attestation policy:



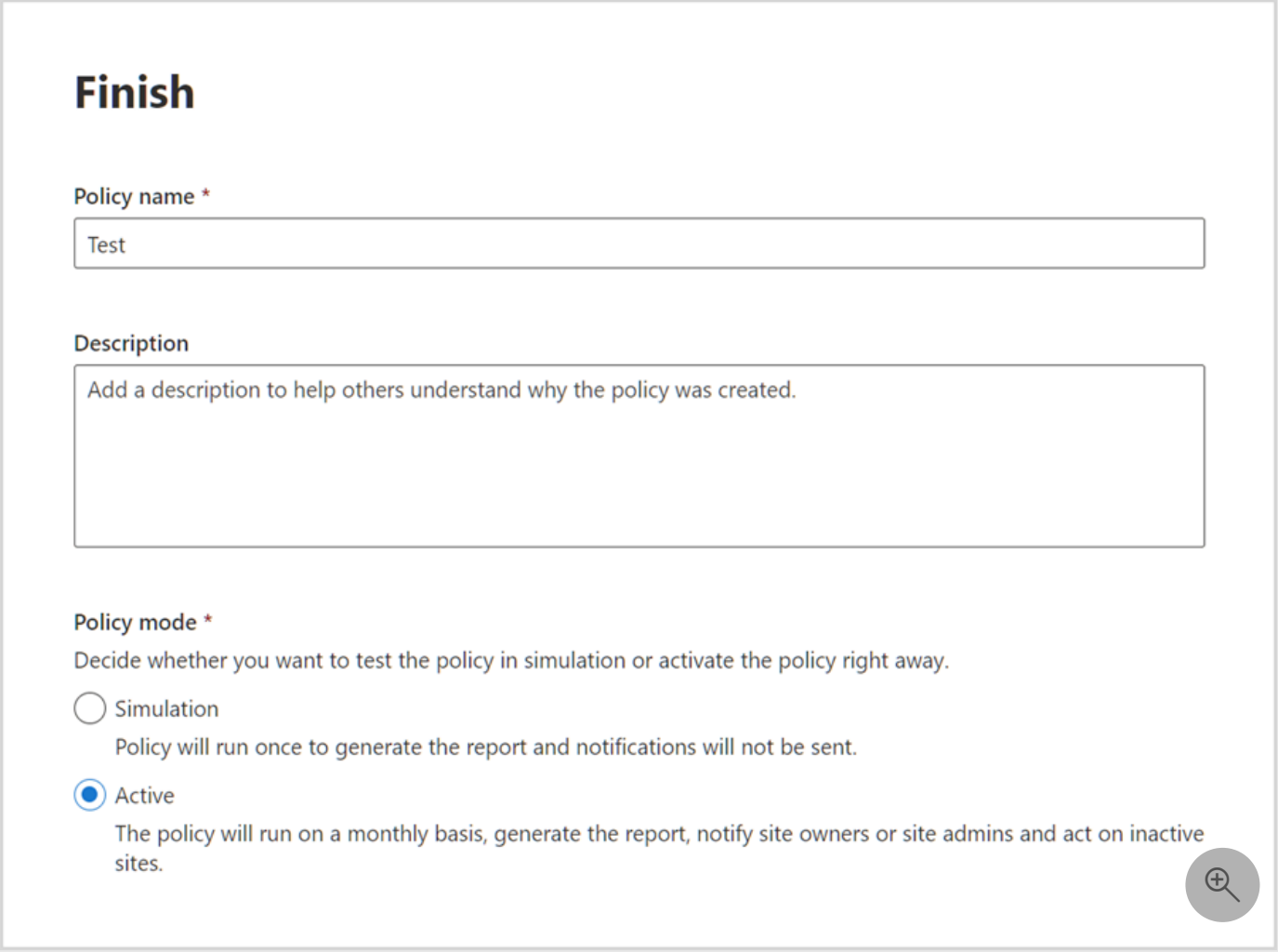
> **Note**
>
> If you configure the policy to take an enforcement action:
>
> - The notifications won't be sent after policy action is successful.

- The site and it's status are included in the monthly report.

7. On the **Finish** step, specify a name and description for your policy, and select a policy mode. Then Select **Finish**.

8. After your policy is created, select **Done**.

Once your policy is deployed, you can view and manage it in the **Site lifecycle management** > **Inactive site policy** dashboard.



Exclude users or groups from a policy

You can exclude specific users, Microsoft 365 Groups, or security groups from receiving site lifecycle management requests and notifications, even if they're site owners or site admins for sites that are included in a policy.

Key behaviors:

- Exclusions are used only to determine notification recipients.

- Excluding a user or group doesn't change site permissions or ownership, and doesn't exclude the site from lifecycle policy evaluation
- Sites continue to be evaluated by the policy as usual.

Limits:

- You can add up to 100 entries to the exclusion list.
- Each entry can be an individual user, a Microsoft 365 Group, or a security group
- The 100-entry limit applies to the number of entries, not the number of users within a group. For example, a group with more than 100 members counts as one entry.

Group exclusion behavior (important):

- When a group is added to the exclusion list for a policy, that group is excluded from notifications only when the group is directly added to the site or is a nested group within other groups that are directly added to the site.
- A member of an excluded group might still receive a notification if they're directly added to the site or are part of some other group that is directly added to the site.

Inactive site notifications to site owners or site admins

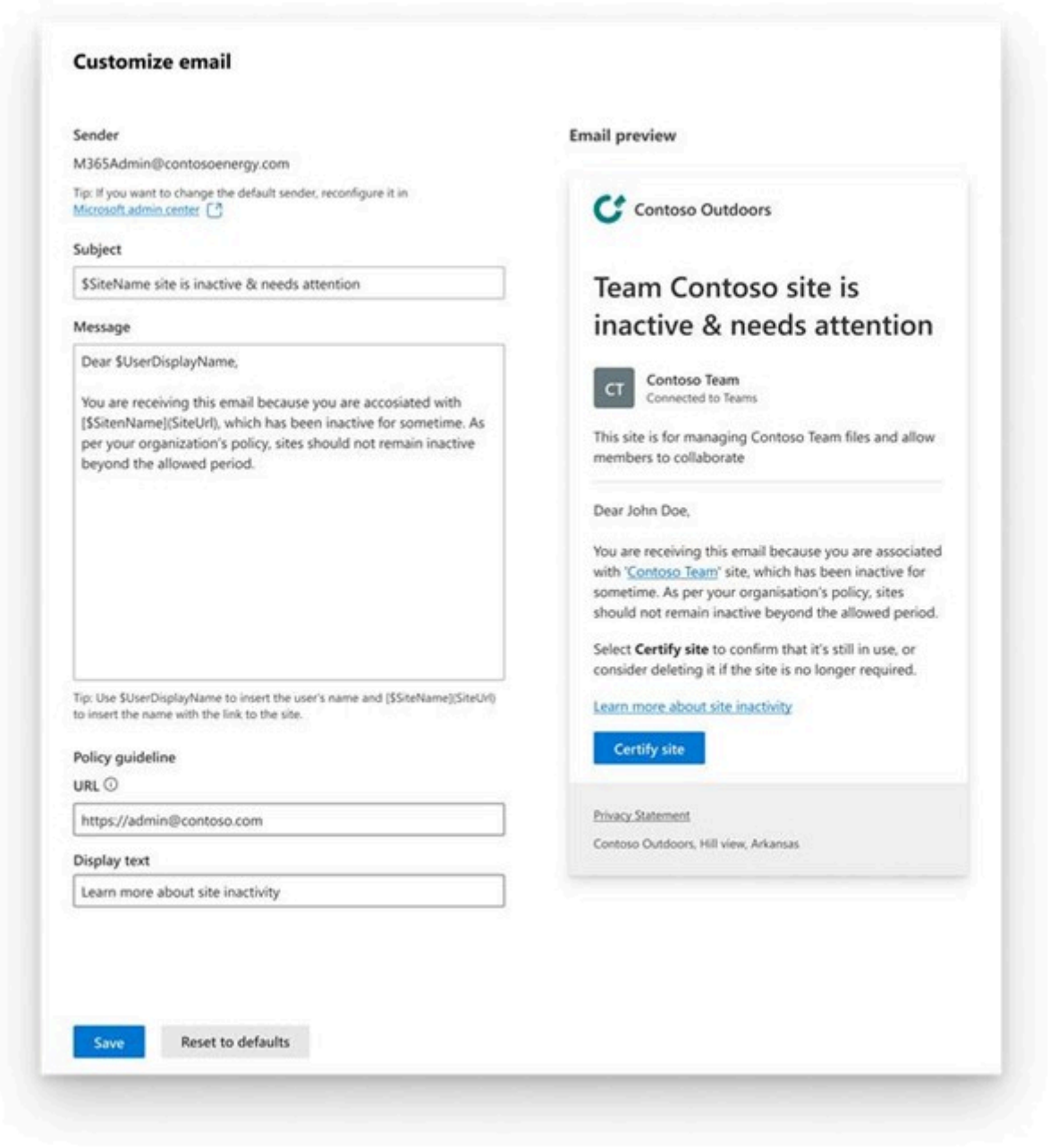
Notifications inform SharePoint site owners or site admins when a site is inactive for a specified number of months. To keep the site, the notification recipients should select the **Certify site** button in the notification email. Once certified, Site lifecycle management doesn't check the site's activity for one year.

Customize email notifications

Administrators can customize the email messages that site lifecycle management policies send when site issues require attention.

Customizing email content helps improve the read-through rate of the emails, which effectively improves response efficiency and contributes to better governance across the tenant.

You can customize emails in the configure step. When you select **Customize email to be sent**, the customization window opens as shown in the following screenshot:



The following table describes the sections you can customize:

Expand table

Customizable section	Description
Sender	You must configure a custom domain in the Microsoft 365 admin center before you can use the email customization feature. For more information, see Choose which domain to use for your email.
Subject (up to 100 characters)	Use `$UserDisplayName` to insert the user's name and `$SiteName` to insert the name of the site.
Message (up to 500 characters)	Use `$UserDisplayName` to insert the user's name, `$SiteName` to insert the name of the site, and `$SiteUrl` to insert the URL of the site.

Customizable section	Description
Policy guideline URL	Only valid HTTP links are allowed.
Policy guideline description text	The default value is the placeholder text.

To customize emails for existing policies, follow these steps:

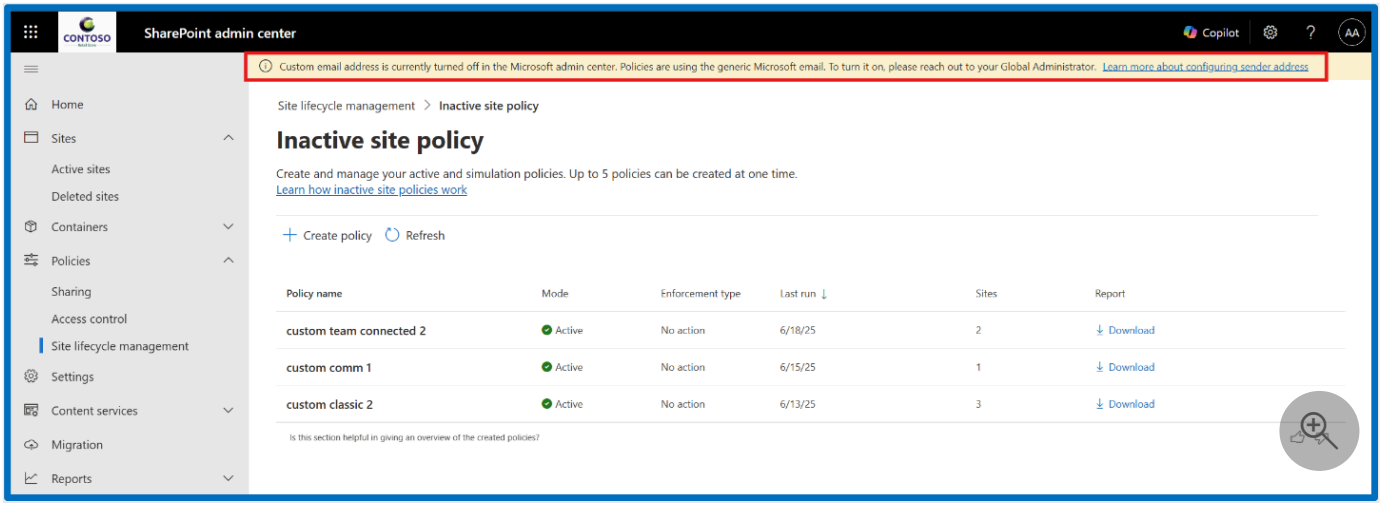
1. Select an existing policy.
2. Select **Edit configuration**.
3. Find the email customization option.

> **Note**
>
> If you don't configure email customization for a policy, the system continues to send default emails from `noreply@sharepoint.com`.

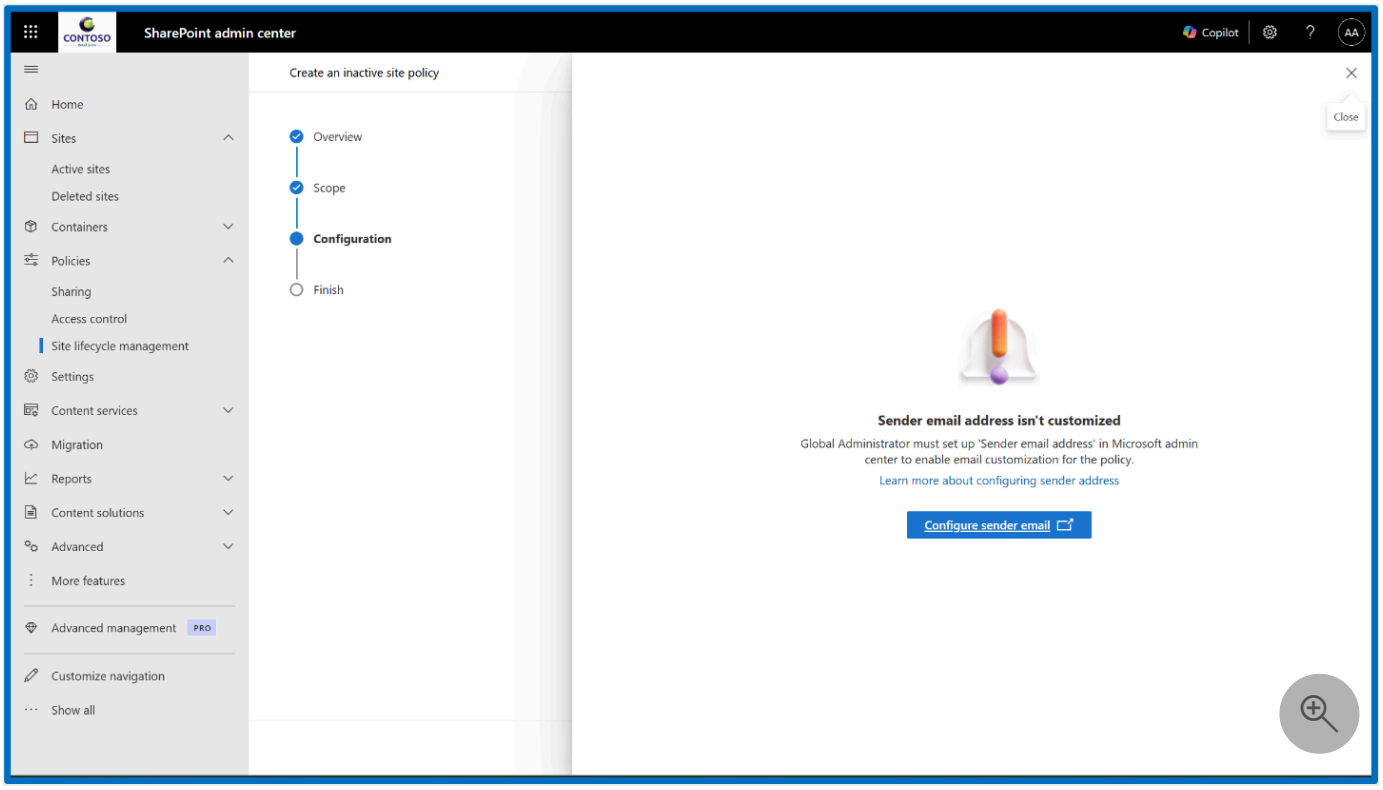
What to do if you can't customize email messages

You can't customize emails if the custom domain setting isn't configured or is turned off.

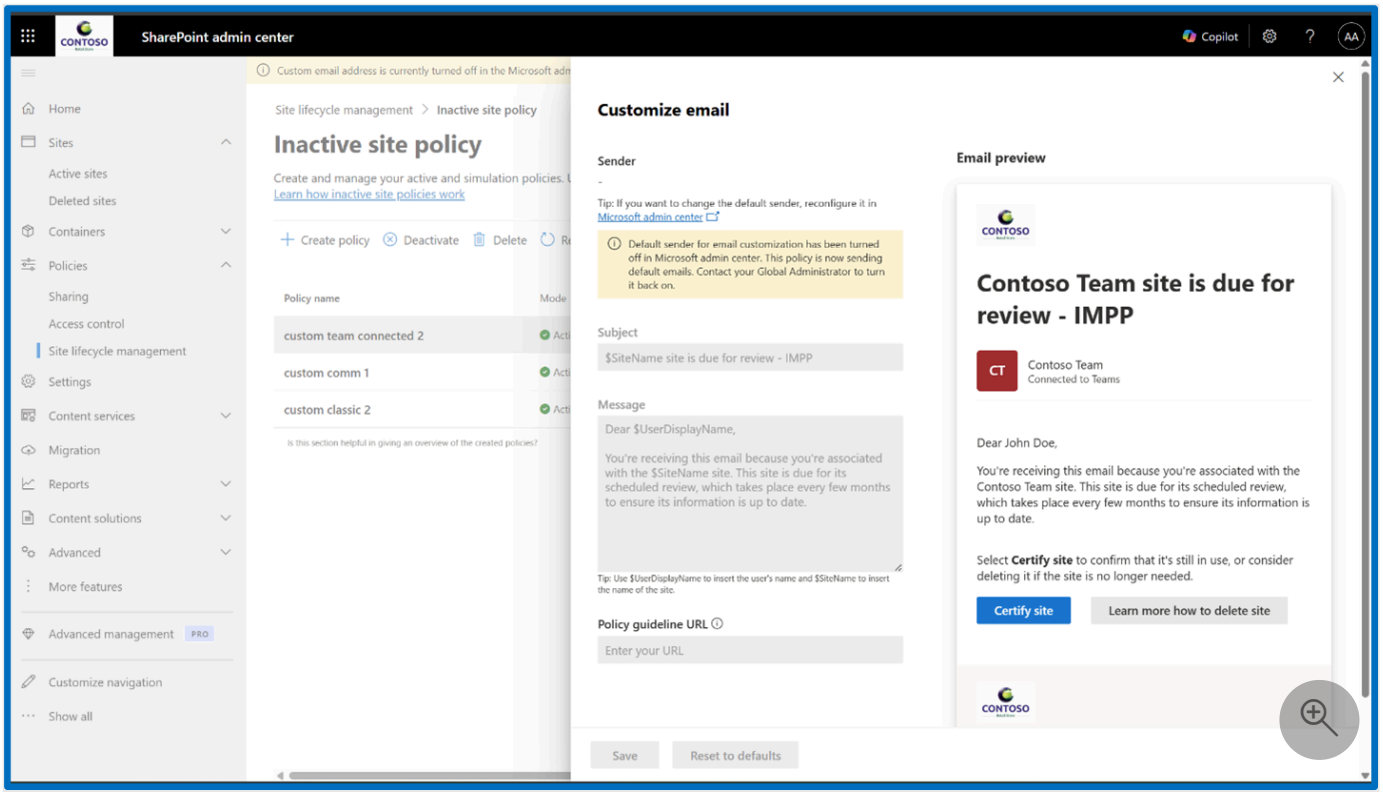
You must configure the **Send email notifications from your domain** setting in the Microsoft 365 admin center before you can customize emails. If you don't configure this setting, you see a warning message at the top of the policy list, as shown in the following image:



You might also see the warning message during the configuration step, as shown in the following screenshot:



If you previously customized emails in one or more policies, but later turn off the **Send email notifications from your domain** setting in the Microsoft 365 admin center, you see the message bar in the policy list, and a warning message in the email customization window, as shown in the following screenshot:



Note

Only someone who has the Global Administrator role can configure domain settings in the Microsoft 365 admin center.

Enforcement actions

The following table summarizes how the inactive site policy behaves based on the selected enforcement action:

Expand table

Enforcement action	Policy behavior
Do nothing	The specified recipients receive monthly notifications for three months. After this period, the policy sends no notifications for the next three months. If the site remains inactive after six months, monthly notifications resume. The policy execution report lists inactive sites as unactioned by the site owner. You can download this report and filter out sites marked as unactioned.
Read-only access	Site owners or site admins receive monthly notifications for three months. If the notification recipients don't mark the site as certified during this period, the site goes into read-only mode.
Archive sites after mandatory read-only period	Site owners or site admins receive monthly notifications for three months. If the notification recipients don't mark the site as certified during this period, then the site goes into a read-only mode for a configurable duration (3, 6, 9, or 12 months). After the configured number of months, the site gets archived through Microsoft 365 Archive. Microsoft 365 Archive must be enabled in the Microsoft 365 admin center.

Important

- Site lifecycle policies use Outlook Actionable Messages to enable site owners or site admins take necessary actions within email.
- For notifications to render properly, ensure Outlook version requirements are met in your organization.
- If you're a US Government cloud customer, see Set up actionable emails for SLM policies in US Government cloud environments (in this article).
- To troubleshoot rendering issues, refer to frequently asked questionnaire.
- When a site owner or site admin selects the site URL in the notification email, this action does **not** count as site activity. The site remains inactive. Additionally, any **read actions** done on the site within one hour of visiting from the email aren't considered

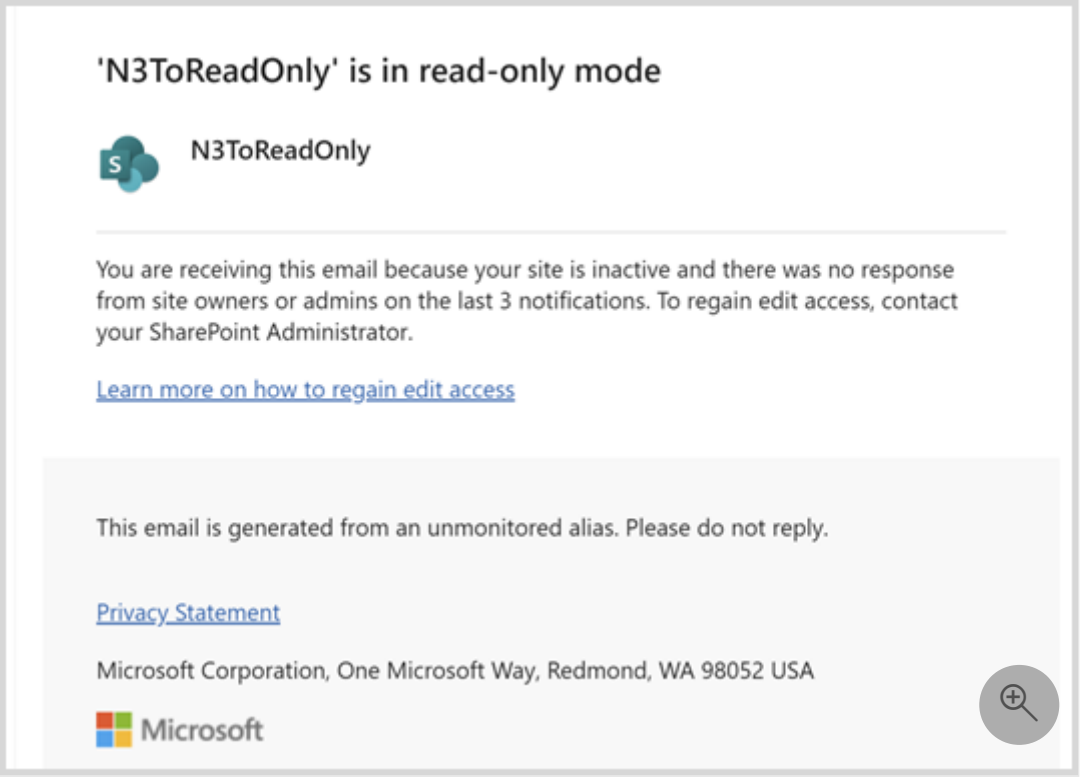
activity. However, any **edits** made to the site count as activity and reset the inactivity status.

> **Tip**
>
> Before creating an inactive site policy, check for any site access restriction policies that could disrupt site attestation by the respective site owner.

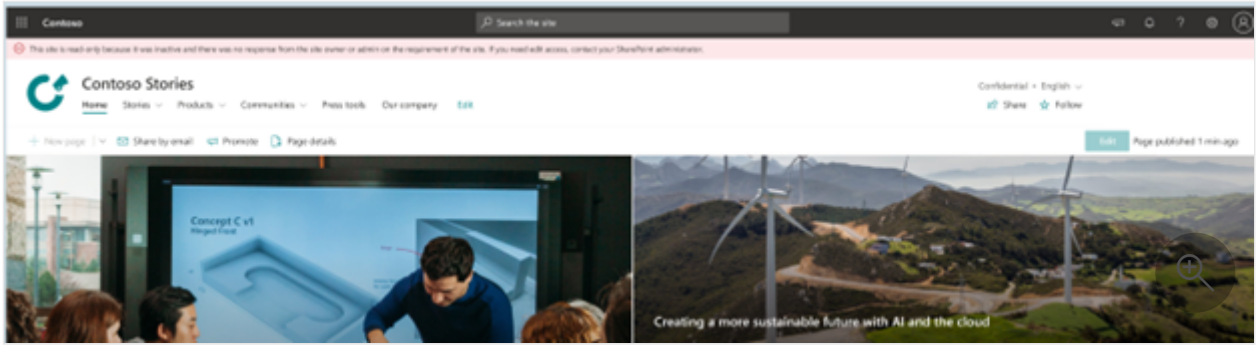
Read-only mode

An inactive site policy configured with the read-only enforcement action sends notifications to inform site owners or site admins when there's no response.

When a site goes into read-only mode, a notification is sent.



If a site is in read-only mode, the following banner is added to the site:



Important points about read-only or locked sites

For sites that are in a read-only or locked state, the following behaviors are expected.

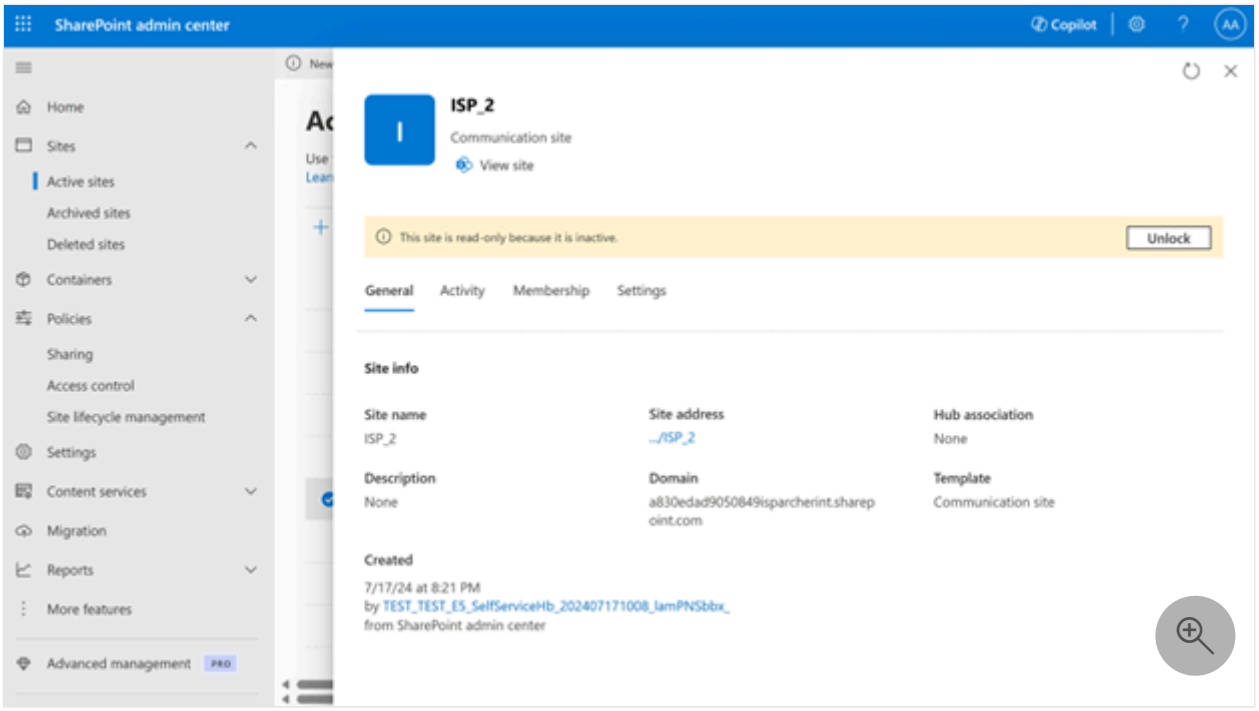
- **Unlocked sites**: Always included in policy scope
- **Read-only sites locked by the same policy type**:
  - Included in scope
  - Report indicates the site was previously actioned by this policy
- **Read-only sites locked by a different policy type**:
  - Excluded from policy scope
  - Another policy already owns and governs this site
- **Read-only sites externally locked** (locked because of reasons other than site lifecycle management):
  - Included in scope
  - External locks do not prevent the site from being evaluated by the policy
- **No-access (fully locked) sites**:
  - Included in scope, but no enforcement action is taken
  - The policy skips action because the site is already in a no access locked state

These are default behaviors that can't be modified through policy configurations.

Remove a site from read-only mode

To remove a site from read-only mode in SharePoint admin center, go to the **Active sites** page, select the site, and then select **Unlock** from the site page panel.

Site owners can't remove a site from read-only mode and must contact the tenant admin to remove read-only mode.



Unarchive a site

To unarchive a site in SharePoint admin center, expand **Sites** and select **Archived sites**. Select the site you want to unarchive and select **Reactivate**.

> **Note**
>
> Only tenant admins can reactivate an archived site.

Reporting

The policy execution report lists sites that are inactive for six months. You can download the report as a .csv file and filter out sites that site owners consider unactioned.

	A	B	C	D	E	F	G	H	I	J	K
1	Site name	URL	Template	Teams	Sensitivity label	Site own	Last site activity (UTC)	Date created	Storage used (GB)	Inactive site status	Action status
2	deleteable_S	https://tenant	Team site (no Microsoft 365 group)	FALSE	Top Secret	[redacted]	7/7/2020	3/15/2019 15:03	0	First notification	Failure
3	deleteable_S	https://tenant	Team site (no Microsoft 365 group)	FALSE		[redacted]	3/14/2019	3/14/2019 17:53	0	First notification	Failure
4	test	https://tenant	Team site (no Microsoft 365 group)	FALSE		[redacted]	6/17/2019	6/17/2019 9:11	0	First notification	Failure
5	deleteable_S	https://tenant	Team site (no Microsoft 365 group)	FALSE		[redacted]	7/19/2019	7/19/2019 12:29	0	First notification	Failure
6	deleteable_S	https://tenant	Team site (no Microsoft 365 group)	FALSE		[redacted]	3/18/2019	3/18/2019 15:29	0	First notification	Failure
7	deleteable_S	https://tenant	Team site (no Microsoft 365 group)	FALSE		[redacted]	3/15/2019	3/15/2019 19:42	0	First notification	Failure
8	deleteable_S	https://tenant	Team site (no Microsoft 365 group)	FALSE		[redacted]	7/19/2019	7/19/2019 11:48	0	First notification	Failure
9	deleteable_S	https://tenant	Team site (no Microsoft 365 group)	FALSE		[redacted]	10/3/2019	10/3/2019 16:56	0	First notification	Failure
10	deleteable_S	https://tenant	Team site (no Microsoft 365 group)	FALSE		[redacted]	3/14/2019	3/14/2019 17:58	0	First notification	Failure

The following table describes the information included in the policy execution report:

Expand table

Column	Definition
Site name	Name of the site
URL	URL of the site
Template	Template of the site
Connected to Teams	Is it a Teams-connected site or not
Sensitivity label	Sensitivity label of the site
Retention policy	Is any retention policy applied to the site or not
Site lock state	State of site access **before** the policy runs (Unlock/Read-Only/No access)
Last activity date (UTC)	Date of last activity detected by inactive site policy across SharePoint site and connected workloads (Exchange, Viva Engage (formerly Yammer), or Teams)
Site creation date (UTC)	Date when the site was created
Storage used (GB)	Storage consumed by the site
Number of site owners	Total count of site owners for the site
Email address of site owners	Email addresses of all site owners
Number of site admins	Total count of site admins for the site
Email address of site admins	Email addresses of all site admins
Action status	Status of the site (First, second, or third notification sent; Site in read-only mode; Site archived; Action taken by another policy: read-only, archive, or notified by another policy)
Total notifications count	Total notifications sent so far by any policy under the same policy template
Action taken on (UTC)	Date on which the enforcement action was taken (date when site was archived or put in read-only mode)
Duration in read-only	Number of days the site is in the enforced read-only state

Overlapping policies of same policy type

When more than one policy of the same policy type includes the same site, SharePoint helps reduce duplicate notifications by using stored site-level policy history.

If a notification was sent within the last 30 days from any policy of that type, and the site remains uncertified, no further notifications are sent and the policy execution report shows the site's status as "Notified by another policy."

For example, if a site is covered by two different inactive site policies and receives a notification email from the first policy, the second policy doesn't send additional notifications within the next 30 days if the site remains uncertified.

We recommend that policies of the same type don't have overlapping scopes. If sites fall under multiple policies of the same type, notification schedules and enforcement actions can become difficult to predict.

Overlapping policies of different types

Policies of different types operate independently for notification purposes. Notification history is tracked separately for each policy type.

For example, if a site falls within the scope of both a Site Ownership policy and an Inactive site policy, site owners might receive notifications from both policies when the respective policy conditions are met.

Enforcement actions are evaluated independently by each policy. If a policy applies an enforcement action that changes the site's state, the site might no longer qualify for processing by other policies:

- If a policy places the site in a read-only (locked) state, the site is no longer included in the scope of other policies.
- If a policy archives the site, the site reaches a terminal state and is no longer considered for enforcement by other policies.

When multiple policy types target the same site, the enforcement action from the policy whose conditions are satisfied first is applied first.

Disabling or deleting a policy

Disabling or deleting a policy stops future activities from that policy, including notifications and enforcement actions. It doesn't automatically reverse previously applied actions.

Notification history is maintained at the site level separately for each policy type. As a result, disabling or deleting one policy doesn't affect notification history associated with other policy types that continue to target the site.

For policies of the same type, stored notification history (including notification count and last notification date) is retained even after a policy is disabled or deleted. This history naturally resets after the site has been absent from the scope of that policy type for 90 days.

If notification history needs to be reset sooner, contact Microsoft Support to determine whether the stored notification state can be cleared.

> **Important**
>
> To ensure predictable behavior, avoid creating overlapping policies of the same type that target the same sites. While SharePoint suppresses duplicate notifications where possible, overlapping policies can make notification timing and enforcement outcomes harder to interpret.

Set up actionable emails for SLM policies in US Government cloud environments

In US Government Cloud (GCC High and DoD) environments, a tenant administrator must complete an extra, one-time setup for SharePoint site lifecycle management (SLM) policies to use actionable messages. This step helps ensure that policy notification emails display and function correctly. For example, site admins and site owners can take actions directly from email.

Unlike other commercial cloud environments, GCC High and DoD tenants require explicit administrator approval of the actionable message provider before it can send interactive email messages. Without this approval, SLM policy emails are delivered, but action buttons don't function as expected.

> **Important**
>
> You must be a Global Administrator or Exchange Administrator in the tenant to set up actionable messages.

Approve the SLM actionable message provider

1. Go to the Outlook Actionable Messages – Connectors admin portal for GCCH or DoD and sign in.
2. In the **Provider Status** filter, select **Approved by Microsoft – Pending Your Approval**.
3. Locate the provider named `InactiveSiteOAMProviderGCCH`.
4. Select the provider, and then select **Approve**.

After you approve the provider, the SLM policy notifications send actionable messages.

> **Note**
>
> This approval applies only to SLM policy notifications. Other applications or services that use actionable messages might require separate approval.

Ensure actionable messages are enabled for the tenant

Site lifecycle management policies use Outlook actionable messages to enable site owners or site administrators to take necessary actions by using links within email messages.

- For notifications to render properly, make sure your organization meets the Outlook version requirements.
- To troubleshoot rendering problems, see frequently asked questions.

Troubleshooting actionable messages

If actionable messages don't work as expected, try these steps:

- Make sure that the `InactiveSiteOAMProviderGCCH` provider is in an approved state.
- Allow sufficient time. It can take up to 24 hours for changes to propagate.

Related articles

- Microsoft 365 group expiration policy
- Restore deleted sites
- Overview of Microsoft 365 Archive

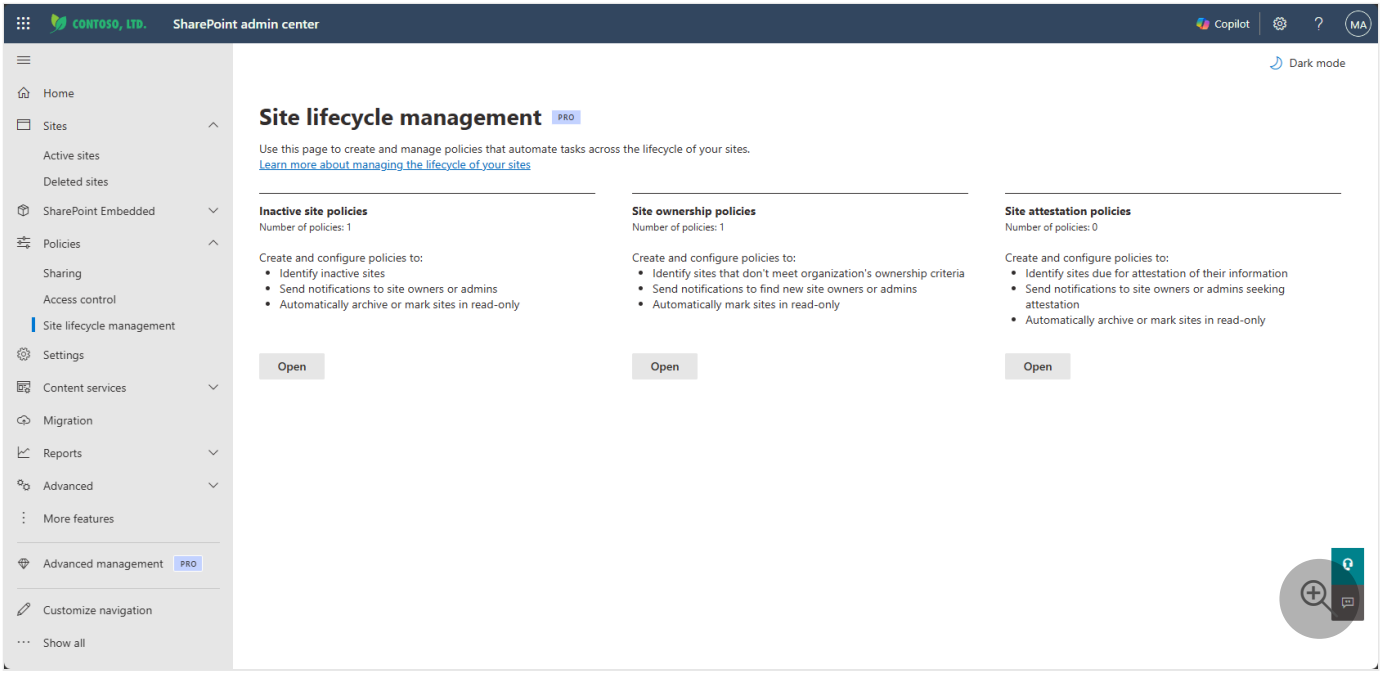
Last updated on 08/19/2026

Request recurring site attestations for SharePoint sites

Site attestation policies help you periodically verify that SharePoint sites continue to meet your organization's governance requirements. These policies request reviews from site owners or site administrators, who confirm whether a site is still needed and whether its ownership, membership, permissions, and sharing settings remain appropriate.

You can configure site attestation policies to send recurring review requests and apply enforcement actions when required reviews aren't completed.

For an overview of site lifecycle management policies, see SharePoint site lifecycle management.



This article describes how to create a site attestation policy with notifications and enforcement actions.

Requirements for a site attestation policy

See SharePoint Advanced Management prerequisites.

How a site attestation policy works

When a site attestation policy runs, SharePoint identifies sites that are due for review based on the policy configuration.

The policy sends attestation requests to designated recipients, such as site owners or site administrators. Recipients review site information and confirm that the site remains necessary and appropriately configured.

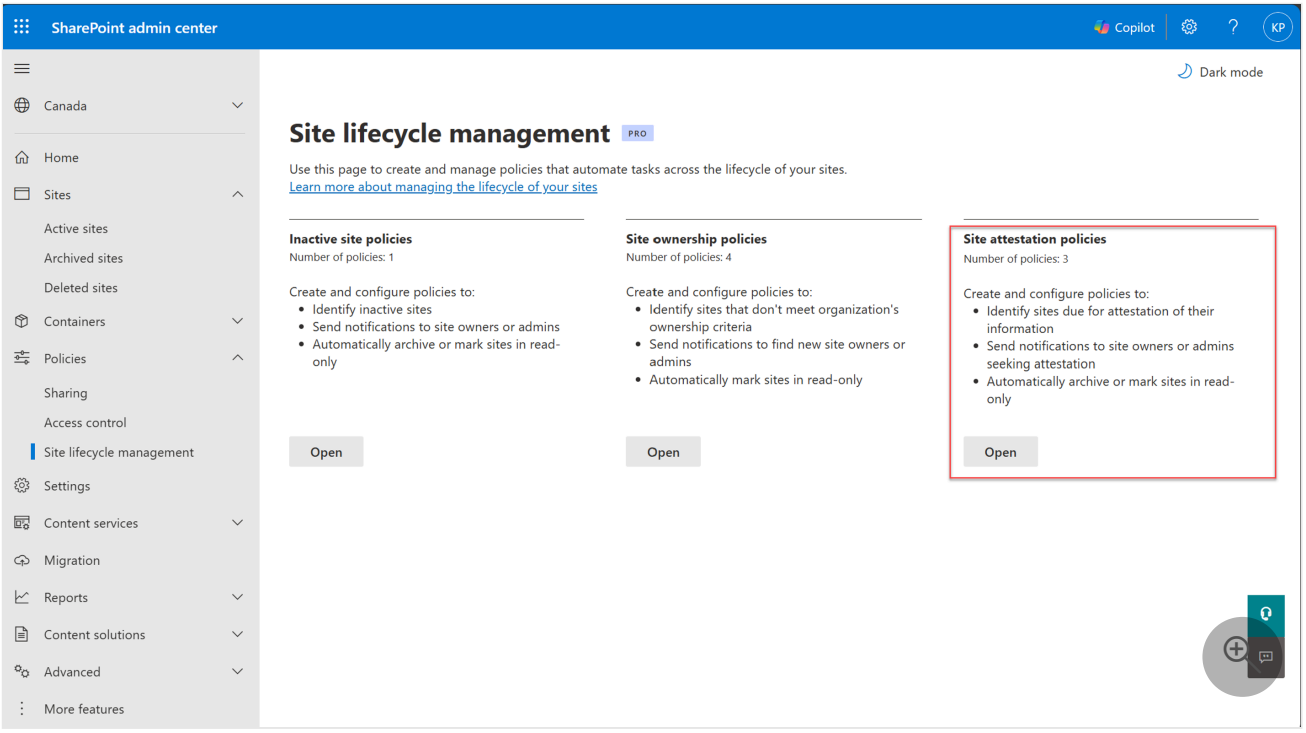
If a review isn't completed after the configured notification cycle, the policy can apply an enforcement action, depending on the policy settings.

Each policy run generates a report that administrators can use to track attestation status and monitor policy compliance.

Create a site attestation policy

1. As a SharePoint administrator, go to the SharePoint admin center and sign in.

2. In the navigation pane, expand **Policies**, and then select **Site lifecycle management**.



3. Under **Site attestation policies**, select **Open**. Then select **Create a policy**.

4. On the **Overview** page of **Manage site attestation**, review the information, and then select **Next**. Then proceed to the next section.

5. To define the scope of a site attestation policy, on the **Set policy scope** page, select one of the following options:

   - **Upload a CSV file with a list of up to 10,000 URLs**; or
   - **Select sites at scale**

For more information, see the following sections in this article:

- About the scope of site attestation policies
- Uploading a CSV file with the list of sites
- Selecting sites at scale

6. On the **Configure policy** step, specify the following options:

   - Choose how often you want the sites to be attested (3 months, 6 months, and 12 months).
   - Identify who is responsible for attesting the site (site owners, site admins, or both).
   - Exclude site owners or admins from receiving requests.
   - Specify what action the policy should take after three notifications.

   Keep the following points in mind:

   - Recently attested sites are skipped.
   - Newly created sites are skipped (because a grace period applies).
   - Only sites that are both old enough and due for reattestation are included.

   For more information about your policy options, see About site attestation policy configuration settings (in this article).

7. On the **Finish** step, specify whether to test your policy or activate it immediately.

   - Give your policy a name and description.
   - Under **Policy mode**, select either the **Simulation** or **Active** mode. For more information, see About policy modes (in this article).

About the scope of site attestation policies

> **Note**
>
> A policy scopes a site for attestation only if **both** of the following conditions are true:
>
> - The site's creation date is older than the attestation threshold
> - The site's last attestation date is also older than the same threshold
>
> The attestation threshold is calculated using the policy run date minus the attestation period (how often you want sites to be attested, configured by SharePoint administrators). If either condition isn't met, the site is excluded from attestation for that run.

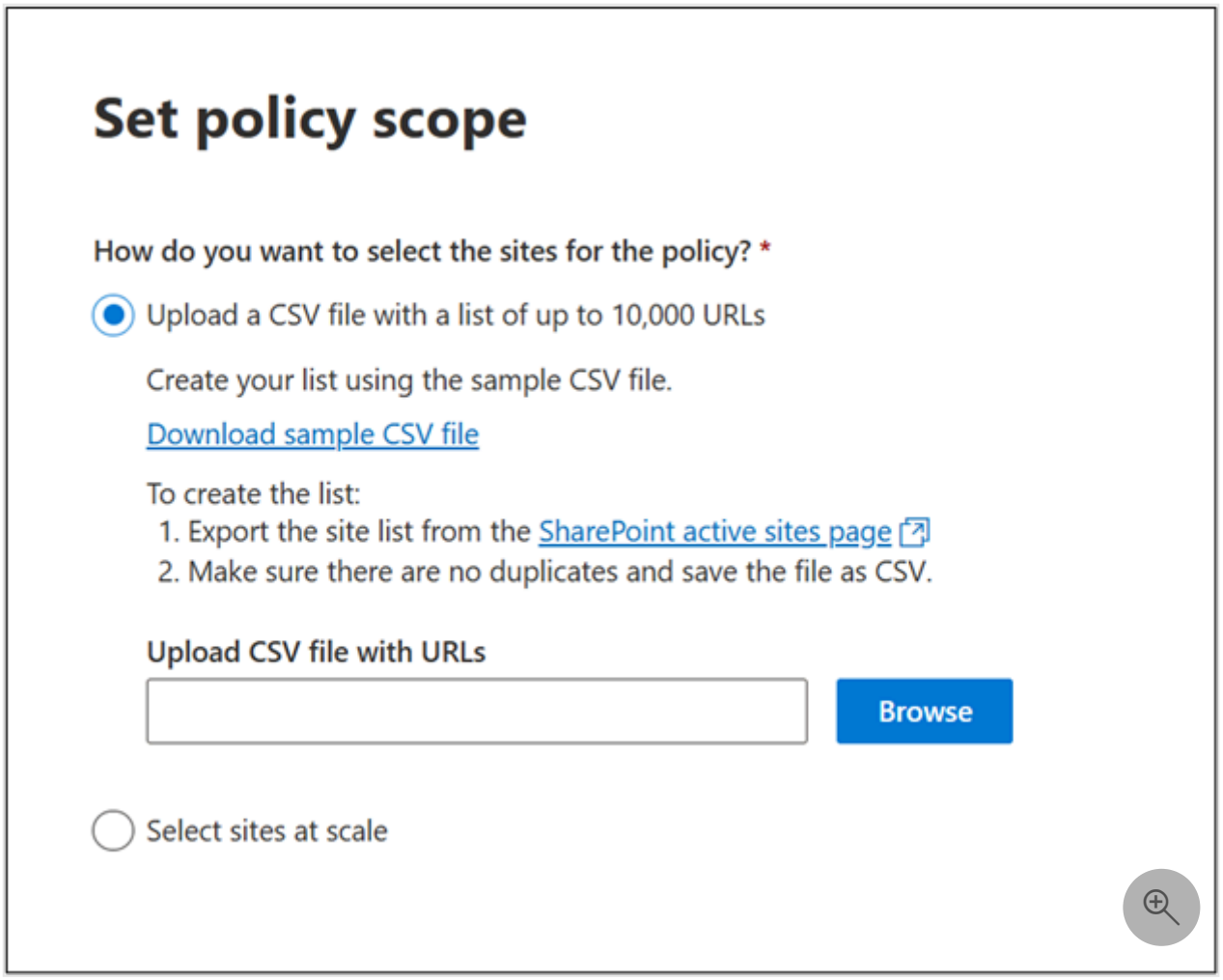
You can create site lifecycle policies with different scopes based on your organization's requirements. Choose the sites to include in the policy based on:

- Site templates
- Creation sources
- Sensitivity labels
- Whether to include sites under retention policies and retention holds

To exclude specific sites, add the site URLs of up to 100 sites in the **Exclude sites** section while configuring the policy.

Uploading a CSV file with the list of sites

If you select **Upload a CSV file with a list of up to 10,000 URLs**, you can upload a list of site URLs for the policy.



Tip

- You can export the site list from the SharePoint active sites page.
- Ensure that the CSV file uses the same format as the sample CSV file and has no duplicate URLs. Also, make sure the URLs are valid and complete.
- Ensure the URLs listed in the CSV file belong to your tenant's domain.

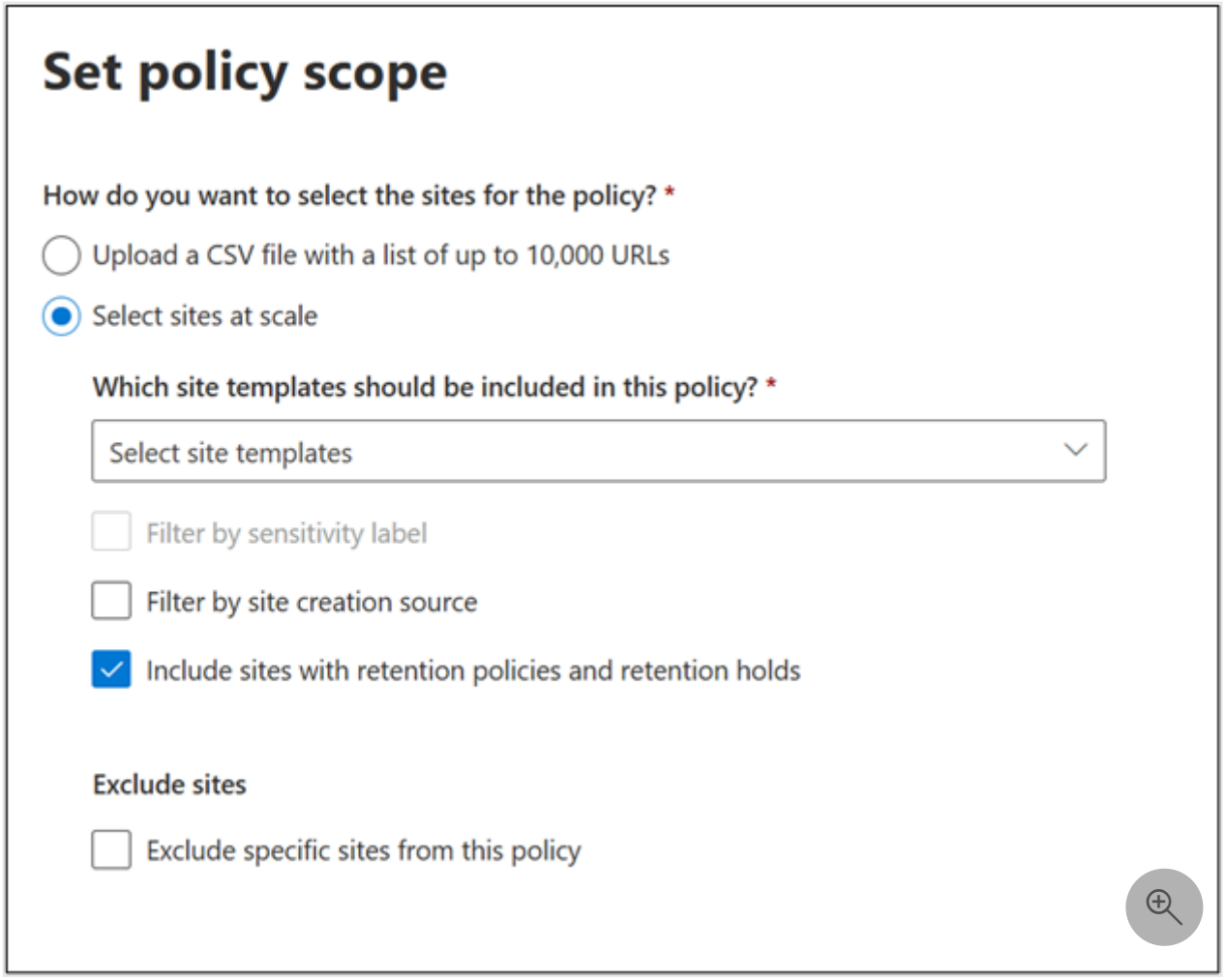
Selecting sites at scale

If you select **Select sites at scale**, you can choose site templates to include in this policy, and then filter them by:

- Sensitivity label
- Site creation source

You can also choose whether to:

- Include sites with retention policies and retention holds
- Exclude specific sites from this policy



Selecting site template types

Select site template types from the following list:

- All sites
- Classic sites
- Communication sites
- Group connected sites without teams
- Team sites without Microsoft 365 group
- Teams-connected sites

Filtering sites by sensitivity labels

Set policy scope by filtering sites by their sensitivity labels.

> **Note**
>
> If your tenant doesn't use sensitivity labels, this option is unavailable.

Filtering sites by creation source

Filter sites for the policy scope by site creation source:

- SharePoint Home
- SharePoint admin center
- PowerShell
- PnP
- Teams

Include sites with retention policies and retention holds

The include or exclude option for sites with retention policies and holds applies only to sites that are governed by Microsoft Purview retention policies and labels.

This setting doesn't impact the inclusion or exclusion of sites that are in read-only or locked states.

For sites that are in a read-only or locked state, the following behaviors are expected:

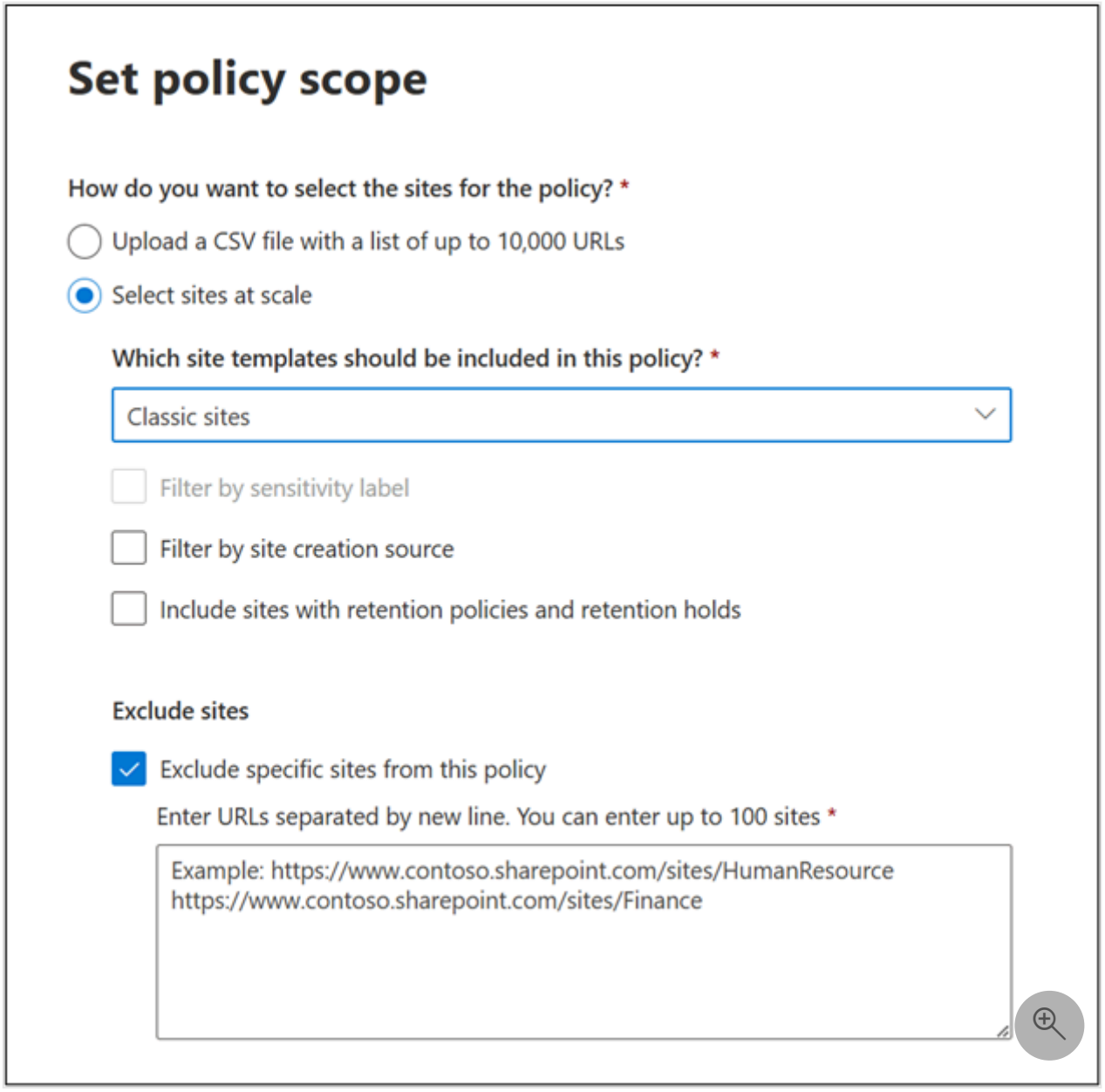
- **Unlocked sites**: Always included in policy scope
- **Read-only sites locked by the same policy type**:
  - Included in scope
  - Report indicates the site was previously actioned by this policy
- **Read-only sites locked by a different policy type**:
  - Excluded from policy scope
  - Another policy already owns and governs this site
- **Read-only sites externally locked** (locked because of reasons other than site lifecycle management):
  - Included in scope
  - External locks don't prevent the policy from evaluating the site
- **No access (fully locked) sites**:
  - Included in scope, but the policy takes no enforcement action
  - The policy skips action because the site is already in a no access locked state

You can't change these default behaviors through policy configuration options.

About site attestation policy configuration settings

Excluding specific sites from the policy

Enter up to 100 sites that you want to exclude from the site attestation policy. Be sure to separate each URL by new lines.



After setting the policy's scope, select **Next**, and then proceed to the next section.

Excluding site owners or admins from receiving requests

You can exclude specific users, Microsoft 365 Groups, or security groups from receiving site lifecycle management requests and notifications, even if they're site owners or site admins for sites that are included in a policy.

Key behaviors:

- Exclusions are used only to determine notification recipients.

- Excluding a user or group doesn't change site permissions or ownership, and doesn't exclude the site from lifecycle policy evaluation
- Sites continue to be evaluated by the policy as usual.

Limits:

- You can add up to 100 entries to the exclusion list.
- Each entry can be an individual user, a Microsoft 365 Group, or a security group
- The 100-entry limit applies to the number of entries, not the number of users within a group. For example, a group with more than 100 members counts as one entry.

Group exclusion behavior (important):

- When a group is added to the exclusion list for a policy, that group is excluded from notifications only when the group is directly added to the site or is a nested group within other groups that are directly added to the site.
- A member of an excluded group might still receive a notification if they're directly added to the site or are part of some other group that is directly added to the site.

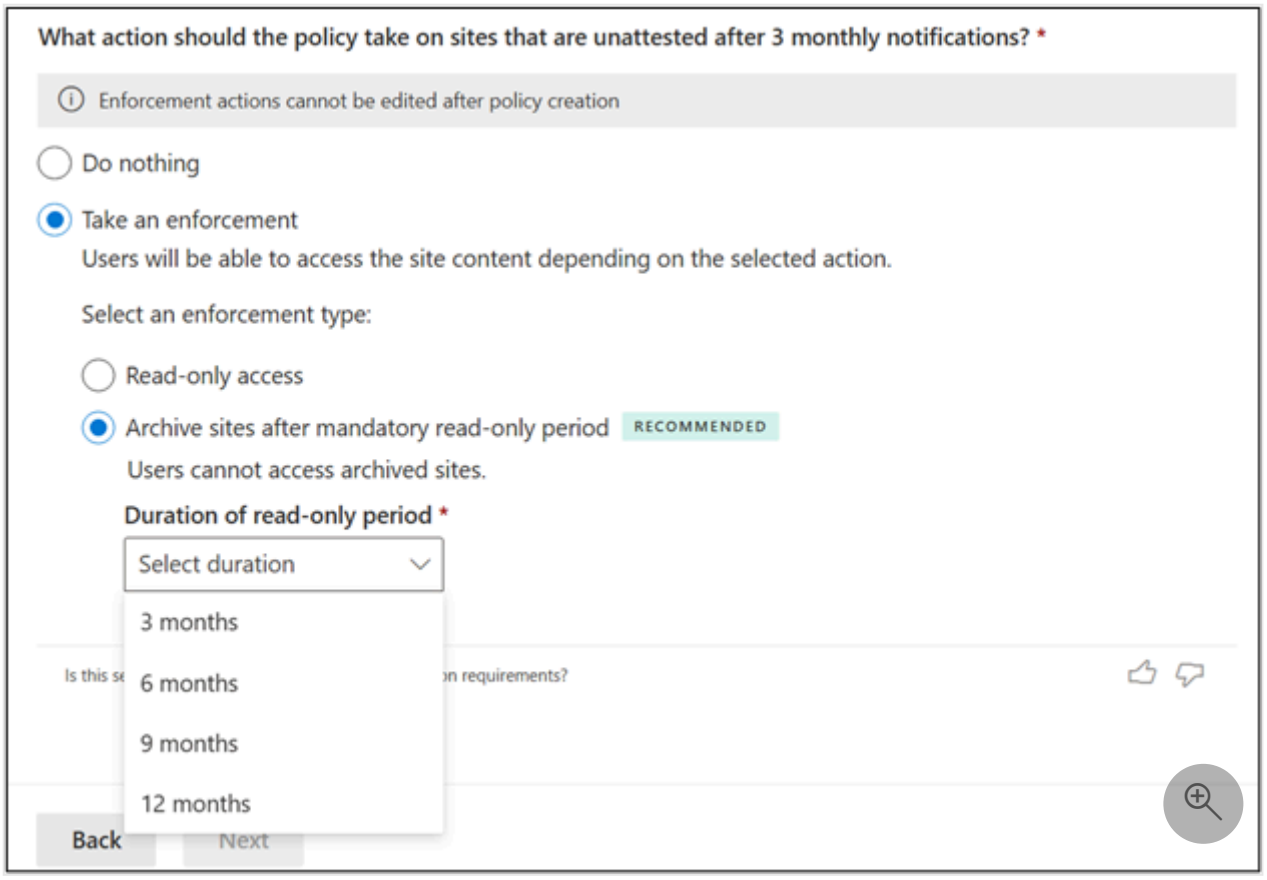
Actions to take on unattested sites after three notifications

For sites that are unattested after three monthly notifications, you can choose to either do nothing or take one of the following enforcement actions. The following table summarizes how the inactive site policy behaves for each selected enforcement action:

Expand table

Enforcement action	Policy behavior
Do nothing	Site owners or site admins receive monthly notifications for three months. After this period, no notifications are sent for the next three months. If the site remains unattested after six months, monthly notifications resume. The policy execution report lists unattested sites as unactioned by the site owner. You can download this report and filter out sites marked as unactioned.
Read-only access	Site owners or site admins receive monthly notifications for three months. If the notification recipients don't mark the site as attested during this period, the site goes into read-only mode.
Archive sites after mandatory read-only period	Site owners or site admins receive monthly notifications for three months. If the notification recipients don't mark the site as attested during this period, then the site goes into a read-only mode for a configurable duration (3, 6, 9, or 12 months). After the configured number of months, the site gets archived through Microsoft 365

Enforcement action	Policy behavior
	Archive. Archival is subject to the tenant enabling Microsoft 365 Archive in the Microsoft 365 admin center.



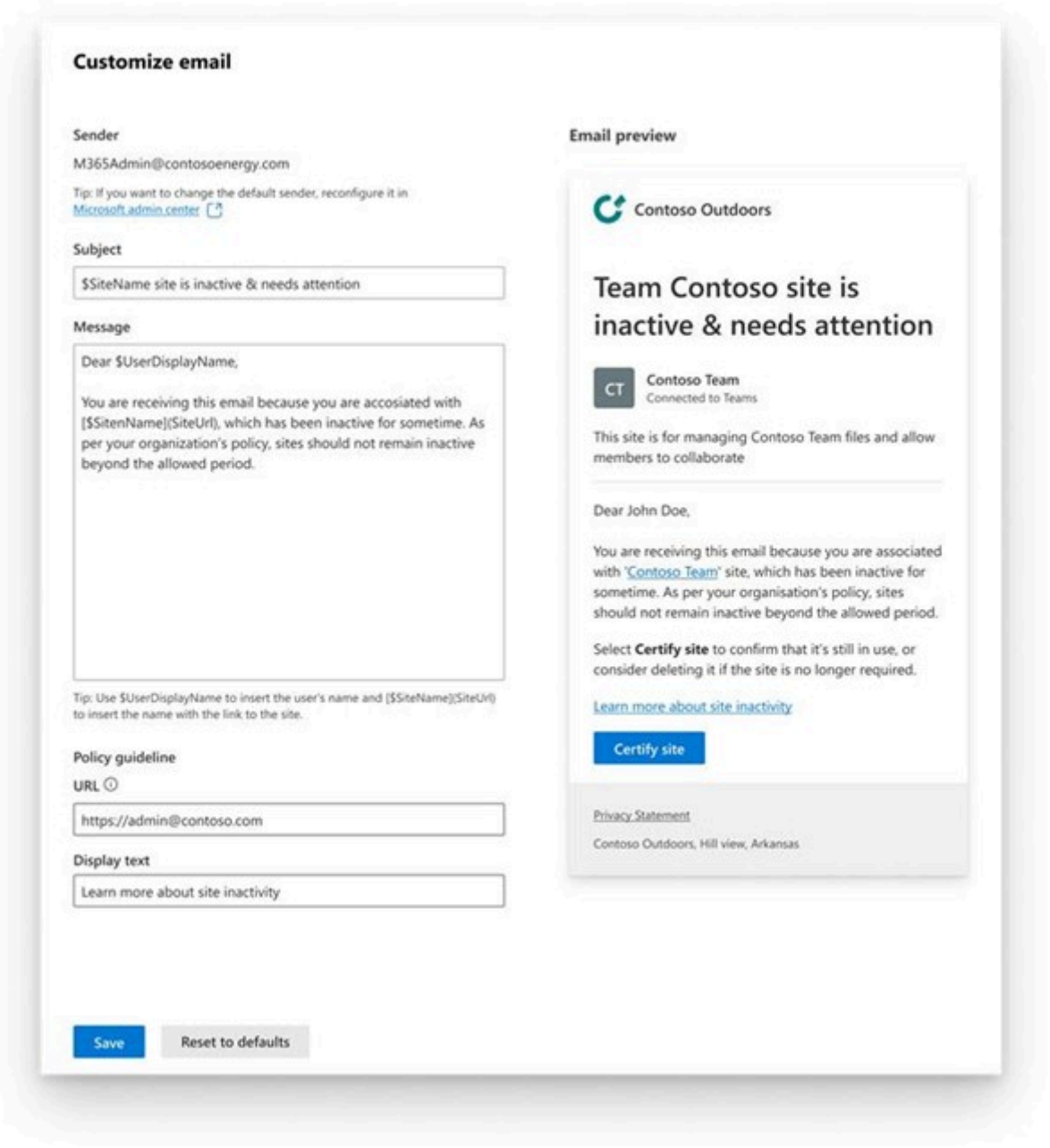
> **Note**
>
> If you configure the policy to take an enforcement action:
>
> - The notifications stop after the policy action succeeds.
> - The site and its status are included in the monthly report.

Customizing email notifications

Administrators can customize the email messages that site lifecycle management policies send when site issues require attention.

Customizing email content helps improve the read-through rate of the emails, which effectively improves response efficiency and contributes to better governance across the tenant.

You can customize emails in the configure step. When you select **Customize email to be sent**, the customization window opens as shown in the following screenshot:



The following table describes the sections you can customize:

Expand table

Customizable section	Description
Sender	You must configure a custom domain in the Microsoft 365 admin center before you can use the email customization feature. For more information, see Choose which domain to use for your email.
Subject (up to 100 characters)	Use `$UserDisplayName` to insert the user's name and `$SiteName` to insert the name of the site.
Message (up to 500 characters)	Use `$UserDisplayName` to insert the user's name, `$SiteName` to insert the name of the site, and `$SiteUrl` to insert the URL of the site.

Customizable section	Description
Policy guideline URL	Only valid HTTP links are allowed.
Policy guideline description text	The default value is the placeholder text.

To customize emails for existing policies, follow these steps:

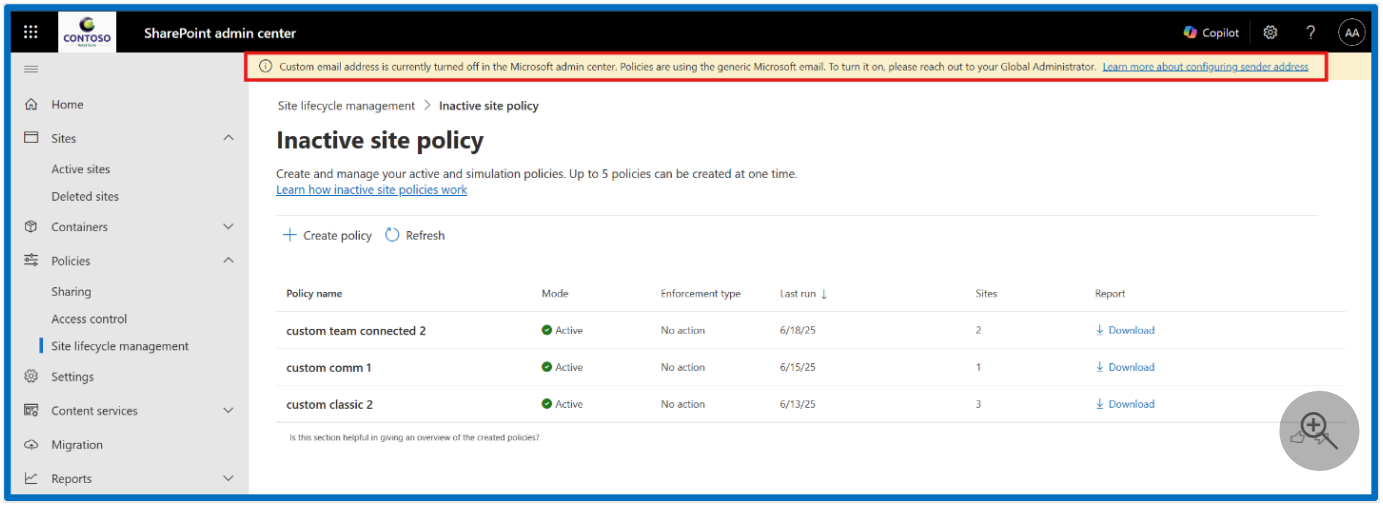
1. Select an existing policy.
2. Select **Edit configuration**.
3. Find the email customization option.

> **Note**
>
> If you don't configure email customization for a policy, the system continues to send default emails from `noreply@sharepoint.com`.

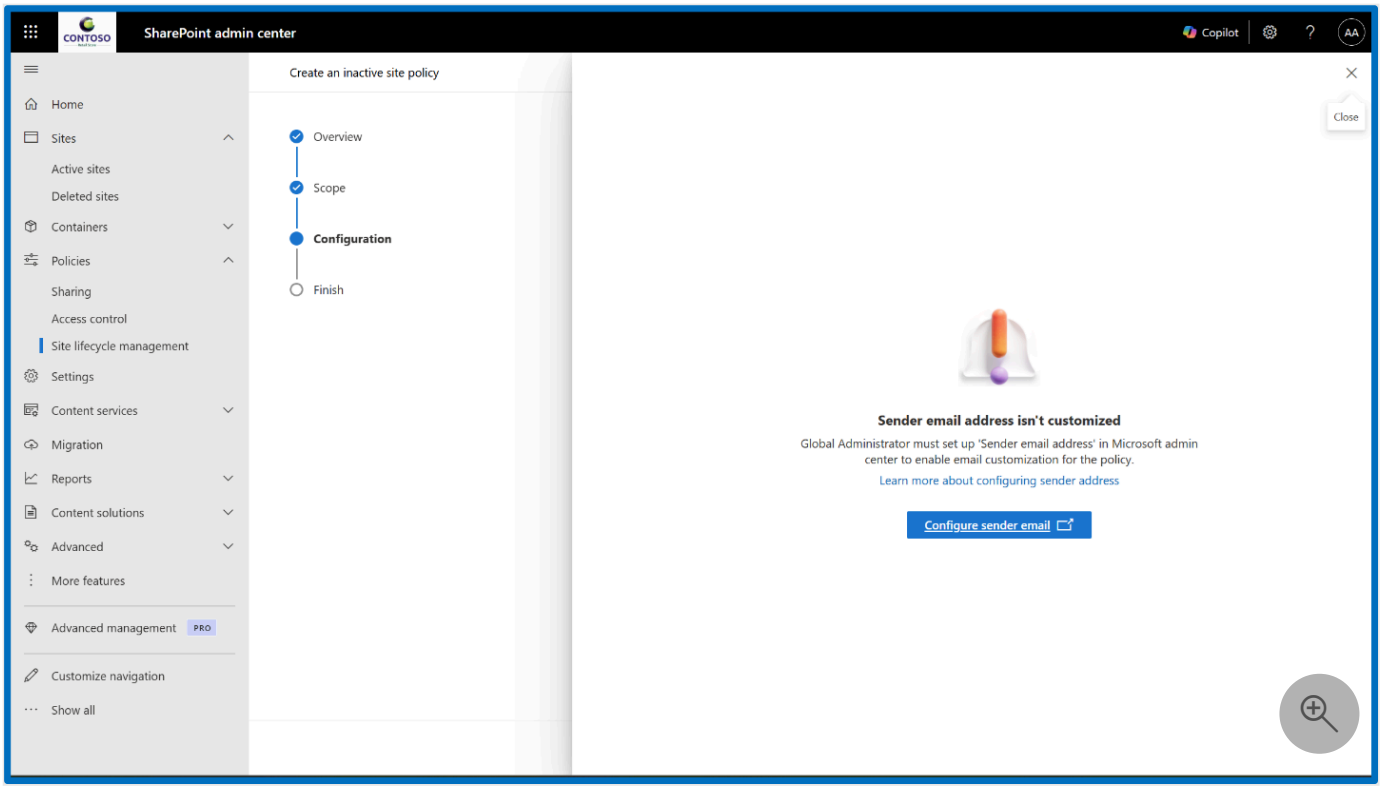
What to do if you can't customize email messages

You can't customize emails if the custom domain setting isn't configured or is turned off.

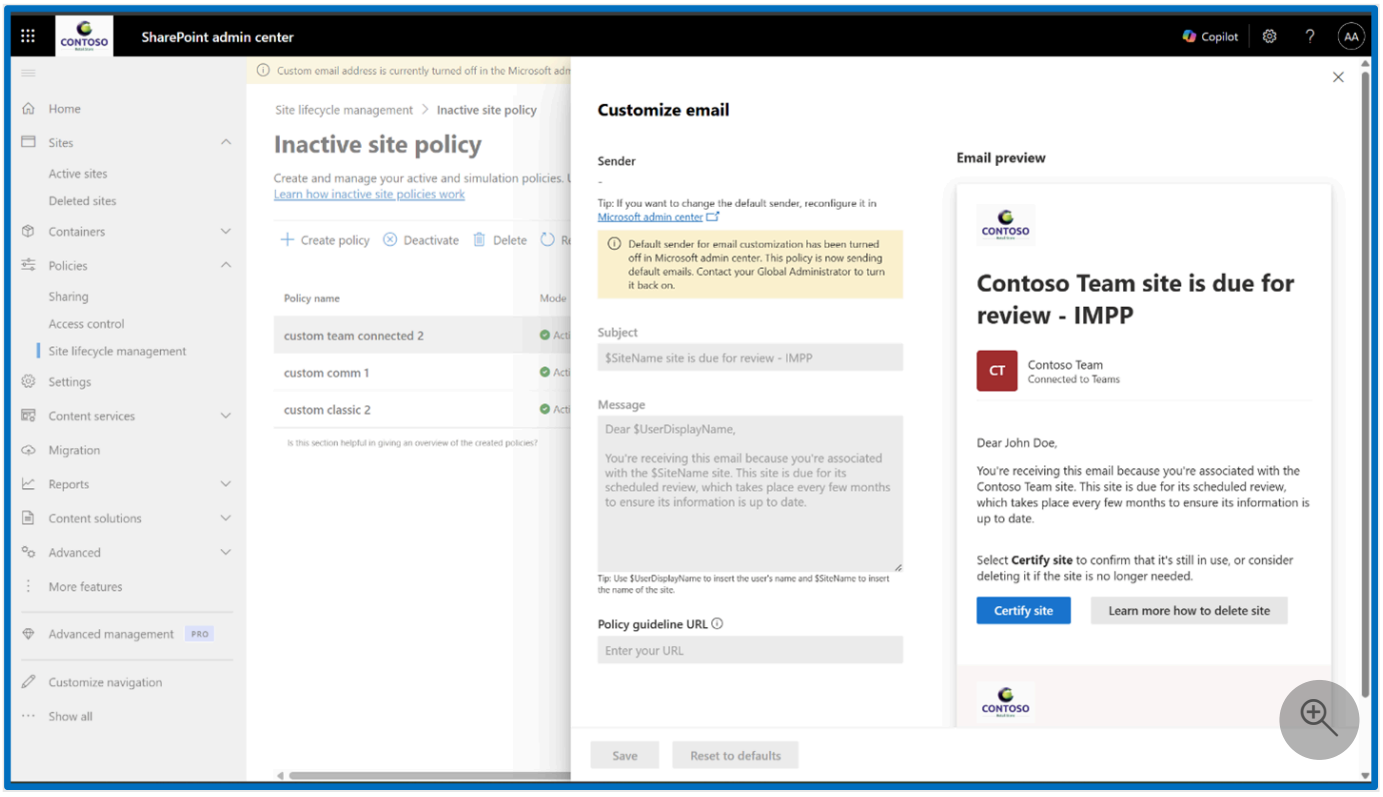
You must configure the **Send email notifications from your domain** setting in the Microsoft 365 admin center before you can customize emails. If you don't configure this setting, you see a warning message at the top of the policy list, as shown in the following image:



You might also see the warning message during the configuration step, as shown in the following screenshot:



If you previously customized emails in one or more policies, but later turn off the **Send email notifications from your domain** setting in the Microsoft 365 admin center, you see the message bar in the policy list, and a warning message in the email customization window, as shown in the following screenshot:



Note

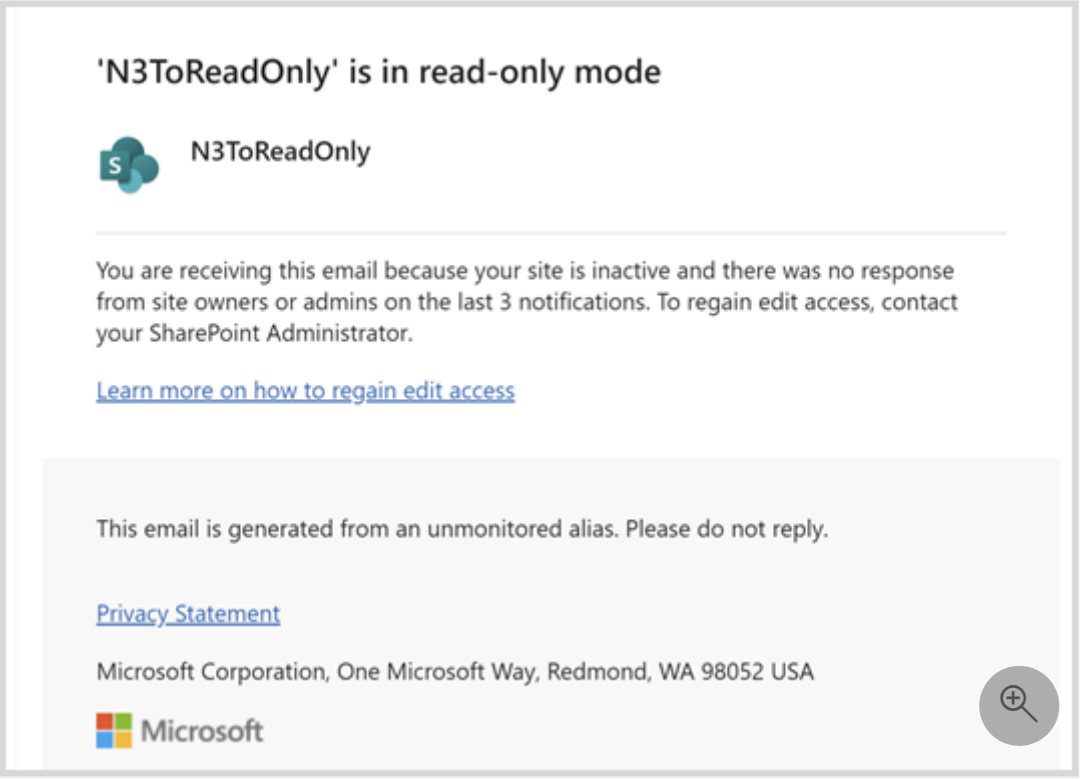
Only someone who has the Global Administrator role can configure domain settings in the Microsoft 365 admin center.

After configuring the policy settings, select **Next** to finish your policy. Name the policy, add a description (optional), and select a policy mode.

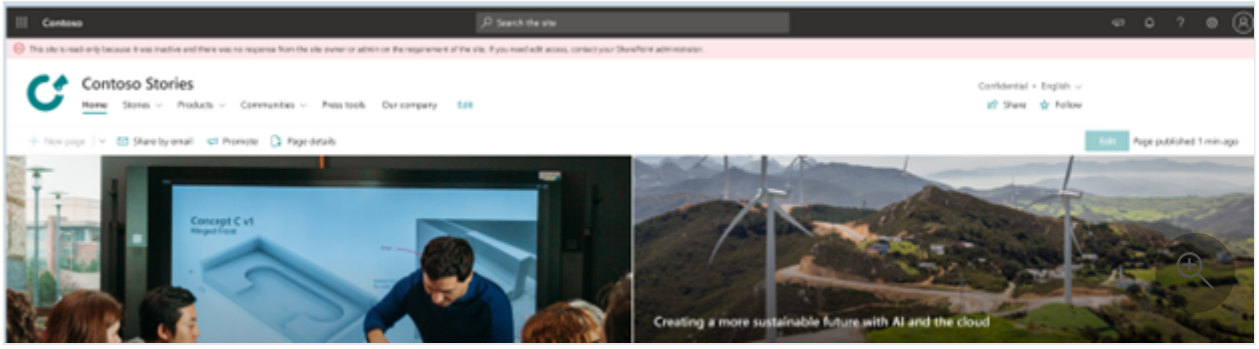
Select **Finish**. You can now view and manage your policy from the **Site lifecycle management** > **Site attestation policy** dashboard.

Read-only mode

When you configure an unattested site policy with the read-only enforcement action, it sends extra notifications to inform site owners or site admins that the site goes into read-only mode.



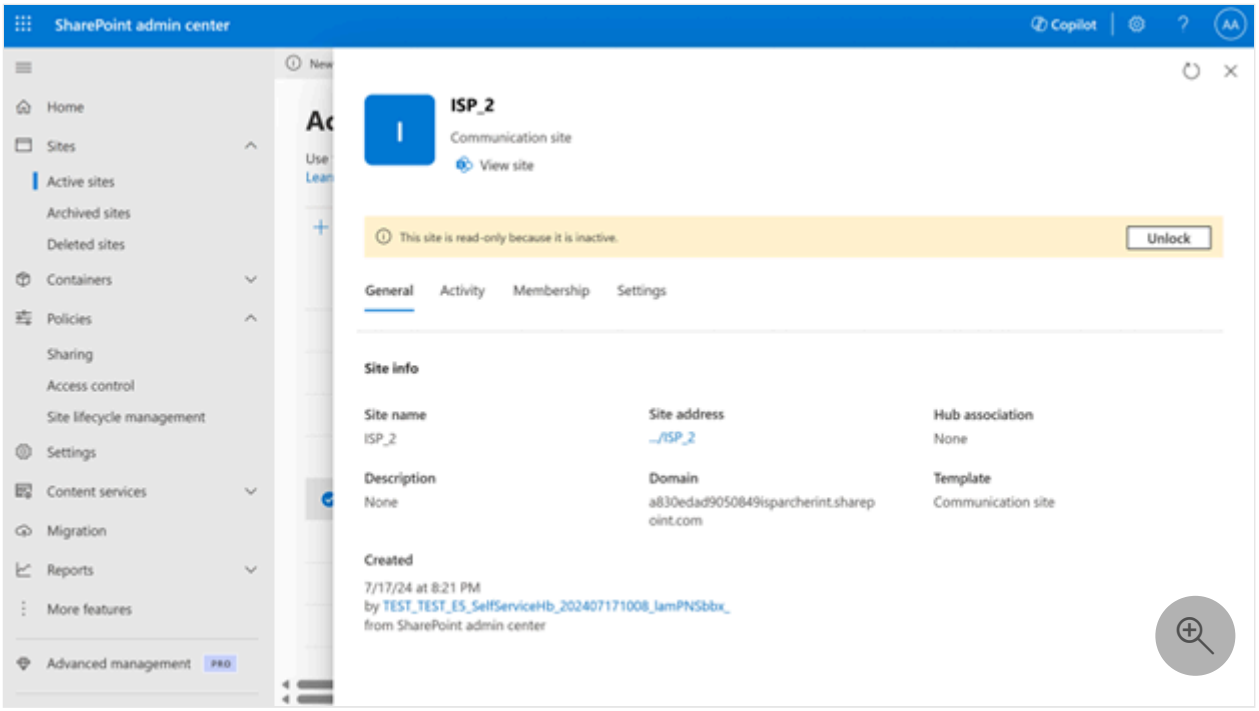
When the site is in read-only mode, the following banner appears on the site:



Removing sites from read-only mode

To remove a site from read-only mode in the SharePoint admin center, go to the **Active sites** page, select the site, and then select **Unlock** from the site page panel.

Site owners can't remove a site from read-only mode. They must contact the tenant admin to remove read-only mode.



Unarchiving a site

To unarchive a site in SharePoint admin center, expand **Sites** and select **Archived sites**. Select the site you want to unarchive and select **Reactivate**.

> **Note**
>
> Only tenant admins can reactivate an archived site.

Overlapping policies of same policy type

When more than one policy of the same policy type includes the same site, SharePoint helps reduce duplicate notifications by using stored site-level policy history.

If a notification was sent within the last 30 days from any policy of that type, and the site remains uncertified, no further notifications are sent and the policy execution report shows the site's status as "Notified by another policy."

For example, if a site is covered by two different inactive site policies and receives a notification email from the first policy, the second policy doesn't send additional notifications within the next 30 days if the site remains uncertified.

We recommend that policies of the same type don't have overlapping scopes. If sites fall under multiple policies of the same type, notification schedules and enforcement actions can become difficult to predict.

Overlapping policies of different types

Policies of different types operate independently for notification purposes. Notification history is tracked separately for each policy type.

For example, if a site falls within the scope of both a Site Ownership policy and an Inactive site policy, site owners may receive notifications from both policies when the respective policy conditions are met.

Enforcement actions are evaluated independently by each policy. If a policy applies an enforcement action that changes the site's state, the site may no longer qualify for processing by other policies:

- If a policy places the site in a read-only (locked) state, the site is no longer included in the scope of other policies.
- If a policy archives the site, the site reaches a terminal state and is no longer considered for enforcement by other policies.

When multiple policy types target the same site, the enforcement action from the policy whose conditions are satisfied first is applied first.

Disabling or deleting a policy

Disabling or deleting a policy stops future activities from that policy, including notifications and enforcement actions. It doesn't automatically reverse previously applied actions.

Notification history is maintained at the site level separately for each policy type. As a result, disabling or deleting one policy doesn't affect notification history associated with other policy types that continue to target the site.

For policies of the same type, stored notification history (including notification count and last notification date) is retained even after a policy is disabled or deleted. This history naturally resets after the site has been absent from the scope of that policy type for 90 days.

If notification history needs to be reset sooner, contact Microsoft Support to determine whether the stored notification state can be cleared.

> **Important**
>
> To ensure predictable behavior, avoid creating overlapping policies of the same type that target the same sites. While SharePoint suppresses duplicate notifications where possible, overlapping policies can make notification timing and enforcement outcomes harder to interpret.

About policy modes

Policy modes

Site ownership policies support two operating modes:

- **Simulation mode** – Runs the policy once and generates a report without ongoing enforcement.
- **Active mode** – Runs monthly, generates reports, sends notifications, and can apply enforcement actions based on policy configuration.

> **Note**
>
> Site lifecycle policies in simulation mode are now available in GCCH and DoD environments as of November 17, 2025.

For more information about policy modes across site lifecycle management policies, see Overview of SharePoint site lifecycle management.

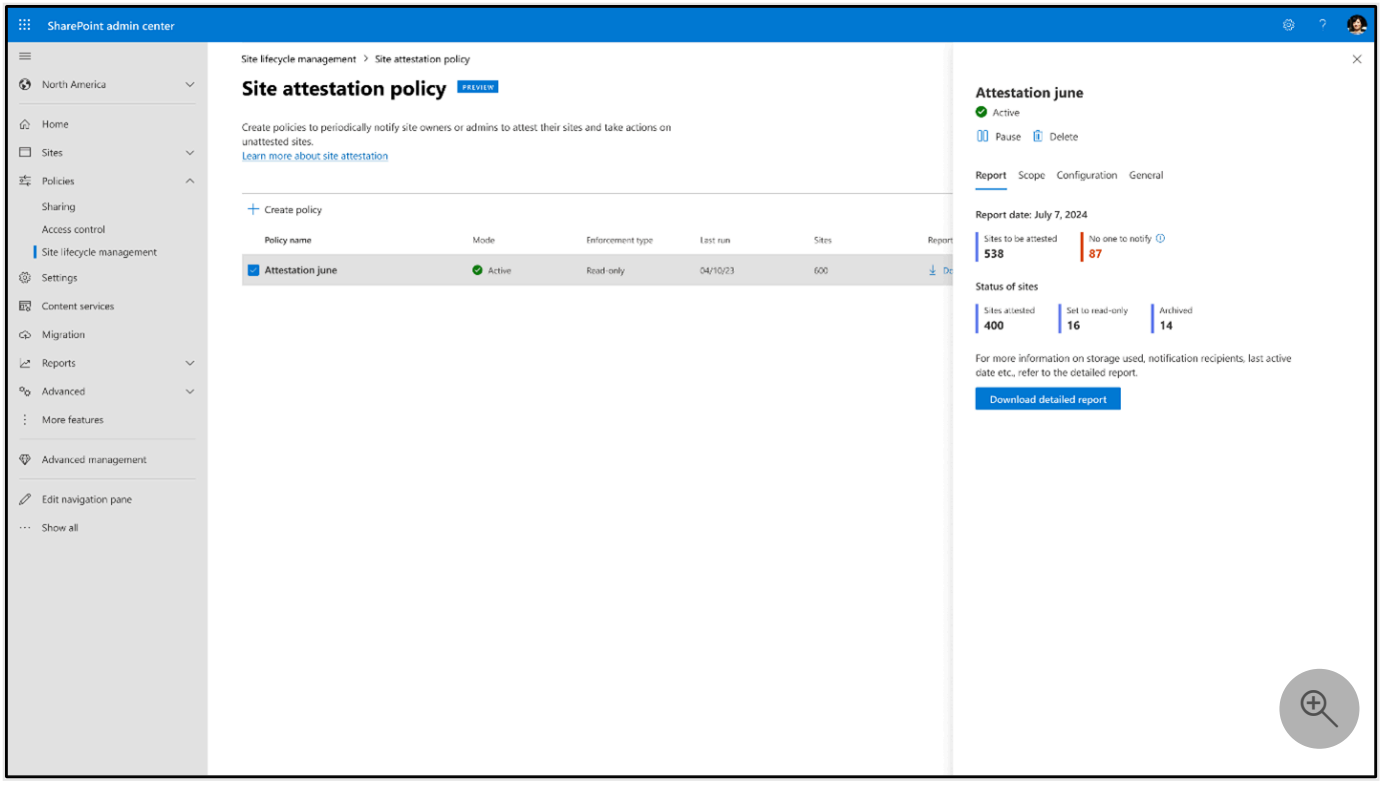
Reporting

After each run of the configured policy, you can view a detailed report about the sites it identifies. In the **Site attestation policies** page, select the desired policy from the list.

The panel outlines the numbers of:

- Sites to attest
- Sites that didn't have anyone to notify
- Sites attested

- Sites set to read-only
- Archived sites You can also view the policy's scope, configuration, and general information on the report.



You can also view the policy's scope, configuration, and general information on the panel. Select the **Download detailed report** option to download the report in CSV containing the following details for each of the sites identified due for attestation:

Expand table

Column	Definition
Site name	Name of the site
URL	URL of the site
Template	Template of the site
Connected to Teams	Indicates if it's a Teams-connected site
Sensitivity label	Sensitivity label assigned to the site
Retention policy	Indicates if any retention policy is applied to the site
Site lock state	State of site access **before** the policy runs (Unlock/Read-Only/No access)
Notified site admins	Email addresses of site admins receiving attestation notifications

Column	Definition
Notified site owners	Email addresses of site owners receiving attestation notifications
Last attested by	Email address of the person who last attested the site
Last attestation date (UTC)	Date when the site was last attested
Number of site owners	Total count of site owners for the site
Email address of site owners	Email addresses of all site owners
Number of site admins	Total count of site admins for the site
Email address of site admins	Email addresses of all site admins
Total notifications count	Total notifications sent so far by any policy under the same policy template
Action status of policy	Status of the site (First, second, or third notification sent, Site in read-only mode, Site archived, Action taken by another policy such as read-only, archive, or notified by another policy)
Action taken on (UTC)	Date on which the enforcement action was taken (date when site was archived or put in read-only mode)
Last activity date (UTC)	Date of last activity detected across SharePoint site and connected workloads
Site creation date (UTC)	Date when the site was created
Storage used (GB)	Storage consumed by the site
Duration in read-only (days)	Number of days the site is in the enforced read-only state

Configure actionable emails for US Government Cloud (GCC High or DoD) environments

In US Government Cloud (GCC High and DoD) environments, a tenant administrator must complete an extra, one-time setup for SharePoint site lifecycle management (SLM) policies to use

actionable messages. This step helps ensure that policy notification emails display and function correctly. For example, site admins and site owners can take actions directly from email.

Unlike other commercial cloud environments, GCC High and DoD tenants require explicit administrator approval of the actionable message provider before it can send interactive email messages. Without this approval, SLM policy emails are delivered, but action buttons don't function as expected.

> **Important**
>
> You must be a Global Administrator or Exchange Administrator in the tenant to set up actionable messages.

Approve the SLM actionable message provider

1. Go to the Outlook Actionable Messages – Connectors admin portal for GCCH or DoD and sign in.
2. In the **Provider Status** filter, select **Approved by Microsoft – Pending Your Approval**.
3. Locate the provider named `InactiveSiteOAMProviderGCCH`.
4. Select the provider, and then select **Approve**.

After you approve the provider, the SLM policy notifications send actionable messages.

> **Note**
>
> This approval applies only to SLM policy notifications. Other applications or services that use actionable messages might require separate approval.

Ensure actionable messages are enabled for the tenant

Site lifecycle management policies use Outlook actionable messages to enable site owners or site administrators to take necessary actions by using links within email messages.

- For notifications to render properly, make sure your organization meets the Outlook version requirements.
- To troubleshoot rendering problems, see frequently asked questions.

Troubleshooting actionable messages

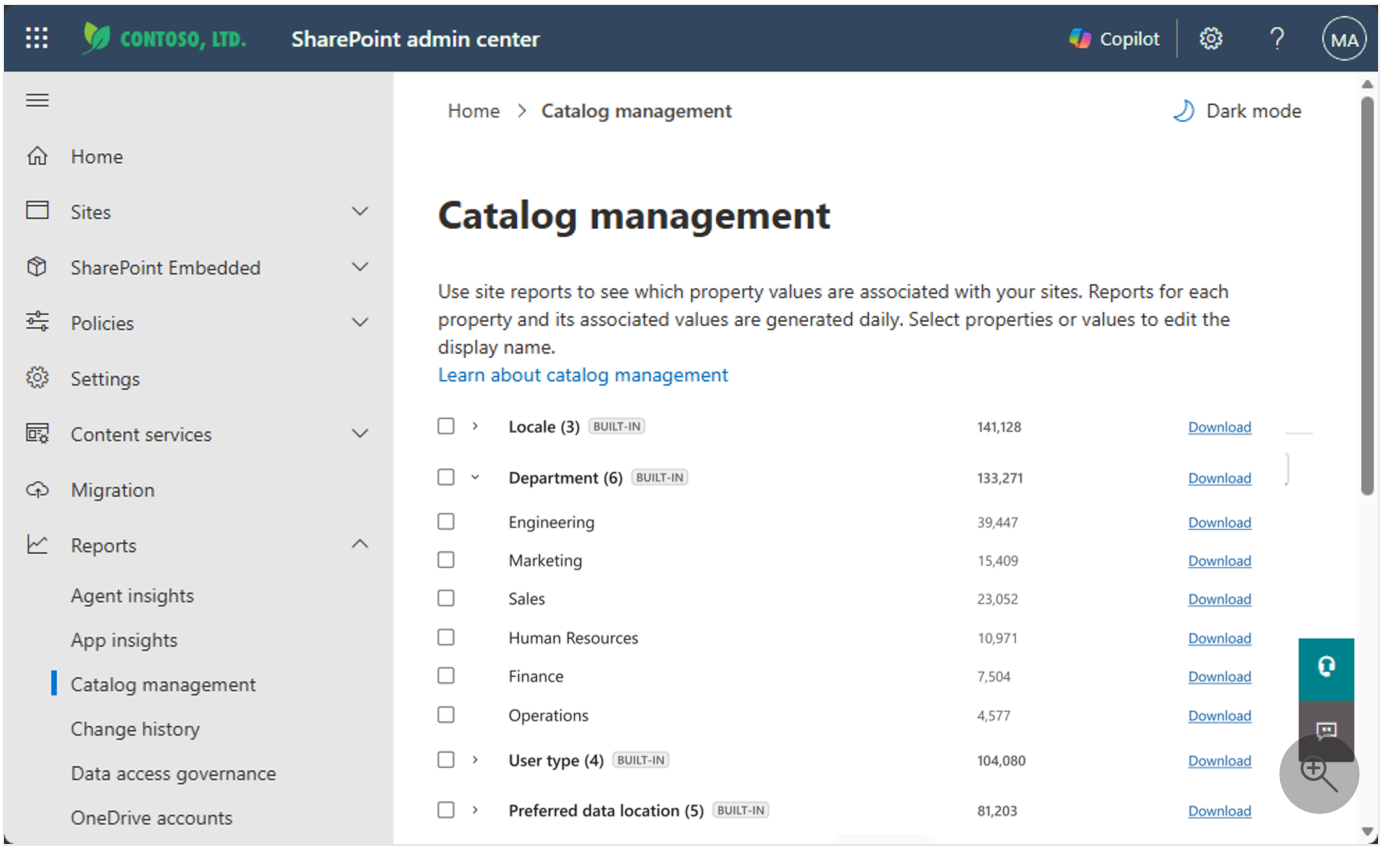
If actionable messages don't work as expected, try these steps:

- Make sure that the `InactiveSiteOAMProviderGCCH` provider is in an approved state.
- Allow sufficient time. It can take up to 24 hours for changes to propagate.

Last updated on 08/19/2026

Catalog management in SharePoint Advanced Management

Catalog management in SharePoint Advanced Management helps you understand how content is organized across your SharePoint environment. It uses existing Microsoft 365 metadata to automatically group sites into meaningful categories, giving you a centralized view of your content landscape.



By grouping sites into categories and groups, you can analyze content, apply governance actions at scale, and gain the insight needed to manage content, reduce risk, and prepare for AI-powered experiences such as Microsoft Copilot.

How catalog management works

Catalog management organizes SharePoint sites into categories and groups based on metadata already present in your Microsoft 365 tenant.

- **Categories** are high-level classifications such as department, user type, or region.
- **Groups** provide more detail within each category. For example, within the Department category, groups might include Marketing, Sales, HR, or Finance.

This structure helps you understand how content is distributed and governed across your organization.

You can use built-in categories or add your own categories. Each category has a label that identifies its type:

- `BUILT-IN`
- `UPLOADED`
- `CUSTOM PROPERTIES`
- `ENTRA ID`

You can use categories with SharePoint Advanced Management capabilities like Restricted Content Discovery. For example, you can apply Restricted Content Discovery to multiple sites by using catalog groups. (See the section, Use catalog groups with Restricted Content Discovery in this article.)

Metadata sources

Catalog management uses metadata from multiple sources to define categories and groups:

- **Microsoft Entra ID**: Organizational attributes such as department, user type, and extension attributes.
- **SharePoint site metadata**: Site properties such as property bag values, site keywords, and other SharePoint-defined properties.

Because catalog management reflects existing metadata, keeping that metadata accurate and consistent is essential for meaningful results.

Built-in categories

Catalog management includes built-in categories derived from Microsoft Entra ID and SharePoint metadata. Common examples include:

- **Locale**: The region where the content is hosted (for example, North America versus Europe).
- **Department**: The organizational units associated with the site (for example, Finance).
- **User type**: Guest or non-guest.
- **Preferred data location (PDL)**: The multi-geo setup for your sites.
- **Information barriers segment**: The segment defined by information barriers policies for organizations that implement information barriers.

These categories are automatically populated, available without configuration, and refreshed every hour.

Categories you can add

> **Note**
>
> You can't use special characters, such as non-English characters, in category names, group names, CSV file names, or display names.

In addition to built-in categories, you can create categories from the following sources:

Expand table

Method	Label	Data refresh
Upload a CSV file that contains a list of sites you want to include in your new category	`UPLOADED`	Right away after the file is uploaded
Use a custom site property	`CUSTOM PROPERTIES`	The first data refresh occurs within 24 hours, and after that, every two weeks.
Use a Microsoft Entra ID extension attribute	`ENTRA ID`	The first data refresh occurs within 24 hours, and after that, every two weeks.

Upload a CSV site list

> **Note**
>
> Each category you add by using this option serves as a snapshot. To update the list of sites, you must update each category manually.

1. In the SharePoint admin center, in the navigation pane, go to **Reports** > **Catalog management**.
2. Select **Add category**. In the **Add category** pane, select **CSV site lists**.
3. Specify a category name and description.
4. Download the CSV template and use it to create your lists. Create one CSV file for each group that you want to create in your category. You can have up to 20 groups in a category.

5. In the **Add category** pane, upload a CSV file. If you have more than one, use **Add group** for each additional CSV file.

6. Select **Save**.

Use a custom site property

Use this option if your organization already stores classification information in SharePoint site properties, such as department, region, business unit, or compliance designation. Catalog management doesn't create or populate the property values. Instead, it reads existing property values and uses them to create categories and groups. By using this approach, you can organize sites with metadata that already exists in your environment without maintaining manual site lists.

Example: Use a Department site property

Suppose your organization already uses a custom site property named **Department** in the SharePoint site property bag. The property might contain values such as:

- Department = Marketing
- Department = Finance
- Department = Human Resources

When you create a catalog category and specify **Department** as the custom property, catalog management scans the selected sites and creates groups based on the values it finds. In this example, catalog management creates separate groups for Marketing, Finance, and Human Resources, and places sites into the appropriate group automatically.

After you determine the site properties you want to use, connect them to catalog management.

Connect custom site properties to catalog management

1. In the SharePoint admin center, in the navigation pane, go to **Reports** > **Catalog management**.

2. Select **Add category**. In the **Add category** pane, select **Custom properties**.

3. In the **Properties** section, enter the name of a property that you want to use. To add more properties, select **Add property**. You can specify up to 20 properties.

4. Under **Sites**, select one of the following options:

- **Most active sites (up to 20,000 sites)**: Data is available within 24 hours and refreshes automatically every two weeks.
- **Upload a list of up to 20,000 sites**: Download the CSV template and use it to create your site list. Then upload the CSV file. Keep in mind that with this option, the list of sites in the category serves as a snapshot that you must update manually.

5. Select **Save**.

Use Microsoft Entra ID extension attributes

If your organization uses Microsoft Entra ID extension attributes, you can create catalog categories based on the values stored in `extensionAttribute1` through `extensionAttribute15`. Extension attributes are predefined attributes in Microsoft Entra ID that organizations can use to store extra string-based metadata for user or device objects.

Catalog management uses these existing attribute values to group SharePoint sites into categories. When you select one or more Microsoft Entra ID extension attributes as catalog categories, Catalog management groups sites based on the extension attribute values associated with site owners. These groupings update when the underlying attribute values or site ownership changes.

For example, your organization might use an extension attribute to identify a business unit, operating model, compliance boundary, program, or other internal classification that isn't represented by a built-in category such as Department or User type. By using that extension attribute as a catalog category, you can view and manage related sites together without manually maintaining a separate site list.

Before you use extension attributes with catalog management, make sure the attributes are populated consistently in Microsoft Entra ID. Catalog management reflects the metadata that already exists in your tenant, so incomplete or inconsistent values can result in incomplete or inconsistent site groupings.

Identify or set extension attributes

To view a list of existing extension attributes or to set them, follow the guidance in Extension attributes. You can identify or set extension attributes by using PowerShell, Python, and more.

After you identify your extension attributes, use them to add categories.

Use extension attributes with catalog management

1. In the SharePoint admin center, in the navigation pane, go to **Reports** > **Catalog management**.
2. Select **Add category**. In the **Add category** pane, select **Entra ID extension attributes**.
3. In the **Entra ID extension attributes** list, select the attributes that you want to use as categories.
4. Select **Save**.

Edit a category or group

You can change the display name of any category, and you can edit categories that aren't built in. Depending on the category type, you can edit display names, descriptions, groups, and site lists. Editing a display name doesn't change the underlying metadata or site grouping.

> ⓘ **Note**
>
> You can't use special characters, such as non-English characters, in category names, group names, CSV file names, or display names.

1. In the SharePoint admin center, in the navigation pane, go to **Reports** > **Catalog management**.
2. Select a category or group to open the editing pane.
3. Take one or more of the following actions:
   a. To change the name of a category, select **Edit display name** and enter a new name.
   b. To edit a category, select **Edit category**, and then modify its name and description as needed.
   c. To edit, add, or remove a group, in the **Groups** section, select **Edit**, **Delete**, or **Add group**.
4. Select **Save**.

Use catalog groups with Restricted Content Discovery

Organizations often need to apply Restricted Content Discovery across large groups of sites during a Copilot deployment or other governance initiatives. You can apply Restricted Content

Discovery to collections of sites instead of configuring sites individually. You can also remove Restricted Content Discovery from a group of sites.

> **Note**
>
> There's a limit of 20,000 sites with Restricted Content Discovery in catalog management. That limit doesn't apply to Restricted Content Discovery at the tenant/service level.

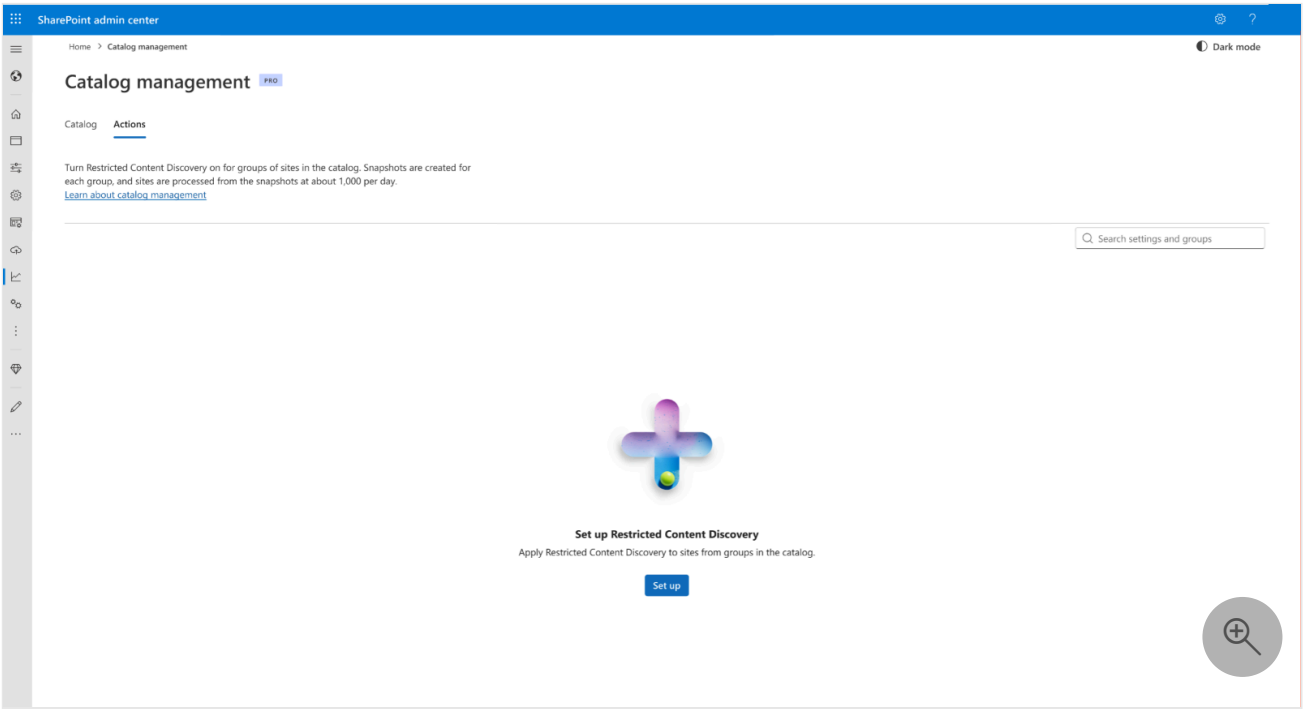
Bulk operations retain existing Restricted Content Discovery behavior.

- Restricted Content Discovery remains a site-level property.
- Sites that already have Restricted Content Discovery enabled aren't modified.
- Existing permissions remain unchanged.
- Standard propagation behavior continues to apply.

Because Restricted Content Discovery must propagate across indexing systems, updates can take time to become fully effective. The amount of time depends on site size, the number of files in each site, and the number of concurrent updates being processed.

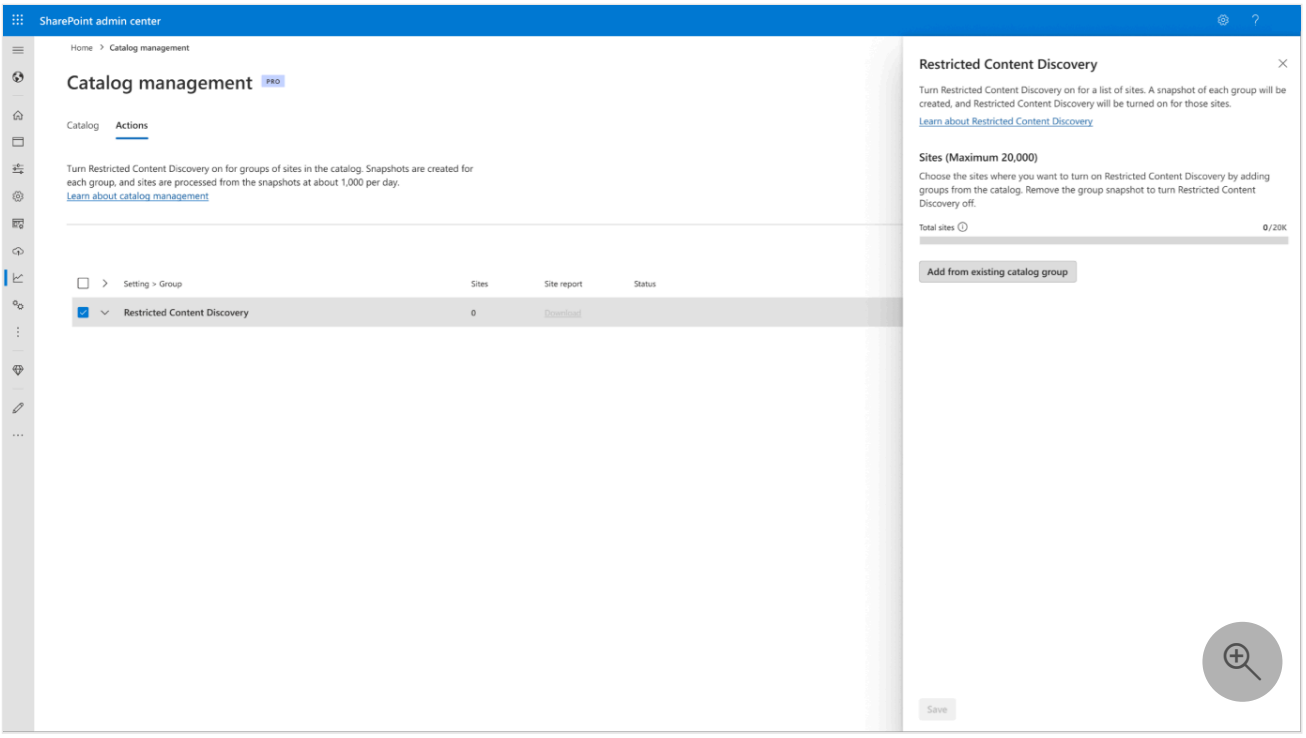
Apply Restricted Content Discovery to a group of sites

1. In the SharePoint admin center, in the navigation pane, go to **Reports** > **Catalog management**. Then select the **Actions** tab.



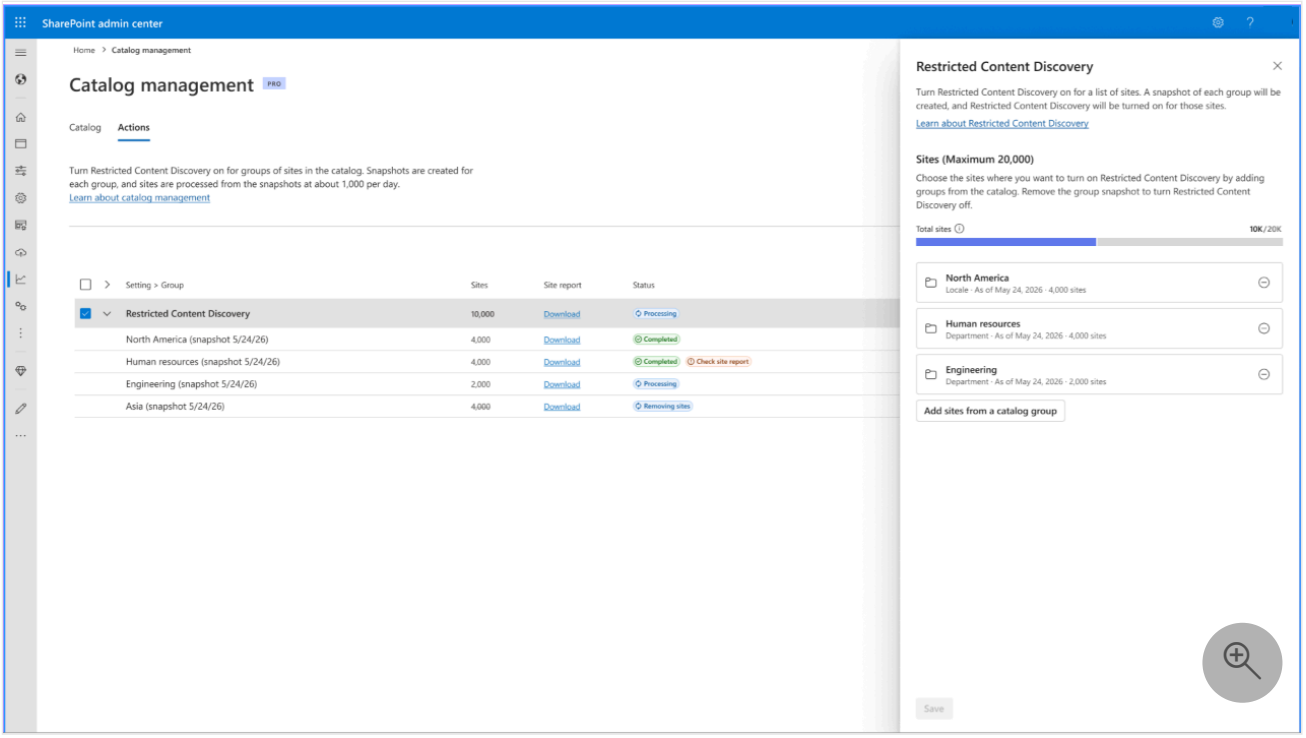
If you didn't already set up Restricted Content Discovery, select the **Set up** button to do that.

2. Select a category to open the Restricted Content Discovery panel. If you didn't apply Restricted Content Discovery to any groups yet, select **Add from existing catalog group**.



3. Review the information shown in the panel. You can see:

   - How many sites have Restricted Content Discovery applied. This number changes in real time as soon as you select or remove groups.
   - A list of groups in the selected category that have Restricted Content Discovery applied.



4. At the bottom of the panel, select + **Add sites from a catalog group**.

5. Use the drop-down menu to select a group.

6. Select **Save**, and then confirm your changes.

Snapshots and subsequent changes to groups

When you add a catalog roup to Restricted Content Discovery, you're adding a snapshot of that group at that point in time. If sites are added or removed from that group, no changes are made to Restricted Content Discovery.

For example, suppose a group is added to Restricted Content Discovery. When it was added, the group had ten sites. Now suppose three more sites are added to the group. In this case, Restricted Content Discovery is applied to the first ten sites, but not to the three new sites yet.

If changes occur to a group, such as sites are added or deleted, and you want to update Restricted Content Discovery application, follow these steps:

1. In the SharePoint admin center, in the navigation pane, go to **Reports** > **Catalog management**.

2. On the **Actions** tab, select a category to open the Restricted Content Discovery panel.

3. In panel, in the list of groups, select the group, and then select **Remove**.

4. Re-add the group that you just removed.

5. Select **Save**, and then confirm your changes.

Remove Restricted Content Discovery from multiple sites

1. In the SharePoint admin center, in the navigation pane, go to **Reports** > **Catalog management**.
2. On the **Actions** tab, select a category to open the Restricted Content Discovery panel.
3. In the information shown in the panel, select the group you want to remove from Restricted Content Discovery.
4. Select **Remove**.
5. Select **Save**, and then confirm your changes.

Restricted Content Discovery states in catalog management

After you apply or remove Restricted Content Discovery to or from a group, expect to see one of the following states in the status column:

- **Completed**: Restricted Content Discovery is applied to sites in the catalog group.
- **Processing**: Changes are still rolling out. The processing time varies depending on the number of files in the sites.
- **Adding sites**: Restricted Content Discovery is being added to sites in the category group.
- **Removing sites**: Restricted Content Discovery is being removed from sites in the category group.
- **Check site report**: Download the site list to see status for each site.
- **Error**: An error occurred during processing.

Integration with the SharePoint Admin Agent

Catalog management provides structure that improves the effectiveness of the SharePoint Admin Agent. When you categorize sites, the SharePoint Admin Agent can provide more targeted insights, analysis, and governance recommendations based on how content is organized across your tenant. For more information, see SharePoint Admin Agent.

See also

- SharePoint Advanced Management overview
- SharePoint Admin Agent

- SharePoint Advanced Management prerequisites

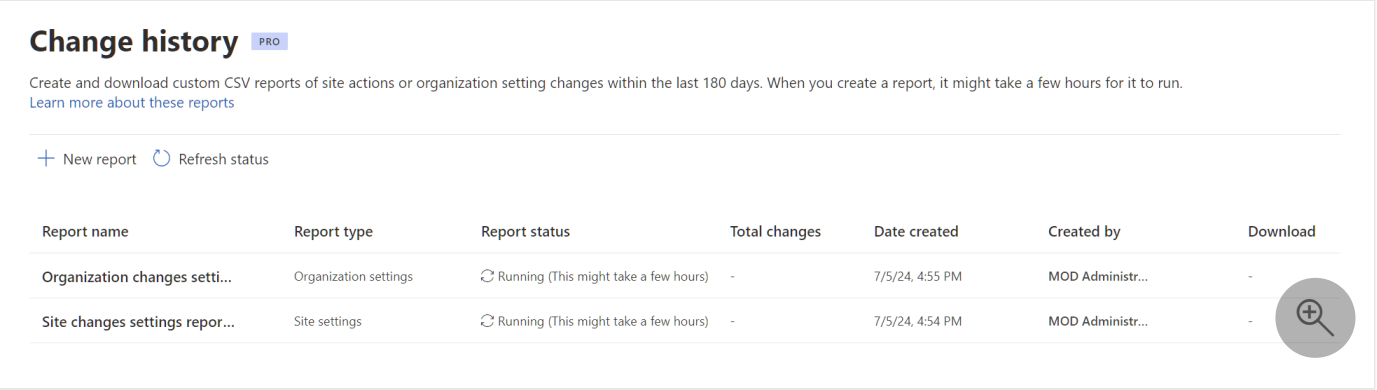
Last updated on 10/08/2026

Track site actions or organization setting changes made within the last 180 days with change history reports

Aa a SharePoint administrator, you can create custom change history reports in the SharePoint admin center to review CSV reports of site actions or organization setting changes made within the last 180 days.

Change history reports can increase visibility and let you monitor changes made to the SharePoint configuration across various levels of your organization.

Create up to 10 reports that track what changed, when it happened, and who initiated the change across the site and organization settings.



Prerequisites

See SharePoint Advanced Management prerequisites.

Also turn on **Audit logging** in the Microsoft Purview portal. Audit logs are essential for tracking user and admin activities across your SharePoint environment. See Turn audit logging on or off.

How do I create a change history report?

1. Go to the SharePoint admin center, and sign in.

2. In the navigation pane, expand **Reports** and select **Change history**. Then select **Create report**.

3. Choose the type of report you want to generate and select **Site settings/Organization settings**.

4. A panel appears where you can specify the type of information you want to include in your change history report. Select **Create report** to generate a new report.

5. The new report is listed on the change history page. Select the report to open the change history report panel and monitor its status.

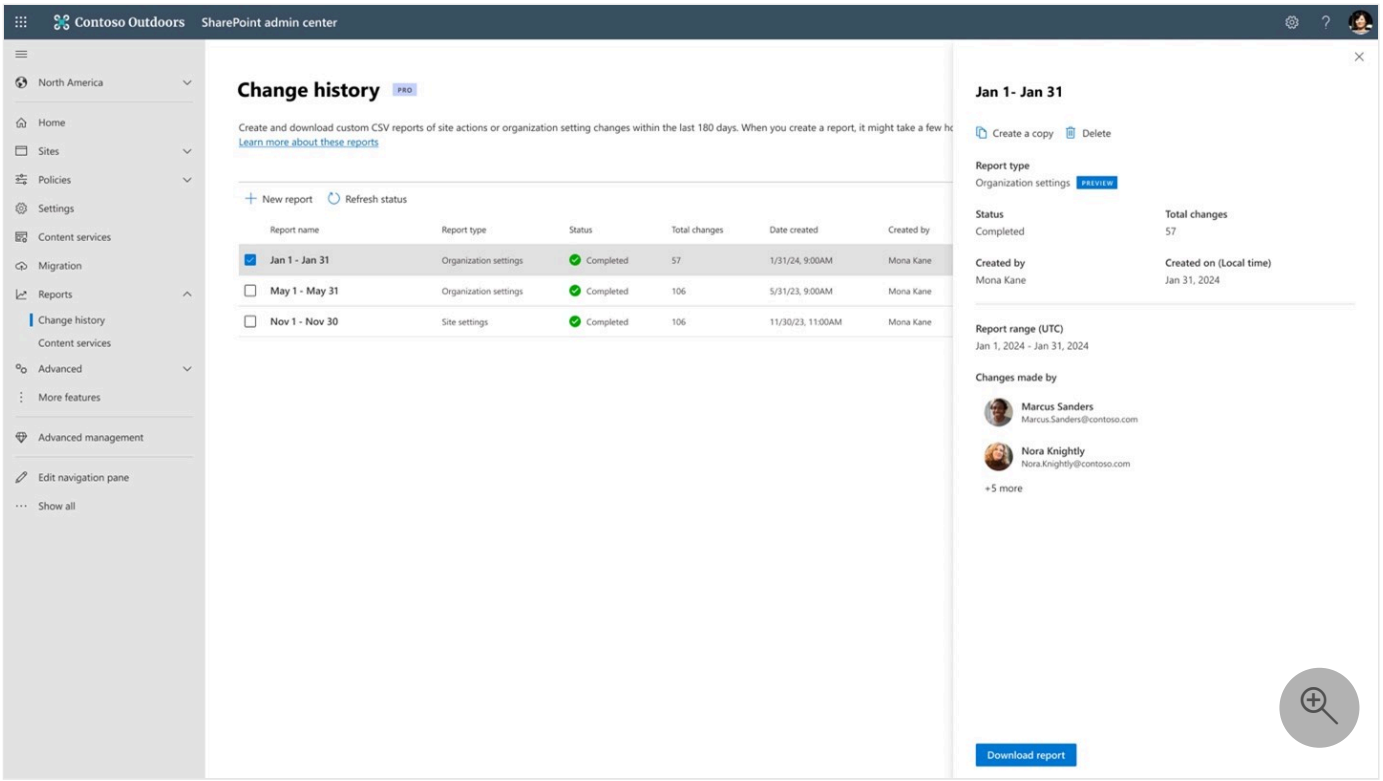
6. Once the report is created, select **Download report** to export the data as a CSV file. The **Create a copy** button allows you to create more reports with similar parameters.

> **Note**
>
> - The report takes a few hours to generate depending on the search criteria selected when creating the report.
> - You can export data for up to 180 days with a change history report depending on the user license. The report may contain data for users that go back 180 days and data for others that don't. Since the type of user license isn't shown on the report, it might appear as if data is missing for some users.
> - Admins assigned the global reader role don't have the permissions to create or delete a report, but can download to review the changes.

View a change history report

To view change history reports, in the SharePoint admin center, expand **Reports**, and select **Change history**.

You can create new reports, delete, and refresh their statuses from the change history page. This page can only show 10 reports at a time. The best practice is to delete a previous report before creating a new one.



What types of change history reports can I create?

You can create two types of change history reports to monitor different aspects of your SharePoint environment. Site settings reports track changes made to individual SharePoint sites, including changes to site properties and configurations performed by Site Administrators and SharePoint Administrators. Organization settings reports monitor changes made at the tenant level through the SharePoint Admin Center, helping you ensure your organization-wide policies and configurations remain aligned with your governance requirements.

Site settings report

Generate a site settings report for a given date range and filter by sites and users. You can download the report as a CSV file to view the site property changes. All site actions performed by Site Administrators and SharePoint Administrators are captured in the report.

Organization settings report

> **Note**
>
> The audited organization settings table listed later in this article reflects the list of settings that are currently tracked under organization settings reports.

You can also generate an organization settings report tracking changes made to organization settings from the SharePoint Admin Center. You can generate these reports for custom date ranges while filtering for specific users of interest. A best practice is to review the downloaded reports to ensure there are no deviations in settings from the desired state.

Any changes made to the following organization settings are reflected in the reports. We're continuously working to bring more settings under the ambit of these reports.

Current audited organization settings

The following table lists the latest set of supported settings found under the **Settings** node:

Expand table

Name	Description
SharePoint Pages	Allow commenting on modern pages Allow users to create new modern pages
SharePoint Site creation	Users can create SharePoint site Create teams sites under Default time zone Default storage limit for new sites
SharePoint Notifications	Allow notifications
SharePoint Site storage limits	Automatic Manual
OneDrive Notifications	Allow notifications
OneDrive Retention	Days to retain a deleted user's OneDrive
OneDrive Storage limit	Default storage limit
OneDrive Sync	Show Sync button on the OneDrive website Allow syncing only on computers joined to specific domains Block download of specific file types
SharePoint Version history limits	Set version history limits

The following table lists the latest set of supported settings found in **Access Control** under the **Policies** node:

Expand table

Name	Description
Unmanaged devices	Restrict access from devices that aren't compliant or joined to a domain
Idle session sign out	Automatically sign out users from inactive browser sessions
Network location	Allow access only from specific IP addresses
Apps that don't use modern authentication	Block access from Office 2010 and other apps that can't enforce device-based restrictions
SharePoint access restriction	Restrict access to SharePoint sites & content by security group
OneDrive access restriction	Restrict access to OneDrive content by security group

The following table lists the latest set of supported settings found in **Sharing** under the **Policies** node:

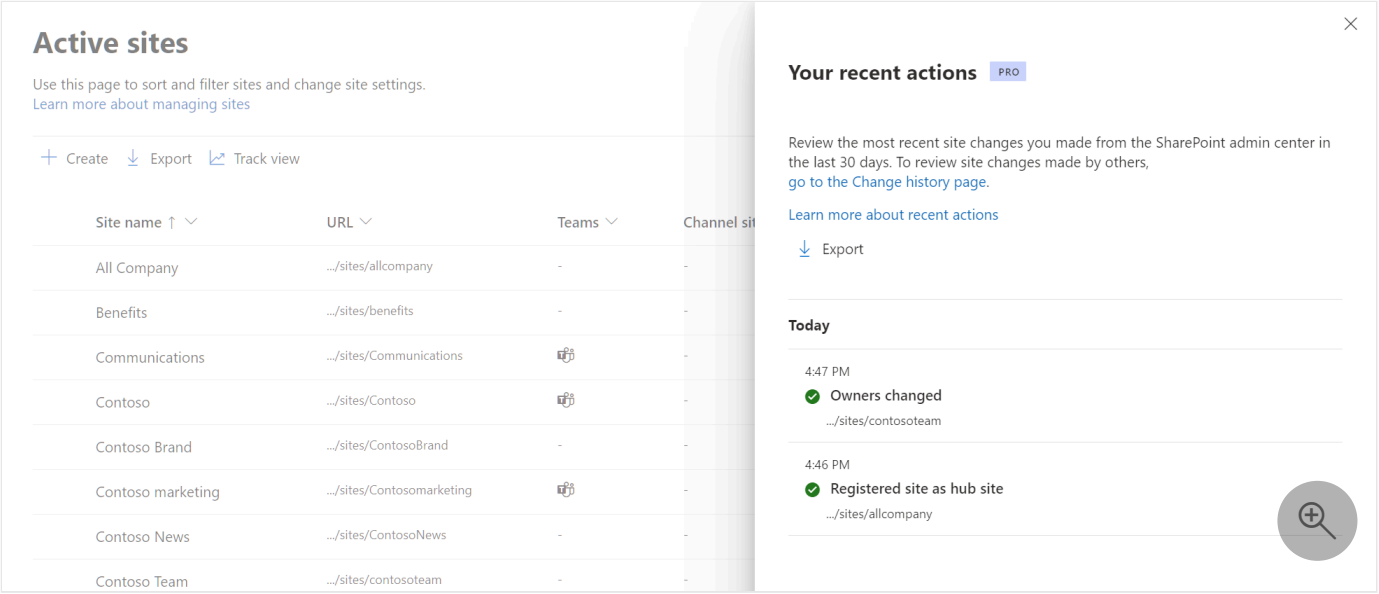
Expand table

Name	Description
External Sharing	Content can be shared with More external sharing settings Other settings
File and folder settings	Choose the type of link selected by default when users share files and folders in SharePoint and OneDrive Choose the permission selected by default for sharing links Choose who can access files with the URL to a file copied from the browser address bar

Last updated on 05/14/2026

Review your recent changes to SharePoint site properties

The recent actions panel lets you review and monitor the last 30 changes you've made to a SharePoint site's properties (such as renaming a site, deleting a site, changing storage quota) within the last 30 days in the SharePoint admin center. This feature only shows changes made by you and not other administrators. Also, changes made to site properties at the organization-level don't show in the panel.



> **Note**
>
> Recent actions panel isn't available for global readers. GDAP administrators can't see the previous and current values of the administrator actions.

Prerequisites to review your recent changes to SharePoint site properties

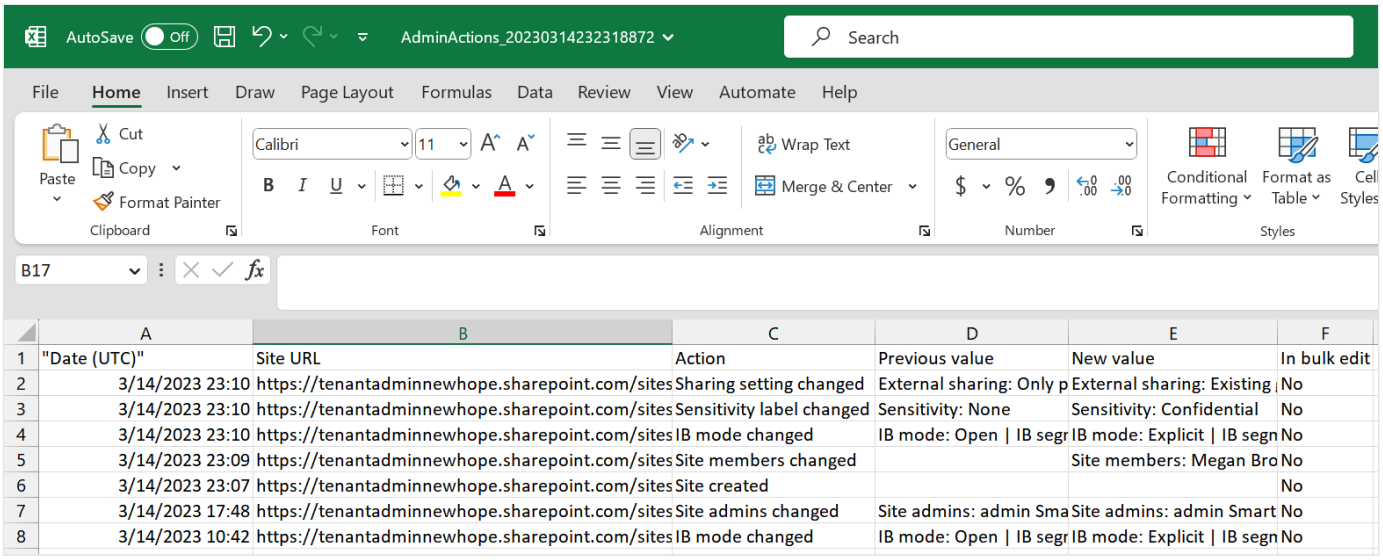
See Prerequisites for SharePoint Advanced Management.

> **Important**
>
> Without Microsoft SharePoint Advanced Management, you can only view actions made in the current session. Once you close the browser or sign out, the recent actions panel clears

the history.

View recent actions of a site

1. In the SharePoint admin center, expand **Sites** and select **Active sites**.
2. Select **Your recent actions**. The recent actions panel appears and lists your most recent 30 actions made within the last 30 days.
3. Select **Export** to download the list as a CSV file.
4. Select **View site details** to open the site info panel. From here, you can make changes to site properties like site name, site address, hub association, and aliases.



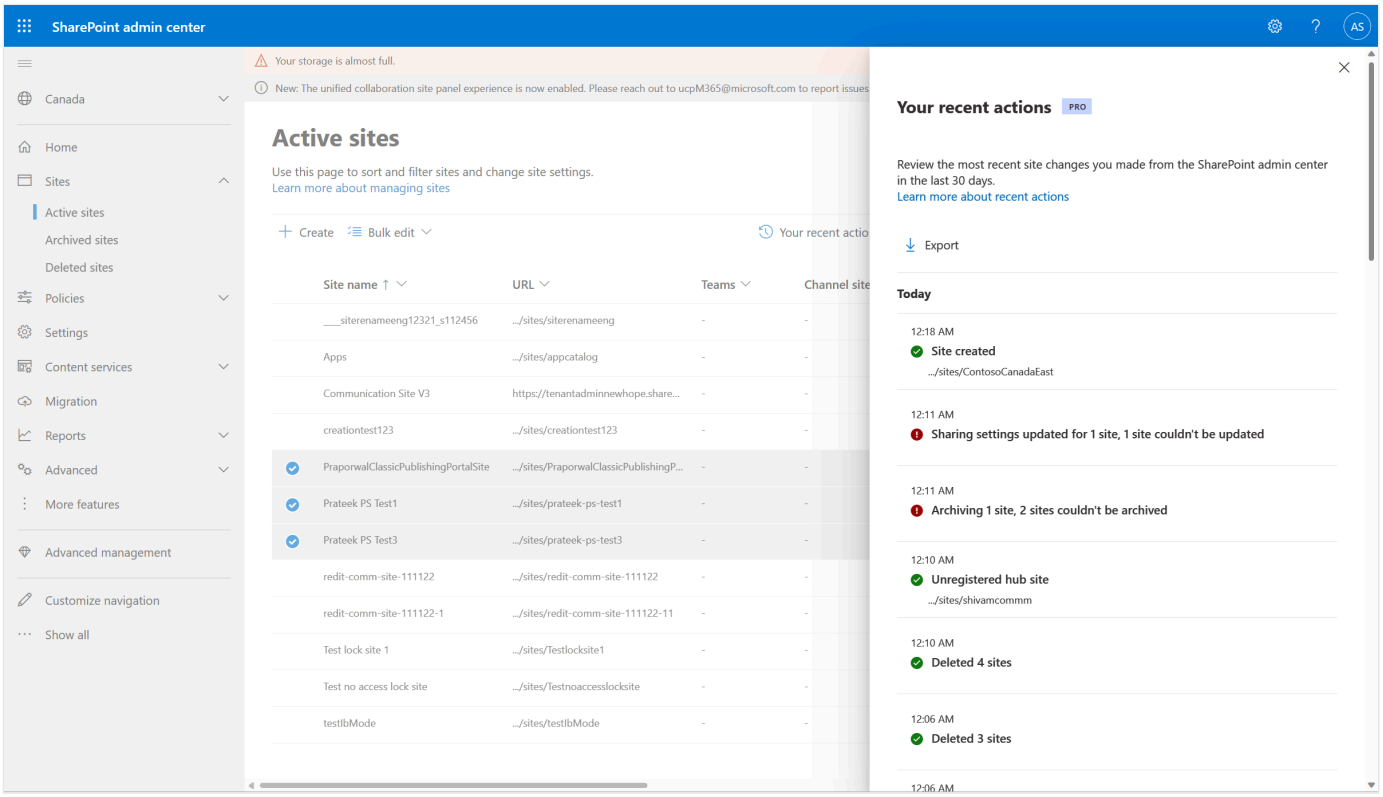
"Date (UTC)"	Site URL	Action	Previous value	New value	In bulk edit
3/14/2023 23:10	https://tenantadminnewhope.sharepoint.com/sites	Sharing setting changed	External sharing: Only p	External sharing: Existing	No
3/14/2023 23:10	https://tenantadminnewhope.sharepoint.com/sites	Sensitivity label changed	Sensitivity: None	Sensitivity: Confidential	No
3/14/2023 23:10	https://tenantadminnewhope.sharepoint.com/sites	IB mode changed	IB mode: Open | IB segr	IB mode: Explicit | IB segn	No
3/14/2023 23:09	https://tenantadminnewhope.sharepoint.com/sites	Site members changed		Site members: Megan Bro	No
3/14/2023 23:07	https://tenantadminnewhope.sharepoint.com/sites	Site created			No
3/14/2023 17:48	https://tenantadminnewhope.sharepoint.com/sites	Site admins changed	Site admins: admin Sma	Site admins: admin Smart	No
3/14/2023 10:42	https://tenantadminnewhope.sharepoint.com/sites	IB mode changed	IB mode: Open | IB segr	IB mode: Explicit | IB segn	No

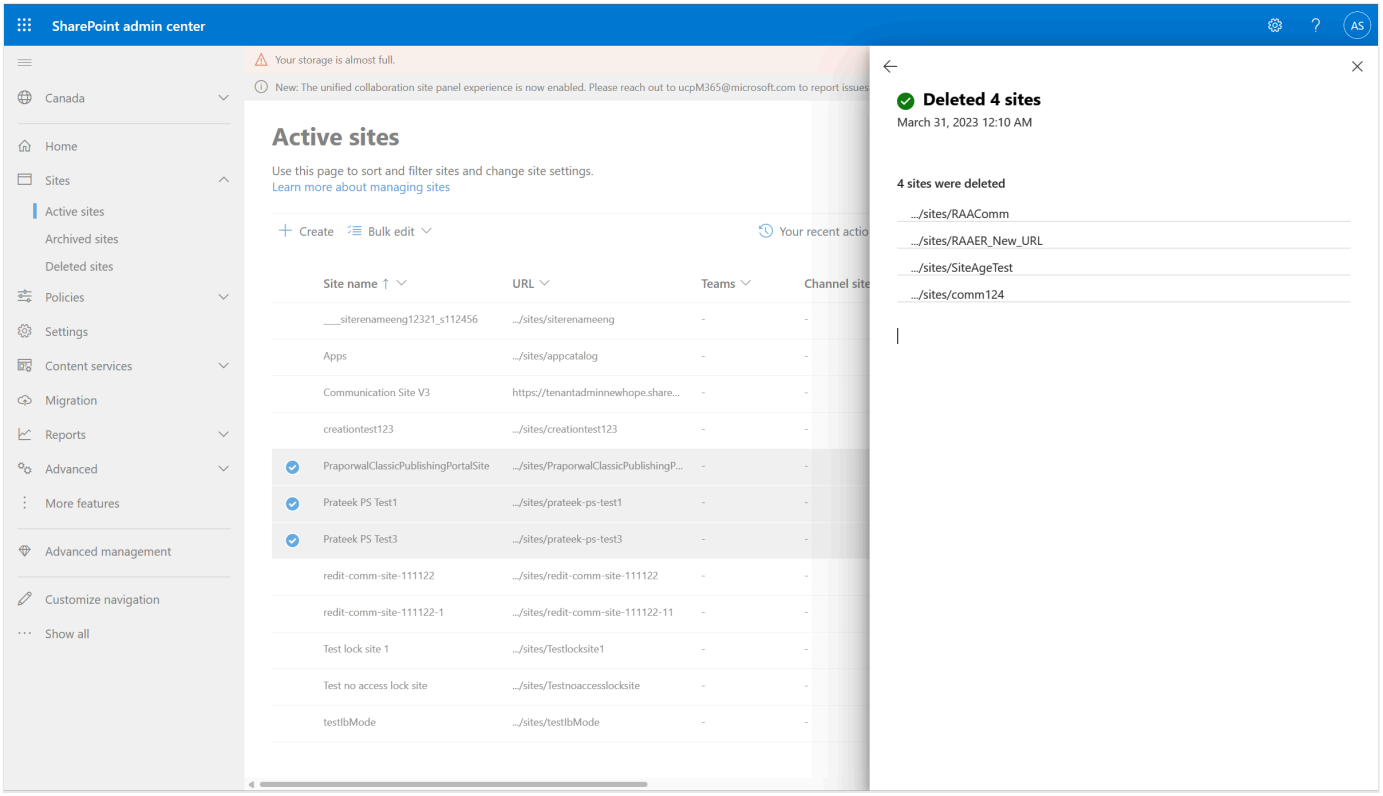
> **Note**
>
> If you close the browser while actions are in-progress, they aren't recorded in the panel or the CSV file. Failed actions are recorded in the panel, but are removed once you exit the current session. The exported CSV file doesn't contain failed actions.

Bulk site edits

Here's an example of how bulk edits are grouped as one action in the recent actions panel:

Suppose that you deleted four SharePoint sites on May 21 at 12:10 AM. The bulk edit shows as one item named **Deleted 4 sites** on the recent actions panel. Select that action and the list of deleted SharePoint sites appears.





Related articles

- What is SharePoint Advanced Management?

Last updated on 05/14/2026

Restrict OneDrive and SharePoint site creation by apps

The **Restricted Site Creation by Apps** feature lets SharePoint Administrators use the SharePoint Online Management Shell to designate which third-party apps can create SharePoint sites in your organization.

You can choose between two ways to manage site creation for apps within your tenant:

- **Deny** mode (the specified apps are unable to create sites)
- **Allow** mode (only the specified apps are allowed to create sites).

When you enable restricted site creation for apps in your tenant, the default mode is set to **deny**.

Keep in mind that these policies only control which apps can create new sites; these policies don't affect site access permissions for users or apps.

> ⓘ **Note**
>
> - The Restrict OneDrive and SharePoint site creation by apps feature is currently in preview.
> - Admins can create separate configurations for the following categories of sites: All sites (including OneDrives), all SharePoint sites (not including OneDrives), OneDrives, Team sites (Group connected and classic), and Communication sites.
> - The Restricted site creation for apps feature has a simulation mode parameter to test hypothetical scenario for policy configuration. -The Restricted site creation for apps feature only affects only non-Microosft (third-party) apps. First-party apps aren't affected.

Prerequisites for restricted site creation

- Your organization must have **SharePoint Advanced Management Plan 1**, an add-on for Microsoft 365. See Prerequisites for SharePoint Advanced Management, including requirements for the SharePoint Online PowerShell module
- Make sure you can configure apps that are allowed to create SharePoint sites.

To get App IDs

Some of the PowerShell commands you'll use call for App IDs. To create your list, follow these steps:

1. Sign in to the Microsoft Entra admin center as at least a Cloud Application Administrator.
2. Browse to **Entra ID** > **Enterprise apps** > **All applications**.
3. Select the application you want, and view its Application ID.

Connect to the SharePoint Online Management Shell

1. If you haven't already done so, download the latest SharePoint Online Management Shell.

   > **Note**
   >
   > If you installed a previous version of the SharePoint Online Management Shell, go to **Add or remove programs** and uninstall "SharePoint Online Management Shell" first. Then, install the latest version.

2. Connect to SharePoint as a SharePoint Administrator or SharePoint Advanced Management Administrator. For more information, see Getting started with SharePoint Online Management Shell.

Use the restricted site creation PowerShell commands

To enable site access restriction

PowerShell

```
Set-SPORestrictedSiteCreationForApps -Enabled $true
```

To allow apps to create sites

PowerShell

```
Set-SPORestrictedSiteCreationForApps -Mode Allow
```

To prevent apps from creating sites

PowerShell

```
Set-SPORestrictedSiteCreationForApps -Mode Deny
```

To add or reconfigure the App ID list

PowerShell

```
Set-SPORestrictedSiteCreationForApps -SiteType <SiteType> -RestrictedSiteCreationApps
<comma separated app IDs>
```

To view your Restricted Sites App list

PowerShell

```
Get-SPORestrictedSiteCreationForApps -SiteType <SiteType>
```

Site types for restricted site creation for apps

Specify `SiteType` parameter when you update and view the App ID list. Here's the SiteType parameter list:

Expand table

Site type	Applies to
All	OneDrive and all SharePoint sites
SharePoint	All SharePoint sites (but not OneDrive)
OneDrive	Only OneDrive
Team	Only SharePoint team sites (group-connected and classic)
Communication	Only SharePoint communication sites

> **Note**
>
> **All Sites** includes all sites except for any template listed in the following table. The *All Sites* SiteType overrides all others.

Expand table

Type	Template Name	Template ID	Reason
SharePoint Embedded	`CSPCONTAINER`	70	SharePoint Embedded experience is managed separately
Redirect site	`REDIRECTSITE`	301	Critical SharePoint functionality
My Site Host	`MYSITEHOST`	54	Core site
Tenant Admin	`TENANTADMIN`	16	Core site

How deny and allow modes work

The restricted site creation for apps mode is shared across all site type policies. It isn't possible to use deny mode for one site type and allow mode for a different site type.

When restricted site creation for apps is in **deny** mode, an app is blocked from creating a site if its App ID is in any list configured with any site type, which applies to the site it's attempting to create. For example, an app is blocked from creating a SharePoint communication site if its App ID is in any list configured with the All, SharePoint, or Communication site types.

When restricted site creation for apps is in **allow** mode, an app is only allowed to create a site if its App ID is in a list configured with a site type, which applies to the site it's attempting to create. For example, an app can create a OneDrive if its App ID is in a list configured with the All or OneDrive site types.

> **Note**
>
> Changing the mode from deny to allow prompts a message: "Are you sure you want to switch from Deny to Allow? Switching will remove all current configuration of restrictions." A similar message appears when you switch from allow to deny mode as well.

Specify the App IDs in the Restricted Sites App list

When you specify App IDs in the Restricted Sites App list, the command replaces the current list with the app IDs that you specify. You can't add or remove individual app IDs. Each time you run the command, it replaces the previous list with a new list for that site type.

To avoid removing access for other apps, always include all app IDs you want to allow in your command.

Here are some examples.

Example 1: Allow only one app to create sites

Suppose we want to allow only one app to create sites. The app has ID `281e395b-7316-4cb2-b5bb-8881426ee411`. We'd use the following command:

PowerShell

```
Set-SPORestrictedSiteCreationForApps -SiteType "All" -RestrictedSiteCreationApps
"281e395b-7316-4cb2-b5bb-8881426ee411"
```

This command replaces the existing list with just the specified app ID. Only this app is able to create sites of type "All".

Example 2: Update the list of apps that are allowed to create team sites

Suppose we want to update the list of apps that can create team sites. We'd use the following command:

PowerShell

```
Set-SPORestrictedSiteCreationForApps -SiteType "Team" -RestrictedSiteCreationApps
"78159241-04a9-41d2-8dd4-ac568e9766a3,1f95829b-e1c8-4406-b2be-508c36f4bca5"
```

This command replaces the current list of allowed apps for Team sites with only the specified app IDs.

Related content

- What is SharePoint Advanced Management?
- Intro to SharePoint Online Management Shell
- Restrict OneDrive access by security group
- Monitor agent access to SharePoint and OneDrive

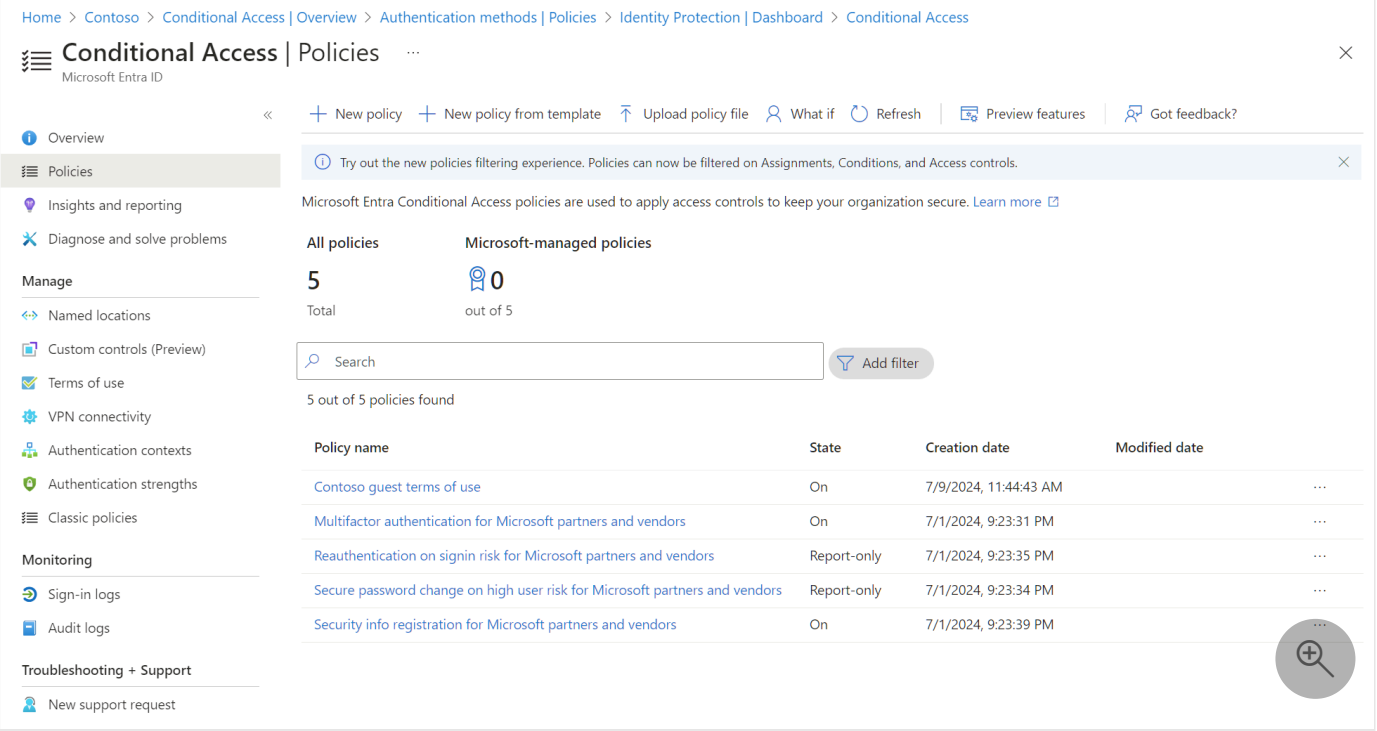
Last updated on 05/14/2026

Conditional Access policies and SharePoint

By using Microsoft Entra authentication context, you can enforce more stringent access conditions when users access SharePoint sites.

Use authentication contexts to connect an Microsoft Entra Conditional Access policy to a SharePoint site. You can apply policies directly to the site or apply them through a sensitivity label.

You can't apply this capability to the root site in SharePoint (for example, https://contoso.sharepoint.com).



Before you begin

Review the SharePoint Advanced Management prerequisites.

In addition, you need one of the following licenses:

- Microsoft 365 E5/A5 Compliance
- Microsoft 365 E5 Information Protection and Governance

Limitations

Some apps don't work with authentication contexts. Test apps on a site with authentication context enabled before broadly deploying this feature.

The following apps and scenarios don't work with authentication contexts:

- Older versions of Office apps (see the list of supported versions)
- SharePoint mobile apps (iOS and Android)
- Viva Engage
- You can't add the OneNote app to a channel if the associated SharePoint site has an authentication context.
- Teams channel meeting recording upload fails on sites with an authentication context.
- SharePoint folder renaming in Teams fails if the site has an authentication context.
- Teams webinar scheduling fails if OneDrive has an authentication context.
- The OneDrive sync app won't sync sites with an authentication context.
- Associating an authentication context to the enterprise application catalog site collection isn't supported.
- The "Visualize SharePoint List in Power BI" feature doesn't currently support authentication context.
- Outlook on Windows, Mac, Android, and iOS don't support communication with SharePoint sites protected by an Authentication Context.
- The multiple-file download feature currently doesn't function when both the authentication context and 'Use Conditional Access App Control' in session control are enabled in the conditional access policy.
- The multiple-file download feature won't work if an authentication context is set directly on a SharePoint site without an active Conditional Access policy using that context, or if the policy exists but is disabled.
- The file copy and move feature between different regions (cross-geo) currently doesn't function when an authentication context is applied to the destination site.
- Exporting to Excel as an Excel Web Query (IQY) doesn't currently support authentication context.
- Recording or running a script using Office Scripts in Excel for the Web fails if OneDrive has an authentication context.

Set up an authentication context

To set up an authentication context for labeled sites, complete these basic steps:

1. Add an authentication context in Microsoft Entra ID.

2. Create a Conditional Access policy that applies to that authentication context and has the conditions and access controls that you want to use.

3. Do one of the following steps:

   a. Set a sensitivity label to apply the authentication context to labeled sites.

   b. Apply the authentication context directly to a site.

In this article, you see the example of requiring guests to agree to a terms of use before gaining access to a sensitive SharePoint site. You can also use any of the other conditional access conditions and access controls that you might need for your organization.

Add an authentication context

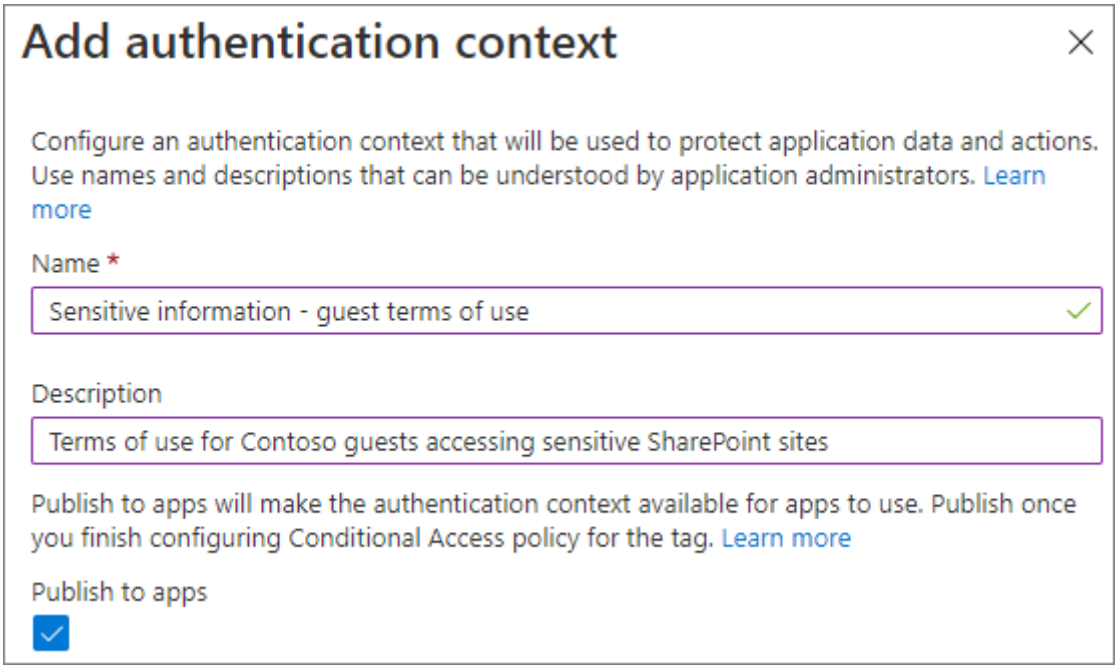
First, add an authentication context in Microsoft Entra ID.

To add an authentication context:

1. In Microsoft Entra Conditional Access, under **Manage**, select **Authentication context**.

2. Select **New authentication context**.

3. Type a name and description, and select the **Publish to apps** check box.



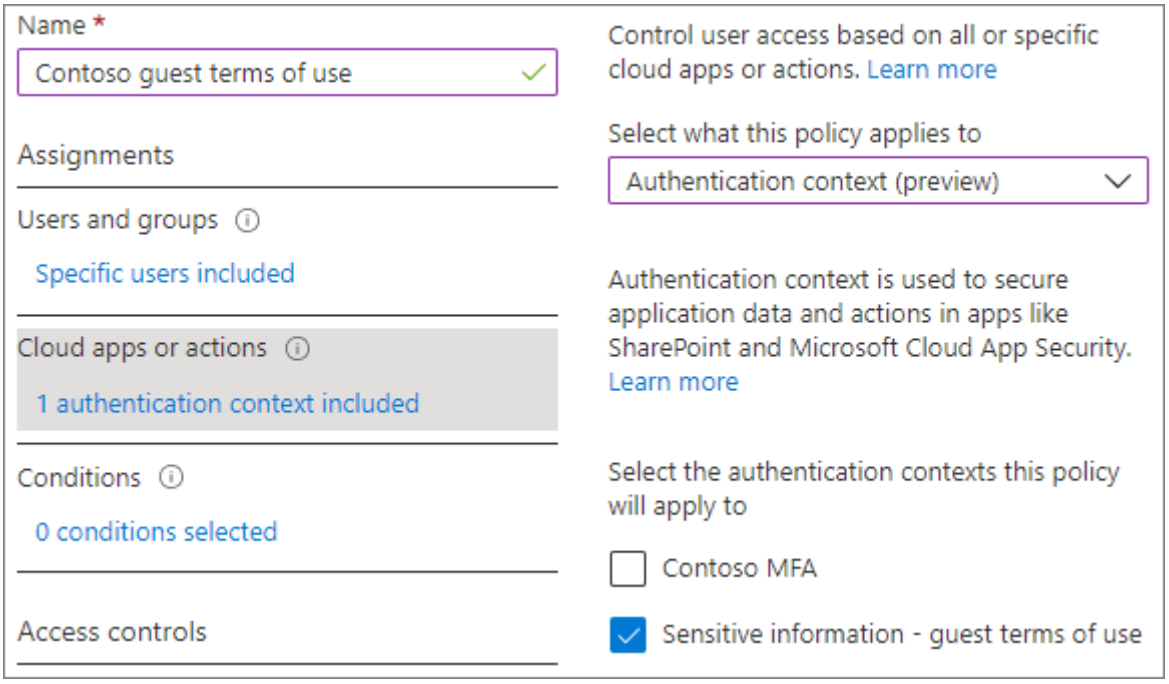
4. Select **Save**.

Create a Conditional Access policy

Next, create a Conditional Access policy that applies to that authentication context and requires guests to agree to terms of use as a condition of access.

To create a Conditional Access policy:

1. In Microsoft Entra Conditional Access, select **New policy**.
2. Enter a name for the policy.
3. On the **Users and groups** tab, choose the **Select users and groups** option, and then select the **Guest or external users** check box.
4. Choose **B2B collaboration guest users** from the dropdown.
5. On the **Cloud apps or actions** tab, under **Select what this policy applies to**, choose **Authentication context**, and select the check box for the authentication context that you created.



6. On the **Grant** tab, select the check box for the terms of use that you want to use, and then select **Select**.
7. Choose if you want to enable the policy, and then select **Create**.

Apply the authentication context directly to a site

You can directly apply an authentication context to a SharePoint site by using the Set-SPOSite PowerShell cmdlet.

> **Note**
>
> This capability requires a Microsoft 365 E5 or Microsoft SharePoint Advanced Management license.

In the following example, you apply the authentication context you created earlier to a site called "research."

PowerShell

```
Set-SPOSite -Identity https://contoso.sharepoint.com/sites/research -
ConditionalAccessPolicy AuthenticationContext -AuthenticationContextName "Sensitive
information - guest terms of use"
```

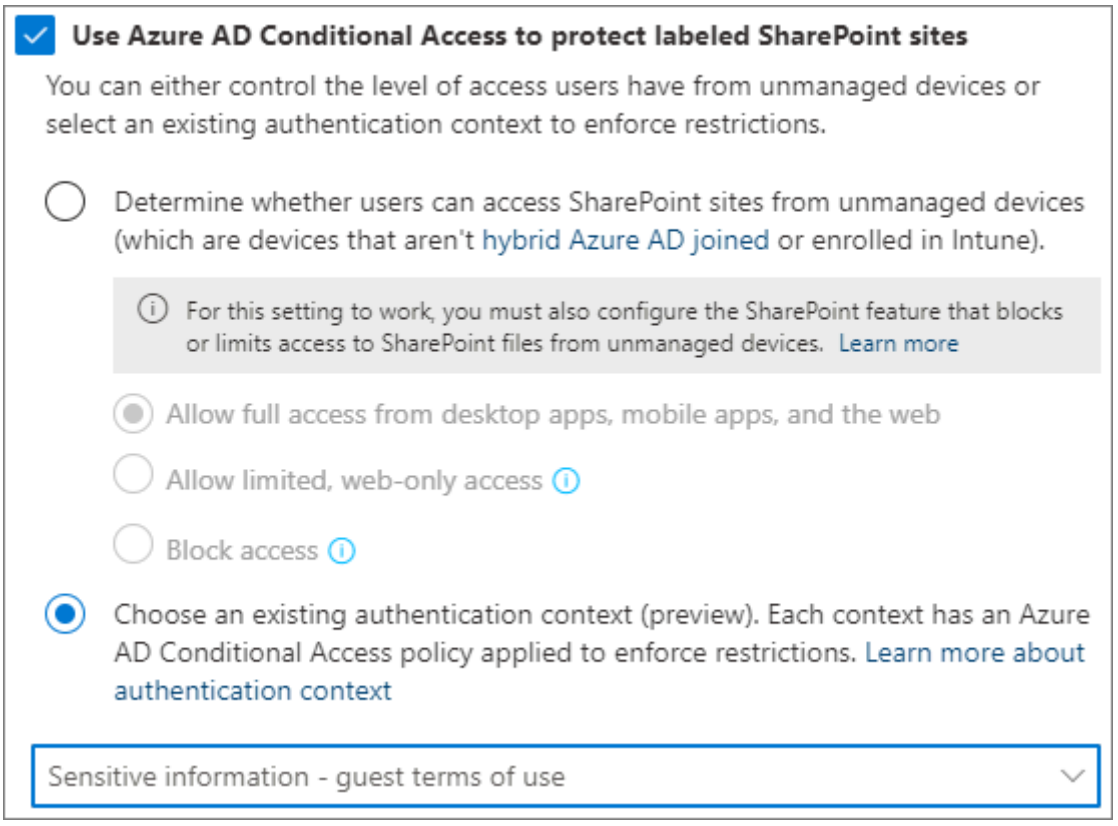
Set a sensitivity label to apply the authentication context to labeled sites

If you want to use a sensitivity label to apply the authentication context, update a sensitivity label (or create a new one) to use the authentication context.

> **Note**
>
> Sensitivity labels require Microsoft 365 E5 or Microsoft 365 E3 plus the Advanced Compliance license.

To update a sensitivity label

1. In the Microsoft Purview portal, on the **Information protection** tab, select the label that you want to update and then select **Edit label**.
2. Select **Next** until you are on the **Define protection settings for groups and sites** page.
3. Ensure that the **External sharing and Conditional Access settings** check box is selected, and then select **Next**.
4. On the **Define external sharing and device access settings page**, select the **Use Microsoft Entra Conditional Access to protect labeled SharePoint sites** check box.
5. Select the **Choose an existing authentication context** option.
6. In the dropdown list, choose the authentication context that you want to use.



7. Select **Next** until you are on the **Review your settings and finish** page, and then select **Save label**.

After you update the label, guests accessing a SharePoint site (or the **Files** tab in a team) with that label must agree to the terms of use before gaining access to that site.

Block background apps

If you set authentication context on a site, admins can choose to prevent background apps from accessing that site for the apps assigned with that authentication context in a Conditional Access policy. You can configure a Conditional Access policy such that a specific authentication context can be assigned to chosen application principals (non-Microsoft applications). You need to explicitly turn on this feature by using the following cmdlet. You should have at least one Conditional Access policy with an application principal configured.

PowerShell

```
Set-SPOTenant -BlockAppAccessWithAuthenticationContext $false/$true (default false)
```

Third-party app integration

Third-party apps that use sites with authentication context attached need to be able to handle claims challenge. See Developer guide to Conditional Access authentication context.

See also

Use sensitivity labels to protect content in Microsoft Teams, Microsoft 365 groups, and SharePoint sites

Conditional Access: Cloud apps, actions, and authentication context

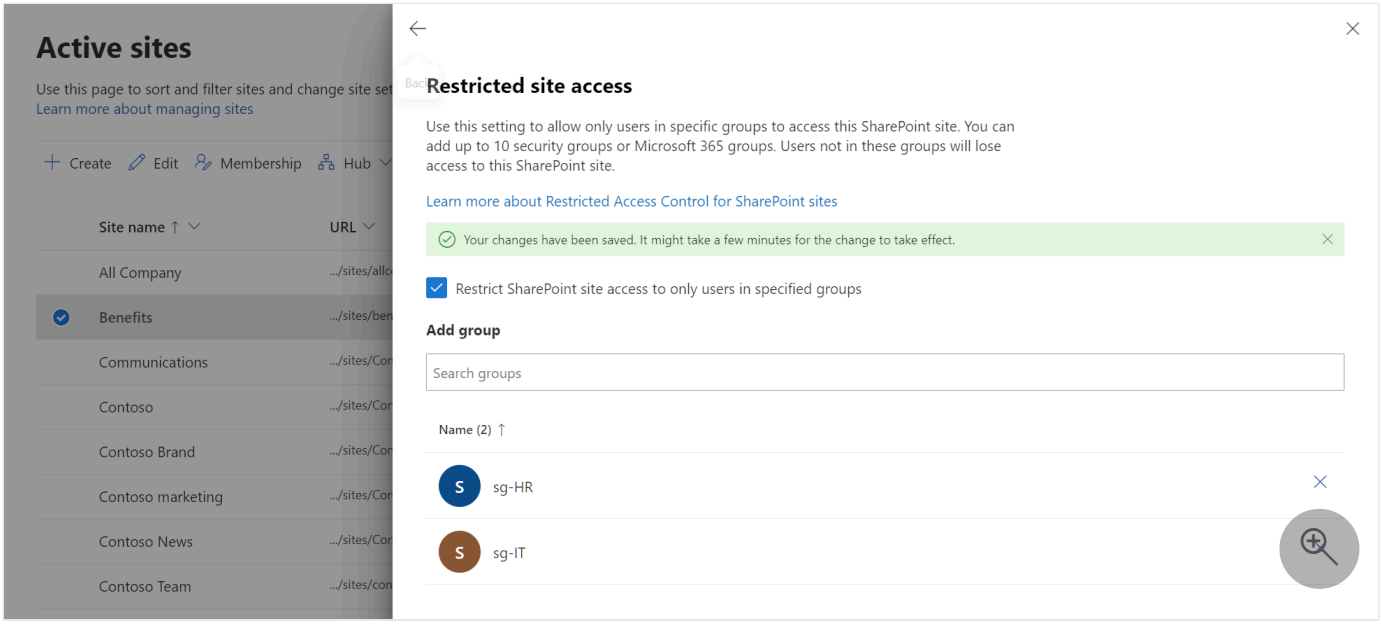
Microsoft 365 licensing guidance for security & compliance

Last updated on 07/28/2026

Restrict SharePoint site access with Microsoft 365 groups and Microsoft Entra security groups

Restricted site access control (also referred to as *restricted access control* or *site access restriction*) helps prevent oversharing by designating access of SharePoint sites and its content to users in the specific control group. Users not in the specified group can't access the site or its content, even if they had prior permissions or a shared link. You can apply this policy on Microsoft 365 group-connected, Teams-connected, nongroup connected sites, and OneDrive by using Microsoft 365 groups or Microsoft Entra security groups.

Site access restriction policy take effect when a user attempts to open a site or access a file. Copilot and organization wide search results also honor the policy. Users with direct permissions to the file but not in the specified control group will not be able to view the file in search or Copilot experiences.



> **Note**
>
> Shared channel sites and private channel sites are separate site collections from the Microsoft 365 group-connected site used by standard channels. Restricted site access policies applied to a team-connected site don't automatically apply to its shared or private

channel sites. Configure site access restriction separately for each shared or private channel site.

Prerequisites for restricted site access

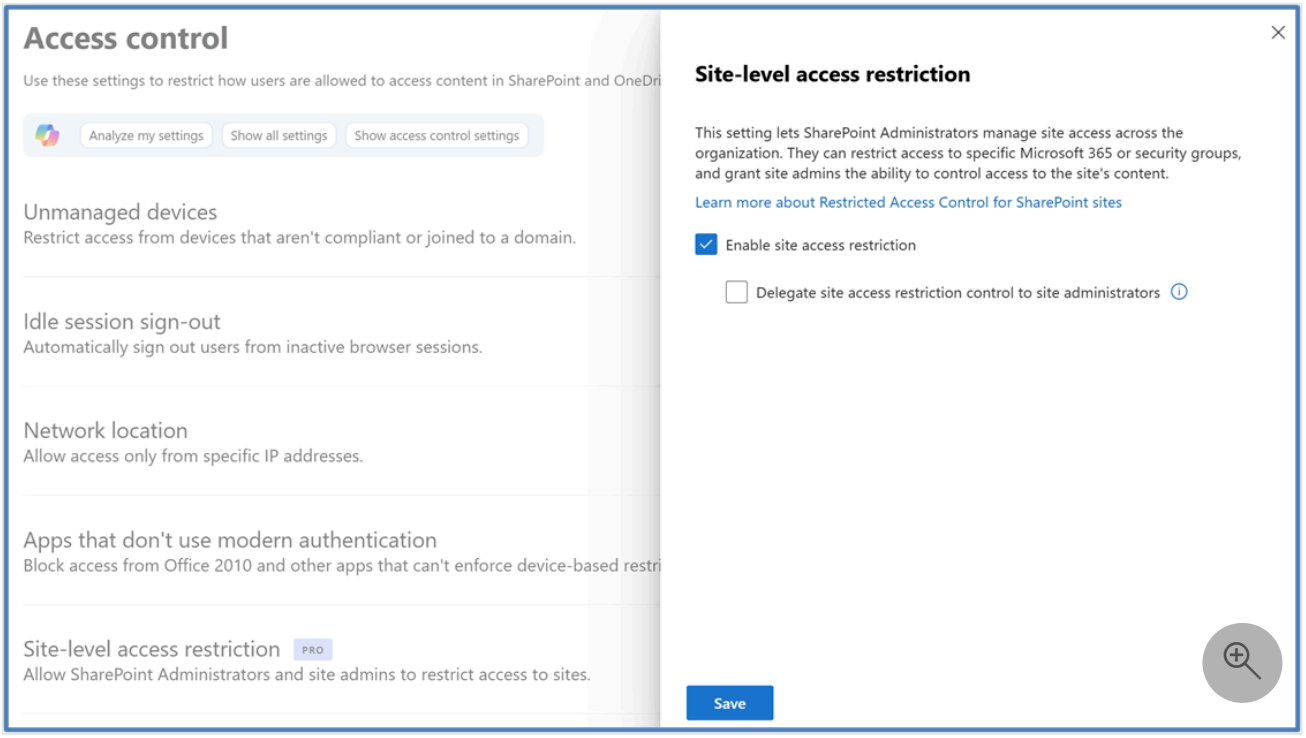
See Prerequisites for SharePoint Advanced Management.

Enable site-level access restriction for your organization

You must enable site-level access restriction for your organization before you can configure it for individual sites. You can also delegate site access restriction control to all the site admins of your organization.

To enable site-level access restriction for your organization in the SharePoint admin center, follow these steps:

1. Expand **Policies** and select **Access control**.
2. Select **Site-level access restriction**.
3. Select **Allow access restriction** and then select **Save**.



To enable site-level access restriction for your organization using PowerShell, run the following command:

```powershell
Set-SPOTenant -EnableRestrictedAccessControl $true
```

It might take up to one hour for the command to take effect.

Delegate management of restricted access control to site admins

As a SharePoint administrator, you can also delegate management of restricted access control to site administrators. If they update the policy, they need to provide appropriate justification on why the policy is being updated.

By default, the delegation is turned off. If you decide to enable it, run the following command:

```powershell
Set-SPOTenant -DelegateRestrictedAccessControlManagement $true
```

Once restricted access control is delegated to all the site admins, they can manage the policy.

Check status of delegate management of restricted access control to site admins

To check the delegation status, run the following command:

```powershell
Get-SPOTenant | Select-Object DelegateRestrictedAccessControlManagement
```

> **Note**
>
> For Microsoft 365 Multi-Geo users, run this command separately for each desired geo-location.

Restrict access to all SharePoint sites using Microsoft 365 group or Microsoft Entra security groups

You can restrict access to a SharePoint site by specifying Microsoft Entra security groups or Microsoft 365 groups as the restricted access control group. The control group should include the users who are allowed access to the site and its content.

For a site, you can configure up to 10 Microsoft Entra security groups or Microsoft 365 groups. Once you apply the policy, users in the specified group who have access permission to the content are granted access.

> **Important**
>
> - Adding people to the restricted access control group (Microsoft Entra security group or Microsoft 365 group) doesn't automatically give the users access permission to the site or the content. For a user to access the content protected by this policy, the user needs both the site or content access permission and be a member of the restricted access control group.
> - You can also use dynamic security groups as a restricted access control group if you want to base group membership on user properties.

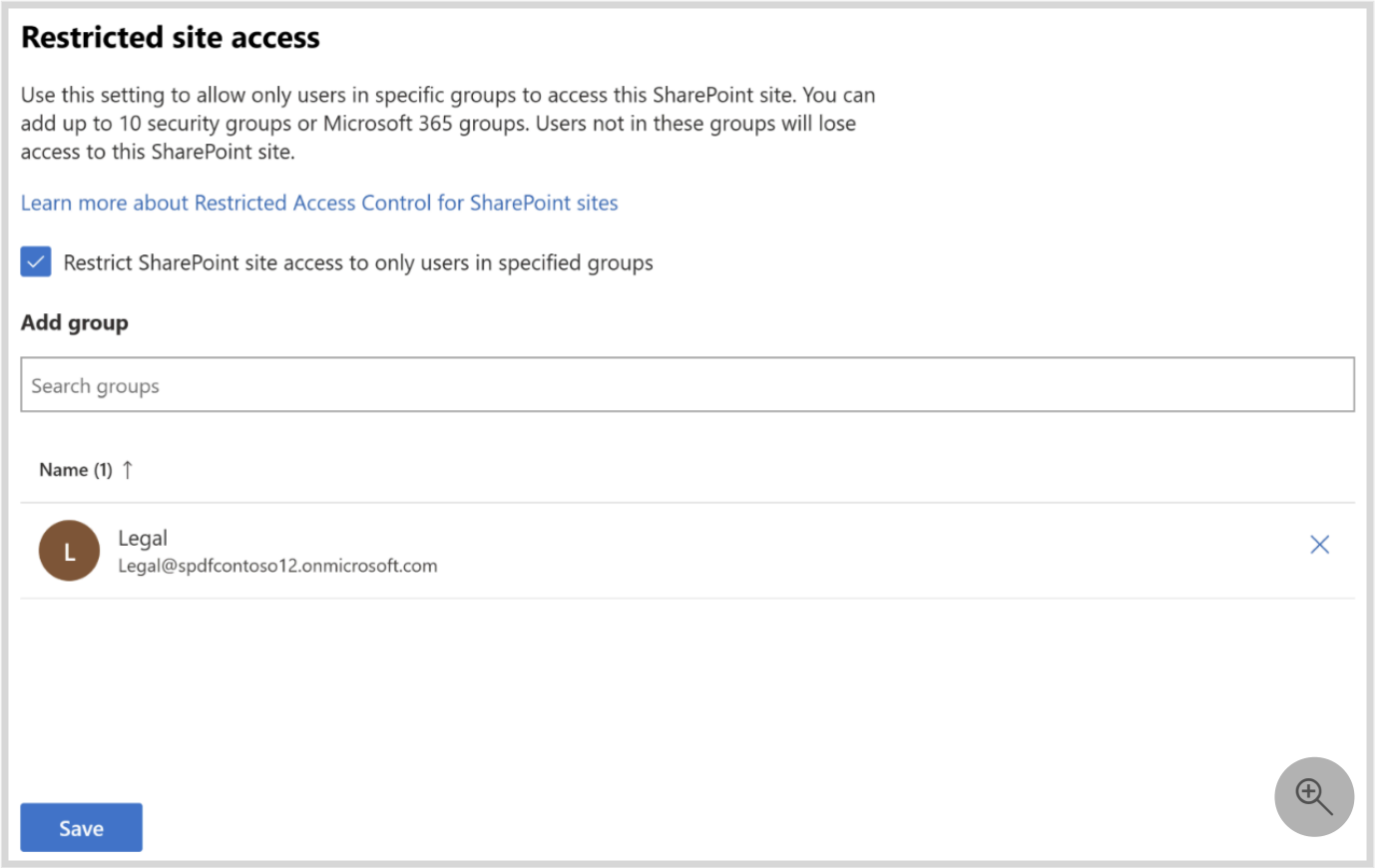
Manage site access for a site

To manage site access for a site, follow these steps:

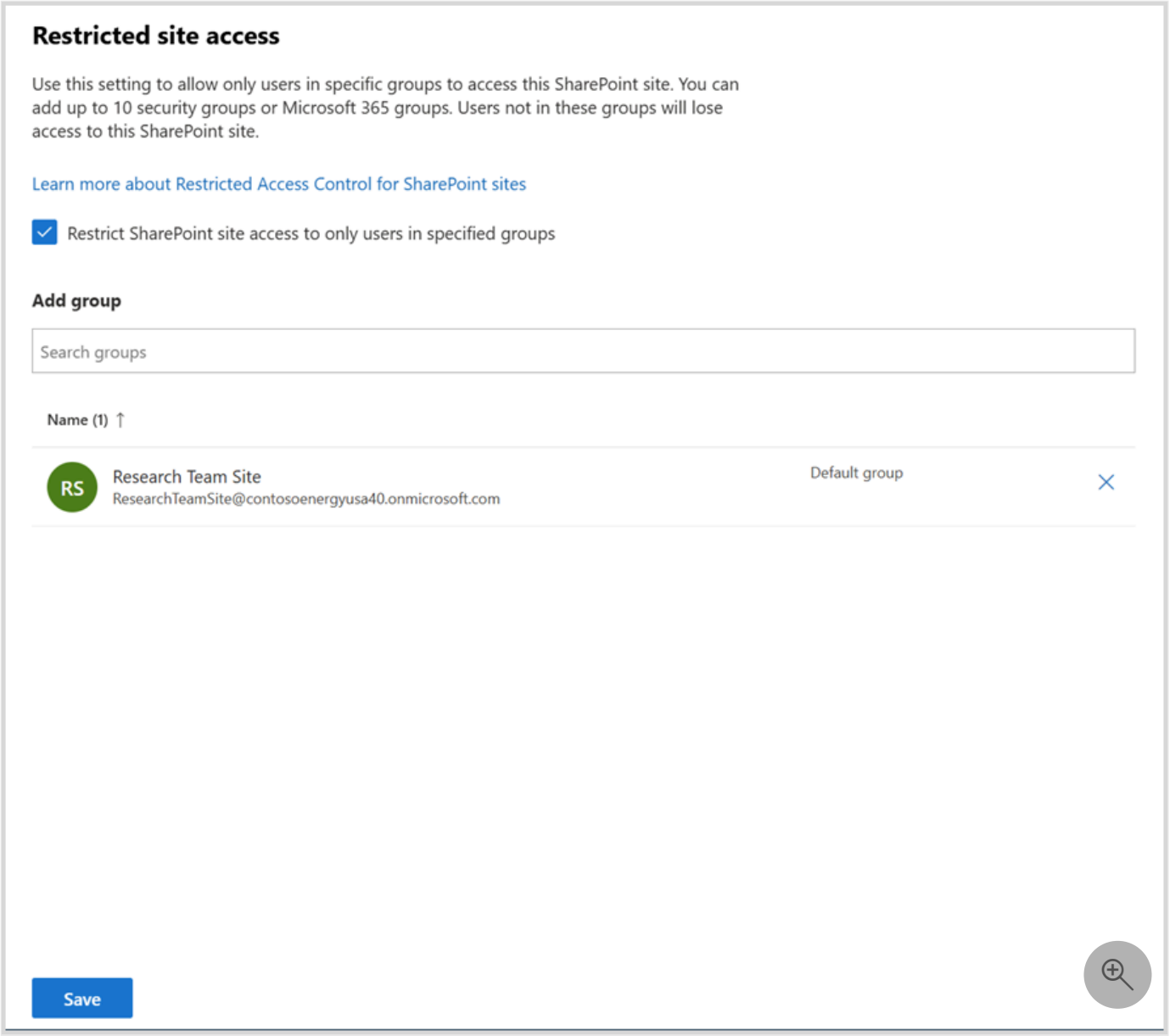
1. In SharePoint admin center, expand **Sites** and select **Active sites**.
2. Select the site you want to manage. The site details panel appears.
3. In the **Settings** tab, select **Edit** in the **Restricted site access** section.
4. Select the **Restrict SharePoint site access to only users in specified groups** check box.
5. Add or remove your security groups or Microsoft 365 groups and select **Save**.

Apply site access restriction to a site

To apply site access restriction to the site, you must add at least one group to the site access restriction policy.



For a group connected site, the Microsoft 365 group connected to the site is the default restricted access control group. You can choose to keep this group and add more Microsoft 365 or Microsoft Entra Security groups as a restricted access control group.



> **Note**
>
> - This behavior doesn't apply to shared channel sites or private channel sites because they aren't connected to the parent team's Microsoft 365 group. Configure restricted access control separately for those sites. See the section Shared and private channel sites (in this article).
> - A **Default group** tag is listed for the Microsoft 365 group connected to the site, as shown in the preceding image.

Manage site access restriction by using PowerShell

To manage site access restriction for a SharePoint site by using PowerShell, use the PowerShell commands described in this section.

Enable site access restriction

PowerShell

```
Set-SPOSite -Identity <siteurl> -RestrictedAccessControl $true
```

Add group

PowerShell

```
Set-SPOSite -Identity <siteurl> -AddRestrictedAccessControlGroups <comma separated
group GUIDS>
```

Edit group

PowerShell

```
Set-SPOSite -Identity <siteurl> -RestrictedAccessControlGroups <comma separated group
GUIDS>
```

View group

PowerShell

```
Get-SPOSite -Identity <siteurl> | Select RestrictedAccessControl,
RestrictedAccessControlGroups
```

Remove group

PowerShell

```
Set-SPOSite -Identity <siteurl> -RemoveRestrictedAccessControlGroups <comma separated
group GUIDS>
```

Reset site access restriction

PowerShell

```
Set-SPOSite -Identity <siteurl> -ClearRestrictedAccessControl
```

Search and Copilot experience

Restricted site access control policy is honored in organization-wide search experiences and Microsoft 365 Copilot experiences. Users who are denied access due to this policy can't view content from this site in either search or Microsoft 365 Copilot experiences. It can take some time for search and Copilot experiences to reflect Restricted site access control policies. The search index update latency depends on the number of items in a site. For example, larger sites with more items can take longer for Restricted site access control policies to be honored in search and Copilot experiences.

Shared and private channel sites

Shared and private channel sites are separate from the Microsoft 365 group-connected site that standard channels use. Because shared and private channel sites aren't connected to the parent team's Microsoft 365 group, Restricted access control policies configured on the team-connected site don't apply to those channel sites. You must enable site access restriction for each shared or private channel site separately as nongroup connected sites.

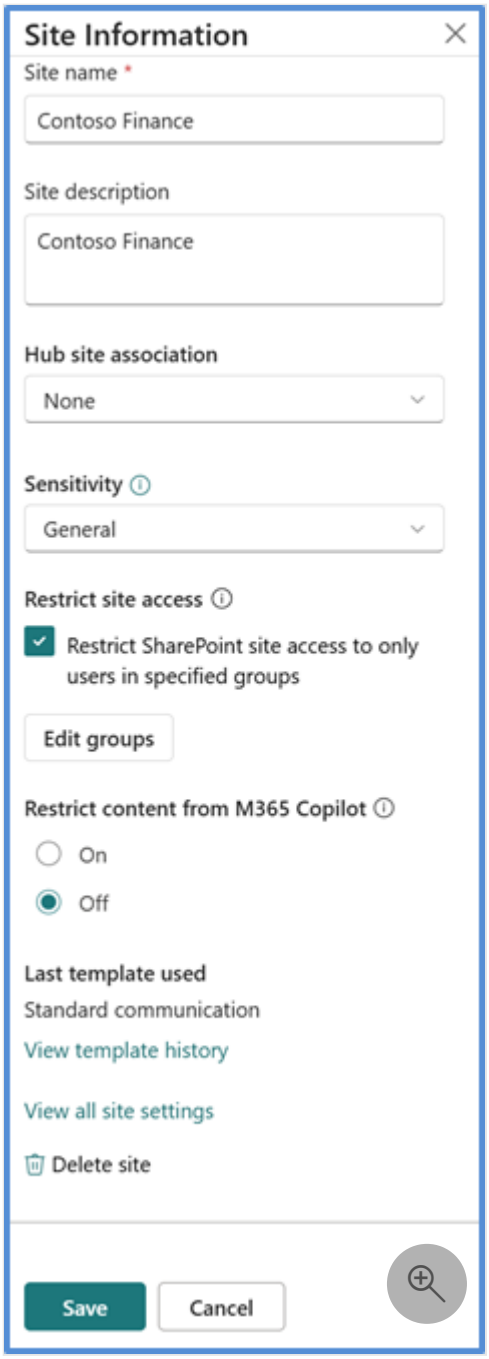
For shared channel sites, restricted access control applies only to internal users in the resource tenant. External participants accessing the shared channel from another tenant aren't evaluated against the restricted access control policy. Their access continues to be determined by the permissions granted to the shared channel and the associated SharePoint site.

This means that adding an external shared channel participant to, or removing them from, a restricted access control group doesn't affect their ability to access the shared channel site.

> **Important**
>
> Adding people to the security group or Microsoft 365 group doesn't give users access to the channel in Teams. Add or remove the same users of the Teams channel in Teams and the security group or Microsoft 365 group, so users have access to both Teams and SharePoint sites.

Site admin experience

After you delegate the site access restriction control to site admins, they can configure the site access restriction setting at the **Site Information** panel.

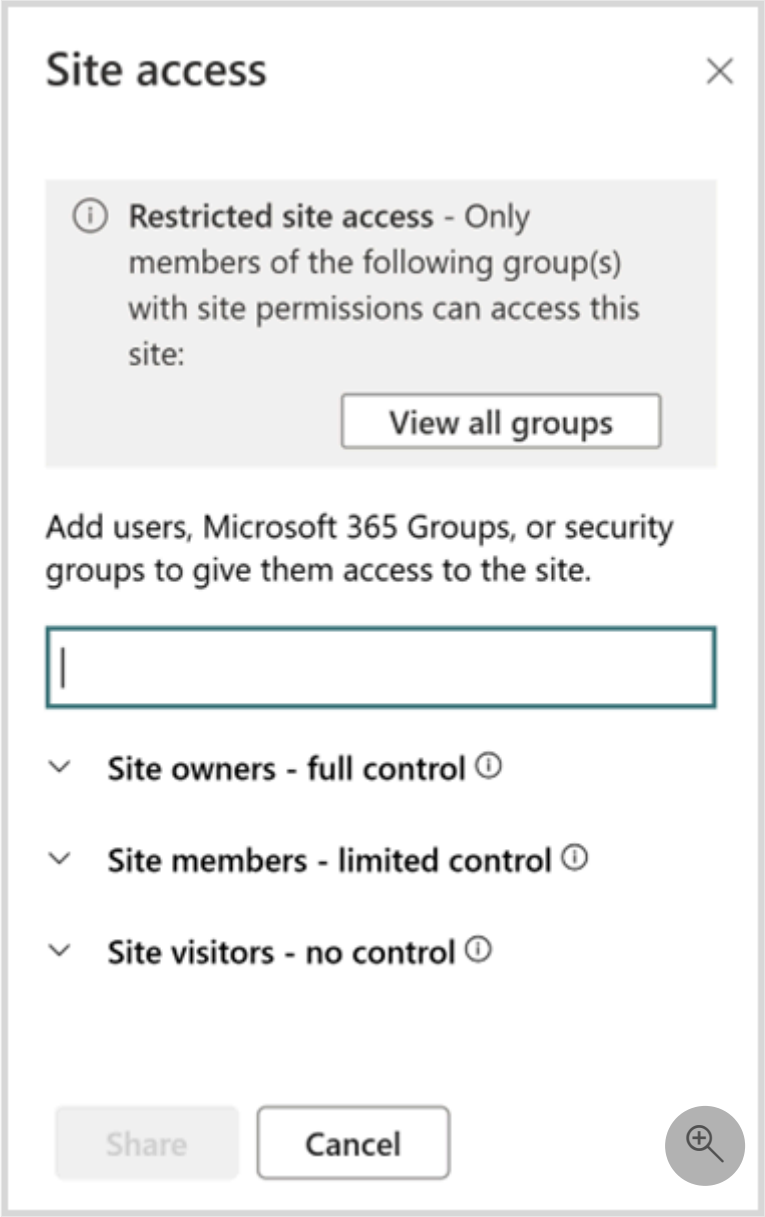


Restrict access to a SharePoint site

1. Limit who can access a site by using Microsoft Entra security groups or Microsoft 365 groups.
2. Add the groups that contain the users who should have access.
3. Add up to 10 groups for each site.
4. When you save the site access restriction setting configuration, only users in those groups and users who already have permission to the content can access the site.
5. Provide justification whenever you update the site access restriction setting.

Site owner experience

After you apply the policy to the site, the **Site access** panel displays the policy status and all configured control groups for site owners, in addition to the **Site Information** and **Permissions** panels.



Auditing

The Microsoft Purview portal provides audit events that help you monitor site access restriction activities. The system logs audit events for the following activities:

- Applying site access restriction for a site
- Removing site access restriction for a site
- Changing site access restriction groups for a site
- Site admin's justification for updating site access restriction

Insights

Restricted site access policy insights

As an IT administrator, you can view the following reports to gain more insight about SharePoint sites protected with restricted site access policy:

- Sites protected by restricted site access policy (`RACProtectedSites`)
- Details of access denials due to restricted site access policy (`ActionsBlockedByPolicy`)

Reports are currently unavailable for Microsoft 365 operated by 21Vianet, even if you have the required licenses.

> **Note**
>
> It can take a few hours to generate each report.

Sites protected by restricted site access policy report

Run the following commands in SharePoint PowerShell to generate, view, and download the reports.

Generate report

PowerShell

```
Start-SPORestrictedAccessForSitesInsights -RACProtectedSites
```

This command generates a list of sites protected by restricted site access policy.

View report

PowerShell

```
Get-SPORestrictedAccessForSitesInsights -RACProtectedSites -ReportId <Report GUID>
```

The report shows the top 100 sites with the highest page views that are protected by the policy.

Download report

PowerShell

```
Get-SPORestrictedAccessForSitesInsights -RACProtectedSites -ReportId <Report GUID> -
Action Download
```

Run this command as an administrator. The downloaded report is located on the path where the command was run.

Percentage of site protected with restricted site access report

PowerShell

```
Get-SPORestrictedAccessForSitesInsights -RACProtectedSites -ReportId <Report GUID> -
InsightsSummary
```

This report shows the percentage of sites that are protected by the policy out of the total number of sites.

Access denials due to restricted site access policy report

Run the following commands to create, fetch, and view a report for access denials due to restricted site access reports.

Create access denials report

PowerShell

```
Start-SPORestrictedAccessForSitesInsights -ActionsBlockedByPolicy
```

This command creates a new report for fetching access denial details.

Fetch access denials report status

PowerShell

```
Get-SPORestrictedAccessForSitesInsights -ActionsBlockedByPolicy
```

This command fetches the status of the generated report.

Latest access denials in the past 28 days

PowerShell

```
Get-SPORestrictedAccessForSitesInsights -ActionsBlockedByPolicy -ReportId <Report ID>
-Content AllDenials
```

This command gets a list of the most recent 100 access denials that occurred in the past 28 days.

View list of top users who were denied access

PowerShell

```
Get-SPORestrictedAccessForSitesInsights -ActionsBlockedByPolicy -ReportId <Report ID>
-Content TopUsers
```

This command gets a list of the top 100 users who received the most access denials.

View list of top sites that received the most access denials

PowerShell

```
Get-SPORestrictedAccessForSitesInsights -ActionsBlockedByPolicy -ReportId <Report ID>
-Content TopSites
```

This command gets a list of the top 100 sites that had the most access denials.

Distribution of access denials across different types of sites

PowerShell

```
Get-SPORestrictedAccessForSitesInsights -ActionsBlockedByPolicy -ReportId <Report ID>
-Content SiteDistribution
```

Shows the distribution of access denials across different types of sites.

> **Note**
>
> To view up to 10,000 denials, you must download the reports. Run the download command as an administrator. The downloaded reports are located on the path where you run the command.

Sharing of site and content with users outside of restricted access control groups (opt-in capability)

By default, sharing SharePoint sites and their content doesn't follow the restricted site access policy. The SharePoint administrator can choose to restrict sharing of a site and its content with users who aren't members of the restricted access control group.

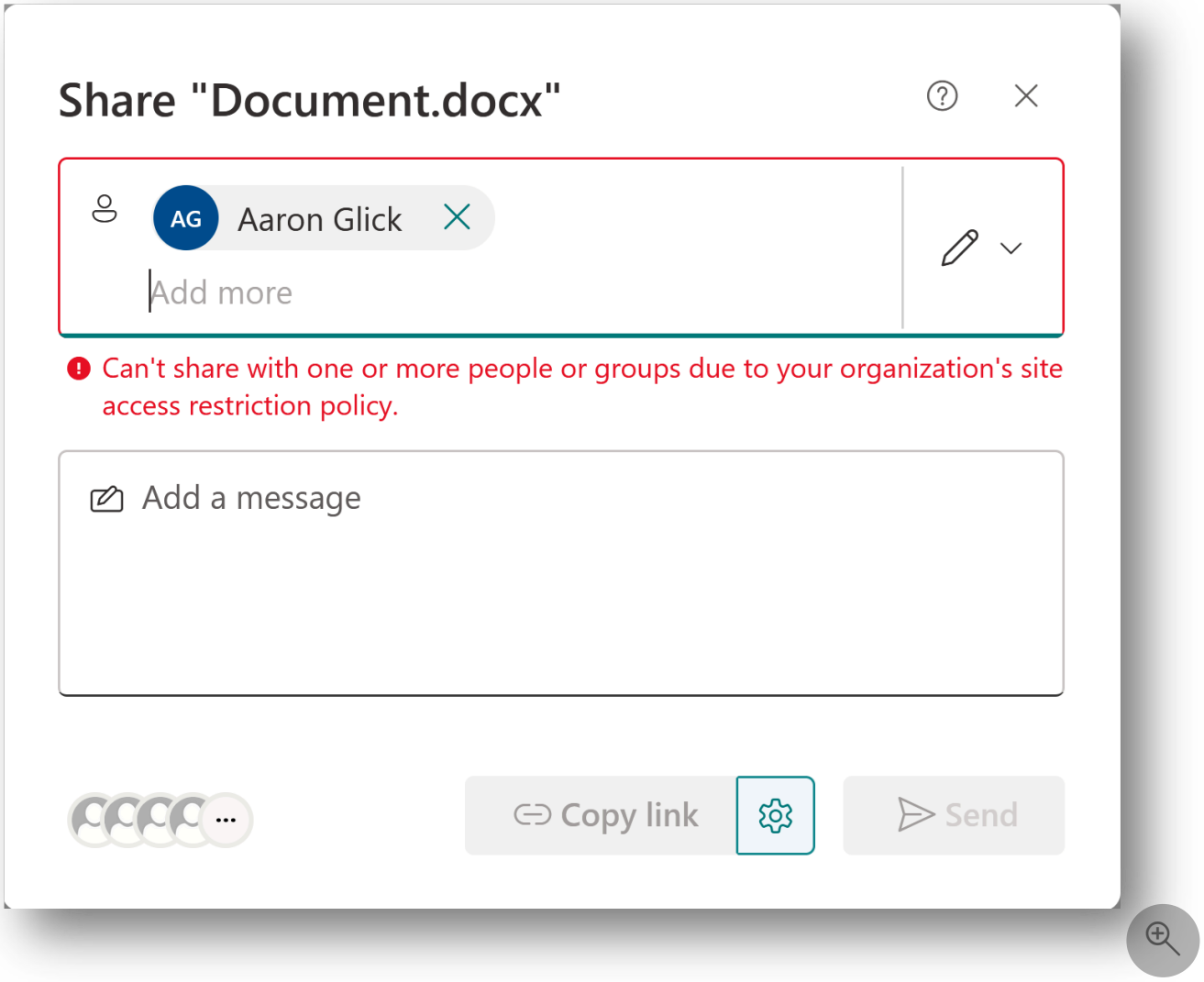
To restrict the sharing capability to users outside of the restricted access control group, run the following PowerShell command in SharePoint Online Management Shell as an administrator:

PowerShell

```
Set-SPOTenant -AllowSharingOutsideRestrictedAccessControlGroups $false
```

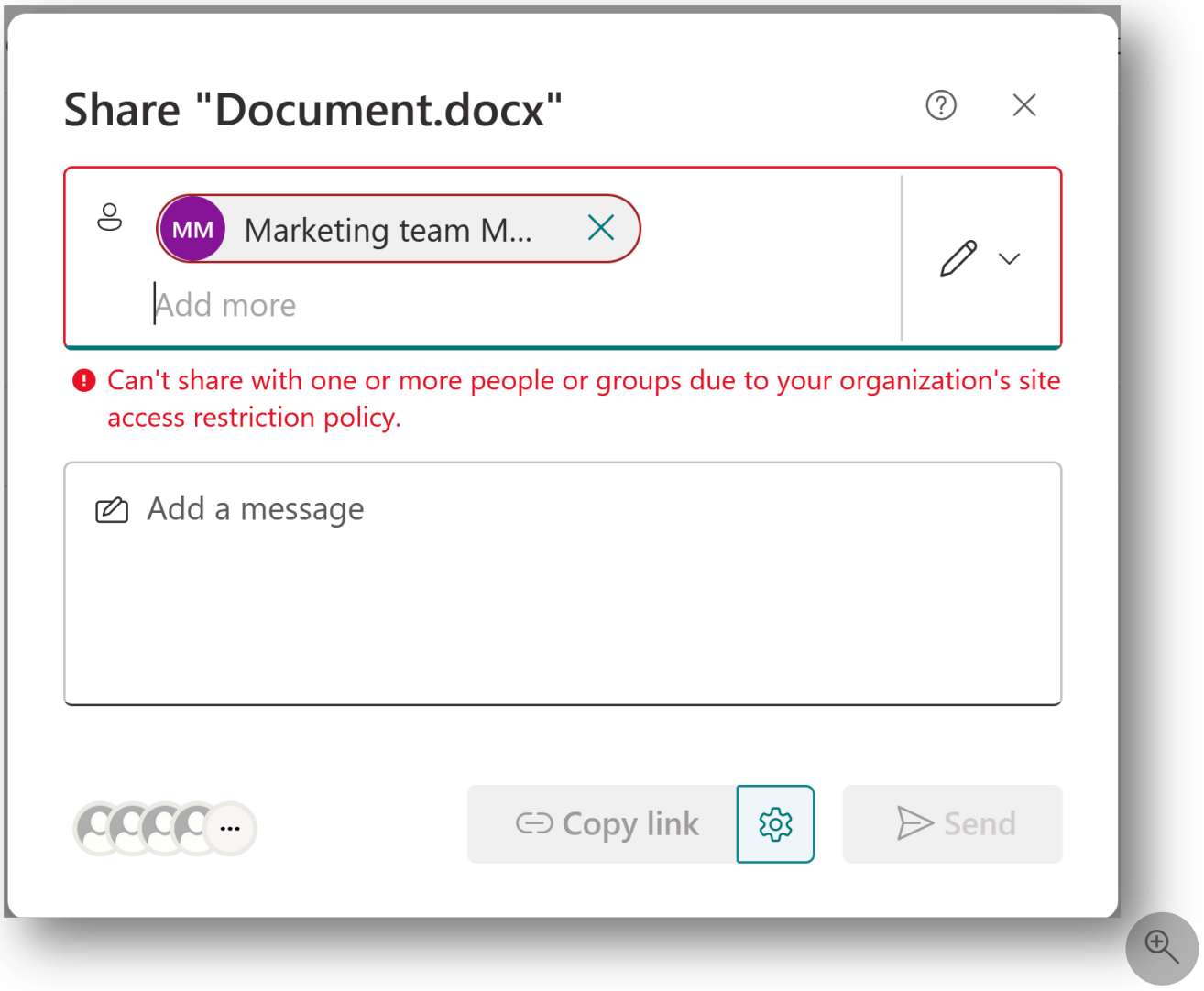
Sharing with users

When you apply the sharing restriction, it blocks sharing for users who aren't members of the restricted access control group.



Sharing with groups

Sharing is allowed with Microsoft Entra Security or Microsoft 365 groups that are part of the restricted access control groups list. Sharing isn't allowed with all other groups, including Everyone except external users or SharePoint groups.



> **Note**
>
> Sharing of a site and its content is now allowed for the nested security groups that are part of the restricted access control groups.

Configure the Learn more link for access denial error page (opt-in capability)

Configure the **Learn more** link to inform users who are denied access to a SharePoint site due to the restricted site access control policy. By customizing this error link, you can provide more information and guidance to your users.

> **Note**

The **Learn more** link is a tenant-level setting that applies to all sites with the restricted access control policy enabled.

To configure the link, run the following command in SharePoint PowerShell:

PowerShell

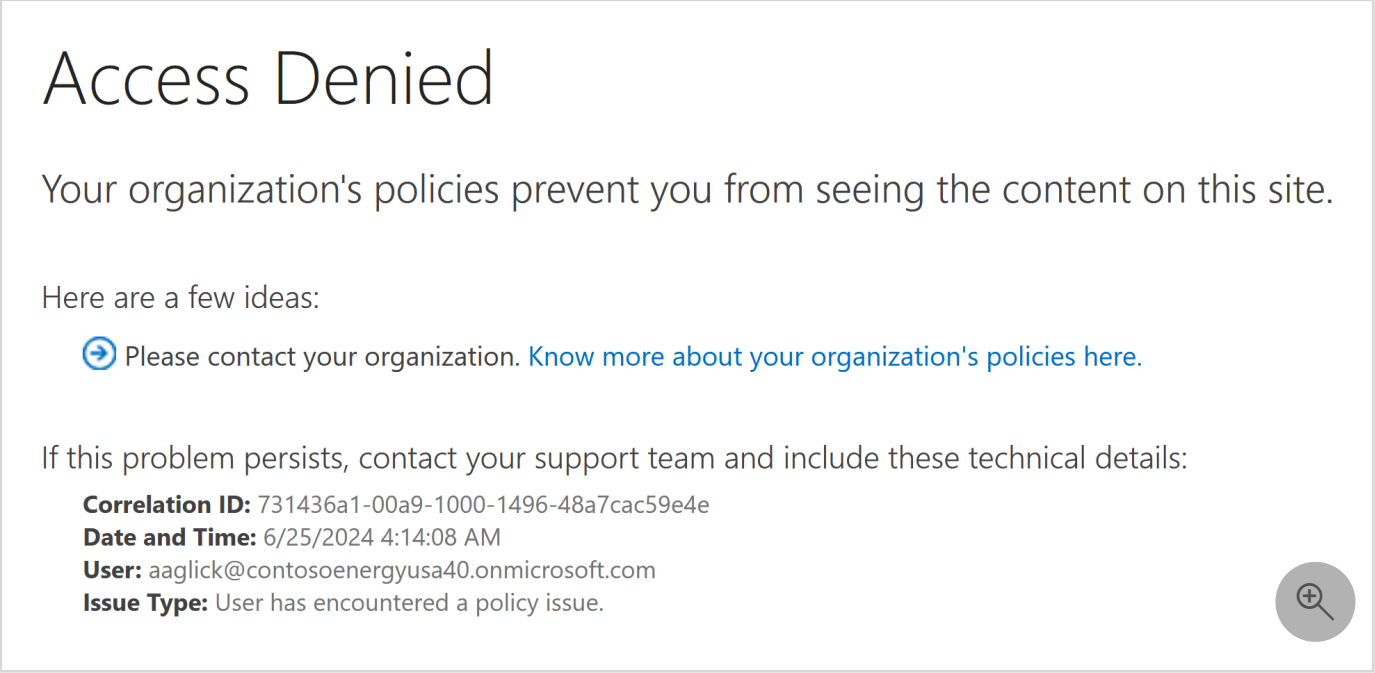
```
Set-SPOTenant -RestrictedAccessControlForSitesErrorHelpLink "<Learn more URL>"
```

To fetch the value of the link, run the following command:

PowerShell

```
Get-SPOTenant | select RestrictedAccessControlForSitesErrorHelpLink
```

The configured **Learn more** link launches when the user selects the **Know more about your organization's policies here** link.



Related articles

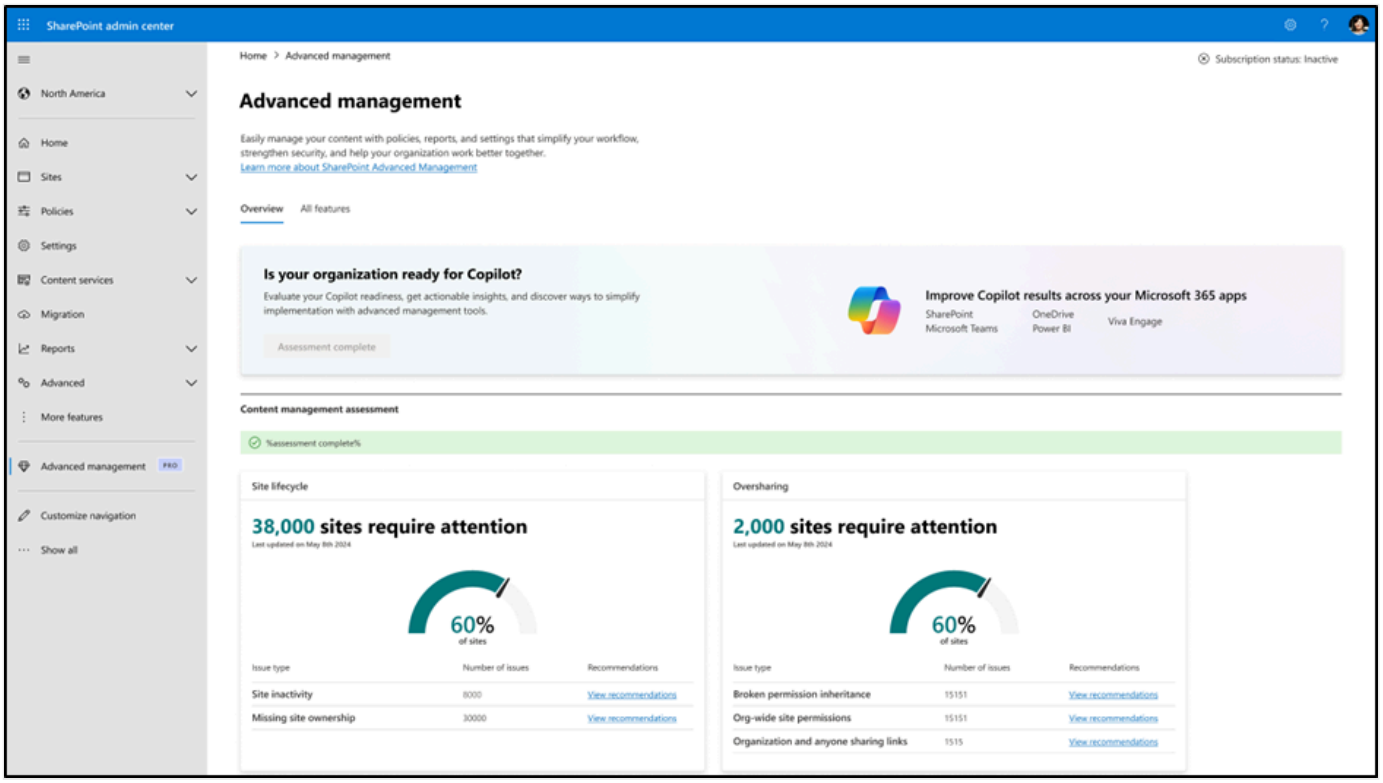
Conditional access policy for SharePoint sites and OneDrive

Data Access Governance reports

Last updated on 07/30/2026

Assess your organization's content management status

SharePoint Advanced Management (SAM) provides a comprehensive set of tools for assessing and improving your organization's content management practices with actionable insights and recommendations. Content Management Assessment is the hub for these capabilities.



What is Content Management Assessment?

Content Management Assessment is a built-in, easy-to-use feature of SharePoint Advanced Management. With just one click, you can quickly check and improve how your organization manages content within SharePoint environments. Content Management Assessment provides a simple, guided process for administrators to:

- Identify potentially overshared content
- Find issues or risks (such as inactive or ownerless sites)
- Define Copilot readiness for the organization
- Ensure compliance and maintain data integrity
- Receive actionable recommendations for remediation
- Track progress over time with recurring assessments

The assessment uses the SharePoint Advanced Management (SAM) toolkit, running a suite of essential reports to surface key findings and categorize sites that might require attention. It makes content governance accessible and actionable, even for admins who might not have deep technical expertise.

Included reports

Currently, the Content Management Assessment includes the following reports:

- **Inactive sites report**: Identifies sites with no activity in the past 180 days.
- **Site ownership report**: Detects sites without owners or with only one owner.
- **Broken inheritance report**: Finds sites where permission inheritance is broken.
- **Unrestricted internal sharing via EEEU (Everyone Except External Users) report**: Locates content shared with all internal users.
- **Unrestricted sharing via sharing links**: Discovers content shared through overly permissive sharing links.

> **Note**
>
> - Depending on the size of the tenant, reports can take between 2 hours and 72 hours to run.
> - Reports run on all sites across the organization. They don't take any action without the admin's consent.

Why use Content Management Assessment?

Organizations face increasing complexity in managing content across large Microsoft 365 tenants. Common challenges include:

- Uncertainty about where to start with governance.
- Difficulty identifying whether there are actual problems or risks.
- Lack of clarity on whether existing governance measures are sufficient.
- The need for ongoing monitoring and improvement.

Content Management Assessment addresses these challenges by:

- **Automating discovery**: Automatically discover and categorize potentially impacted sites without manual intervention.

- **Clear, actionable findings**: Provide a clear list of issues with specific recommended next steps for each finding.
- **Eliminating manual work**: Reduce the need for custom scripts or manual audits, which can be time-consuming and error-prone.
- **On-demand reassessment**: Allow administrators to rerun the assessment monthly to ensure continuous improvement and compliance.

What do you need to access Content Management Assessment?

See SharePoint Advanced Management prerequisites.

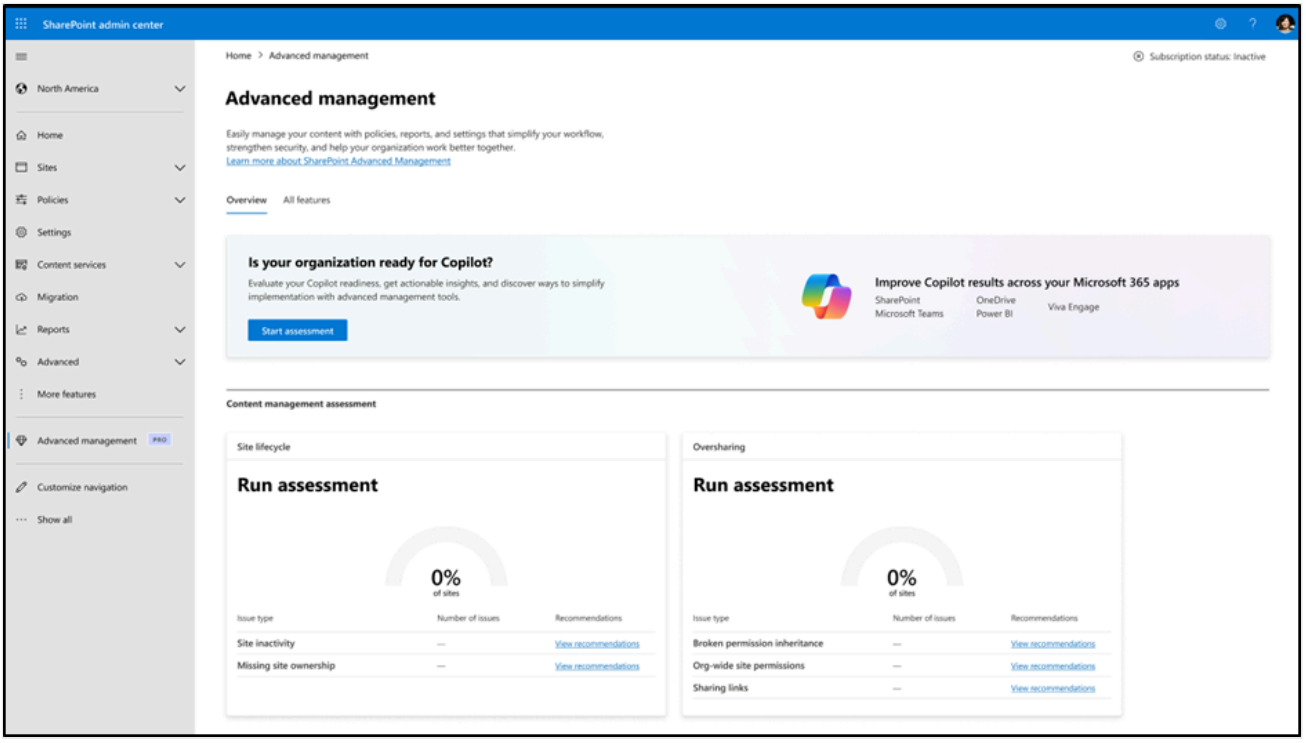
Where to find Content Management Assessment

You can access Content Management Assessment in the SharePoint Admin Center:

1. Sign in to the SharePoint admin center.

2. In the navigation pane, select **Advanced Management**.

3. Look for the new assessment starting screen, as shown in the following image:



   (Previously, the menu-based view was available under **All Features**).

4. Select **Start assessment**.

The assessment automatically runs the relevant SAM reports, analyzes the results, and presents findings in a user-friendly dashboard, which includes:

- Visual summary of impacted sites
- Report findings, which list impacted sites, specific findings, and recommended actions for remediation. You can select each of the findings to see more details and related Microsoft Learn documentation to address the issue.
- The latest guidelines and documentation related to these policies.

Next steps after running the assessment

1. **Review findings**: Examine the list of sites flagged as potentially impacted. The dashboard shows both the number and details of these sites.

2. **Take action**: For each finding, follow the recommended steps provided. These steps might include:

    - Creating or adjusting site policies, such as for potential oversharing, inactivity, or ownership.
    - Using built-in tools to fix problems.
    - Consulting linked documentation for further guidance.

3. **Monitor progress**: Rerun the assessment every 30 days to track improvements and catch new problems.

Last updated on 05/12/2026

Block download policy for SharePoint sites and OneDrive

As a SharePoint Administrator in Microsoft 365, you can use the PowerShell (Set-SPOSite) to block the download of files from SharePoint sites or OneDrive. This feature allows you to control access without using Microsoft Entra Conditional Access policies. You can set this feature for individual sites, but not at the organization level.

When you deploy a policy to block downloads from SharePoint sites or OneDrive, it also prevents users from moving files to other SharePoint sites. File moves are also blocked through other means, such as by using Power Automate or Quick Steps.

Blocking file downloads allows users to remain productive while reducing the risk of accidental data loss. Users have browser-only access with no ability to download, print, or sync files. They also can't access content through apps, including the Microsoft 365 Apps (like Word, Excel, PowerPoint, and so on). When web access is limited, users see this message at the top of sites, "Your organization doesn't allow you to download, print, or sync from this site. For help, contact your It department."

You can also block the download of Microsoft Teams meeting recording files. See Block the download of Teams meeting recording files from SharePoint or OneDrive.

Before you begin

Make sure your organization meets the SharePoint Advanced Management prerequisites, including requirements for SharePoint Online PowerShell module.

Use PowerShell to set a block downloads policy

In PowerShell, run the following command:

PowerShell

```
Set-SPOSite -Identity <SiteURL> -BlockDownloadPolicy $true
```

Here's an example showing a site URL:

PowerShell

```
Set-SPOSite -Identity https://contoso.sharepoint.com/sites/research -
BlockDownloadPolicy $true
```

To apply this command to OneDrive, change the URL, as shown in the following example:

PowerShell

```
Set-SPOSite -Identity https://contoso-my.sharepoint.com/personal/John -
BlockDownloadPolicy $true
```

You can use certain parameters with this command, as shown in the following examples:

Example 1: Exclude site owners from the policy so they can download content from the site

PowerShell

```
Set-SPOSite -Identity <SiteURL> -BlockDownloadPolicy $true -
ExcludeBlockDownloadPolicySiteOwners $true
```

Example 2: Exclude users in specific groups using group IDs so they can download content from the site

PowerShell

```
Set-SPOSite -Identity <SiteURL> -BlockDownloadPolicy $true -
ExcludedBlockDownloadGroupIds <comma separated group IDs>
```

Example 3: Exclude users in specific groups by group name so they can download content from the site

PowerShell

```
Set-SPOSite -Identity <SiteURL> -BlockDownloadPolicy $true -
ExcludeBlockDownloadSharePointGroups <comma separated group names>
```

Example 4: Mark a site as read-only in addition to preventing downloads from the site

PowerShell

```
Set-SPOSite -Identity <SiteURL> -BlockDownloadPolicy $true -
ReadOnlyForBlockDownloadPolicy $true`
```

Example 5: Attach the block download policy to a site sensitivity label

PowerShell

```
Set-Label -Identity 'Internal' -AdvancedSettings @{BlockDownloadPolicy="true" |
"false" }
```

Understand how blocking downloads can affect apps

Blocking download might affect the user experience in some apps, including some Office apps. We recommend that you turn on the policy for some users and test the experience with the apps used in your organization. In Office, make sure to check the behavior in Power Apps and Power Automate when your policy is on.

> **Note**
>
> Apps that run in "app-only" mode in the service, like antivirus apps and search crawlers, are exempted from the policy.
>
> If you're using classic SharePoint site templates, site images might not render correctly. This issue can occur because the policy prevents the original image files from being downloaded to the browser.

Need more help?

SharePoint Question & Answers

Related article

Configure a default sensitivity label for a SharePoint document library

---

Last updated on 05/14/2026

Generate App insights reports to monitor non-Microsoft applications

App insights is a SharePoint Advanced Management feature that lets IT administrators gain insights on the various non-Microsoft applications registered to your Microsoft Entra admin center and how they access your SharePoint content. This report can help you maintain and protect the integrity of your content.

The report is based on the Microsoft audit data logged when a non-Microsoft application accesses content through the following set of events:

- `FileAccessed`
- `FileDownloaded`
- `FileModified`
- `FileUploaded`

Prerequisites to generate App insights reports

See SharePoint Advanced Management prerequisites, including requirements for SharePoint Online PowerShell module.

App insights reports in SharePoint admin center

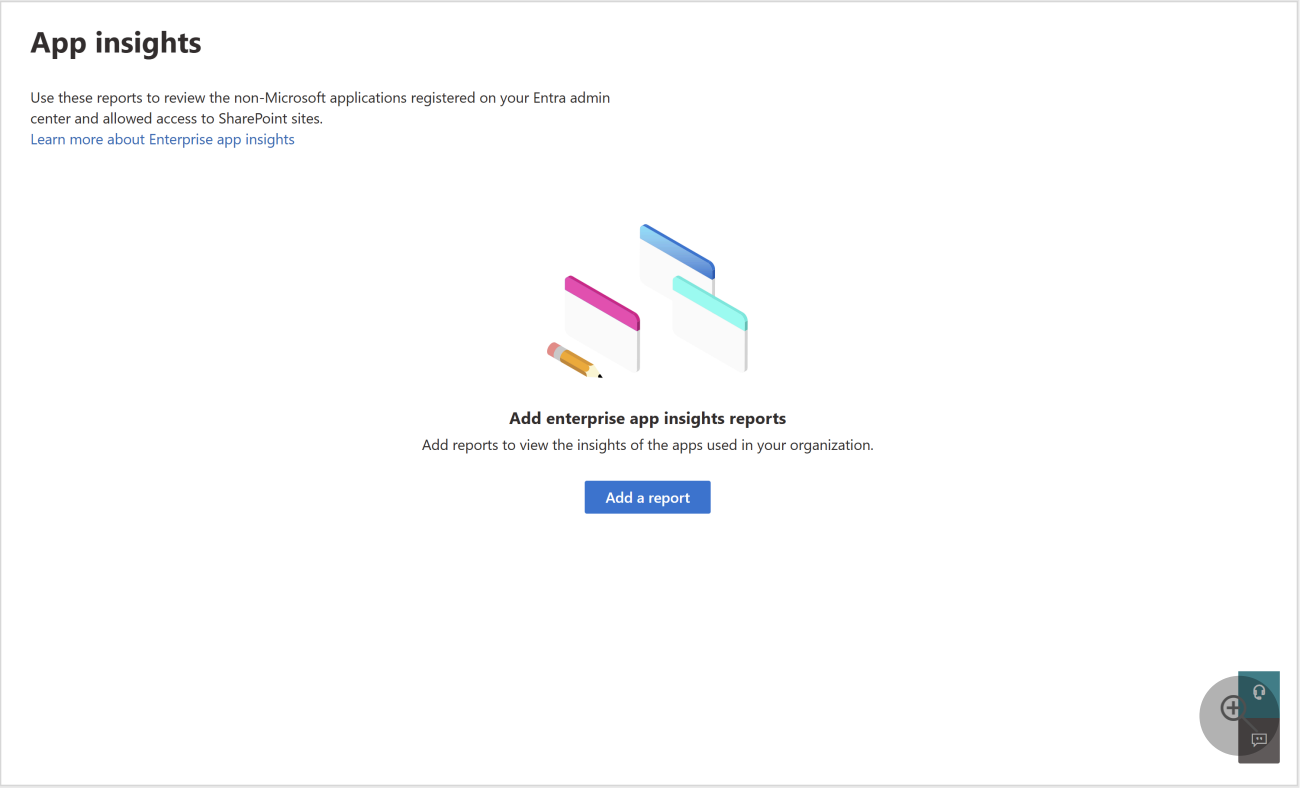
Data collection for Enterprise App Insight report

> **Important**
>
> As a one time activity you will see a pop up on the UI to enable data collection for 'Enterprise App Insight' reports, so that the product starts to collect the relevant audit data to build this report. Once enabled, the reports can be generated 24 hours later and contains data from the time of data collection. Data is stored for 28 days. If no reports are generated even once in three months, data collection is paused and should be enabled again.

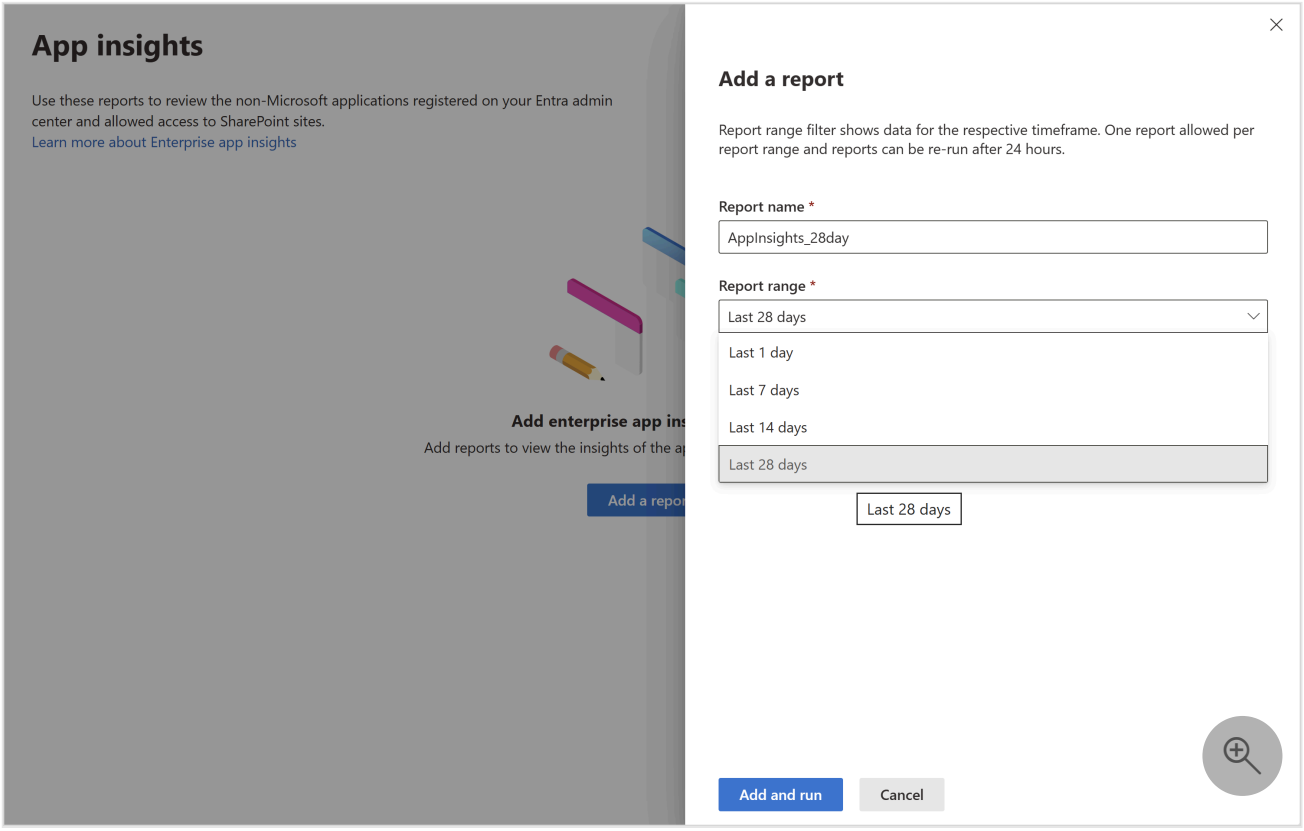
Create report

1. In to SharePoint admin center, in the navigation pane, expand **Reports** and then select **App insights**.

2. Once on the **App insights** landing page, select **Add a report** to generate a new report.



3. Under **Report range**, you can specify and filter data from a respective time frame for your report.



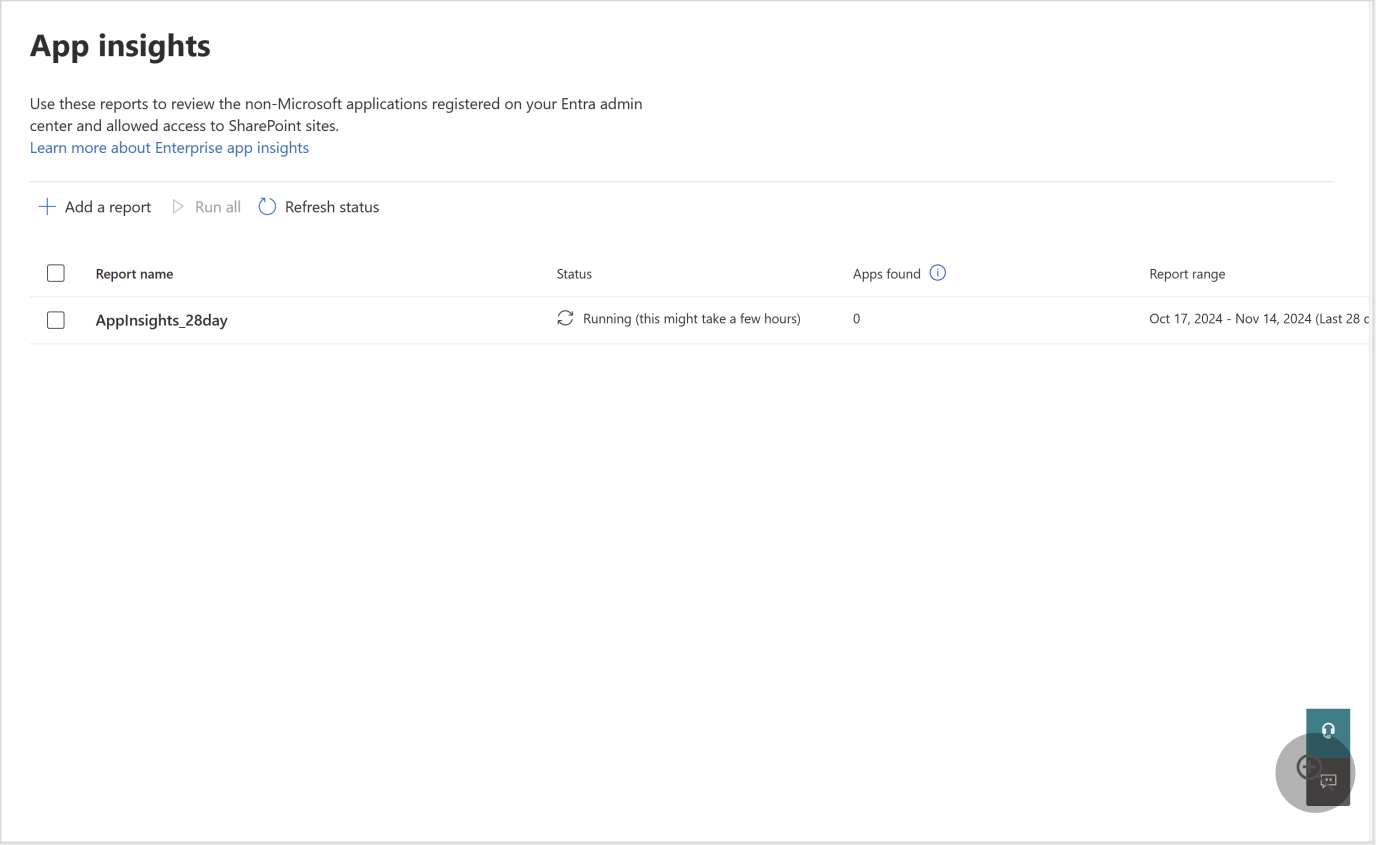
4. Select **Add and run**.

> **Note**
>
> - It can take up to several hours for generated reports to be available.
> - Only one report is allowed per report range.
> - Reports can be rerun after 24 hours.

Manage reports in SharePoint admin center

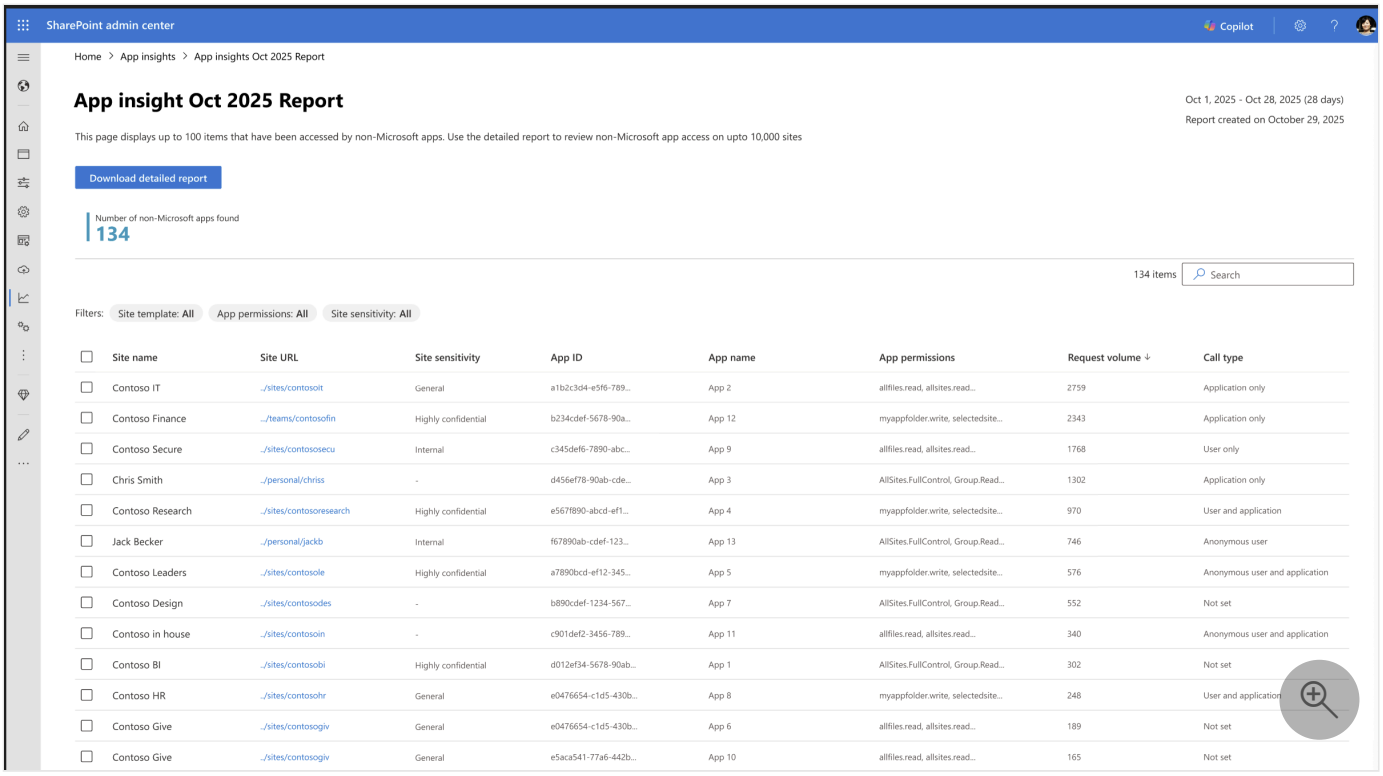
View report status

To check if a report is ready or when it was last updated, see the **Status** column. When a report is ready, select it to view the data.



You're able to see the top 100 (by request volume) results on the screen.

You can also filter by **App name**, **App permissions**, and **Site sensitivity** to view relevant results from the top 100 rows.



> **Important**
>
> To view up to 1 million results, you must select **Download detailed report**.

Delete report

To delete a report, select the existing report you want to delete, and then select **Delete report**.

Rerun a report

To get updated data for a given report range, select an existing report, and then select **Run**.

> **Tip**
>
> A rerun prompt also appears if you select **Add a report** and select a report range for which there already exists a report.

App insights reports in SharePoint PowerShell Module

You can generate and manage App insights reports using SharePoint Online Management Shell.

Create a one-day default duration report

To generate report for the default duration of one day, run the following command:

PowerShell

```
Start-SPOEnterpriseAppInsightsReport
```

Create report for any other duration

To generate report for any other duration, run the following command:

PowerShell

```
Start-SPOEnterpriseAppInsightsReport -ReportPeriodInDays $ReportPeriodInDays (possible
values = 1, 7, 14, 28)
```

Check status of all active and available reports

To check status of all active and available reports, run the following command:

PowerShell

```
Get-SPOEnterpriseAppInsightsReport
```

Check status of a specific report

To check status of a specific report, run the following command:

PowerShell

```
Get-SPOEnterpriseAppInsightsReport -reportID $reportID (for the given report ID)
```

View a specific report

To view a specific report, run the following command:

PowerShell

```
Get-SPOEnterpriseAppInsightsReport -reportID $reportID
```

Download a report

To download the report, run the following command:

PowerShell

```
Get-SPOEnterpriseAppInsightsReport -reportID $reportID -action download
```

> **Important**
>
> Rerun and delete report capabilities are unavailable for PowerShell. The Create report cmdlets can be used with relevant report duration.

Known issues

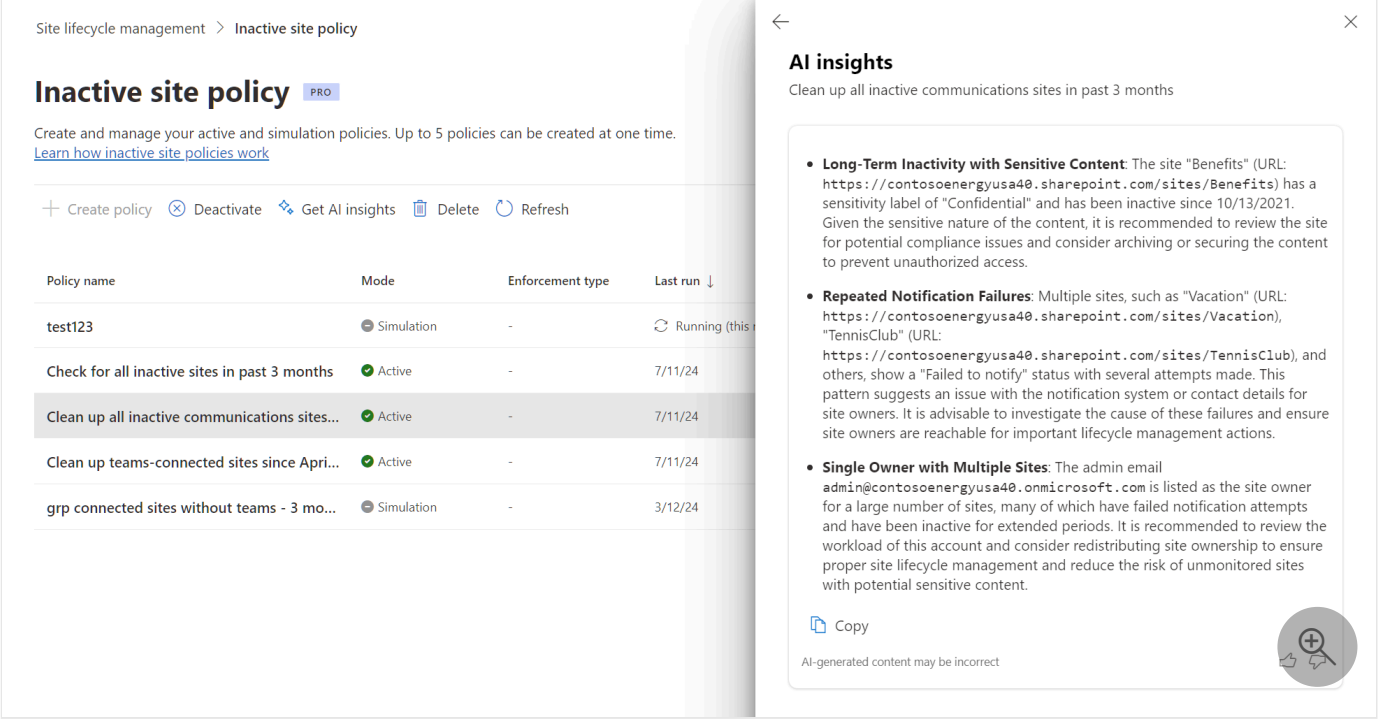
- In new tenants, it can take a few days for data to be available and for these reports to be generated successfully. In large tenants, the data can be delayed by up to 48 hours (about two days).
- A report can be rerun only after 24 hours since the last report generation.
- There can only be one report for each value of **Report range**. This means that you can see a maximum of four reports in the **Enterprise Application Insights** homepage.
- These reports are powered by Audit data and don't include all audit events.
- You might see App ID of a non-Microsoft app, but App name of a middle-tier app in some cases.

Last updated on 05/14/2026

Generate AI insights for SharePoint Advanced Management

The AI insights feature for SharePoint Advanced Management uses a language model to identify patterns and potential issues from reporting and receive actionable recommendations to solve issues.

As an IT administrator, you can reduce the manual effort required to review reports during audits, and mitigate content governance issues with the AI insights feature in SharePoint admin center.



Key capabilities of AI insights for SharePoint Advanced Management include:

- Automated analysis of reports and insights generated by SharePoint Advanced Management
- Detection of patterns and potential content governance issues, such as misapplied or missing labels and excessive permissions on site content
- Suggestion of practical recommendations for resolving these issues using the tools and strategies available in the SharePoint ecosystem

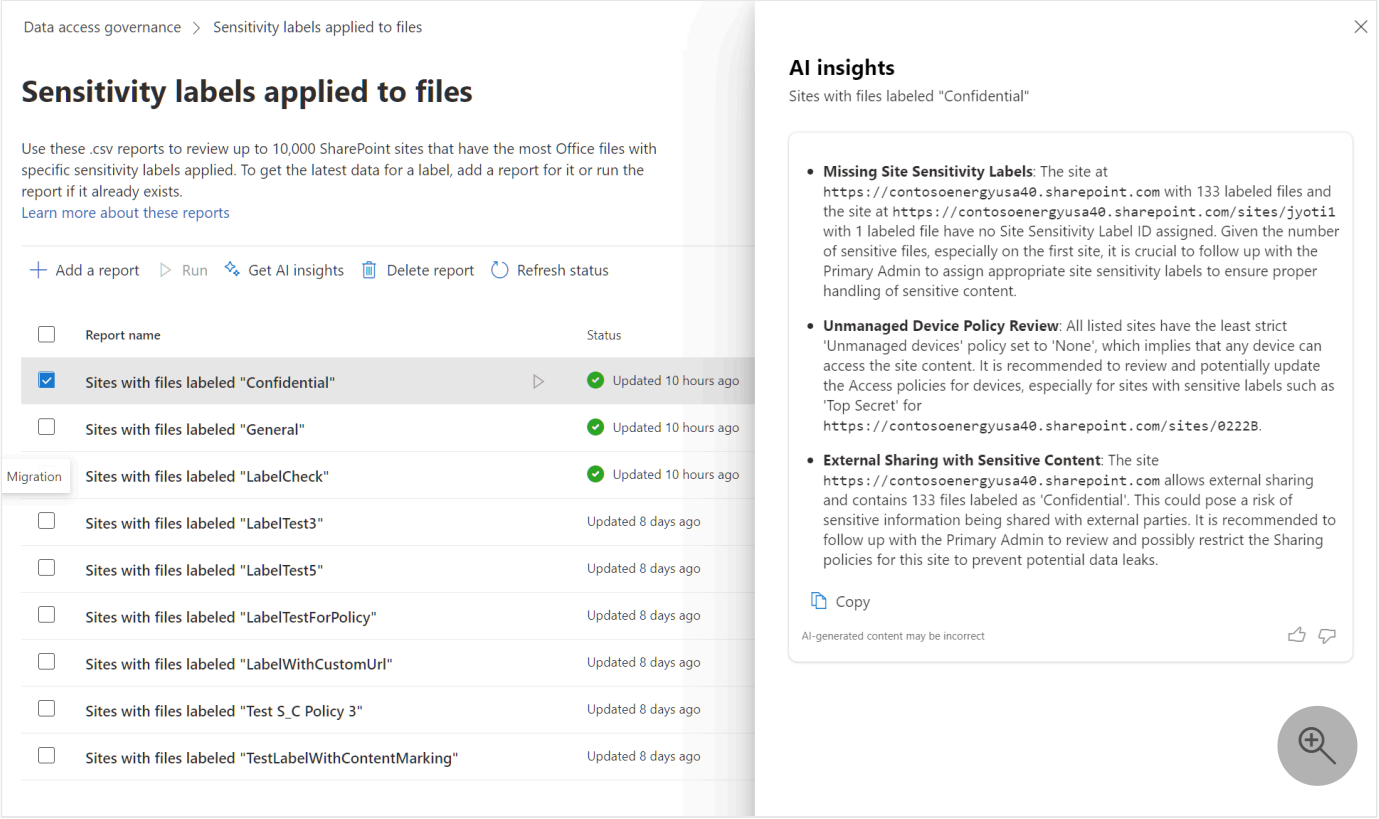
What do you need to get started with AI insights?

See SharePoint Advanced Management prerequisites.

Where can you find AI insights?

You can find the **Get AI insights** button next to various reports in the SharePoint admin center. Once selected, the AI insights feature extracts patterns from the report and offers a list of potential actions.

> **Note**
>
> You can generate up to five AI insights for each report, depending on the size of the report.



The AI insights feature is available for the following reports:

Expand table

Feature	Report name	Description
Data access governance	Sharing links	View sites where users created the most new sharing links
Data access governance	Sensitivity labels applied to files	View sites that have the most Office files that have sensitivity labels applied
Site lifecycle management	Inactive site policies	View sites that are in an inactive state

Feature	Report name	Description
Change history	Sites	View recent site actions or changes to organization settings

> **Note**
>
> Generated AI insights are based on a partial set of data, and not the report as a whole. If you choose to generate another insight, the data will be based on the next set of data of the report.

Related articles

Data access governance reports

Create change history reports

Last updated on 05/12/2026

Insights report on agents in SharePoint

The insights report on agents in SharePoint provides SharePoint administrators with rich information on the recently created agents across all SharePoint sites and OneDrive sites within their organization. This report helps admins learn about the sites with the highest number of agents created. By using this report, SharePoint admins can further govern and maintain the integrity of the content used by agents as grounding data.

The insights report is based on the Microsoft audit data logged for the agents created in SharePoint through the FileCreated and FileRenamed events.

You can generate and manage the agent insights report in SharePoint Admin Center or by using SharePoint Online Management Shell.

What you need to access agent insights report

See SharePoint Advanced Management prerequisites.

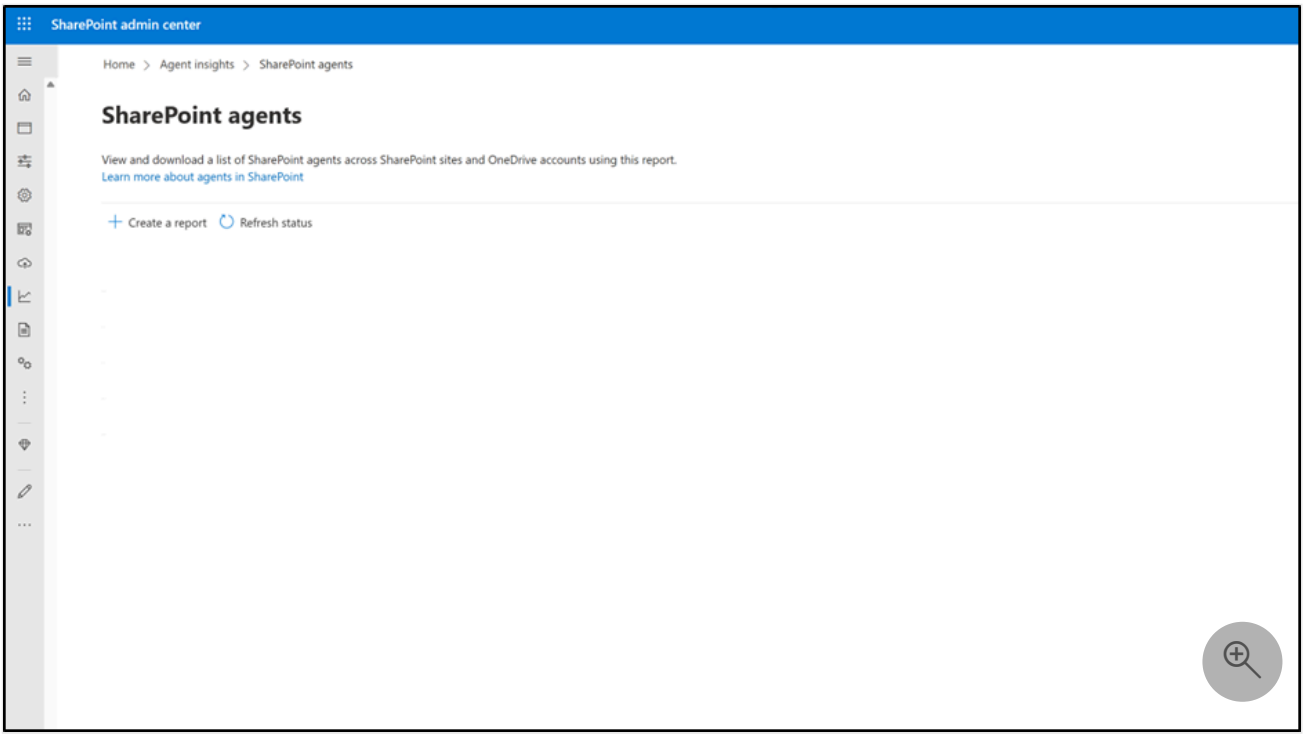
> **Important**
>
> If you don't have a Microsoft SharePoint Advanced Management license, you're asked to enable data collection so that relevant audit data is collected to build the report. Once enabled, you can generate the reports 24 hours later and they contain data from the point of collection. Data is stored for 28 days. If you don't generate reports at least once in three months, data collection pauses and you need to enable it again. To enable data collection for these reports, see the Data collection for insights report on agents in SharePoint section (in this article).

How to access agent insights report in SharePoint Admin Center

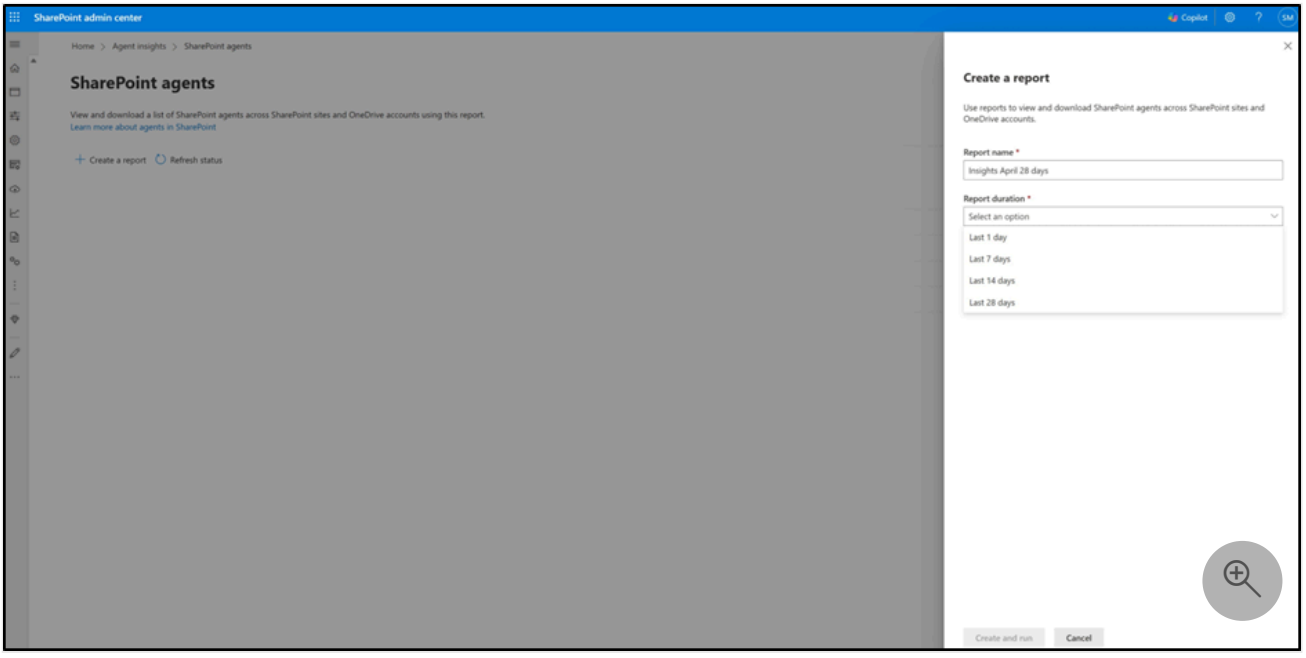
1. Sign in to the SharePoint admin center with the SharePoint administrator credentials for your organization.
2. In the navigation pane, expand **Reports** and then select **Agent Insights**.

How to create reports in SharePoint Admin Center

1. As a SharePoint Administrator, select **Create a report** to create the report.



2. Enter the report name. Under **Report duration**, specify the time frame for the report.

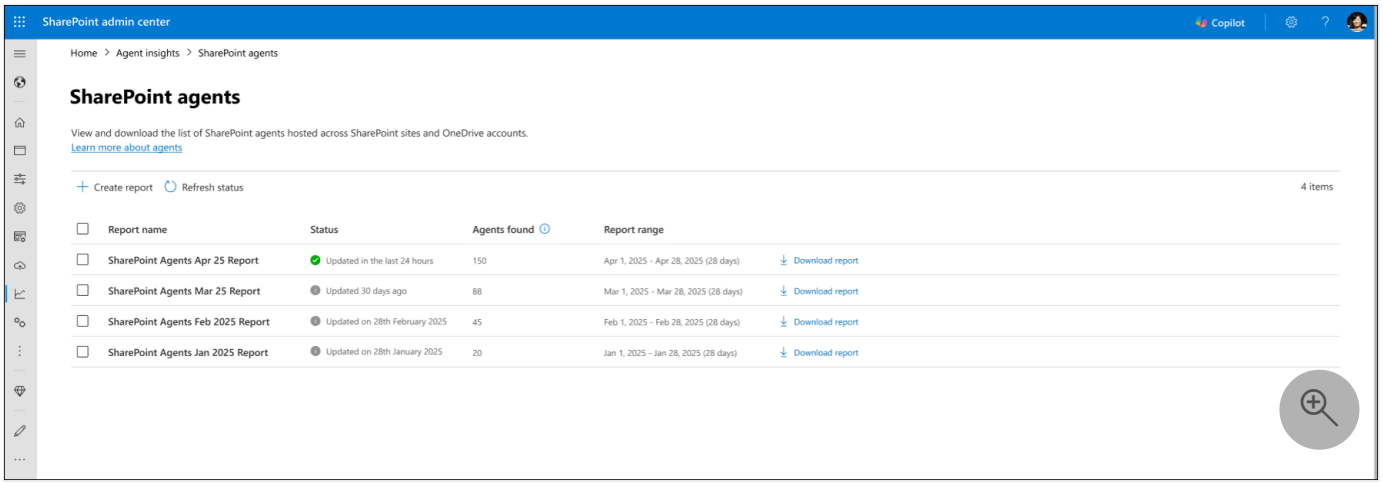


3. Select **Create and run**.

> **Note**
>
> You can create a report for the past 1, 7, 14, or 28 days.

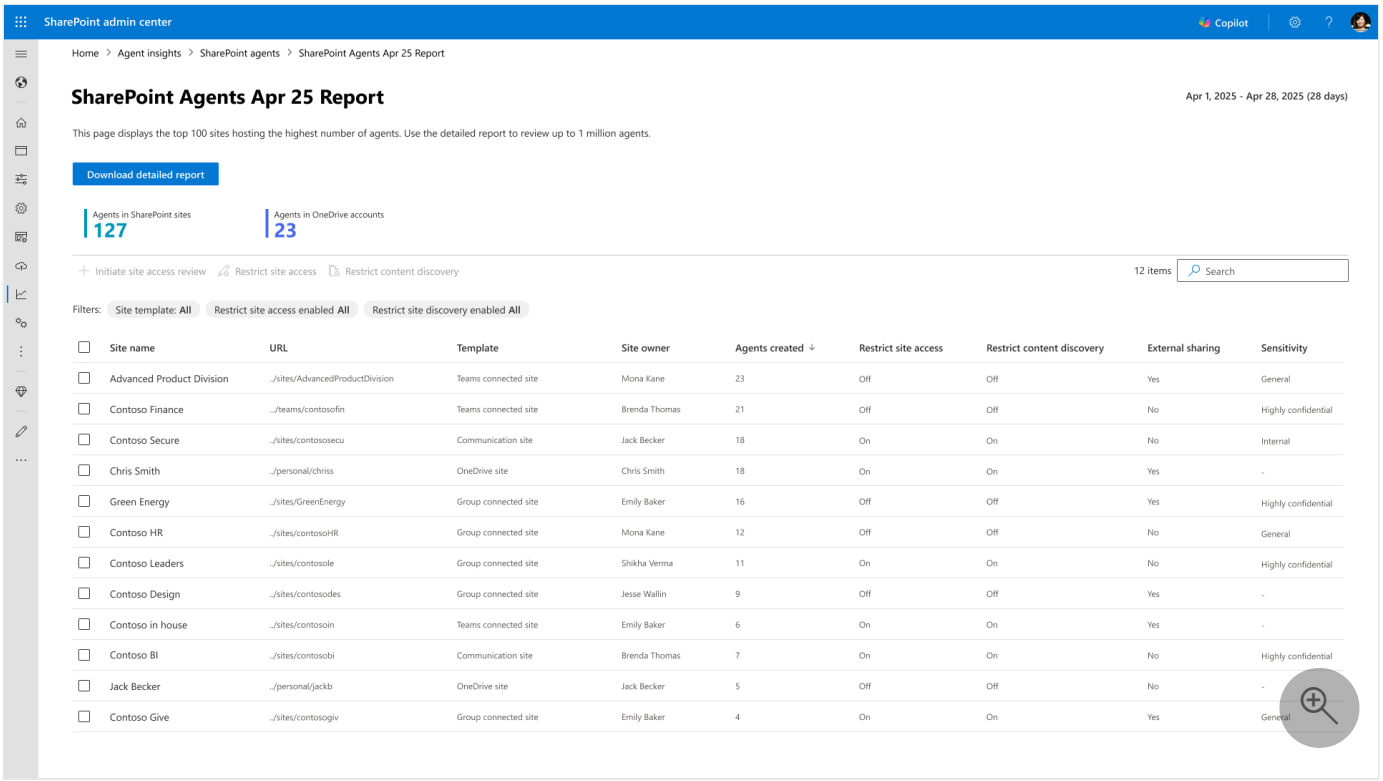
View report status in SharePoint Admin Center

To check if a report is ready or when it was last updated, see the **Status** column.



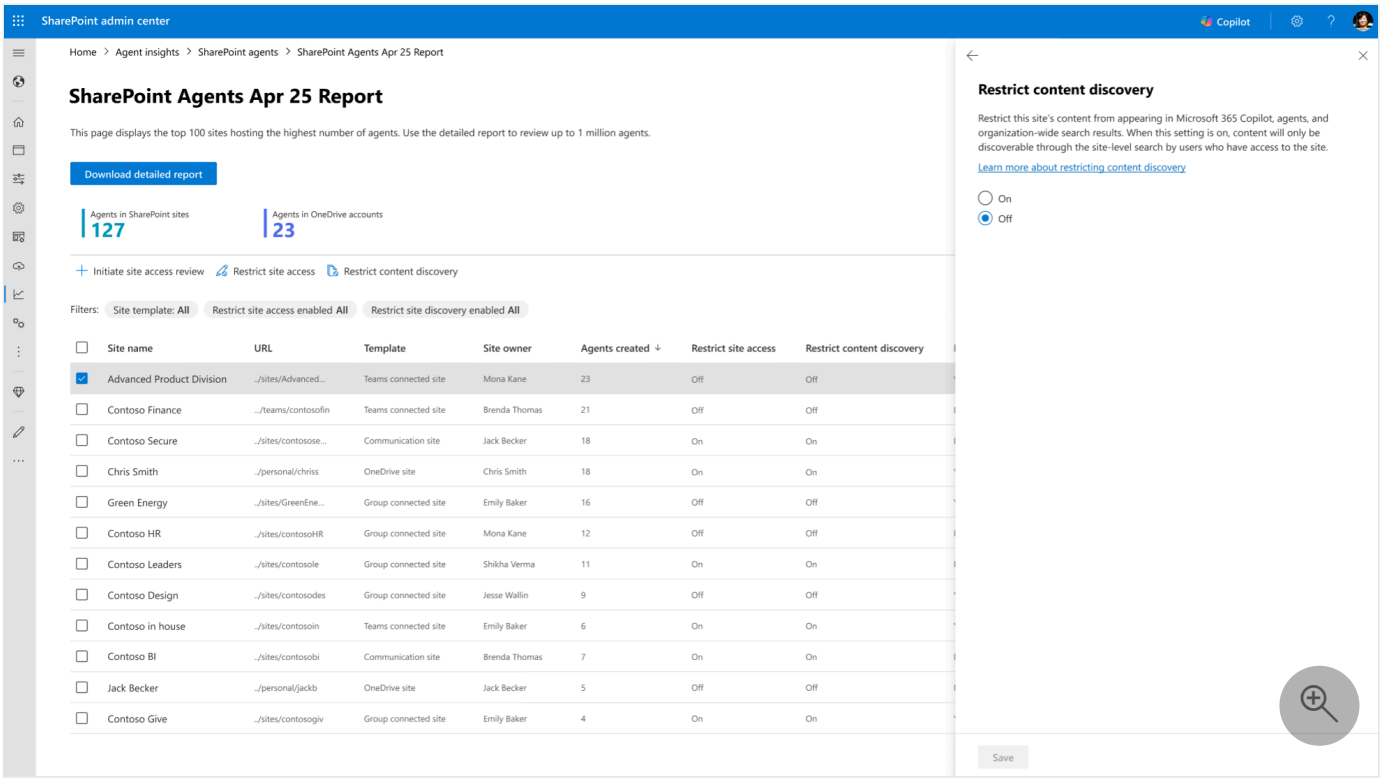
View report in SharePoint Admin Center

When a report is ready, select it to view the data. You can view the top 100 records hosting the highest number of agents. You can search for sites or filter on the site template, and governance policies.



Apply content governance policies in SharePoint Admin Center

You can apply content governance policies on the sites from the insights report. The available policies are Restrict site access policy and Restrict Content Discovery policy.



> **Note**
>
> After you apply a policy to the site from the insights report, the policy status on the existing report doesn't update. To view the updated status of the policy on the site, select the policy to view the latest status or access the Active site panel and review the site settings.

Agent insights report in SharePoint Online Management Shell

You can generate and manage agent insights reports by using SharePoint Online Management Shell.

1. If you haven't already done so, download and install the latest version of SharePoint Online Management Shell.

2. Connect to SharePoint Online as at least a SharePoint administrator in Microsoft 365. For more information, see Getting started with SharePoint Online Management Shell.

3. To generate and view these reports, ensure the organization has the SharePoint Advanced Management add-on SKU or Microsoft 365 Copilot license.

With permissions of at least a SharePoint administrator, you can generate and view the insights report by using the following commands:

1. To generate a report for the default one-day report duration, run the following command:

```
PowerShell
Start-SPOCopilotAgentInsightsReport
```

2. To generate a report for any other duration (7, 14, or 28 days), run the following command:

```
PowerShell
Start-SPOCopilotAgentInsightsReport -ReportPeriodInDays
```

For example, to generate a report for the past 28 days, run the command:

```
PowerShell
Start-SPOCopilotAgentInsightsReport -ReportPeriodInDays <28>
```

3. To check the status of all active and available reports, run the following command:

```
PowerShell
Get-SPOCopilotAgentInsightsReport
```

4. To check the status of a specific report, run the following command:

```
PowerShell
Get-SPOCopilotAgentInsightsReport –ReportId
```

5. To download and view the report, run the following command:

```
PowerShell
Get-SPOCopilotAgentInsightsReport –ReportId -Action Download
```

> **Note**
>
> PowerShell displays up to 100 records, but downloaded reports can contain up to 1 million records.

```powershell
Get-SPOCopilotAgentInsightsReport –ReportId -Action View
```

6. To view more detailed reports, use the following options:

   a. `CopilotAgentsOnSites`: Provides the name of all the agents currently available on all sites. This report contains up to 1,000,000 records.

   > **Note**
   >
   > The default value for the `-Content` parameter is `CopilotAgentsOnSites`.

   ```powershell
   Get-SPOCopilotAgentInsightsReport –ReportId -Content CopilotAgentsOnSites
   ```

   b. `TopSites`: Provides a list of 100 sites with the number of agents available on each site.

   ```powershell
   Get-SPOCopilotAgentInsightsReport –ReportId -Content TopSites
   ```

   c. `SiteDistribution`: Provides the summarized view of agents across all types of sites like Communication sites, Microsoft 365 Group connected sites, OneDrive sites, and more.

   ```powershell
   Get-SPOCopilotAgentInsightsReport –ReportId -Content SiteDistribution
   ```

Data collection for insights report on agents in SharePoint

If you don't have a Microsoft SharePoint Advanced Management license, you need to enable data collection. This section explains how to enable and check the status of data collection for the Insights report on agents in SharePoint.

Enable data collection

This PowerShell command starts collecting audit data for reports on activities from the last 28 days.

PowerShell

```
Start-SPOAuditDataCollectionForActivityInsights
```

Disable data collection

This PowerShell command stops collecting audit data for reports on activities from the last 28 days.

PowerShell

```
Stop-SPOAuditDataCollectionForActivityInsights
```

Check the data collection status

After you enable data collection, you can generate the reports after 24 hours. To check whether you can generate reports, use the PowerShell command `Get-SPOAuditDataCollectionStatusForActivityInsights`. The command returns the current data collection status, which can be `NotInitiated`, `InProgress`, or `Paused`. You can generate reports when the status is `InProgress`.

PowerShell

```
Get-SPOAuditDataCollectionStatusForActivityInsights
```

Known experiences with agent insights reports in SharePoint

The following experiences are known with agent insights reports generated in SharePoint Admin Center or by using SharePoint Online Management Shell:

- You can rerun a report only after 24 hours since the last report generated.
- In large tenants, it might take up to 48 hours for the data to be available.
- Only one report can exist for each report range value (1, 7, 14, or 28 days). This limitation means you can see a maximum of four reports at a given point.
- The newly generated report replaces the previously created report with the same date range. To preserve the previously created report, download the report first before creating a new report for the same date range.

- These reports use Microsoft 365 unified audit data and might not cover all audit events.

Related articles

- Restrict SharePoint site access with Microsoft 365 groups and Microsoft Entra security groups
- Restrict discovery of SharePoint sites and content
- Microsoft.Online.SharePoint.PowerShell Module

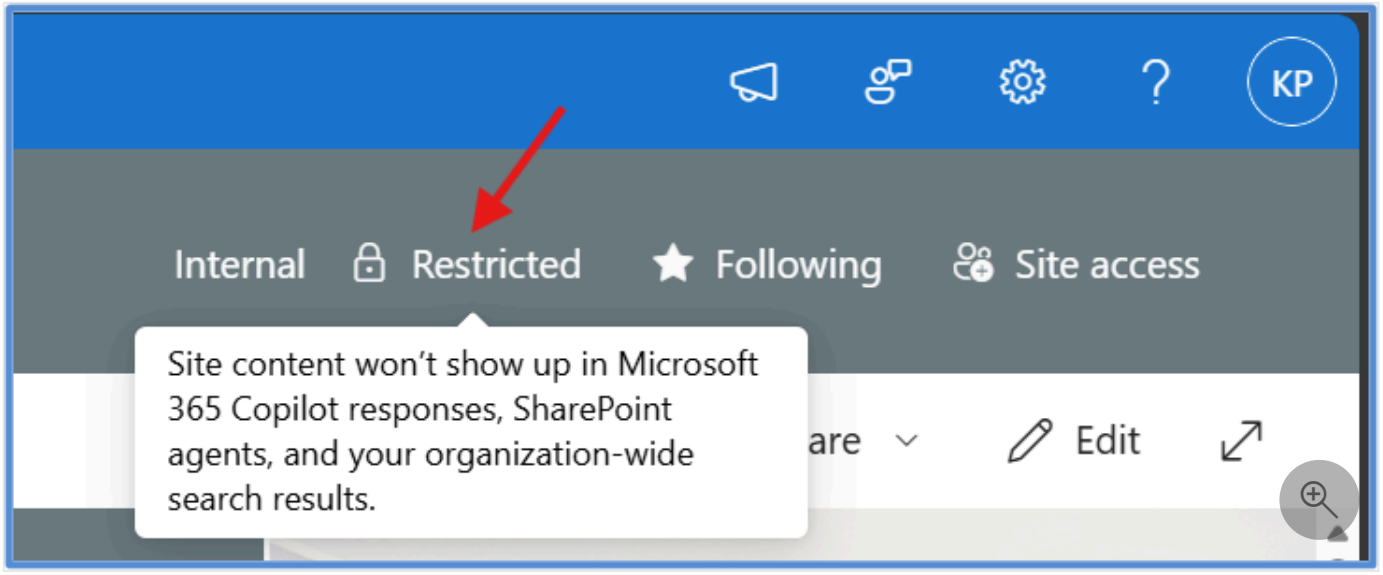
Last updated on 05/13/2026

Restrict discovery of SharePoint sites and content

Organizations preparing for Microsoft Copilot often need time to review SharePoint sites, validate permissions, and implement governance controls before making content broadly discoverable. Restricted Content Discovery helps you limit discovery of content from specific SharePoint sites, including recently interacted files, in organization-wide search results and Microsoft Copilot responses while those reviews are taking place.

Restricted Content Discovery also removes AI-powered entry points from these SharePoint sites. Users don't see entry points such as the Copilot button, AI actions menus (including creating agents), or **Create pages with AI**. This restriction helps reduce the likelihood of accidental discovery of content while permissions and governance controls are being evaluated.

When a site has a Restricted Content Discovery policy applied to it, a Restricted tag is visible, as shown in the following screenshot:



Restricted Content Discovery is designed as a temporary governance control that gives organizations time to review and right-size access while continuing their Copilot deployment.

> **Note**
>
> - Restricted Content Discovery doesn't change existing permissions. Users who already have access to content can continue to access that content directly.

- You can only apply this feature to SharePoint sites. It's not supported for OneDrive sites.
- Restricted Content Discovery doesn't affect searches that originate from site context or other intelligent experiences such as Microsoft 365 Feed and Recommendations.

Caution

Use Restricted Content Discovery selectively. Excessive use can reduce the amount of content available to organization-wide search and Microsoft Copilot experiences, which can affect the completeness and relevance of search results and AI-generated responses.

When to use Restricted Content Discovery

Use Restricted Content Discovery for sites that might need extra review before they become broadly discoverable through organization-wide search and Microsoft Copilot experiences.

Common scenarios include:

- Sites with a high risk of oversharing.
- Sites undergoing permissions review.
- Phased Microsoft Copilot rollouts.
- Governance initiatives that require content validation before wider discovery.

For example, you might temporarily apply Restricted Content Discovery to a group of Finance or Human Resources sites while site owners review permissions and access. After the review is complete, you can remove the restriction and allow the sites to become discoverable again.

Before enabling Restricted Content Discovery, consider using one or more of the following tools and reports to identify sites that require review:

- SharePoint Admin Agent
- Content management assessment
- Data Access Governance reports
- Catalog management

How Restricted Content Discovery works

Restricted Content Discovery is a site-level setting. When you turn on the setting, Microsoft 365 search systems propagate it so that content from the site doesn't appear in organization-wide

discovery experiences.

Even when Restricted Content Discovery is enabled:

- Site permissions stay the same.
- Users can continue to access content they already have permission to access.
- The feature doesn't remove content from the Microsoft 365 search index.

Because the setting must propagate across indexing systems, updates can take time to become fully effective. The amount of time depends on site size, the number of files in each site, and the number of concurrent updates being processed.

Prerequisites

Before configuring Restricted Content Discovery:

1. Review the SharePoint Advanced Management prerequisites, including:
    - SharePoint Online PowerShell module requirements
    - Role-based access control (RBAC) role assignments
2. Ensure your organization has a Microsoft Copilot license. Restricted Content Discovery is intended for Microsoft Copilot deployment and governance scenarios.
3. Review your organization's existing categories, and if necessary, add categories. See Catalog management.

Enable Restricted Content Discovery for a site

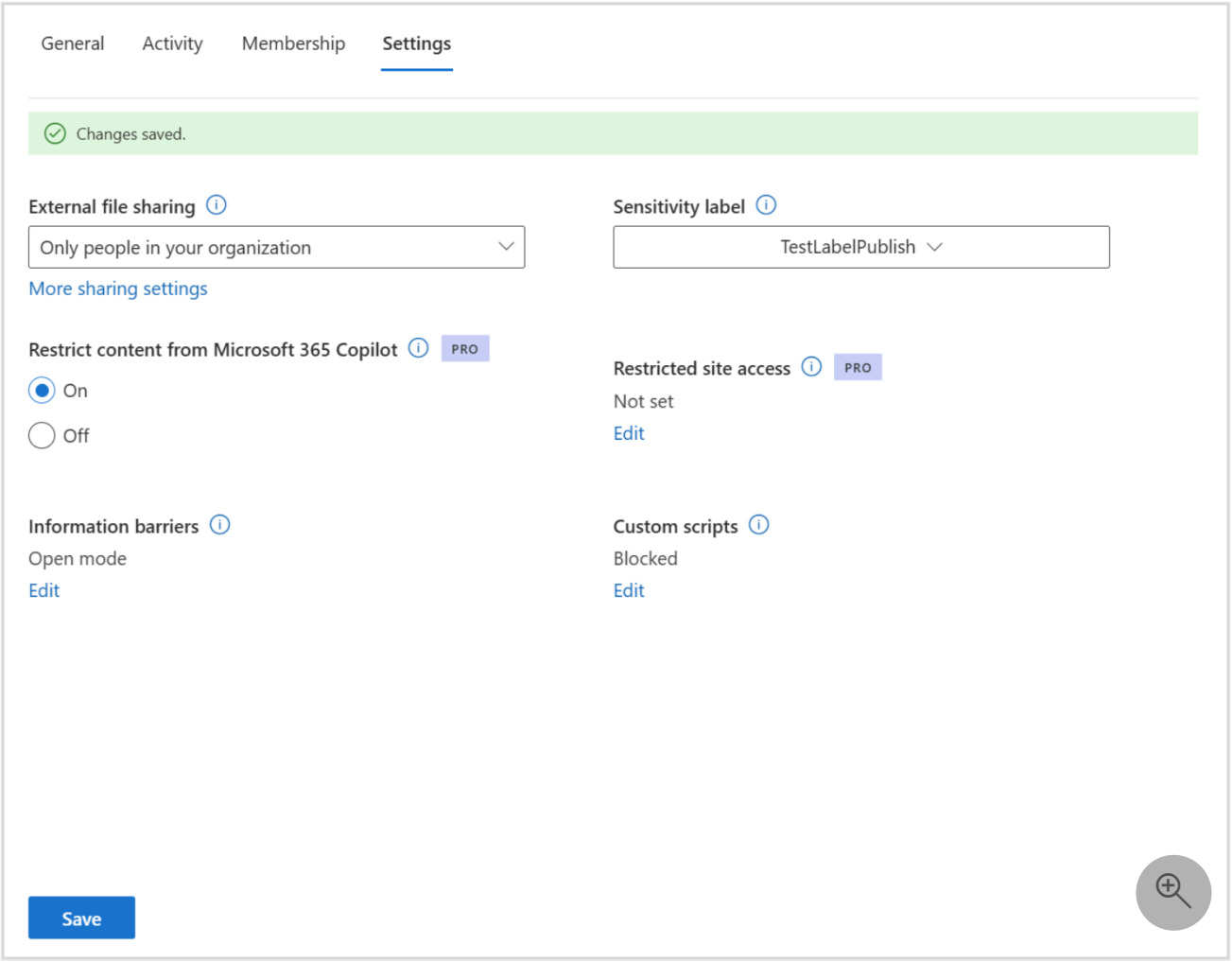
You can enable Restricted Content Discovery from the SharePoint admin center or by using PowerShell.

> ⓘ **Note**
>
> Updates can take time to propagate throughout search and Microsoft Copilot experiences.

Use the SharePoint admin center

1. In the SharePoint admin center, expand **Sites** and select **Active sites**.
2. Select the site you want to configure.

3. Open the **Settings** tab, and then turn **Restrict content from Microsoft Copilot** on.



4. Select **Save**.

Use PowerShell

Open PowerShell as an administrator and run the following command:

PowerShell

```
Set-SPOSite -Identity <site-url> -RestrictContentOrgWideSearch $true
```

Remove Restricted Content Discovery from a site

To disable Restricted Content Discovery for a site, open PowerShell as an administrator and run the following command:

PowerShell

```
Set-SPOSite -Identity <site-url> -RestrictContentOrgWideSearch $false
```

Delegate management to site administrators

By default, only SharePoint administrators can manage Restricted Content Discovery.

If you want site administrators to manage the setting for their own sites, enable delegation by using the following PowerShell command:

PowerShell

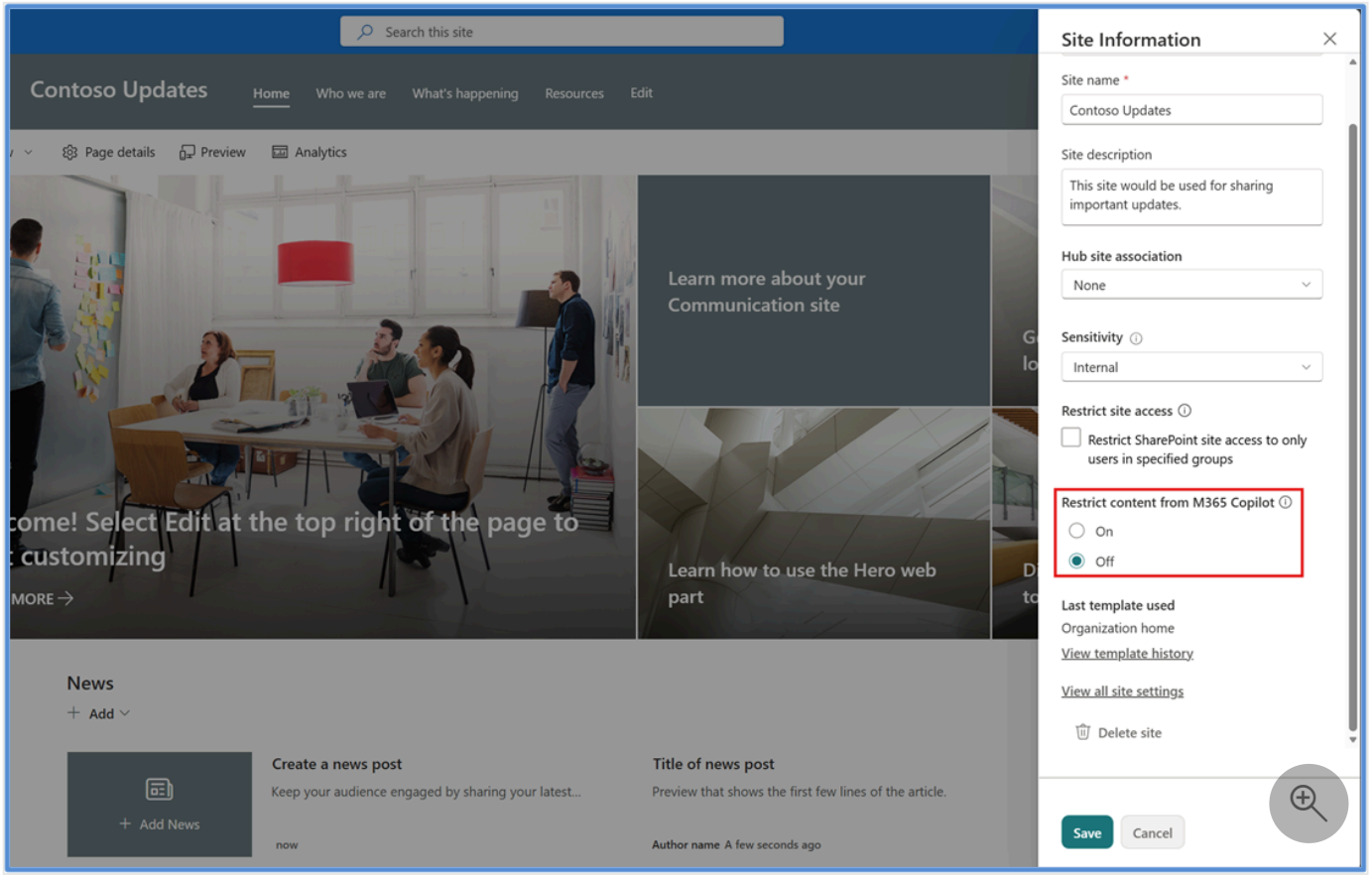
```
Set-SPOTenant -DelegateRestrictedContentDiscoverabilityManagement $true
```

To verify delegation status, run:

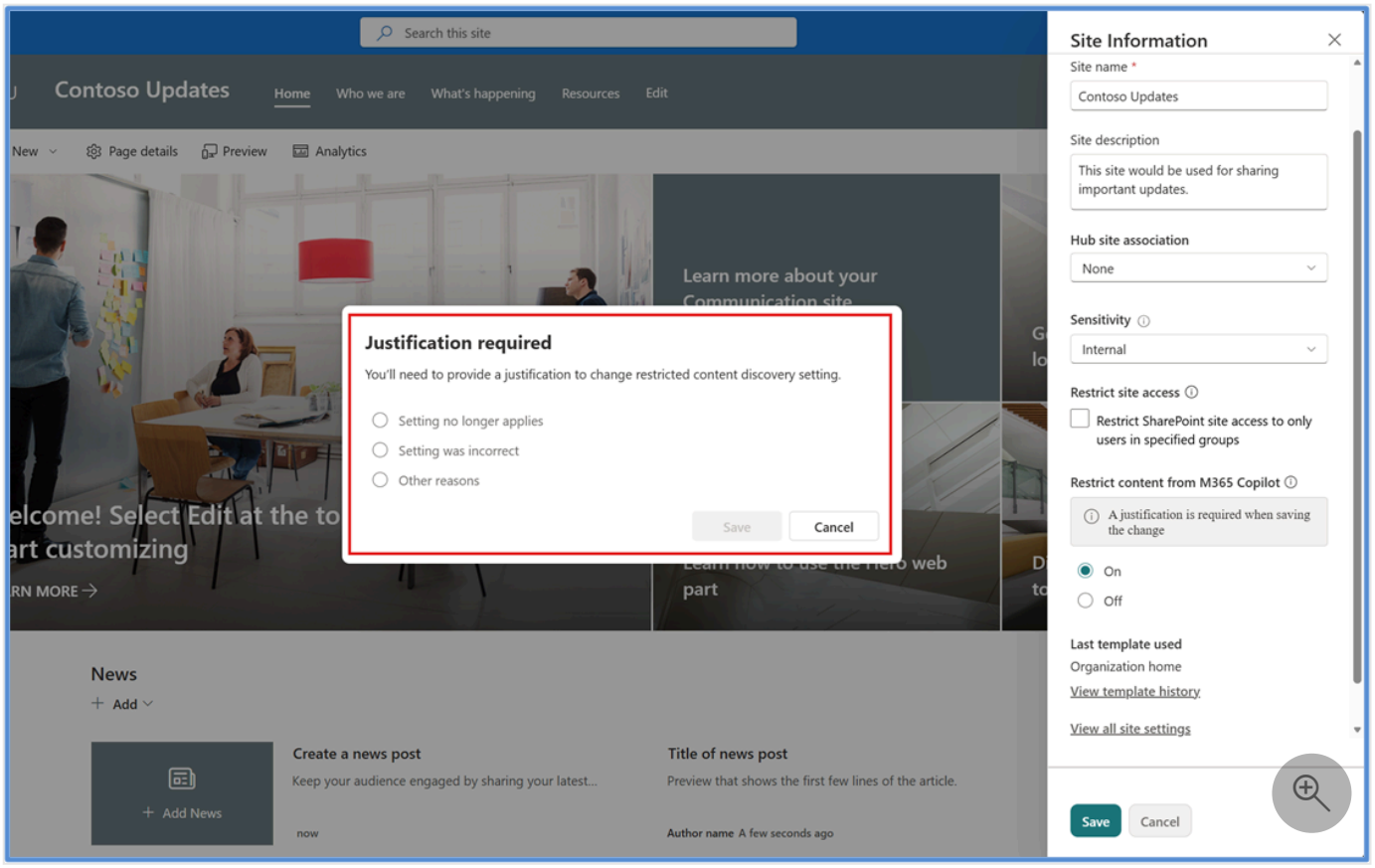
PowerShell

```
Get-SPOTenant | Select-Object DelegateRestrictedContentDiscoverabilityManagement
```

When delegation is enabled, site administrators can manage Restricted Content Discovery for their sites.



If a site administrator makes a change to Restricted Content Discovery settings, they must provide a justification for the change.



Check Restricted Content Discovery status for a site

Open PowerShell as an administrator and run the following command:

PowerShell

```
Get-SPOSite -Identity <site-url> | Select RestrictContentOrgWideSearch
```

Monitor Restricted Content Discovery across your tenant

Administrators can use PowerShell to generate reports that identify sites where Restricted Content Discovery is enabled.

Generate a report

Open PowerShell as an administrator and run the following command:

PowerShell

```
Start-SPORestrictedContentDiscoverabilityReport
```

View report status

Open PowerShell as an administrator and run the following command:

PowerShell

```
Get-SPORestrictedContentDiscoverabilityReport
```

Download a report

Open PowerShell as an administrator and run the following command:

PowerShell

```
Get-SPORestrictedContentDiscoverabilityReport -Action Download -ReportId <ReportGUID>
```

> **Tip**
>
> If a site is configured for Restricted Content Discovery but continues to appear in search results, allow time for index propagation and review the number of items stored in the site. Large sites can require extra processing time before changes are fully reflected.

Auditing

You can view audit events through Microsoft Purview audit log activities for activities involving Restricted Content Discovery.

These events include:

- Enabling Restricted Content Discovery.
- Disabling Restricted Content Discovery.
- Justifications provided when updates are made to the setting.

Frequently asked questions

Is my organization eligible to use Restricted Content Discovery?

You can configure Restricted Content Discovery if your organization is licensed for Copilot and has SharePoint Advanced Management available. See Prerequisites for SharePoint Advanced Management.

Does Restricted Content Discovery change user permissions?

No. Restricted Content Discovery affects discoverability, not access permissions. Users who already have access to content can continue to access it.

What search experiences are affected?

Restricted Content Discovery affects organization-wide search experiences (SharePoint home, Office.com, Bing) and Microsoft Copilot discovery scenarios, including experiences that rely on tenant-wide content discovery. Restricted Content Discovery doesn't affect experiences that operate on content that's already in use by the user, such as summarizing an open document.

How does Restricted Content Discovery affect the end user experience in SharePoint?

Restricted Content Discovery restricts usage of AI-powered features in SharePoint. Users don't see entry points such as the Copilot button, AI actions menus (including creating agents), or **Create pages with AI**.

Does Restricted Content Discovery affect Microsoft Purview features?

No. Restricted Content Discovery doesn't remove content from the search index. Microsoft Purview capabilities such as eDiscovery and auto-labeling continue to function.

How long does it take for updates to Restricted Content Discovery to take effect?

Restricted Content Discovery is a site-level property. Index update latency is highly dependent on the number of items in the site and the number of sites getting updated at the same time. For sites with more than 500,000 items, an update to Restricted Content Discovery could take more than a week to fully process and reflect in search and Copilot experiences.

How does Restricted Content Discovery fit into a Copilot readiness strategy?

Restricted Content Discovery helps organizations temporarily limit discovery of selected sites while permissions, ownership, and governance controls are reviewed. It's one component of a broader SharePoint governance and Copilot readiness strategy. See the following resources:

- Secure and govern Microsoft Copilot: Foundational deployment guidance
- Get ready for Microsoft Copilot and agents with SharePoint Advanced Management

Next steps

- Review Data access governance reports for SharePoint and OneDrive sites
- Implement SharePoint site lifecycle management policies
- See Assess your organization's content management status

Last updated on 10/11/2026

Data access governance reports for SharePoint and OneDrive sites

As sprawl and oversharing of SharePoint sites increase with exponential data growth, organizations need help with governing their data. Data access governance reports can help you govern access to SharePoint data. The reports let you discover sites that contain potentially overshared or sensitive content. You can use these reports to assess and apply the appropriate security and compliance policies.

What you need to create a data access governance report

See Prerequisites for SharePoint Advanced Management.

The reports are currently unavailable for Microsoft 365 operated by 21Vianet, even if you have the required licenses.

How to access the Data access governance reports in the SharePoint admin center

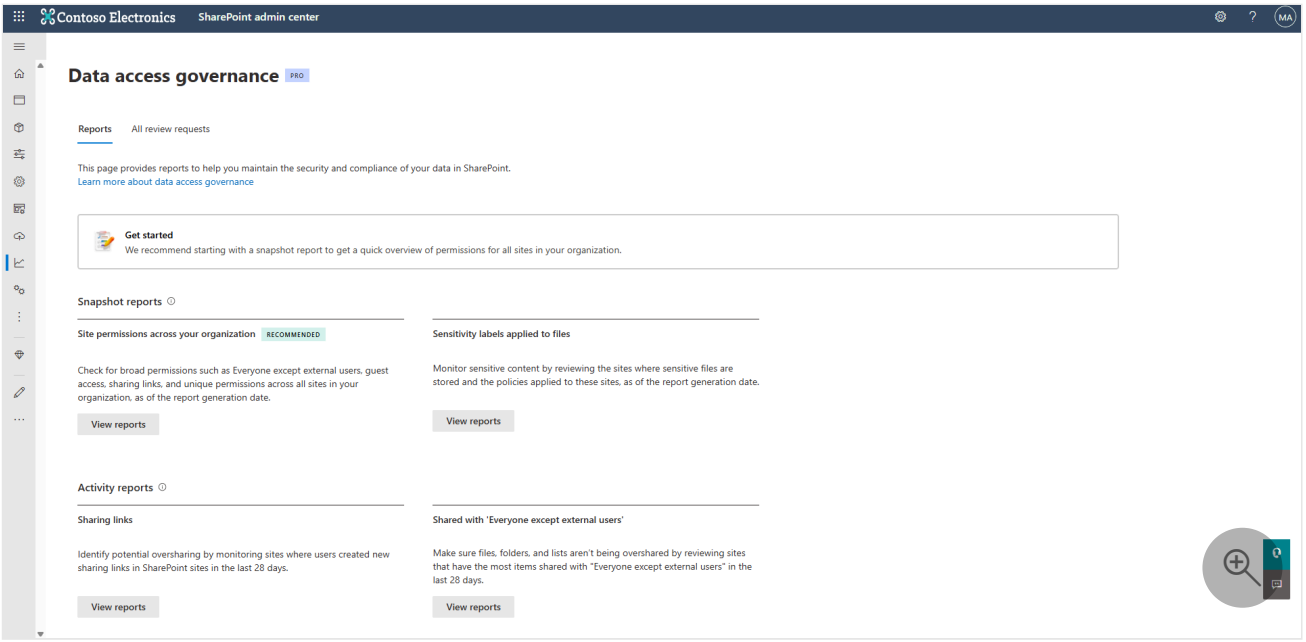
1. Sign in to the SharePoint admin center with the SharePoint administrator credentials for your organization.

2. In the left pane, expand **Reports** and then select **Data access governance**.

   The following reports are currently available from the Data access governance landing page:

   - **Snapshot reports**
     - Site permissions across your organization (Recommended)
     - Sensitivity label applied to files

   - **Activity reports**
     - Sharing links
     - Shared with 'Everyone except external users'



> **Note**
>
> IT administrators with Microsoft 365 E5 licensing can access Data access governance reporting, but can't view or use the other SharePoint Advanced Management features. The reports don't provide snapshot reports or remedial actions. Activity reports are available but can return only up to 10,000 sites.

What are snapshot reports?

Snapshot reports give you a snapshot of your organization's current status based on specific reporting criteria. These reports show data as of the date they were generated.

Currently, three types of snapshot reports are available:

- **Site permissions report**: Provides a comprehensive snapshot of the permission structure across all SharePoint and OneDrive sites. It helps you identify sites with the broadest user access, such as sites with thousands of users, external guests, or "Everyone except external users" permissions.
- **Site permissions for users report**: Lists all sites a specified user can access. Admins can use this report to determine whether the user can access the entire site or specific sections, granted directly to the user or indirectly through groups.
- **Sensitivity label for files report**: Identifies SharePoint sites containing files with specific sensitivity labels applied. You can use this report to verify that appropriate security policies are in place for your most sensitive content.

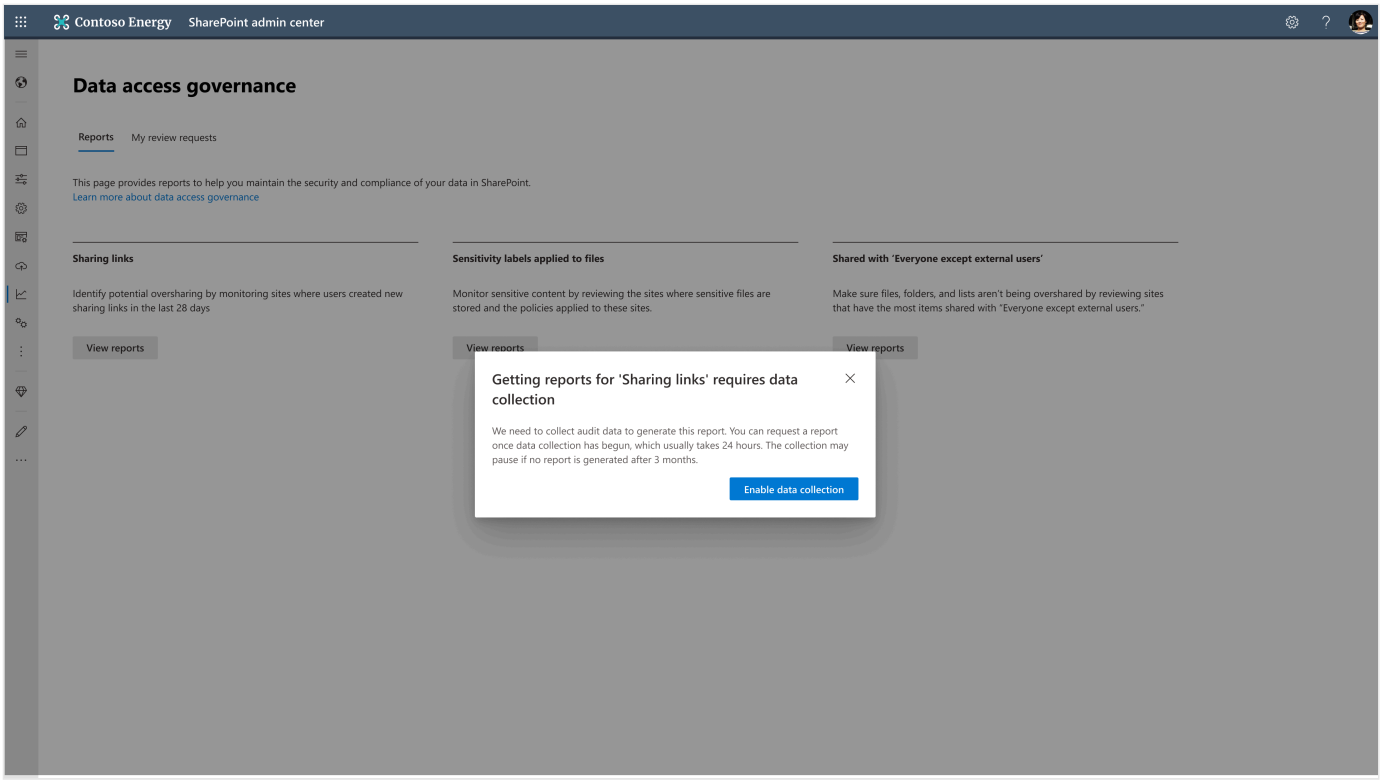
What are activity reports?

Activity reports help you track potential oversharing activities that occurred in the last 28 days. These reports focus on "recently active" sites where users created sharing links or shared content with large groups. For all activities tracked in activity reports, you can find corresponding "baseline" data in the snapshot reports.

Currently, two types of activity reports are available to help you identify potential oversharing:

- **Sharing links reports**: Identifies sites where users recently created the most sharing links (including "Anyone," "People in the organization," and "Specific people" links) to help you catch potential oversharing as it happens.
- **Shared with 'Everyone except external users' reports**: Tracks sites where content is shared with all internal users in your organization, helping you identify broad internal exposure that could lead to unintended data access.

> ⓘ **Important**
>
> **For organizations without SharePoint Advanced Management:** You must enable data collection before you can generate activity reports. Here's what you need to know:
>
> - After enabling data collection, the system starts collecting audit data
> - Data is stored for 28 days
> - Reports become available 24 hours after enabling collection
> - Reports only contain data from when collection was enabled
> - If no reports are generated for 3 months, data collection pauses and must be re-enabled



How do you use snapshot and activity reports?

As part of your governance strategy, combine both snapshot and activity reports to get a complete picture of your organization's data access landscape. Here's how to use them together effectively:

1. **Start with snapshot reports**: Run site permissions reports first to understand your baseline permission structure and identify sites with the broadest exposure. Run these reports quarterly to maintain a comprehensive view of your organization's data access.

2. **Follow up with activity reports**: Use sharing links and EEEU activity reports to monitor recent oversharing activities and catch emerging risks. Run these reports monthly to stay on top of ongoing sharing activities.

This combination ensures you have both a complete picture of your current state and visibility into ongoing sharing activities that could create new exposure risks.

What is the site permissions for your organization report?

The site permissions for your organization report is the first snapshot report that provides a comprehensive view of your organization's current permission structure across all SharePoint and OneDrive sites. This report analyzes every site to help you understand how broadly your data is

exposed and identify potential oversharing risks. This snapshot approach helps you quickly assess your overall security posture and identify sites that need immediate attention.

Learn how to create and use the site permissions for your organization report.

What is the site permissions for users report?

The site permissions for users report is the next snapshot report that provides a comprehensive view into permissions of the specified users across all SharePoint and OneDrive sites. This report lists all sites a user can access and allows admins to determine whether they can access the entire site or specific sections, granted directly to the user or indirectly through groups. This approach helps you quickly assess your overall security posture and identify sites that need immediate attention.

Learn how to create and use the site permissions for users report.

What is the sites and files shared via special SharePoint groups report?

The sites and files shared via special SharePoint groups report is a snapshot report that identifies all sites, folders, and files across SharePoint and OneDrive that are effectively public because of the special SharePoint groups 'Everyone except external users' (EEEU) or 'Everyone'. While the site permissions for your organization report tells you which sites are overshared, this report tells you exactly which items are overshared and how access was granted, so you can accelerate cleanup through scripting instead of depending on site owners.

Learn how to run and use the sites and files shared via special SharePoint groups report.

What is the sensitivity labels for files report?

The sensitivity labels for files report is another snapshot report that helps you control access to sensitive content across your organization. This report identifies sites containing files with sensitivity labels applied, allowing you to verify that appropriate security policies are applied.

Learn how to use the sensitivity labels for files report.

What is the sharing links report?

The sharing links report is one of two activity reports that helps you identify sites where users created the most new sharing links in the last 28 days.

Learn how to create and use the sharing links report.

What is the 'Everyone except external users' (EEEU) report?

EEEU is a built-in SharePoint group that automatically includes all internal users but excludes any external guests. The 'Everyone except external users' (EEEU) report is one of two activity reports that helps you identify sites where content is shared with your entire organization in the past 28 days. You can run the site permissions for your organization report first to understand your organization's current EEEU sharing status, then use this activity report to monitor ongoing EEEU sharing activities. See Monitor 'Everyone except external users' (EEEU) sharing with the EEEU activity report.

Limitations or known issues

- Reports might not work if you select nonpseudonymized report data for your organization. To change this setting, you must be a Global Administrator. Go to the Reports setting in the Microsoft 365 admin center and clear **Display concealed user, group, and site names in all reports**.

Remedial actions from Data access governance reports

After discovering potential oversharing through Data access governance reports, take several actions to address these risks. When deciding which actions to take, consider:

- The sensitivity of the exposed content
- The amount of content at risk
- The potential disruption to users and workflows

Available remediation options

For immediate action:

- Use Restricted access control (RAC) to limit access to a specific group.
- Review the 'Change history' report to identify recent permission changes that might have led to oversharing.

For collaborative remediation:

- Use the Site access review feature to request that site owners review and update permissions.

This approach ensures you can balance security needs with minimal disruption to your organization's productivity.

ⓘ**Note:** The author created this article with assistance from AI. Learn more

---

Last updated on 07/30/2026

Get your organization's site permissions baseline with the snapshot report

Site permissions for your organization report is one of the Data access governance snapshot reports available with SharePoint Advanced Management. This report provides a snapshot of your organization's current permission structure across all SharePoint and OneDrive sites, helping you understand how broadly your data is exposed and identify potential oversharing risks. This snapshot approach helps you quickly assess your overall security posture and identify sites that need immediate attention.

What does the site permissions for your organization report show me?

The site permissions for your organization report captures your organization's permission state at a specific point in time, giving you a complete overview of:

- **Total permissioned users**: All unique users who can access the site and its content at site level and item level. This helps you compare sites and identify those with the broadest exposure.
- **Microsoft Entra groups**: Number of cloud-only groups with permissions at all scopes. This helps you understand how group-based access contributes to overall exposure.
- **Broken inheritance**: Reveals how many items have unique permissions that override the site's default settings.
- **Everyone except external users (EEEU) permissions**: Content shared with all internal users
- **Everyone permissions**: Content shared with all users, including guests
- **Guest user permissions**: Access granted to guests marked with #EXT# in their identities
- **External participant permissions**: Access for external users who can sign in with their own credentials
- **Sharing links**: Counts the number of:
  - Anyone links
  - People in your organization links

...and more. For the complete list of metrics captured in the report, see the Download the site permissions for your organization reports section later in this article.

When to use the site permissions for your organization report?

We recommend running the site permissions for your organization report in combination with other Data access governance reports, to get a complete and ongoing picture of your organization's data access landscape. Here's how to use them together effectively:

1. **Start with snapshot reports**: Run site permissions for your organization and for your users reports, along with sensitivity label reports first to understand your baseline permission structure and identify sites with the broadest exposure. We recommend running these reports quarterly to maintain a comprehensive view of your organization's data access.
2. **Follow up with activity reports**: Use sharing links and EEEU activity reports to monitor recent oversharing activities and catch emerging risks. We recommend running these monthly to stay on top of ongoing sharing activities.

Why the site permissions for your organization report matters for Copilot?

Since Copilot respects existing permissions, understanding your current permission structure is critical before deployment. Sites with many users accessing content pose higher risk for unintended data exposure through Copilot interactions. The site permissions for your organization report prioritizes sites with the highest user counts, helping you focus remediation efforts where they're most needed.

Run the site permissions for your organization report

> **Important**
>
> Review these important details before creating your first report:
>
> - The system creates separate reports for SharePoint and OneDrive sites
> - The first report takes up to 5 days to complete, regardless of your organization's size
> - Subsequent reports complete within 24 hours
> - Reports capture data from up to 48 hours before generation
> - You can run reports again every 30 days

> **Note**

Not all sites in your organization are included in this report. Sites with a NoAccess (lock status) are excluded because role assignments and group information can't be retrieved for them. Archived sites are also excluded for the same reason. Sites that are unlocked or in a **ReadOnly** lock state are included.

Here's how to run the site permissions for your organization report:

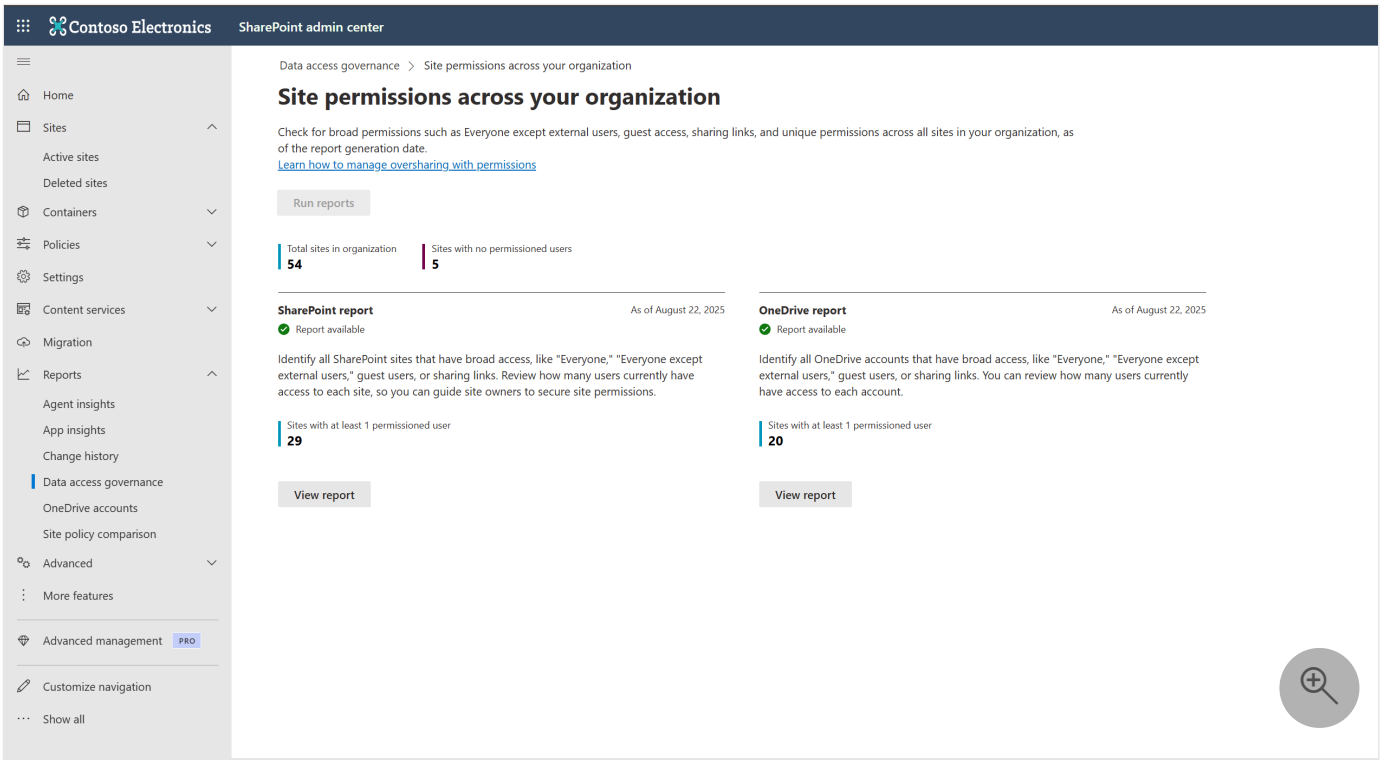
1. From the Data access governance landing page, select **View reports** under **Site permissions across your organization**.
2. Select **Create report** to generate your first report. If you've already created reports, select **Run reports** (when enabled) to get the latest data.

How to view the site permissions for your organization report?

After your report is ready, you can view a summary of the permissions across your organization.

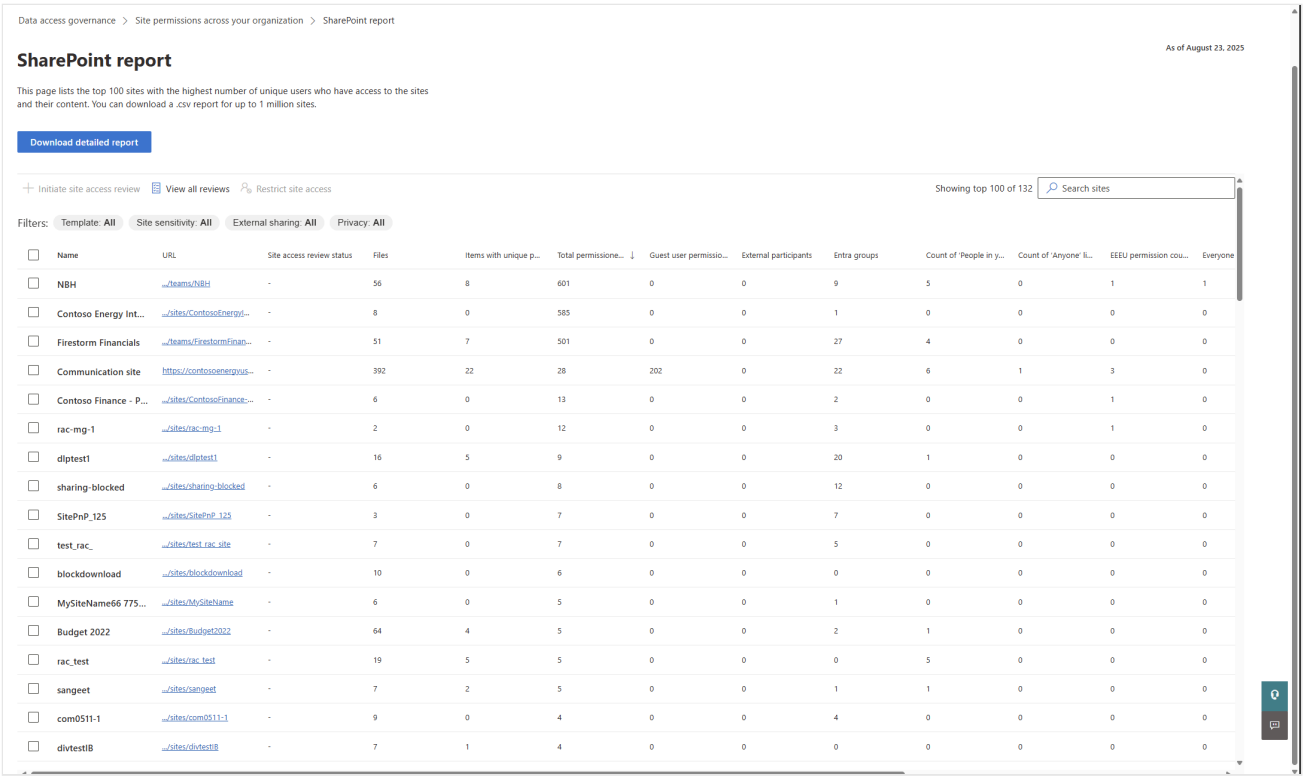
The report summary page displays:

- **Total sites scanned**: The number of SharePoint and OneDrive sites analyzed for permissions
- **Sites without users**: How many sites have no user permissions assigned
- **Sites with user permissions**: The remaining sites that have at least one user with access permissions (separated by SharePoint and OneDrive)
- **Report date**: When the data was captured (up to 48 hours before generation)



To view detailed results:

1. Select **View report** under either the SharePoint or OneDrive section
2. The report displays the top 100 sites with the highest number of users who have permissions



Name	URL	Site access review status	Files	Items with unique p...	Total permissione...	Guest user permissio...	External participants	Entra groups	Count of 'People in y...	Count of 'Anyone' li...	EEEU permission cou...	Everyone
NBH	.../teams/NBH	-	56	8	601	0	0	9	5	0	1	1
Contoso Energy Int...	.../sites/ContosoEnergyI...	-	8	0	585	0	0	1	0	0	0	0
Firestorm Financials	.../teams/FirestormFinan...	-	51	7	501	0	0	27	4	0	0	0
Communication site	https://contosoenergyus...	-	392	22	28	202	0	22	6	1	3	0
Contoso Finance - P...	.../sites/ContosoFinance-...	-	6	0	13	0	0	2	0	0	1	0
rac-mg-1	.../sites/rac-mg-1	-	2	0	12	0	0	3	0	0	1	0
dlptest1	.../sites/dlptest1	-	16	5	9	0	0	20	1	0	0	0
sharing-blocked	.../sites/sharing-blocked	-	6	0	8	0	0	12	0	0	0	0
SitePnP_125	.../sites/SitePnP_125	-	3	0	7	0	0	7	0	0	0	0
test_rac_	.../sites/test_rac_site	-	7	0	7	0	0	5	0	0	0	0
blockdownload	.../sites/blockdownload	-	10	0	6	0	0	0	0	0	0	0
MySiteName66 775...	.../sites/MySiteName	-	6	0	5	0	0	1	0	0	0	0
Budget 2022	.../sites/Budget2022	-	64	4	5	0	0	2	1	0	0	0
rac_test	.../sites/rac_test	-	19	5	5	0	0	0	5	0	0	0
sangeet	.../sites/sangeet	-	7	2	5	0	0	1	1	0	0	0
com0511-1	.../sites/com0511-1	-	9	0	4	0	0	4	0	0	0	0
divtestIB	.../sites/divtestIB	-	7	1	4	0	0	0	0	0	0	0

This visualization helps you quickly identify sites with the broadest access, making them priority candidates for review and potential remediation.

How "Total permissioned users" is calculated

This critical metric represents all unique users who can access the site and its content at any level:

- **Site-level access**: Users in SharePoint groups (owners, members, visitors) have access to all site content. These groups can include both individual users and Microsoft Entra groups.
- **Item-level access**: Users granted permissions to specific files or folders through broken inheritance. These permissions can be assigned to individuals, SharePoint groups, or Microsoft Entra groups.

  The system calculates this number by:
  - Expanding all groups across all permission levels
  - Removing duplicate users
  - Counting the remaining unique users

Understanding current vs. potential exposure

- **Current exposure**: When you add users directly or through Microsoft Entra groups, the "Total permissioned users" count increases immediately based on the group size or number of individuals added.
- **Potential exposure**: Creating sharing links or granting access to "Everyone except external users" doesn't automatically increase the user count. These actions create potential exposure that only becomes actual exposure when users access the content through these links.

Download the site permissions for your organization reports

You can download the report as a CSV file to analyze up to 1 million sites offline.

The downloaded report contains the following information:

Expand table

Column	Description
TenantID	GUID identifying the organization
Site ID	GUID identifying the organization
Site Name	Name of the site
Site URL	URL of the site
Site Template	Specifies the type of site. Has values such as Communication site, Team site, Team site (no Microsoft 365 Groups), Other sites
Primary admin	Site administrator marked as Primary in Active sites page
Primary admin email	Email of primary site administrator
ExternalSharing	Specifies whether content can be shared with external guests. Yes or No.
Site Privacy	Applicable in Microsoft 365 connected team sites. Specifies the privacy setting of the group. Has values Public or Private
Site Sensitivity	Specifies the sensitivity label applied to the site
Number of users having access	Unique number of users having access to site content at any level/scope
Guest user permissions	Count of permissions to guests at any level/scope. These users are marked with #EXT# in their Microsoft Entra identities

Column	Description
External participant permissions	Count of permissions to external users who can directly use their own credentials to sign-in and collaborate, such as in Shared channels
Microsoft Entra group permission count	Number of permissions to Microsoft Entra cloud only groups at all scopes
File count	Approximate number of all files in the site
Items with unique permissions count	Extent of broken inheritance. Count of all items where inheritance was broken and unique permissions were assigned
People In Your Org link count	Number of existing PeopleInYourOrg links across all the files in the site
Anyone link count	Number of existing Anyone links across all the files in the site
EEEU permission count	Number of permissions with 'Everyone except external users' as the recipient at any level/scope
Everyone permission count	Number of permissions with 'Everyone' as the recipient at any level/scope
Report Date	Time of generation of report. It might take up to 48 hours to reflect any changes in the report

> **Important**
>
> Note that the EEEU and Everyone permission counts don't include permissions assigned through hidden system files or hidden system groups. These permissions are typically present by design and shouldn't be treated as oversharing. For example, in classic publishing site templates, the Everyone group appears within the **Style Resources Reader** system group. This group controls read access to the Master Page Gallery and provides limited access to the Style Library. Including Everyone in this group is intentional because these shared resources apply to all pages in the site. Without access to them, users might see pages that are broken or missing styling when content is shared.

Take action based on site permissions for your organization report findings

After discovering potential oversharing through site permissions for your organization reports, you can take action to remediate risks and improve your organization's data access governance. See Remedial actions from data access governance reports.

Last updated on 07/16/2026

Discover sites accessible by a given user with the snapshot report

The **Site permissions for users** report is one of the Data access governance snapshot reports available with SharePoint Advanced Management. This report lists all sites a user can access and helps admins determine whether they can access the entire site or specific sections, granted directly to the user or indirectly through groups. This approach helps you quickly assess your overall security posture and identify sites that need immediate attention.

What does the site permissions for users report show me?

The site permissions for users report captures the permission state of given users at a specific point in time. It gives you a complete overview of sites accessible to these users along with the extent of access. You can determine whether the entire site is shared with the user or only a few files or items are shared. For the complete list of metrics captured in the report, see the Download the site permissions for users section.

When should I use the site permissions for users report?

Use the report when you want to review permissions for users before assigning them a Copilot license. Use it if you want to clean up permissions when the user is about to leave the organization or changed departments.

Run the site permissions for users report

> **Important**
>
> Review these important details before creating your first report:
>
> - Make sure that the site permissions for your organization report is generated at least once.
> - Reports capture data from up to 48 hours before generation.
> - You can have up to five reports.

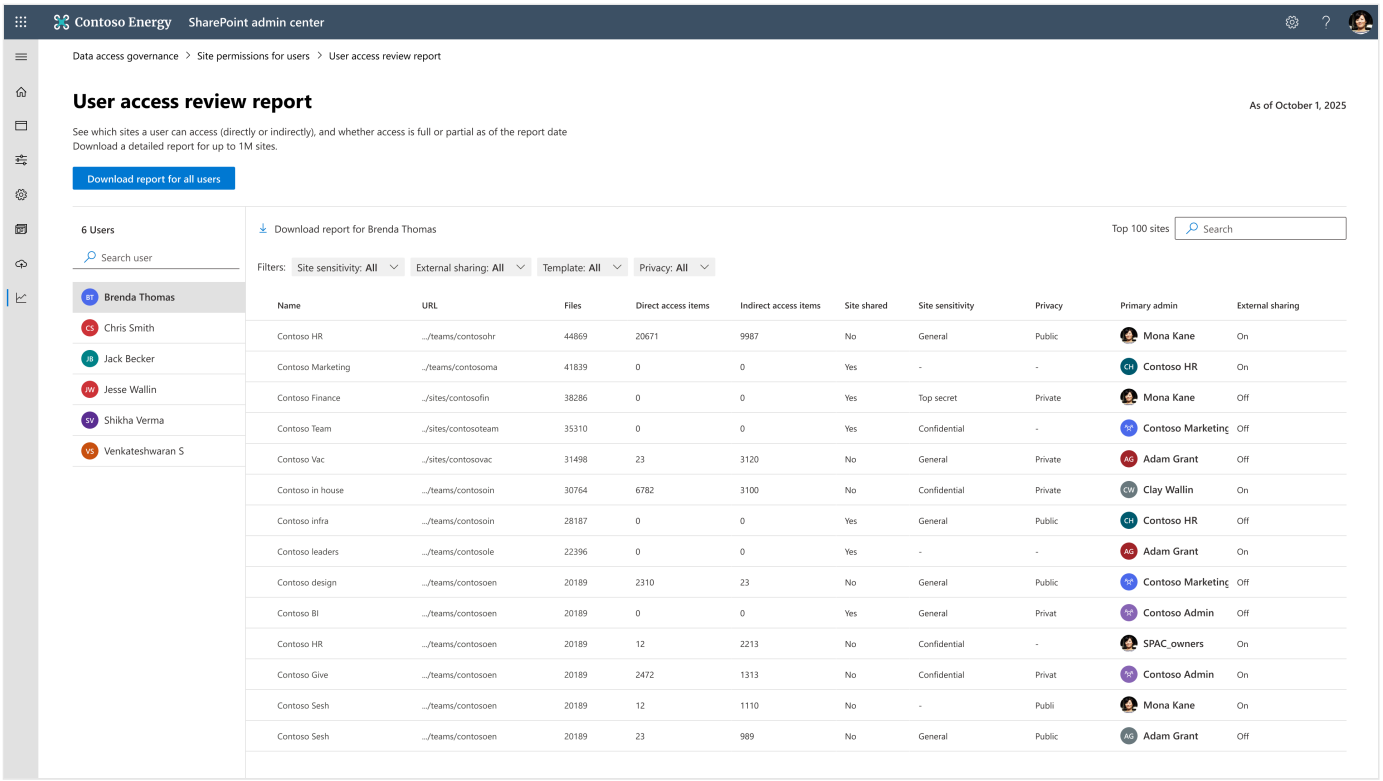
- You can run reports again every 30 days.

Here's how to run the site permissions for users report:

1. From the Data access governance landing page, select **View reports** under **Site permissions for users**.
2. Select **Create report** to generate your report.
3. Select **Add users to report** to select the users for whom you want to generate the report. Select **Save** to save the selections. You can also edit the selection and remove users or add new users, if required.
4. Specify the **Scope** - either SharePoint or OneDrive.
5. Provide the **Report name** - a unique name to identify this report.
6. Select **Create and run** to trigger the creation of report.
7. Check the **Status** column to see if a report is ready or when it was last updated.

How do I view the site permissions for users report?

1. From the Data access governance landing page, select **View reports** under **Site permissions for users**.
2. Review all the available reports and their corresponding status, the list of users for whom the report is generated, how many sites are present in the report, and a button to download the entire report.
3. Select the relevant **Report name**.
4. You see all the users as a list to the left. The right side shows the list of sites accessible to the selected user. The right side also displays whether the user can access the entire site or has access to specific items directly or indirectly.



Download the site permissions for users report

You can download the report for a specific user or for all users by using one of the following options:

1. Select **Download report for** the selected user option to download the report as a CSV file. The file has a limit of 1 million sites.

2. Select **Download detailed report** to get CSV files for all the users given as input, as a ZIP file.

3. On the previous page where all the reports are listed, select **Download report** to get CSV files for all the users given as input, as a ZIP file.

The downloaded report contains the following information:

Expand table

Column	Description
TenantID	GUID identifying the organization
Site ID	GUID identifying the organization
Site Name	Name of the site
Site URL	URL of the site

Column	Description
Site Template	Specifies the type of site. Has values such as Communication site, Team site, Team site (no Microsoft 365 Groups), Other sites
Primary admin	Site administrator marked as Primary in Active sites page
Primary admin email	Email of primary site administrator
ExternalSharing	Specifies whether content can be shared with external guests. Yes or No.
Site Privacy	Applicable in Microsoft 365 connected team sites. Specifies the privacy setting of the group. Has values Public or Private
Site Sensitivity	Specifies the sensitivity label applied to the site
Files	Approximate number of all files in the site
Is site shared	Specifies if the user is part of one or more SharePoint groups with site-level access. Yes or No.
Items with direct access count	Number of files or folders shared directly with the user
Items with indirect access count	Number of files or folders the user can access by being part of a group.
Microsoft Entra object ID	GUID identifying the user in Microsoft Entra
User principle name	Unique name identifying the user in Microsoft Entra
Display name	Name as displayed in people selection/search related experiences
Report Date	Time of generation of report. It might take up to 48 hours to reflect any changes in the report

Last updated on 07/01/2026

Get item-level permission details for "Everyone except external users" and "Everyone"

The **Sites and files shared via special SharePoint groups** report is one of the Data access governance snapshot reports available with SharePoint Advanced Management. This report provides exact item-level permission details for every item where the special SharePoint groups **Everyone except external users** (EEEU) or **Everyone** are the recipients.

What does the report show?

The report captures the permission state of the EEEU and Everyone groups at a specific point in time. Each row identifies a single item that either group can access, along with the full hierarchy of identifiers from your organization down to that item, the permission level granted, and the parent group when access is indirect. For the complete list of metrics captured in the report, see the Download the report section.

When should I use this report?

Use this report when you want to find exactly where oversharing happens in your organization and fix it through scripting, rather than depending on individual site owners to review and modify permissions.

Unresolved EEEU permissions are a top oversharing risk. Content shared with these groups is visible to every internal user, and it surfaces directly in Microsoft 365 Copilot search results, which makes cleanup critical for Copilot adoption. Because the report identifies each affected item individually, you can build targeted cleanup programs and scripts instead of reviewing sites one at a time.

Before you begin

Review Prerequisites for SharePoint Advanced Management.

> **Important**
>
> Review these important details before you run your first report:

- Make sure that the site permissions for your organization report is generated at least once.
- Reports capture data from up to 48 hours before generation.
- You need the SharePoint Advanced Admin role. See Assign the SharePoint Advanced Management Administrator role.
- The report covers both SharePoint and OneDrive. You can't scope the report to a single workload.
- The downloaded file is limited to 1 million rows.
- The report doesn't include permissions granted to EEEU or Everyone for system files and system groups.
- You can run reports again every 30 days.

Assign the SharePoint Advanced Management administrator role

Standard SharePoint administrators and Global administrators can't view file properties across sites they don't own. The **SharePoint Advanced Management Administrator** role lets you view file names, paths, and URLs, and modify permissions as appropriate.

A Global administrator must assign the SharePoint Advanced Admin role before you can run this report.

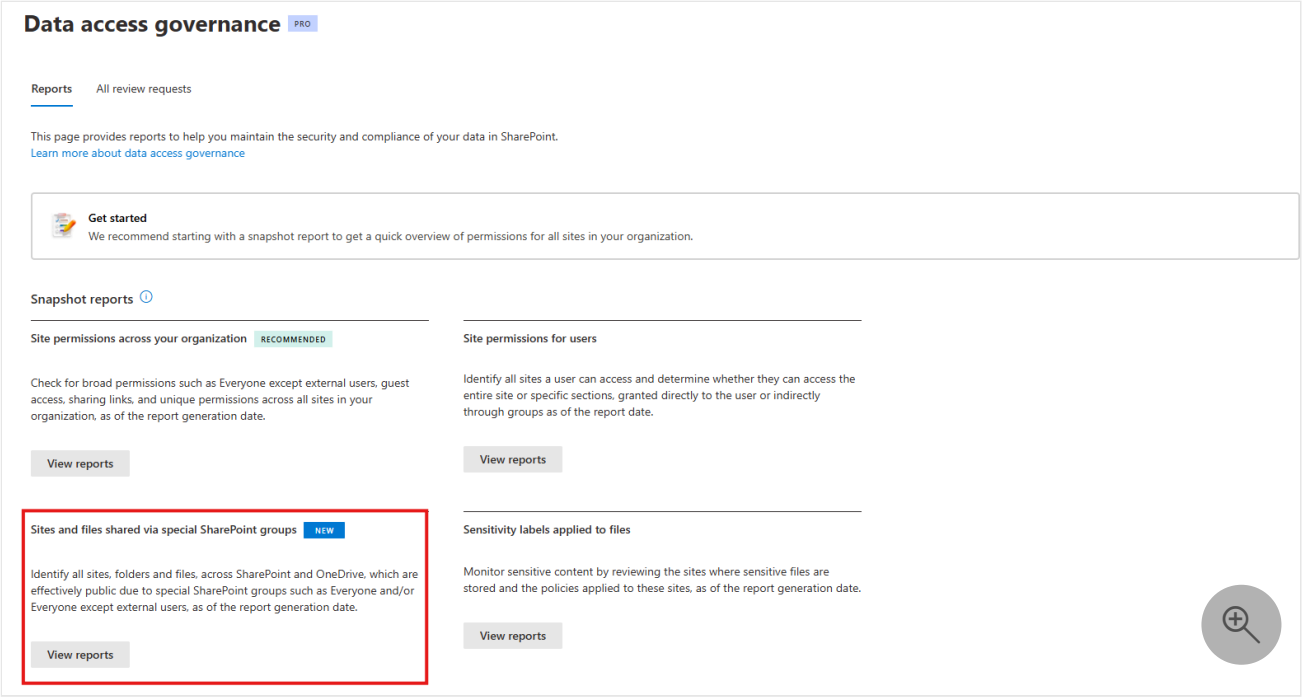
For more information, see RBAC role assignements.

Run the report

The report is available for two special SharePoint groups, and each group has its own report. Here's how to run either one:

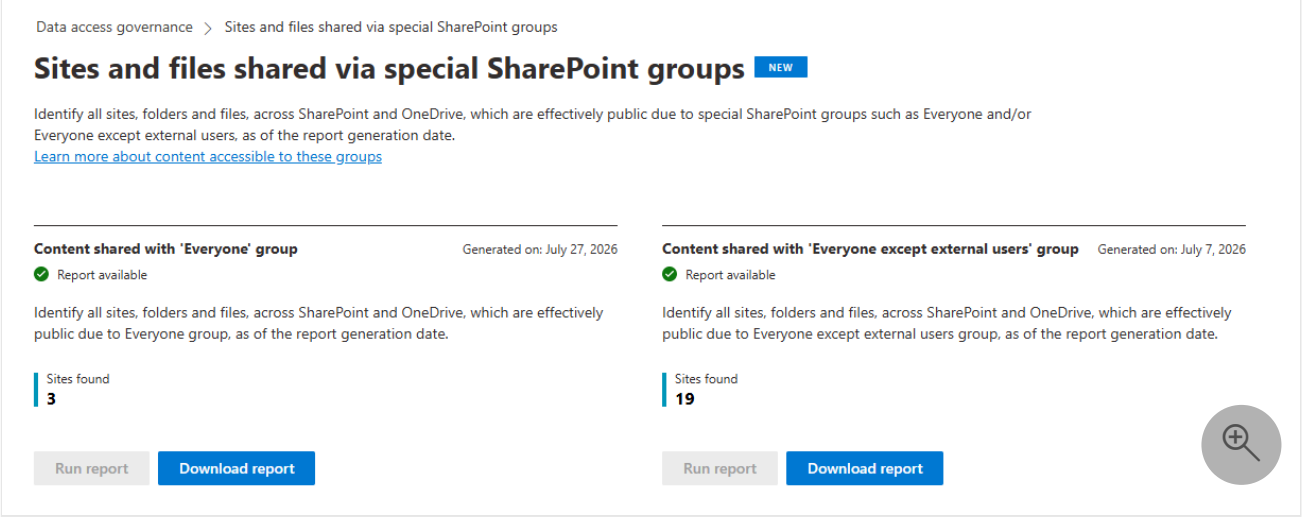
1. In the SharePoint admin center, in the navigation pane, expand **Reports**, and then select **Data access governance**.

2. Under **Snapshot reports**, in the **Sites and files shared via special SharePoint groups** section, select **View reports**.



3. Select **Run report** under either **Content shared with 'Everyone' group** or **Content shared with 'Everyone except external users' group**.

4. Check the status of the report. When the report is ready, the status shows **Report available** along with the date it was generated and the number of sites found.



Download the report

Select **Download report** on the report for the group you want. The download is a ZIP file that contains a CSV file listing all items where that group has direct or indirect access.

The downloaded report contains the following information:

Expand table

Column	Description
TenantId	GUID identifying the organization
SiteId	GUID identifying the site collection
WebId	GUID identifying the root web of the site collection or a subsite
ListId	GUID identifying the list, if applicable
ScopeId	GUID identifying a specific scope of permissions in SharePoint or OneDrive
UniqueId	GUID identifying a specific file or folder. Use it to connect permission data with file metadata.
ListItemId	Position of the item within the list, if applicable
ItemType	Type of the permissioned item. Has values Web (site), List, Folder, or File. File includes list items.
Item Url	URL that gives the name and the absolute path of the item
Role definition	Permission level on the item. Has values such as Full control, Read, Edit, Contributor, Creator, or Viewer.
LinkId	ID of the sharing link, if applicable
LinkScope	Scope of the sharing link permission, such as Read, Write, or Edit
Recipient	Everyone except external users, or Everyone
UserPrincipalName	Everyone except external users, or Everyone
ParentObjectID	Microsoft Entra object ID of the parent entity, when access is indirect
ParentGroupName	Name of the parent group, when access is indirect
ParentGroupEmail	Email of the parent group, if applicable
ParentGroupType	Type of the parent group. Has values Security group, SharePoint group, or Microsoft 365 group.
TotalUserCount	Number of users who accessed the item at least once. The item is already shared with all internal users or with everyone, so this number tells you the actual exposure.
ReportDate	Time of generation of the report

The identifier columns form a hierarchy, from your organization down to the individual item, which lets you pivot or summarize across a specific identifier. For example, filtering on a single site ID shows all permissions within that site across all scopes.

Examples

EEEU is part of a SharePoint group

If EEEU is part of the Contoso Finance visitors group, which makes the Contoso Finance site accessible to your entire organization, the key columns show the following values:

Expand table

Column	Value
ItemType	Web
Item Url	/sites/ContosoFinance
Role definition	Read
Recipient	Everyone except external users
ParentGroupType	SharePointGroup
ParentGroupName	Contoso finance visitors

Any unique permissions for the Contoso Finance visitors group also appear in the report.

A single file is shared with EEEU

If only the file `Doc1.docx` is shared with EEEU, which makes that file accessible to your entire organization, the key columns show the following values:

Expand table

Column	Value
ItemType	File
Item Url	/teams/ContosoFinance/Shared Documents/Doc1.docx
Role definition	Read
Recipient	Everyone except external users
ParentGroupType	Empty
ParentGroupName	Empty

Exceptions

This report doesn't show permissions granted to EEEU or Everyone for system files and system groups.

For example, the report doesn't include the **Everyone** group inside the **Style Resource Readers** group. In classic publishing site templates, the Style Resource Readers group controls read permissions for the Master Page Gallery and restricted access to the Style Library. Including Everyone in this group is intentional, because the master page and style library apply to all pages within the site. Without access to these style resources, users might see broken or unstyled pages when a page is shared with them.

Take action based on the report findings

After you discover potential oversharing, take action to remediate risks and improve your organization's data access governance. For more information, see Remedial actions from Data access governance reports.

Related articles

- What is SharePoint Advanced Management?
- Data access governance reports for SharePoint and OneDrive sites
- Monitor "Everyone except external users" (EEEU) sharing with the EEEU activity report
- Manage Data access governance reports by using SharePoint Online PowerShell

ⓘ**Note:** The author created this article with assistance from AI. Learn more

---

Last updated on 07/30/2026

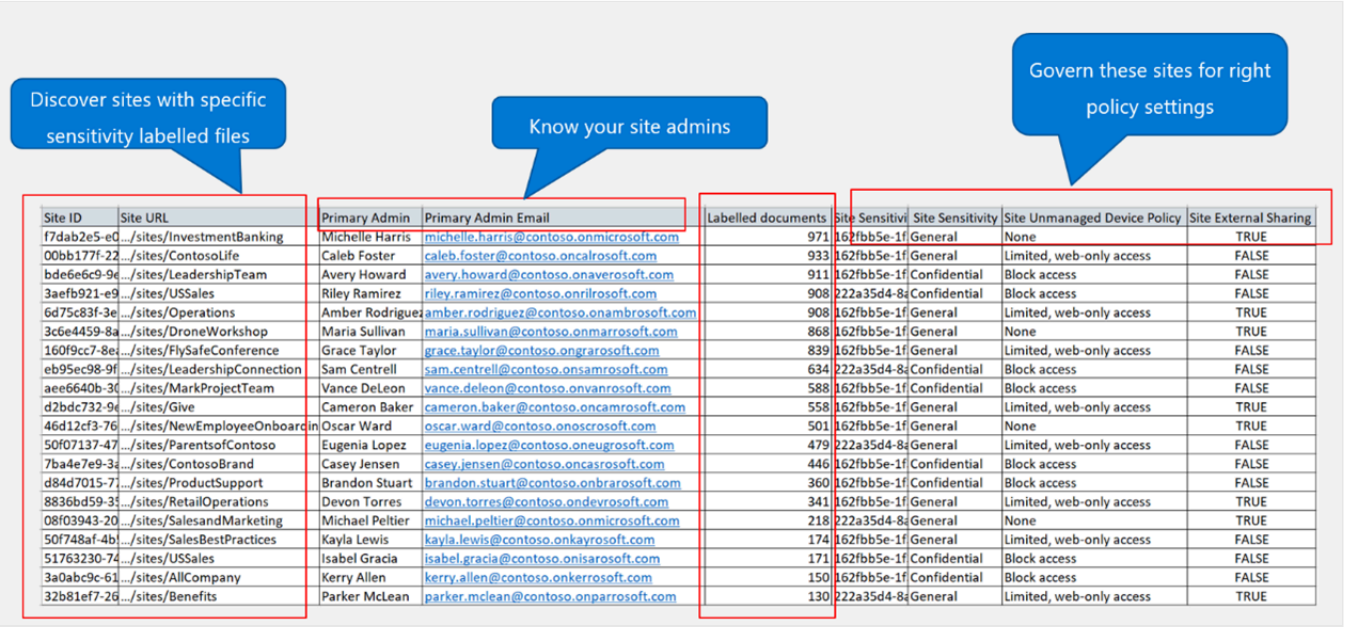
Get the sensitivity label snapshot report for SharePoint and OneDrive sites

Sensitivity label for files report is one of the Data access governance snapshot reports available with SharePoint Advanced Management. This report provides a snapshot of your organization's current sensitivity label distribution across all SharePoint and OneDrive sites, helping you understand how your data is classified and protected. This snapshot approach helps you quickly assess your overall data protection posture and identify sites that need immediate attention.

What does the sensitivity label report show me?

The sensitivity label report includes the following information:

- **Sites with labeled files**: Lists sites containing the highest number of Office files with the selected sensitivity label applied
- **Applied policies**: Shows which security policies are active on each site:
  - Site sensitivity labels
  - Site unmanaged device access controls
  - Site external sharing settings



Site ID	Site URL	Primary Admin	Primary Admin Email	Labelled documents	Site Sensitivi	Site Sensitivity	Site Unmanaged Device Policy	Site External Sharing
f7dab2e5-e0	.../sites/InvestmentBanking	Michelle Harris	michelle.harris@contoso.onmicrosoft.com	971	162fbb5e-1f	General	None	TRUE
00bb177f-22	.../sites/ContosoLife	Caleb Foster	caleb.foster@contoso.oncalrosoft.com	933	162fbb5e-1f	General	Limited, web-only access	FALSE
bde6e6c9-9c	.../sites/LeadershipTeam	Avery Howard	avery.howard@contoso.onaverosoft.com	911	162fbb5e-1f	Confidential	Block access	FALSE
3aefb921-e9	.../sites/USSales	Riley Ramirez	riley.ramirez@contoso.onrilrosoft.com	908	222a35d4-8a	Confidential	Block access	FALSE
6d75c83f-3e	.../sites/Operations	Amber Rodriguez	amber.rodriguez@contoso.onambrosoft.com	908	162fbb5e-1f	General	Limited, web-only access	TRUE
3c6e4459-8a	.../sites/DroneWorkshop	Maria Sullivan	maria.sullivan@contoso.onmarrosoft.com	868	162fbb5e-1f	General	None	TRUE
160f9cc7-8e	.../sites/FlySafeConference	Grace Taylor	grace.taylor@contoso.ongrarosoft.com	839	162fbb5e-1f	General	Limited, web-only access	FALSE
eb95ec98-9f	.../sites/LeadershipConnection	Sam Centrell	sam.centrell@contoso.onsamrosoft.com	634	222a35d4-8a	Confidential	Block access	FALSE
aee6640b-3(	.../sites/MarkProjectTeam	Vance DeLeon	vance.deleon@contoso.onvanrosoft.com	588	162fbb5e-1f	Confidential	Block access	FALSE
d2bdc732-9(	.../sites/Give	Cameron Baker	cameron.baker@contoso.oncamrosoft.com	558	162fbb5e-1f	General	Limited, web-only access	TRUE
46d12cf3-76	.../sites/NewEmployeeOnboardin	Oscar Ward	oscar.ward@contoso.onoscrosoft.com	501	162fbb5e-1f	General	None	TRUE
50f07137-47	.../sites/ParentsofContoso	Eugenia Lopez	eugenia.lopez@contoso.oneugrosoft.com	479	222a35d4-8a	General	Limited, web-only access	FALSE
7ba4e7e9-3a	.../sites/ContosoBrand	Casey Jensen	casey.jensen@contoso.oncasrosoft.com	446	162fbb5e-1f	Confidential	Block access	FALSE
d84d7015-7	.../sites/ProductSupport	Brandon Stuart	brandon.stuart@contoso.onbrarosoft.com	360	162fbb5e-1f	Confidential	Block access	FALSE
8836bd59-3	.../sites/RetailOperations	Devon Torres	devon.torres@contoso.ondevrosoft.com	341	162fbb5e-1f	General	Limited, web-only access	TRUE
08f03943-20	.../sites/SalesandMarketing	Michael Peltier	michael.peltier@contoso.onmicrosoft.com	218	222a35d4-8a	General	None	TRUE
50f748af-4b	.../sites/SalesBestPractices	Kayla Lewis	kayla.lewis@contoso.onkayrosoft.com	174	162fbb5e-1f	General	Limited, web-only access	FALSE
51763230-74	.../sites/USSales	Isabel Gracia	isabel.gracia@contoso.onisarosoft.com	171	162fbb5e-1f	Confidential	Block access	FALSE
3a0abc9c-61	.../sites/AllCompany	Kerry Allen	kerry.allen@contoso.onkerrosoft.com	150	162fbb5e-1f	Confidential	Block access	FALSE
32b81ef7-26	.../sites/Benefits	Parker McLean	parker.mclean@contoso.onparrosoft.com	130	222a35d4-8a	General	Limited, web-only access	TRUE

This data helps you verify that sites containing sensitive content have appropriate security policies in place.

When to use the sensitivity label report?

We recommend running the sensitivity label report in combination with other Data access governance reports, to get a complete and ongoing picture of your organization's data access landscape. Here's how to use them together effectively:

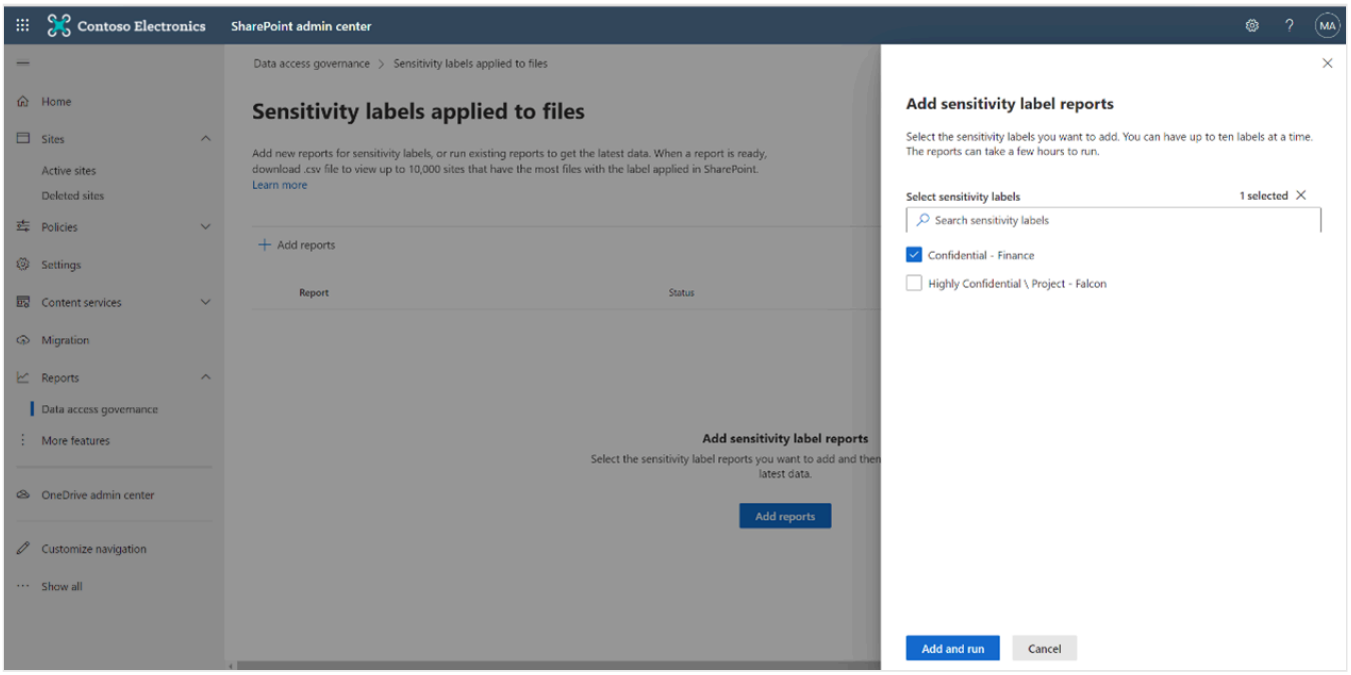
1. **Start with snapshot reports**: Run site permissions reports and sensitivity label reports first to understand your baseline permission structure and identify sites with the broadest exposure. We recommend running these quarterly to maintain a comprehensive view of your organization's data access.
2. **Follow up with activity reports**: Use sharing links and EEEU activity reports to monitor recent oversharing activities and catch emerging risks. We recommend running these monthly to stay on top of ongoing sharing activities.

How to add sensitivity label reports?

> **Important**
>
> Review these important details before creating your first report:
>
> - Reports are created for SharePoint sites only (OneDrive is not currently supported)
> - Reports may take up to 24 hours to complete
> - Reports capture data from up to 120 hours before generation
> - You can run reports again every 24 hours

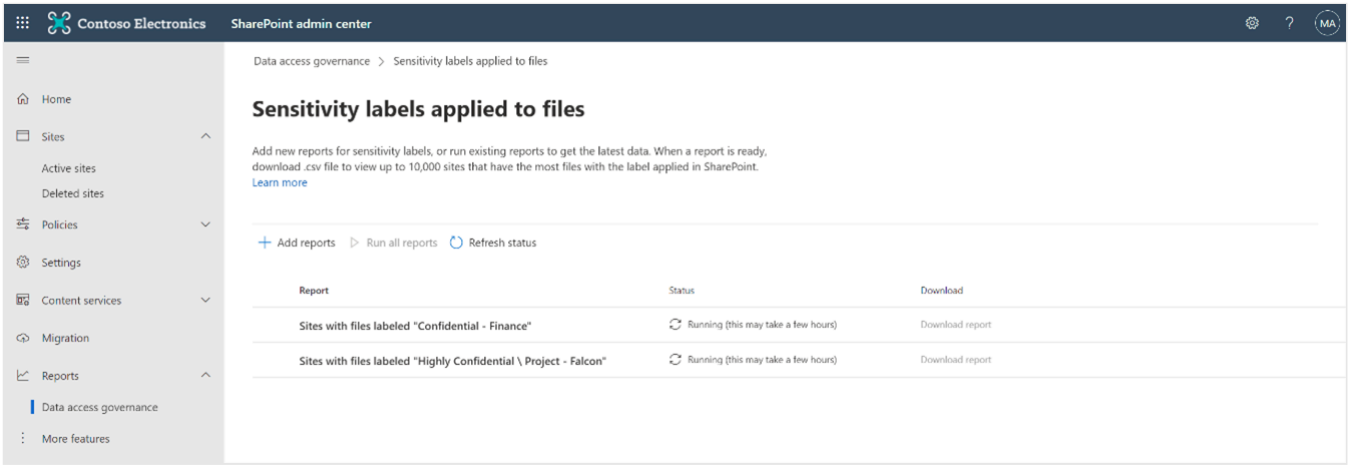
You can create a sensitivity label report for each label you want to monitor. When you add a report, the system automatically runs it for the first time.

> **Note**
>
> You can only create reports for sensitivity labels that have 'File' included in their scope.



Run sensitivity label reports

To get the latest data for each report, you need to manually run it. You can run all reports at once or select individual reports to run. To check if a report is ready or see when it was last updated, check the **Status** column.



Download the sensitivity label reports

After running a report, you can download the data as a CSV file for offline analysis. Here's how:

1. Select the report name to access the download option
2. Download the CSV file containing up to 10,000 sites

Take action based on sensitivity label report findings

After discovering potential oversharing through sensitivity label reports, you can take action to remediate risks and improve your organization's data access governance. See Data access governance reports.

Last updated on 04/03/2026

Monitor sharing activities in SharePoint with sharing links activity reports

Sharing links activity reports are one of the two types of Data access governance activity reports available with SharePoint Advanced Management. These reports help you identify sites where users have created the most new sharing links in the last 28 days. Combined with other Data access governance reports, this report helps you monitor sharing activities and identify potential oversharing risks in your organization.

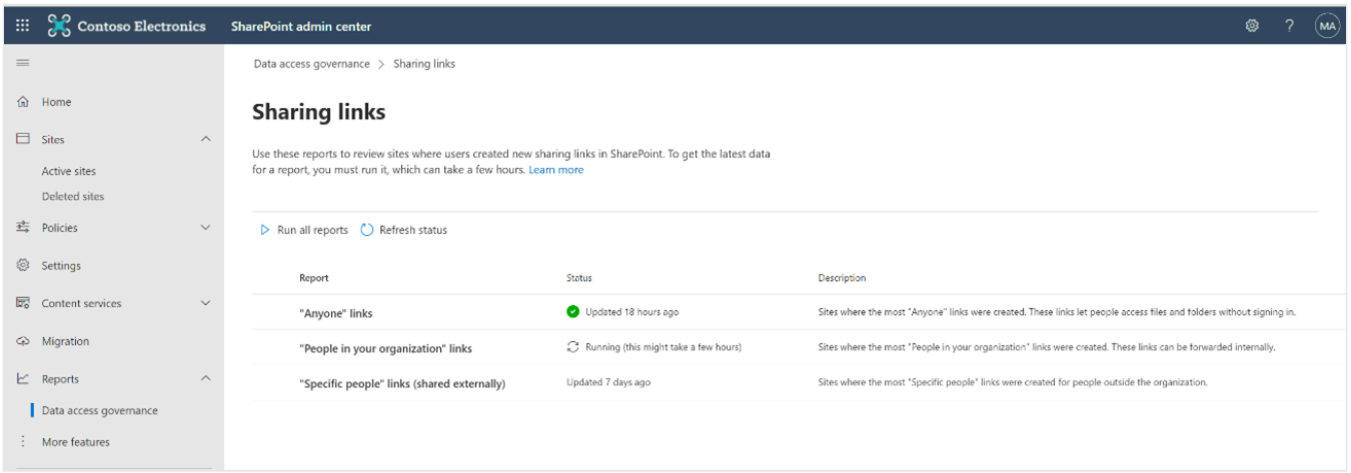
What do sharing links activity reports show me?

Sharing links reports show information for the following types of links:

Expand table

Name of report	Description
'Anyone' links	This report provides a list of sites in which the highest number of "Anyone" links were created. "Anyone" links allow anyone to access files and folders without signing in.
'People in the organization' links	This report provides a list of sites in which the highest number of 'People in the organization' links were created. These links can be forwarded internally and allow anyone in the organization to access files and folders.
'Specific people' links shared externally	This report provides a list of sites in which the highest number of 'Specific people' links were created for people outside the organization.

> **Note**
>
> We recommend running the site permissions report first to understand your organization's current link sharing baseline, then use this activity report to monitor ongoing link sharing activities.



When to use sharing links reports?

We recommend running the sharing links reports in combination with other Data access governance reports, to get a complete and ongoing picture of your organization's data access landscape. Here's how to use them together effectively:

1. **Start with snapshot reports**: Run site permissions reports and sensitivity label reports first to understand your baseline permission structure and identify sites with the broadest exposure. We recommend running these quarterly to maintain a comprehensive view of your organization's data access.
2. **Follow up with activity reports**: Use sharing links and EEEU activity reports to monitor recent oversharing activities and catch emerging risks. We recommend running these monthly to stay on top of ongoing sharing activities.

Run sharing links reports

> **Important**
>
> Review these important details before creating your first report:
>
> - Reports are created for SharePoint sites only. OneDrive support is available via PowerShell
> - Reports may take up to 24 hours to complete
> - Reports capture data from up to 24 hours before generation
> - You can run reports again every 24 hours

To get the latest data for each report, you need to manually run it. You can run all reports at once or select individual reports to run. To check if a report is ready or see when it was last

updated, check the **Status** column.

View sharing links reports

After your report is ready, select the report name to view the data. Each sharing link report displays:

- **Top 100 sites**: Sites with the highest number of sharing links created in the last 30 days
- **Applied policies**: Security policies active on each site:
  - Site sensitivity labels
  - Site unmanaged device controls
  - Site external sharing settings
- **Primary administrator**: The designated admin for each site

> **Note**
>
> OneDrive data is now available via PowerShell.

Download sharing links reports

You can download any report as a CSV file for offline analysis, containing data for up to 1 million sites.

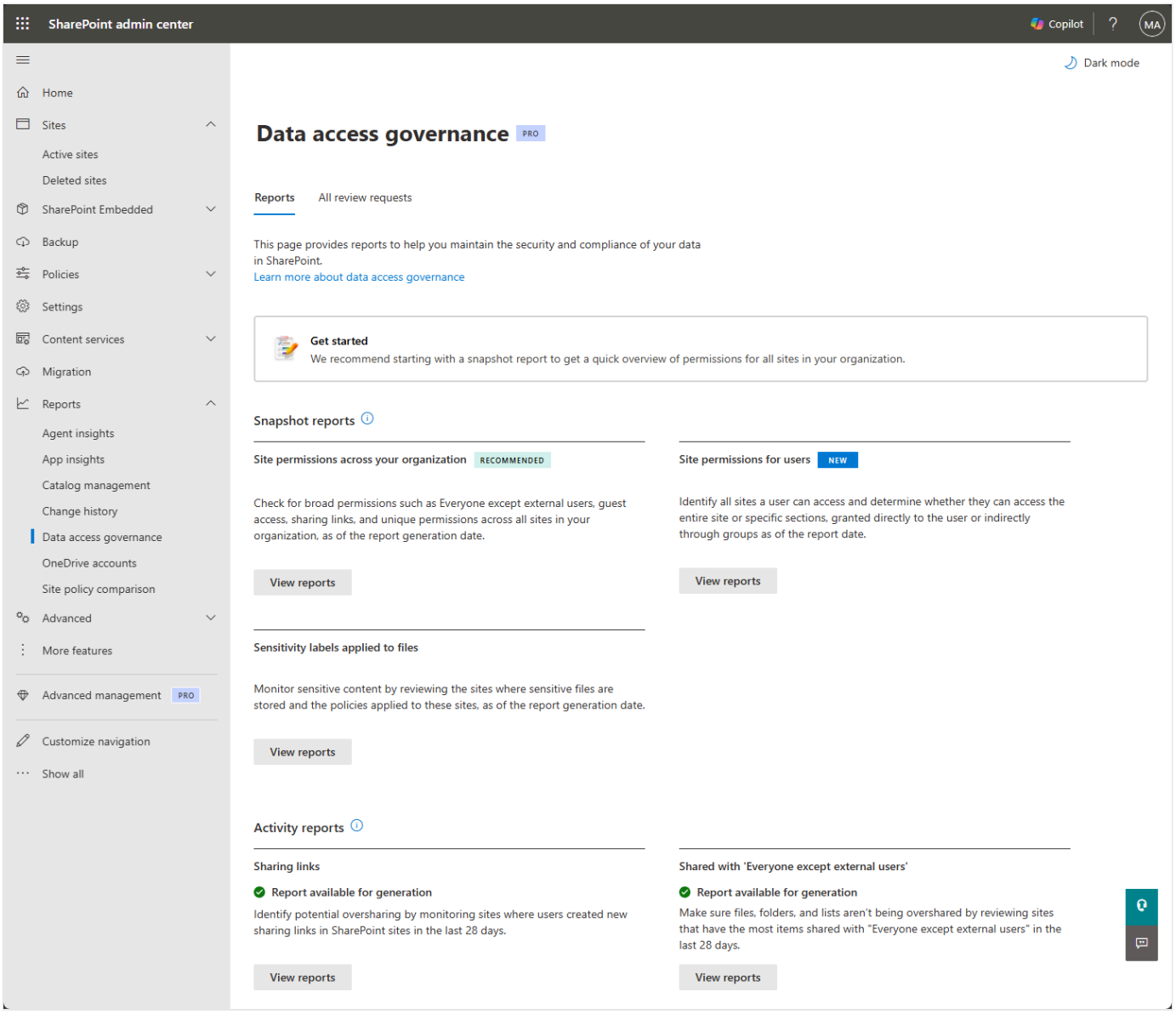
Take action based on sharing links report findings

After discovering potential oversharing through sharing links reports, you can take action to remediate risks and improve your organization's data access governance. See Data access governance reports.

Last updated on 04/03/2026

Monitor "Everyone except external users" (EEEU) sharing with the EEEU activity report

"Everyone except external users" (EEEU) is a built-in SharePoint group that automatically includes all internal users but excludes any external users (guests). The EEEU report is one of the two types of data access governance activity reports that are available with SharePoint Advanced Management.



EEEU activity reports help you identify sites where content is shared with your entire organization in the past 28 days. You can run the site permissions report first to understand your organization's current EEEU sharing baseline, and then use the EEEU activity report to monitor ongoing EEEU sharing activities.

Understand EEEU sharing through public sites and files

Content can be shared with EEEU in two ways:

- **Public sites**: When a site is configured as public, the EEEU group becomes part of the site's membership (owners, members, or visitors). Setting a site as public makes all site content visible to everyone in your organization.
- **Public items**: Individual files or folders can be shared directly with EEEU using the people picker. Setting a file or folder as public makes it accessible to your entire organization, while keeping the rest of the site private.

Monitor EEEU sharing to identify potential risks

Sharing with EEEU can lead to unintended data exposure because it grants access to all current and future employees. You can use EEEU activity reports together with the site permissions report to help you:

- Discover sites with the most EEEU sharing activity in the last 28 days
- Identify potential oversharing risks before they impact your organization
- Take appropriate actions to limit access when necessary

Information shown in EEEU activity reports

Each EEEU activity report shows:

- **Top 100 sites**: Sites with the highest number of items or groups shared with EEEU in the last 28 days
- **Security policies**: Current policies applied to each site:
  - Site sensitivity labels
  - Site privacy settings
  - Site external sharing settings
- **Primary administrator**: The designated admin responsible for each site

Snapshot and activity reports

Use EEEU reports together with other data access governance reports, such as the site permissions report, to get a complete and ongoing picture of your organization's data access landscape.

1. **Start with snapshot reports**: Run site permissions reports first to understand your baseline permission structure. Specifically, get the current state of EEEU sharing.

2. **Follow up with activity reports**: Run the EEEU activity reports to monitor recent EEEU sharing activities and catch emerging risks. Run these reports monthly to stay on top of ongoing sharing activities.

Before you begin

Review Prerequisites for SharePoint Advanced Management.

Keep these important points in mind:

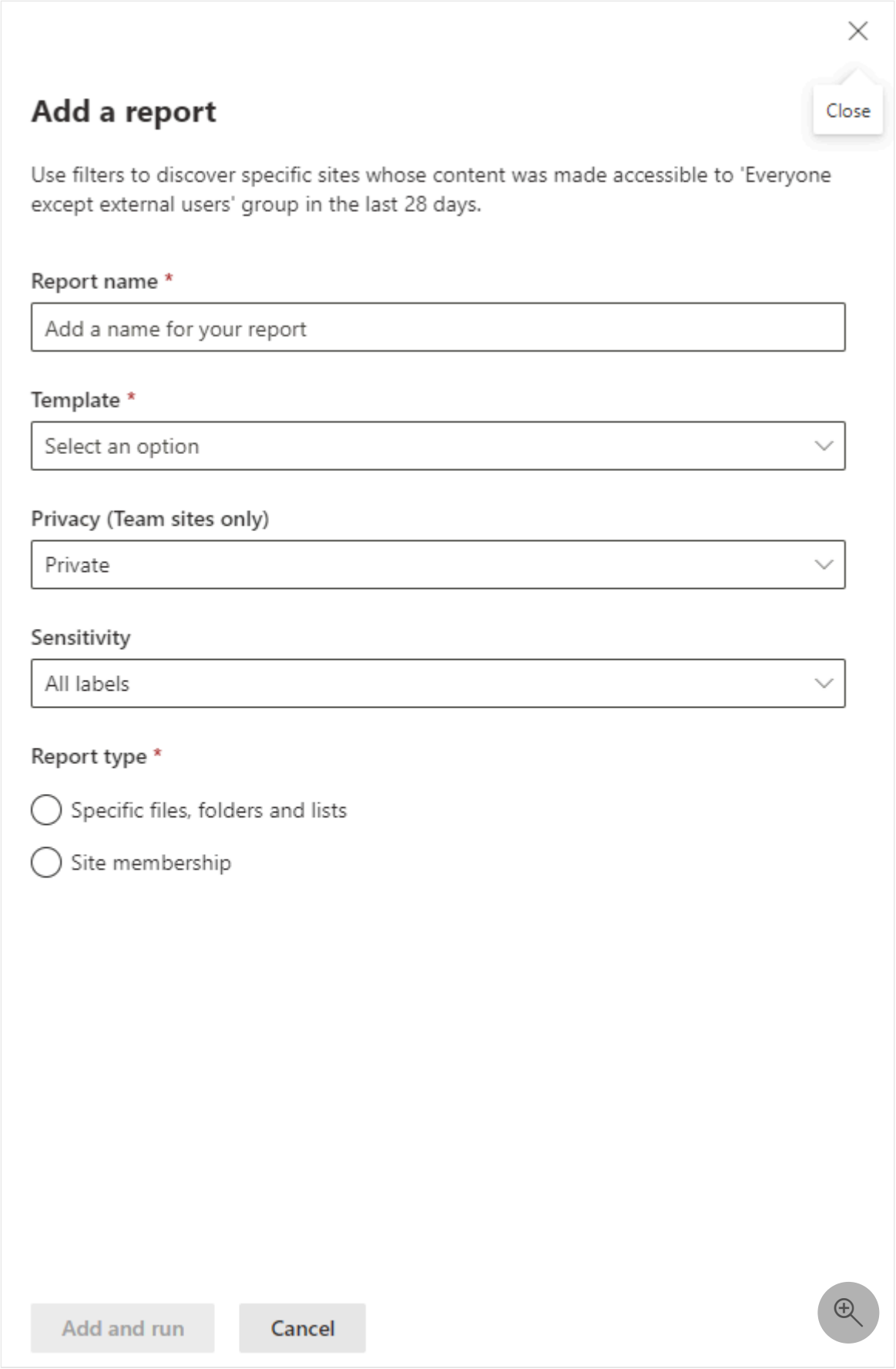
- The EEEU report in the SharePoint admin center covers SharePoint sites only. To get an EEEU report for items in OneDrive, use Identify content shared with "Everyone except external users" in last 28 days.
- You can have up to 10 reports.
- Reports might take up to 24 hours to complete.
- Reports capture data from up to 24 hours before report generation.
- You can run reports again every 24 hours.

Create an EEEU report

1. In the SharePoint admin center, in the navigation pane, expand **Reports**, and then select **Data access governance**.

2. In the **Activity reports** section, under **Shared with 'Everyone except external users'**, select **View reports**.

3. Select **Create report**. The **Create a report** panel opens.



4. Configure your report as follows:

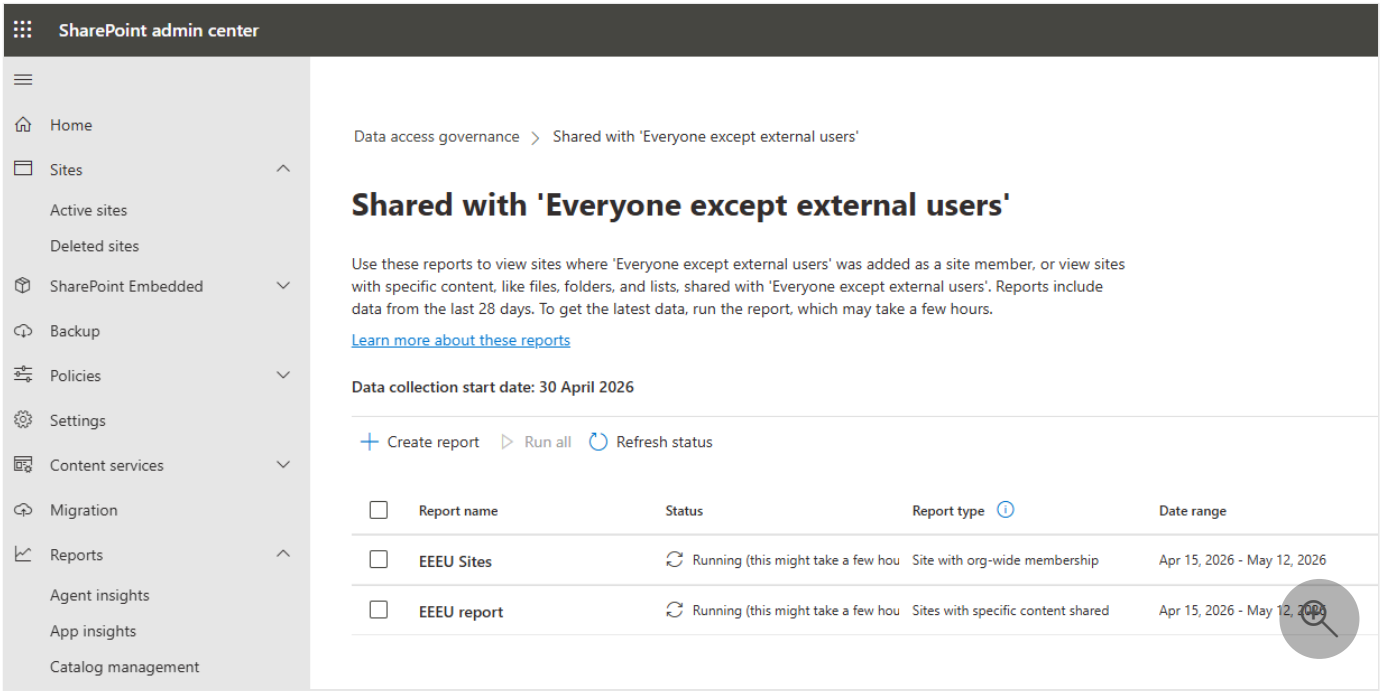
- **Report name**: Enter a unique name to identify this report.
- **Template**: Select which SharePoint site templates to include. You can select multiple template types or choose **All sites**:

    - **Classic sites**
    - **Communication sites**
    - **Team sites**
    - **Others**
- **Privacy**: For Team sites, filter by privacy setting:
    - **Private**
    - **Public**
    - **All** (both private and public)
- **Site sensitivity**: Choose specific sensitivity labels to focus on sites with particular security classifications. For example, you can identify files shared with EEEU within sites labeled as "Confidential" in the last 28 days.
- **Report type**: Select which EEEU scenario to analyze:
    - **Specific files, folders and lists**: Individual files or folders shared with EEEU.
    - **Site membership**: Sites where EEEU is part of the site membership.

5. Select **Create and run**. It might take a few hours for the report to run.

Use the Shared with 'Everyone except external users' report

To view the latest data, run each report manually. The **Status** column indicates whether the report is running or ready to view.



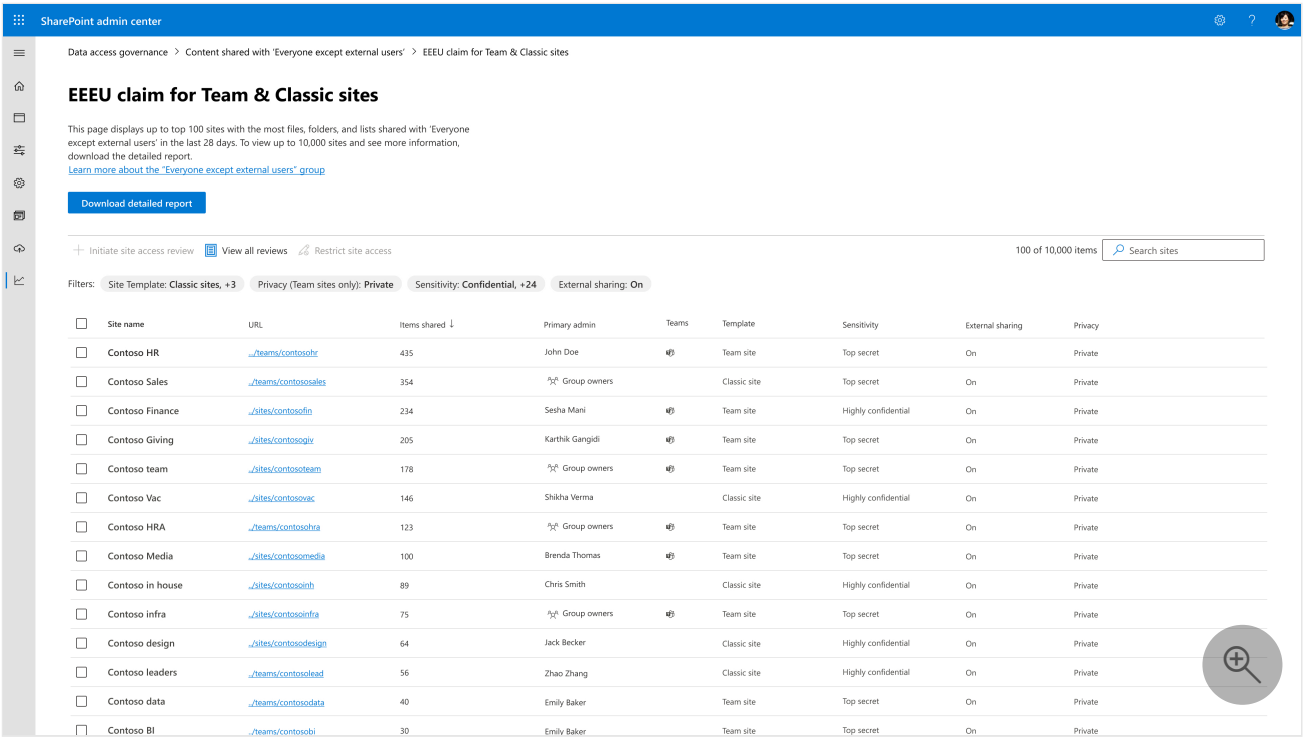
1. In the SharePoint admin center, in the navigation pane, expand **Reports**, and then select **Data access governance reports**.

2. In the **Activity reports** section, under **Shared with 'Everyone except external users'**, select **View reports**.

3. Select one or more reports, and then select **Run**.

4. After your report completes, the **Status** column updates.

5. Select a report to view insights about EEEU sharing activity:



6. To download a report, select **Download detailed report**. You get a CSV file that you can use for detailed analysis.

   The downloaded report contains the following information:

   - Up to 1 million sites sorted by EEEU sharing activity (highest first)
   - Complete site information including:
     - Primary administrator name and email
     - Site template type
     - Privacy settings
     - Sensitivity labels
     - Additional site metadata

Take action based on EEEU report findings

After discovering potential oversharing through EEEU reports, take action to remediate risks and improve your organization's data access governance. For more information, see Data access

governance reports for SharePoint and OneDrive sites.

Related articles

- What is SharePoint Advanced Management?
- Data access governance reports for SharePoint and OneDrive sites

---

Last updated on 05/13/2026

Initiate site access reviews for data access governance reports

Site access reviews in the SharePoint admin center enable IT administrators to delegate the process of reviewing data access governance reports to site owners of overshared sites.

This review process is crucial because:

- Compliance reasons prevent IT administrators from accessing file-level or item-level details.
- Site owners are best positioned to review and address oversharing issues for their own sites.

> **Note**
>
> Site access review supports only SharePoint sites. It currently doesn't support OneDrive accounts.

What do you need to initiate a site access review?

See SharePoint Advanced Management prerequisites.

In addition, before initiating a site access review, make sure site owners are available to respond to review requests, take necessary actions, and complete the review.

Microsoft 365 operated by 21Vianet doesn't support site access reviews, even if you have the required licenses.

How site access review works

- You can initiate site access reviews for up to 100 sites directly from the web view of data access governance reports.
- If you need to review a larger number of sites, use PowerShell to initiate reviews.
- When you initiate a review, the site owner receives an email tailored to the specific oversharing issue identified in the selected report. For example, if the review is for the "Content shared with 'Everyone except external users'" category, the email focuses only on sharing concerns related to that report.

Supported reports

Site access reviews are available for the following reports:

- Sharing link reports (Anyone, PeopleInYourOrg, Specific People shared externally)
- "Content shared with 'Everyone except external users'" reports
- Oversharing baseline report using permissions

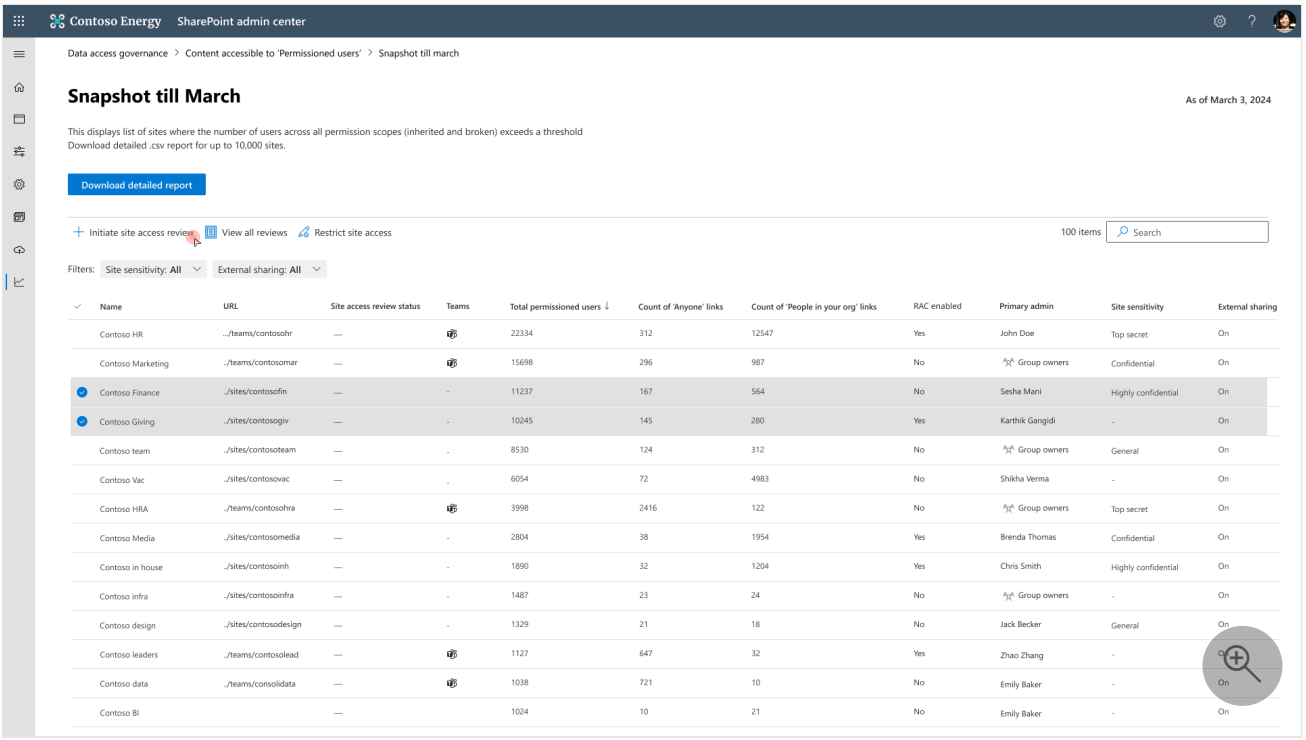
How to initiate a site access review

1. Sign in to the SharePoint admin center with your admin credentials.

2. Expand the **Reports** section and select **Data access governance**.

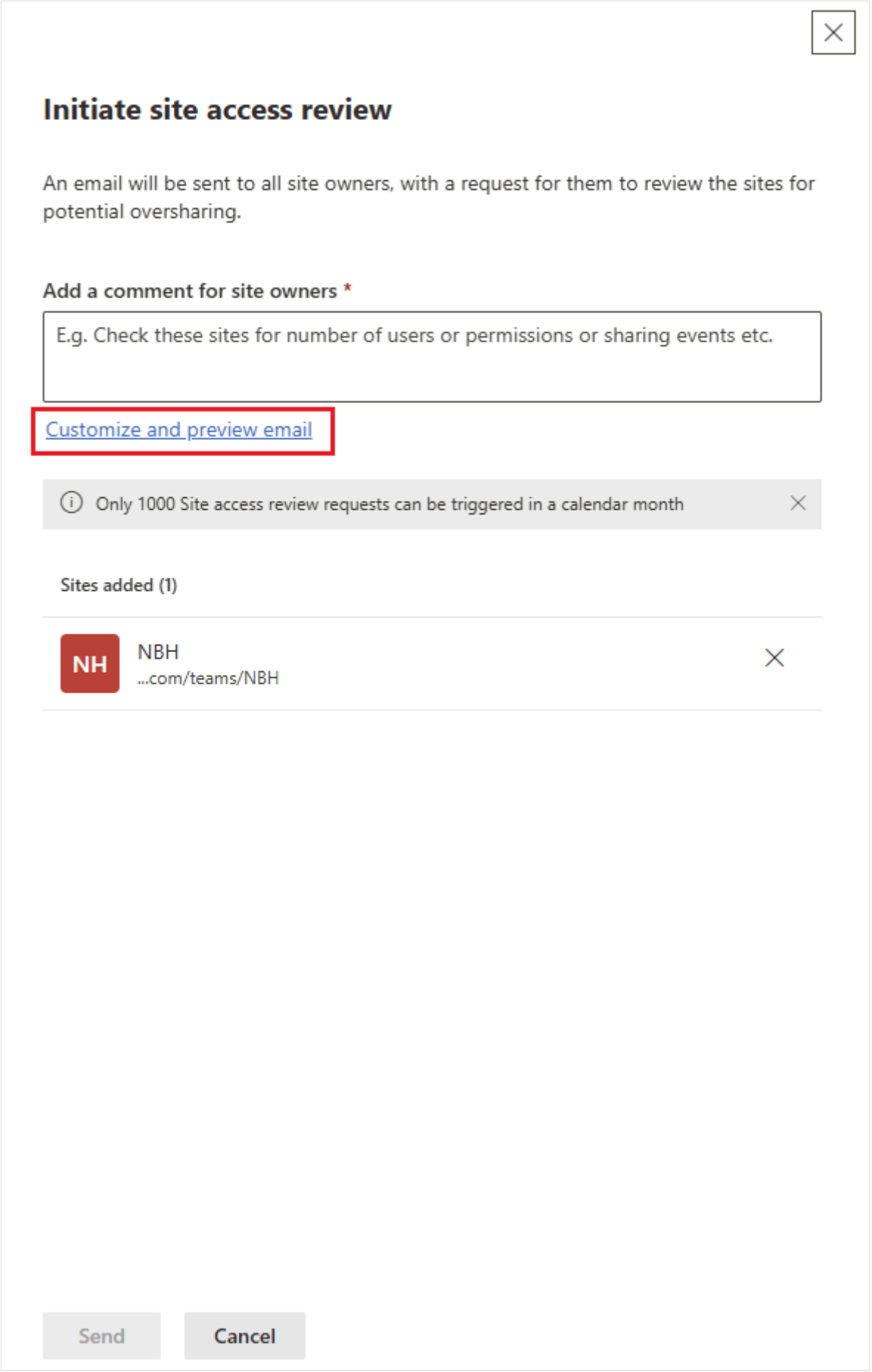
3. Select **View reports** for any one of the supported reports.

4. Choose a report and select the sites you want to review.



5. Select **Initiate site access review**.

6. Select **Customize and preview email** to customize the email contents for site owners.



7. Customize the message to site owners as described in the email customization section.

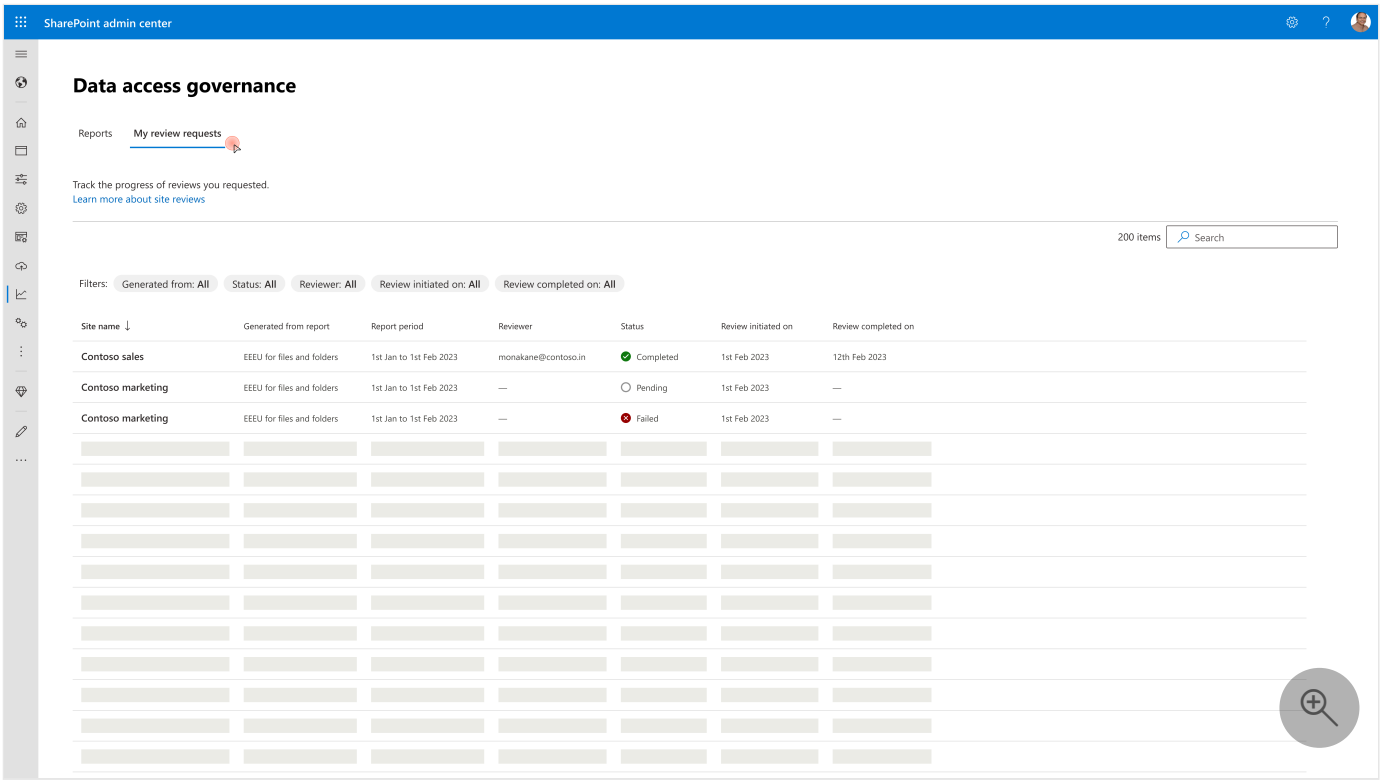
8. Select **Send** to initiate the review request.

You can also initiate site access reviews by using PowerShell.

> **Important**
>
> You can initiate up to 1,000 site access reviews from the **Site permissions across your organization** report each calendar month. The limit resets when the month changes.

Track site access reviews

To track all initiated site access reviews, go to the **My review requests** tab on the Data access governance landing page.



Once a review is initiated, its status stays "pending" until the site owner completes it. After completion, the review status and comments update with the reviewer's name and the date and time of completion. If a review fails (for example, due to an invalid email for the site owner), it's marked as failed.

You can also Track site access reviews by using PowerShell.

Site access review process for site owners

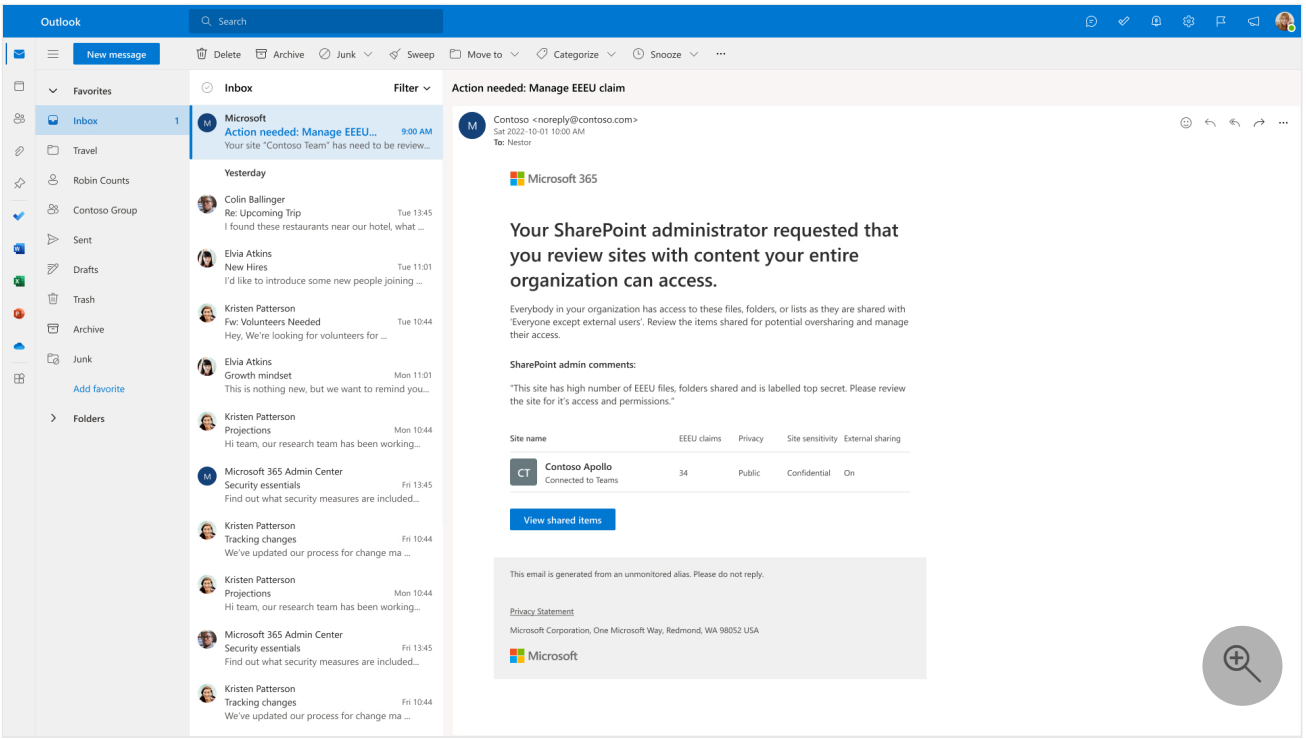
When you start a review, site owners get an email that includes:

- A relevant title.

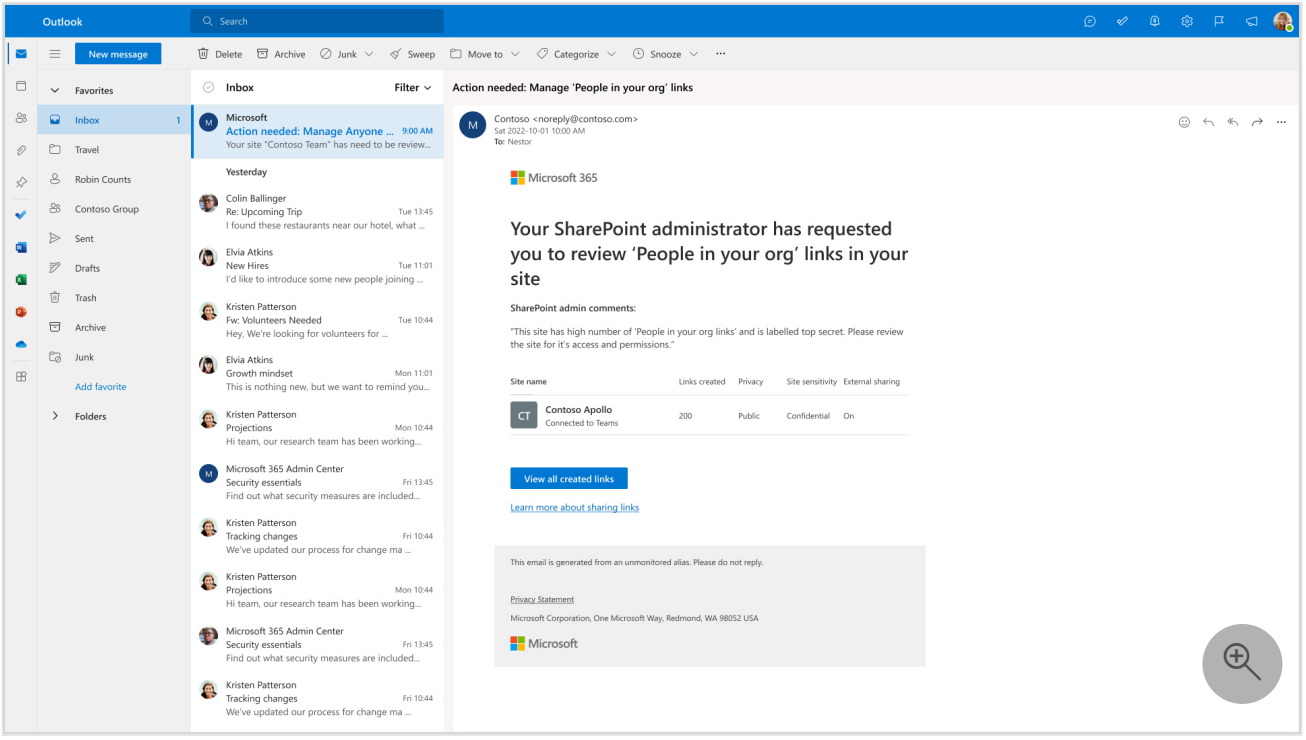
- Your comments, if any.
- A request to review site permissions.
- A link to a detailed access review page, specific to the identified issue in the data access governance report.

Here are examples of the different emails a site owner might receive:

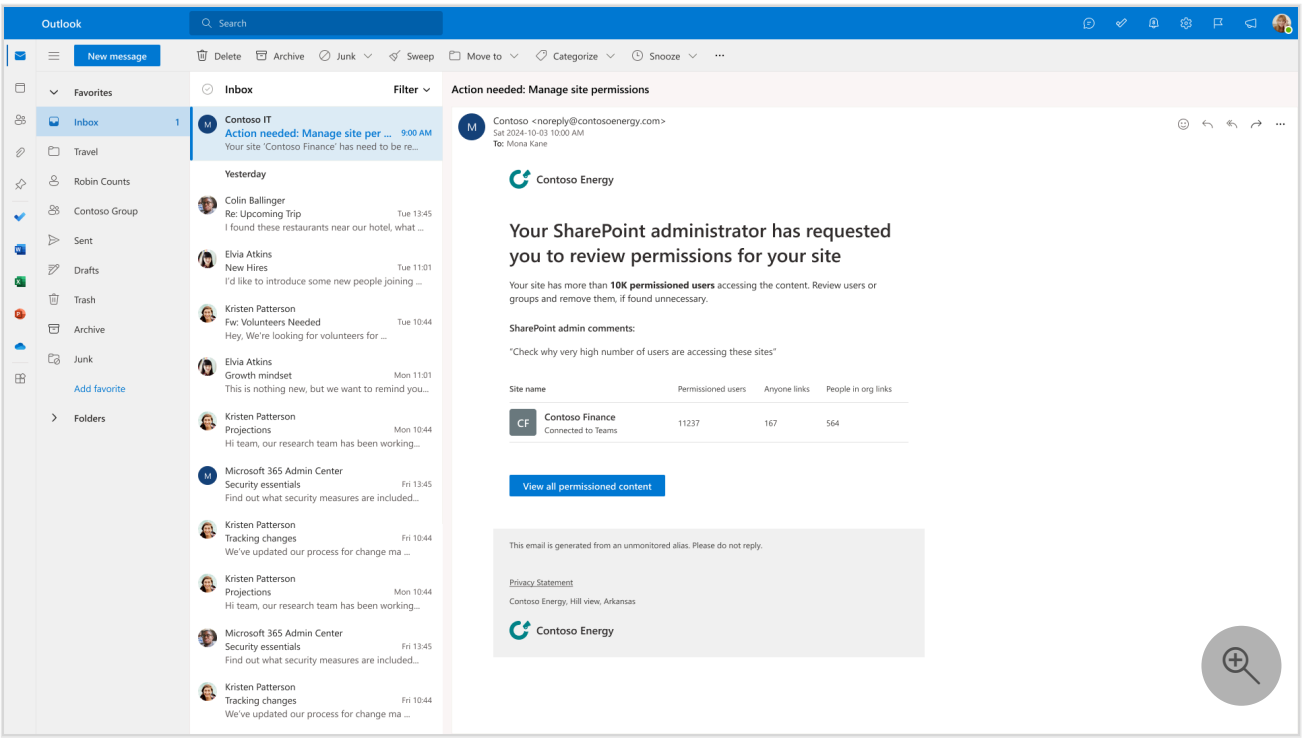
- Content shared with 'Everyone except external users' report for the past 28 days:



- Sharing links report for the past 28 days:



- Oversharing baseline report using permissions:



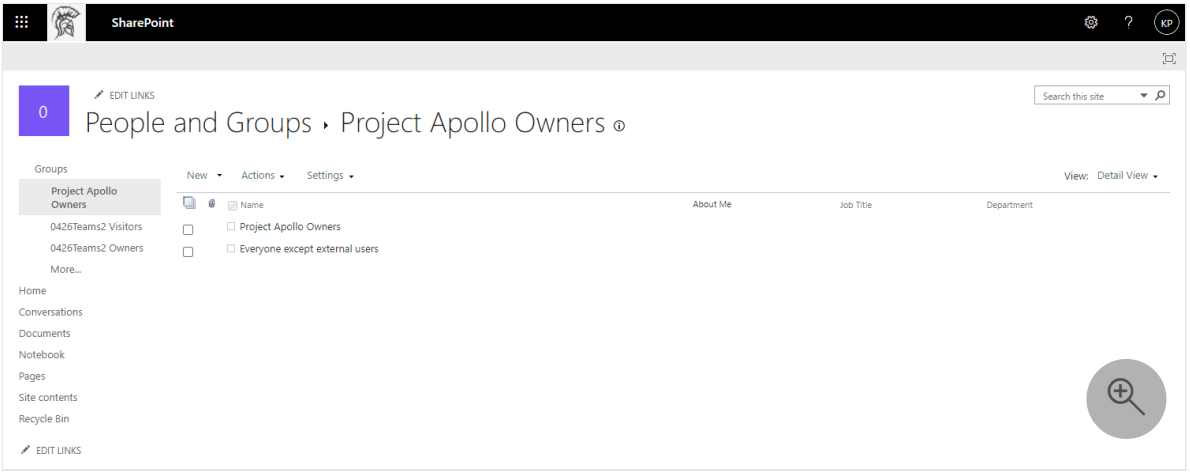
Review 'Everyone Except External Users' site access requests

Site owners can review and manage access in two main areas:

- **SharePoint groups:**
  - View which groups contain 'Everyone except external users.'
  - See when and by whom the group was added.
  - Remove 'Everyone except external users' from groups if necessary:

    1. Open the SharePoint group membership page.

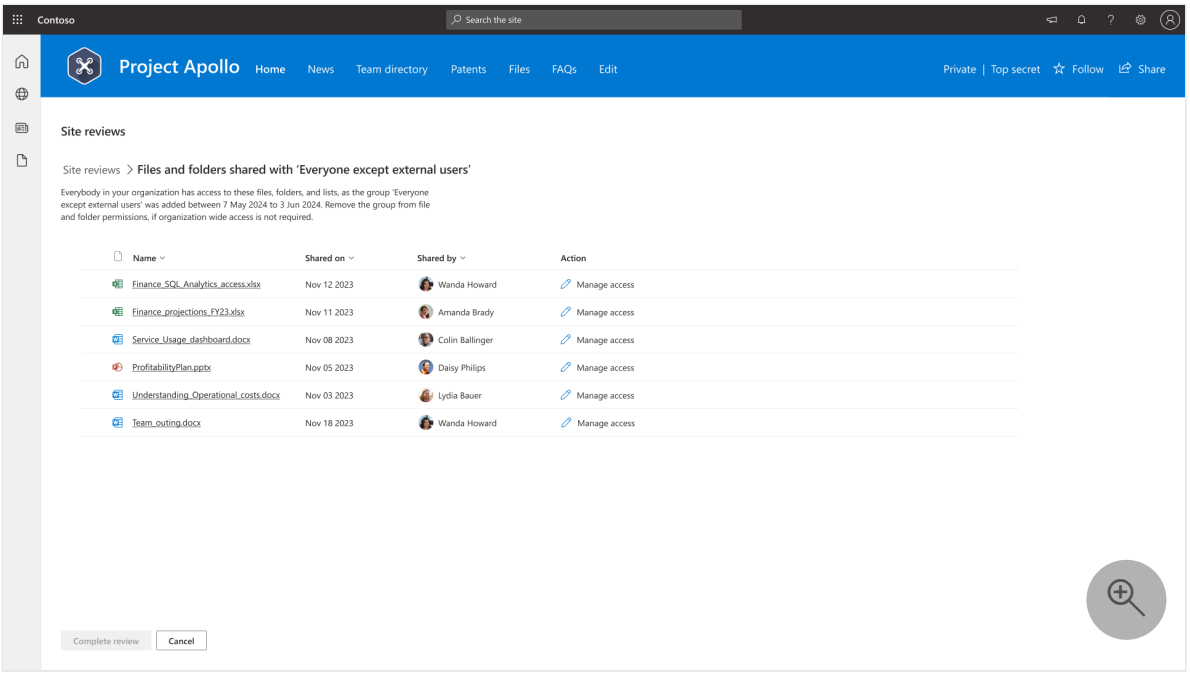
    2. Select **Everyone except external users**, select **Actions**, and select **Remove users from group**.



- **Individual items (files/folders/lists):**
  - View items shared with 'Everyone except external users' in the last 28 days.
  - See sharing details (who shared and when).
  - Manage access and remove permissions as needed:

    1. Select **Manage access**.

    2. Under the 'Everyone except external users' group in the **Groups** tab, select the group and select **Remove access**. See Stop sharing OneDrive or SharePoint files or folders, or change permissions for more information.

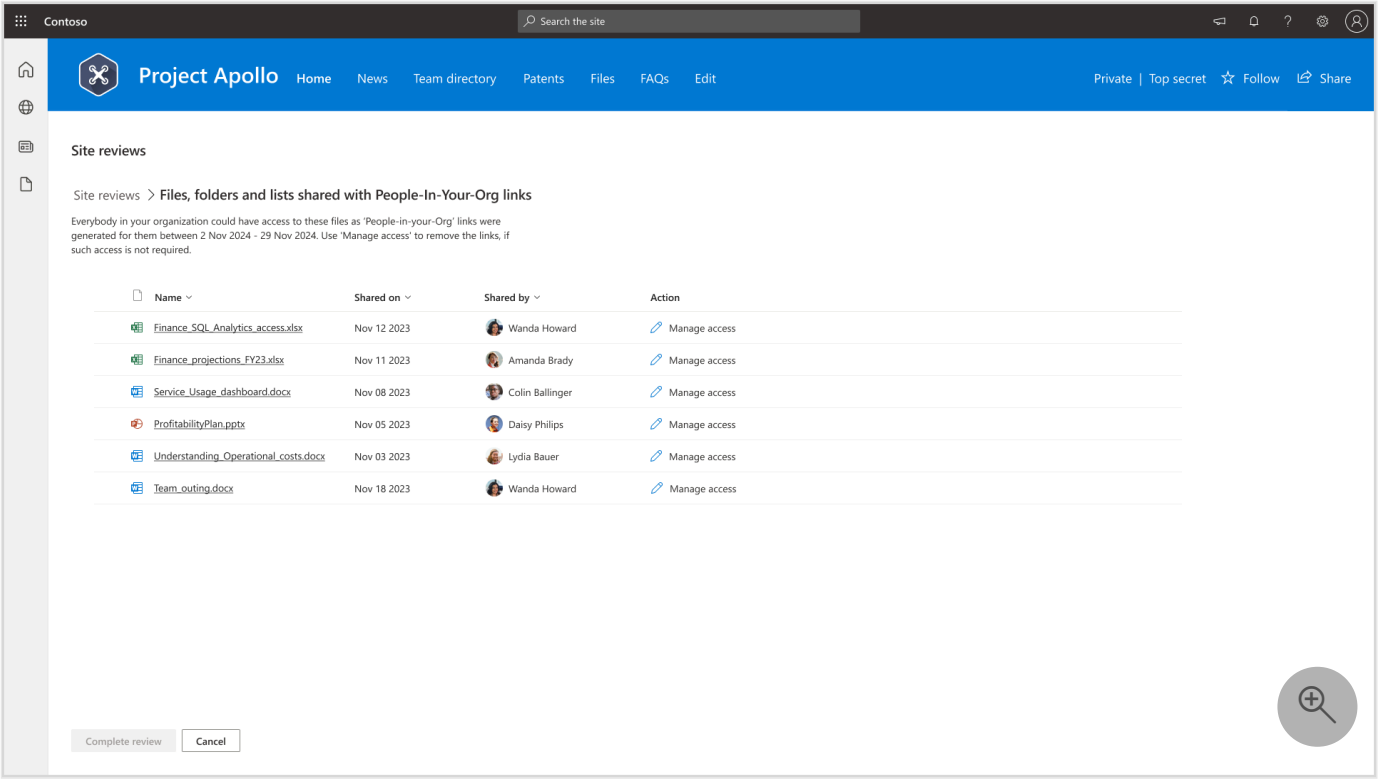


Review 'Sharing link' reports

When the site owner opens the email, they're redirected to a detailed sharing links report. This report shows:

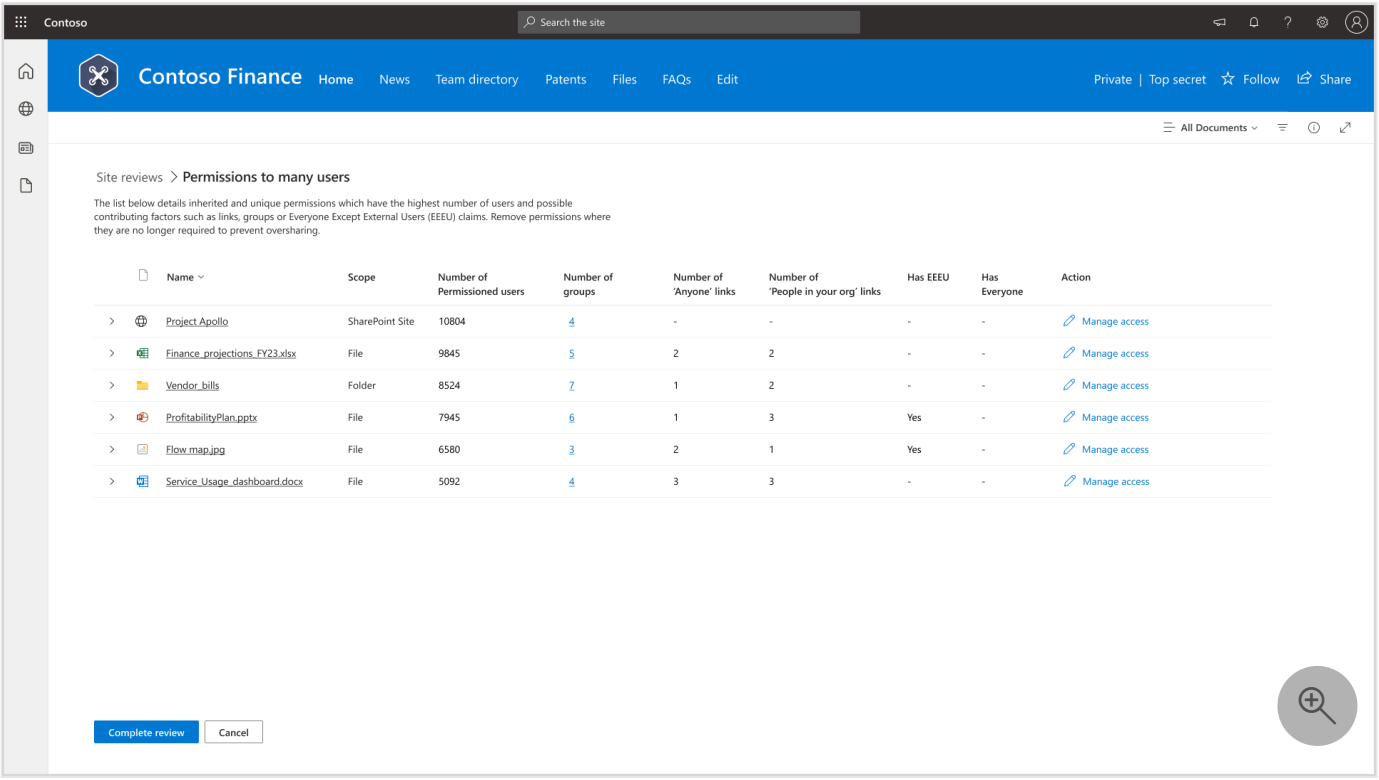
- Files for which links were generated, with the date and the user who created the link.
- The **Manage access** button that site owners use to remove or modify permissions.

The following screenshot shows the detailed sharing links report:



Review 'Oversharing baseline using permissions' reports

When site owners select the email, they're redirected to the site access review page, where they can see the oversharing baseline using permissions report. This report helps site owners identify items with excessive permissions and take necessary actions.



The SharePoint admin views the number of users with permissions to a site in the Data access governance report. Site owners can see this number, along with how permissions are distributed

across different site items. Items with the highest number of permissioned users are shown first, so the site owner can address the most exposed items.

Understanding the permissions report

Number of permissioned users

This column shows the total number of users who have permissions to a specific scope (Site, List, Folder, or File). It reflects the exposure of that item compared to others. However, this number isn't unique - if the same user has both direct and indirect permissions, they're counted multiple times.

Example:

Imagine a folder "F" with the following permissions:

- 40 users from Group "A"
- 10 users with direct permissions
- 20 users with permissions via sharing links

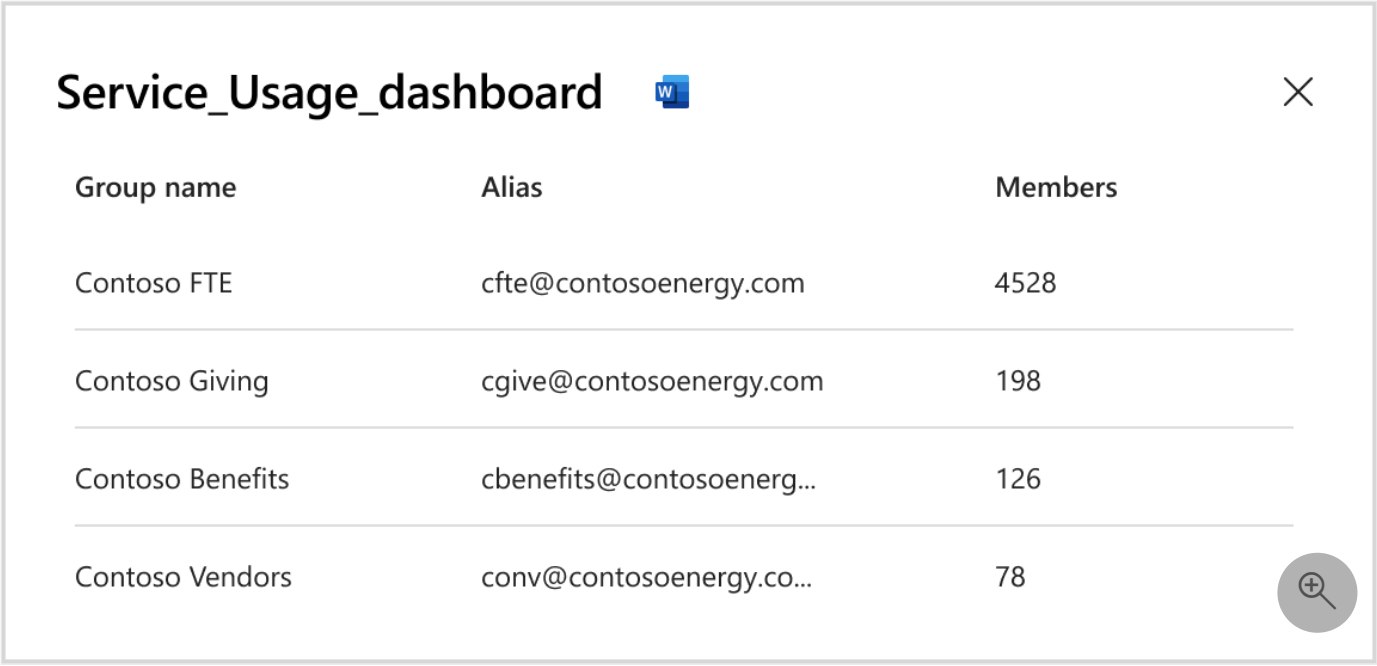
The total number of permissioned users for folder "F" is 80 (40 from Group "A" + 10 direct + 20 via sharing links). No deduplication is applied, so if the same user is in both Group "A" and has access via a sharing link, they're counted twice.

Additionally, the total number of permissioned users across all scopes might exceed the number of users shown in the email or Data Access Governance report. This situation happens because users can have permissions on multiple items. While a user might be counted once at the site level, they're counted separately for each item they have access to.

Number of groups

This column shows how many groups have permissions to a specific item or scope. Often, a large portion of exposure comes from permissions granted to groups, especially those with many members. You can reduce exposure by adjusting group memberships or removing unnecessary groups from permissions.

Select the **Group number** to see the membership count of each group. This information helps you identify which groups to target for reducing permissions.



Service_Usage_dashboard

Group name	Alias	Members
Contoso FTE	cfte@contosoenergy.com	4528
Contoso Giving	cgive@contosoenergy.com	198
Contoso Benefits	cbenefits@contosoenerg...	126
Contoso Vendors	conv@contosoenergy.co...	78

Links and EEEU/Everyone

This section displays:

- The number of links (for example, "Anyone" or "People in your organization") that are shared for the scope.
- Whether the item is exposed to Everyone or EEEU (Everyone Except External Users).

If the number of links is high or the EEEU/Everyone column says "Yes," this condition is an immediate indicator that the item has broad exposure, and the site owner should focus on reducing permissions for that item.

Manage Access

The **Manage Access** button provides a way for the site owner to take action by:

- Removing individual users
- Modifying group memberships
- Deleting links
- Adjusting permissions

For a SharePoint site, selecting this button redirects to the **SharePoint group management** page. For individual items, it opens the **Manage Access** interface, which provides more granular control over permissions.

Complete site access reviews

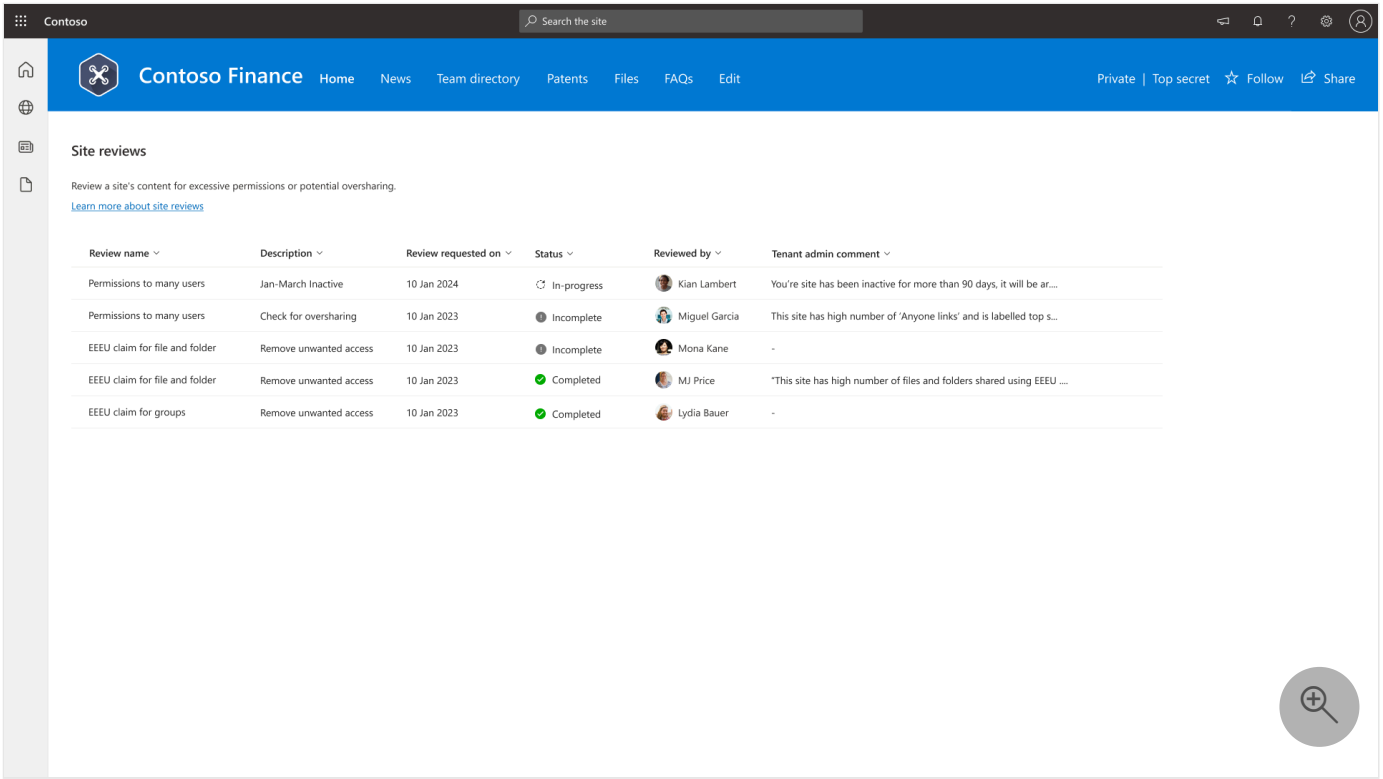
After the site owner makes the necessary changes, such as modifying or removing permissions, they should:

1. Select **Complete review**.
2. Add any relevant comments.
3. Submit the review.

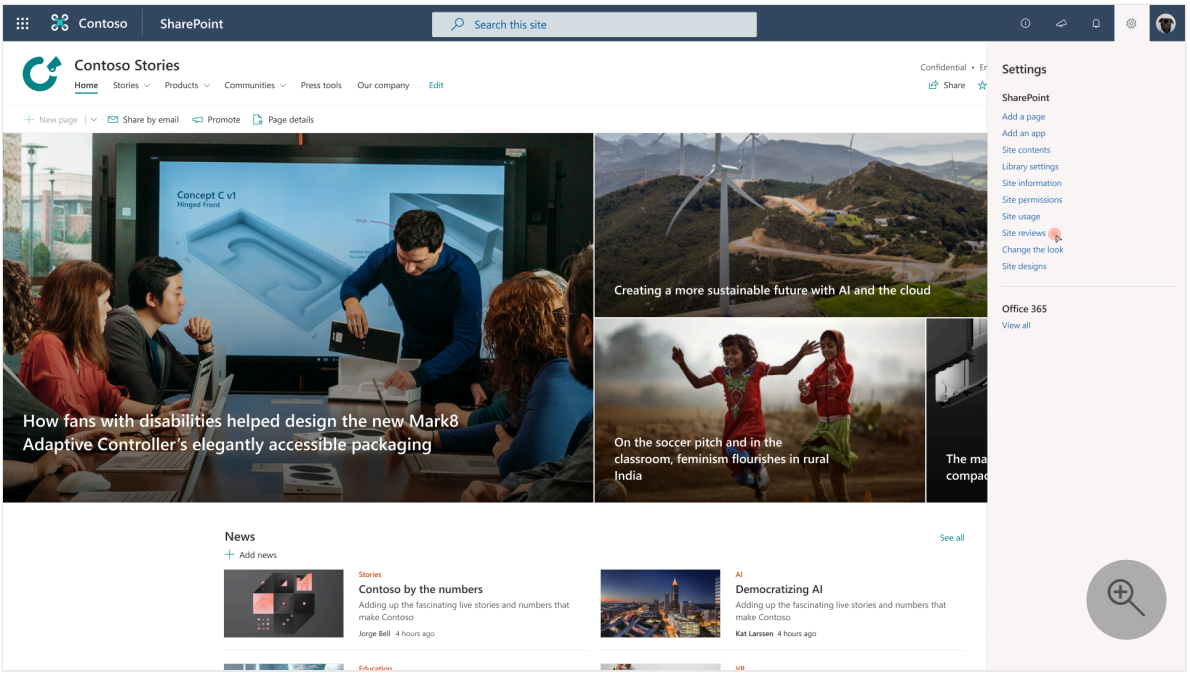
The process sends comments back to the IT administrator, and the review is marked as completed.

Manage multiple site access reviews

Site owners can receive and handle multiple site access review requests simultaneously. To track all review requests:



1. Go to the **Site reviews** page via:
    - The link in the review email.
    - The gear icon on the site home page:
        a. Select **Site settings**.
        b. Select **Site reviews**.



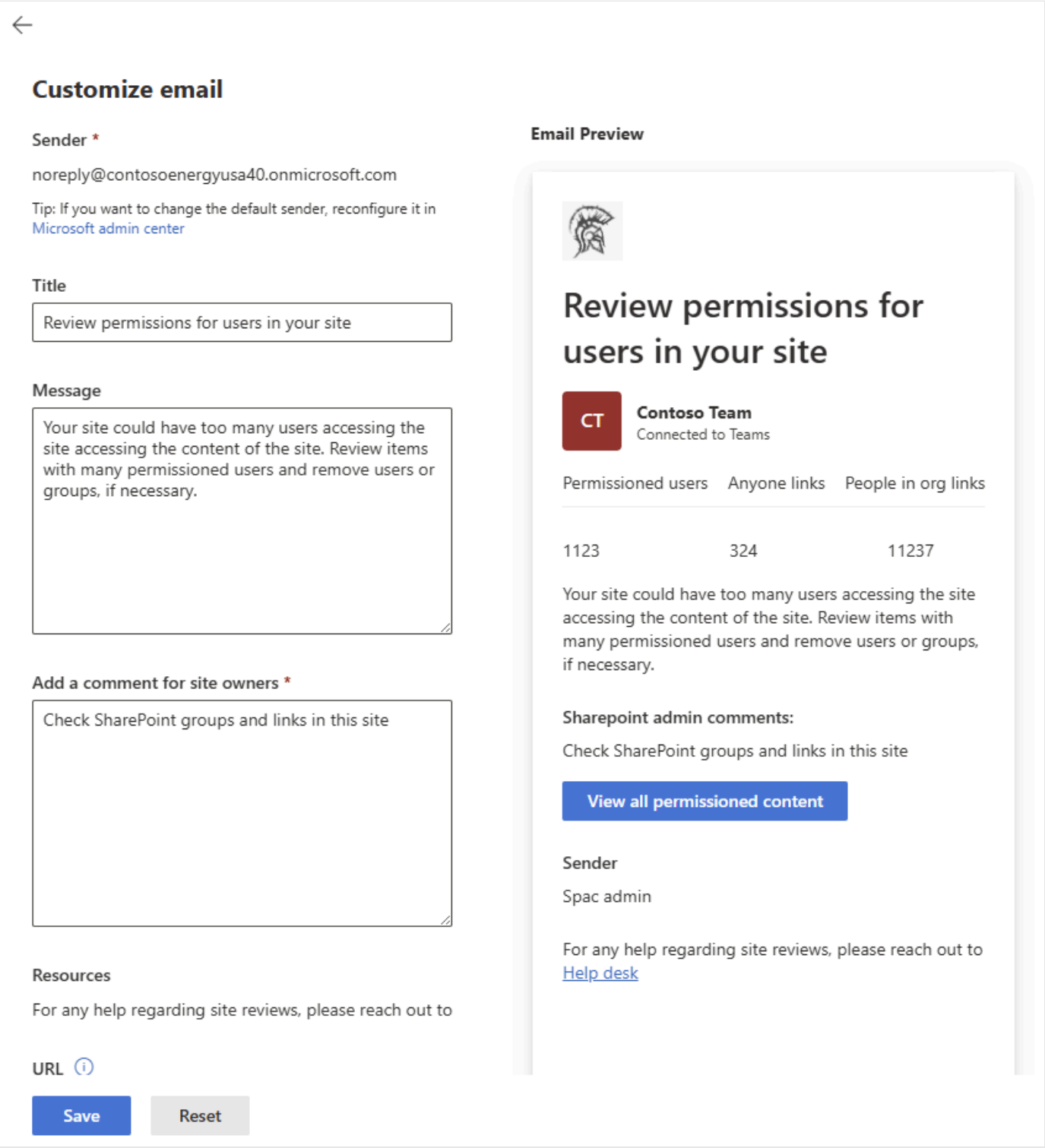
c. View all pending site access reviews.

d. Complete reviews as necessary.

Customize email to site owners

Now you can customize the email sent to site owners to increase the likelihood that site owners see the email as a genuine request from SharePoint admins and not as a suspicious email. The following values are new and available for customization:

- From address: The custom username you specify in the Microsoft 365 admin center under organizational profile automatically provides this value.
- Title of the email
- Message to the site owner that usually describes the scenario
- Any additional comments related to the ask to review
- A link to any SharePoint page or document that lists details or further instructions



Select **Save** to save your customizations for this report type. This action overrides any previous changes and automatically applies to subsequent site reviews from that report type. In other words, you can save a customized version for each report type, as shown in the Data Access Governance landing page. Select **Reset** to revert all customizations to product defined defaults.

Last updated on 07/09/2026

Manage Data access governance reports by using SharePoint Online PowerShell

While Data access governance is available in the SharePoint admin center, some organizations prefer to use PowerShell to manage settings at scale through scripting and automation. This article describes how to use the SharePoint Online PowerShell module to manage Data access governance reports.

Before you begin

Make sure your organization meets the Prerequisites for SharePoint Advanced Management, including SharePoint Online PowerShell module requirements.

PowerShell support for Data access governance is available from module `Microsoft.Online.SharePoint.PowerShell` and version `16.0.25409` or later.

When you connect to SharePoint, run the Connect-SPOService command *without* the **Credential** parameter. In line with security best practices, signing in by using the credential parameter isn't supported.

Create reports by using PowerShell

For general PowerShell syntax, parameters, and examples, see Start-SPODataAccessGovernanceInsight.

For specific report examples, see the following sections in this article.

Generate a site permission state report

You need to understand the permissions setup in your organization, particularly in the wake of Copilot adoption, as it respects user and content permissions. Copilot's data exposure risk increases with the number of users having permissions or access. The site permission state report provides deep insights into potential exposure, based on the unique number of users who have permissions to every SharePoint and OneDrive site in your organization.

Run this report first to get a quick overview of permissions in your organization. This report is a snapshot report. It provides the latest snapshot or status of the entire organization as of the

report generation date.

To generate a report for all your SharePoint sites, run the following command:

PowerShell

```
Start-SPODataAccessGovernanceInsight -ReportEntity PermissionedUsers -ReportType
Snapshot -Workload SharePoint -CountOfUsersMoreThan 0  -Name
"OrgWidePermissionedUsersReportSharePoint"
```

To generate a report for all your OneDrive for business accounts, run the following command:

PowerShell

```
Start-SPODataAccessGovernanceInsight -ReportEntity PermissionedUsers -ReportType
Snapshot -Workload OneDriveForBusiness -CountOfUsersMoreThan 0  -Name
"OrgWidePermissionedUsersReportODB"
```

Keep these important points in mind about the report:

- Because these reports are comprehensive and likely to cover all data in your tenant, you can create up to two reports. You can create one report per workload.
- The first report always takes up to five days to complete, regardless of the size of your organization. Subsequent reports complete within 24 hours.
- These reports capture data up to 48 hours before the report generation.
- Once generated, you can run these reports again once every 30 days.

These commands generate a list of all sites where at least one user can access any content within the site. For more information about how to interpret the report, see How to view the site permissions for your organization report.

Once you understand the extent of oversharing in your tenant, you can track further deviations specifically from active sites in last 28 days. You can generate reports on sites that are active in key factors of potential oversharing such as "Sharing links" or content shared with "Everyone except external users" in the last 28 days.

Generate a user permission state report

While the site permission report for the entire organization helps you understand the current state of permissions in the entire tenant, some scenarios require discovering sites accessible to a given user. For more information, see Get your organization's site permissions baseline with the

snapshot report. The following section describes how data access governance helps you generate such a report by using PowerShell.

First, fetch the UPN or User principal name of the user for whom you want to generate the report by using the Get-MgUser command. Then run the following PowerShell command, which triggers the report listing SharePoint sites accessible to those users.

PowerShell

```
Start-SPODataAccessGovernanceInsight -ReportEntity PermissionsReport -ReportType
Snapshot -Workload SharePoint -Name "UserSharePointReport" -UserEmailList
"a@contoso.com","b@contoso.com"
```

> **Important**
>
> While the parameter is named `UserEmailList`, the report requires user principal names. You can include up to 100 users in a single request.

To list OneDrive accounts accessible to the given users, specify the workload as `OneDriveForBusiness`.

PowerShell

```
Start-SPODataAccessGovernanceInsight -ReportEntity PermissionsReport -ReportType
Snapshot -Workload OneDriveForBusiness -Name "UserOneDriveReport" -UserEmailList
"a@contoso.com","b@contoso.com"
```

Generate a report on sites and files shared via special SharePoint groups

The site permission reports tell you which sites are overshared. To find the exact items where the special groups "Everyone except external users" (EEEU) or "Everyone" are the recipients, generate this report. For more information about the report and how to interpret its output, see Get item-level permission details for "Everyone except external users" and "Everyone".

> **Important**
>
> This report requires module `Microsoft.Online.SharePoint.PowerShell` version `16.0.27215.12000` or later, published April 30, 2026. You also need the SharePoint Advanced

Management Administrator role, which a Global administrator must assign. For more information, see [Assign the SharePoint Advanced Management Administrator role](#).

To generate the report for EEEU, run the following command:

PowerShell

```
Start-SPODataAccessGovernanceInsight -ReportEntity EveryoneExceptExternalUsers -
ReportType Snapshot
```

To generate the report for Everyone, change the **ReportEntity** parameter value:

PowerShell

```
Start-SPODataAccessGovernanceInsight -ReportEntity Everyone -ReportType Snapshot
```

Keep these important points in mind about the report:

- The report doesn't take a **Workload** parameter. The output covers both SharePoint and OneDrive.
- The output file is limited to 1 million rows.
- Permissions granted to EEEU or Everyone for system files and system groups aren't included.

To track the report and download the results, see Track reports by using PowerShell and View and download reports by using PowerShell.

Generate a sensitivity label in files report with PowerShell

Run this PowerShell command to trigger the report to list sites where specific items were labeled with a given label, as of the report generation date.

First, retrieve the label name or label GUID by using the Security & Compliance PowerShell module.

PowerShell

```
Get-Label | Format-Table -Property DisplayName, Name, GUID, ContentType
```

Then, use the name and GUID to retrieve sites with files labeled with the given label name or GUID.

PowerShell

```
Start-SPODataAccessGovernanceInsight -ReportEntity SensitivityLabelForFiles -Workload SharePoint -ReportType Snapshot -FileSensitivityLabelGUID "a0a0a0a0-bbbb-cccc-dddd-e1e1e1e1e1e1" -FileSensitivityLabelName Secret
```

> ⓘ **Note**
>
> Currently, the report for `OneDriveForBusiness` accounts with labeled files isn't supported.

Generate sharing link activity reports

Use sharing link activity reports to identify sites that are active in collaboration and need quicker intervention to mitigate any potential oversharing risk. These recent activity based reports identify sites that generate the most sharing links in the last 28 days.

Generate the following sharing link activity reports:

- Sites that created **Anyone** sharing links in the last 28 days
- Sites that created **People in your organization** sharing links in the last 28 days
- Sites that created **Specific people** (guests) sharing links in the last 28 days

Report on Anyone sharing links created in last 28 days

PowerShell

```
Start-SPODataAccessGovernanceInsight -ReportEntity SharingLinks_Anyone -Workload SharePoint -ReportType RecentActivity
```

Provide the workload value as `OneDriveForBusiness` to get all OneDrive accounts with the same criteria.

Report on PeopleInYourOrg sharing links created in the last 28 days

PowerShell

```
Start-SPODataAccessGovernanceInsight -ReportEntity SharingLinks_PeopleInYourOrg -
```

```
Workload SharePoint -ReportType RecentActivity
```

Provide the workload value as `OneDriveForBusiness` to get all OneDrive accounts with the same criteria.

Report on specific people (guests) sharing links created in the last 28 days

PowerShell

```
Start-SPODataAccessGovernanceInsight -ReportEntity SharingLinks_Guests -Workload
SharePoint -ReportType RecentActivity
```

Provide the workload value as `OneDriveForBusiness` to get all OneDrive accounts with the same criteria.

Identify content shared with "Everyone except external users" in last 28 days

While sharing links can contribute to potential oversharing, another key contributor is "Everyone except external users" (EEEU). EEEU makes content public (visible to the entire organization) and makes it easy for others to discover content and get access. These reports identify sites that actively used EEEU at various scopes in the last 28 days.

You can generate the following EEEU activity reports:

- Sites shared with Everyone except external users in last 28 days
- Items shared with Everyone except external users in last 28 days

> **Important**
>
> Currently, the EEEU report for OneDrive for Business only supports the item level. EEEU reports for OneDrive for Business at the site level aren't supported. If you don't have a Microsoft SharePoint Advanced Management license, you must enable data collection for recent activity based reports so that relevant audit data is collected to build the report. After you enable it, the data is collected and stored for 28 days. You can generate the report 24 hours later, and it contains data from the point of collection. If you don't generate reports even once in three months, data collection is paused and you must enable it again. To

enable data collection for these reports, see the section [Manage data collection for recent activity based reports](#).

Identify sites shared with "Everyone except external users" in last 28 days

When you add EEEU to a site membership (owners, members, or visitors), the entire content of the site becomes public and more prone to oversharing. Run the following PowerShell command to trigger the report to capture such sites in the last 28 days for SharePoint sites:

PowerShell

```
Start-SPODataAccessGovernanceInsight -ReportEntity EveryoneExceptExternalUsersAtSite -
Workload SharePoint -ReportType RecentActivity -Name "PublicSiteViaEEEU"
```

Identify items shared with "Everyone except external users" in last 28 days

Run the following PowerShell command to trigger the report to capture specific items (files, folders, or lists) that you shared with EEEU in the last 28 days for SharePoint sites:

PowerShell

```
Start-SPODataAccessGovernanceInsight -ReportEntity EveryoneExceptExternalUsersForItems
-Workload SharePoint -ReportType RecentActivity -Name "PublicItemsViaEEEU"
```

> **Note**
>
> Replace the workload value with `OneDriveForBusiness` to get items shared with "Everyone except external users" for all OneDrive accounts with the same criteria.

Manage data collection for recent activity based reports

> **Important**
>
> If you don't have a Microsoft SharePoint Advanced Management license, you must enable data collection for recent activity based reports so that relevant audit data is collected to

build the report. After you enable it, you can generate the report 24 hours later, and it will contain data from the point of collection. Data is stored for 28 days. If you don't generate reports even once in three months, data collection is paused and you must enable it again.

Enable data collection for recent activity based reports

This PowerShell command starts collecting audit data for reports on activities from the last 28 days.

PowerShell

```
Start-SPOAuditDataCollectionForActivityInsights -ReportEntity SharingLinks_Anyone
```

The applicable values for the ReportEntity parameter are SharingLinksAnyone, SharingLinksPeopleInYourOrg, SharingLinksGuests, EveryoneExceptExternalUsersAtSite, EveryoneExceptExternalUsersForItems, CopilotAppInsights

Disable data collection for recent activity based reports

This PowerShell command stops collecting audit data for reports on activities from the last 28 days.

PowerShell

```
Stop-SPOAuditDataCollectionForActivityInsights -ReportEntity SharingLinks_Anyone
```

Check the data collection status for recent activity based reports

Once data collection is enabled, the reports can be generated after 24 hours. To check whether reports can be generated, use the PowerShell command Get-SPOAuditDataCollectionStatusForActivityInsights. The command returns the current data collection status, which can be `NotInitiated`, `InProgress`, or `Paused`. Reports can be generated when the status is `InProgress`.

PowerShell

```
Get-SPOAuditDataCollectionStatusForActivityInsights -ReportEntity SharingLinks_Anyone
```

Track reports by using PowerShell

> **Important**
>
> Each report creation returns a GUID that you can use to track the report status.

PowerShell

```
Start-SPODataAccessGovernanceInsight -ReportEntity SensitivityLabelForFiles -Workload
SharePoint -ReportType Snapshot -FileSensitivityLabelGUID "a0a0a0a0-bbbb-cccc-dddd-
e1e1e1e1e1e1" -FileSensitivityLabelName Secret
```

Console

```
ReportId                             Status
--------                             ------
a0a0a0a0-bbbb-cccc-dddd-e1e1e1e1e1e1 NotStarted
```

Use the Get-SPODataAccessGovernanceInsight command to get the current status of a specific Data access governance report by using the report ID.

PowerShell

```
Get-SPODataAccessGovernanceInsight -ReportID a0a0a0a0-bbbb-cccc-dddd-e1e1e1e1e1e1
```

Console

```
ReportId          : a0a0a0a0-bbbb-cccc-dddd-e1e1e1e1e1e1
ReportEntity      : SharingLinks_Anyone
Status            : InQueue
Workload          : SharePoint
TriggeredDateTime : 11/13/2024 19:32:34
CreatedDateTime   : 11/13/2024 20:09:23
ReportStartTime   : 10/17/2024 19:32:33
ReportEndTime     : 11/13/2024 19:32:33
ReportType        : RecentActivity
SitesFound        : 120
```

The `ReportStartTime` and `ReportEndTime` show the period of data for the report. The status changes to `Completed` when the report generation finishes.

You can also view the current status of DAG reports by using the filter `ReportEntity` instead of ID. The `reportID` appears in the output and is needed later to download a specific report.

PowerShell

```
Get-SPODataAccessGovernanceInsight -ReportEntity PermissionedUsers
```

Console

```
ReportId             : a0a0a0a0-bbbb-cccc-dddd-e1e1e1e1e1e1
ReportName           : PermissionReportFor1AsOfSept
ReportEntity         : PermissionedUsers
Status               : Completed
Workload             : SharePoint
TriggeredDateTime    : 09/18/2024 11:06:16
CreatedDateTime      : 09/22/2024 12:12:48
ReportType           : Snapshot
CountOfUsersMoreThan : 1
CountOfSitesInReport : 7
CountOfSitesInTenant : 22
Privacy              : All
Sensitivity          : {All}
Templates            : {All}

ReportId             : b1b1b1b1-cccc-dddd-eeee-f2f2f2f2f2f2
ReportName           : PermissionReportFor1AsOfOct
ReportEntity         : PermissionedUsers
Status               : Completed
Workload             : SharePoint
TriggeredDateTime    : 10/09/2024 14:15:40
CreatedDateTime      : 10/09/2024 15:18:23
ReportType           : Snapshot
CountOfUsersMoreThan : 100
CountOfSitesInReport : 0
CountOfSitesInTenant : 26
Privacy              : All
Sensitivity          : {All}
Templates            : {All}
```

View and download reports by using PowerShell

To download a specific report, you need the reportID. Get the reportID by using the Get-SPODataAccessGovernanceInsight command. Then, use the Export-SPODataAccessGovernanceInsight command to download the report to a path you specify.

PowerShell

```
Export-SPODataAccessGovernanceInsight -ReportID a0a0a0a0-bbbb-cccc-dddd-e1e1e1e1e1e1
-DownloadPath "C:\Users\TestUser\Documents\DAGReports"
```

This command downloads a CSV file to the path you specify. You can find details about the CSV and view for each report in How to access the Data access governance reports in the SharePoint admin center.

> **Note**
>
> The default download path is the **Downloads** folder.

Perform remedial actions by using PowerShell

After you generate data access governance reports, you can perform remedial actions as described in Remedial actions from Data access governance reports.

The following section describes PowerShell commands to initiate and track site access reviews as a remedial action.

Initiate site access review by using PowerShell

Use the Start-SPOSiteReview command to initiate a site access review for a specific site, listed under a data access governance report. The data access governance report provides the context under which you should initiate the review. Retrieve the report ID and site ID from the CSV file and provide comments to give clarity to the site owner regarding the purpose of the review.

PowerShell

```
Start-SPOSiteReview -ReportID a0a0a0a0-bbbb-cccc-dddd-e1e1e1e1e1e1 -SiteID c2c2c2c2-
dddd-eeee-ffff-a3a3a3a3a3a3 -Comment "Check for org wide access"
```

Console

```
ReviewId                : a0a0a0a0-bbbb-cccc-dddd-e1e1e1e1e1e1
SiteId                  : c2c2c2c2-dddd-eeee-ffff-a3a3a3a3a3a3
ReviewInitiatedDateTime : 13-11-2024 20:55:41
ReportEntity            : PermissionedUsers
Status                  : Pending
AdminComment            : Check for org wide access
SiteName                : All Company
```

This command generates emails to site owner as described in How to initiate a site access review.

> **Important**

You can initiate up to 1,000 site access reviews per calendar month from the **Site permissions across your organization** report. This limit resets at the start of each new month.

Track site access reviews by using PowerShell

Use Start-SPOSiteReview command to track the status of site access reviews. For specific reviews, use the `ReviewID` value as shown in the output. To retrieve all reviews related to a reporting module, use the `ReportEntity` parameter.

PowerShell

```
Get-SPOSiteReview -ReportEntity PermissionedUsers
```

Console

```
ReviewId                : a0a0a0a0-bbbb-cccc-dddd-e1e1e1e1e1e1
SiteId                  : c2c2c2c2-dddd-eeee-ffff-a3a3a3a3a3a3
ReviewInitiatedDateTime : 13-11-2024 20:55:41
ReviewCompletedDateTime :
ReportCreatedDateTime   : 13-11-2024 23:25:41
ReportEndDateTime       : 13-11-2024 23:25:41
ReportEntity            : PermissionedUsers
Status                  : Pending
AdminComment            : Check for org wide access
SiteName                : All Company
ReviewerEmail           :
ReviewerComment         :

ReviewId                : a0a0a0a0-bbbb-cccc-dddd-e1e1e1e1e1e1
SiteId                  : c2c2c2c2-dddd-eeee-ffff-a3a3a3a3a3a3
ReviewInitiatedDateTime : 24-10-2024 11:07:39
ReviewCompletedDateTime : 15-11-2024 11:07:39
ReportCreatedDateTime   : 15-10-2024 09:24:47
ReportEndDateTime       : 15-10-2024 11:39:52
ReportEntity            : PermissionedUsers
Status                  : Completed
AdminComment            : Check for org wide access
SiteName                : All Company
ReviewerEmail           : Jon@contosofinance.com
ReviewerComment         : Removed EEEU for sensitive documents
```

Related articles

- Data access governance reports for SharePoint and OneDrive sites
- Get ready for Microsoft 365 Copilot and agents with SharePoint Advanced Management

ⓘ**Note:** The author created this article with assistance from AI. Learn more

---

Last updated on 07/30/2026

Compare site policies with the site policy comparison reports for SharePoint sites

As a best practice, SharePoint admins should use the same security policies for similar sites. Usually, admins organize sites by department, location, or nature of content, and then apply consistent security settings. For example, a site containing legal contracts should have strict security measures, such as preventing external sharing, applying conditional access, restricting access to specific groups, and blocking downloads. However, when there are hundreds or thousands of sites, it can be challenging for SharePoint admins to find sites with similar content and ensure they all have the right security policies.

Now with the power of AI, you can select one or more reference sites as your baseline and compare them against up to 10,000 target sites. The AI identifies sites with similar content and highlights any differences in their policy settings compared to your reference sites. This report is called the "site policy comparison report."

What do you need to create site policy comparison reports?

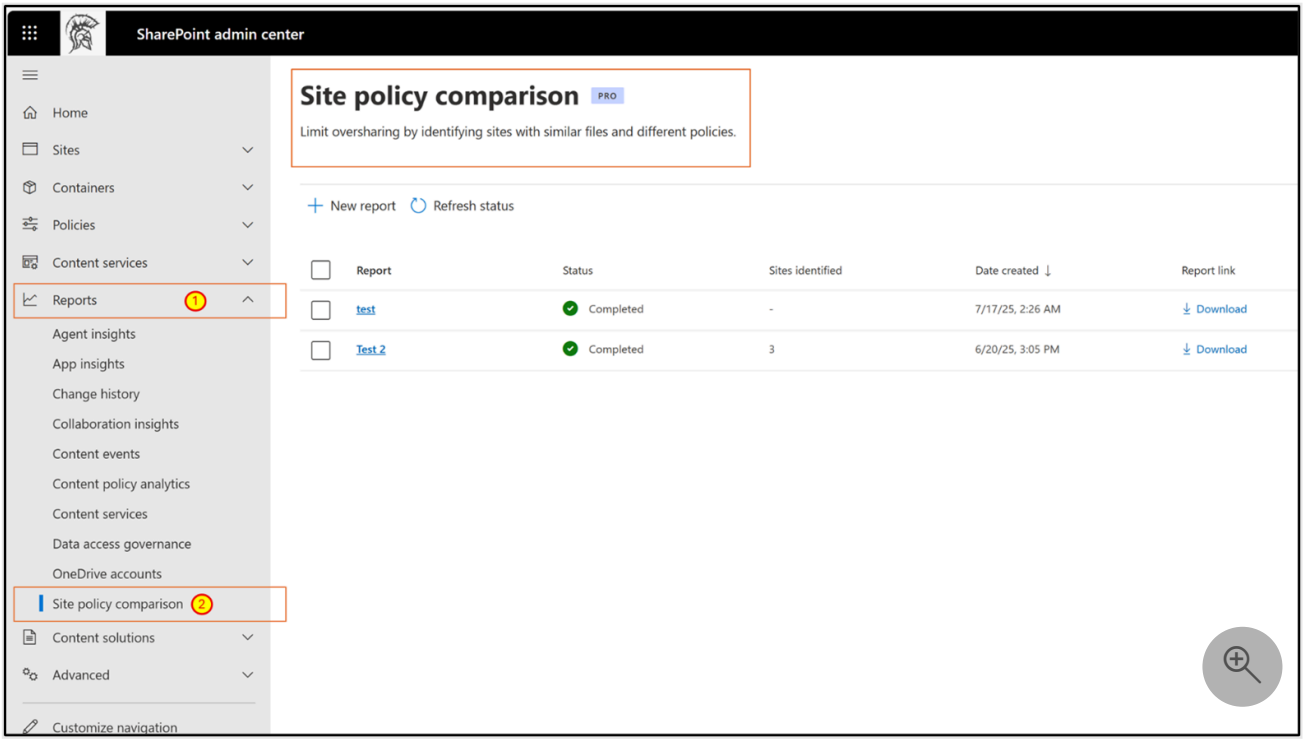
See SharePoint Advanced Management prerequisites.

How to create site policy comparison reports

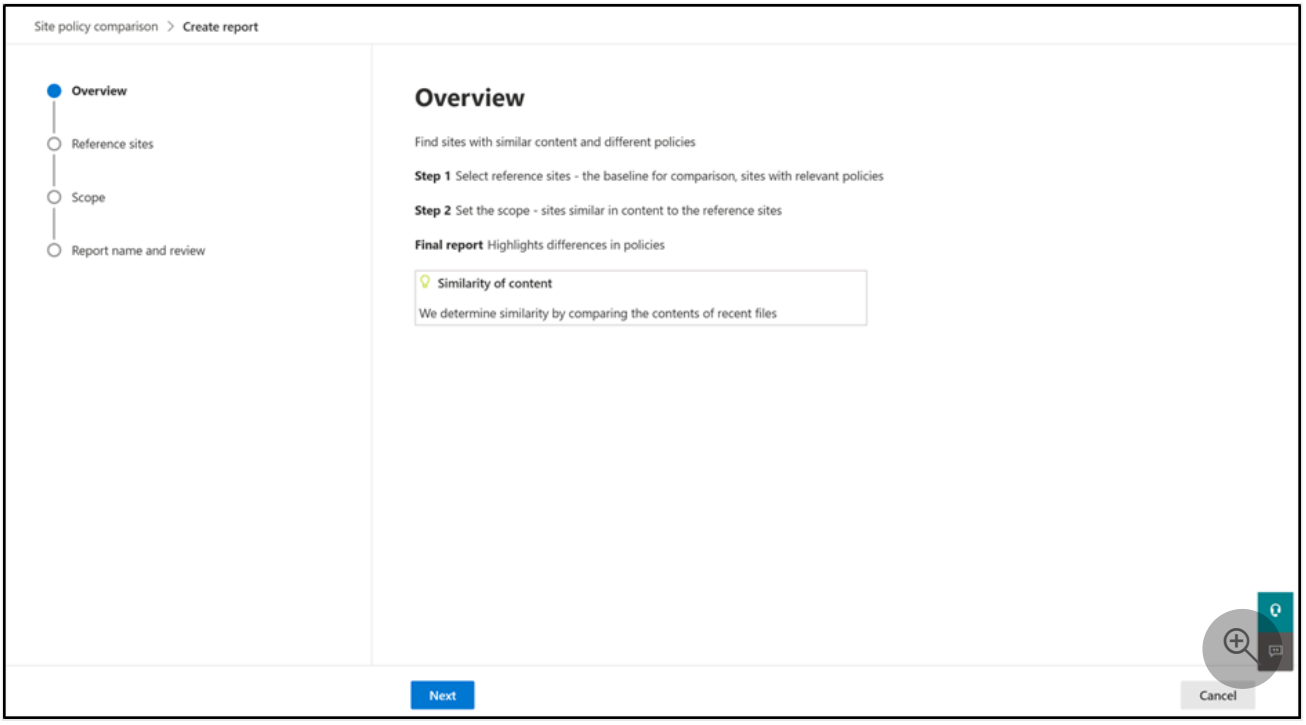
To create site policy comparison reports, follow these steps:

1. **Locate the report**: Sign in to the SharePoint admin center with the SharePoint administrator credentials for your organization. In the left pane, expand **Reports** and then

select **Site Policy configuration**.

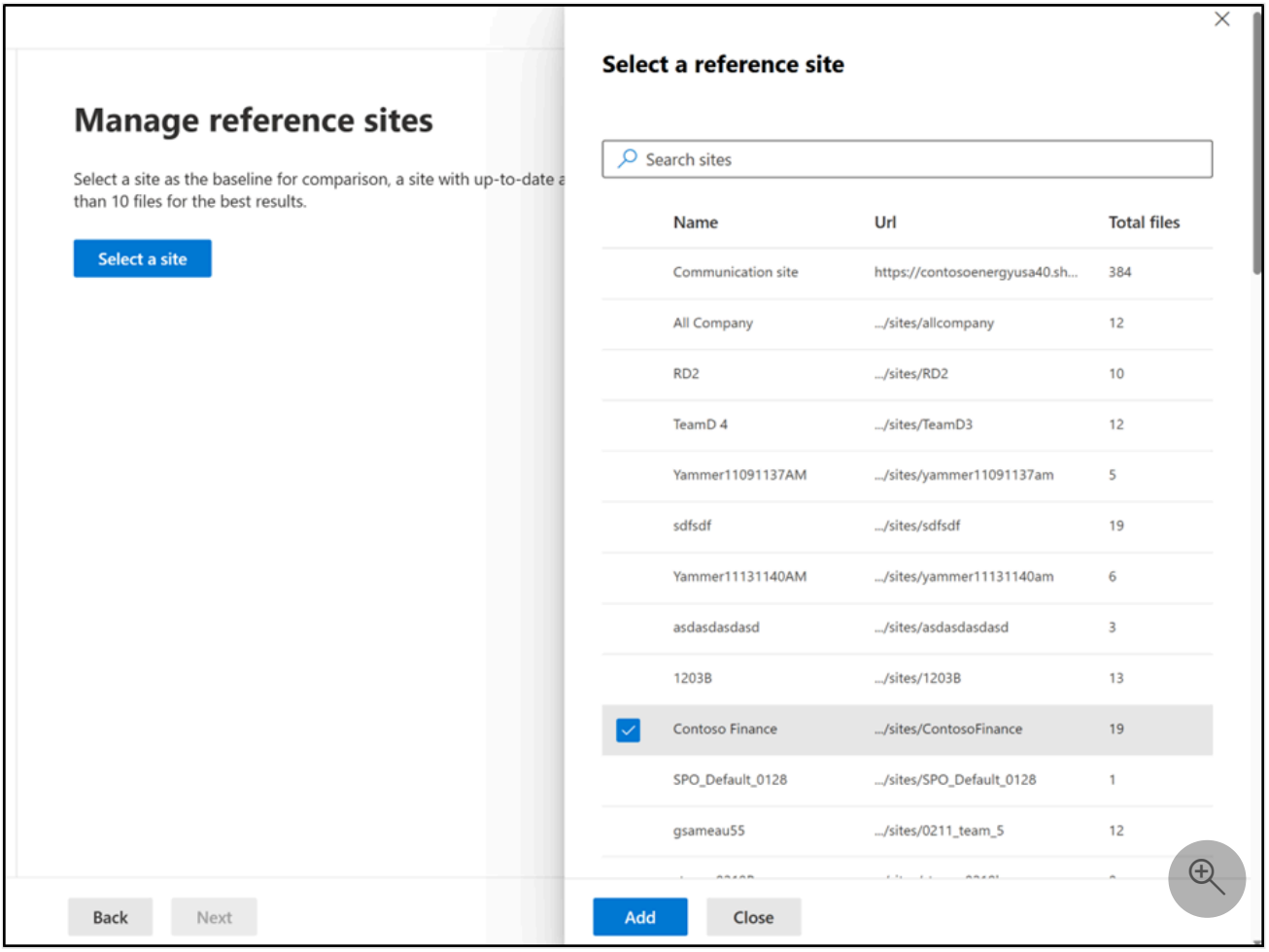


2. **Start creating the new report**: Select the **New report** button to bring up the report wizard. You'll be guided through two steps to create your report. Watch for the callout that explains what "Similarity of content" means—the system looks at up to 5 of the most recently used files in your chosen site or sites and compares them semantically to files in the target sites.

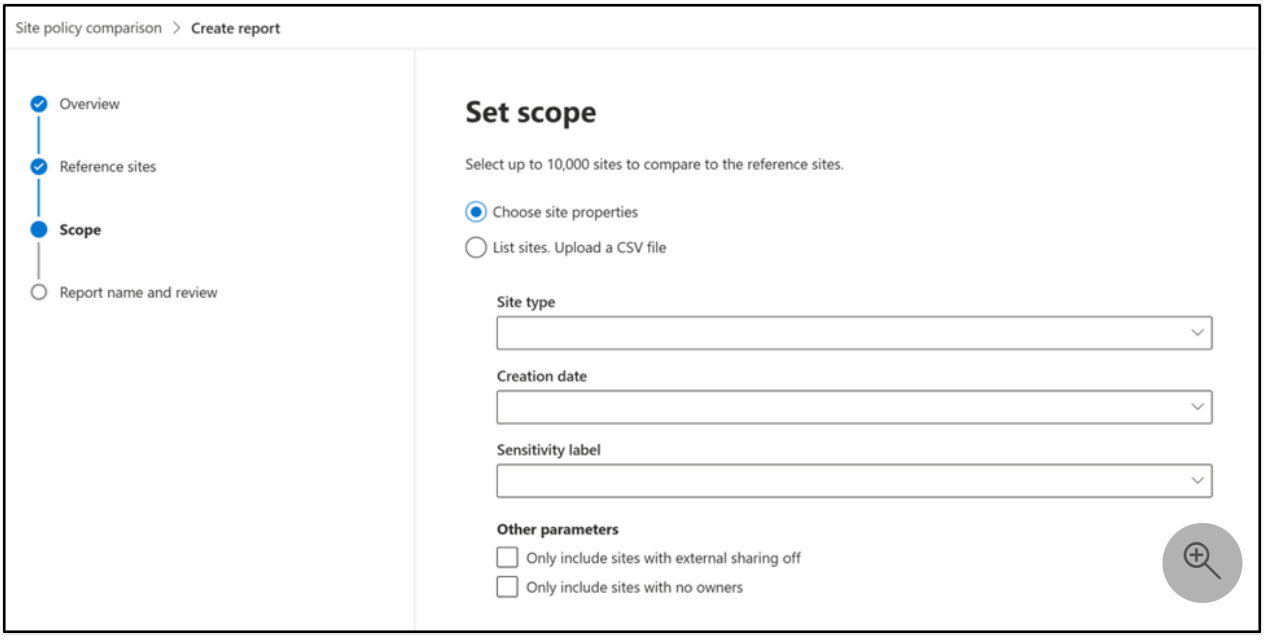


3. **Select the reference sites**: On the **Reference sites** page, pick up to 5 reference (input) sites that will serve as the basis for your comparison. Choose a site that contains files with similar types of content, such as contracts, agreements, statements of work, or project specifications. If the files in your reference site aren't alike, the matching results may not be

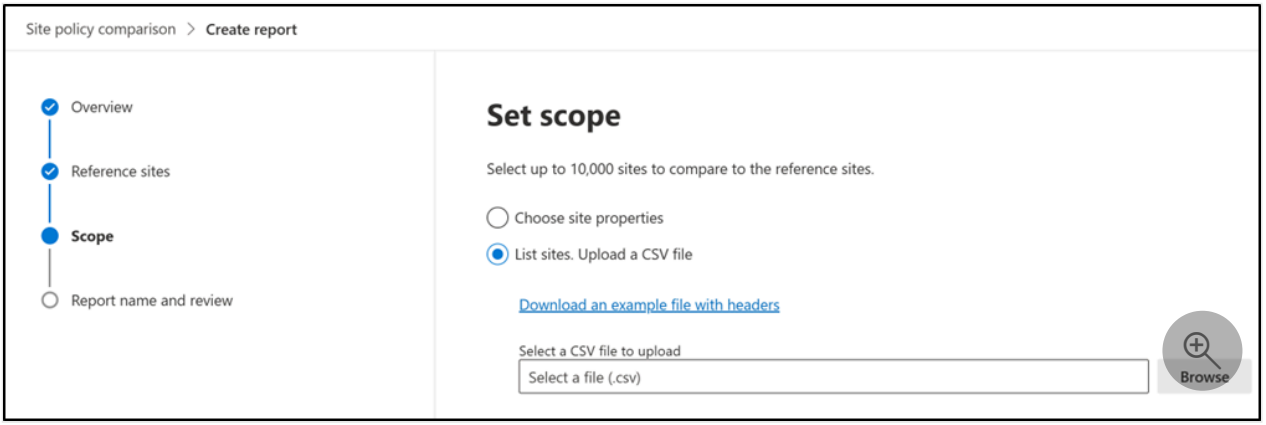
as accurate.



4. **Select the scope of comparison**: On the **Scope** page, pick which sites to compare, known as the "target" sites. You can compare up to 10,000 target sites. There are two ways to provide information about the target sites.
   a. As the first option, the admin can select specific site properties, and only the top sites that match those properties will be included in the comparison.

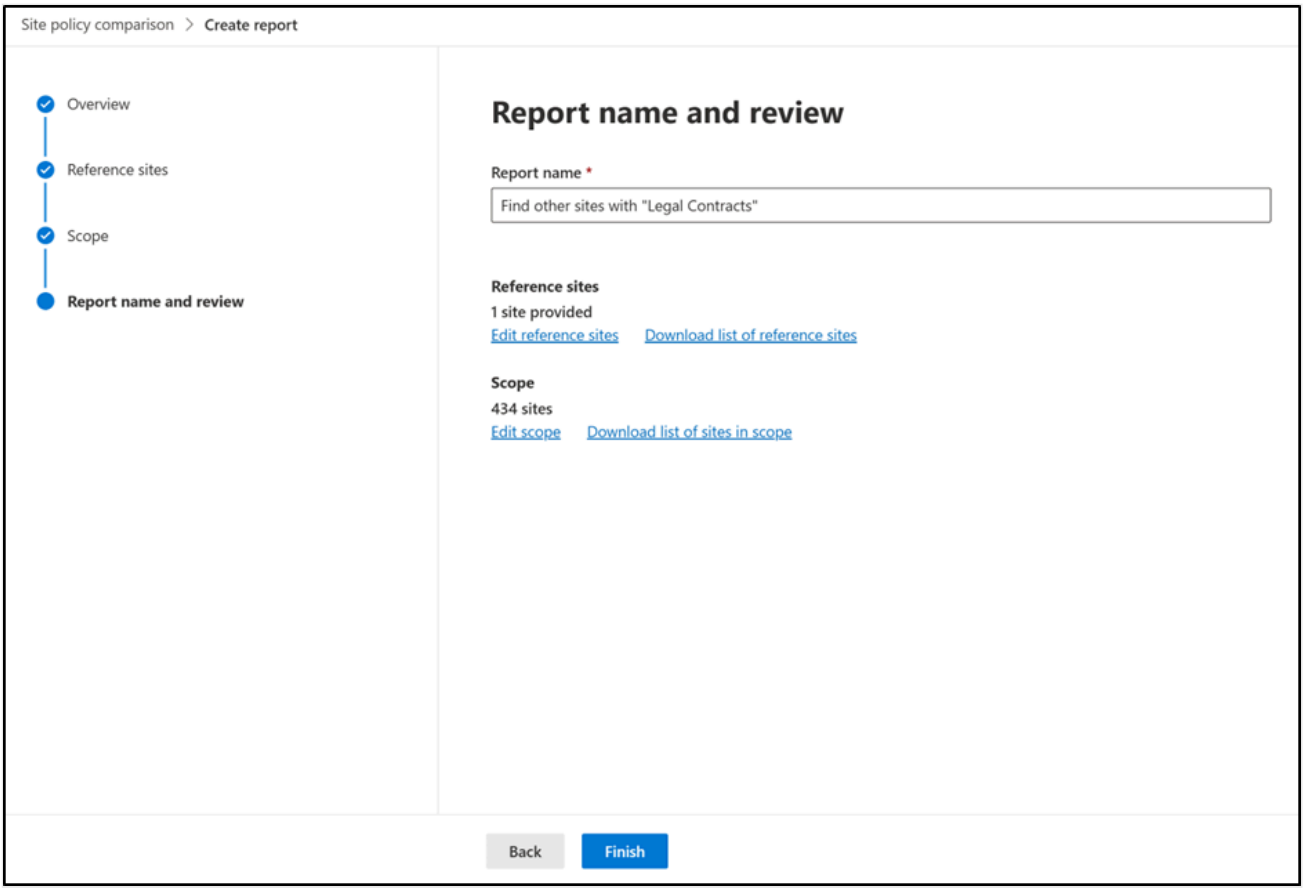


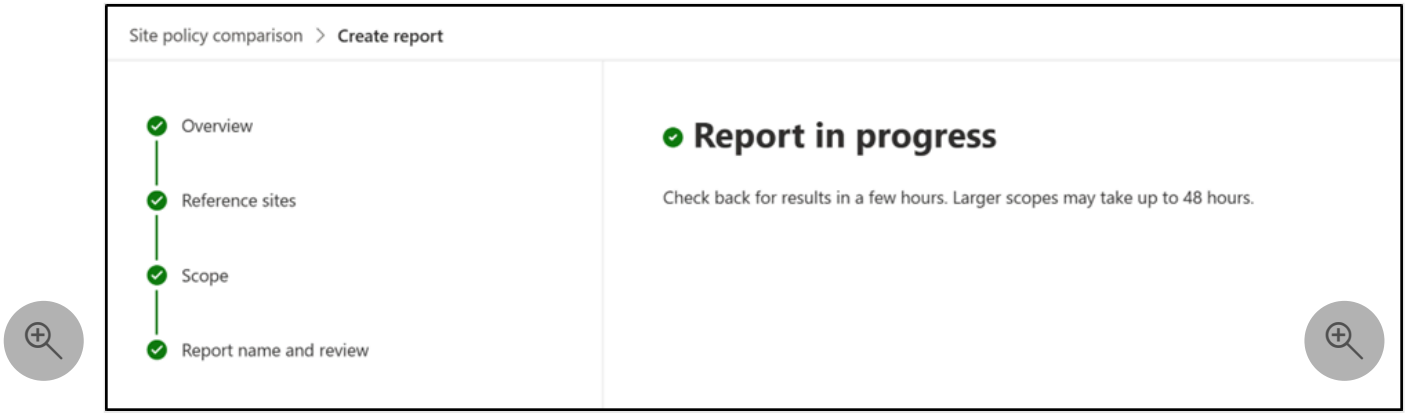
b. Another option is to upload a CSV file with site URLs. The CSV file should have a header named "SiteURL" and contain the URLs of the target sites you want to compare. You can download a sample CSV file from the **Set scope** page.



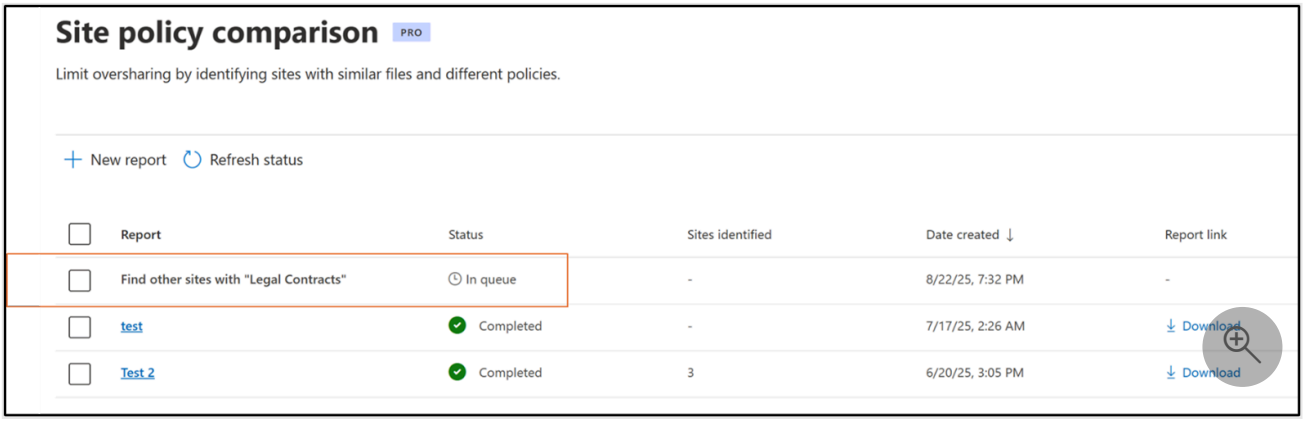
> **Note**
>
> For comparison, only the top 10 recently used files in a site for both reference sites and target sites.

1. **Name the report**: On the **Report name and review** page, provide an appropriate name for the report, review your reference sites and target sites. Then select **Finish**.



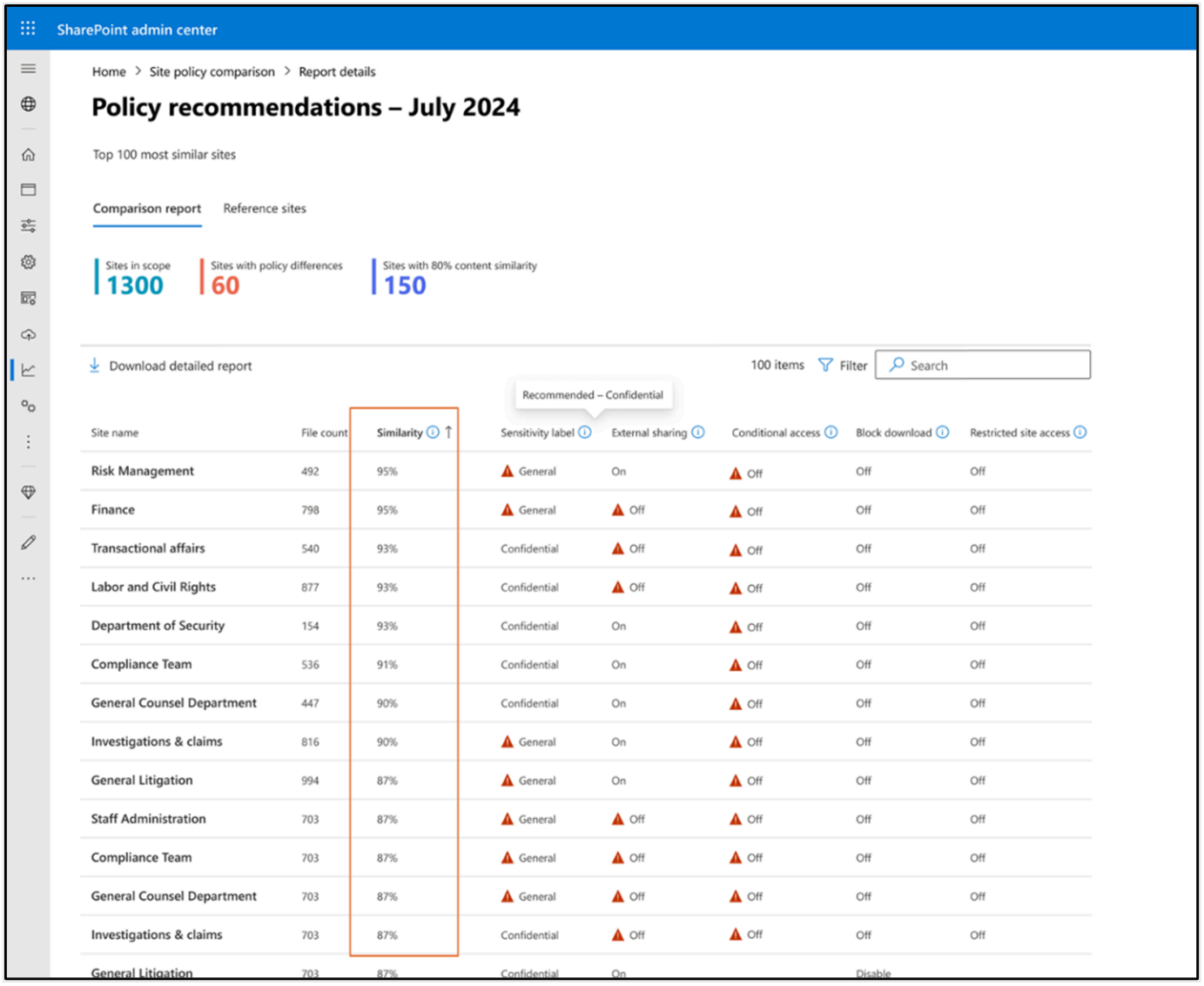


The report is now placed in a queue for processing. For large number of sites, it can take up to 48 hours to finish processing and generate the report.



How to read the site policy comparison report

Let's use the following sample report to understand the different sections of the site policy comparison report, and what each part means.



This report displays sites that have been semantically matched with your reference site or sites and got a "similarity" score of 80% or higher. While the visual report shows the top 100 matched sites, you can download a complete list of all matched sites as a CSV file.

In this example:

- **Total sites analyzed**: 1,300 sites were included in the comparison scope
- **Sites with high similarity**: 150 sites got a similarity score of 80% or higher
- **Policy mismatches identified**: 60 sites have one or more policy settings that differ from the reference site or sites

Policies included in the comparison

The report compares five key security policies across your sites:

1. **Sensitivity label**: The sensitivity label applied to the site

2. **External sharing**: Whether external users can access the site
3. **Conditional access**: Access restrictions based on conditions like location or device
4. **Block download**: Whether users are prevented from downloading files
5. **Restricted site access**: Access limited to specific groups or users

The report helps you quickly identify sites with similar content but different security policies. This ensures you can apply consistent policies across your organization.

To investigate policy differences:

- Look for exclamation marks (!) that highlight policy mismatches
- Select the site name to examine its content and settings
- Navigate to the **Active sites** page in SharePoint admin center for additional management options

Limitations

- **Maximum sites**: You can include up to 10,000 sites in the target scope for comparison.
- **Site access review**: Currently, you can't initiate a site access review from this report.

Last updated on 05/12/2026

Monitor agent access to SharePoint and OneDrive

The agent access insights report provides SharePoint administrators with rich information on how the agents access content across all SharePoint and OneDrive sites in your organization. The report includes all registered and activated agents, such as:

- Agents created in SharePoint
- Declarative agents
- Custom agents
- ... and more

By using this report, you can see how agents interact with your content, spot access patterns, and view agent distribution across sites. Use these insights to strengthen your security and apply governance controls like Restricted access control and Restricted content discovery.

Agent access insights use Microsoft 365 unified audit logs to track how agents access your SharePoint sites and OneDrive accounts. These logs capture signals like reading, searching, and interacting with content, giving you a clear view of agent activity.

You can generate and manage the agent access insights report in the SharePoint Admin Center or by using SharePoint Online Management Shell. You must have an appropriate role assigned, such as SharePoint administrator, to create or view agent access reports.

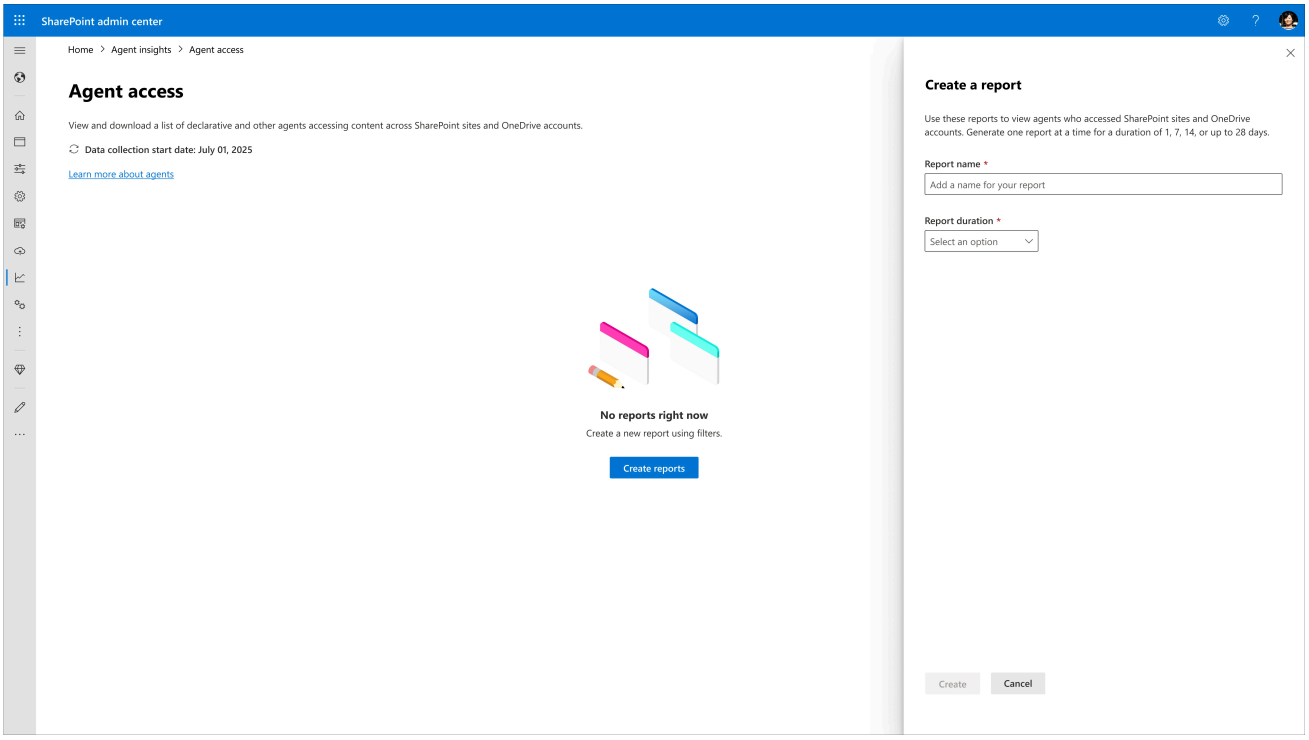
Before you begin

See SharePoint Advanced Management prerequisites.

> **Important**
>
> If you don't have a Microsoft SharePoint Advanced Management license, you're asked to enable data collection, so that the product starts to collect the relevant audit data to build this report. Once enabled, the reports can be generated 24 hours later and contain data from the point of collection. Data is stored for 28 days. If no reports are generated at least once in three months, data collection is paused and should be enabled again. To enable data collection for these reports, refer to the Data collection for agent access insights report section in this article.

How do I access the agent access insights report in the SharePoint admin center?

1. Go to the SharePoint admin center and sign in.
2. In the navigation pane, expand **Reports**, and then select **Agent insights**.
3. Select **Agent access**.
4. Review the report details, including agent activity, access patterns, and site distribution.

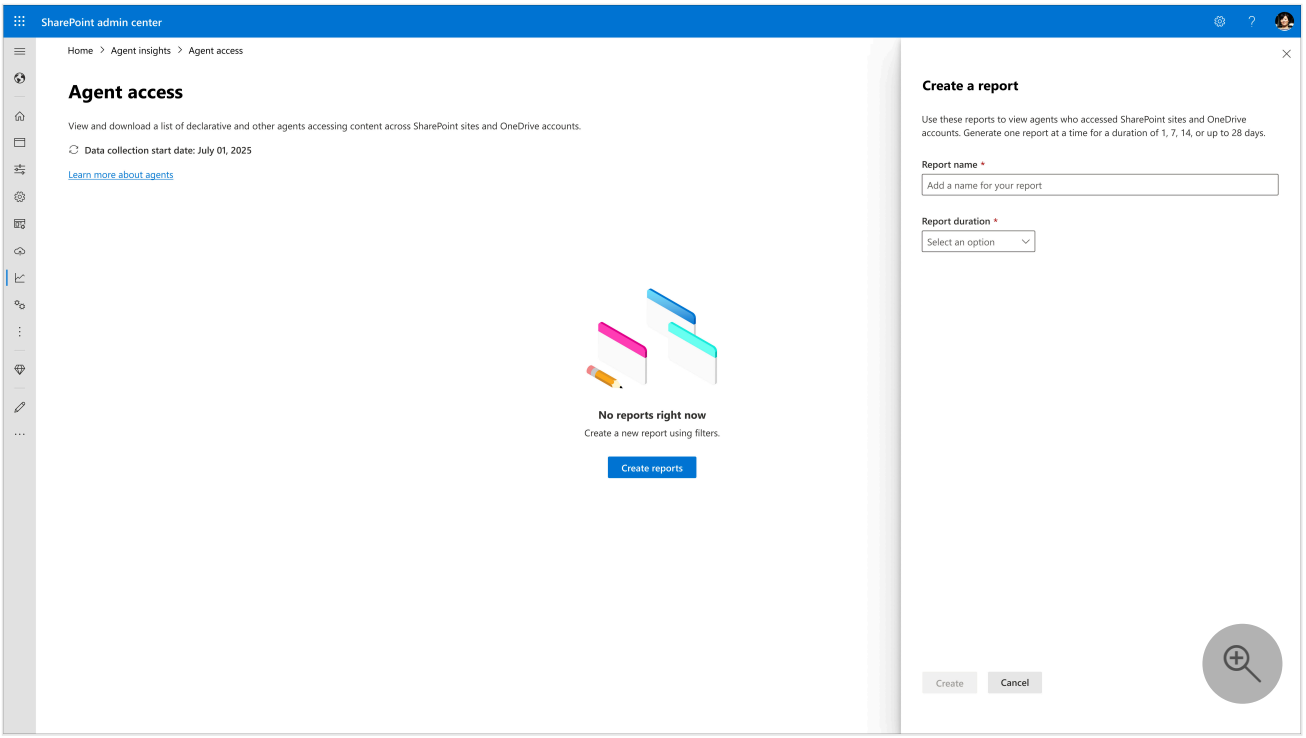


How to create agent access reports in the SharePoint admin center

> **Note**
>
> You can create reports for the past 1, 7, 14, or 28 days. Data older than 28 days is automatically rolled off.

1. In the SharePoint admin center, in the navigation pane, expand **Reports**, and then select **Agent insights**.
2. Select **Create a report**.
3. Specify a name for the report and the report duration (1, 7, 14, or 28 days).

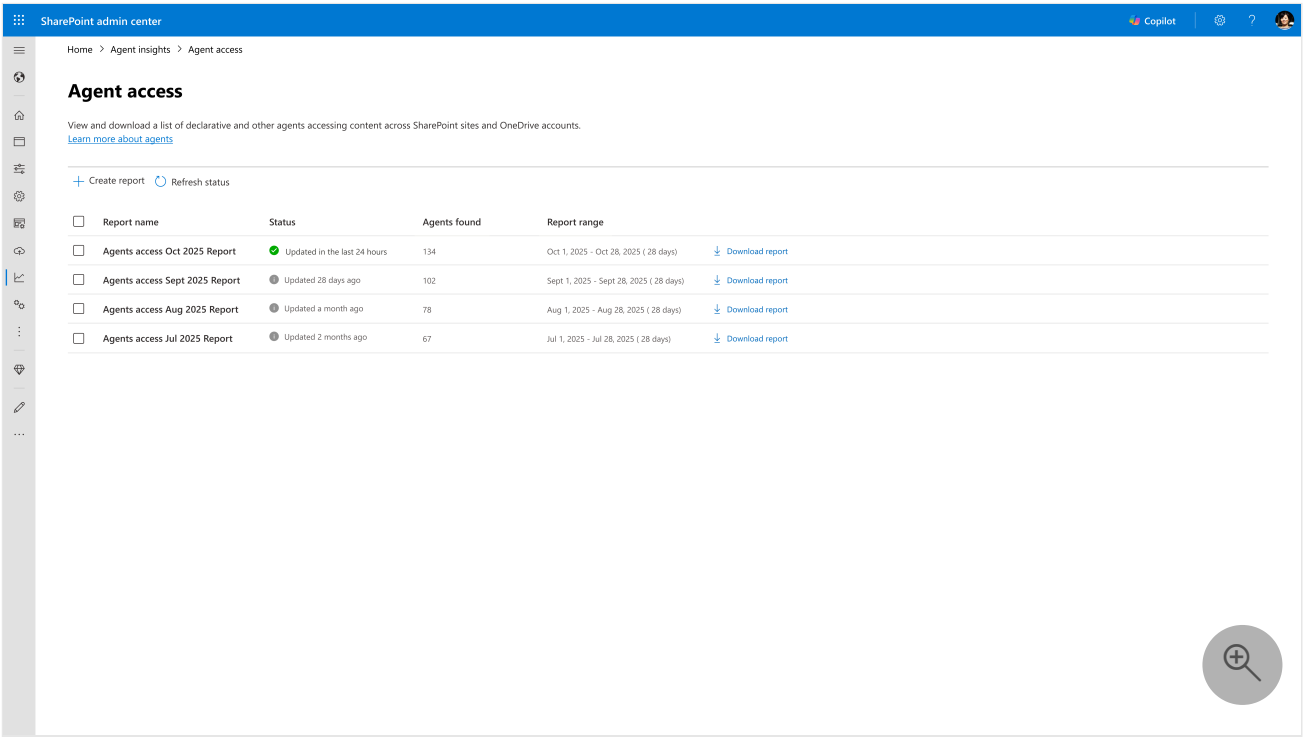
4. Select **Create and run** (or **Create**).



View the agent access report status in the SharePoint admin center

1. In the SharePoint admin center, in the navigation pane, expand **Reports**, and then select **Agent insights**.

2. Check the **Status** column to see if a report is ready or when it was last updated.

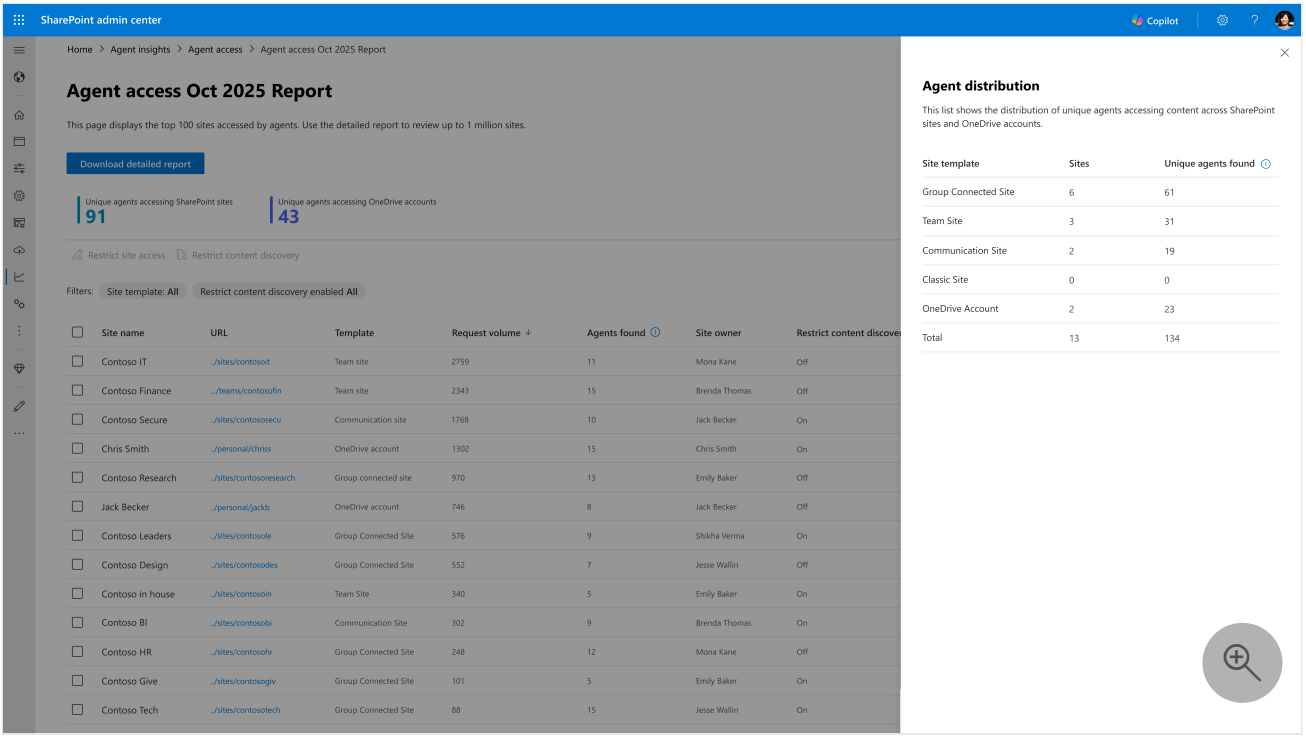


View the agent access report details in the SharePoint admin center

1. In the SharePoint admin center, in the navigation pane, expand **Reports**, and then select **Agent insights**.

2. Check the **Status** column to see if a report is ready or when it was last updated.

3. Select a report to view the data. You can view the top 100 sites hosting the highest number of agents. You can search for sites or filter by site template and governance policies.

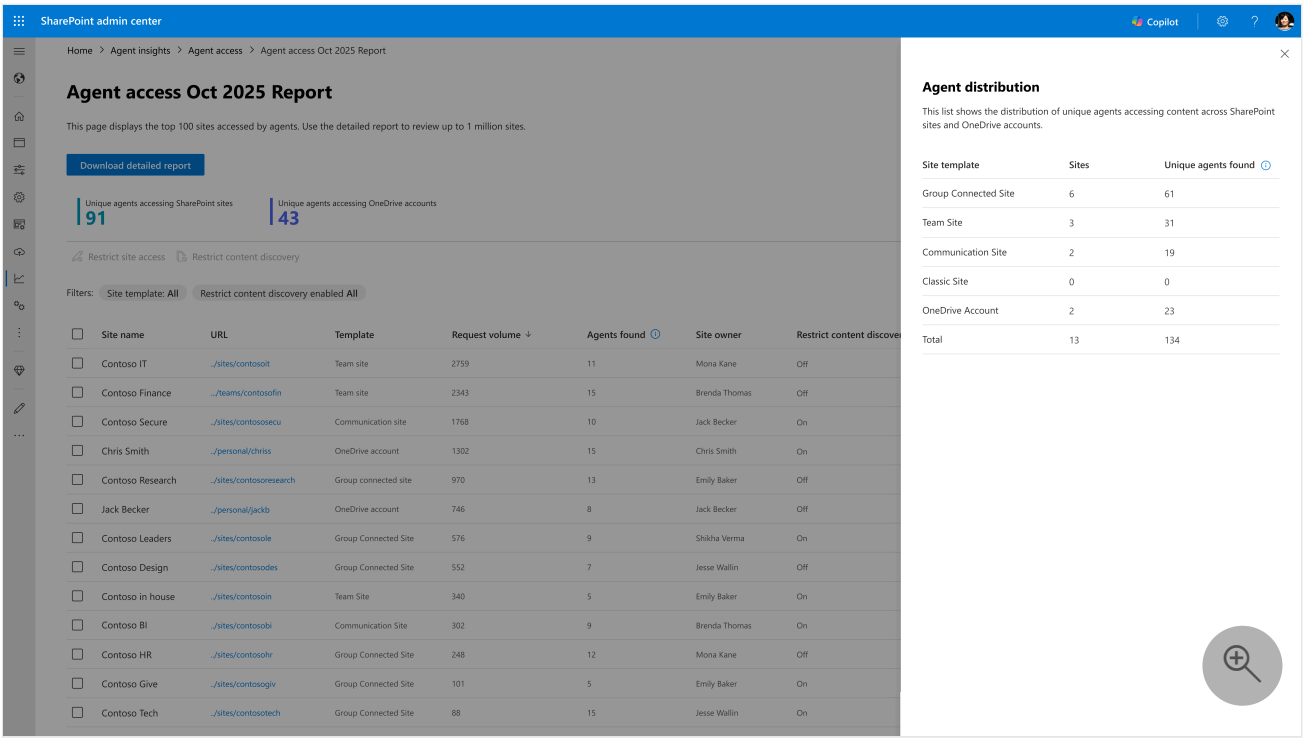


View top 20 agents for a specific site

1. In the SharePoint admin center, in the navigation pane, expand **Reports**, and then select **Agent insights**.

2. Select **Agent access**.

3. Select a site to view the top 20 agents accessing the content across the selected site.



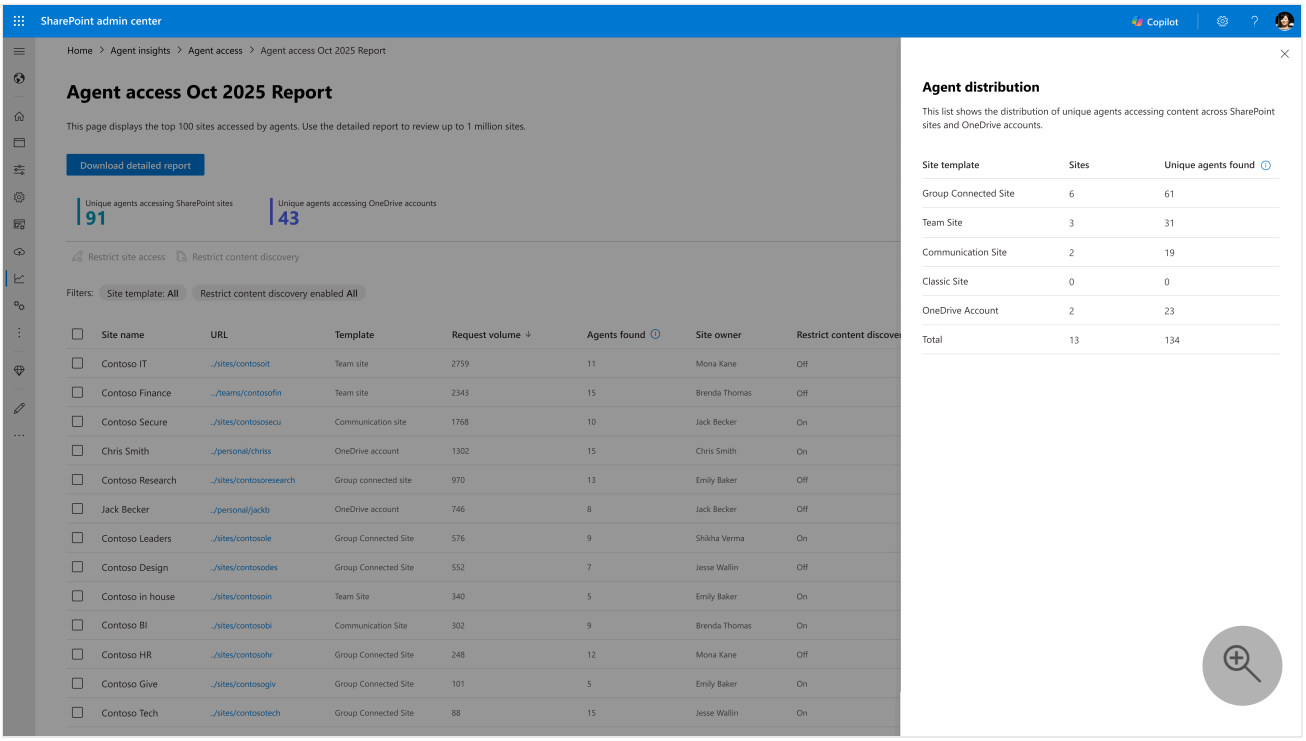
View agent distribution across sites

1. In the SharePoint admin center, in the navigation pane, expand **Reports**, and then select **Agent insights**.

2. Select **Agent access**.

3. Choose **Unique Agents found in SharePoint Sites** or **Unique Agents in OneDrive Account**.

   This view displays how agents are distributed across your organization's sites. You can quickly see the number of sites in each site template category and how many unique agents are accessing them.



Apply content governance policies from the access report

You can apply content governance policies on the sites from the access insights report. The available policies are:

- Restrict site access policy
- Restrict Content Discovery policy

> **Important**
>
> After you apply a policy to the site from the insights report, the policy status on the existing report doesn't update. To view the updated status of the policy on the site, select the policy to view the latest status or access the **Active site** panel and review the site settings.

Access the agent access insights report by using SharePoint Online Management Shell

You can generate, check, and manage agent access insights reports by using SharePoint Online Management Shell.

Prerequisites

- If you didn't already, download and install the latest version of SharePoint Online Management Shell.
- You must have at least a SharePoint administrator assigned in Microsoft 365.
- Connect to the SharePoint Online Management Shell. See Getting started with SharePoint Online Management Shell.
- Make sure your organization has a license for the SharePoint Advanced Management add-on or Microsoft 365 Copilot.

Create and view an agent access insights report with SharePoint Online Management Shell

With permissions of at least a SharePoint administrator, you can generate and view the insights report by using the following commands:

1. To generate a report for the default one-day report duration, run the following command:

   PowerShell
   ```
   Start-SPOM365AgentAccessInsightsReport
   ```

   This command generates an agent access insights report for the past one day by default.

2. You can specify a different duration (7, 14, or 28 days) by using the `-ReportPeriodInDays` parameter. For example, to create a report for the past 28 days, run:

   PowerShell
   ```
   Start-SPOM365AgentAccessInsightsReport -ReportPeriodInDays <28>
   ```

3. To check the status of all active and available reports, run the following command:

   PowerShell
   ```
   Get-SPOM365AgentAccessInsightsReport
   ```

4. To view the details of a specific report, run the following command:

   PowerShell
   ```
   Get-SPOM365AgentAccessInsightsReport -ReportId <ReportId>
   ```

   Replace `<ReportId>` with the actual Report ID obtained from the previous command.

5. To download and view the report, run the following command:

```
PowerShell
Export-SPOM365AgentAccessInsightsReport -ReportId <ReportId> -Action Download
```

> **Note**
>
> PowerShell displays up to 100 sites but downloaded reports can contain up to 1 million sites.

```
PowerShell
Export-SPOM365AgentAccessInsightsReport -ReportId <ReportId> -View Download
```

Replace `<ReportId>` with the actual Report ID.

6. You can also view summarized insights of agents across all site types by running the following command:

```
PowerShell
Get-SPOM365AgentAccessInsightsReport –ReportId -Content SiteDistribution
```

SiteDistribution provides the summarized view of agents across all types of sites like Communication sites, Microsoft 365 group connected sites, OneDrive accounts, and more.

Data collection for agent access insights report

If you don't have a Microsoft SharePoint Advanced Management license, you need to enable data collection. This section explains how to enable and check the status of data collection for the agent access insights report.

Enable data collection

The following PowerShell command starts collecting audit data for reports on activities from the previous day:

```
PowerShell
```

```
Start-SPOAuditDataCollectionForActivityInsights –ReportEntity M365AgentInsights
```

Check data collection status

After you enable data collection, you can generate the reports after 24 hours. To check whether you can generate reports, use the following PowerShell command:

PowerShell

```
Get-SPOAuditDataCollectionStatusForActivityInsights -ReportEntity M365AgentInsights
```

This command returns the current data collection status, which can be `NotInitiated`, `InProgress`, or `Paused`. You can generate reports when the status is `InProgress`.

Known experiences with Microsoft 365 agent access insights

Keep these important known experiences in mind when working with agent access insights reports in the SharePoint admin center or SharePoint Online Management Shell:

- You can run a report only after 24 hours pass since the last report generation.
- For large tenants, it can take up to 48 hours for data to become available.
- Only one report can exist for each report range value (1, 7, 14, or 28 days). This limitation means you can see a maximum of four reports at any given point.
- When you generate a new report for the same date range, it replaces the previous report. To keep the old report, download it before creating a new one.
- Reports use Microsoft 365 unified audit data, which might not include every audit event.

Related articles

- Manage access to agents in SharePoint
- Insights on agents created in SharePoint
- Restrict SharePoint site access with Microsoft 365 groups and Microsoft Entra security groups
- Restrict discovery of SharePoint sites and content

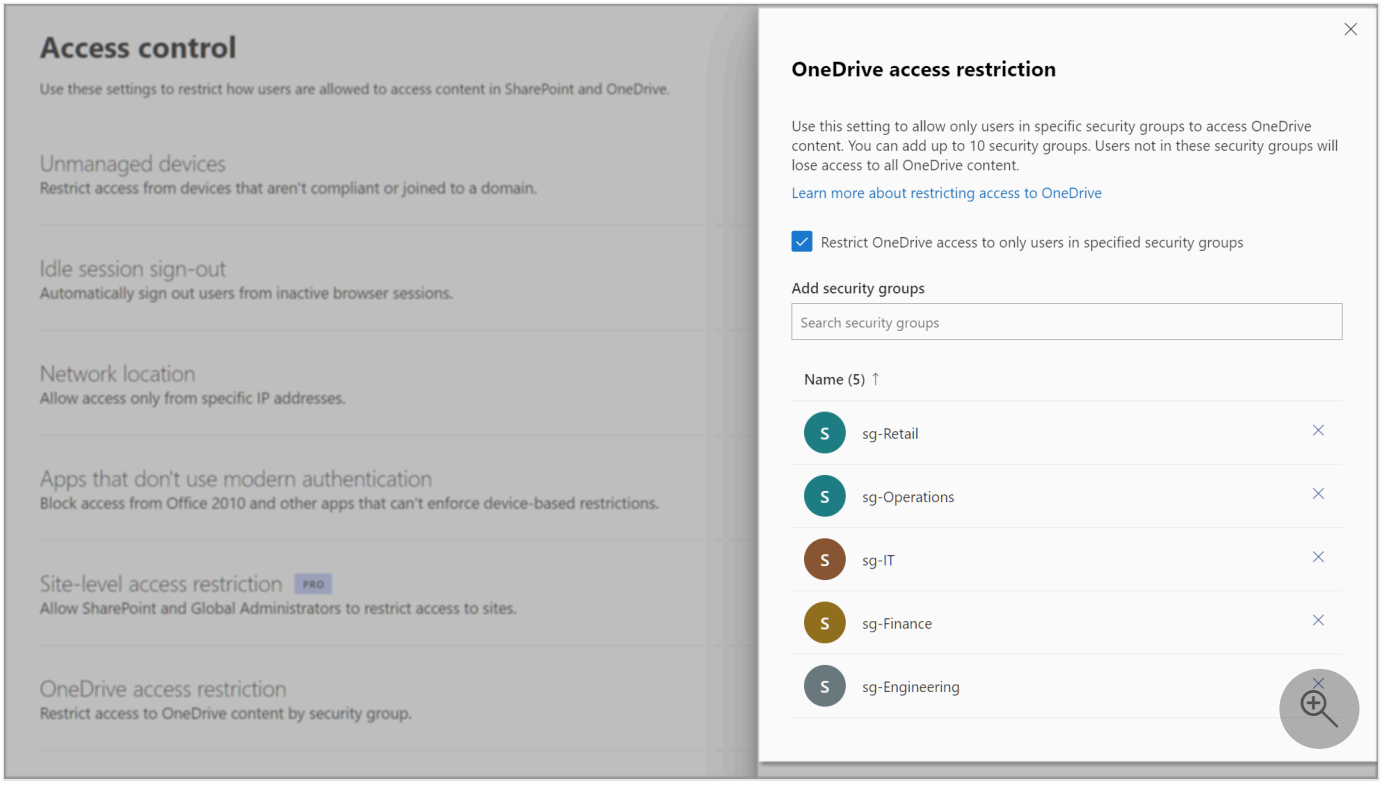
Last updated on 05/13/2026

Restrict OneDrive access by security group

You can restrict access and sharing of OneDrive content to users in specified Microsoft Entra ID security groups. Even if other users outside of these security groups are licensed for OneDrive, they won't have access to their own OneDrive or any shared OneDrive content when this policy is in effect. OneDrive access restriction at tenant level is applied when a user attempts to open a OneDrive or a file.

You can use this to prevent new users from accessing any OneDrive content. For example, you can restrict OneDrive access and sharing to your new users, guest or frontline users.

Users who aren't members of the specified security group can still see files in organization-wide search and Copilot experiences if they have existing permissions to the file prior to the policy configuration. However they won't be able to open the file or OneDrive if they aren't part of the specified security group.



> **Note**
>
> If you want to prevent oversharing of OneDrive content also for users with existing permissions, we recommend you to enforce OneDrive site access restriction to an individual

user's OneDrive. For more information, see Restrict access to a user's OneDrive content to people in a security group.

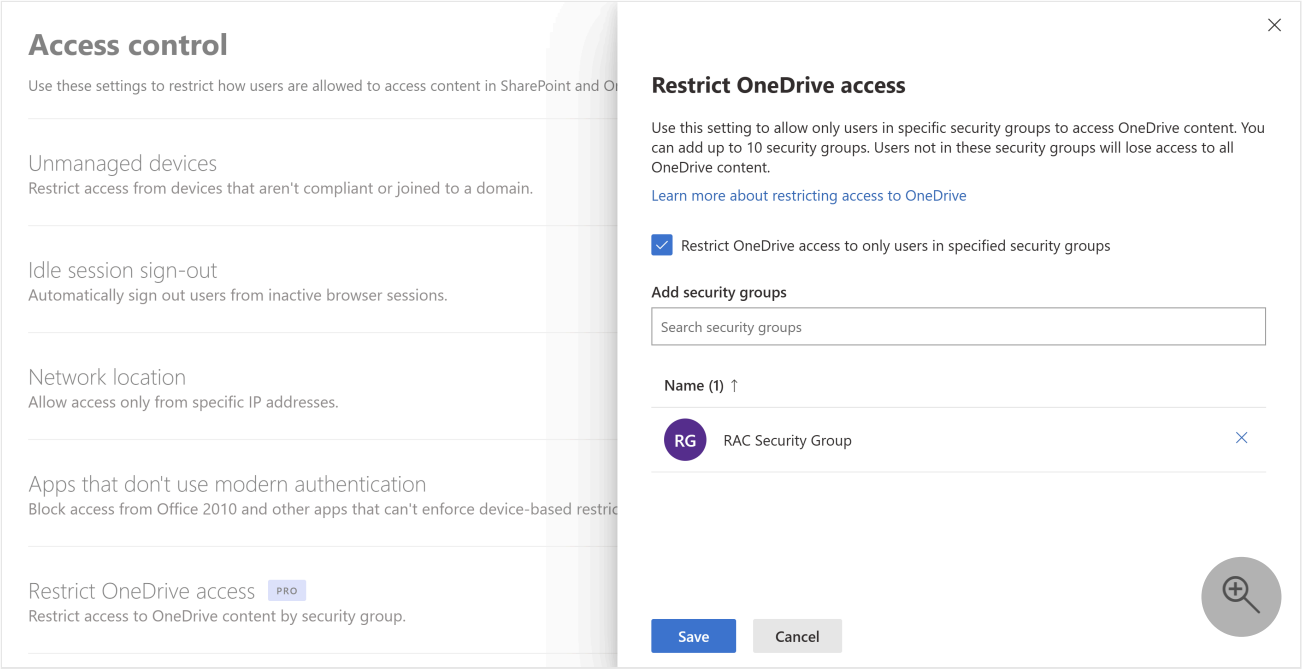
What you need to restrict OneDrive access?

See Prerequisites for SharePoint Advanced Management.

Specify security groups for OneDrive access

To enable this feature:

1. Go to Access control in the SharePoint admin center, and sign in with an account that has admin permissions for your organization.
2. Select **Restrict OneDrive access**.
3. Select **Restrict OneDrive access to only users in specified security groups**.



4. Add the security groups (maximum of 10) you want to be able to use OneDrive.
5. Select **Save**.

Important

Users who aren't members of the specified security groups lose access to their own OneDrive and any shared OneDrive content. Sharing of content is allowed only for the specified security group or members of the specified security group.

Configure learn more link for access denial error page

Configure your learn more link to inform users who were denied access to a OneDrive site due to the OneDrive access restriction policy. With this customizable error link, you can provide more information and guidance to your users.

> **Note**
>
> The learn more link is a tenant-level setting that applies to all OneDrive sites.

To configure the link, run the following command in SharePoint PowerShell:

PowerShell

```
Set-SPOTenant -RestrictedAccessControlForOneDriveErrorHelpLink "<Learn more URL>"
```

To fetch the value of the link, run the following command:

PowerShell

```
Get-SPOTenant | select RestrictedAccessControlForOneDriveErrorHelpLink
```

The configured learn more link is launched when the user selects the **Know more about your organization's policies here** link.

Audit events

Audit events are available in Microsoft Purview portal to help you monitor restricted access control activities. Audit events are logged for the following activities:

- Enabled Restricted OneDrive access and sharing
- Disabled Restricted OneDrive access and sharing

Related topics

Restrict access control for SharePoint sites

Data access governance insights for SharePoint sites

Last updated on 07/01/2026

Restrict access to a user's OneDrive content to people in a group

You can restrict access to an individual user's OneDrive content to users in a security group or Microsoft 365 group by using a site access restriction policy. Users not in the specified group can't access the content, even if they had prior permissions or shared link.

Apply the policy by using Microsoft Entra security groups or Microsoft 365 groups that contain the people who should be able to access files in that OneDrive.

When you apply the policy, the people in the specified groups aren't granted permissions to any files directly. The OneDrive owner must share the content as they normally would. The site access restriction policy prevents anyone who isn't in the security group or the Microsoft 365 group from accessing the OneDrive content even if it's shared with them.

Access restriction policies are applied when a user attempts to access a file. Users can still see files in search results if they have direct permissions to the file, but they can't access the file if they're not part of the specified group.

You can also restrict access to the OneDrive service itself to people in a security group. For more information, see Restrict OneDrive access by security group.

Before you begin

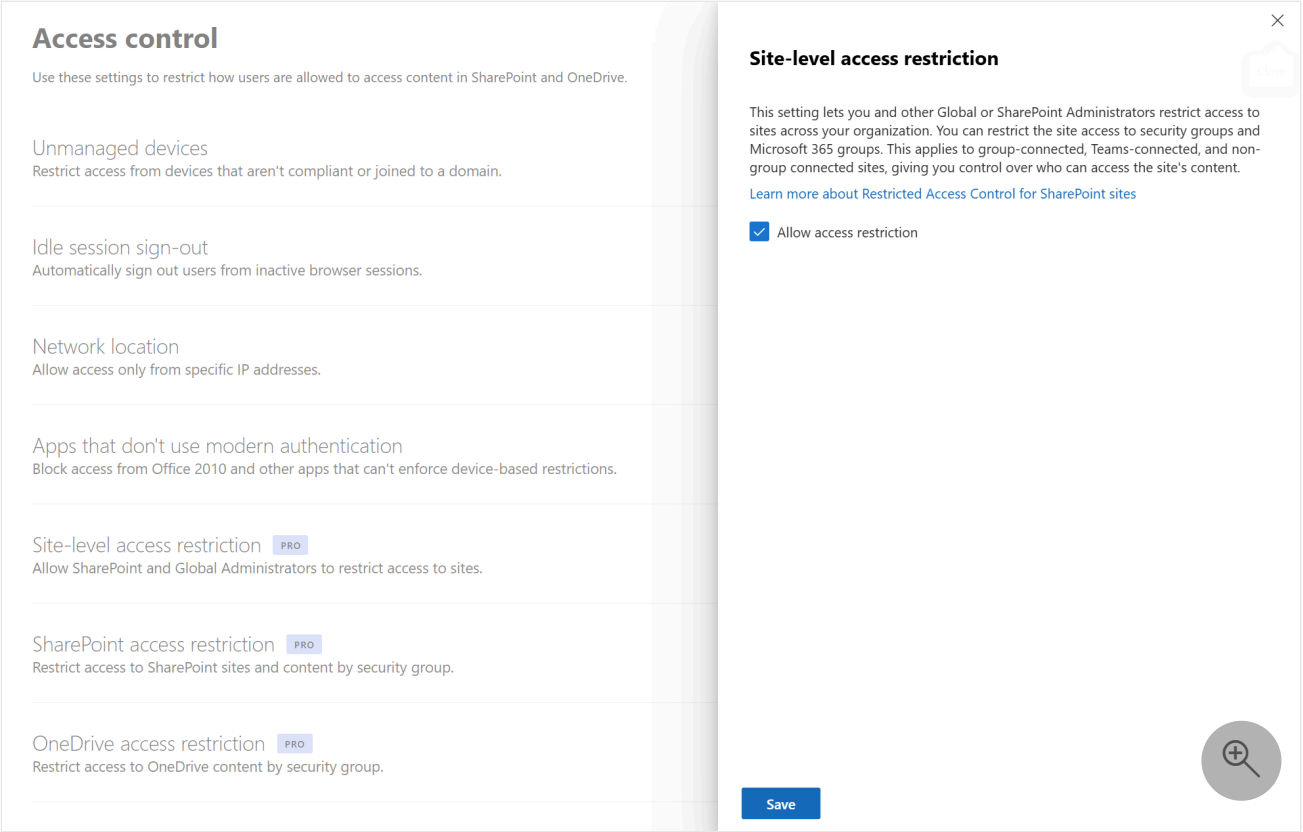
Make sure your organization meets the Prerequisites for SharePoint Advanced Management, including requirements for SharePoint Online PowerShell module.

Enable site access restriction for your organization

You must enable site access restriction for your organization before you can configure it for a user's OneDrive.

To enable site access restriction for your organization in SharePoint admin center:

1. Expand **Policies** and select **Access control**.
2. Select **Site access restriction**.
3. Select **Allow access restriction** and then select **Save**.



To enable site access restriction for your organization using PowerShell, run the following command:

Powershell

```
Set-SPOTenant -EnableRestrictedAccessControl $true
```

It might take up to one hour for command to take effect.

> **Note**
>
> For Microsoft 365 Multi-Geo users, run this command separately for each desired geo-location.

Restrict access to a user's OneDrive content

Assign up to 10 Microsoft Entra security or Microsoft 365 groups to each OneDrive. After you add a group, only users in the groups can access content in that OneDrive that you shared with them. Use dynamic security groups if you want to base group membership on user properties.

> **Important**

> The owner of the OneDrive must be included in one of the security or Microsoft 365 groups that you specify or they lose access to their OneDrive and its contents.

To manage access restriction for OneDrive, use the PowerShell commands in this section.

Enable access restriction for a given OneDrive library

Run the following command before adding security or Microsoft 365 groups.

PowerShell

```
Set-SPOSite -Identity <siteurl> -RestrictedAccessControl $true
```

Add a security group or a Microsoft 365 group

Run the following command:

PowerShell

```
Set-SPOSite -Identity <siteurl> -AddRestrictedAccessControlGroups <comma separated
group GUIDS>
```

Edit a security group or a Microsoft 365 group

Run the following command:

PowerShell

```
Set-SPOSite -Identity <siteurl> -RestrictedAccessControlGroups <comma separated group
GUIDS>
```

View a security group or a Microsoft 365 group

Run the following command:

PowerShell

```
Get-SPOSite -Identity <siteurl> Select RestrictedAccessControl,
RestrictedAccessControlGroups
```

Remove a security group or a Microsoft 365 group

Run the following command:

```
PowerShell
Set-SPOSite -Identity <siteurl> -RemoveRestrictedAccessControlGroups <comma separated group GUIDS>
```

Reset site access restriction

Run the following command:

```
PowerShell
Set-SPOSite -Identity <siteurl> -ClearRestrictedAccessControl
```

Site sharing and restricted site access policies

Block OneDrive site sharing for users and groups who aren't allowed as per the restricted access control policy.

The sharing control functionality is disabled by default. To enable it, run the following command:

```
PowerShell
Set-SPOTenant -AllowSharingOutsideRestrictedAccessControlGroups $false
```

Sharing with users

Allow sharing only with users who are part of restricted access control groups. Block sharing with anyone outside of the restricted access control groups as shown in the following image:

Sharing with groups

You can share with Microsoft Entra Security or Microsoft 365 groups that are part of the restricted access control groups list. You can't share with all other groups, including Everyone except external users or SharePoint groups.

> **Note**

Currently, you can't share a site and its content with nested security groups that are part of the restricted access control groups.

Configure learn more link for access denial error page

Configure your "learn more" link to inform users who were denied access to a OneDrive site because of a restricted site access control policy. By using this customizable error link, you can provide more information and guidance to your users.

> **Note**
>
> The "learn more" link is a tenant-level setting that applies to all OneDrive sites that have restricted access control policy enabled.

Configure the "learn more" link

Run the following command:

PowerShell

```
Set-SPOTenant -RestrictedAccessControlForSitesErrorHelpLink "<Learn more URL>"
```

Fetch the value of the link

Run the following command:

PowerShell

```
Get-SPOTenant | select RestrictedAccessControlForSitesErrorHelpLink
```

The configured learn more link launches when the user selects the **Know more about your organization's policies here** link.

Restricted site access policy insights

As an IT administrator, you can view the following reports to gain more insight about OneDrive sites protected with restricted site access policy:

- Sites protected by restricted site access policy (RACProtectedSites)

- Details of access denials due to restricted site access (ActionsBlockedByPolicy)

> **Note**
>
> It can take a few hours to generate each report.

Sites protected by restricted site access policy report

Use the following commands to generate, view, and download reports.

Generate a report

Run the following command:

```
PowerShell
Start-SPORestrictedAccessForSitesInsights -RACProtectedSites
```

This command generates a list of sites protected by restricted site access policy.

View a report

Run the following command:

```
PowerShell
Get-SPORestrictedAccessForSitesInsights -RACProtectedSites -ReportId <Report GUID>
```

This command creates a report that shows the top 100 sites with the highest page views that are protected by the policy.

Download a report

Run the following command:

```
PowerShell
Get-SPORestrictedAccessForSitesInsights -RACProtectedSites -ReportId <Report GUID> -
Action Download
```

This command must be run as an administrator. The downloaded report is located in the path where the command was run.

View the percentage of sites protected with restricted site access

Run the following command:

PowerShell

```
Get-SPORestrictedAccessForSitesInsights -RACProtectedSites -ReportId <Report GUID> -
InsightsSummary
```

This report shows the percentage of sites that are protected by the policy out of the total number of sites.

Access denials due to restricted site access policy

Use the commands in this section to create, fetch, and view reports for access denials due to restricted site access reports.

To create an access denials report

Run the following command:

PowerShell

```
Start-SPORestrictedAccessForSitesInsights -ActionsBlockedByPolicy
```

This command creates a new report for fetching access denial details.

To get the status of an access denials report

Run the following command:

PowerShell

```
Get-SPORestrictedAccessForSitesInsights -ActionsBlockedByPolicy
```

This command fetches the status of the generated access denials report.

To see the latest access denials in the past 28 days

Run the following command:

PowerShell

```
Get-SPORestrictedAccessForSitesInsights -ActionsBlockedByPolicy -ReportId <Report ID>
-Content AllDenials
```

This command creates a list of the most recent 100 access denials that occurred in the past 28 days.

To view a list of top users who were denied access

Run the following command:

PowerShell

```
Get-SPORestrictedAccessForSitesInsights -ActionsBlockedByPolicy -ReportId <Report ID>
-Content TopUsers
```

This command creates a list of the top 100 users who received the most access denials.

To view a list of top sites that received the most access denials

Run the following command:

PowerShell

```
Get-SPORestrictedAccessForSitesInsights -ActionsBlockedByPolicy -ReportId <Report ID>
-Content TopSites
```

This command creates a list of the top 100 sites that had the most access denials.

To see the distribution of access denials across different types of sites

Run the following command:

PowerShell

```
Get-SPORestrictedAccessForSitesInsights -ActionsBlockedByPolicy -ReportId <Report ID>
-Content SiteDistribution
```

This command shows the distribution of access denials across different types of sites.

Note

To view up to 10,000 denials, download the reports. Run the download command as an administrator. The downloaded reports are located in the path from where the command was run.

Auditing

The Microsoft Purview portal provides audit events that help you monitor site access restriction activities. The system logs audit events for the following activities:

- Applying site access restriction for a site
- Removing site access restriction for a site
- Changing site access restriction groups for a site

Related articles

- What is SharePoint Advanced Management?
- Data access governance insights for SharePoint sites

Last updated on 07/01/2026

Restrict OneDrive and SharePoint site creation by users

The restricted site creation feature IT administrators use SharePoint Online Management Shell to designate which Microsoft Entra security groups in their tenant can create OneDrive and SharePoint sites.

You can choose between two ways to manage site creation within your tenant: deny mode (the specified groups can't create sites) and allow mode (only the specified groups can create sites). When you enable this feature for your tenant, restricted site creation defaults to **deny** mode.

Restricted site creation policies only control site provisioning capabilities and not site access permissions.

Prerequisites

Your organization needs **SharePoint Advanced Management Plan 1**. See Prerequisites: SharePoint Advanced Management Plan 1 add-on.

Also see the requirements for the SharePoint Online PowerShell module.

Site types for restricted site creation by users

Each restricted site creation policy includes a *site type* specifying the types of sites users in the specified groups are either allowed or denied from creating.

Expand table

Site type	Applies to
All	OneDrive and all SharePoint sites
SharePoint	All SharePoint sites (but not OneDrive)
OneDrive	Only OneDrive
Team	Only SharePoint team sites (classic)
Communication	Only SharePoint communication sites

You can specify up to 10 Microsoft Entra security groups for each site type.

How do restricted site creation deny and allow modes work?

The restricted site creation by users mode is shared across all site type policies. You can't use deny mode for one site type and allow mode for a different site type.

When you set restricted site creation by users to **deny** mode, users can't create a site if they belong to any security group configured for a site type that matches the site they want to create. For example, if a user is in a group listed under the All, SharePoint, or Communication site types, they can't create a SharePoint communication site.

When you set restricted site creation by users to **allow** mode, users can only create a site if they belong to a security group configured for a site type that matches the site they want to create. For example, a user can create a OneDrive site only if they're in a group listed under the All or OneDrive site types.

Current limitations of restricted site creation by users

- Only Microsoft Entra security groups (mail-enabled or non-mail-enabled) are supported at this time.
- You can configure up to 10 security groups per site type.
- This feature isn't currently available for Microsoft 365 government cloud environments, such as GCC, GCC-High, DoD, or Microsoft 365 operated by 21Vianet.

Manage restricted site creation by users

The Set-SPORestrictedSiteCreation and Get-SPORestrictedSiteCreation commands allow administrators to configure and view the restricted site creation feature and policies for the tenant.

> **Important**
>
> You must use version 16.0.25513.12000 (published November 2024) or later of the SharePoint Online Management Shell for these commands to function properly. Earlier versions don't have the current list of site types and don't operate correctly.

Enable restricted site creation by users

To enable restricted site creation by users, run the following command in the SharePoint Online Management Shell:

PowerShell

```
Set-SPORestrictedSiteCreation -Enabled $true
```

Restricted site creation by users starts in deny mode without any policies, and doesn't affect any users by default.

Set Allow or Deny mode for restricted site creation by users

After you turn on the restricted site creation by users feature, decide whether you want to deny certain groups of users from creating sites or allow certain groups to create sites.

For example, the following command sets restricted site creation to deny mode:

PowerShell

```
Set-SPORestrictedSiteCreation -Mode Deny
```

> **Important**
>
> Swapping between the two modes removes all existing site type configurations. The restricted site creation feature only supports either all deny or all allow configurations.

Configure policies for site types

You can specify a comma-separated list of up to 10 Microsoft Entra security groups for each site type. For example, if restricted site creation is in deny mode, the following command creates a policy blocking users in either of the following two groups from creating any SharePoint site.

PowerShell

```
Set-SPORestrictedSiteCreation -SiteType SharePoint -RestrictedSiteCreationGroups
"00aa00aa-bb11-cc22-dd33-44ee44ee44ee,11bb11bb-cc22-dd33-ee44-55ff55ff55ff"
```

> **Note**

> You must specify Microsoft Entra security groups by using the Object ID shown in the Microsoft Entra admin center.

To clear the configuration for a site type, specify "" for the RestrictedSiteCreationGroups:

PowerShell

```
Set-SPORestrictedSiteCreation -SiteType All -RestrictedSiteCreationGroups ""
```

View configuration

Use the following command to view the existing restricted site creation configurations:

PowerShell

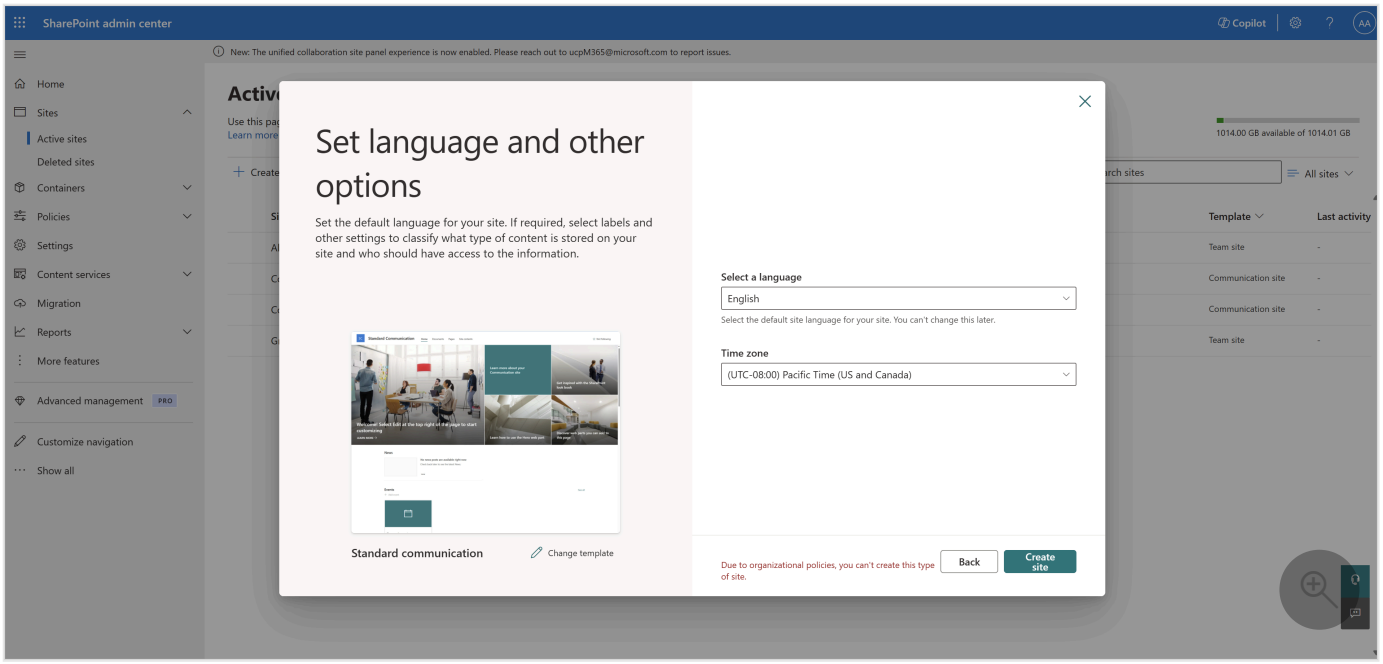
```
Get-SPORestrictedSiteCreation
```

What messages do users see when restricted from site creation?

When a user is blocked from creating a site by a restricted site creation by users policy, they receive a message depending on the type of site they're creating and how they're creating it. See the following examples for reference:

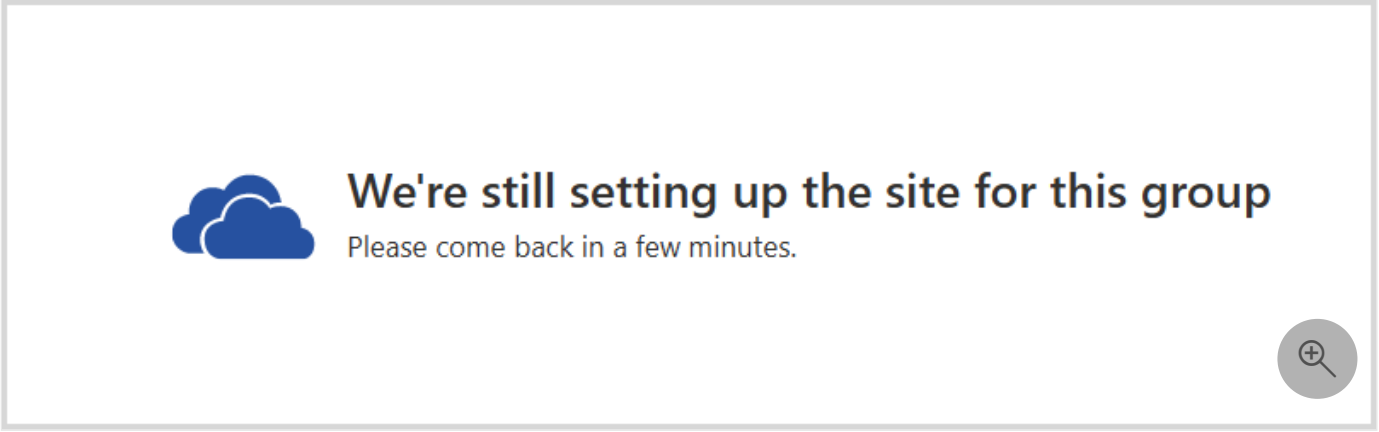
Example 1: User can't create a communication site

When a user creates a communication site from the web, they see the error message "Due to organizational policies, you can't create this type of site."



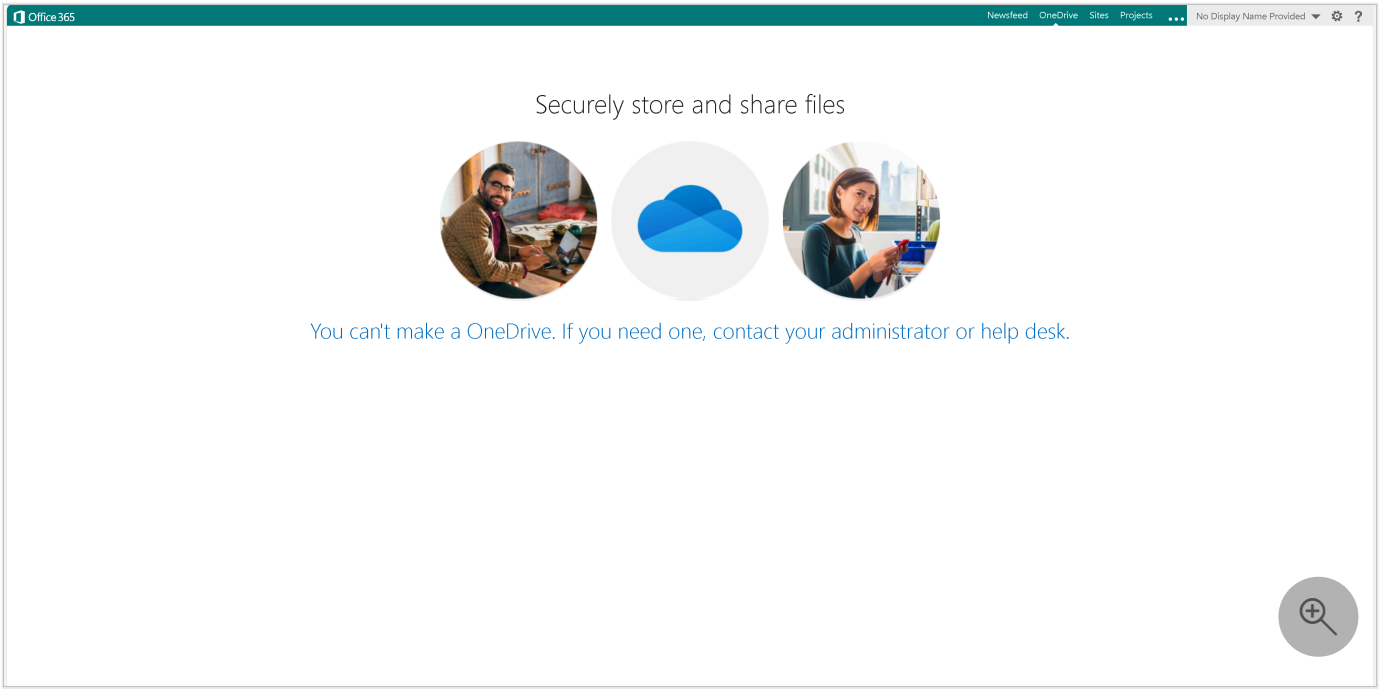
Example 2: User can't create a team site

When a user creates a team site from the web, the user sees the message "We're still setting up the site for this group," but the site isn't created.



Example 3: User can't access OneDrive

When first signing in to their OneDrive from the web, the user sees the error message "You can't make a OneDrive. If you need one, contact your administrator or help desk."



Example 4: User can't create a site using PowerShell

When creating sites through the SharePoint Online Management Shell, the cmdlet fails with the exception "Due to organizational policies, you can't create this type of site."

Related articles

- Microsoft SharePoint Premium – SharePoint Advanced Management overview
- Set-SPORestrictedSiteCreation
- Get-SPORestrictedSiteCreation

Last updated on 09/02/2026

Restrict SharePoint site access for applications and agents with Application Restrictions

Application Restrictions helps prevent oversharing to *applications* by designating which apps and agents can access a SharePoint site and its content. Applications not permitted by the policy can't access the site or its content, even when they hold Microsoft Entra consent and SharePoint permissions.

Application Restrictions adds an authorization boundary for applications that already have Entra consent and SharePoint permissions. It never grants permissions and it doesn't replace Entra consent. A request must pass **both** the existing permission model and Application Restrictions.

The policy is enforced when an application accesses SharePoint sites and content, either by itself (app-only) or on behalf of a signed-in user (app-plus-user, also called delegated).

> **Note**
>
> Application Restrictions governs **applications and agents**. To restrict which *users* can access a site, see Restrict SharePoint site access with Microsoft 365 groups and Microsoft Entra security groups. The two policies are independent and can be configured on the same site.

How the policy is evaluated

Application Restrictions has two scopes that work together, and they're evaluated in a fixed order.

Expand table

Order	Scope	Effect
1	**Not an app request, or not a third-party app**	Allowed. Application Restrictions doesn't apply.
2	**Tenant switch is off**	Allowed. All Application Restrictions enforcement is disabled, including any configured site policies.
3	**Tenant deny list**	Denied if the application matches. A site policy can't override this.

Order	Scope	Effect
4	**Site policy absent or disabled**	Allowed.
5	**Site policy in `Allow` mode**	Allowed only if the application matches the allow list. All other governed apps are denied.
6	**Site policy in `Deny` mode**	Denied if the application matches the deny list. All other governed apps are allowed.

Two consequences matter for planning:

- **The tenant switch is the master switch.** While it's off, nothing is enforced, including the tenant deny list and any configured site policies. Turning it on begins enforcement tenant-wide, including every site policy already staged.
- **The tenant deny list is your emergency brake.** It always outranks site configuration, so a site allow list can never re-admit an application denied at tenant scope.

Microsoft applications are excluded

Microsoft first-party and core applications are excluded from both configuration and enforcement. You can't add a first-party application ID to a tenant or site list. The cmdlet rejects the change. At runtime, only applications positively classified as third-party are governed; an unclassified or first-party caller is never blocked by this policy.

Applications and agent blueprints

A list entry is either a concrete application ID or a **parent agent blueprint ID**. A blueprint entry applies to the blueprint application itself and to every current or future agent app created from that blueprint. This lets you govern a whole family of agents with one entry.

You don't need to know which kind of ID you're supplying. Provide the application IDs and the service classifies and stores each one for you. Likewise, the allow and deny lists are returned to you as a single, duplicate-free list of GUIDs.

Prerequisites

- You must be at least a SharePoint Administrator.
- Install and connect to SharePoint Online Management Shell.
- Collect the Entra **application (client) IDs** you intend to govern. These are application IDs, not directory object IDs.

> **Important**
>
> Application Restrictions doesn't apply to personal sites in this release. It also doesn't trim search results or enumeration, and it doesn't offer granular access levels. A request is either allowed to continue through existing authorization or blocked from the site.

Step 1: Turn on Application Restrictions for your organization

Enforcement is off until you enable it at tenant scope. Nothing you configure at site scope takes effect until you do.

PowerShell

```
Enable-SPOTenantRestrictedAppAccessControl
```

Enabling begins enforcement tenant-wide, including all configured site policies, so the cmdlet warns you before it commits. To confirm the current state at any time:

PowerShell

```
Get-SPOTenantRestrictedAppAccessControl
```

The cmdlet returns `Enabled` and `RestrictedAppIds`—the tenant deny list. Reads are always authoritative and uncached, so the values reflect the latest committed policy.

> **Tip**
>
> A safer sequence for a first rollout is to stage site policies first (steps 3 and 4), verify them, and turn on the tenant switch last. Nothing is enforced until the switch is on.

Step 2: Block an application across the entire organization

The tenant list is a deny list, and it's intended as an emergency control for an application you want kept out of every site. Use it sparingly. For scoped restrictions, prefer a site policy.

Add one or more applications:

PowerShell

```
Set-SPOTenantRestrictedAppAccessControlList -AddRestrictedAppIds "11111111-1111-1111-1111-111111111111","22222222-2222-2222-2222-222222222222"
```

Remove an application:

PowerShell

```
Set-SPOTenantRestrictedAppAccessControlList -RemoveRestrictedAppIds "11111111-1111-1111-1111-111111111111"
```

Notes on behavior:

- Additions and removals apply as one atomic update, and removals are applied before additions. An ID can't appear in both parameters.
- Adding is all-or-none. If any supplied ID belongs to a Microsoft first-party application or the service can't classify it, the whole change is rejected and nothing is written.
- Removing doesn't require the application to still exist, so you can always clean up stale or deleted app IDs.
- List changes never turn the tenant switch on or off. Configuration and enablement stay independent.
- The tenant deny list holds a maximum of **100** application IDs.

Step 3: Choose the enforcement mode for a site

Each site has an active mode that decides which of its two lists is enforced.

Expand table

Mode	Behavior	Use when
`Allow`	Only applications on the allow list can access the site. All other governed apps are denied.	You want a known, closed set of apps on a sensitive site.
`Deny`	Applications on the deny list are blocked. All other governed apps are allowed.	You want to exclude specific apps and leave the site otherwise open.

PowerShell

```
Set-SPOSiteRestrictedAppAccessControlMode -Identity "https://contoso.sharepoint.com/sites/Finance" -Mode Allow
```

You must set a mode before you enable Application Restrictions on a site. Every site cmdlet accepts `-Identity` as either a site URL or a site ID.

Both lists are stored permanently, and a mode change preserves both of them. Only the list selected by the active mode participates in enforcement; the other is kept for later and has no runtime effect. When you switch modes, the cmdlet warns you first, identifying the current mode, the target mode, the size of the newly active list, and the new default decision.

> **Important**
>
> An empty active **allow** list blocks every governed third-party and agentic application from the site. An empty active **deny** list blocks nothing.

Step 4: Add applications to the site's allow or deny list

Specify which list you're changing with `-ListType`, then add or remove IDs:

PowerShell

```
# Add two applications to the allow list
Set-SPOSiteRestrictedAppAccessControlList -Identity
"https://contoso.sharepoint.com/sites/Finance" -ListType AllowList -
AddRestrictedAppIds "11111111-1111-1111-1111-111111111111","22222222-2222-2222-2222-
222222222222"

# Remove an application from the allow list
Set-SPOSiteRestrictedAppAccessControlList -Identity
"https://contoso.sharepoint.com/sites/Finance" -ListType AllowList -
RemoveRestrictedAppIds "11111111-1111-1111-1111-111111111111"
```

The same rules as the tenant list apply: updates are atomic, removals occur before additions, an ID can't appear in both parameters, and all additions fail if any ID belongs to a first-party application. If you try to remove an ID that isn't present, the cmdlet returns a validation error.

Each site list holds up to **100** entries, and the two lists together hold up to **200**.

List and mode changes update only the configuration. They never turn enforcement on. That's deliberate: it prevents a single added ID from instantly activating an allow list on an unconfigured site and locking out every other application.

Step 5: Turn on enforcement for the site

Once the mode and lists are staged and reviewed, enable the site:

PowerShell

```
Enable-SPOSiteRestrictedAppAccessControl -Identity
"https://contoso.sharepoint.com/sites/Finance"
```

The cmdlet fails if no mode is set on the site. Set a mode first by completing step 3.

Step 6: Verify the policy

PowerShell

```
Get-SPOSiteRestrictedAppAccessControl -Identity
"https://contoso.sharepoint.com/sites/Finance"
```

The cmdlet returns `SiteUrl`, `Enabled`, `Mode`, `AllowList`, and `DenyList`. Because the returned object carries its own `SiteUrl`, you can pipe sites into the cmdlet and still identify each result.

Confirm all three layers before you rely on the outcome:

PowerShell

```
# Is the master switch on, and is the app denied tenant-wide?
Get-SPOTenantRestrictedAppAccessControl

# What is this site enforcing right now?
Get-SPOSiteRestrictedAppAccessControl -Identity
"https://contoso.sharepoint.com/sites/Finance"
```

If the returned policy includes `IsPolicyDataMalformed`, the stored site policy couldn't be read. Application Restrictions doesn't enforce on that site until the policy is rewritten. Existing SharePoint authorization still applies, so reapply the configuration to replace it.

Change or roll back a policy

Choose the narrowest action that achieves what you want.

Expand table

Goal	Cmdlet	What it preserves
Stop enforcing on one site, keep the	`Disable-SPOSiteRestrictedAppAccessControl`	Mode and both lists

Goal	Cmdlet	What it preserves
configuration		
Empty one list, keep everything else	`Clear-SPOSiteRestrictedAppAccessControlList -ListType <AllowList or DenyList>`	The other list, the mode, and site enablement
Remove a site's policy entirely	`Clear-SPOSiteRestrictedAppAccessControlPolicy`	It preserves nothing. The cmdlet disables enforcement and removes the mode and both lists.
Stop enforcing organization-wide, keep the deny list	`Disable-SPOTenantRestrictedAppAccessControl`	The tenant deny list and all site configuration
Remove the tenant policy entirely	`Clear-SPOTenantRestrictedAppAccessControlPolicy`	It preserves nothing. The cmdlet disables the switch and clears the deny list.

Examples:

PowerShell

```powershell
# Pause enforcement on a site without losing the configuration
Disable-SPOSiteRestrictedAppAccessControl -Identity
"https://contoso.sharepoint.com/sites/Finance"

# Empty the deny list but keep the allow list, mode, and enablement
Clear-SPOSiteRestrictedAppAccessControlList -Identity
"https://contoso.sharepoint.com/sites/Finance" -ListType DenyList

# Remove the site policy entirely
Clear-SPOSiteRestrictedAppAccessControlPolicy -Identity
"https://contoso.sharepoint.com/sites/Finance"
```

> ⚠ **Warning**
>
> Clearing the list that the active mode enforces changes enforcement immediately. Clearing an active **allow** list means no third-party applications can access the site; clearing an active **deny** list means all of them can. The cmdlet warns you and states whether the change takes effect now or when enforcement is next enabled.

Disabling or clearing at **tenant** scope stops every configured site policy from enforcing, not just the tenant deny list. Both cmdlets warn you before committing.

Confirmation prompts and automation

Every cmdlet that changes policy supports `-WhatIf` and `-Confirm`, and prompts for confirmation by default.

PowerShell

```powershell
# Preview the impact of a mode switch without changing anything
Set-SPOSiteRestrictedAppAccessControlMode -Identity
"https://contoso.sharepoint.com/sites/Finance" -Mode Deny -WhatIf

# Suppress the prompt in an automated script
Enable-SPOSiteRestrictedAppAccessControl -Identity
"https://contoso.sharepoint.com/sites/Finance" -Confirm:$false
```

`-WhatIf` shows the same impact summary as the interactive prompt. Using `-Confirm:$false` suppresses only the prompt. It doesn't bypass validation, authorization, auditing, or first-party protection.

Auditing

Policy changes are recorded in the unified audit log with dedicated operations:

Expand table

Operation	Raised by
`RestrictedAppAccessControlTenantPolicyUpdated`	Tenant mutations
`RestrictedAppAccessControlTenantPolicyCleared`	A complete tenant clear
`RestrictedAppAccessControlSitePolicyUpdated`	Site mutations
`RestrictedAppAccessControlSitePolicyCleared`	A complete site clear

Records contain only the policy fields you already see in PowerShell. Tenant records may include `Enabled`, `RestrictedAppIds`, and `IsPolicyDataMalformed`; site records may include `Enabled`, `Mode`, `AllowList`, `DenyList`, and `IsPolicyDataMalformed`, with `SiteUrl` and the acting administrator supplied by the audit envelope. No secrets or access tokens are recorded.

A record is written only after a change is persisted and only for properties whose values actually changed. An update that changes nothing emits no record.

Cmdlet reference

Tenant

Expand table

Cmdlet	Purpose
Get-SPOTenantRestrictedAppAccessControl	Return the tenant switch and deny list
Set-SPOTenantRestrictedAppAccessControlList	Add or remove applications on the tenant deny list
Enable-SPOTenantRestrictedAppAccessControl	Turn on enforcement organization-wide
Disable-SPOTenantRestrictedAppAccessControl	Turn off enforcement, preserving the deny list
Clear-SPOTenantRestrictedAppAccessControlPolicy	Turn off enforcement and clear the deny list

Site

Expand table

Cmdlet	Purpose
Get-SPOSiteRestrictedAppAccessControl	Return a site's enablement, mode, and both lists
Set-SPOSiteRestrictedAppAccessControlMode	Set the active mode to `Allow` or `Deny`
Set-SPOSiteRestrictedAppAccessControlList	Add or remove applications on a site list
Enable-SPOSiteRestrictedAppAccessControl	Turn on enforcement for the site
Disable-SPOSiteRestrictedAppAccessControl	Turn off enforcement, preserving mode and lists
Clear-SPOSiteRestrictedAppAccessControlList	Empty one list
Clear-SPOSiteRestrictedAppAccessControlPolicy	Remove the site policy entirely

Application Restrictions is managed only through these dedicated cmdlets. `Get-SPOTenant` and `Get-SPOSite` don't return the policy, and `Set-SPOTenant` and `Set-SPOSite` can't change it.

Limits

Expand table

Limit	Value
Applications on the tenant deny list	100
Entries per site list	100

Limit	Value
Combined entries per site	200

Related articles

Restrict SharePoint site access with Microsoft 365 groups and Microsoft Entra security groups

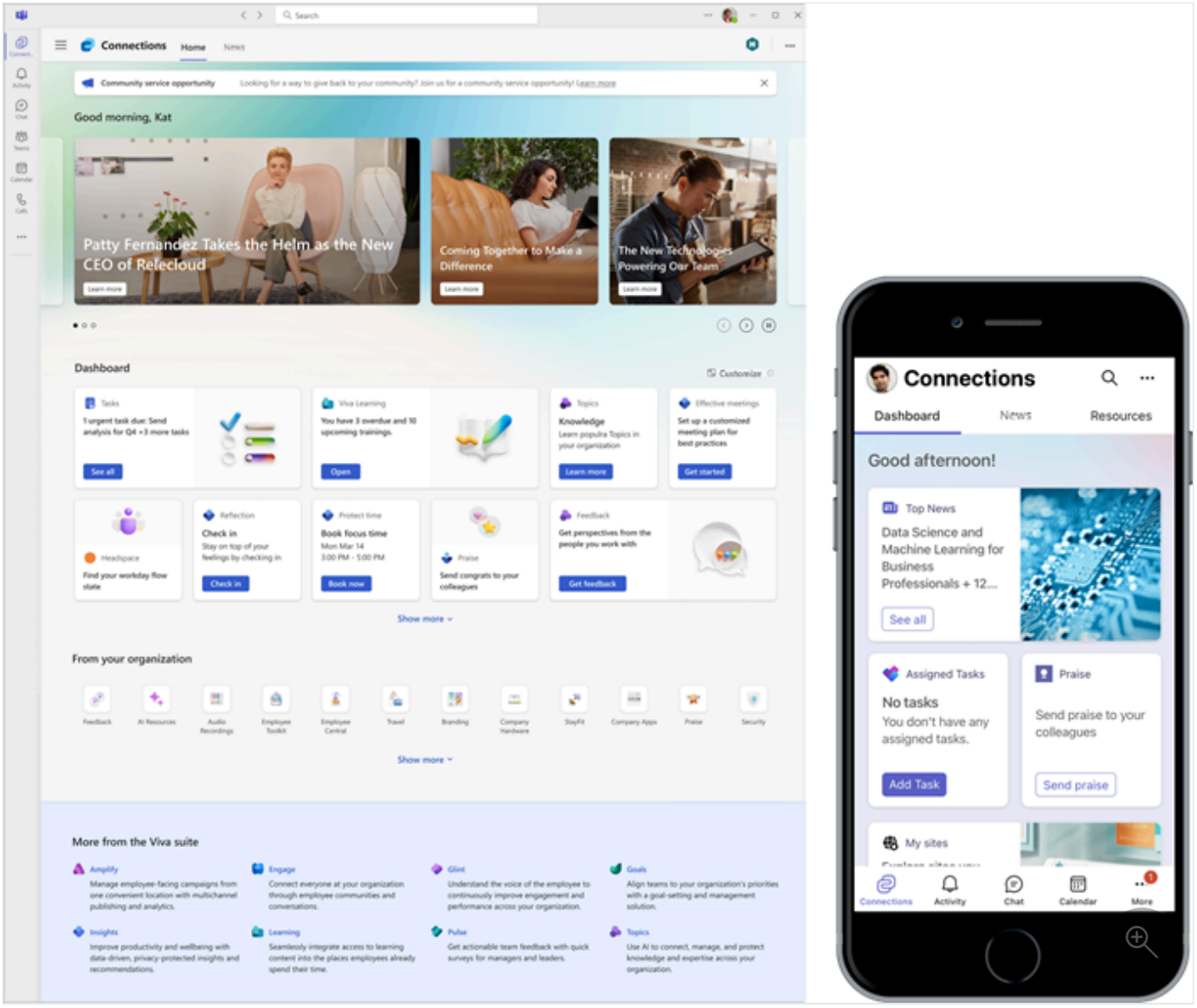
Conditional access policy for SharePoint sites and OneDrive

Get started with SharePoint Online Management Shell

Last updated on 10/13/2026

Overview of the SharePoint app in Teams

The SharePoint app in Teams, formerly Viva Connections, brings full SharePoint capabilities into Microsoft Teams. It is built on the SharePoint home site technology. A SharePoint home site provides a customized landing experience that reflects the organization's brand, voice, and priorities. A SharePoint home site also serves as the gateway to other portals in your organization's intranet. The SharePoint app in Teams is customizable and can be accessed through Microsoft Teams or the web from your desktop, mobile, or table device.



Use the quick guide to set up SharePoint in Teams or get more detailed guidance on how to plan, build, and launch.

The SharePoint app in Teams is:

- A user experience app in Microsoft Teams that allows organizations to create unique experiences for different audiences like information workers, frontline workers, educators, researchers, or students.
- A gateway to curate specific content and tools by providing easy access to resources, apps, services, relevant news, announcements, and popular destinations.
- Built on trusted technology: SharePoint, Teams, and Microsoft Entra.
- Easily accessed through the desktop, tablet, or mobile versions of the Microsoft Teams app, or through your company's SharePoint home site on the Web.
- Learn more about Microsoft Viva and Viva licensing.

Primary components of the SharePoint app in Teams

The SharePoint app in Teams is composed of four primary components - News, dashboard, announcements, and resources.

Expand table

Component	Description
News	The News reader provides users with SharePoint news from across the organizational sites, boosted news, user's followed sites, frequent sites, and people the user works with. Users can easily Like interesting news and Save content for later. Users with a Microsoft 365 Copilot license can access a Copilot powered news summary from the desktop version of Microsoft Teams. For more information on News, see the article on the news in the ShaerPoint app in Teams
Dashboard	The dashboard is your user's digital toolset that brings together the resources your users need whether they are in the office or in the field. The dashboard uses dynamic (adaptive) cards that users can interact with to do things like clock in for a shift, access training materials, review paystub information, or book a shuttle. It can also be used as a web part on SharePoint home sites. For more information on customizing the dashboard, see the article on creating and editing a dashboard.
Resources	The Resources web part enables way finding across popular destinations. Organizations can curate a list of useful links that appear to users such as health benefits, important forms, and department websites.
Announcements	The Announcements web part display short messages for important communications in your Home site, typically at the top of the page. Announcements are created first and then displayed using this web part. This web part is available only in SharePoint home sites.

Since the SharePoint app in Teams is based on the SharePoint platform, you can fully leverage SharePoint navigation, search, pages, web parts, lists, and libraries to design and configure your overall experience.

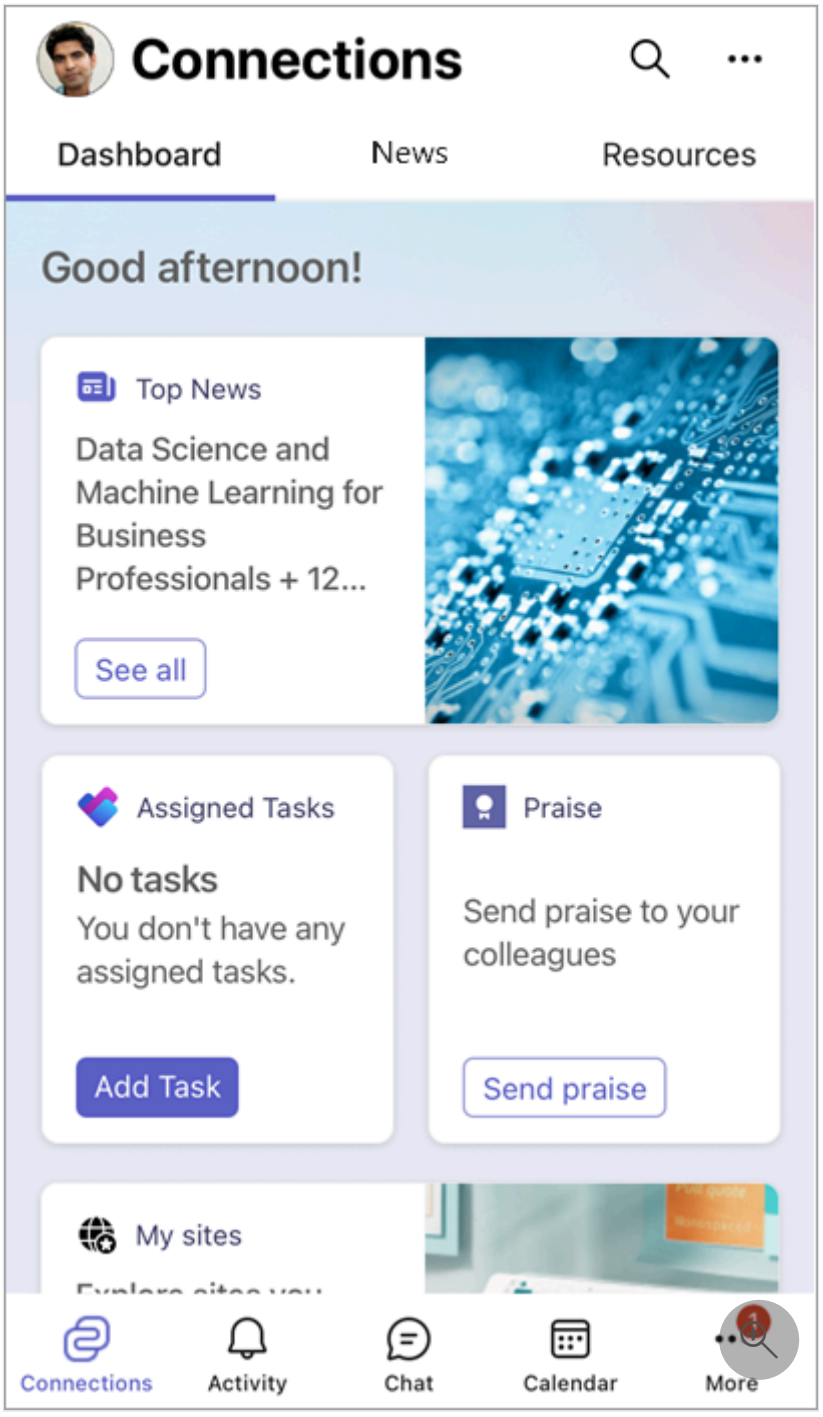
Mobile and desktop experiences

The desktop and mobile experiences are centered around the three main components of the dashboard, News, and resources. Users accessing the SharePoint app from Teams desktop app, SharePoint home page, or the Viva Suite home website features all three components at-a-glance.

Accessing the SharePoint app in Teams from a tablet or mobile device features a more compact experience for the three components and uses tabs to make it easier to scroll through content.

The SharePoint app in Teams mobile experience

The experience in the SharePoint app in Teams mobile is responsive and brings in the content in its full fidelity.



For more detailed information, see the article on SharePoint app in Teams on mobile devices.

Additional capabilities:

- **Accessible from the web:** Users can access the your company's SharePoint home site, without needing the Microsoft Teams app.
- **Access specific tools and information based on roles**: Throughout the SharePoint app in Teams, content can be targeted to specific audiences to ensure they have the right tools and information at the right time.
- **Easily share content**: Content consumed within Teams can be easily shared into chats or channels, making collaboration easier.

Branding

Matching your organizational brand is integral to your users' relationship with your company's values and goals. The branding you apply – including your logo and colors – is automatically applied across the various end user experiences on Web, desktop and mobile. For information on how to apply your branding in an app, review how to customize apps in Microsoft Teams. The desktop app offers an opportunity for further branding by customizing the banner image and customizing the theme.

> **Note**
>
> - Organization branding in the SharePoint app for Teams is currently disabled for users on mobile and desktop who have enabled dark mode under their Microsoft Teams Appearance and Accessibility settings.
> - Custom fonts are not currently supported on mobile.

Localization

The SharePoint app in Teams is available in most major languages used in Microsoft 365. Learn more about how to set up the SharePoint app in Teams mobile experience in a specific language and how to create a dashboard in more than one language.

- **Dashboard:** Content can be set by dashboard authors to support multiple languages.
- **News:** The content is available in the format in which it was authored, and SharePoint news posts display author-translated posts in the user's preferred language.
- **Resources:** Content follows the site's default language.

Extensibility

Many components to the SharePoint app in Teams experience can be customized. The SharePoint Framework (SPFx) is the recommended SharePoint customization and extensibility model for developers because of the native integration between SharePoint and Microsoft Teams. SPFx is the only extensibility and customization option for the SharePoint app in Teams. Learn more about SharePoint app in Teams extensibility.

The SharePoint app in Teams allows for multiple home sites across multiple experiences

Depending on the size of your organization and the information to communicate, you might decide to create a separate experience for each audience you wish to target. Organizations are able to set multiple home sites, creating a targeted experience that is content specific for that group of users (for example, a dashboard and resources with a frontline worker focus or for different geographic locations).

> **Note**
>
> Users with a Microsoft 365 subscription (E, F, or A license) are limited to creating and using one SharePoint app in Teams experience. If you want to create or use two or more experiences (up to 50), then every user in your tenant must have a Microsoft Viva Suite or Viva Communications and Communities license. See Microsoft Viva plans and pricing for more info.

Resources to prepare for the SharePoint app in Teams

There are several options to learn more about how to get and use the SharePoint app in Teams for your organization.

Expand table

Option	Description	Time to complete
Quick guide	Use the quick guide to get a high-level overview of how to get the SharePoint app in Teams.	10 minutes
Plan, build, and launch guidance	Get more detailed guidance that focus on tasks in the plan, build, and launch phases.	30 minutes
Learning path	Get in-depth guidance that includes fictitious business stories and examples. Complete knowledge checks to confirm learnings.	Two hours

Privacy, Security, and Compliance in the SharePoint app in Teams

Privacy, security, and compliance are essential aspects of your organization. The SharePoint app in Teams takes advantage of Microsoft 365 tools and services, which are governed under the Microsoft Product Terms and the Data Protection Agreement (DPA). For more information, see the Microsoft Trust Center and the article on Microsoft Viva Compliance.

Learn more about how the SharePoint app in Teams inherits privacy features and settings from Microsoft 365, Teams, SharePoint, and Viva Engage (where applicable). Owners and members setting up a SharePoint app in Teams experience should confirm who has access to certain sites within SharePoint to ensure only authorized users have access to certain data and features. For more information, see the article on understanding how security works in Microsoft Viva.

More resources

Learn how to plan, build, and launch a home site

SharePoint app for Teams adoption resources

SharePoint app for Teams guidance for end users

Last updated on 09/20/2026

What's new for SharePoint home sites

This article highlights SharePoint home site updates rolling out starting May 2026 and details the specific changes due to the rename of Viva Connections to SharePoint app.

> **Note**
>
> SharePoint home site technology fully powers the Connections experience in Teams, now branded as the **SharePoint app in Teams.** Targeted Release rollout of all these updates is planned for early May 2026 with GA by end of June 2026. You can track progress on the related Microsoft 365 public roadmap: ID 557983.

A SharePoint home site provides a customized landing experience that reflects the organization's brand, voice, and priorities. A SharePoint home site also serves as the gateway to other portals in your organization's intranet. It's simply a special communication site in your organization. You can either create a new home site or set an existing communication site as your home site. An admin can do this action in the SharePoint admin center.

Viva Connections is a customizable employee engagement experience app in Teams. It is how your SharePoint intranet can be deployed within Teams desktop and mobile. With the rename of Viva Connections to SharePoint app in Teams, this functionality becomes a prominent feature of a SharePoint home site.

With this update, you can:

- Create or set a Home site in SharePoint admin center.
- Configure your home site with web parts and deploy it to your organization, just like any portal launch.
- In the home site, under **Settings**, set up the SharePoint app for Teams.

SharePoint home site updates - May-June 2026

What's not changing

- Existing home sites, site content, branding, and overall look and feel stay the same.
- Existing Viva Connections configurations, including customized app names and logos, keep working as configured.

- Existing Viva Connections deployments stay available as a branded employee experience within SharePoint.
- Organizations that require multiple home sites still need the appropriate licensing.

What's new

- SharePoint administrators can now create and designate home sites directly from the SharePoint admin center.
- A new Resources web part is available for curated links and employee resources.
- A new Announcements web part is available. We have also removed the extra Viva license requirement for using Announcements feature.
- New filmstrip layout options are available for the News web part.
- A simplified experience for configuring SharePoint app in Teams is now available directly from the home site experience.

What's changing in the user experience

- The Teams desktop and mobile branding change from the default Viva Connections to SharePoint for noncustomized experiences.
- The default app experience aligns with SharePoint branding and removes Viva-specific default content, including the "Go to Connections" UX in the default app experience. Users can get back to the default experience by double clicking the app logo in Teams left navigation and clicking on the app name in the panel.
- The global navigation experience within the SharePoint app in Teams desktop displays either SharePoint or your organization's customized app name.
- The Dashboard web part "See all" experience now supports end-user personalization and customization.

Create and designate home sites directly from the SharePoint admin center

You can now create and establish a communication site as a SharePoint home site directly within your organization's SharePoint admin center. Previously, you needed to go to the Viva Connections management console within Microsoft 365 admin center. Use the following step-by-step instructions to help set up your SharePoint home site. You must be assigned the role of SharePoint admin to accomplish these steps.

Once established, you can configure and manage your site content like any other SharePoint site - choosing your preferred theme, layouts, pages, navigation, and more.

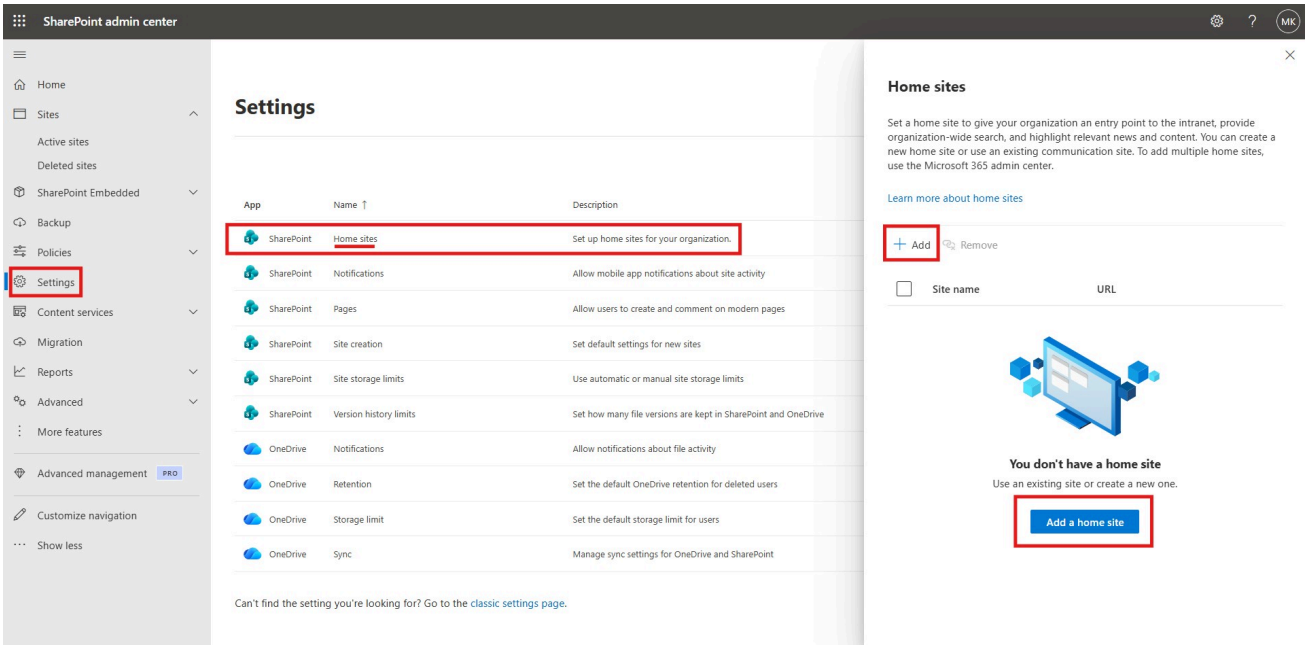
To create a SharePoint home site, follow these steps:

1. Go to your SharePoint admin center and sign in. (The URL resembles `https://tenantname-admin.sharepoint.com/`.)

2. In the navigation pane, select **Settings**.

3. Under **SharePoint apps**, select **Home sites** to open a configuration panel called **Home sites**.

4. Select either + **Add** or **Add a home site**.



5. Select the type of home site you want to add. To create a new site, go to *step 6*. To use an existing communication site, go to *step 7*.

6. To create a new site to use as your home site:

   a. Select **Create a new site**, and then select **Next**.

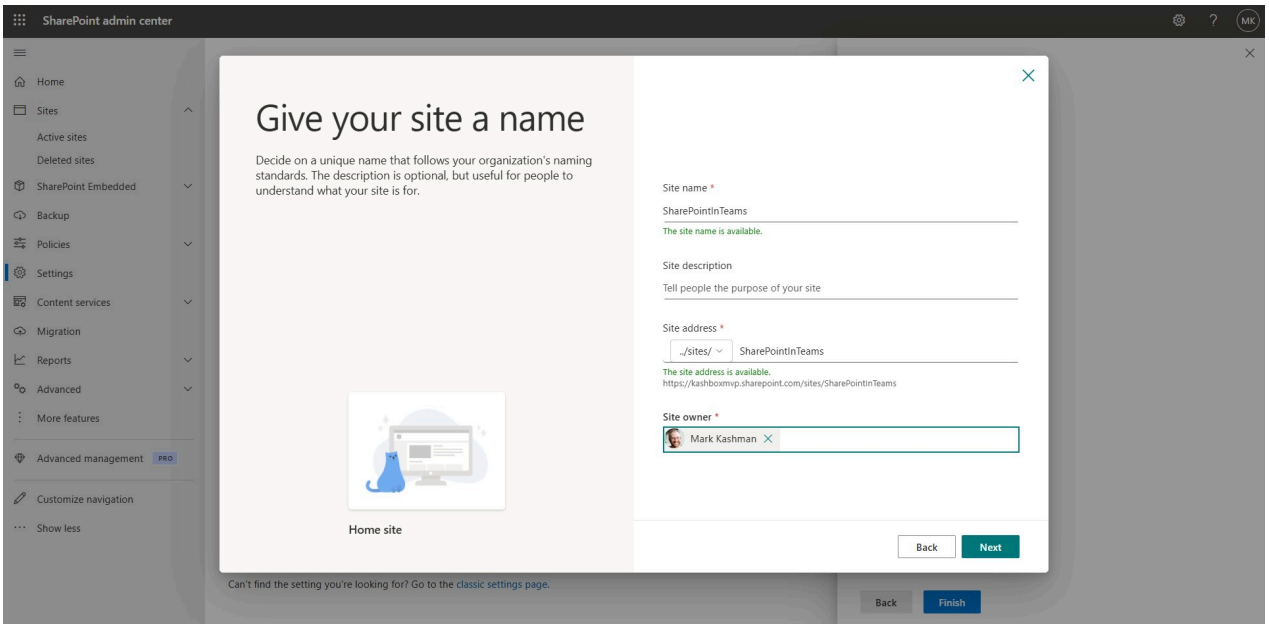
   b. On the **Preview and use 'Home site' template** page, select **Use template**.

   c. Give your site a unique name in the text box under **Site name**.

   d. Validate your site name and URL, add a site owner, and then select **Next**.

   e. Set your language and time zone, and then select **Create site**.

   The site gets created as a home site, with Site name and URL.



7. To use an existing communication site:

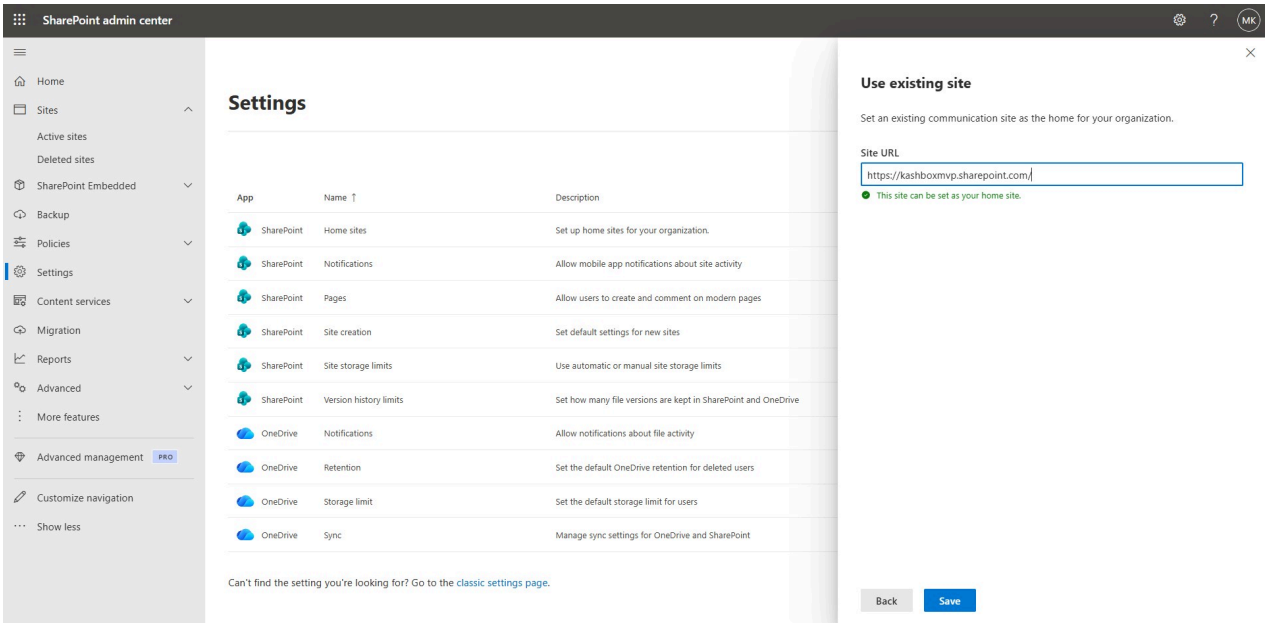
   a. Select **Use an existing communication site**, and then select **Next**.

   b. Specify the site URL of the existing communication site you want to set as your home site.

   c. Validate that this site can be set as your home site. Green text indicates that the site meets the criteria.

   d. Select **Save**.

   The specified site is assigned as a home site, with its site name and URL.



Note

To add multiple home sites, you must still go to Viva Connections in the Microsoft 365 admin center.

Last updated on 09/28/2026

Overview of how to plan, build, and launch the SharePoint app in Teams

The SharePoint app in Teams helps engage and empower different user groups like frontline workers and information workers across your organization. It helps keep them updated on news, announcements, and provides access to important resources from a desktop, mobile, or tablet device. Once established, end users can access these resources and information from within Microsoft Teams desktop, mobile, and web.

> **Note**
>
> - You must have an Enterprise (E), Frontline (F), or Academic (A) license type to create a SharePoint app in Teams experience.
> - Users with a Microsoft 365 subscription (E, F, or A license) are limited to creating and using one experience. If you want to create or use two or more experiences (up to 50), then every user in your tenant must have a Microsoft Viva Suite or Viva Communications and Communities license. See Microsoft Viva plans and pricing for plan information and a comparison table.
> - There are no requirements to get started with the SharePoint app in Teams.
> - You must have SharePoint admin permissions to access the SharePoint admin center where you create and establish a communication site as a SharePoint home site.

Once you establish the SharePoint app in Teams, you work within the designated SharePoint site(s) to add and adjust content, assign permissions, designate targeted audiences, order the view priority of your experiences, and more.

- Use this guide to prepare your organization for the SharePoint app in Teams through the planning, building, and launching phases.
- Review the different roles and activities in each phase. This will help determine if you need moer than one instance of the SharePoint app in Teams and the use of audience targeting throughout.
- Discover planning considerations and best practices.
- Get guidance for change management, adoption, and end-user training.

Step-by-step guidance to provision the SharePoint app in Teams

There are two options that provide in-depth information about how to get the SharePoint app in Teams for your organization.

Expand table

Option	Description
Quick guide	Get basic instructions on how to set up the SharePoint app in Teams.
Planning guidance	Get planning guidance that leads to successful build out and launch phases.

Overview of activities in each phase

Expand table

Phase	Steps and tasks
Plan	**Step 1: Plan for the SharePoint app in Teams** Identify and align on key tasks and scenarios. **Step 2: Plan the dashboard** Learn more about the different kinds of cards and how they can support specific scenarios. **Step 3: Get ready for news publishing** Consider audience targeting to show news content to specific groups of people aggregated from various sites. **Step 4: Plan Resources** Determine which links belong in the resources web part. **Step 5: Create an adoption plan** Create a plan to help the rest of the organization adopt the ShaerPoint app in Teams. Learn more about SharePoint app in Teams adoption. **Step 6: Consider success metrics** Think about how your organization determines if the SharePoint app in Teams is meeting your specific needs. **Step 7: Plan for maintenance over time** Consider which content and components might need to be refreshed over time.
Build	**Step 1: Create and designate home sites directly from the SharePoint admin center** Choose to create a single experience for the whole organization, or multiple experiences that

Phase	Steps and tasks
	service distinct audiences. **Step 2: Configure the SharePoint app in Teams** Design the overall experince across Microsoft Teams desktop and mobile from within the SharePoint admin center. **Step 3: Pin the SharePoint app in Teams to the left side portion of Microsoft Teams** After the creation of your first experience, pin the app in the Teams admin center to make the SharePoint app in Teams easily discoverable. Navigate to your Teams admin center > **Teams apps** > **Setup policies**. Select **Global**. Scroll down to **Pinned apps**. Select **Add apps to add the SharePoint app in Teams**. If your users have an F license, the SharePoint app in Teams is pinned by default. **Step 4: Ensure high-traffic sites and portals are healthy** Run a health check and make sure everyone has access to the right content. **Step 5: Test and refine the experience** Find people in your organization who can test the experience before being released more broadly.
Launch	**Step 1: Consider tactics to spread the news** Think about where different audiences usually get news. Consider email campaign, outreach through SharePoint news and Teams posts, out to broader company Viva Engage communities, and specific training or All Hands meetings. **Step 2: Announce the SharePoint app in Teams** Use more than one communication channel to reach audiences. **Step 3: Use champions and provide continued support** Continue to use early adopters to help others get the most out of the SharePoint app in Teams and route feedback. Encourage organization leaders and stakeholders to notify others about the launch and progress each week, month, or quarter.

Overview of roles in each phase

Expand table

Phase	Roles
Plan	Work with **your organization's stakeholders** and business partners (from groups like HR, operations, facilities, communications specialists, and technology advocates) to identify the most valuable content and tasks that can be completed in the SharePoint app in Teams. **Key administrative stakeholders typically include:** - **Business owners**, who lead efforts in different departments like sales, operations, design, engineering, etc. - **HR professionals**, who manage team members and oversee company and organizational structure and efficiency.

Phase	Roles
	- **Internal communication specialists**, who facilitate and manage communications between users and various internal teams. - **Communications coordinators and specialists**, who execute and maintain company-wide communications and brand management. - **Administrative assistants**, who complete and oversee various administrative tasks. The more people that are informed, the more they will share progress and encourage others to participate.
Build	- The **SharePoint admin center admin** will set up the initial experience, add audiences, designate owners who can edit and customize each SharePoint app in Teams experience, and pins the app in Teams (if needed). - **Site owners and authors for the SharePoint home site** design the site content, global navigation, and the dashboard. - Other **site owners and authors** can be involved to update content or news posts that are relevant to the overall experience.
Launch	- Collaborate with **champions** (early adopters) to help other people at the organization implement the SharePoint app in Teams. - Use **executive sponsors** who can help evangelize the app at large company meetings and in broad communications. - **Business owners and managers** at all levels can help teams and individuals find value and adopt new ways of working. Be open to feedback from all levels. It will be successful if everyone feels the SharePoint app in Teams was designed for them and maintained for them as business needs and culture change over time.

Next, plan the SharePoint app in Teams for your organization

After reviewing the phases, tasks, and roles, you're ready to begin planning the ShaerPoint app in Teams for your organization.

Last updated on 09/20/2026

Plan for the SharePoint app in Teams

In the planning phase, build a team of stakeholders to align the goals and primary use cases for your organization's user experience strategy, then start by planning for each component of the SharePoint app in Teams experience. Consider success metrics and adoption tactics to ensure it meets the needs of your organization and users.

> **Note**
>
> - You must have an Enterprise (E), Frontline (F), or Academic (A) license type to create a the SharePoint in Teams experience.
> - Users with a Microsoft 365 subscription (E, F, or A license) are limited to creating and using one experience. If you want to create or use two or more experiences (up to 50), then every user in your tenant must have a Microsoft Viva Suite or Viva Communications and Communities license. See Microsoft Viva plans and pricing for more info.
> - You must have SharePoint admin permissions to access the SharePoint admin center. SharePoint in Teams is available on mobile and tablet devices in GCC, GCC High, and DoD environments with limited features. For more information, see the list of service availability.

Step 1: Plan for the SharePoint app in Teams

The SharePoint app in Teams is designed to help users complete high-priority tasks and easily access important information. It is built on the SharePoint home site technology. This experience can be built over time as your organization adapts and scales. Organizations can use an existing SharePoint home site or create a new site and establish it as a home site for the SharePoint app in Teams.

The SharePoint app in Teams is composed of four main components:

- **Dashboard**: The dashboard is your user's digital toolset. It brings together the tools your users need, enabling quick and easy access whether they are in the office or in the field.
- **News**: You can program News to flow in from organizational sites, boosted news, user's followed sites, frequent sites, and people users work with in an immersive reader

experience.

- **Resources**: Resources provide links to the most popular destinations at your organization. Create your own links and choose to target specific audiences.
- **Announcements**: Use the Announcements web part to display short messages for important communications in your Home site. This web part is available only in SharePoint home sites.

These components can be featured across Web, desktop, and mobile, but display differently based on screen resolution.

Step 2: Establish a SharePoint home site either using an existing communication site or create a new one

A SharePoint home site acts as the front door to your organization's intranet and a gateway to other popular portals that are relevant to the entire organization. A SharePoint home site is a SharePoint communication site that acts as a front door to your organization's intranet. Once a SharePoint home site is set, the news posted from that site is prioritized across the intranet. A SharePoint home site can be set in the SharePoint admin Center when creating a new experience, or assigned to an existing SharePoint home site. Having a SharePoint home site also allows you to take advantage of the SharePoint app bar.

Set up global navigation in the SharePoint app bar (optional)

Once you have a SharePoint home site, you can set up the SharePoint app bar to improve navigation to intranet resources through global navigation, and personalized content like sites, news, files, and lists. Links from the Global Navigation bar can also be imported into the Resources web part.

For more information, see the introduction to the SharePoint app bar.

Review, prioritize, and modernize content to align with key scenarios and tasks (optional)

After defining the key scenarios and tasks in the planning phase, ensure priority content is located on modern SharePoint communication sites and team sites. Both modern and classic sites can be used, but only modern sites appear in the Microsoft Teams app. Classic sites open in a separate browser window.

If you have many SharePoint sites, make sure you focus on sites, pages, and content that are relevant to your employee base. Sites and content that are unrelated to key tasks and scenarios can be modernized later.

Sites that should be reviewed and prioritized:

- Sites that dashboard cards link to.
- Sites that are displayed in global navigation.
- Sites that frequently publish organizational news.
- Sites that help users complete the most important day-to-day tasks or access important information.

Resources to help you modernize:

- Use the SharePoint modernization scanner to create a dashboard that helps you determine modernization readiness.
- Learn more about how to transform classic sites to modern sites, or consider creating new modern sites using SharePoint site templates.
- See the article on healthy portal guidance for high-traffic sites for more guidance on how best practices and recommendations for popular sites that are expected to get a high amount of traffic.

Step 3: Plan the dashboard

Start by identifying the key scenarios that the SharePoint app in Teams needs to support and identify owners of those user experiences. Common scenarios include view paystubs and vacation hours, submit help tickets, catch up on news, check daily lunch menus, find people in a directory, and shift management. For more information, see the full list available dashboard cards. If your organization has a specific need that calls for a custom card, consider using the card designer to build your own.

These scenarios can be targeted to specific audiences using Microsoft 365 Groups. Consider which groups of users need access to specific resources.

Expand table

General	For information workers	For frontline workers
- View pay and benefits - Submit a ticket to the help desk - Access lunch and café options - Catch up on news and announcements	- Find people and team information - Complete required training - View company holidays	- View and manage shifts - Access time sheets and popular forms - View workplace policies and resources

Collaborate and align with business groups that manage these experiences to determine the best design.

Planning process

As you work with business owners and key stakeholders to align your overall design strategy, answer the following questions for each task:

- Who is the audience?
- What do users need to accomplish or learn?
- What tools or technology do they use today?
- What tools or technology do you want visitors to use to accomplish their key tasks?
- What information needs to be promoted?

Design with your audience in mind

As a best practice, it's important to make decisions that are rooted in specific tasks for certain audiences:

- Consider using a common framework for scenario planning that starts by selecting a certain role or audience "In my role as a...".
- Then, narrow down the objective in "I need to...".
- Next, consider the ideal tool or process to meet the objective in "So that I...".
- Lastly, script out what success looks like in "I know this is successful when...".

For example, create a table like the following to list business scenarios that you want to address with cards in the dashboard:

Expand table

In my role as...	I need to...	So that...	I know this is successful when...
Full time user	Easy access to benefit and payroll information	I can quickly check important information without needing help from HR	Requests for help with benefits and payroll to the HR team are reduced
Frontline worker	Clock in and out from a mobile device	I can create efficiencies in my workflow	Schedules and breaks are managed from the SharePoint app in Teams
People manager	Welcome and onboard new team members	I can grow and develop talent	I spend less time managing standard onboarding functions
Sales representative	Access specific product training materials while on a mobile device	Can quickly resolve customer issues	Most customer issues get resolved in real-time
HR specialist	Promote the use of the self-service benefits	I can spend more time working with users on unique benefits questions and scenarios	All of my user interactions are about individual critical scenarios

Keep in mind that not every task should be turned into a card on the Dashboard. Focus on tasks that are the most impactful to your users that can be executed within a short amount of time.

Step 4: Get ready for News

News presents SharePoint news from organizational sites, boosted news, user's followed sites, frequent sites, and people users work with in an immersive reader experience. This gives content publishers a reliable method of distributing important news and information, while keeping frontline workers, information workers, and hybrid workers alike engaged and informed on important news and announcements. And it is all based on what permissions a user has to vew various news and their main source site.

Audience targeting can be used to show news content to specific groups of people if you want to present information that is relevant only to a particular group of people. For example, you can target news stories about a specific project to only team members and stakeholders of the project. For more information, see the article on audience targeting.

Users can access their news from the News tab.

Step 5: Plan the resources

Resources are the navigational links to portals and other popular destinations. Resources should be the most important and popular portals for your target audience and can be targeted to specific audiences. If you configured the SharePoint app bar, you can also provide users with links to resources. The global navigation bar can only be accessed outside SharePoint by users through the SharePoint app in Teams by selecting the organizations logo on the Teams app rail.

For more information, see the article on editing resources. For more information on SharePoint navigation, see the introduction to SharePoint information architecture.

Step 6: Create an adoption plan

Planning for change and helping users adopt new resources are different for every organization. Use the considerations and best practices here as a starting point to creating an adoption plan that fits your organization's needs. Include considerations for change management and training materials for end-users in your plan.

Adoption considerations

- Users can access the SharePoint app in Teams from Microsoft Teams and SharePoint on desktop or mobile devices.
- Use early adopters and champions to extend their enthusiasm to the rest of the organization.
- Plan to engage with users where they typically meet and share information (for example, if your organization already meets in Teams, plan to post in channels.)
- Determine where questions about the SharePoint app in Teams should go, and who should answer them. Consider using a Viva Engage community, a SharePoint site with guidance and Frequently Asked Question (FAQs), or a specific, monitoed Teams channels to allow users to ask questions or see commonly asked questions.

Change management considerations

- Start by creating awareness and interest in multiple channels to appeal to different audiences. Consider common spaces for on-site users like the break room or conference rooms. For remote workers and the rest of the organization, plan to post announcements in Teams, Viva Engage, and SharePoint.

- Make sure different audiences of end-users can easily understand how this new tool helps improve their day-to-day work.
- Create opportunities for users to ask questions, get help, and see live demonstrations. Consider setting up weekly training sessions or office hours during the first month of adoption. Use champions where possible.
- Reinforce change by creating incentives for using the new tools.
- Clearly explain how to use the SharePoint app in Teams on desktop and mobile devices, how to engage with the Dashboard, where to find announcements and resources, and where to view the latest news and announcements.
- Create specialized guidance for different audiences like frontline workers or hybrid workers.

Training considerations

- Use training to help raise awareness about how to use the SharePoint app in Teams on desktop and mobile devices.
- Showcase different ways to connect and engage with cards on the dashboard.
- Consider providing different training guidance for different audiences.
- Highlight popular links that can be found in the Resources web part when on a mobile device.

Step 7: Consider success metrics

Part of the planning process includes determining which metrics will be used to measure how effective the SharePoint app in Teams is in bringing your organization together and keeping specific audiences informed.

- **Use the analytics feature within the SharePoint app in Teams:** Use analytics to understand how and when users engage with various components, the content types users engage with, and the platforms used to access.
- **High-level view of usage across M365 apps:** Use Microsoft 365 usage analytics to access a prebuilt dashboard that contains several prebuilt reports that focus on adoption of Microsoft 365 apps, usage, communication, and collaboration.

- **Site or page level data:** Get site level and page level usage reports in SharePoint to gauge engagement and learn more about when users access content and what devices they're using.
- **Get direct feedback from users:** Usage analytics aside, you can ask users directly about their overall satisfaction. Consider creating a card on the Dashboard that links to a Microsoft Form where you can ask users to rate satisfaction and provide feedback.

Step 8: Plan for maintenance over time

As your business grows and evolves, you'll likely identify new scenarios that can be supported by the SharePoint app in Teams. Over time, you might decide to retire cards on the dashboard or rearrange global navigation in resources.

Additionally, users will share feedback that can be used to improve the experience. Each of these scenarios requires time to implement and to communicate as needed. Plan to have a point-person, or team of people, who can manage these tasks over time, update the dashboard, adjust resources, and more.

Next, build and customize the SharePoint app in Teams for your organization

After you meet requirements, have a plan for the dashboard, and are prepared to help users adopt the SharePoint app in Teams experience, it's time to move on to the build phase.

Last updated on 09/20/2026

Build and test your design for the SharePoint app in Teams

After deciding which tasks, audiences, and resources to promote using the SharePoint app in Teams in the planning phase, you're ready to move onto the building phase.

You know you're ready to move onto the building phase if you've met the following requirements and reviewed best practices:

- The most valuable tasks and processes can be completed using the SharePoint app in Teams.
- Considerations have been made for specific audiences.
- You have started an adoption and launch plan along with success metrics.

Start by creating your SharePoint app in Teams experience. You can create a new SharePoint communication site and enable it as a SharePoint home site. Or, you can leverage an existing communication site and enable it as a SharePoint home site.

Learn more how to convert a SharePoint communication site into a SharePoint home site.

Step 1: Configure your SharePoint app in Teams experience

Once you enabled a SharePoint communication site as your SharePoint home site, you can adjust all content, design, and permissions with its site settings - within the home site itself.

You can:

- Assign permissions
- Decide which Microsoft 365 groups to associate with the new experience
- Add and adjust the home page and its web parts
- Set the order of experiences (if more than one is created)
- Enable the experience.

For more information, learn how to configure the SharePoint app in Teams for use across dekstop and mobile.

Step 2: Customize the SharePoint app in Teams dashboard

The dashboard brings it all together; providing a personalized landing experience for users and is designed to be the central destination where everyone can discover your organization's resources and complete daily tasks. Users with site owner and site member permissions are able to customize the dashboard, apply audience targeting to role-specific cards, preview, and publish the dashboard.

Learn more about the SharePoint Dashboard web part.

Step 3: Ensure high-traffic content provides an ideal viewing experience

For a smooth launch, you want to make sure information can be easily accessed and that high-traffic sites and pages are high-performing.

1. Test the performance of the home site to ensure an optimal viewing experience.
2. Share the SharePoint home site with the entire organization before launching. Make sure that the target audiences for the cards in the SharePoint app in Teams dashboard are shared with the right audiences.
3. Consider using the Portal launch scheduler to monitor performance for high-traffic sites that are being shared for the first time.

Step 4: Test and refine the SharePoint app in Teams

Before sharing the SharePoint app in Teams with the rest of your organization, recruit a small group of users to test and refine popular workflows to ensure end-users have a great experience using the SharePoint app in Teams for the first time. Consider recruiting specific people from different audiences to complete popular tasks.

If your organization has a Viva suite or Viva Communications and Communities license, use analytics data for that SharePoint app in Teams experience to review data on overall traffic, usage, and engagement. Make improvements until the experience is ideal for the rest of the organization.

Best practices for testing:

- Test SharePoint app in Teams through SharePoint on the web - viewing the SharePoint home site native within a modern browser.
- Depending what devices your organization prefers, test SharePoint app in Teams on desktop, mobile, and tablet devices.
- Make sure all links are active and there aren't any dead ends.
- Pay attention to labels on dashboard cards and buttons – do they make sense to the rest of the organization?
- Evaluate the quality and effectiveness of icons and images.
- Check for performance issues like slow loading times or missing images.
- Ask testers about the navigation experience.
- Test with early adopters and champions and capture their feedback.

Next, launch SharePoint app in Teams for your organization

After you have finished planning, building, and testing the SharePoint app in Teams, it's time to let the rest of the organization know that it's available for use. Learn more about how to launch the SharePoint app in Teams.

Last updated on 09/20/2026

Launch the SharePoint app in Teams for your organization

After your organization has finished the planning, building, and testing the SharePoint app in Teams, it's time to let the rest of the organization know that it's available for use.

Step 1: Consider tactics to spread the news

Consider where and how different audiences get news and announcements. For example, frontline workers might get the most important news in team meetings and hybrid workers might be used to getting SharePoint news in Outlook.

- **Announce your organization's instance of the SharePoint app in Teams at an event:** Kick off the announcement about the availability of the SharePoint app in Teams at an all-hands or Town Hall meeting where everyone in the organization attends or can view a recording later.
- **Use communication tools like SharePoint news and Viva Engage communities:** Share details about the SharePoint app in Teams launch along with any change management guidance or end-user training in an organizational news post, Viva Engage communities, and Microsoft Teams channels.
- **Consider hosting training events or offering office hours:** Make sure end-users get the most from the SharePoint app in Teams by offering ongoing support the first 30 days after launching.

Step 2: Announce the SharePoint app in Teams

One final task is announcing the SharePoint app in Teams. Communications should be engaging and interactive where possible. Ensure end users can quickly understand how this new tool improves their jobs and makes getting news and access to important resources easier than before. Emphasize that the SharePoint app in Teams is a customized and personalized experience that is accessed in Microsoft Teams or through SharePoint on the web.

Best practices for launching the SharePoint app in Teams

- Plan to engage with users where they already meet and share information (for example, if your organization already meets in Teams, plan to post in appropriate channels.)

- Reach most of your target audience by using multiple communication methods and channels.
- Continue to engage early adopters and champions and use their enthusiasm and expertise to engage the rest of the organization during meetings or training sessions.
- Regularly revisit success metrics over the first 90 days to track progress and learn more about how audiences engage with the SharePoint app in Teams. Learn more about analytics for the SharePoint app in Teams.
- Ask end users for feedback and provide multiple ways to connect so that the experience can be improved over time.

Step 3: Use champions and provide continued support

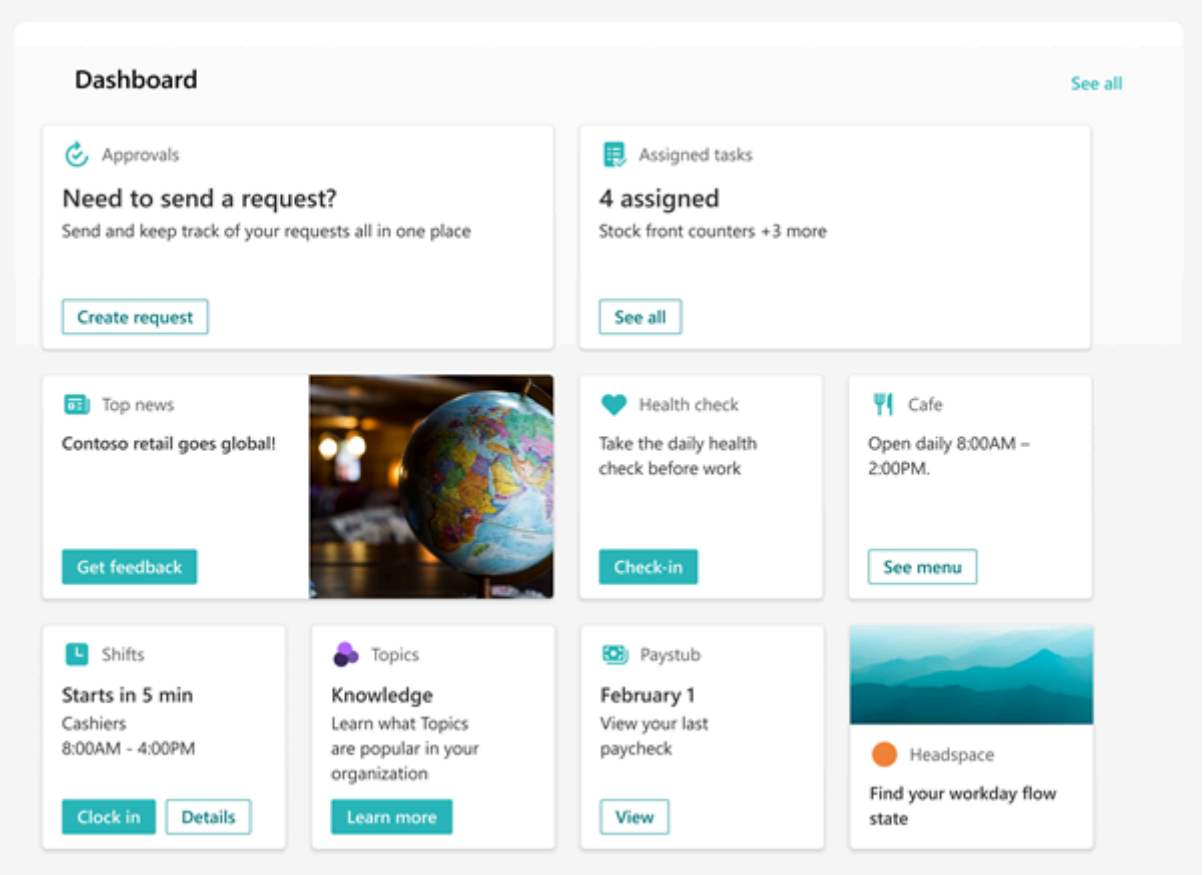
Champions are critical to the success of adoption. They're power-users with a desire to help others along the way. Often, they're closest to the business outcomes your organization is trying to realize. And become one yourself by learning in our worldwide community. Use champions to help others adopt the SharePoint app in Teams by providing ongoing support in training events and other learning opportunities.

See the example of using a champion program for Microsoft Teams for some ideas when creating a champion program for the SharePoint app in Teams.

Last updated on 10/09/2026

Edit the SharePoint app in Teams dashboard

The SharePoint app in Teams dashboard web part provides fast and easy access to information and job-related tasks. Content on the dashboard can be customized and then targeted to users in specific roles, markets, and job functions. It consists of cards that engage viewers with existing Microsoft Teams apps, partner apps, custom solutions using the SharePoint Framework (SPFx), internal links, and external links. You edit the dashboard directly from within the SharePoint app in Teams user interface.



> **Note**
>
> - You're asked to select your primary audience to generate a set of default dashboard cards for when setting up your experience for the first time.
> - Operators or members should limit the number of dashboard cards to about 20 for the best viewing experience.
> - Operator or member permissions are required to edit the SharePoint app in Teams dashboard.
> - Users are able to customize their dashboard in the SharePoint app in Teams on desktop and mobile by reordering, hiding, and showing cards. These changes only

affect the experience for the user.

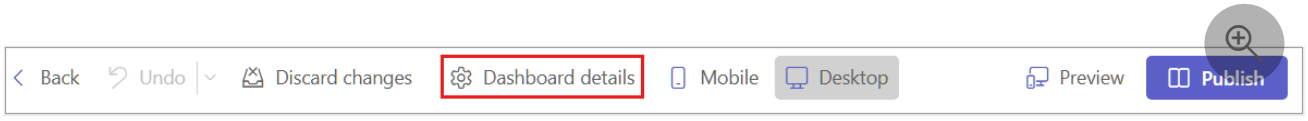
1. From within your SharePoint app in Teams experience, select **Edit** in the dashboard section.
2. Select + **Add a card**.
3. Select **Edit** (pencil icon) for each card to edit properties like the label, icon, image, and audience targeting settings where applicable.
4. Select **Delete** (trash can icon) to remove cards.
5. Preview the experience on all devices to ensure usability before publishing or republishing.
6. **Publish** or **Republish** when you're done to share the edits with others.

Change the dashboard settings

The dashboard details contain settings for your dashboard, page versioning, and controls for the Editor and enabling user customization on their personal dashboard view.

> **Note**
>
> Some settings are only available to the SharePoint app in Teams owner.

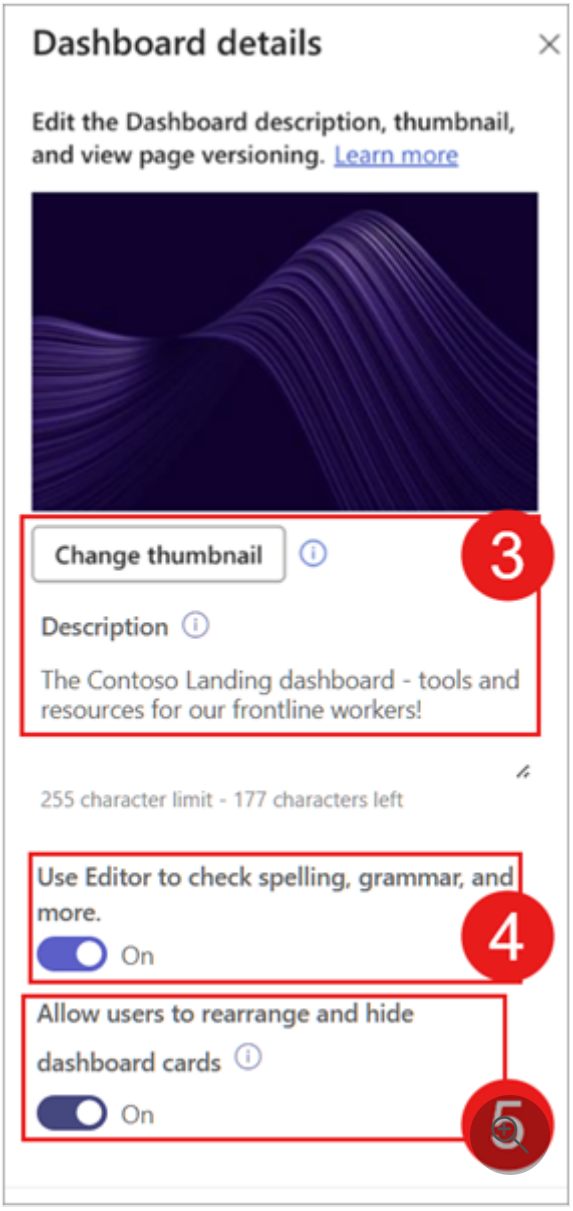
1. From the SharePoint app in Teams, select **Edit**.
2. Select **Dashboard details** above the dashboard.



3. In the Dashboard details pane, you can add a thumbnail and description to show in search results:
   - **Change Thumbnail**: Select to add an image to be shown in search results.
   - **Description**: Enter a description in the text field to be shown in search results.
4. The **Editor** can be toggled off or on. When enabled, the editor checks spelling and grammar (Enabled by default).
5. **Allow users to rearrange and hide dashboard cards** can be enabled or disabled (Enabled by default):

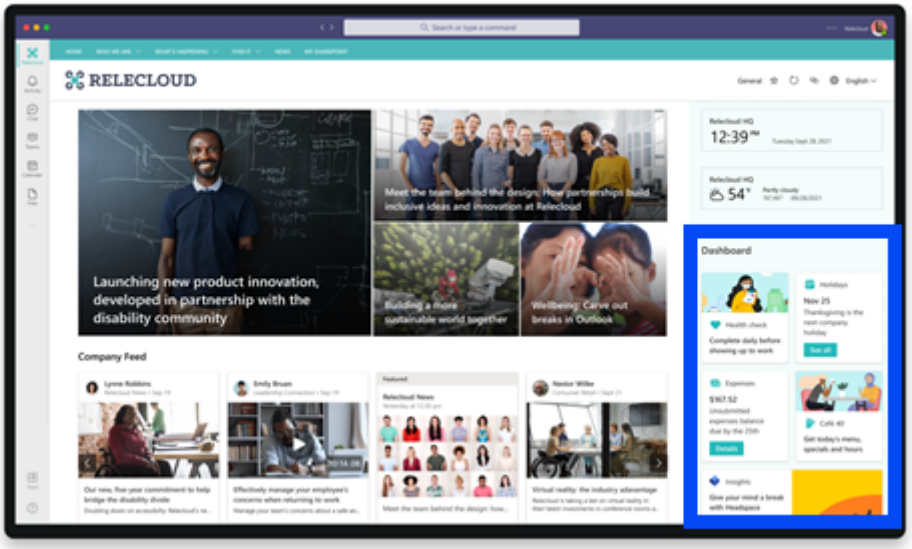
- If enabled, users see the **Customize** button on their dashboard, which enables them to show or hide unused dashboard cards, reorder their dashboard card view, and add their own cards.
- Changes users make to their dashboard are only seen by that user. Any updates or changes to the dashboard by an owner or member of the experience will override the user's personal changes.

> **Note**
>
> Disabling user customization resets all user dashboard views to what the organization created. This includes removing any dashboard cards the user added to their dashboard.



6. When finished making your changes, select the **X** to close the Dashboard details pane.

> **Note**
>
> - After editing content on the dashboard, it might take several minutes until the new content is available in the Dashboard web part.
> - Dashboard cards are refreshed when users manually select Refresh in the SharePoint app in Teams or restart Teams app or navigate away from and back to the SharePoint app in Teams. If Teams remains open and idle in the background, dashboard content may not automatically update until one of these actions occurs.
> - For best results, we recommend placing the Dashboard web part in a right vertical section.
>
> - > Images are an important aspect to making your cards rich and inviting. If you're a SharePoint admin, we recommend enabling a Content Delivery Network (CDN) to improve performance for getting images. Consider when storing images that /siteassets is by default a CDN source when Private CDN is enabled while /style library is the default source when the Public CDN is enabled. Learn more about CDNs.



You can set the maximum number of cards you want to display.

Customize your dashboard with cards and audience targeting

Further customize your dashboard by adding various cards meant to help specific users perform specific tasks. Audience targeting and unique dashboard cards can show specific content for specific groups within your organization.

For a list of available dashboard cards, along with a description of the tool and steps for setting up, refer to the article on Available dashboard cards for the SharePoint app in Teams.

For more information on audience targeting and aspects of your SharePoint app in Teams experience it can be applied to, see the article on applying audience targeting to dashboard cards.

How URLs and single sign-on works

For some cards, you'll use links to URLs. Depending on the location of the content, links to URLs might display content in Microsoft Teams or elsewhere and Single sign-on (SSO) behavior can differ. Get more information about how links to URLs and SSO behave depending on the location of the content you're linking to.

> **Note**
>
> When SSO isn't supported, users are asked to enter their sign-in credentials.

Expand table

Opens URL to...	On Teams mobile	On Teams desktop
Teams App	Teams apps (like Shifts, Approvals, or Kudos) open within Teams and user doesn't need to authenticate again.	Teams apps (like Shifts, Approvals, or Kudos) open within Teams and user doesn't need to authenticate again.
Forms	Forms open within Teams, user is asked to sign-in on the first time, and user doesn't need to authenticate again if they stay signed in.	Forms open within Teams, user is asked to sign-in on the first time, and user doesn't need to authenticate again if they stay signed in.
Viva Engage	Viva Engage opens within Teams, user is asked to sign-in on the first time and user doesn't need to authenticate again if they stay signed in.	Opens a web browser session and the user might need to reauthenticate depending on browser and machine settings.

Opens URL to...	On Teams mobile	On Teams desktop
Power Apps	Power Apps opens within Teams, user is asked to sign-in on the first time and user doesn't need to authenticate again if they stay signed in.	Opens a web browser session and the user might need to reauthenticate depending on browser and machine settings.
Power Portals	Power portals open within Teams, user is asked to sign-in on the first time and user doesn't need to authenticate again if they stay signed in.	Opens a web browser session and the user might need to reauthenticate depending on browser and machine settings.
Stream	Stream opens within Teams, user is asked to sign-in on the first time and user doesn't need to authenticate again if they stay signed in.	Opens a web browser session and the user might need to reauthenticate depending on browser and machine settings.
External Links	Web view opens within Teams and the user might need to authenticate again (depending on the site.)	Opens a web browser session and the user might need to reauthenticate depending on browser and machine settings.

Related resources

Learn more about how to plan a dashboard

Design your own dashboard card with the card designer

Available dashboard cards for the SharePoint app in Teams

Last updated on 09/20/2026

Available dashboard cards for the SharePoint app in Teams

The SharePoint app in Teams dashboard uses dynamic cards that can be targeted to specific users to help them perform tasks like clock in for a shift, access training materials or links to department resources, look up contact information, manage assigned tasks, and more. If your organization has a specific task in mind, you can also use the card designer to quickly build "custom" cards using a template, without the need for custom code. A number of the dashboard cards can be configure to use audience targeting. Learn more how to use audience targeting in the SharePoint app in Teams.

> **Note**
>
> You need member or owner level permissions to access the card designer from the dashboard card toolbox.

Available dashboard cards

Select a dashboard icon for more information.

Expand table

Toolbox icon	Description
Card designer	Create your own cards or use quick views for a more interactive experience utilizing the adaptive cards framework.
Approvals	Use Approvals to approve vacation requests, documents, and expense reports.

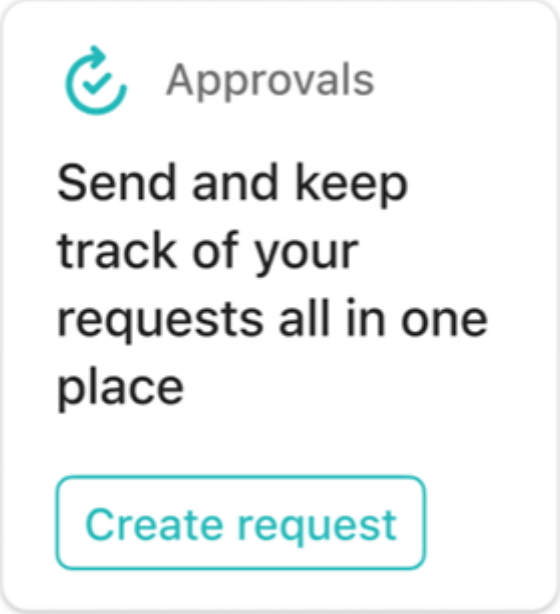
Toolbox icon	Description
Assigned Tasks	Use Tasks to manage your team's work, assign tasks, and track tasks.
Assignments	Display a summary of upcoming and past due assignments for students.
Courses	Display a summary of courses a student is enrolled in.
Events	View and join upcoming events within your organization.
Folder	Provide easy access for users to an existing SharePoint document library in your SharePoint app in Teams experience.
My sites	Provide users links to frequently accessed SharePoint sites.
News	Promote news from various sources that you wish to prominently display, including boosted news from SharePoint.
OneDrive	View and access recent, shared, and favorite files from your OneDrive account.

Toolbox icon	Description
People	Provide an option to look up contact information and directly chat, email, or call with others in your organization.
Power Apps	Design a lightweight card using your power apps account for simple tasks like checking sales requests, vacation requests, and more.
Quick links	Provide list of relevant links or files to users selected by admins.
Shifts	Display information about the next or current shift from the Shifts app in Teams.
Stay Engaged	Users can access their Viva Engage feed conversations from within the SharePoint app in Teams.
Stream playlist	Display a list of videos to users that can be viewed in Microsoft Stream.
Teams app	Use to open a Teams personal app or bot specified by the dashboard author.
Varies	Use cards that integrate partner services.
Viva Learning	Provide a link to the Viva Learning app that can be targeted to show to certain audiences.

Toolbox icon	Description
Viva Pulse	Provide a short status of a recently sent pulse with a link to the Viva Pulse app for users to learn more.
Web link	Access a site without leaving the SharePoint app in Teams.

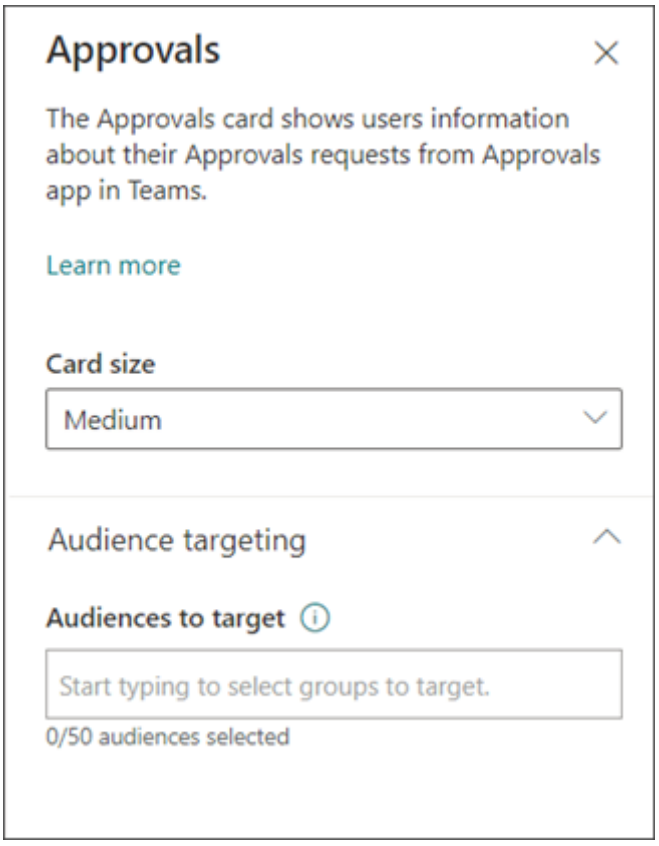
Add the Approvals card

The Approvals card connects to Approvals in Microsoft Teams and is a way to streamline all of your requests and processes with your team or partners. You can create new approvals, view the ones sent your way, and see all of your previous approvals in one place.



1. While in edit mode, select + **Add a card** from the dashboard.
2. Select **Approvals** from the dashboard toolbox.

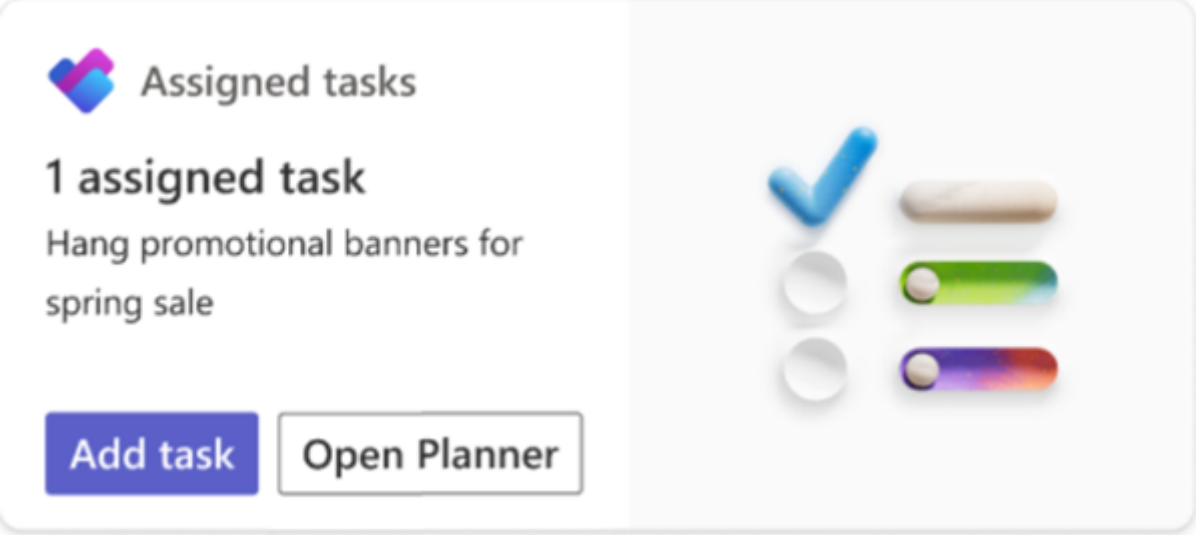
3. Select the pencil icon to **Edit** the card. In the property pane that opens on the right side of the screen, choose your card size from the **Card size** drop-down list.



4. Once you're satisfied with how the dashboard looks in preview, select **Publish** or **Republish** at the top-right of your dashboard to make it available for use for your SharePoint app in Teams across web, mobile, and desktop.

Add the Assigned tasks card

The Assigned tasks card allows users to create and view tasks from the card or open the Planner app from the card. Task information is retrieved from the Planner app in Teams.



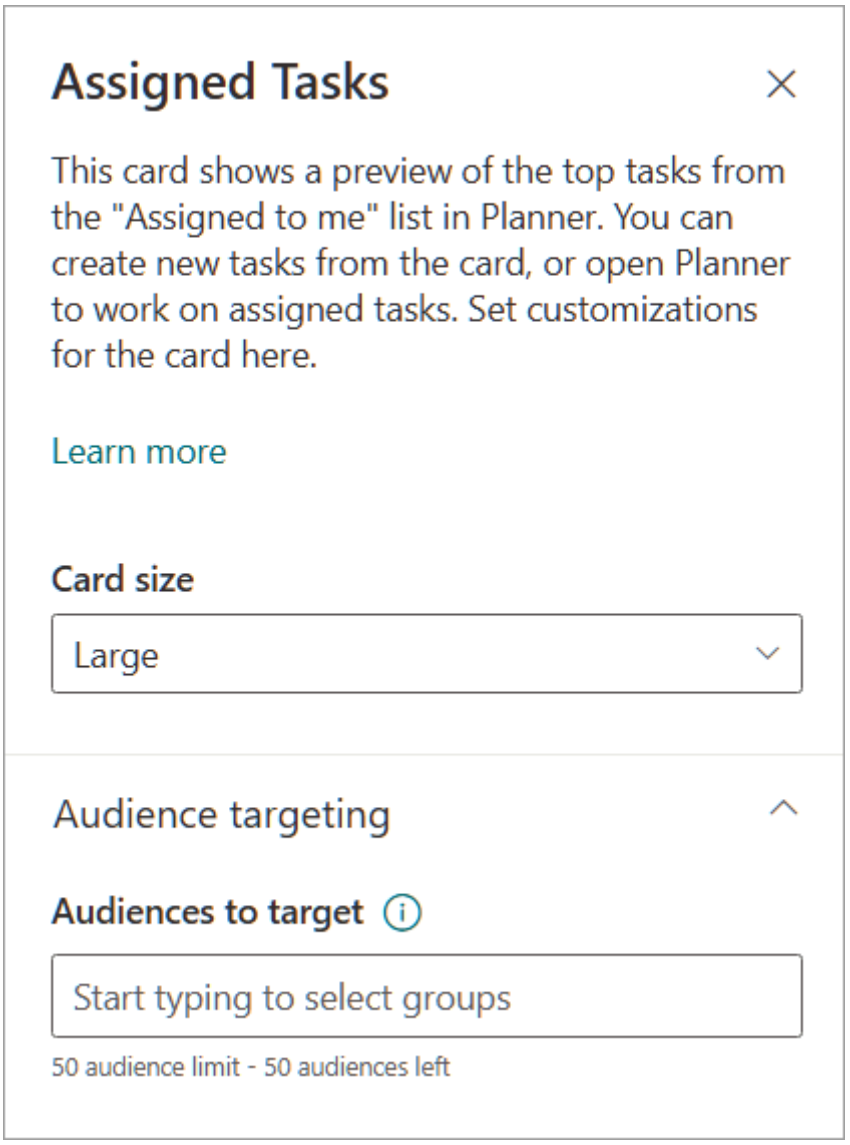
1. While in edit mode, select + **Add a card** from the dashboard.

2. Select **Assigned Tasks** from the dashboard toolbox.

3. In the property pane on the right, choose your card size from the **Card size** drop-down list.

4. To target your card to specific audiences (that is, the card only displays in the dashboard to the audience you specify), **enable audience targeting**.

> ⓘ **Note**
>
> The size of the card affects how many buttons are available on the card. The **Add tasks** and **Open Planner** buttons appear on large cards (default size), while on medium sized cards only the **Add tasks** button is shown.

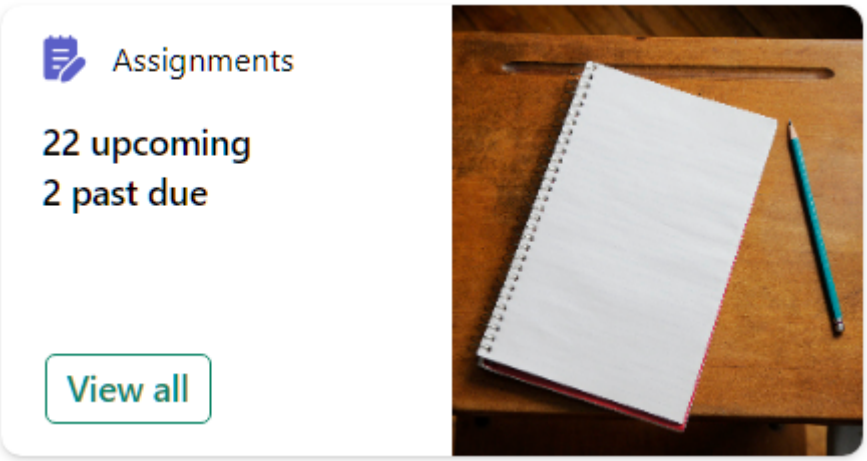


For more information on using the Planner app, see the articles on how to Manage the Planner app for your organization in Microsoft Teams and Getting started with Planner in Teams.

Add the Assignments card

The Assignments card displays a summary of upcoming and past due assignments. Students can select the card to view more details on their assignment list and open them in Microsoft Teams.

> **Note**
>
> The Assignments card is only available to Education tenants.



1. While in edit mode, select + **Add a card** from the dashboard.

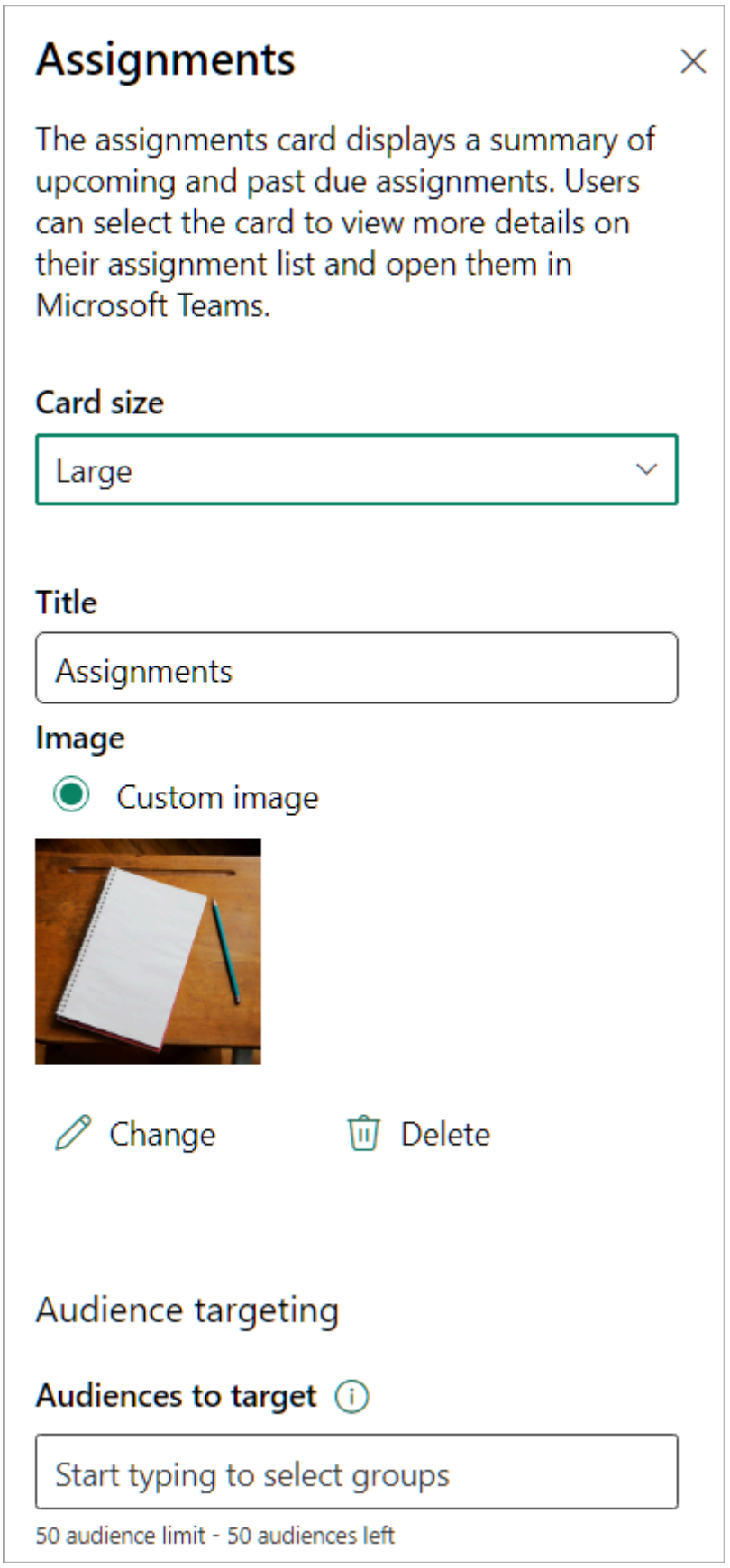
2. Select **Assignments** from the dashboard toolbox.

3. In the property pane on the right, choose your card size from the **Card size** drop-down list.

4. Enter a **Title** for the assignments card.

5. To change the card image, select **Change**, then select an image or upload your own.

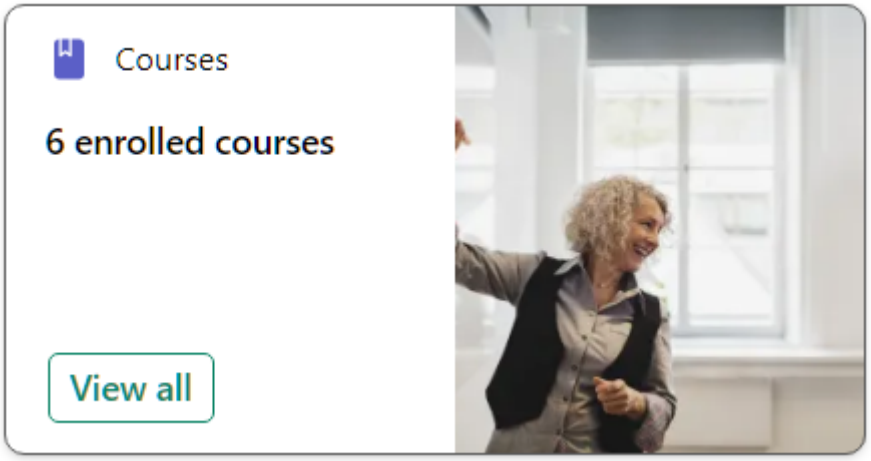
6. To target your card to specific audiences (that is, the card only displays in the dashboard to the audience you specify), **enable audience targeting**.



Add the Courses card

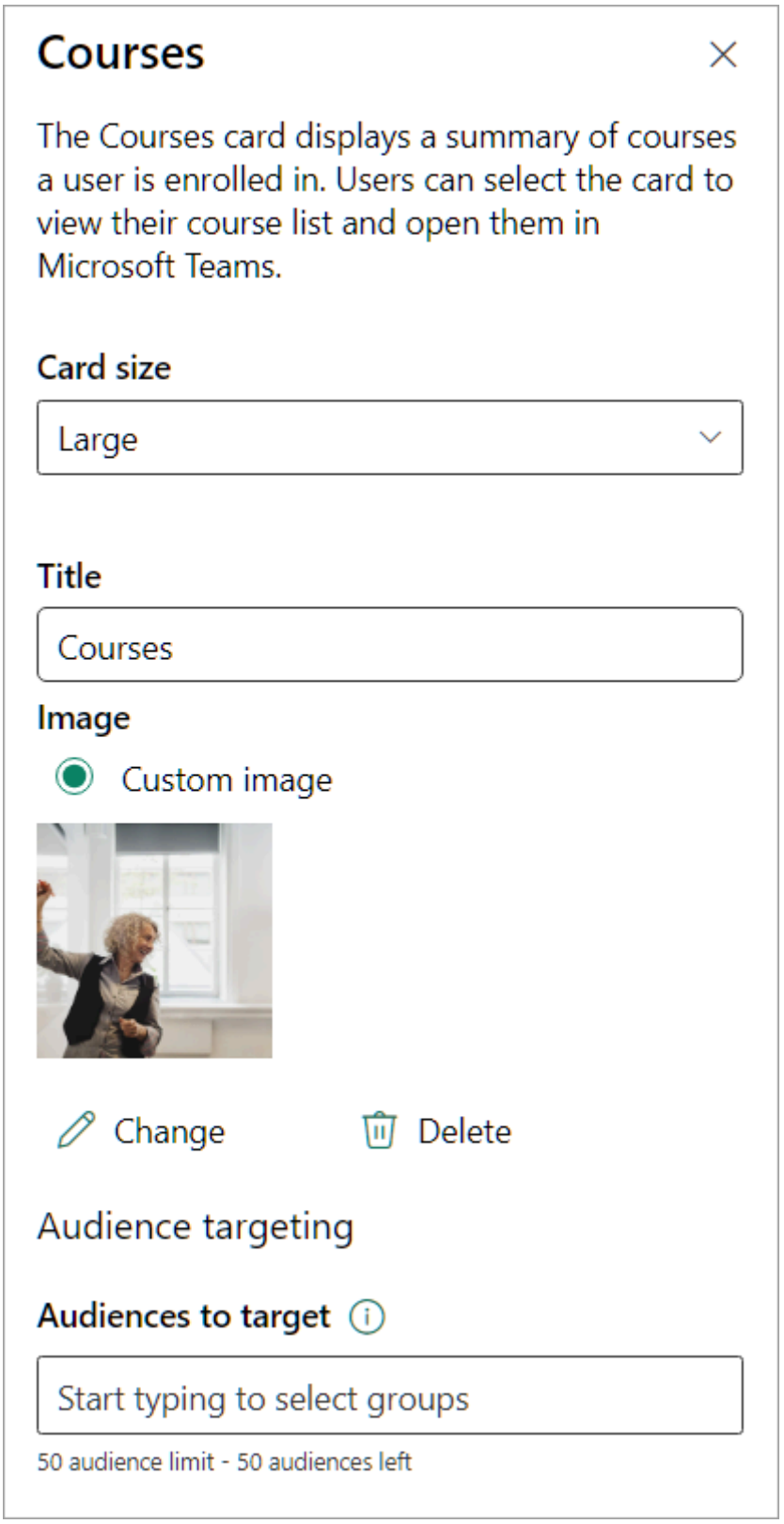
The Courses card displays a summary of courses a student is enrolled in. Students can select the card to view their course list and open them in Microsoft Teams.

> **Note**
>
> The Courses card is only available to Education tenants.



1. While in edit mode, select **+ Add a card** from the dashboard.
2. Select **Courses** from the dashboard toolbox.

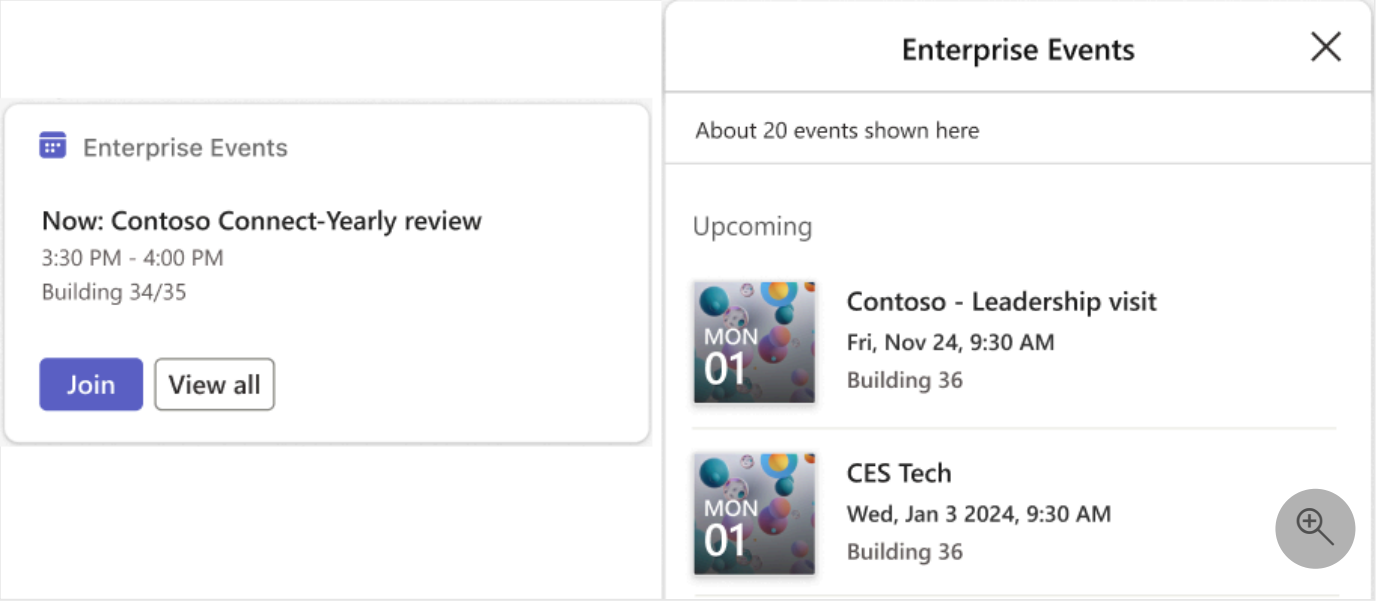
3. In the property pane on the right, choose your card size from the **Card size** drop-down list.
4. Enter a **Title** for the assignments card.
5. To change the card image, select **Change**, then select an image or upload your own.
6. To target your card to specific audiences (that is, the card only displays in the dashboard to the audience you specify), **enable audience targeting**.



Add the Events card

The events card can help your users stay informed and engaged with upcoming events in their organization, such as webinars, trainings, town halls, and celebrations. Users can view more upcoming events or join via teams via the links on the Events card. The card can be customized and even targeted to specific audiences so only relevant events are displayed.

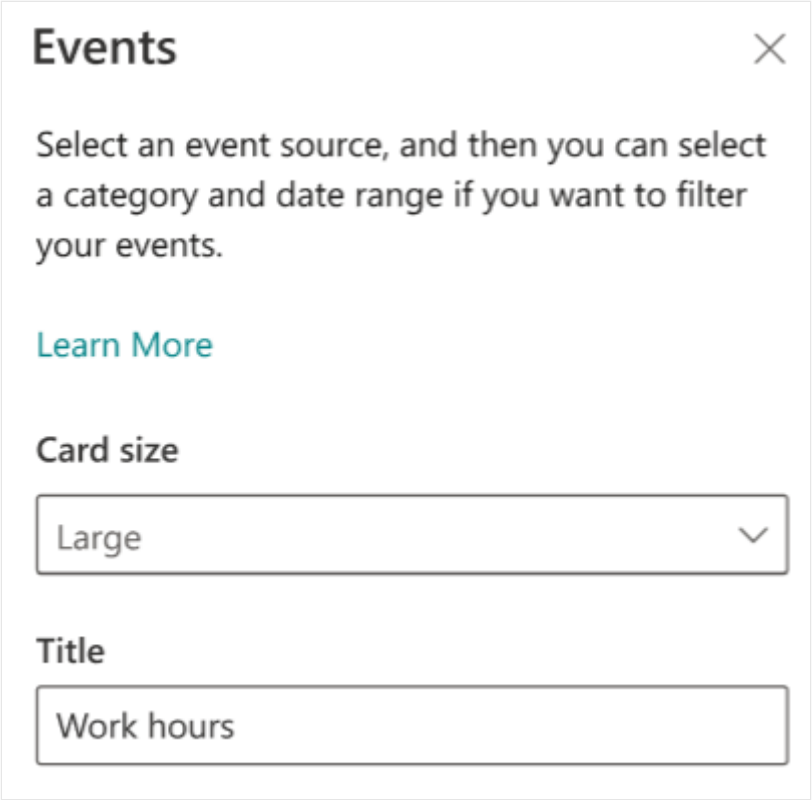
The Events card is tied to the SharePoint Events web part. Site owners and members need to access their SharePoint site and use the SharePoint Events web part to add events to their site. For more information, see the article on using the Events web part.



> **Note**
>
> Recurring events aren't supported, even if you manually set up a recurrence in the events list that you're using. You need to create a new event for each occurrence.

1. While in edit mode, select **+ Add a card** from the dashboard.
2. Select **Events** from the dashboard toolbox.

3. Select the **edit pencil** to the left of the card to open the properties pane for the Event card.
4. In the property pane on the right, choose your card size from the **Card size** drop-down list.
5. Enter a **Title** for the event card.



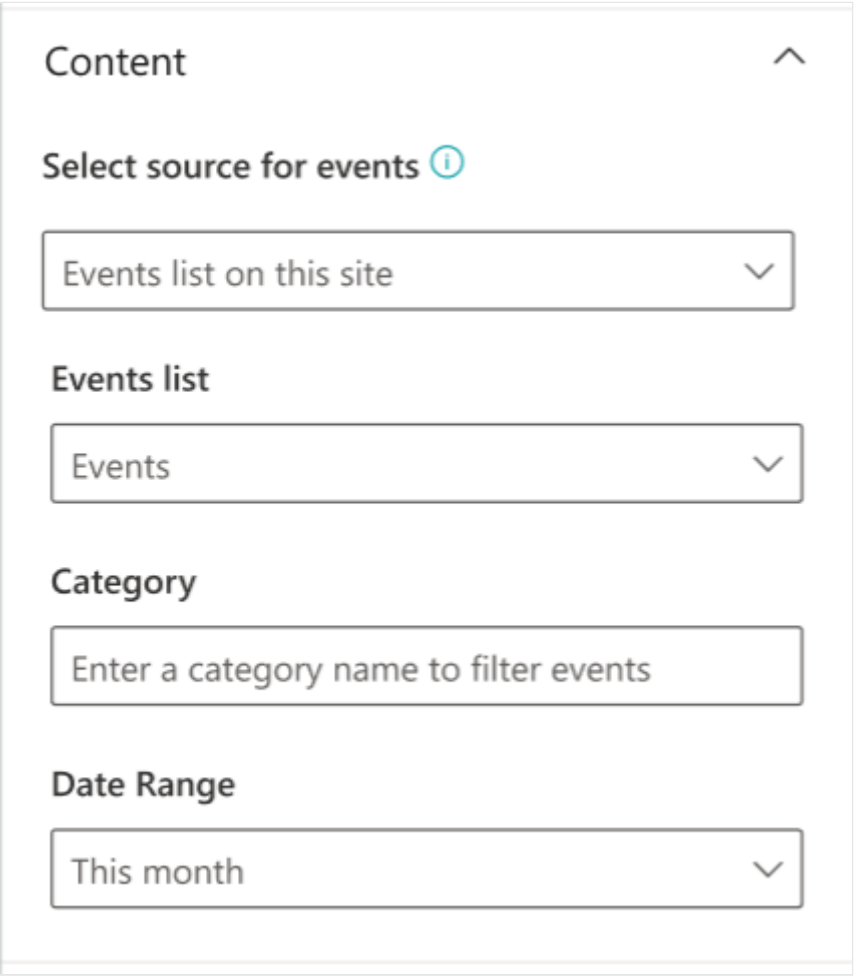
6. Under Content, select a **Source** for your events: **Events list on this site**, **This site**, **This site collection**, **Select sites**, or **All sites**. If your site is connected to a hub site, you'll also able to select **All sites in the hub** or **Select sites from the hub**.

> **Note**
>
> - When you choose **Select sites**, you can search for the site you want to add, or select one or more sites from **Frequent sites**, or **Recent sites**. You can select up to 30 sites.
> - The **Select sites** option isn't available in SharePoint Server, U.S. Government GCC High and DoD, and Office 365 operated by 21Vianet.
> - If there's more than one **events list** on the site, you can select the one you want. If you don't have an existing list, the **Events** card creates an empty Events list for you, with the default settings of a Calendar list.
> - If you choose to show events from multiple sites, and don't see all of your events displayed on the page, see How events from multiple sites are found and displayed.

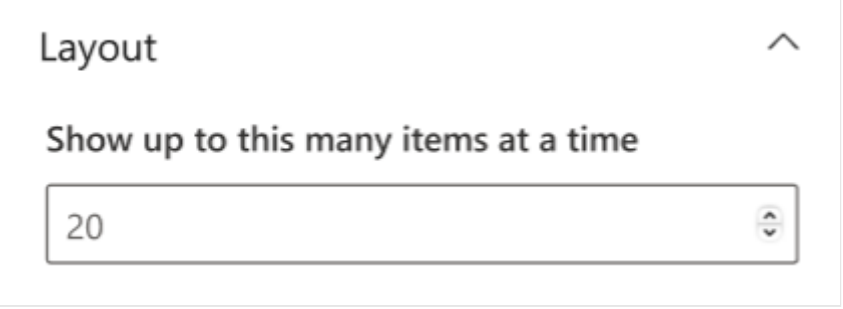
7. If your list has **categories**, you can select one by which to filter the events you show.

8. Select a date range by which to filter your events in the **Date range** drop-down list. You can choose **All upcoming events** (the default), **This week**, **Next two weeks**, **This month**, or **This**

quarter.



9. Under the layout section, select how many events to be shown at once from the dropdown. Up to 30 events can be shown on one event card.



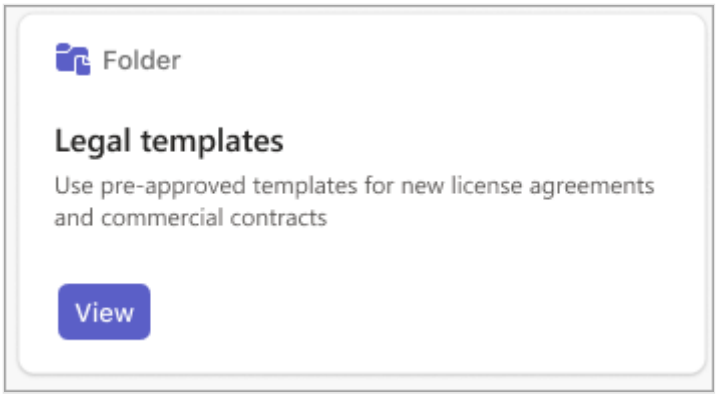
10. To target your card to specific audiences (that is, the card only displays in the dashboard to the audience you specify), **enable audience targeting**.

11. When finished with your selection, you can close the panel. Your settings will autosave.

Add the Folder card

Provide easy access for users to an existing SharePoint document library in your SharePoint app in Teams experience by using the Folder card. For more information, see the article on document

libraries .



1. While in edit mode, select + **Add a card** from the dashboard.

2. Select **Folder** from the dashboard toolbox.

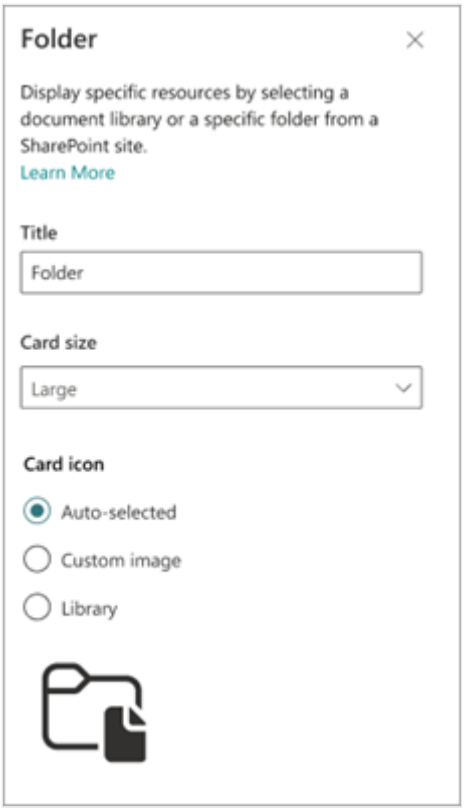
3. Select the **edit pencil** to the left of the card to open the properties pane for the Folder card.

4. In the property pane on the right, enter a **Title** for the Folder card.

5. Choose your card size from the **Card size** drop-down list.

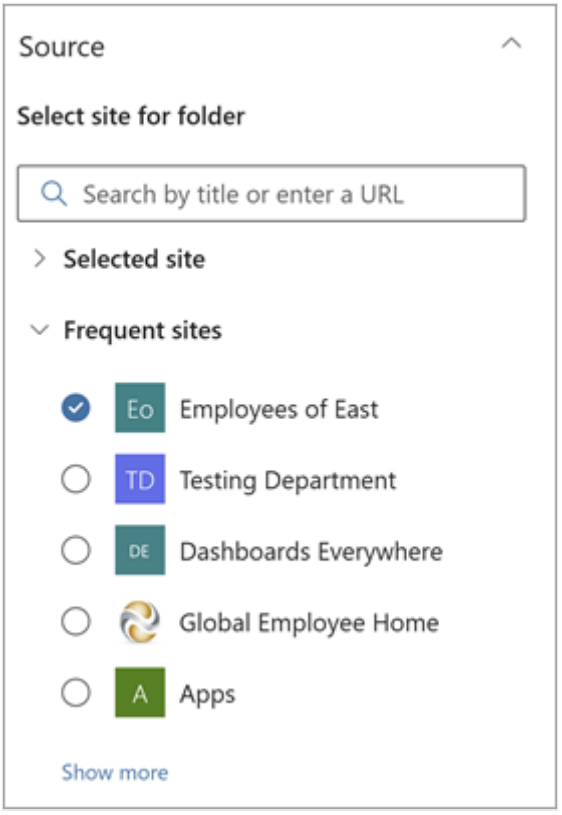
6. Under Card icon, select one of the following options that enable the icon to be displayed on the left side of the card title:

    - **Auto-selected**: This option when chosen automatically displays a built-in icon associated with the page.
    - **Custom image**: This option when chosen enables the Change button. You can select this button to choose an image you want to use as an icon.
    - **Library**: Select from a list of Microsoft provided icons.



7. In the **Select site for this folder** field, enter a **title** or **URL** of a SharePoint site that has an existing document library.

    - You can also select a SharePoint site from a list of **frequent sites**.

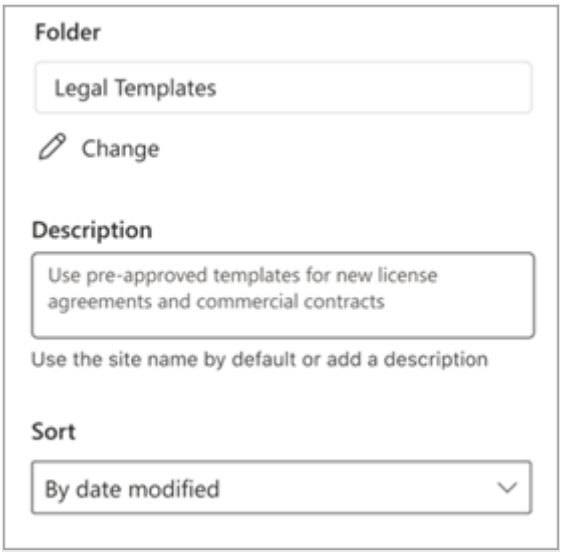


8. The document library in the selected SharePoint site will show in the **Folder** field.

- If the chosen SharePoint site has more than one document library, select **change** to choose a different library.

9. Enter a **description** for your card.

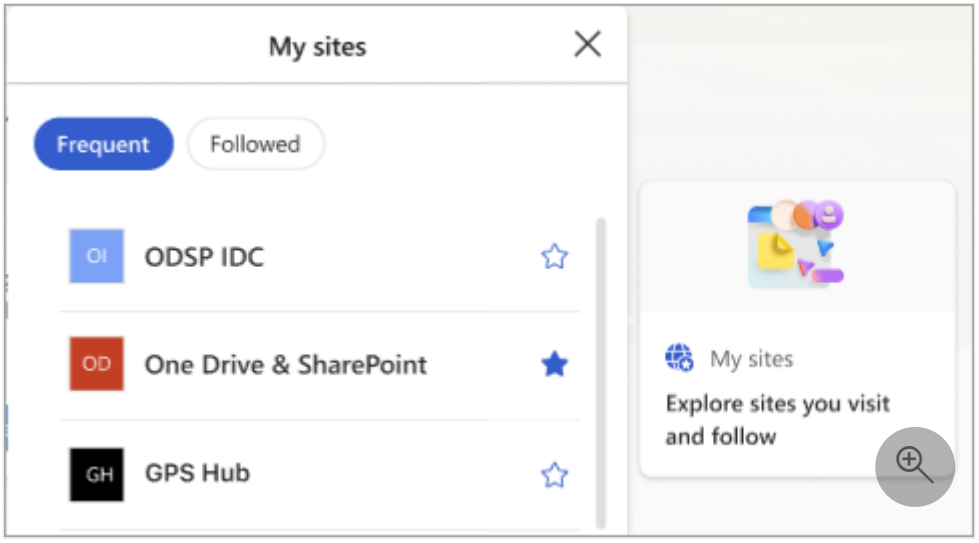
10. Under **sort**, select to order documents by date modified, A-Z, or Z-A.



11. To target your card to specific audiences (only audiences you specify will see the card in the dashboard), enter one or more M365 group into the Audience targeting field.

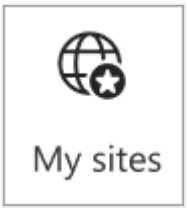
Add the My Sites card

Add the My Sites card to provide users links to their frequently visited or followed SharePoint sites in an easily accessible list.



1. While in edit mode, select + **Add a card** from the dashboard.

2. Select **My Sites** from the dashboard toolbox.

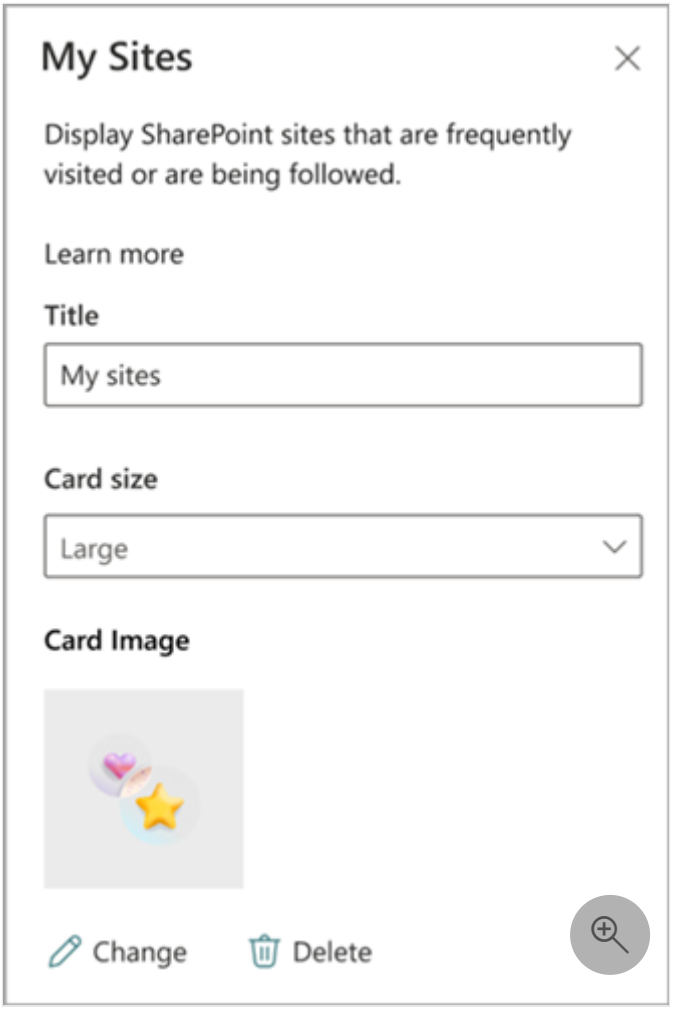


3. Select the **edit pencil** to the left of the card to open the properties pane for the My Sites card.

4. Enter a **Title** for the card.

5. Choose your card size from the **Card size** drop-down list.

6. To change the card image, select **Change**, then select an image or upload your own.



7. To target your card to specific audiences (that is, the card only displays in the dashboard to the audience you specify), select one or more groups to target.

Add the News card

Add the News card to the SharePoint app in Teams Dashboard to promote news from various sources that you wish to prominently display, including boosted news from SharePoint. If you

choose a boosted news post, they'll display in the News card during the boost period.

1. While in edit mode, select + **Add a card** from the dashboard.

2. Select **News** from the dashboard toolbox.

3. Select the **edit pencil** to the left of the card to open the properties pane for the News card.

4. Add a title and select a card size.

5. To target your card to specific audiences (that is, the card only displays in the dashboard to the audience you specify), select one or more groups to target.

6. For a news source, select one of the following options:

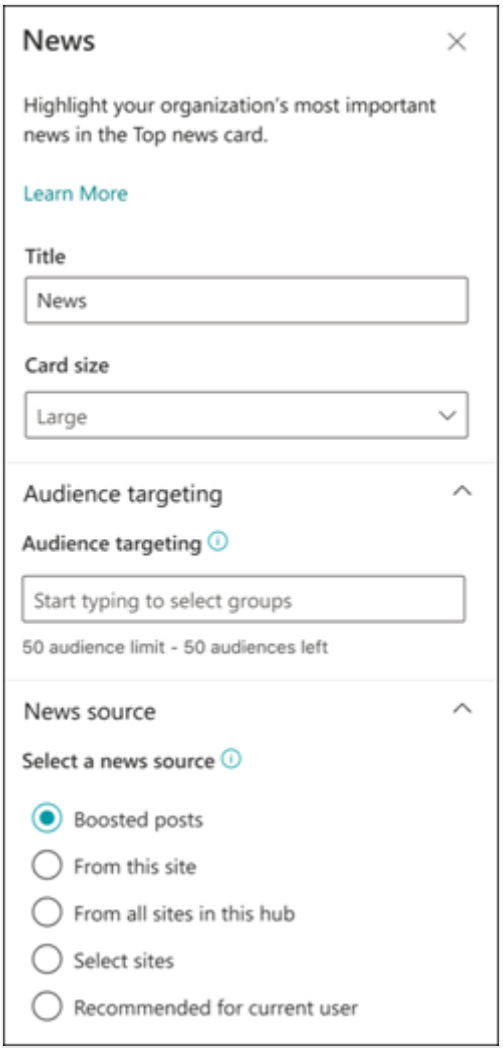
   - **Boosted posts**: Displays any SharePoint boosted news posts from the organization's news sites only. The word "Boosted" displays at the top of the card.

   - **From this site**: Pulls news from the hub site that the current site is a part of.

   - **From all sites in this hub**: Pulls news from all sites within your SharePoint hub.

   - **Select sites**: Pulls news from one or more individual sites (if selected, a list of sites associated with your SharePoint hub displays).

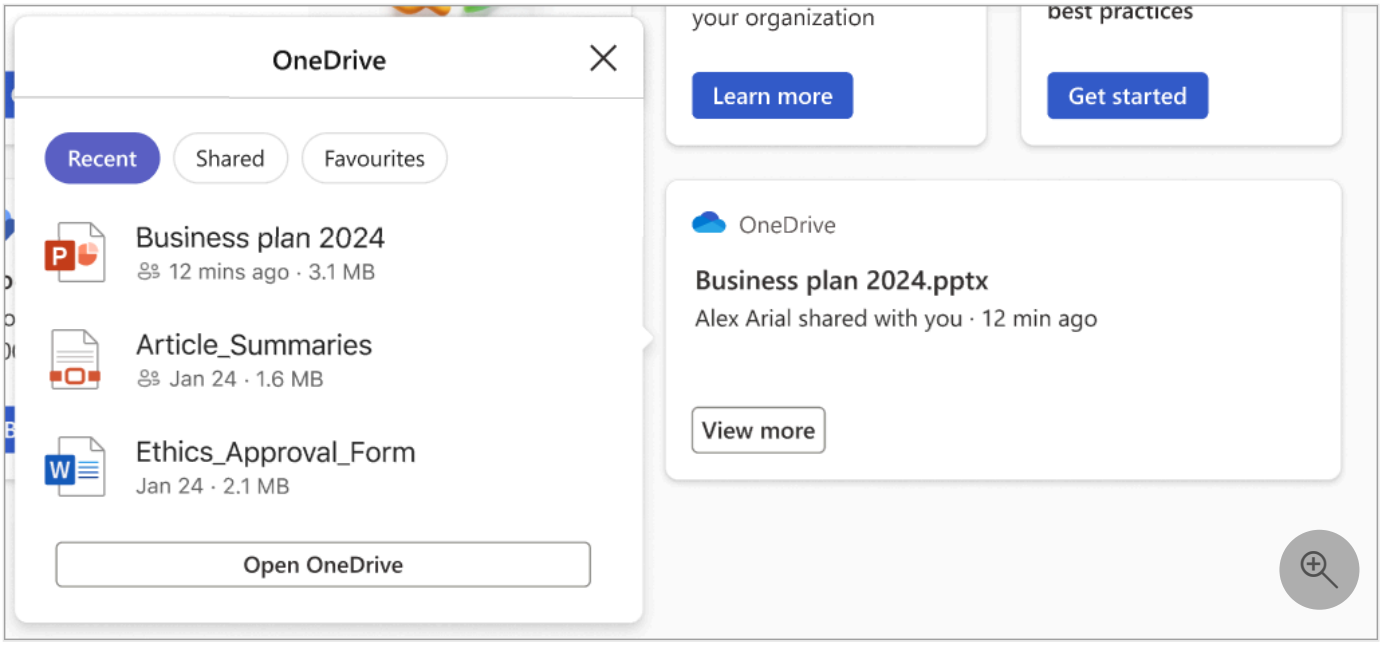
   - **Recommended for current user**: Displays news posts for the current user from people the user works with; managers in the chain of people the user works with, mapped against the user's own chain of management and people connections; the user's top 20 followed sites; and the user's frequently visited sites.



Add the OneDrive card

The OneDrive card (previously known as Files) connects individuals to their own recent, shared, or favorite files in their OneDrive account. Users can review files they have access to from their SharePoint app in Teams experience and open them from the OneDrive card.

> **Note**
>
> Office files like Word, PowerPoint, and Excel will be opened in their respective Teams app. All other file types will be opened in their respective web or local app.



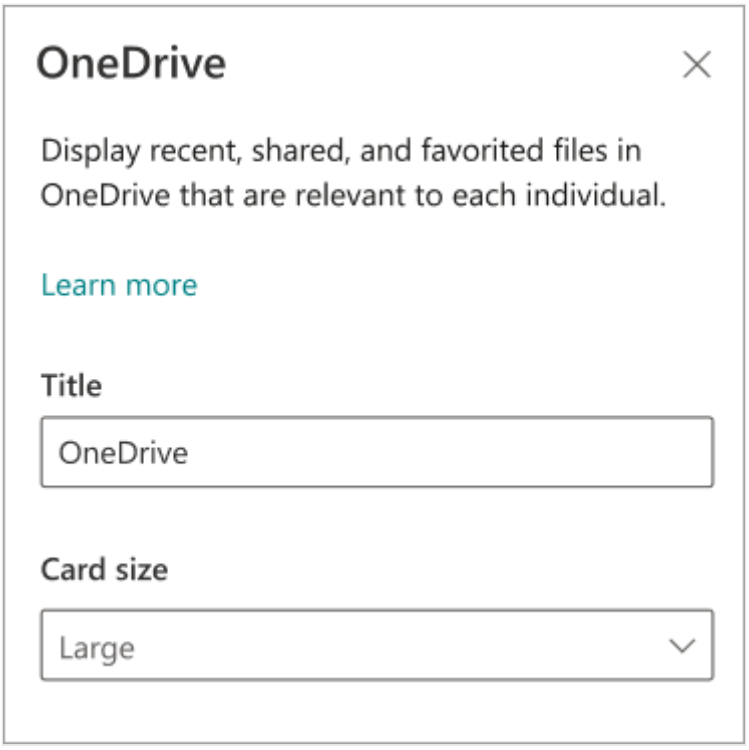
1. While in edit mode, select + **Add a card** from the dashboard.

2. Select **OneDrive** from the dashboard toolbox.

3. Select the **edit pencil** to the left of the card to open the properties pane for the OneDrive card.

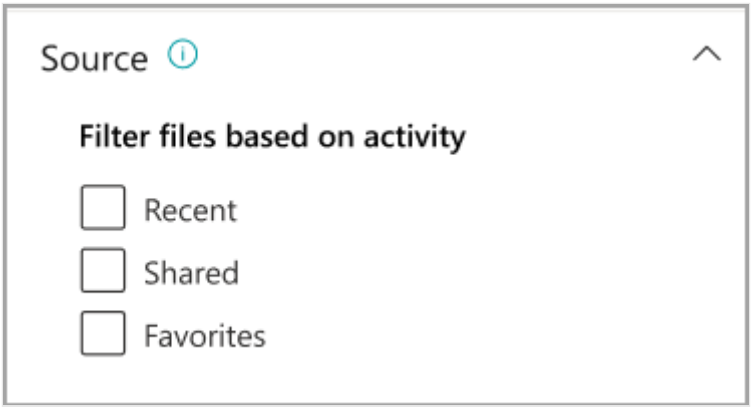
4. In the property pane on the right, enter a **Title** for the OneDrive card.

5. Choose your card size from the **Card size** drop-down list.



6. Select a **Source** for files to be displayed from:

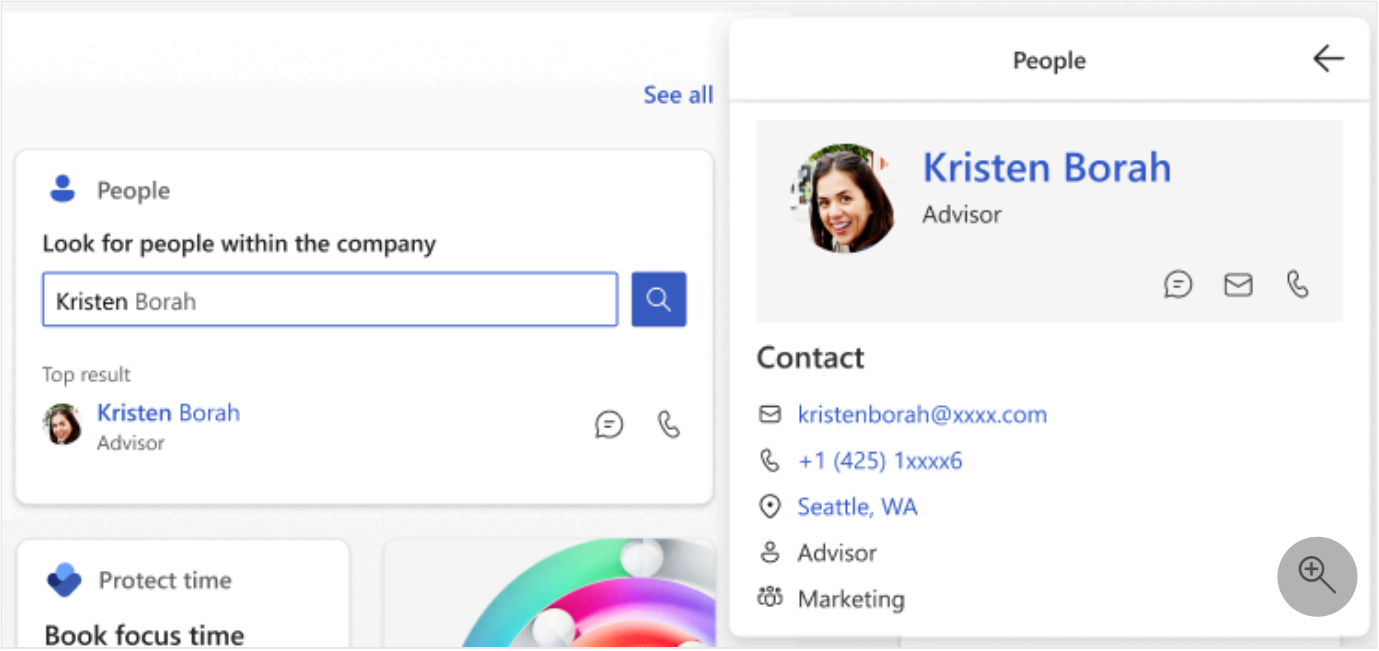
   - **Recent**: Recent files the user accessed display.
   - **Shared**: Files that shared with the user display.
   - **Favorites**: Files that the user marked as "favorite" display.



7. To target your card to specific audiences (that is, the card only displays in the dashboard to the audience you specify), enter one or more Microsoft 365 groups into the **Audience targeting** field.

Add the People card

The People Search card automatically retrieves contact information from members of your organization using Microsoft Entra ID. Users can access the People Search card to look up contact information and can jump into chat, email, or a call with the contact directly from the card view.



1. While in edit mode, select + **Add a card** from the dashboard.

2. Select **People** from the dashboard toolbox.

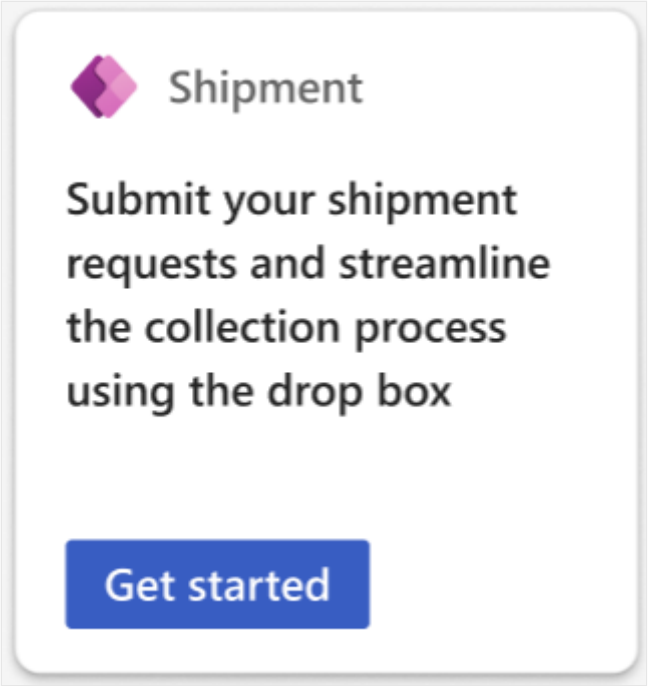
3. Select the **edit pencil** to the left of the card to open the properties pane for the People card.

4. In the property pane on the right, choose your card size from the **Card size** drop-down list.

5. To target your card to specific audiences (that is, the card only displays in the dashboard to the audience you specify), select one or more groups to target.

Add the Power Apps card

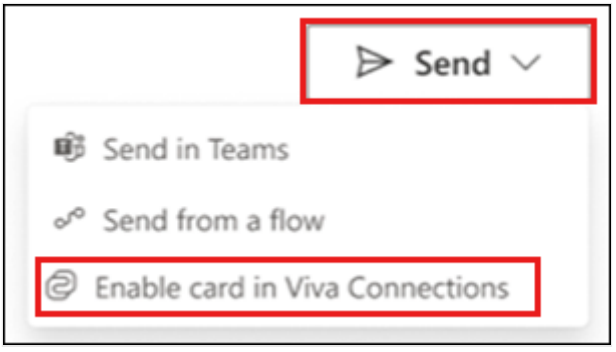
You can create a dashboard card using Power Apps for use in the SharePoint app in Teams. Design a lightweight power app to check daily sales numbers, shipment requests, vacation requests then bring it into the SharePoint app in Teams by pasting a URL.



> **Note**
>
> - You'll need a Power Apps account and have created a card in Power Apps in order to bring one into the SharePoint app in Teams.
> - Only cards based on the Dataverse connector are supported.
> - All SharePoint app in Teams users need to have the Basic User security role in the Power Apps environment where the card is created.

1. Access your Power Apps account to create your card. For more information about cards for Power Apps, see the overview documentation.

2. After creating your Power App, select **Send** and choose **Enable card in SharePoint app in Teams**.



3. When asked to Enable as a card in the SharePoint app in Teams, select **Enable**.

> **Note**

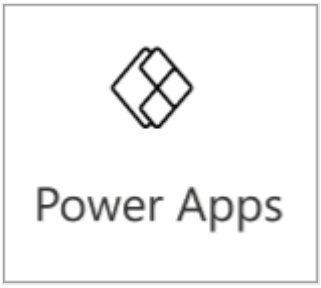
> If you're updating a Power App card that was previously enabled and added to the SharePoint app in Teams, the new version will automatically update once enabled.

4. Copy the **URL** for your card.

5. Access your SharePoint app in Teams instance.

6. While in edit mode, select **+ Add a card** from the dashboard.

7. Select **Power Apps** from the dashboard toolbox.

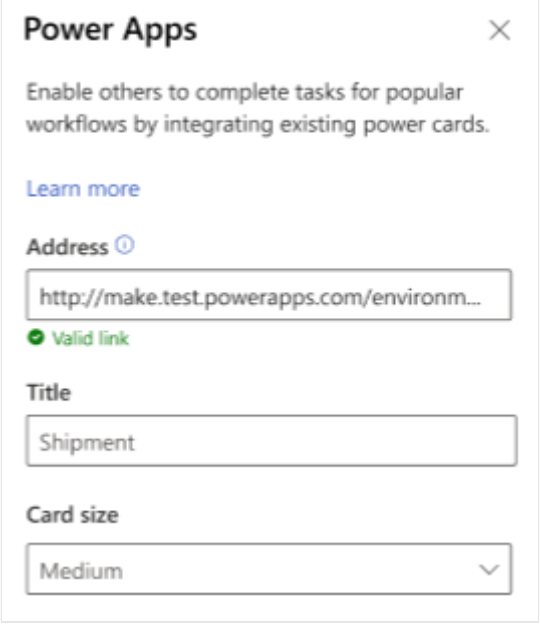


8. Select the **edit pencil** to the left of the card to open the properties pane for the Power Apps card.

9. In the property pane on the right, paste the URL from your created Power Apps card in the **Address** field.

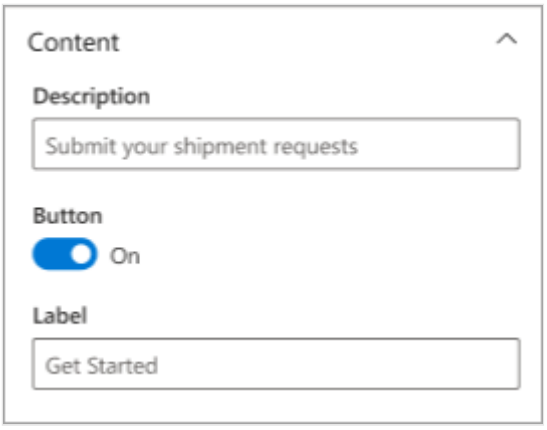
10. Enter a **Title** for the event card.

11. Choose your card size from the **Card size** drop-down list.



12. Enter a **Description** for your card.

13. The **Button** can be toggled on and off. If enabled, enter a name in the **Label** field.

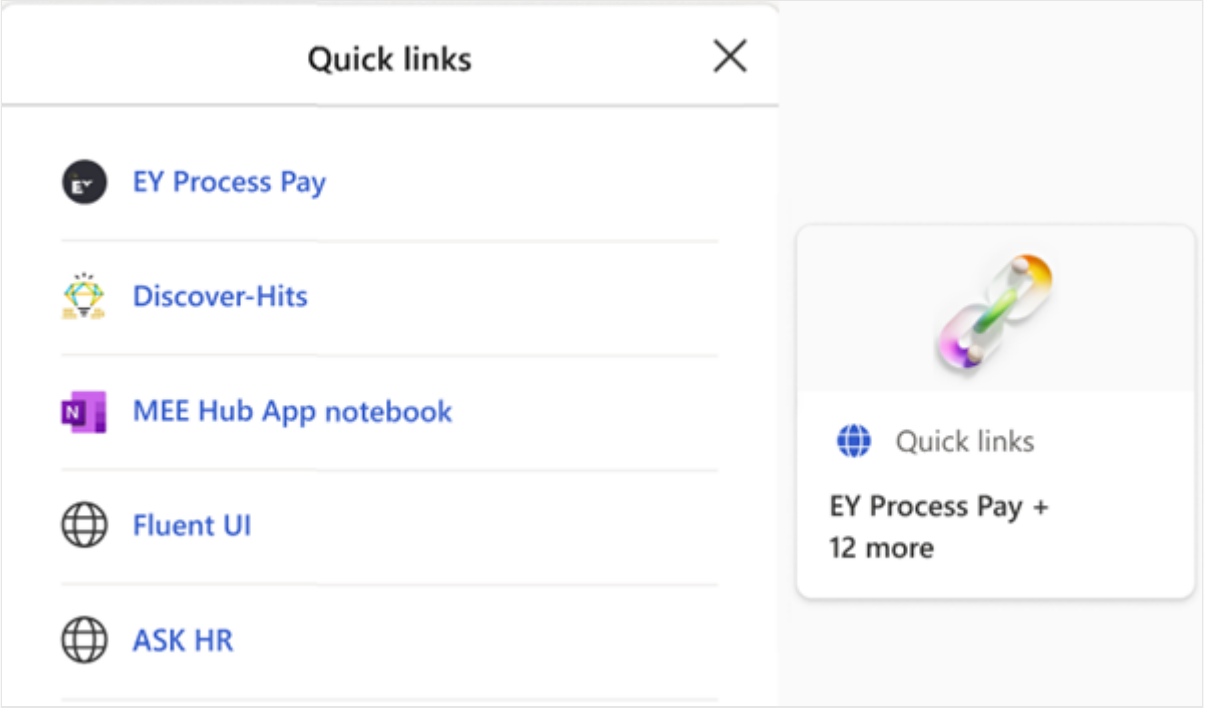


14. To target your card to specific audiences (that is, the card only displays in the dashboard to the audience you specify), select one or more groups to target.

For more information, see the documentation on using Power Apps.

Add the Quick links card

Use the Quick links card to provide a list of relevant links or files selected by admins to users. Users can select the link to be taken to the respective web page or file.



1. While in edit mode, select + **Add a card** from the dashboard.

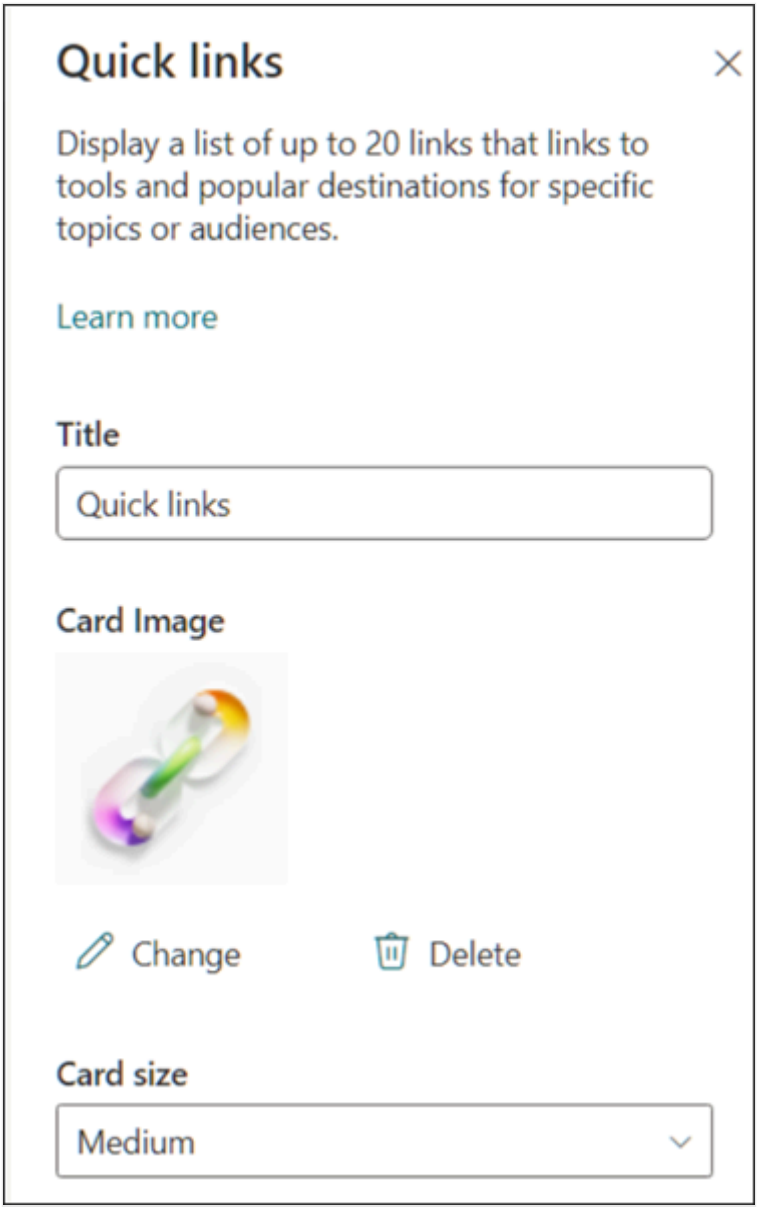
2. Select **Quick links** from the dashboard toolbox.

3. Select the **edit pencil** to the left of the card to open the properties pane for the Quick links card.

4. In the property pane on the right, enter the **title** for the Quick links card.

5. To change the card image, select **Change**, then select an image or upload your own.

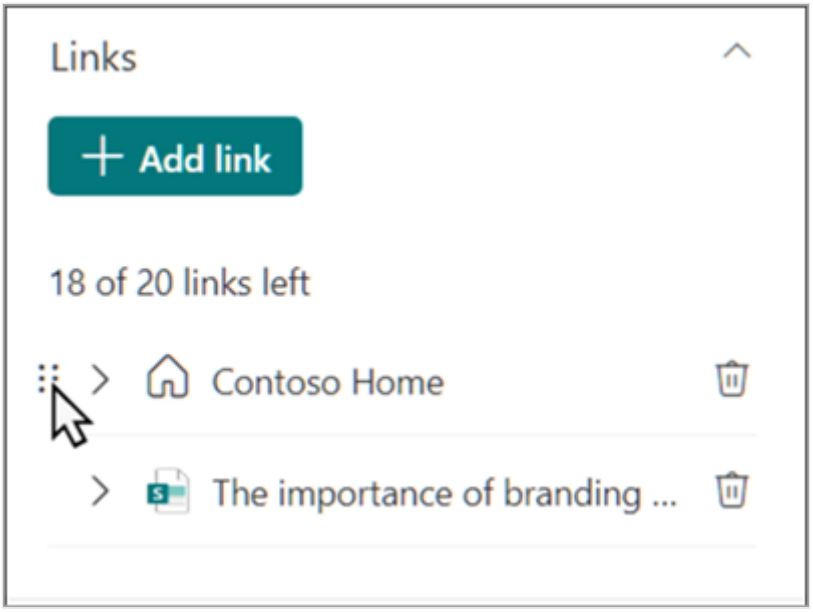
6. Select a **card size** for the Quick links card.



7. Under links, select + **Add link** to add a URL, SharePoint page, or files. Added links show below the + **Add link** button. You can add up to 20 links.

8. Once added, links can be edited in the following ways:

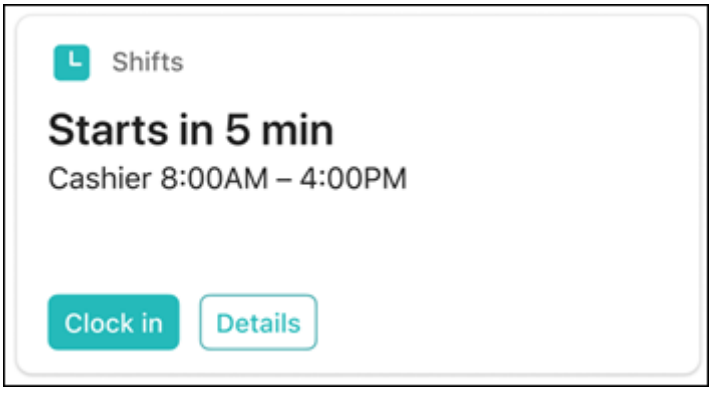
- **Rearrange** – Select and drag to the left of the link to reposition it within your quick link list.
- **Delete** – Select the trashcan to delete the selected link.
- **Edit** – Select the arrow to edit the link URL, title, and thumbnail image.



9. To target your card to specific audiences (that is, the card only displays in the dashboard to the audience you specify), select one or more groups to target.

Add the Shifts card

The Shifts card shows users information about their next or current shift from the Shifts app in Teams. They can also clock in and out and track break time when Time clock is enabled in Teams.



1. While in edit mode, select + **Add a card** from the dashboard.

2. Select **Shifts** from the dashboard toolbox.

3. In the property pane on the right, choose your card size from the **Card size** drop-down list.
4. To target your card to specific audiences (that is, the card only displays in the dashboard to the audience you specify), select one or more groups to target.

Add the Stay Engaged card

The Stay Engaged card can be added to help users access their Viva Engage feed conversations from within the SharePoint app in Teams, enabling employees to stay updated with important communications and relevant updates from their organization. Users can easily engage with conversations relevant to them without needing to switch apps.

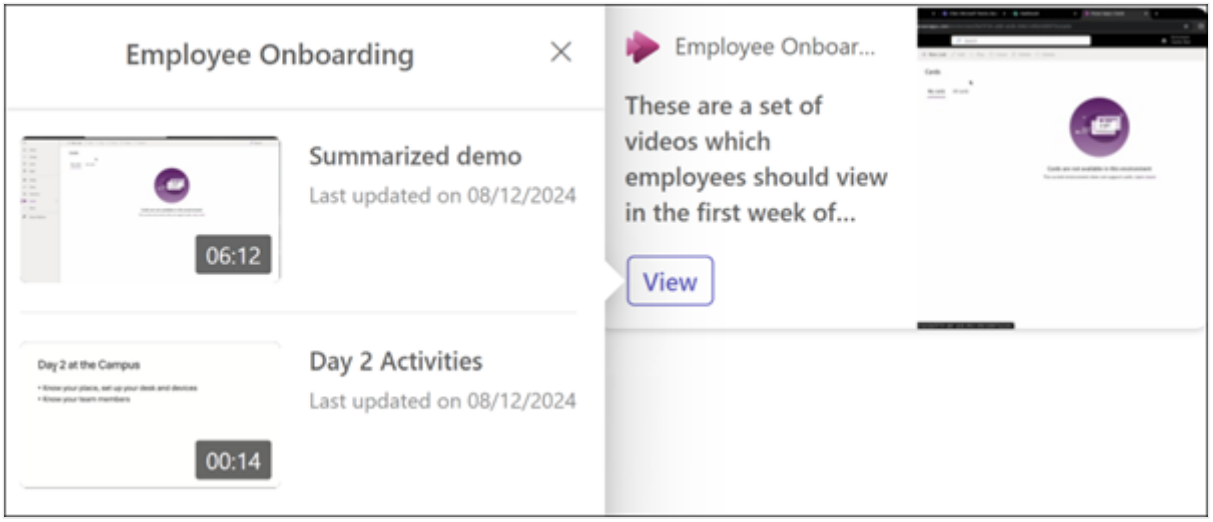
> **Note**
>
> The Stay Engaged card will be automatically added to unconfigured dashboards.

1. While in edit mode, select **+ Add a card** from the dashboard.
2. Select **Stay Engaged** from the dashboard toolbox.

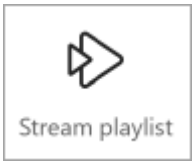
3. Select the edit pencil to the left of the card to open the properties pane for the Stay Engaged card.
4. In the property pane on the right, choose your card size from the **Card size** drop-down list.
5. To target your card to specific audiences (only audiences you specify will see the card in the dashboard), **enable audience targeting**.

Add the Stream playlist card

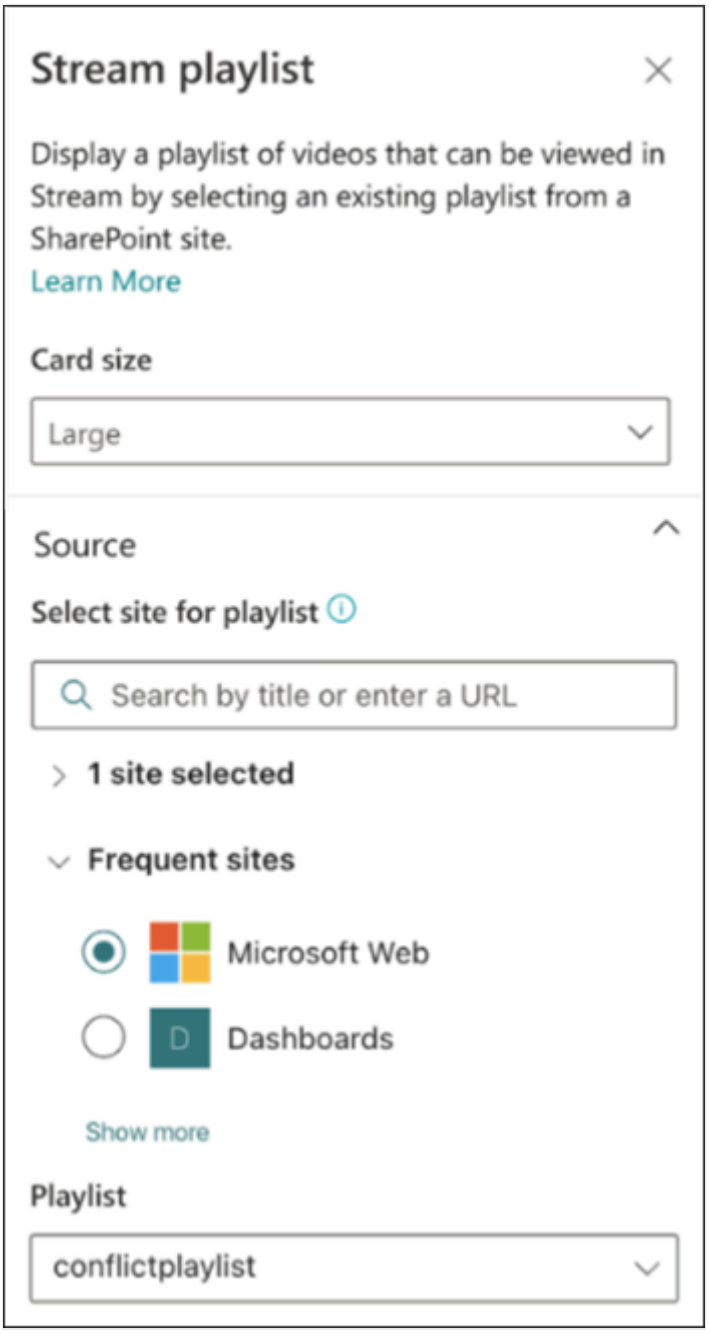
The Stream playlist card displays a list of videos to users that can be viewed in Microsoft Stream by selecting an existing playlist from a SharePoint site. For more information, see the article on creating a playlist from SharePoint.



1. While in edit mode, select + **Add a card** from the dashboard.
2. Select **Stream playlist** from the dashboard toolbox.



3. Select the **edit pencil** to the left of the card to open the properties pane for the Play list card.
4. In the property pane on the right, choose your card size from the **Card size** drop-down list.
5. Under source, select a **SharePoint site** that has the playlist you wish to display. You can search for a SharePoint site by its title, URL, or select from a list of frequented sites.



6. Under playlist, select the **playlist** from the drop-down of available playlists found from your selected source.

7. Enter a **Title** and **Description** for the selected playlist.

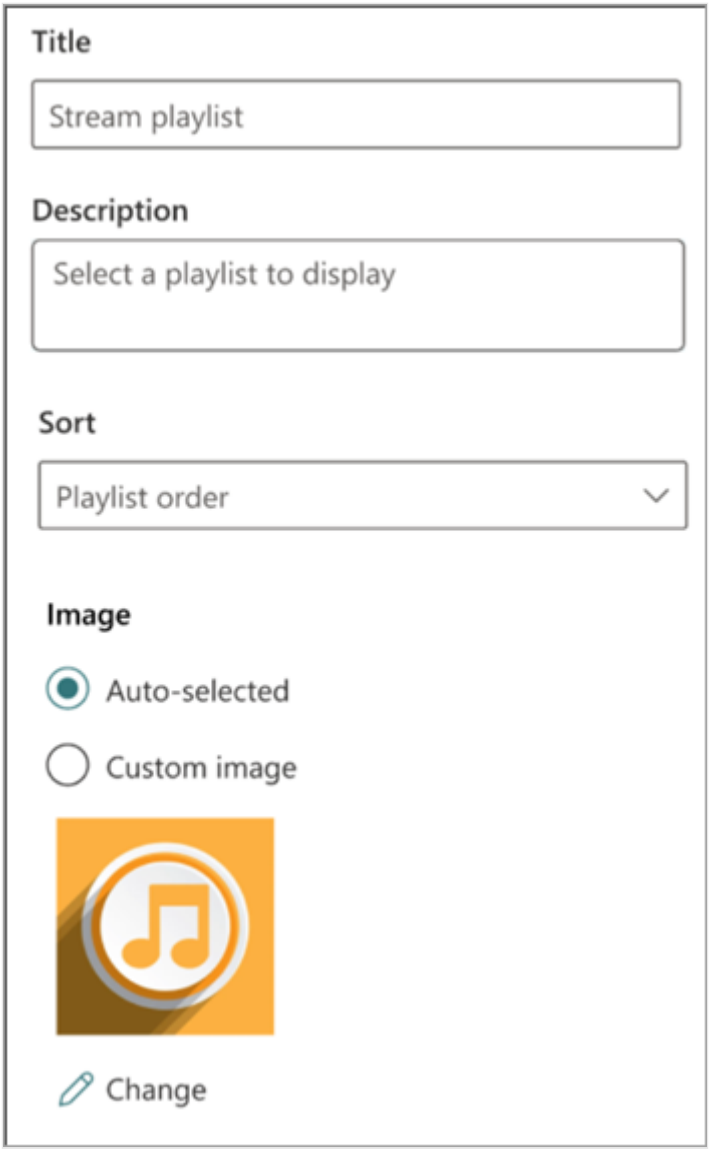
8. Under sort, select one of the following options:

   - **Playlist Order**: Videos play in the order set within the selected SharePoint playlist.
   - **Last Created**: Videos play in order based on the date they were last created.
   - **Last Updated**: Videos play in order based on the date they were last updated.

9. Under Image, select **Auto-selected** or **Custom image**:

   - **Auto-selected**: Displays an image for your playlist that comes from your selected SharePoint page.

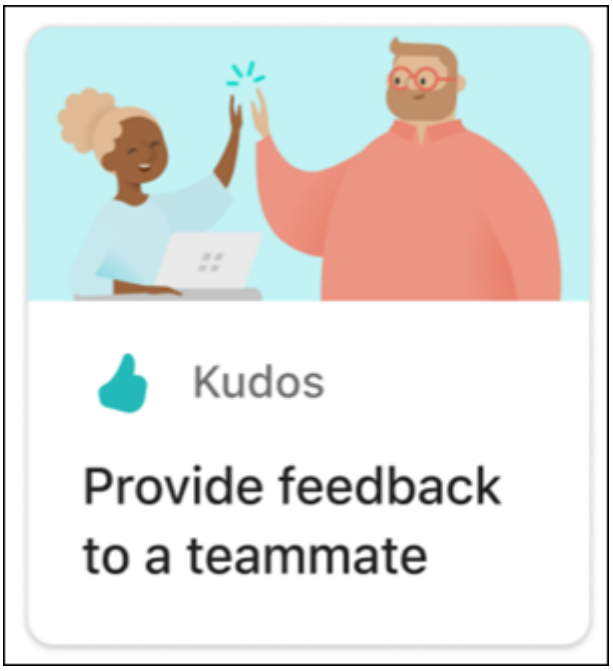
- **Custom image**: Select custom image then Change to upload your own image or select an existing image from your site or from an online source (for example, web search, OneDrive, Site).



10. To target your card to specific audiences (that is, the card only displays in the dashboard to the audience you specify), select one or more groups to target.

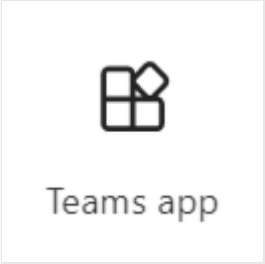
Add the Teams app card

A Teams app card allows you to create a card for an existing Teams app.

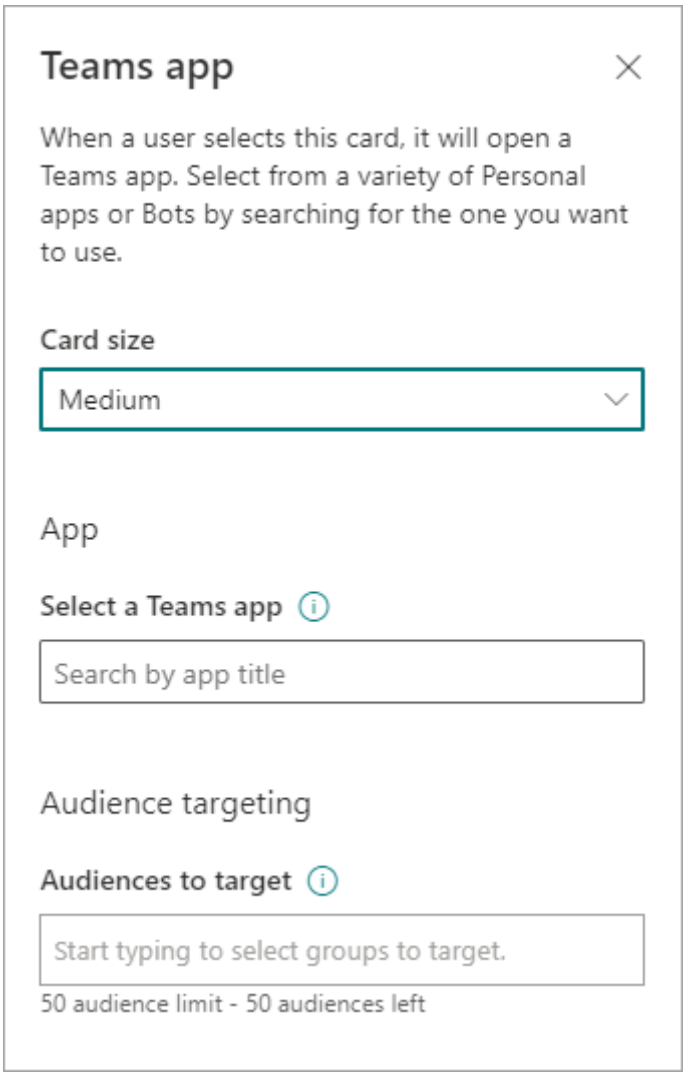


1. While in **edit** mode, select **+ Add a card** from the dashboard.

2. Select **Teams app** from the web toolbox.



3. In the **property** pane on the right side of the page, select your options.



4. Select a size for the card from the **Card size** drop-down list.

5. Search for the Teams app you want to use, and then select it from the list.

6. Set the card-display options:

    - Enter a title for the card in the **Card title** text box. (This title won't change your page title; it's the title that is displayed on the top of the card.)
    - Enter a description for the card in the **Card description** text box. This description is displayed in larger text under the title.

7. If you want to target your card to specific audiences (that is, the card only displays in the dashboard to the audience you specify), select one or more groups to target.

Add a partner card or Microsoft app

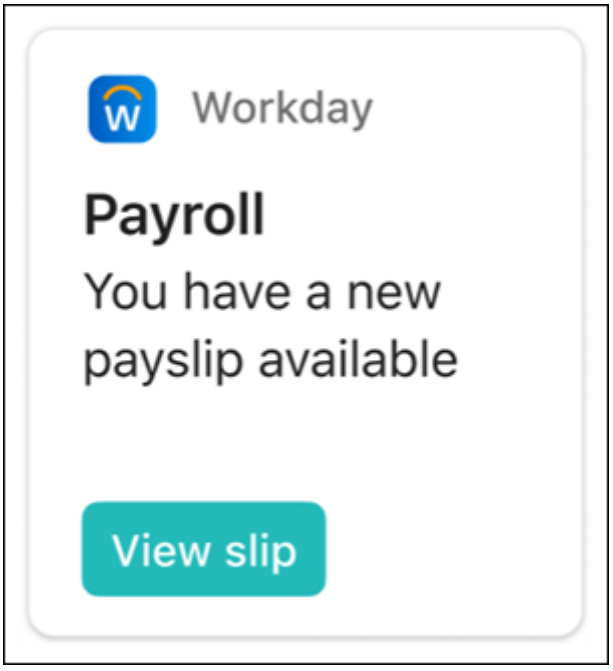
The SharePoint app in Teams dashboard and mobile experience can be extended and customized using cards, which are based on adaptive cards and the SharePoint Framework (SPFx). These

adaptive cards are used to display data, and complete tasks. They provide a low-code solution to bring your line-of-business apps into the dashboard.

To create custom experiences for the SharePoint app in Teams dashboard across web, desktop and mobile, developers must use the SPFx to create custom Adaptive Card Extensions (ACE). To learn more about creating ACE, see the following tutorial: Build your first SharePoint Adaptive Card Extension. Learn more about SharePoint app in Teams extensibility.

Add a partner card

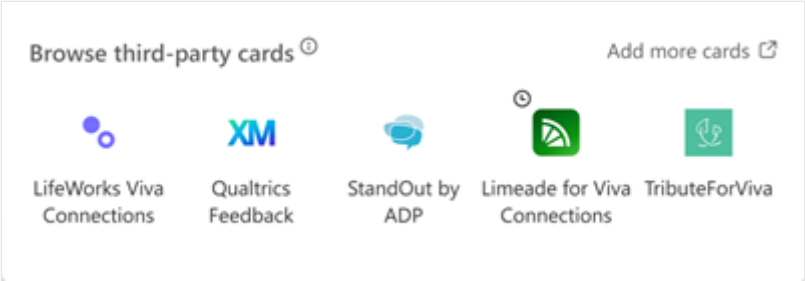
There are three ways to get partner apps and solutions integrated with the VSharePoint app in Teams dashboard. The following image shows an example of a partner card.



Option 1: Discover and request apps from the SharePoint app in Teams card toolbox

Partner cards and an entry point to browse more cards in the app store will automatically display in the card toolbox. Depending on your level of permissions, you might need to request the app before it can be used on the dashboard. Learn more about managing partner apps.

> **Note**
>
> - Site owners managing the SharePoint app in Teams dashboard will need to request partner apps before they're available in the card toolbox.
> - Some partner apps require a service plan agreement with your organization.



1. While in edit-mode, select + **Add card** from the dashboard.
2. Partner options appear in the **Suggested cards** section. Select one of the cards displayed or browse more cards by selecting **Add more cards**.
3. Request the cards you'd like to add to the toolbox and the requests will be sent to the App Catalog Admin for their approval.
4. You'll receive an email to confirm if your request has been approved or denied by the App Catalog Admin.
5. Once your request has been approved, refresh the page to see the new card display in the toolbox.

Option 2: Acquire the app from a Microsoft AppSource or the SharePoint store

- If you're building a dashboard, you can request the app directly, but you need approval from an admin of the tenant-level app catalog to continue with the installation
- If you're an **admin** of a tenant-level app catalog, you can deploy business apps directly. You can acquire apps from non-Microsoft developers by browsing the Microsoft AppSource or SharePoint store (recommended).

Get step-by-step guidance on how to request and deploy an app, and add an app to your site. For tenant admin, learn how to manage apps in the App Catalog.

Option 3: Acquire the app directly from the partner developer

> **Note**
>
> SharePoint administrative permissions are required to complete this task.

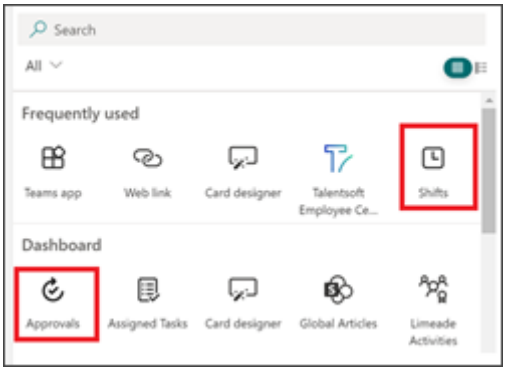
You can request apps directly from the SharePoint app in Teams partner developers and partners. Admin permissions are required to add the app to tenant level app catalog.

Add a Microsoft app as a card on the dashboard

A Microsoft app card allows you to create a card that links to Microsoft apps (For example: Shifts, Approvals, Task, etc.). Microsoft apps cards are available out of the box when SharePoint app in Teams is enabled.

1. While in edit mode, select + **Add a card** from the dashboard.

2. Select the Microsoft App you want to add from the web toolbox.



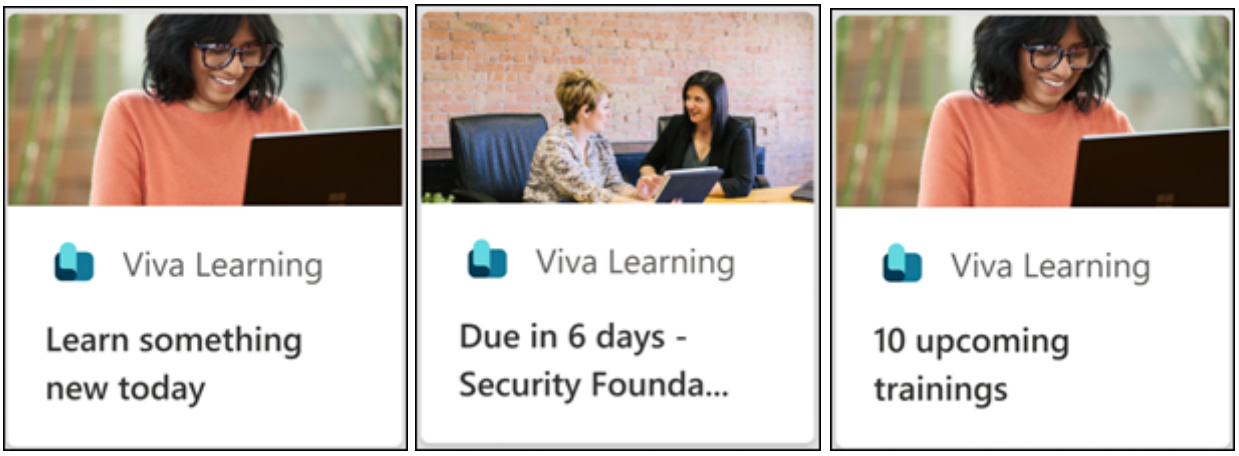
3. Select your options in the property pane on the right side of the page.

4. When you **Republish**, the card appears on your dashboard.

Add the Viva Learning card

The Viva Learning card provides users quick-links to recommended trainings, and can be set to target specific trainings to certain individuals. Users can easily access their required trainings by selecting the Viva Learning link.

Content in the cards is dynamic and changes according to settings in Viva Learning. The following are three examples of Viva Learning card states that display different information depending on the viewer and Viva Learning settings.



1. While in edit mode, select + **Add a card** from the dashboard.

2. Select **Viva Learning** from the dashboard toolbox.

3. In the property pane on the right, choose your card size from the **Card size** drop-down list.

4. To target your card to specific audiences (that is, the card only displays in the dashboard to the audience you specify), select one or more groups to target.

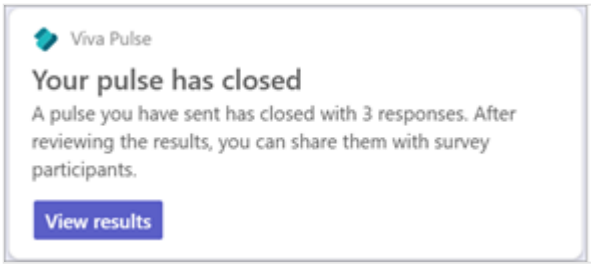
Add the Viva Pulse card

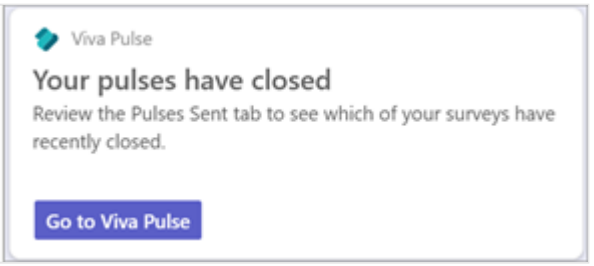
Invite managers and team leads to send requests for feedback or view feedback results using the Viva Pulse card. The card provides a way for feedback authors to access and interact with active or recently closed feedback pulses. This provides feedback authors and feedback providers with a direct link to their account in the Viva Pulse Teams app.

> ⓘ **Note**
>
> - It's recommended admins set up the Viva Pulse app for their organization and pin it as an app in Microsoft Teams so users can fully experience the Viva Pulse card. For more information, see the article on manage, install, and pin Viva Pulse in the Teams admin center.
> - Users will only see the Viva Pulse card if their organization is licensed for Viva Pulse.

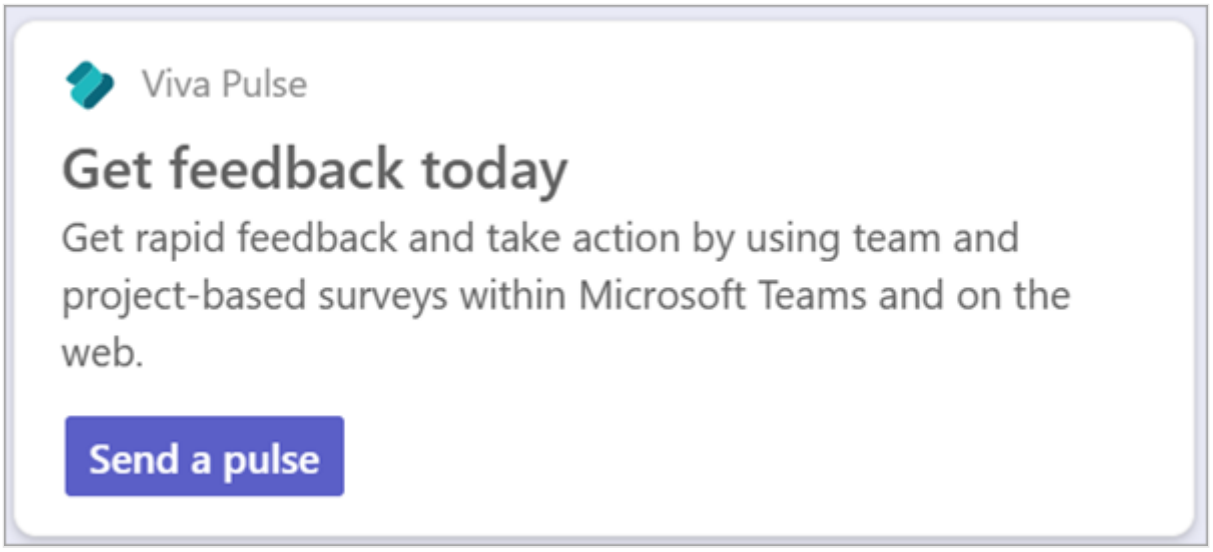
Content in the card is dynamic and changes according to the users role in Viva Pulse and if a feedback pulse is active. The following are examples of Viva Pulse card states that display different information depending on the viewer's role and if any active or recently closed feedback pulses are available.

The Pulse card tells feedback authors the number of responses an active or recently closed pulse received and provides a link to feedback results in their Viva Pulse account for the recently closed pulse. When multiple feedback results are available, authors are directed to their **Pulses sent** tab within the Viva Pulse Teams app.





When no open pulses are available, the card displays **send a pulse**, which brings the author to the Viva Pulse Teams app where they can create a new request for feedback to be sent out.



> ⓘ **Note**
>
> - Viva Pulse requires a license to send pulse requests for feedback and to review results. A license is **not required** to respond to a pulse. For more information on Viva Pulse licensing, see the article on Licensing requirements.
> - The Viva Pulse card requires the Viva Pulse app to be enabled in Microsoft Teams for the card to display information

To add the Viva Pulse card to your dashboard:

1. While in edit mode, select + **Add a card** from the dashboard.

2. Select **Viva Pulse** from the dashboard toolbox.

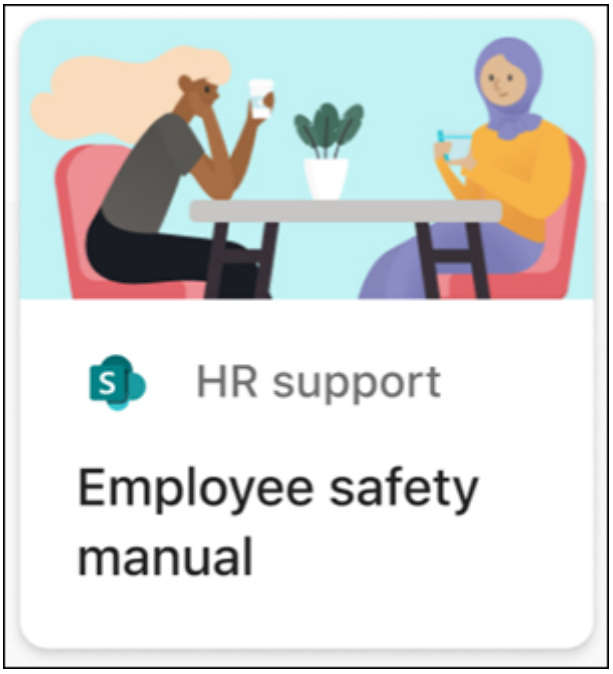
3. In the property pane on the right, choose your card size from the **Card size** drop-down list.

4. To target your card to specific audiences (that is, the card only displays in the dashboard to the audience you specify), select one or more groups to target.

For more information on using Viva Pulse as a feedback author or feedback recipient, see the Viva Pulse documentation here.

Add the Web link card

Add a web link card when you want your users to go to an internal or external link on a web site.



1. While in **edit** mode, select **+ Add a card** from the dashboard.

2. Select **Web link** from the web toolbox.

3. In the property pane on the right side of the page, select your options.

4. Select a size for the card from the **Card size** drop-down list.

5. Enter the URL for your link in the **Link** text box.

6. Set the card-display options:

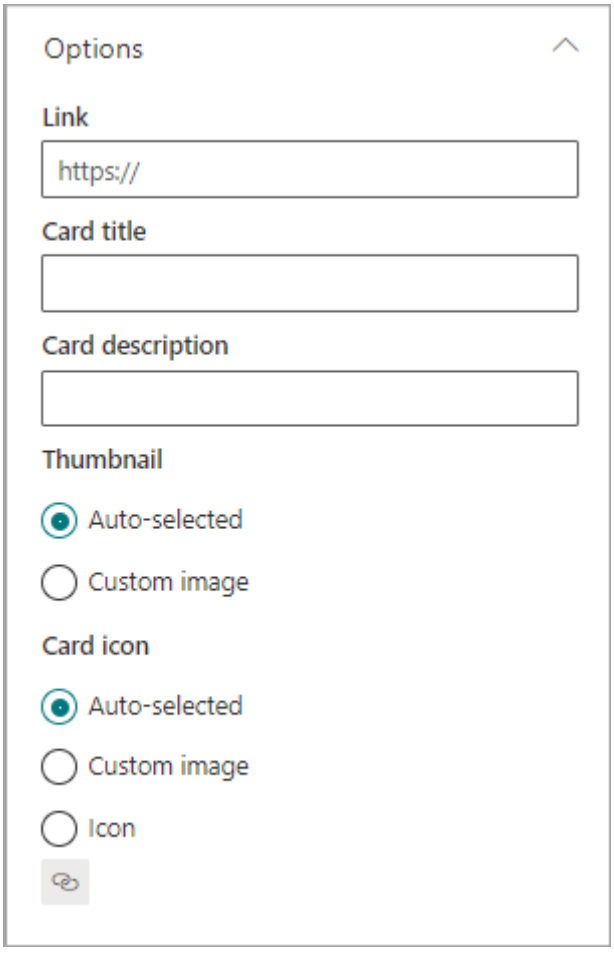
- Enter a title for the card in the **Card title** text box. (This title won't change your page title; it's the title that is displayed on the top of the card.)
- Enter a description for the card in the **Card description** text box. This description is displayed in larger text under the title.

7. Under **Thumbnail**, select one of the following options:

   - **Auto-selected**: This option when chosen automatically displays an image at the top of your card that comes from your page.
   - **Custom image**: This option when chosen enables the **Change** button. You can select this button to choose an image you want to use.

8. Under **Card icon**, select one of the following options that enable the icon to be displayed on the left side of the card title:

   - **Auto-selected**: This option when chosen automatically displays a built-in icon associated with the page.
   - **Custom image**: This option when chosen enables the **Change** button. You can select this button to choose an image you want to use.
   - **Icon**: This option when chosen enables the **Change** button. You can select this button to choose from a set of stock icons.



9. To target your card to specific audiences (that is, the card only displays in the dashboard to the audience you specify), select one or more groups to target.

More Resources

Create a SharePoint app in Teams dashboard and add cards

Design your own dashboard card with the card designer

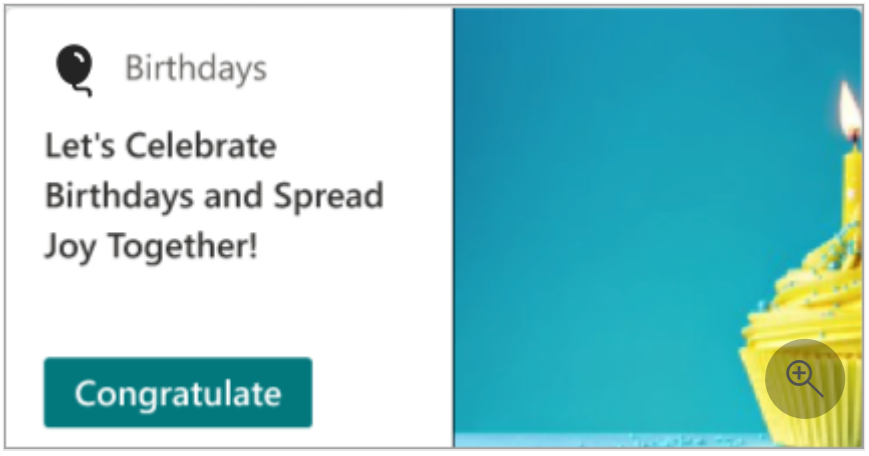
Last updated on 09/20/2026

Design your own dashboard card with the card designer

Use the Card Designer within the SharePoint app in Teams to create cards that can link to other sites, open media, display a location, open a teams app, and more. Card designer gives users the ability to quickly build "custom" cards without the need for custom code by using a template with the option to create a secondary view, also called a quick view.

Quick view is a powerful tool that enables the card designer to create cards that go beyond the traditional dashboard cards to create something interactive and informative using Adaptive Card JavaScript Object Notation (JSON). You're able to "code" a single quick view by using the power of Adaptive Card markup to make their cards dynamic. The result can be previewed within the card designer before sharing with others.

> **Note**
>
> To design your own cards using quick view, you should be familiar with JSON and Adaptive Card templates. For more information, see Adaptive Cards Templating.



Edit the dashboard

You need member or owner level permissions to access the card designer from the dashboard card toolbox.

Use a card template

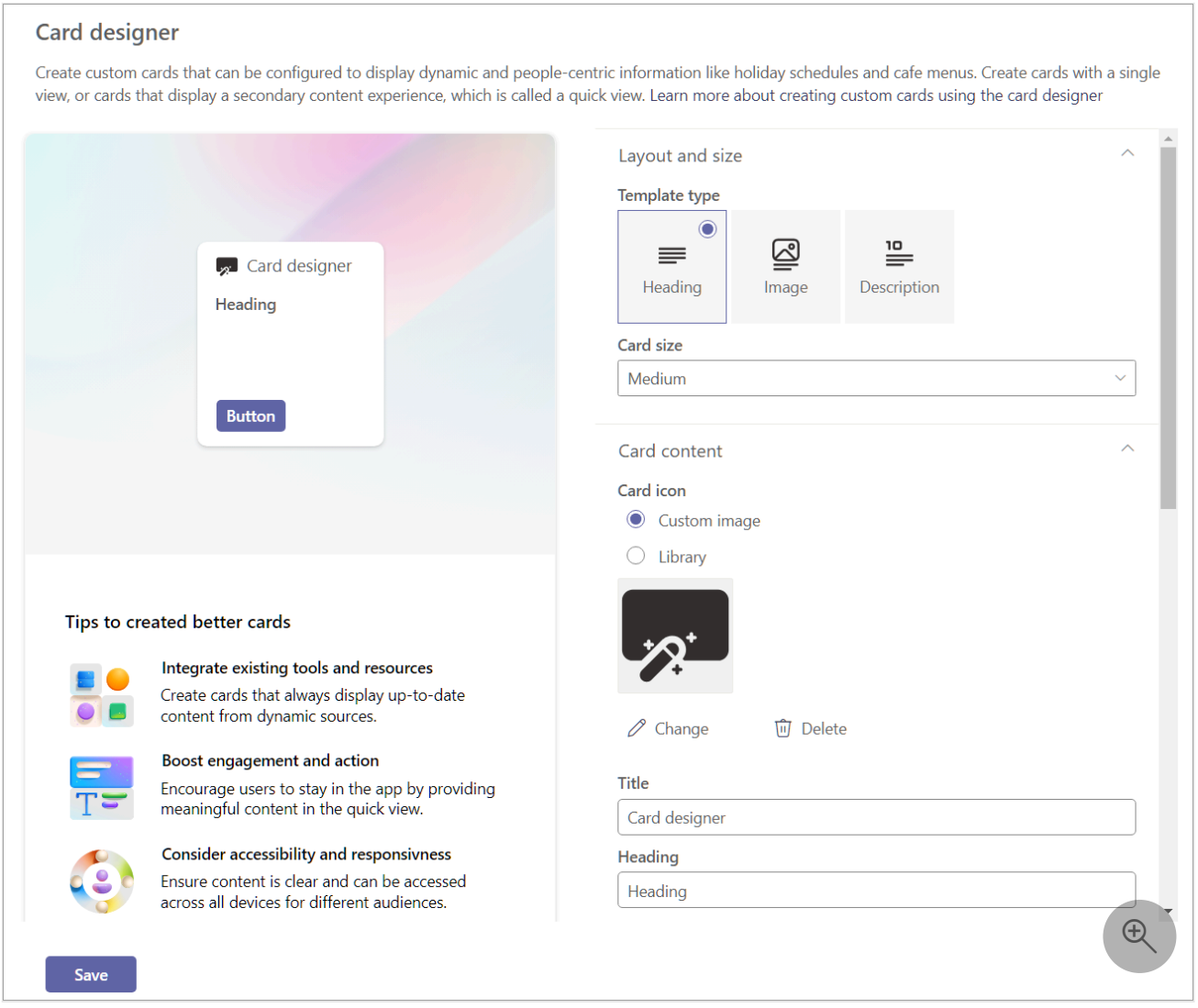
The card designer has a set of card view templates that can be used to easily create cards with helpful information, links, and media. The following steps walk you through creating a new large sized card using the image template to create a link for users.

1. While in **edit** mode, select **+ Add a card** from the dashboard.

2. Select **Card designer**.

3. After selecting the Card designer card, select the **Edit** icon to open the property pane.

4. As you create your card through selecting options, a preview of how the card looks appears to the left of the options.



5. Under **Template type**, select one of three **templates** to apply:

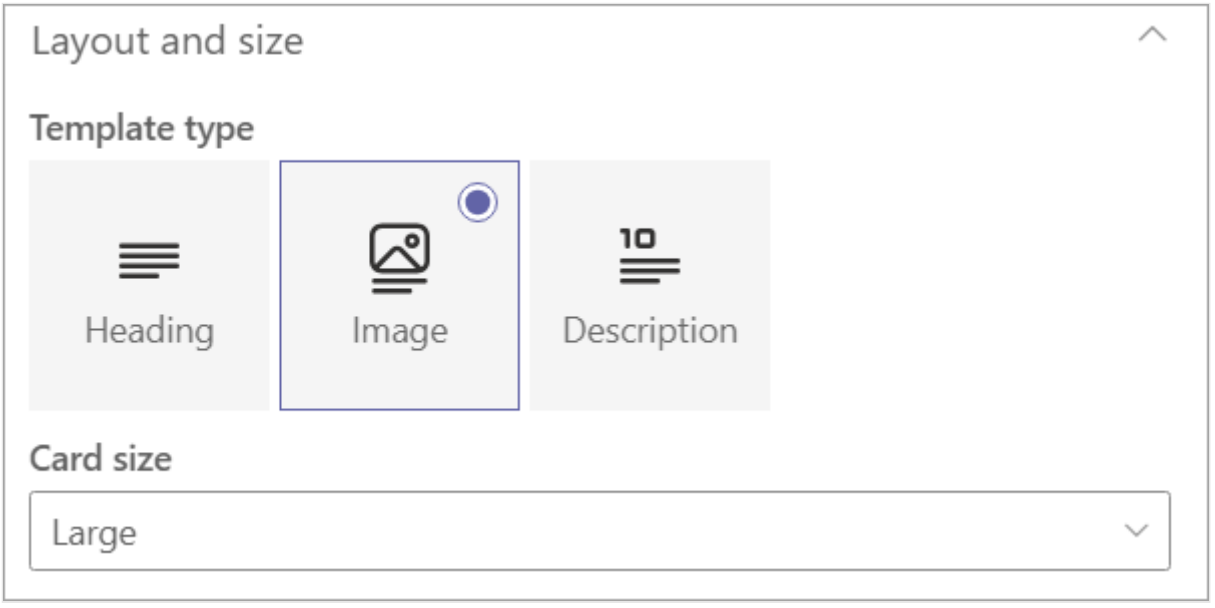
- **Heading**: Create a card with a simple heading.
- **Image**: Create a card with a heading and image.
- **Description**: Create a card with a heading and description.

> ⓘ **Note**
>
> Buttons are disabled when selecting the Image template for a medium sized card, but a card action can still be assigned to trigger when the user selects the card.

Depending on the template type chosen, fields matching the template type populates in the **card content** section. For example, if you chose the Image template, you can enter values for the Image and Heading properties in their respective text boxes.

6. Select a **card size**:

- **Medium**: the default card size and allows you to add one button to the Heading and Description templates.
- **Large**: takes the space of two medium cards together and allows the use of two buttons.



7. Under **Card icon** select one of the following options:

- **Custom image**: Select **custom image** then **Change** to upload your own image or select an existing image from your site or from an online source (for example, web search, OneDrive, Site).

- **Library**: Select an icon from a pre-existing list of available icons. For example, select **Library** then **Change** to choose a new icon.

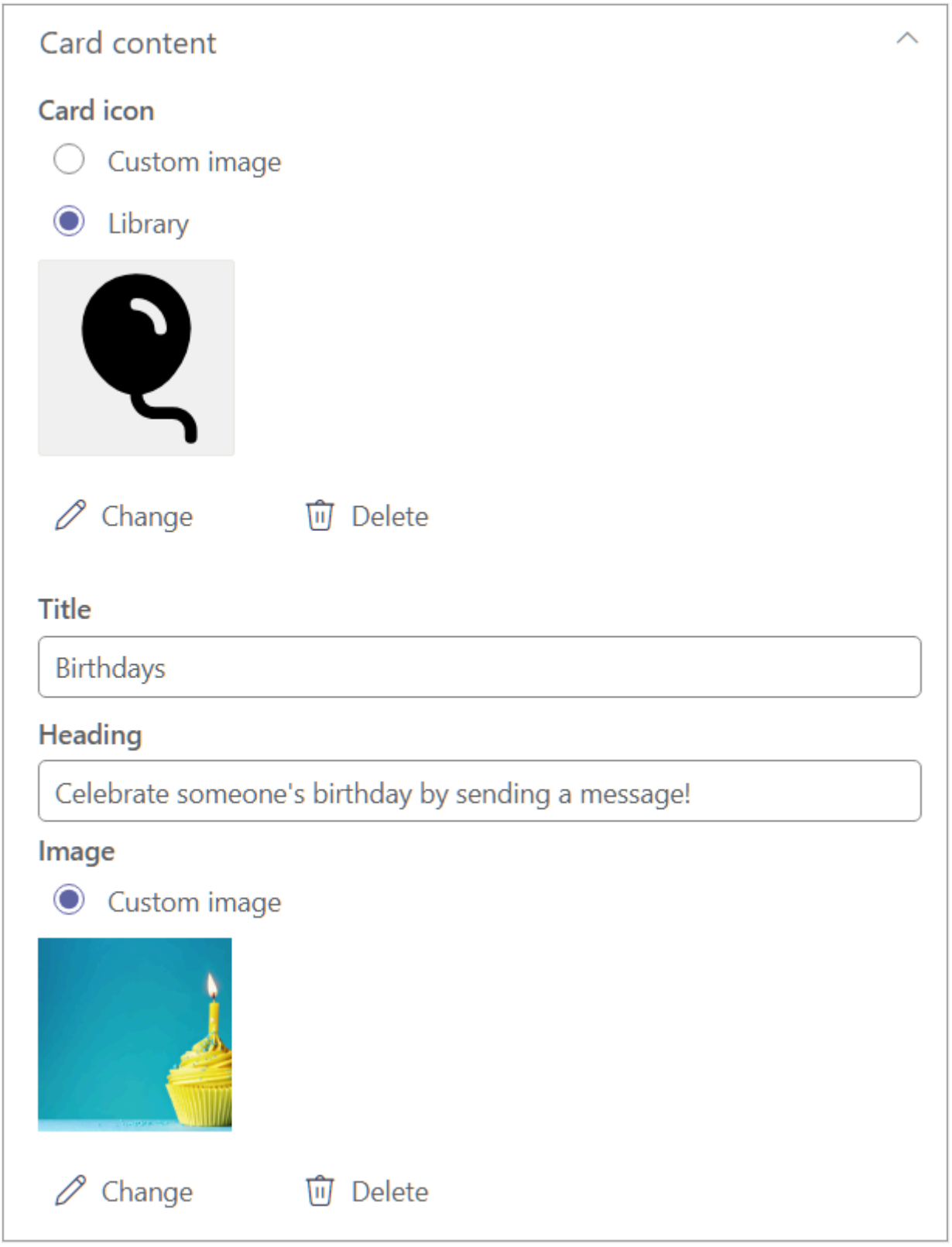
> ⓘ **Note**
>
> When uploading custom images for your icons, we recommend using PNG images between 24x24 and 32x32 pixels.

8. Enter a **Title** to be displayed at the top of your card.

9. Enter a **Heading**.

10. Depending on the template type chosen, enter values for the properties corresponding to your selection below the heading field. For this example, the image template is being shown:

    - **Image**: Select **change** to upload your own image or select an existing image from your site or from an online source (for example, web search, OneDrive, Site).



Note

- Image recommendations for cards in the dashboard: medium cards should be 300x150 to 400x200 with 2:1 aspect ratio and large cards 300x300 to 400x400 with 1:1 aspect ratio to prevent stretching in the mobile app.
- Image URLS in card properties must be an absolute URL for the link to work in the mobile app.

11. Under card action, select an action to be performed when a user selects the card. Depending on the action selected, more fields appear to customize the action.

> ⓘ **Note**
>
> The card action cannot be disabled.

- **Show the quick view**: Select to use JSON code to create a more interactive dashboard card. If selected, the **Save** button changes to **Next**, which leads to more settings for customizing your quick view card. One quick view is available for each card, which can be opened as the card action, or by using a button. For steps on using quick view, refer to add a quick view to a card.

- **Go to a link**: Enter a URL to direct users to.

- **Go to teams app**: the user is directed to the specified teams app by the URL provided (admins can also use the appID to direct users to the appropriate Teams app). For more information, see Deep link to an application.

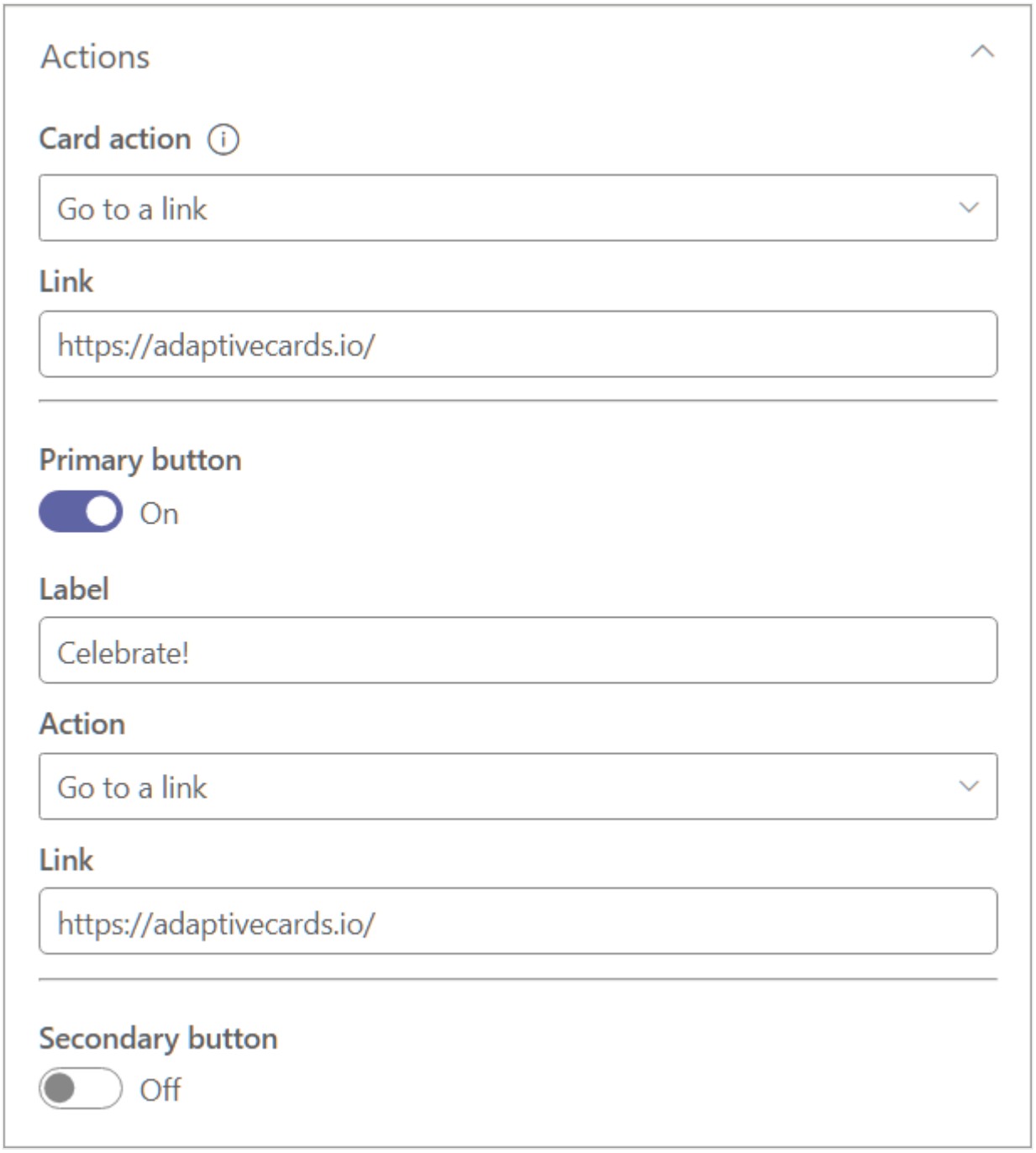
  For example, selecting **Go to a link** from the dropdown displays a field for entering the link.

12. Under **Link**, enter the **URL** you wish users to be directed to.

13. Buttons can be toggled on and off (where available). If enabled, the same values found under card action can be selected for the **Primary** and **Secondary** buttons.

> ⓘ **Note**
>
> When using a medium sized card, only one button can be enabled using the heading or description template. The image template will disable the use of buttons when medium size is selected.

For this example, the **Primary button** is set to direct users to the same link as the card action. The **Secondary button** is disabled.



14. Under **Audiences to target** enter one or more groups to target so only those audiences specified see the card in the dashboard. For more information, see audience targeting in the SharePoint app in Teams.

15. Select **Save** to save the updates to your card.

Add a quick view to a card

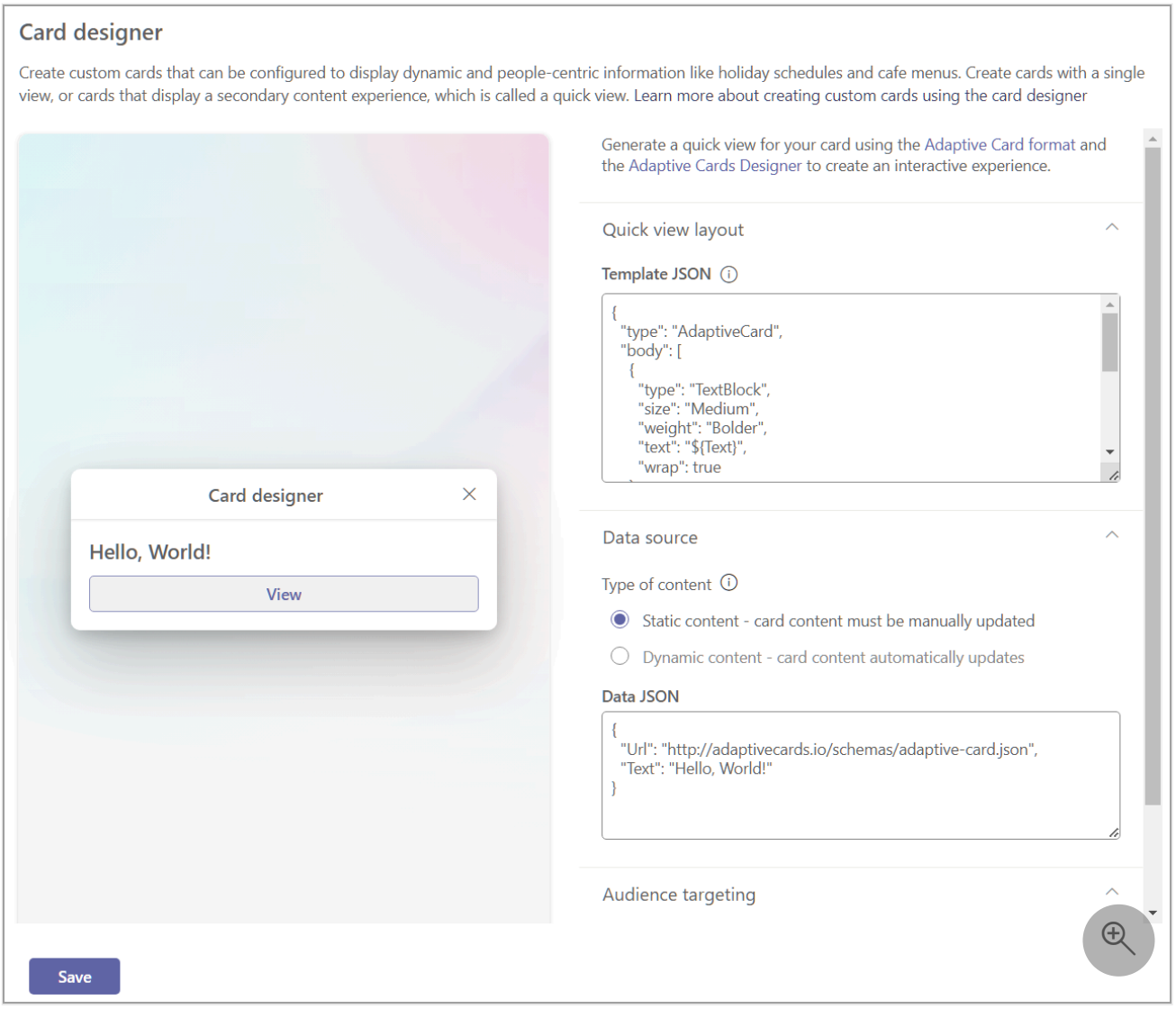
Quick view allows you to add adaptive card JSON code to Dashboard cards to provide a more comprehensive, interactive, and engaging experience to users. By using static or dynamic data sources (like SharePoint Representational State Transfer (REST) API or Microsoft Graph API), cards can be created that provide information within the SharePoint app in Teams experience, without the user having to navigate away.

To get started, follow the steps in use a card template up to selecting a **Card action**.

1. Under **card action** select **Show the quick view**.
2. Finish setting up your card by enabling or disabling buttons and selecting actions for active buttons.

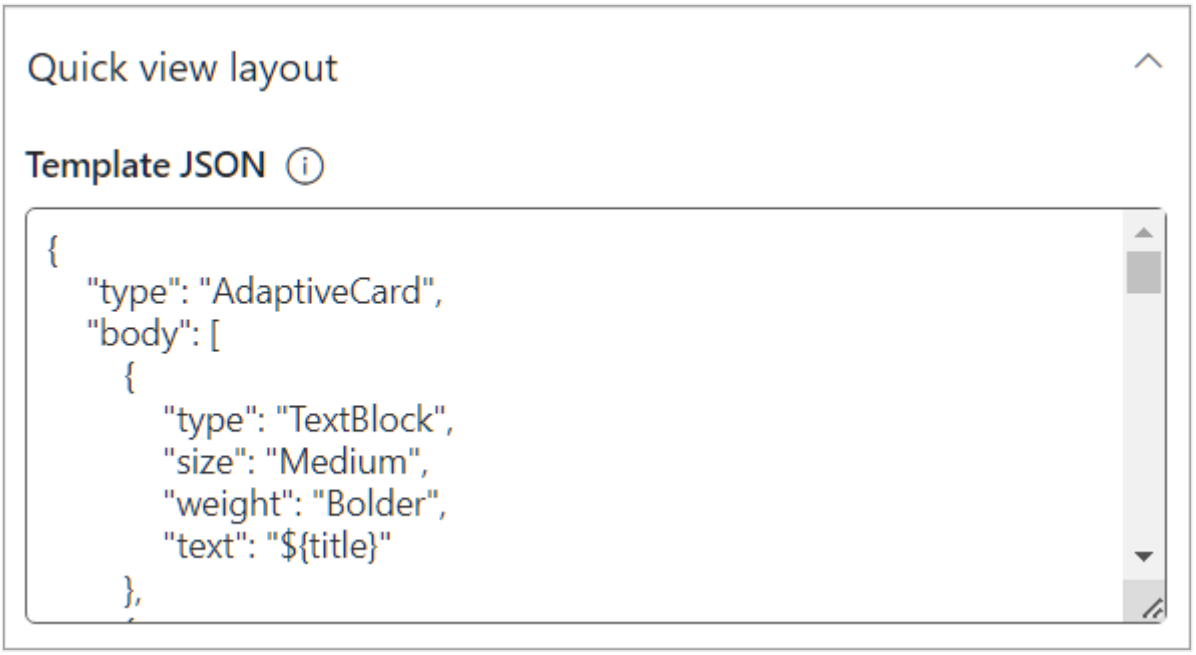
   > **Note**
   >
   > One quick view is available for each card, which can be opened as the card action, or by using a button.

3. Select **Next** to display the quick view layout.
4. A preview of how the card looks on the dashboard displays to the left of the options.



> **Note**
>
> The Adaptive Card designer tool can be used to help create the JSON Template and Data code for your card. For more information on the adaptive card structure and creating adaptive cards, see Getting Started - Adaptive Cards.

5. In the **Template JSON** field, enter your JSON code that contains the structure of your Adaptive Card.



6. Under **Type of Content**, select one of the following options for your data set:

   - **Static**: displays static information and must be manually updated.
   - **Dynamic**: integrates with data sources from SharePoint API or Microsoft Graph to automatically update content.

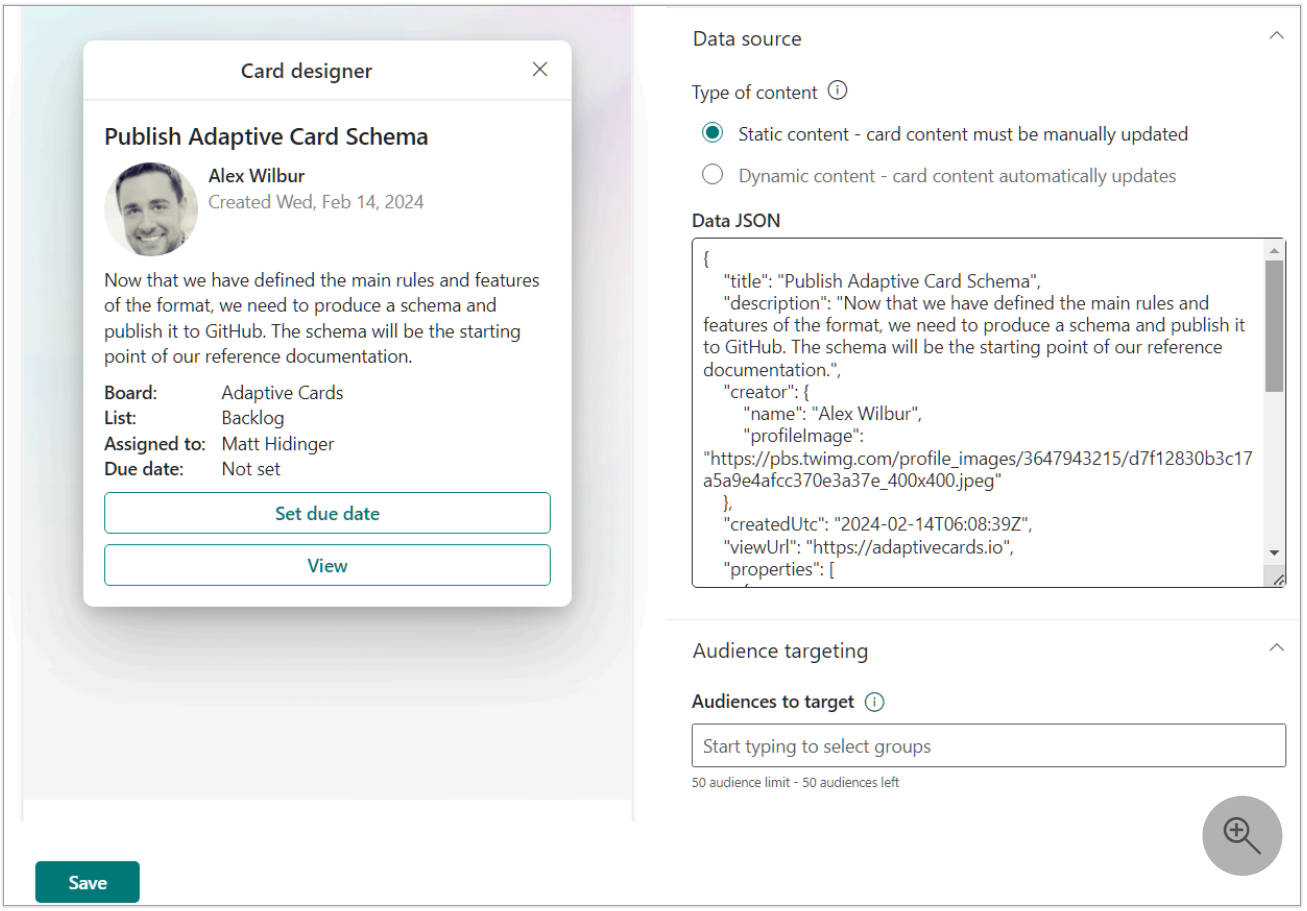
> **Note**
>
> Selecting **Dynamic** content will display additional options allowing you to select the data source and API endpoint.

Selecting Static as the type of content

1. In the **Data JSON** field, enter your JSON code that contains the data to be displayed within your Adaptive Card.

2. In the **Audiences to target** field, enter any audiences you wish to target the card to.

3. Select **Save** to your updates.



Selecting Dynamic as the type of content with SharePoint as the data source

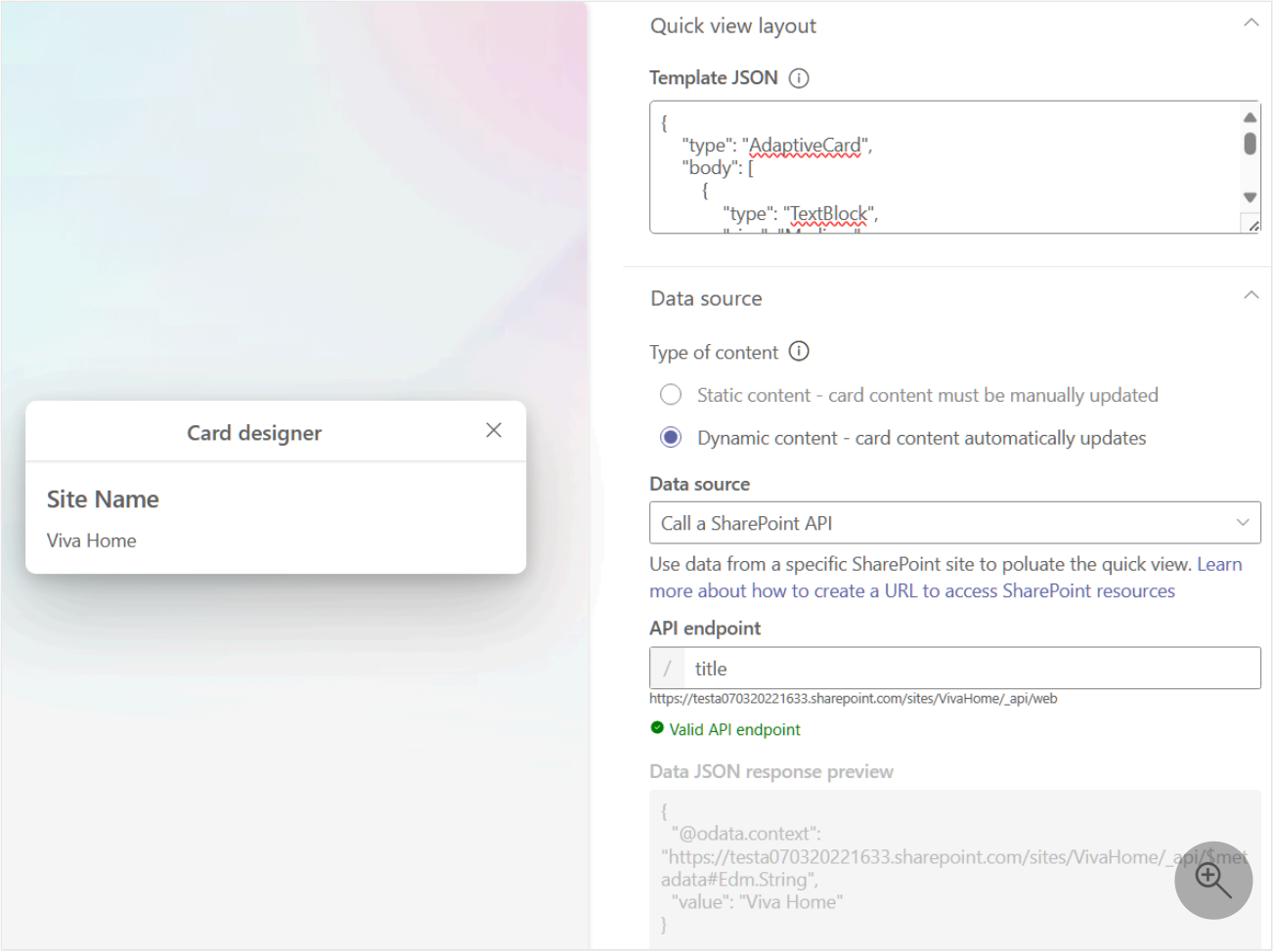
1. From the **Data Source** dropdown, select **SharePoint API**.

2. In the **API endpoint**, enter the REST URL endpoint you wish to use.

   For example, if you wanted to retrieve the title of a SharePoint site, you would enter `title` in the **API Endpoint** field (since `web/` is already part of the default prefix). See this article for more examples of SharePoint REST endpoints.

3. The **Data JSON response preview** will open and display the code used. A preview of how the card looks on the dashboard appears to the left of the property pane.

4. In the Audiences to target field, enter any audiences you wish to target the card to.



5. Select **Save** to save your updates to your custom card.

Selecting Dynamic as the type of content with Microsoft Graph as the data source

1. From the **Data Source** dropdown, select **Microsoft Graph**.

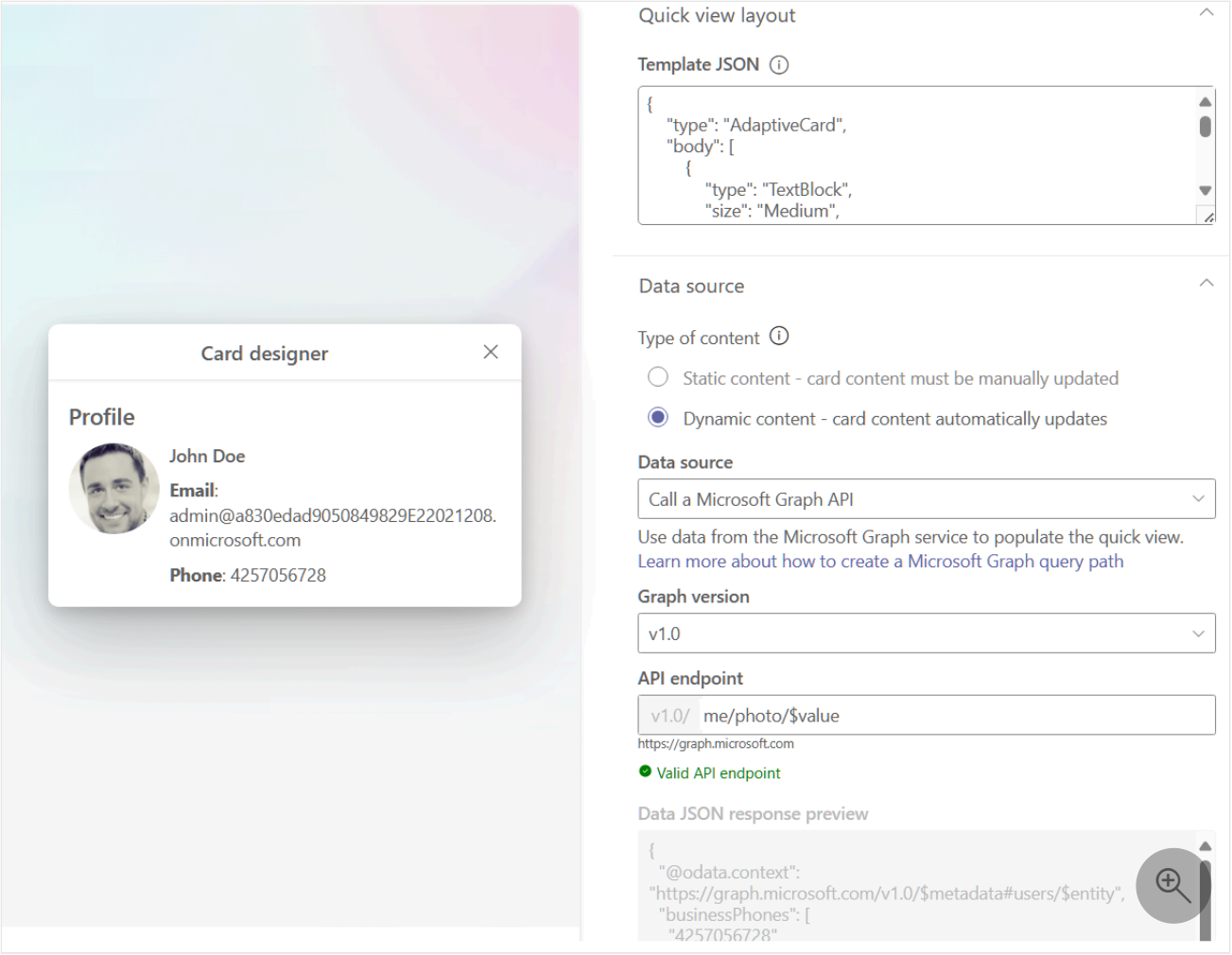
2. Select the **Graph version** from the dropdown (where version is the target service version, usually 1.0).

3. In the **API endpoint**, enter the REST URL endpoint you wish to use.

   For example, if you wanted to retrieve the profile and photo of a specific user, you would enter the Microsoft Graph REST URL `me/photo/$value` in the **API Endpoint** field. See more common use cases in 1.0 for Microsoft Graph REST API here.

4. The **Data JSON response preview** will open and display the code used and a preview of how the card looks on the dashboard appears to the left of the property pane.

5. In the **Audiences to target** field, enter any audiences you wish to target the card to.



6. Select **Save** to save updates to your custom card.

More Resources

Create a SharePoint app in Teams dashboard and add cards

Available dashboard cards

Last updated on 09/20/2026

Create a SharePoint app in Teams dashboard in more than one language

Create a SharePoint app in Teams dashboard that can be viewed in multiple languages. Start by enabling the multilingual experience, select languages, and then assign translators.

> ⓘ **Note**
>
> You must have site member level permissions or higher to edit multilingual settings.

Step 1: Navigate to the SharePoint app in Teams dashboard

Depending on whether your organization has a SharePoint home site or not determines where you go to access the multilingual settings.

1. Navigate to your organization's home site in SharePoint.
2. Select **Edit** in the dashboard section.
3. Then select **Dashboard details**.
4. Copy the link to the dashboard under **Properties** > **Name**.
5. Paste the link in a browser and then go to **Settings** in the top-right corner.

Step 2: Enable the multilingual experience and choose languages in Site settings

1. Select **Settings** from the top right, and then select **Site information**.

2. At the bottom of the site information pane, select **View all site settings**.

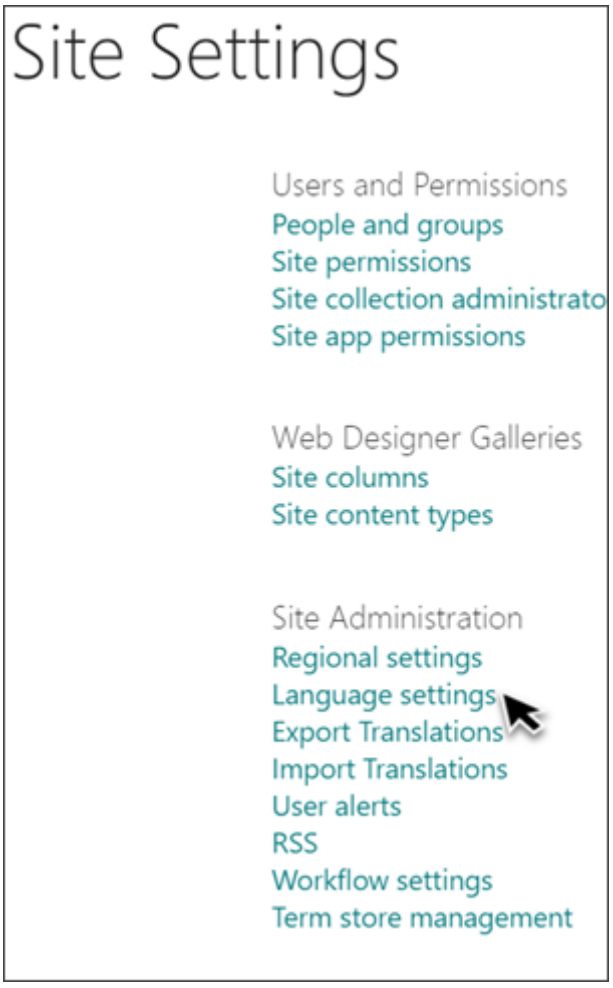
3. Under **Site Administration**, select **Language settings**.

4. Under **Enable pages and news to be translated into multiple languages**, slide the toggle to **On**.

Step 3: Select languages and assign translators

1. Under **Add or remove site languages**, start typing a language name in **Select or type a language**, or choose a language from the dropdown. You can repeat this step to add multiple languages. You can add or remove languages from your site at any time by going back to this page.

2. In the **Translator** column, start typing the name of a person you want to be a translator, and then select the name from the list.



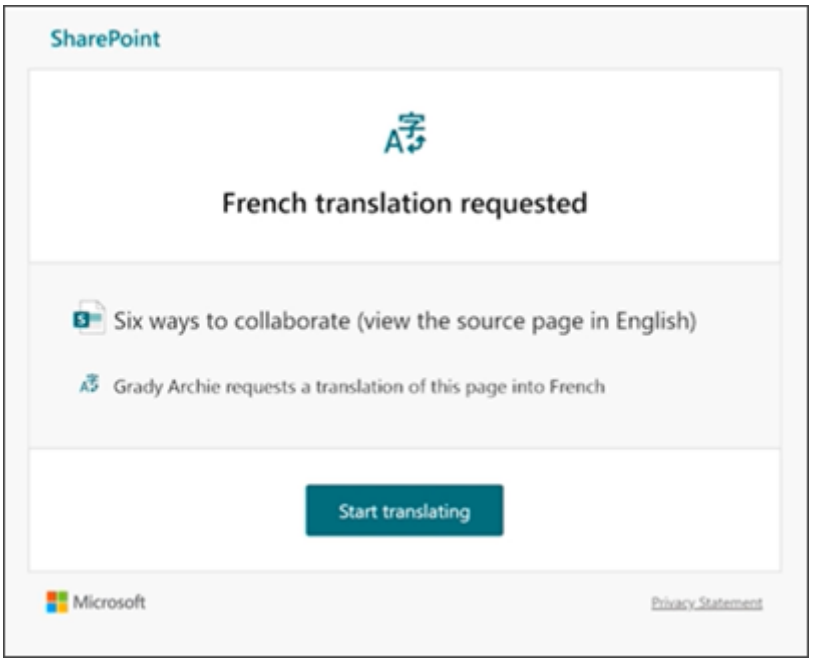
3. Select **Save**.

> ⓘ **Note**
>
> - Anyone in your organization's Active Directory can be assigned as a translator. People assigned as translators won't automatically be given appropriate permissions. When someone without edit permissions to the dashboard tries to access the site, they're directed to a web page where they can request access.
> - You can add or remove languages from your dashboard at any time by going back to this settings page.
> - The default language of a dashboard is set to the language chosen when the dashboard is created. However, when English is among the supported languages, English is treated as the preferred language if the user's preferred language isn't supported by the dashboard. This is a known issue.

Step 4: Create dashboards in specific languages

Translators manually translate copies of the dashboard into one or more languages specified. When you select a language and assign a translator, a copy of the dashboard is created, and translators are notified in an email that a translation is requested. The email includes a link to a copy of the dashboard. An email notification is sent to the person who requested the translation when it's finished. The translator will:

1. Select the **Start translating** button in the email.



2. Select **Edit** on the top right of the dashboard and translate the content.

3. When the translation is done, select **Save as draft** (if you're not ready to make it visible to readers) or, if the dashboard is ready to be visible to everyone who is using that language on the site, select **Publish**.

> ⓘ **Note**
>
> Some components of 2nd and 3rd party Dashboard cards (for example, the card name) might not be translatable.

Step 5: Add a translated dashboard name and description

1. To edit the description, from the dashboard, select **Dashboard settings** in the command bar.
2. **Edit** the dashboard description.

3. To edit the name of the dashboard, navigate to **Settings**, and then **Site contents**, and then find the translated dashboard in **Site pages**. Hover over the dashboard that you want to rename and select the ellipsis **(...)** and then select **Rename.**

Email notifications

The default dashboard owner and assigned translators receive emails when content is edited, with email notifications batched in 30-minute increments as needed. For example, after the first email related to a page is sent, and an update is made to the default language page, the next notification email or any others that need to be sent, will be batched and sent after 30 minutes.

- When a translation dashboard is created, an email is sent to one or more assigned translators to request a translation. The email includes a Start translating button.
- When a translation dashboard is published by a translator, an email is sent to the person who requested the translation.
- When an update is made to the default language dashboard and saved as a draft or is published, an email is sent to the translator to notify them that an update to the translation dashboard might be required.

More tasks for your multilingual dashboard

After creating dashboards in additional languages, you should confirm which languages are available, update translated versions, and delete translations that are no longer needed.

Confirm the languages the dashboard can be viewed in

The status of the translation of the dashboard (draft saved, published, and so on) is shown in the Translation pane next to each language. To see the status:

1. Go to the default dashboard.
2. Select **Translation** at the top of the page.
3. In the Translation pane on the right, the status of each language is shown, and a link to view the dashboard in that specific language.

Find a translated dashboard

You can use the language dropdown at the top of the page, the translation panel, or find the dashboard in the Pages library.

To find it in the Pages library, follow these steps:

1. Go to the Pages library for the home site.
2. Find the dashboard you want to delete in the language folder next to the default language page. The folder can be identified by its two or four letter language code. For example, the French folder is identified as "fr."

Delete a version of the dashboard for a specific language

To delete a translated dashboard, you must perform a few extra steps to break the association between the default language dashboard and the deleted dashboard.

1. Go to the **Pages library** for the dashboard.
2. Find the version of the dashboard you want to delete in the language folder next to the default language page. The folder can be identified by its two or four letter language code. For example, the French folder is identified as "fr."
3. Select the dashboard you want within the folder, and then select the ellipsis (...) to the right of the selected page.
4. Select **Delete**.
5. After you've deleted the version of the dashboard that’s no longer needed, go to the default language dashboard, and select **Edit** at the top right. If you aren't in edit mode, the rest of the steps won't work.
6. Select **Translation** at the top of the page.
7. In the Translation panel, you should see a message indicating that an association with the page has been removed.
8. **Republish** the default language dashboard.

Update the dashboard with new changes or edits

Make changes as needed over time to the dashboard and select **Save as draft** or **Republish**. Then, the translators for the translated dashboard are notified in email that an update has been made so updates can be made to the individual translation pages as well.

Update the default language page

When the default language dashboard is updated, it must be republished. Then, the translators for the translated dashboard are notified in email that an update has been made so updates can be made to the individual translation pages. Translators need to view the version history of the default dashboard to see what content has changed.

Translated dashboards in the Dashboard web part

The Dashboard web part can be used once the dashboard has been published. The Dashboard web part will display in the users preferred language (if different from the default language) if a translated dashboard has been provided.

> **Note**
>
> - Translation dashboards must be approved and published before they appear.
> - Some components of partner dashboard cards (like the card name) might not be translatable.

More resources

Set up the SharePoint app in Teams experience in a specific language

Edit the SharePoint app in Teams dashboard

Create multilingual SharePoint sites, pages, and news

Last updated on 09/20/2026

SharePoint app in Teams News notifications

The SharePoint app in Teams delivers News notifications via Microsoft Teams and links users to the SharePoint in Teams app through the notification. This document describes when notifications are sent, and the conditions that need to be met for receiving notifications.

When notifications are sent via Microsoft Teams

News notifications are delivered via Microsoft Teams in the desktop, mobile, and web environments in the following scenarios:

- News is published to a SharePoint team or communication site a user follows or by someone a user works closely with.
- News that is targeted to a user is boosted.
- Someone comments on a new News post that a user posted.
- Someone "Likes" a News post that a user posted.
- Someone is @mentioned in a comment on a news post that a user posted.

> **Note**
>
> - Notifications are pulled from the top 100 collaborators that an author works with. If an author works with more than 100 collaborators, the most relevant notifications will be pulled.
> - Authors can set an audience on their news posts and notifications will honor the audience that is set. Only users part of the selected Microsoft 365 audience(s) specified receive notifications. Learn more about audience targeting in SharePoint.
> - Notifications triggered when a News link is published will be available only on Microsoft Teams mobile.

Who receives notifications and when

End-users only receive notifications through Microsoft Teams when the following conditions are met:

1. The SharePoint app in Teams is installed for Microsoft Teams.

2. Notifications are enabled in the Teams mobile app and are enabled in the notification settings option in Teams desktop.
3. The notification is outside of the user's set quiet hours as configured in Microsoft Teams.
4. The user has permissions access to the news post.
5. The user is part of the selected Microsoft 365 audience if Audience targeting is enabled for the news post.

Once these conditions are met, end-users receive a notification when news is published by someone they work closely with, or a site they follow. Authors also receive notifications when posts they publish are liked or commented on.

End-users receive notifications when

- A SharePoint news page is published to a site you follow.
- A SharePoint news page is published by someone you work closely with.
- A SharePoint news page is boosted, and the user is part of the audience target.
- You're "@mentioned" in a comment left on a SharePoint news page.

Authors can receive extra notifications when posts they publish are liked or commented on.

Authors receive notifications when

- A user 'likes' a SharePoint news page the author created.
- A user comments on a SharePoint news page the author created.

After an author receives a notification of either of these type, the SharePoint app in Teams will batch more notifications of the same type. After the first comment notification to a user, Comments are batched in 20-min intervals. After the first like to a user, likes are batched in 60-min intervals.

How can notifications be controlled?

The SharePoint app in Teams notifications follow the Microsoft Teams notification settings, including Quiet Hours settings, and are only sent if users have the SharePoint app in Teams installed.

> **Note**

There is no organization-wide method for an administrator to control the SharePoint app in Teams notifications.

Users can control what notifications they want to see in the following ways:

- On Teams desktop and web, specific notification types can be selectively enabled or disabled under **Settings** > **Notifications and activity** > **SharePoint**. These settings are respected on Teams mobile as well.
- On Teams mobile, notifications can't be selectively enabled or disabled, but users can toggle all push notifications in the Teams mobile app:
  - For iOS: **Settings** > **Notifications** > **Custom** > under **Notify me for** > **Apps on Teams**.
  - For Android: **Settings** > **Notifications** > **Custom** > under **Teams - General** > **Apps on Teams**.

    Notifications will still be visible under the Microsoft Teams activity feed.

Frequently Asked Questions

What defines 'people I work with'?

You can read more about how this list of people is determined and how to disable it in this documentation.

How do notifications work?

If the user selects a notification from their home screen within Microsoft Teams, or from the Microsoft Teams activity feed, the notification takes the user directly to the source news post within the SharePoint app in Teams.

Will SharePoint app in Teams users be notified every time a user reacts to a news post?

No. Only authors who created the news post receive notifications when someone likes or comments on a post.

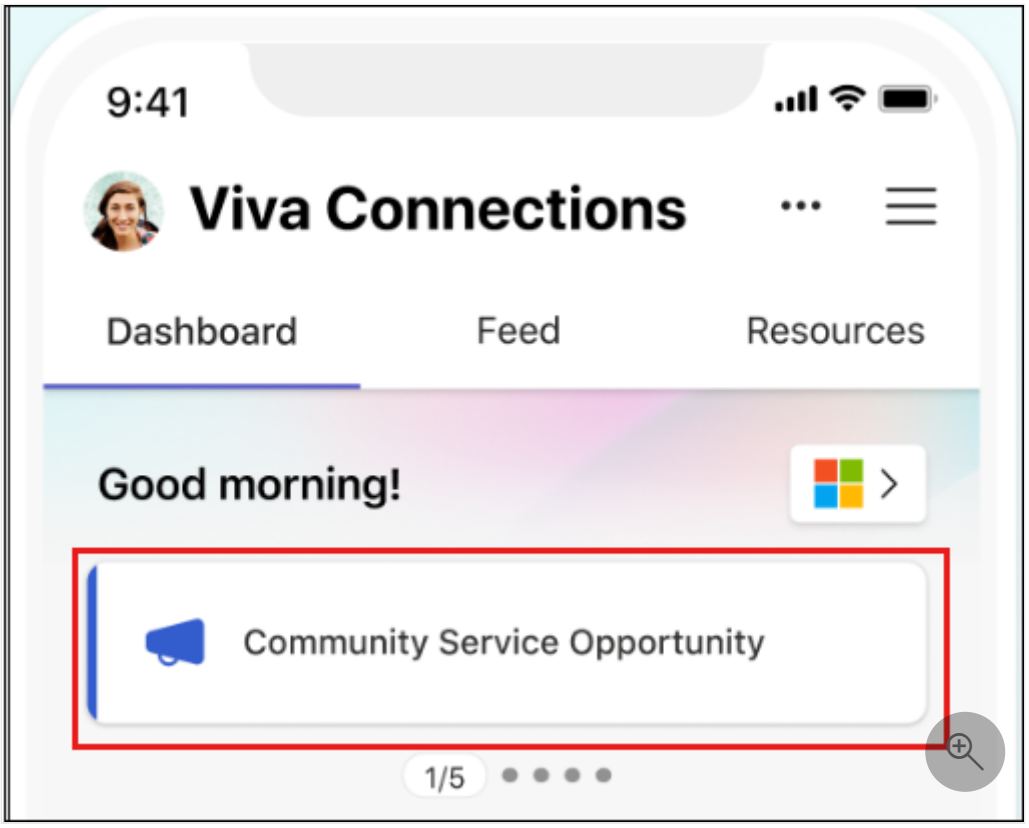
Why isn't boosted news displaying in the Top News Card?

It can take up to 24 hours for boosted news created from those sites to appear in the Top News card in the SharePoint app in Teams dashboard.

Last updated on 09/20/2026

Use announcements in Viva Connections

Announcements allow you to create, manage, and schedule time-sensitive messages in Connections to users in your organization, all from your Connections experience.



> ⓘ **Note**
>
> - Only email-enabled security groups are supported.
> - You must have edit permissions or higher to your organization's SharePoint home site or Viva Connections to author and manage announcements.
> - Announcements are unavailable in GCC, GCC High, and DoD environments. For more information, see the list of platform features in Viva Connections.

When to use announcements

Announcements are the best way to communicate targeted, time-sensitive information in the Connections app. Some examples include:

- To remind users of a specific role about upcoming deadlines, like time sheets, application deadlines, etc.

- To share details about open enrollment benefits with a link to your organization's Human Resources website.
- To send a specific call to action for new users, such as reminders of required security trainings, morale events, etc.

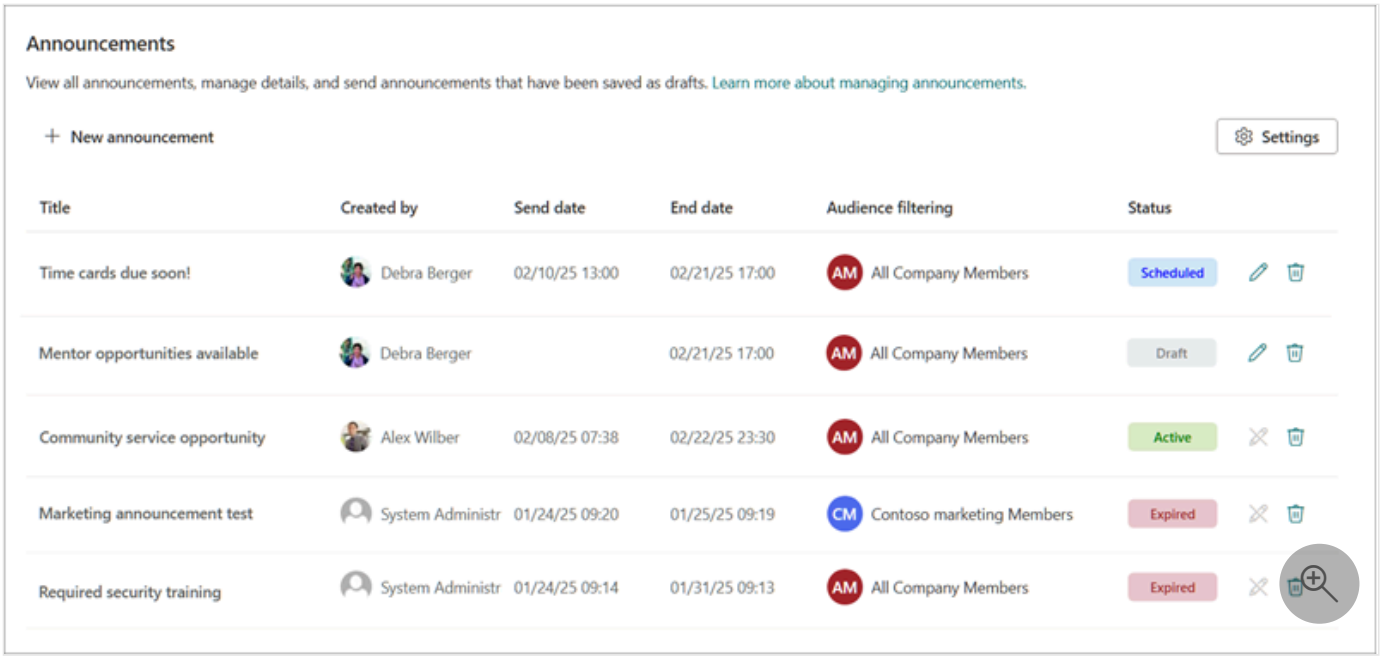
> **Important**
>
> For emergencies such as a safety hazard, it's recommended to use multiple modes of communication.

Best practices for using and writing announcements

- Announcements aren't designed for life-threatening emergencies.
- Keep messages short with a clear call to action. Provide a link to more information for more complex topics.
- Use audience targeting to specify which audiences need to receive the announcement to ensure the highest engagement possible.
- Use announcements sparingly so that users understand their importance. Sending them too frequently can cause users to disregard the notifications.
- Allow users to dismiss announcements for less-urgent topics or when there are several high priority announcements active at the same time.
- The delivery time increases with the size of the targeted audience. Sending an announcement to a group of 50 users might take a few minutes but sending one to 100,000 users can take several hours.

Manage announcements from the announcements page

You can view, create, and manage all announcements (active, scheduled, drafts, and expired) from the Announcements page from your Connections experience or SharePoint home site.



To access the announcements page in Connections:

1. Select the **ellipsis** (•••) in the upper-right of the Connections experience.
2. Select **Manage announcements** from the list.
3. The announcements page opens where users can select + **New announcement** to begin drafting an announcement.

To access the announcements page from the SharePoint home site:

1. Select the **Settings icon** ( ) in the upper-right of SharePoint to open settings.
2. Select **Manage Viva Connection**.
3. Select **Manage Announcements**.
4. The announcements page opens where users can select + **New announcement** to begin drafting an announcement.

Create a new announcement

When creating a new announcement, you can choose up to 10 audiences to send to, set an expiration date, schedule a future send date, provide a link to users for more information, and allow users to dismiss the announcement.

1. From the Announcement page, select + **New Announcement**.

> ⓘ **Note**

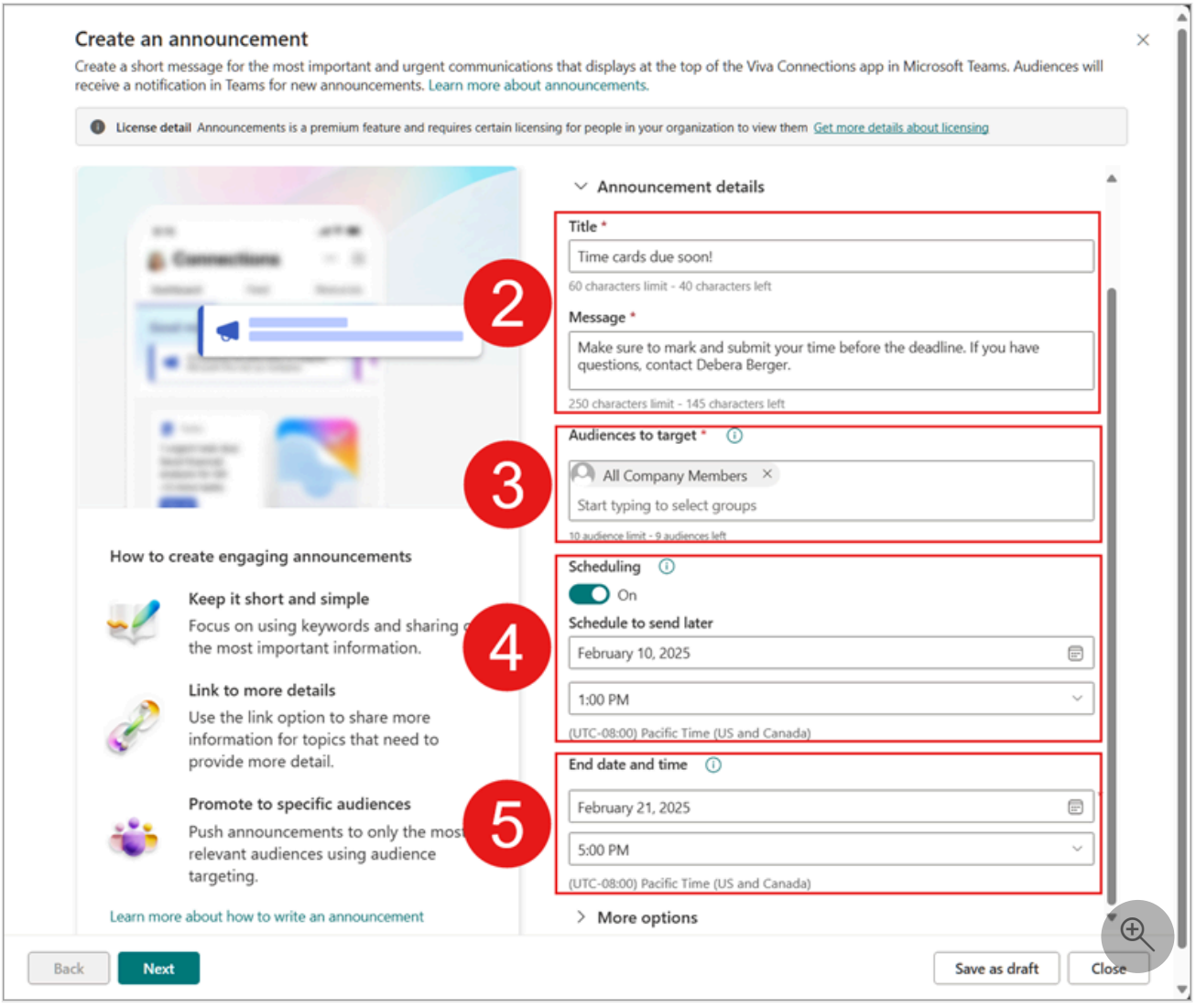
You can also create a new announcement from your SharePoint home site by selecting **+ New**, then select **Announcement** to begin creating your announcement.

2. Add a **title** and **message**.

3. Select up to 10 audiences to distribute the announcement to. Audiences can be Microsoft Entra groups, Microsoft 365 Groups, or Microsoft Entra dynamic groups.

4. To schedule the message, enable **Scheduling** and enter the **date** and **time** the announcement should be set (Scheduling is off by default and the scheduling date and time fields only display if scheduling is enabled).

5. Select an **end date and time** (up to two weeks from posting) for the announcement to expire. Expired announcements won't display to users.

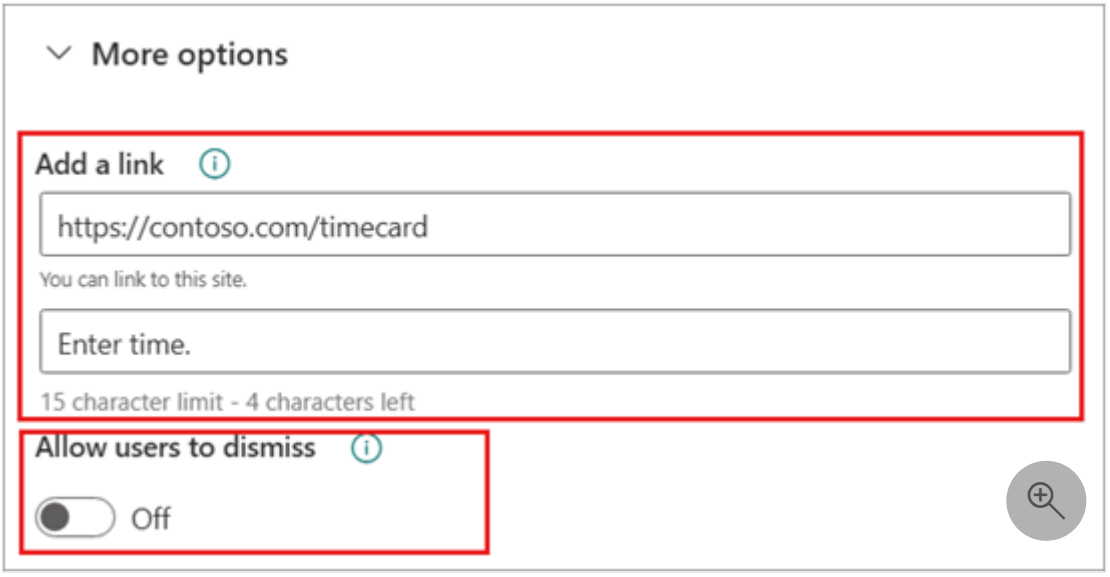


ⓘ Note

At any time while creating your announcement, you can select **Save as draft** to save the announcement as a draft and work on it later from the announcement page.

6. Under **More options**, you can **add a link** to more information. Enter a URL and label for the link.

7. To allow users to dismiss the announcement after viewing, enable the **Allow users to dismiss setting**.

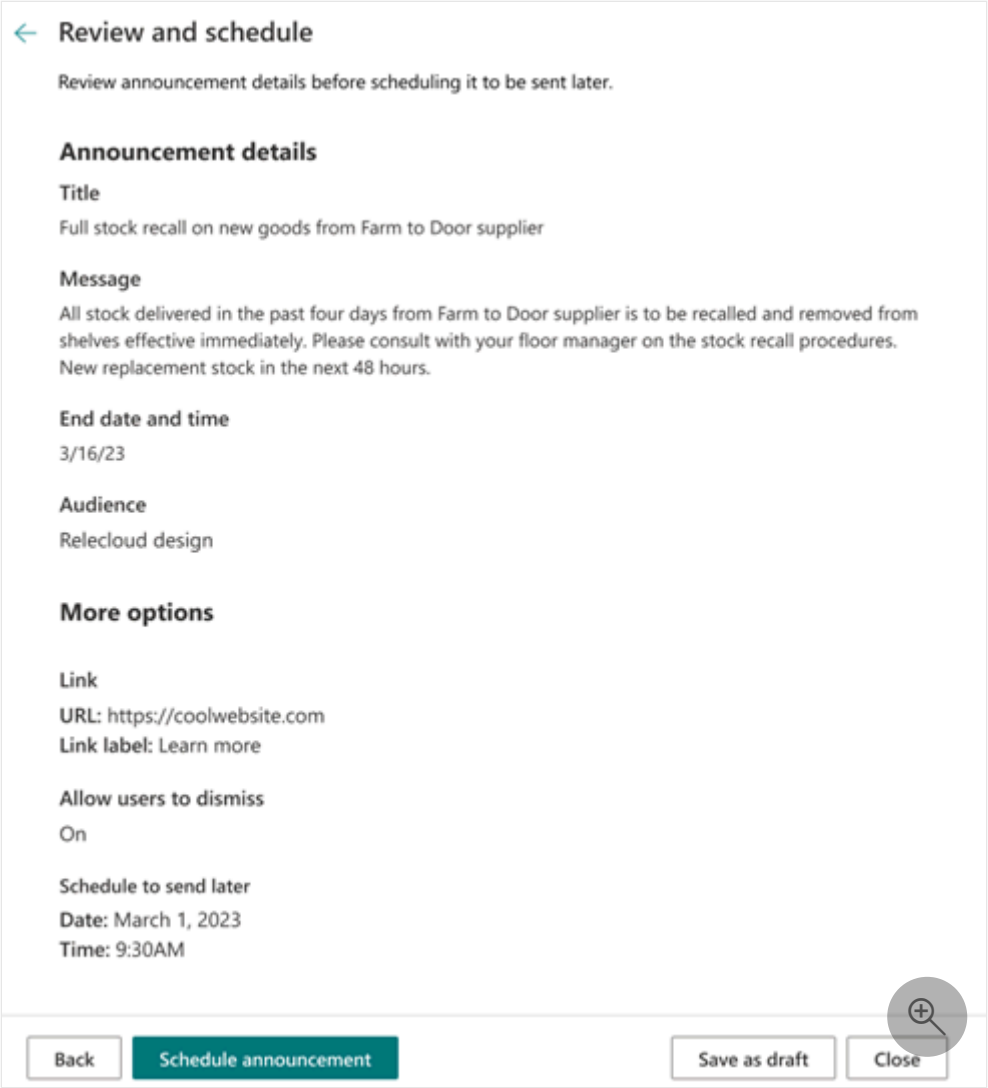


8. Select **Next** to review the details of your announcement.

9. Select **Send announcement** when you're ready to send.

   If the announcement is scheduled for a future date, send announcement will instead become **Schedule announcement**.

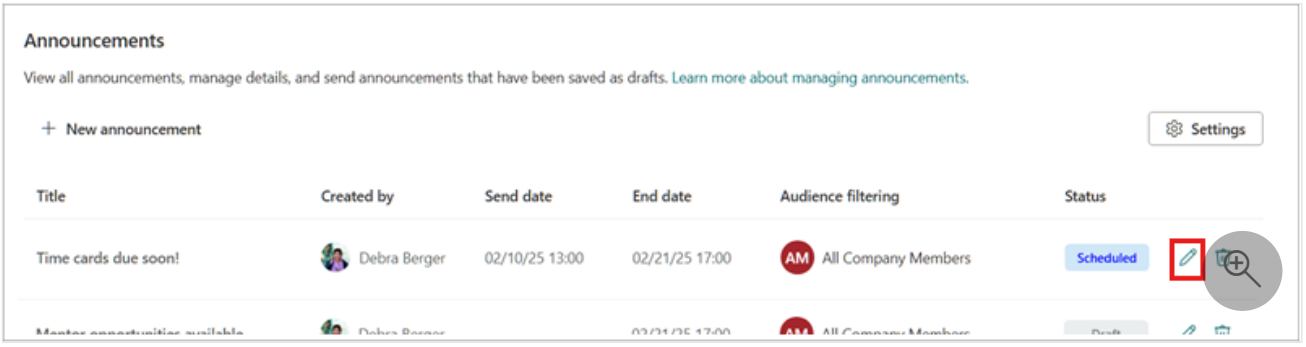
> **Note**
>
> Once an announcement is sent, message details and end date can still be edited.



Edit an active, scheduled, or draft announcement

1. Access the **Announcements** page.

2. Select the **pencil** icon next to the announcement you want to edit.



3. Make any desired changes in the **Announcement details**, then select **Next**.

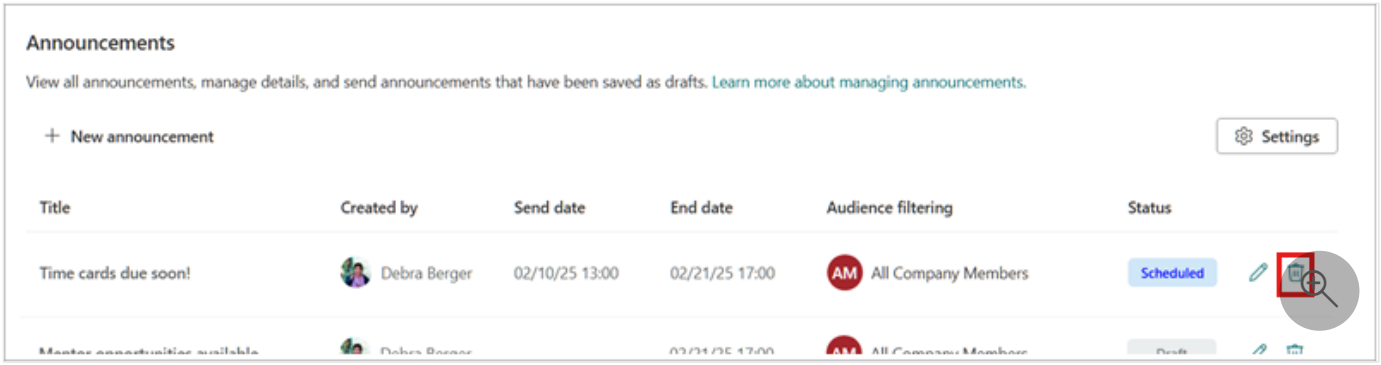
4. Choose to send, schedule, or save as draft to apply your edits.

Delete an announcement

1. Access the **Announcements** page.

2. Select the **trashcan** icon next to the announcement you want to delete.

> ⓘ **Note**
>
> Deleted announcements can't be recovered.



3. When prompted, choose **Yes, delete**.

4. If the announcement was active, users won't be able to view it, but might still be accessible through a Teams notification.

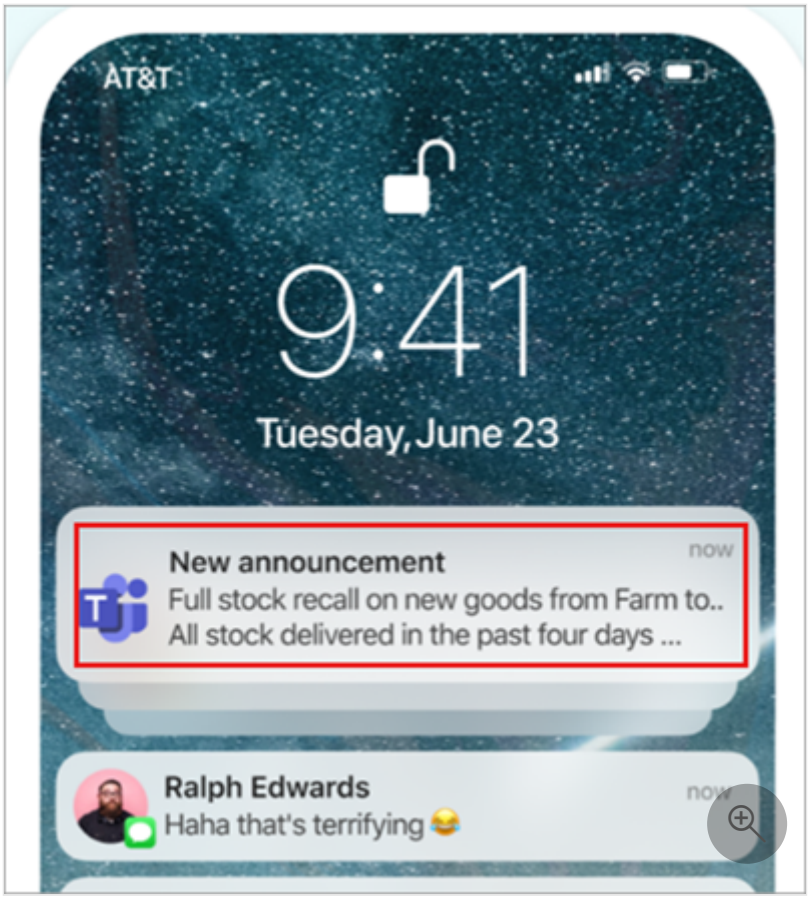
How announcements display in Connections

Announcements sent to users appear differently depending on if they're accessing their Connections experience from a mobile, tablet, or desktop device.

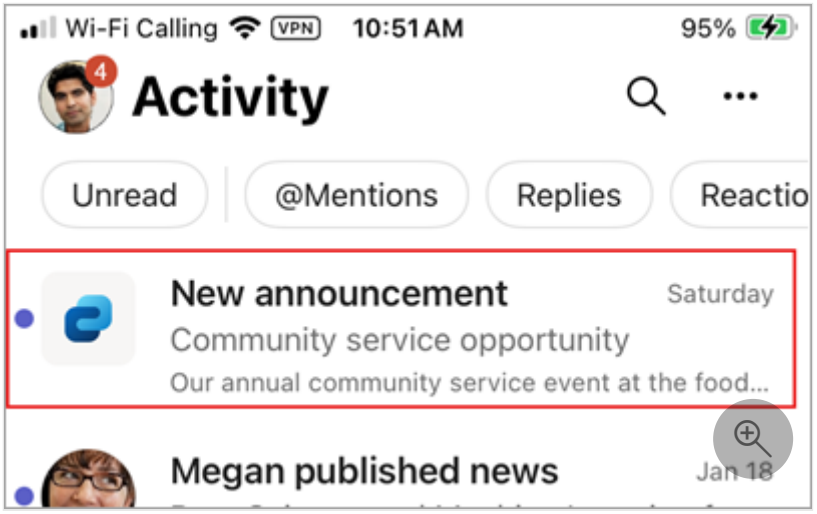
> ⓘ **Note**
>
> For details on how announcements display for frontline workers, see the section on Teams Channel announcements in Viva Connections.

How announcements display on mobile and tablet devices

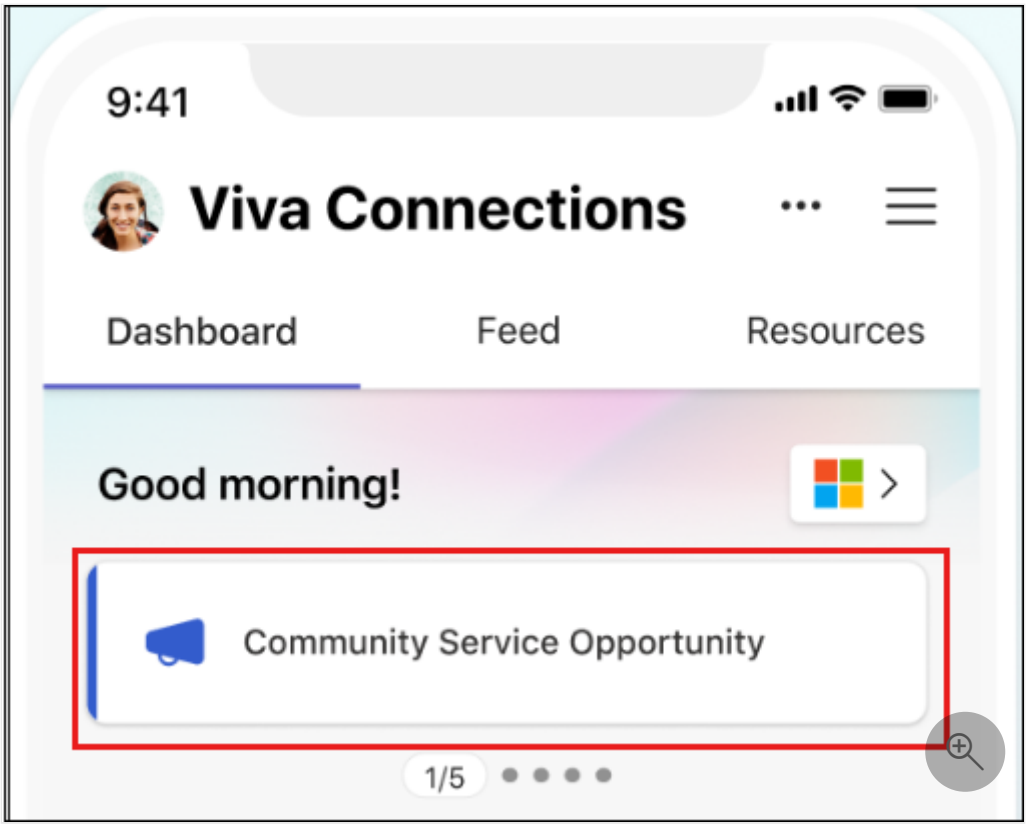
In the Teams mobile app: Users get a Teams notification displayed on the lock screen of their mobile device alerting them of a new announcement (Teams notifications must be enabled by the user).



Users can also see the announcement appear under the **Activity** tab in Microsoft Teams. Selecting the announcement opens it in the Connections app on the Teams mobile app.

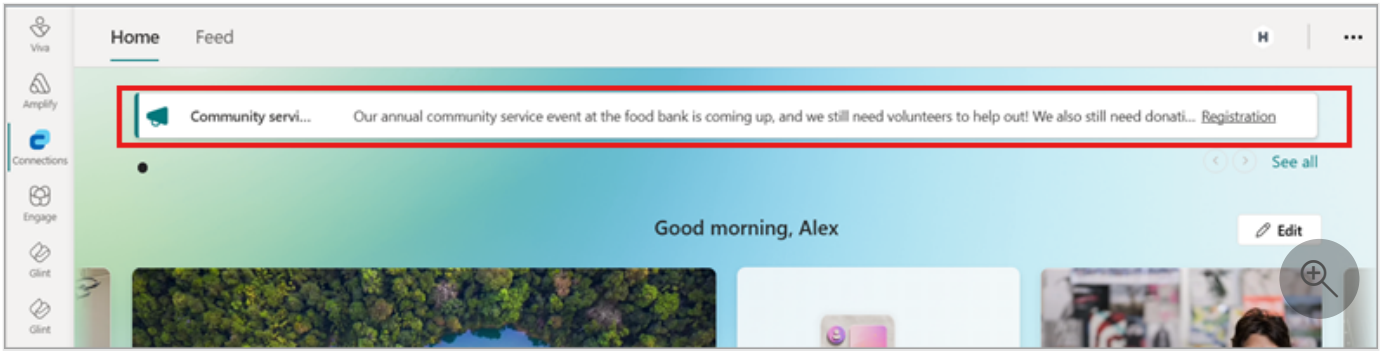


From the Connections app in Teams mobile: Announcements display at the top of the Connections mobile experience.

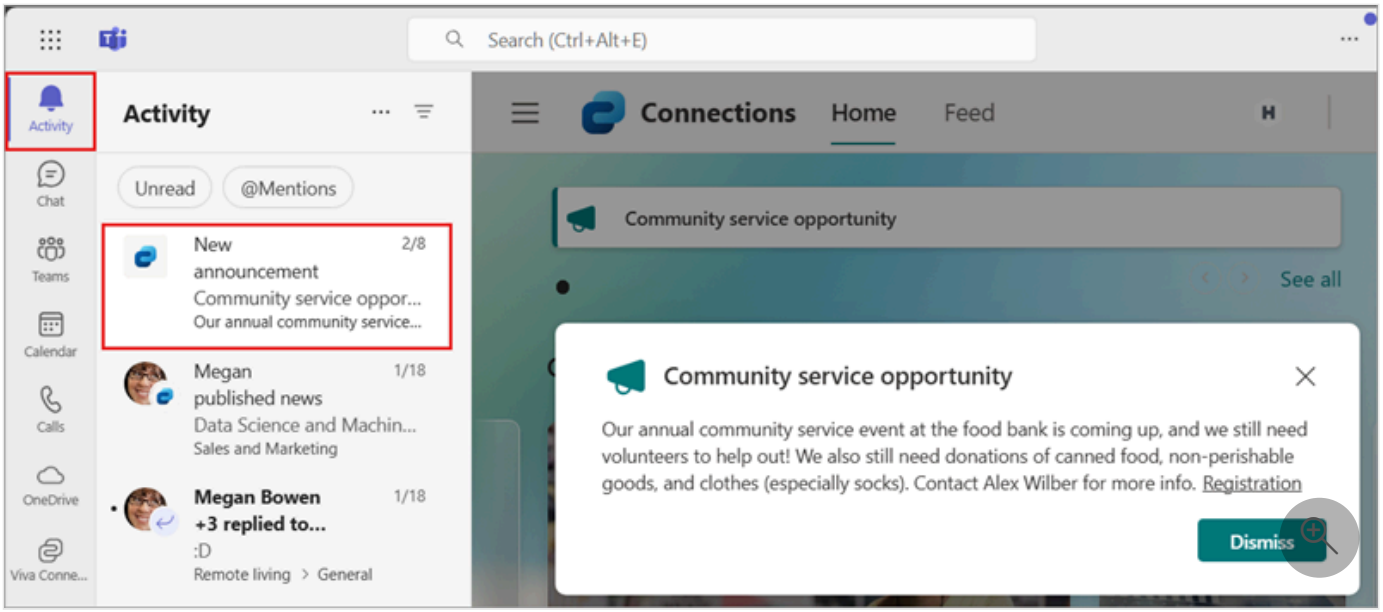


How announcements display on desktop

When users access their Connections experience through SharePoint, Microsoft Teams, or the Viva Home suite, announcements display above the news spotlight.



When in Microsoft Teams, the announcement also appears in the **Activity** tab. Selecting the announcement opens it within the Connections experience.



Announcements for frontline workers

The following section covers topics related to sending announcements to Frontline workers. Learn how to:

- Use @mentions in a Teams channel to send an announcement in Connections to Frontline workers.
- Target announcements to Frontline workers based on job attributes (location, title, etc.).
- How to map Frontline attributes to workers
- How to enable regional filtering.
- How to filter announcements based on Frontline worker attributes.

How @ messages in a Teams channel display as an announcement in Connections for frontline workers

Frontline managers can communicate important updates to Frontline workers in Connections by using their Teams channel. Adding an @mention in the Teams channel message displays it to Frontline workers as an announcement in Connections across desktop and mobile experiences.

Frontline workers can then select the link within the Connections announcement to be redirected to the Teams channel where the announcement was made.

A Teams channel announcement is displayed in the Connections experience only if:

- The user is assigned a Microsoft 365 F1 or F3 license; and

- Channel mentions are enabled under the Teams channel notification settings; and
- The Teams channel announcement is tagged with an @mention and is unread.

For more information, see sending an announcement to a channel in Microsoft Teams.

> **Note**
>
> - If you have authentication issues, disable the **Limited-access user permission lockdown mode** under site collection features from your SharePoint site. Learn more about enabling or disabling site collection features.
> - Vanity domains aren't supported. Contact your organization's support team for more information.
> - An update to an existing Teams Channel announcement won't display in Viva Connections. Users need to follow the link from the original announcement in Viva Connections to view the Teams Channel announcement.
> - Teams Channel announcements that are deleted and then undone show as unread.

Target announcements to frontline audiences based on department, location, and job title

Managers can now send targeted announcements based on a user's department, location, and job title to frontline workers on a time-sensitive basis using Regional filtering.

Before Regional filtering can be enabled, Dynamic Teams at Scale (DTAS) and your organizations Hierarchy needs to be set up within the Teams admin center in order for the proper information to be available to filter.

> **Note**
>
> - It's recommended to set up DTAS and your Hierarchy configuration before using this feature to avoid users receiving an error.
> - After DTAS and your Hierarchy are configured, regional filtering must be enabled in Connections.

Map frontline attributes in the admin center

There's some preliminary configuration required before regional filtering can be enabled in Connections.

1. First, your organization needs to set up DTAS within the Teams admin center.
2. If DTAS is set up for your organization, you need to set up your frontline operational hierarchy through a CSV file uploaded to the Teams admin center. The CSV file enables you to map your organization's structure of frontline teams and locations to a hierarchy.
3. After the hierarchy is in place, you'll be able to map your frontline attributes to the Microsoft Entra ID attributes that represent your organization's departments and job titles.
4. Your final step is to enable regional filtering in Viva Connections.

For more information, see the article on deployment of frontline dynamic teams at scale.

To get started creating your CSV hierarchy file

1. In the left navigation of the Teams admin center, choose **Teams** > **Manage frontline teams**.
2. Go to the **Operational hierarchy tab**.
3. Choose **Get Started**. The **Operational hierarchy** pane opens, and from here, you can upload your hierarchy CSV file or download a CSV template to create one.
4. Select **Download the CSV template** to create your file.
5. After creating the file, return to the **Operational hierarchy tab**.
6. Choose **Get Started** and upload your CSV file.

For more information, see the article about deploying your frontline operational hierarchy.

To map frontline attributes

Map your attributes on the Map frontline attributes page of the deploy frontline dynamic teams experience. Select the Microsoft Entra attribute for **Department** and **Job title** that best represents the departments and job titles in your organization. You can map one or both attributes.

For more information, see the article on setting up for targeted communications for your frontline.

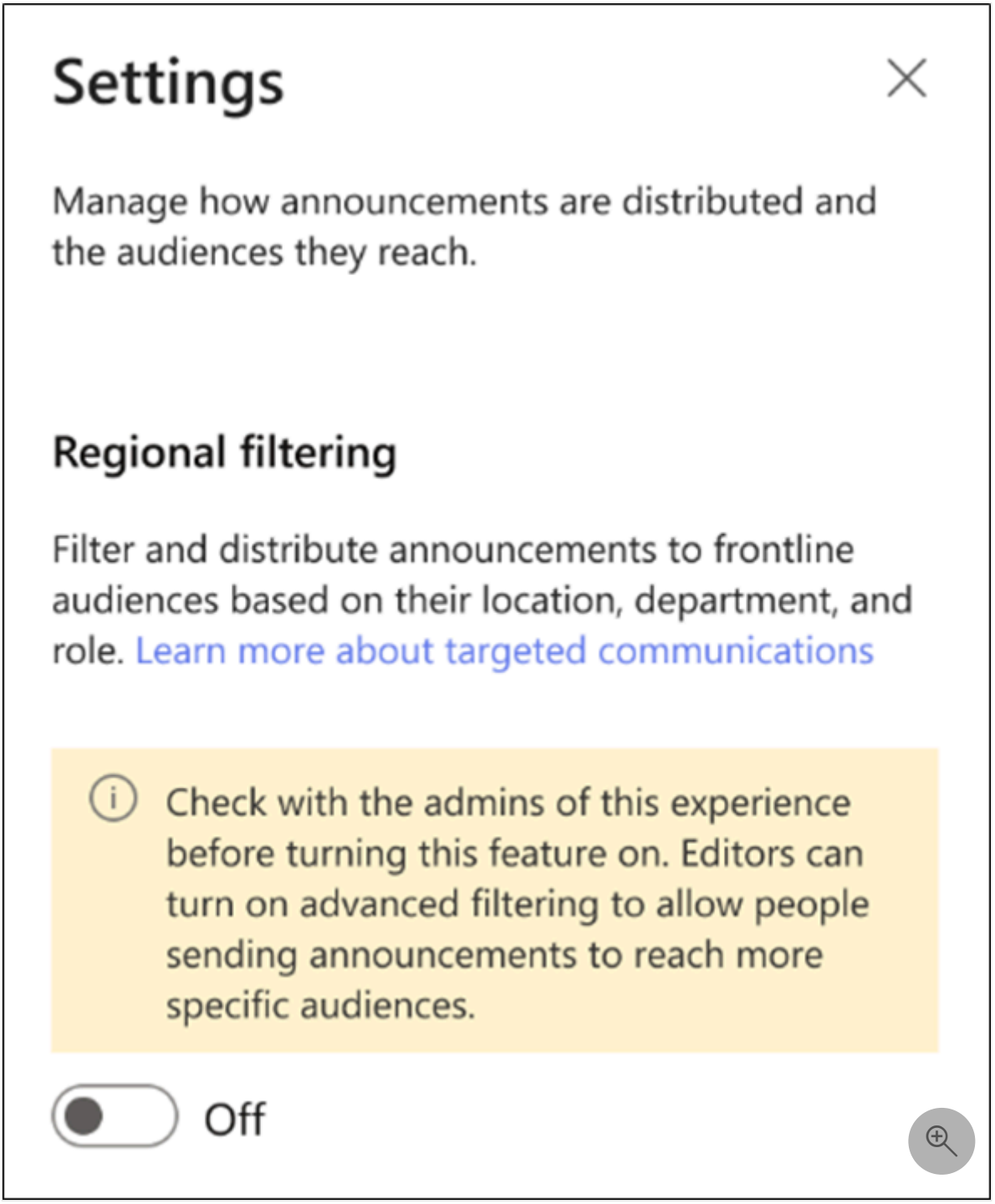
Enable Regional filtering

After the DTAS and Hierarchy service is configured in Microsoft Teams, enable **Regional filtering** within the Announcements page in Viva Connections (or from your SharePoint home site).

To enable from Viva Connections:

1. After accessing the announcements page, select **Settings** in the upper-right corner of the page.

2. In the Settings pane, select the toggle to enable **Regional filtering**.



3. Select **Save** to save your changes.

To enable from a SharePoint home site:

1. After accessing the announcements page, select **Settings** in the upper-right corner of the page.
2. In the Settings pane, select the toggle to enable **Regional filtering**.
3. Select **Save** to save your changes.

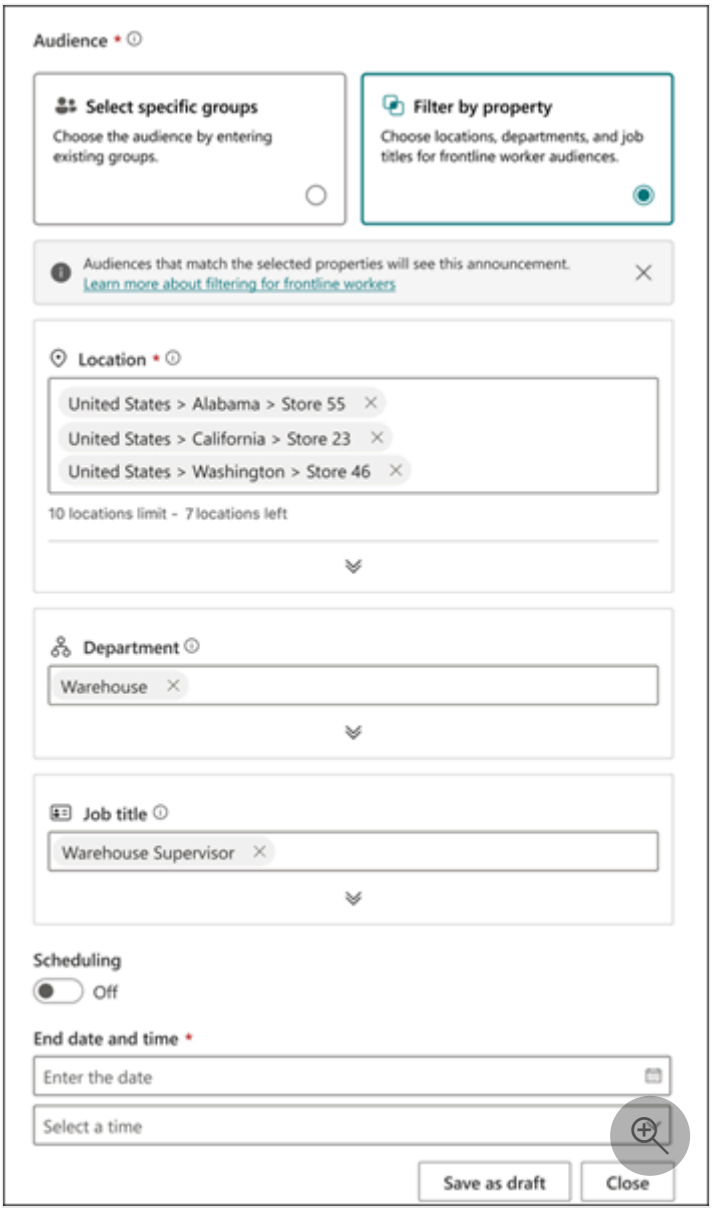
Filter announcement by Frontline worker properties

After location, department, and role values have been set up in Microsoft Teams, and regional filtering is enabled in Viva Connections, owners and members will see options to filter their announcement based on the new set of frontline worker properties created in Microsoft Teams.

To create an announcement filtered by frontline worker properties, follow the steps for creating your announcement up to selecting your audience:

1. Select **Filter by property**.
2. Select from three properties to enable announcement filtering based on the following variables:

- **Location**: enter a location in the text field to filter down based on available choices or select the drop-down arrows to choose multiple locations from a list of available options. Up to 10 locations can be selected.
- **Department**: enter a department in the text field to filter down based on available choices or select the drop-down arrows to choose multiple departments from a list of available options.
- **Job title**: enter a job title in the text field to filter down based on available choices, or select the drop-down arrows to choose multiple job titles from a list of available options.



3. Continue creating your announcement until you're ready to send.

Last updated on 09/20/2026

Configure the SharePoint app in Teams

The SharePoint app in Teams configuration flow gives home site owners control over how the app appears for everyone in their organization — both on mobile and desktop. Home site owners can choose which tabs are shown, the order they appear in, and whether the desktop experience opens with the home site or the preset layout.

> ⓘ **Note**
>
> - You must be a **home site owner** to access the configuration flow.
> - Configuration changes apply to **all users** associated with your home site.
> - The configuration flow is accessed through the home site settings.

What is the configuration flow?

The configuration flow is a settings experience built into your SharePoint home site. It lets home site owners make two key decisions:

Use the configuration flow to:

- Control which tabs appear in the SharePoint app in Teams on **mobile** and in what order.
- Choose whether the SharePoint app in Teams on **desktop** opens with your home site as the landing page or defaults to the preset railed experience.

Once a home site owner saves a configuration, it takes effect for all users associated with that home site. No per-user configuration is required.

Access the configuration flow

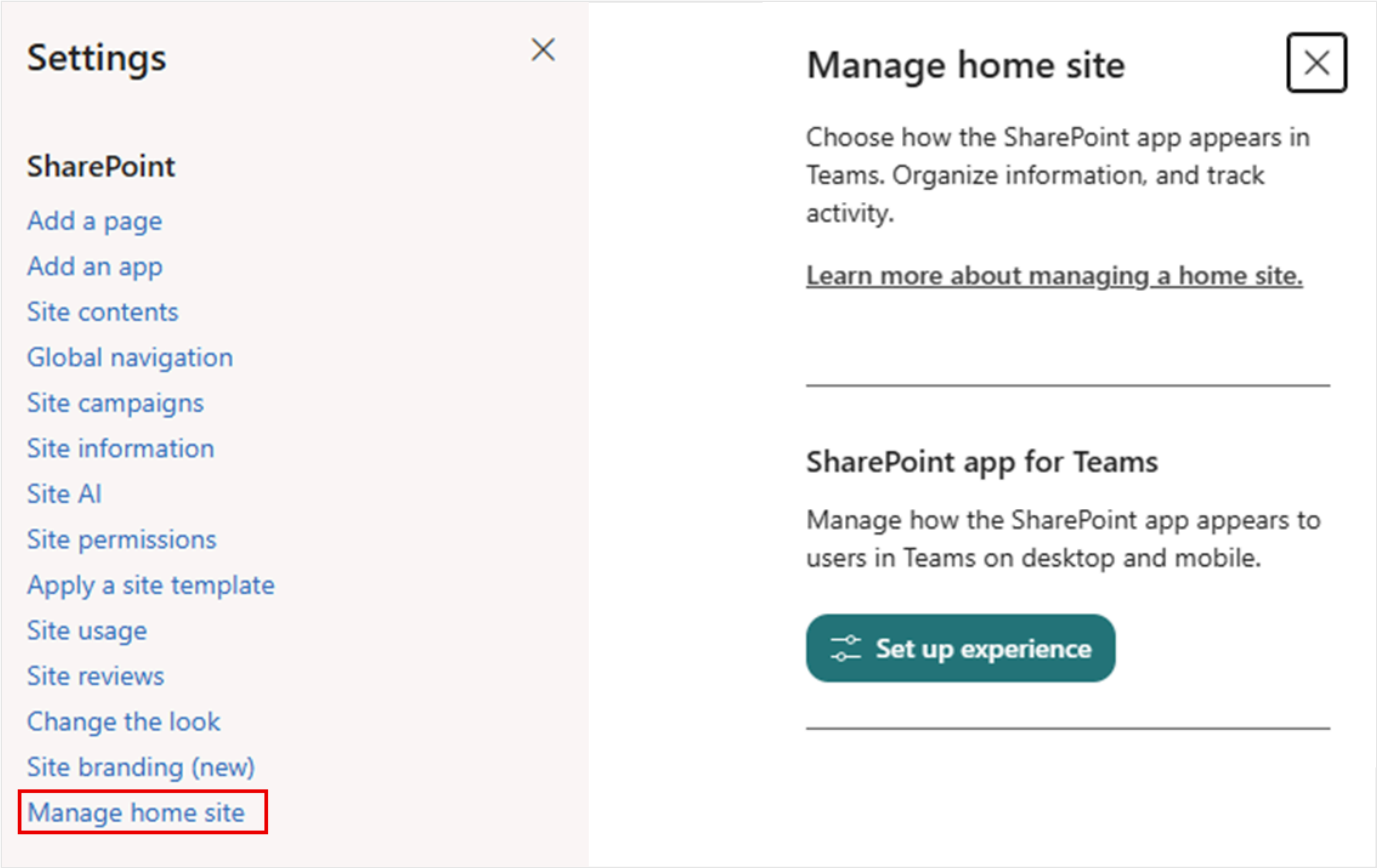
To open the configuration flow, navigate to your organization's home site and follow these steps:

1. Select the **Settings cog** on the home site.

2. Select **Manage home site**.

3. Select **SharePoint app for Teams**.

   This opens the configuration panel where you can set preferences for both the mobile and desktop experiences.



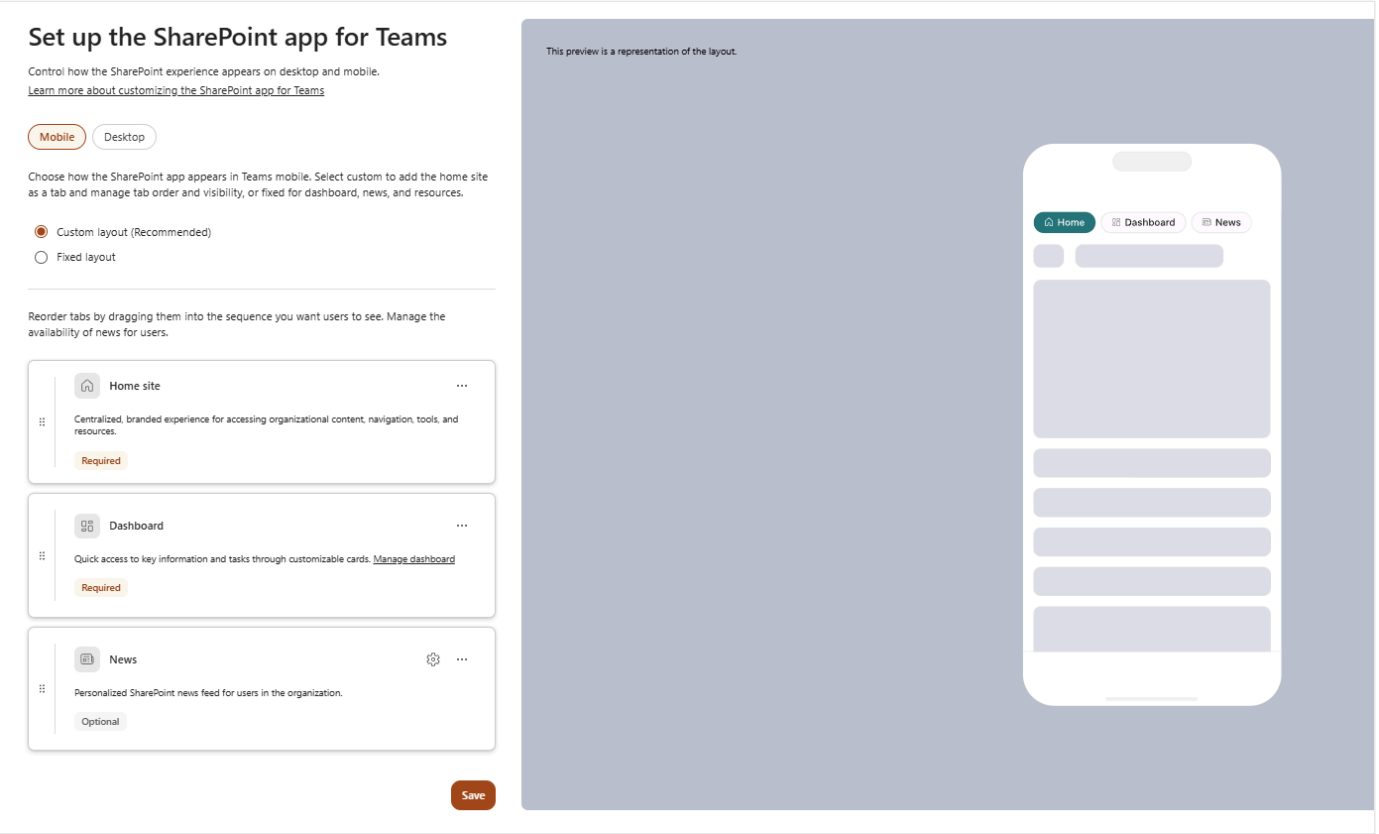
Configure the mobile experience

The mobile configuration controls which tabs appear in the SharePoint app in Teams on mobile devices and in what order. There are two layout options to choose from.

Custom layout (recommended)

The custom layout gives home site owners flexibility to tailor the mobile experience for their organization.

- **Tabs included**: Home, Dashboard, and News — in any order you choose.
- **Reorder tabs**: Use drag and drop to arrange the tabs in your preferred order.
- **Optional**: Hide the News tab if it isn't relevant to your organization's experience.

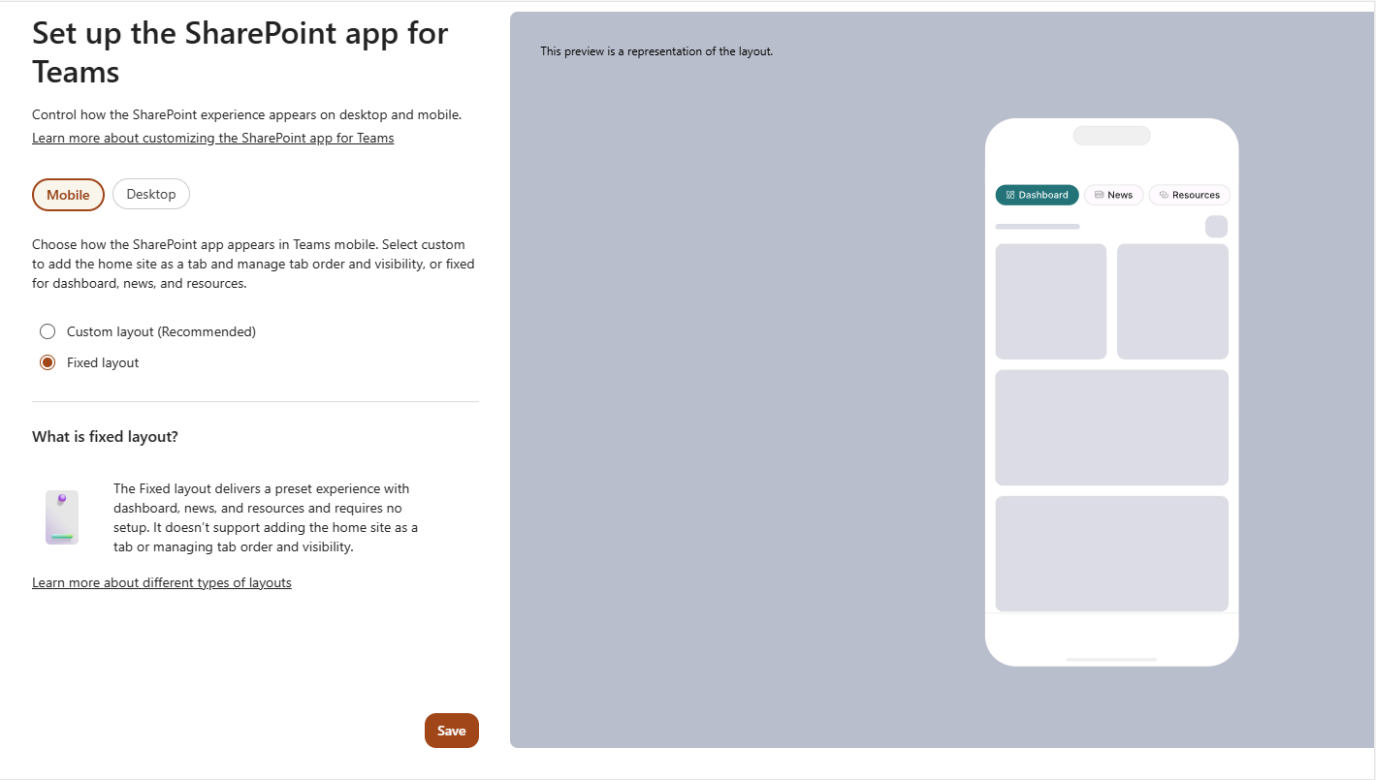


> **Note**
>
> The **Resources tab is not available** in the custom layout. Users can still access resources through:
>
> - **Global navigation** on the home site, if resources have been set up with global navigation links. Learn how to enable and customize global navigation.
> - A **Resources web part** added to the home site.
> - **News links cards** on the Dashboard.

Fixed layout

The fixed layout preserves the original tab structure for organizations that prefer the classic experience.

- **Tabs included**: Dashboard, News, and Resources — in the original order.
- No reordering or tab visibility options are available in this mode.



Configure the desktop experience

> **Note**
>
> The history of navigation in the SharePoint app in Teams desktop is available while you are in the app using the **Back** < or **Forward** > arrow to the left of the search bar. Once you leave, that history isn't retained. You'll return to the default experience of the app the next time you open the app either directly or using the history navigation of the app.

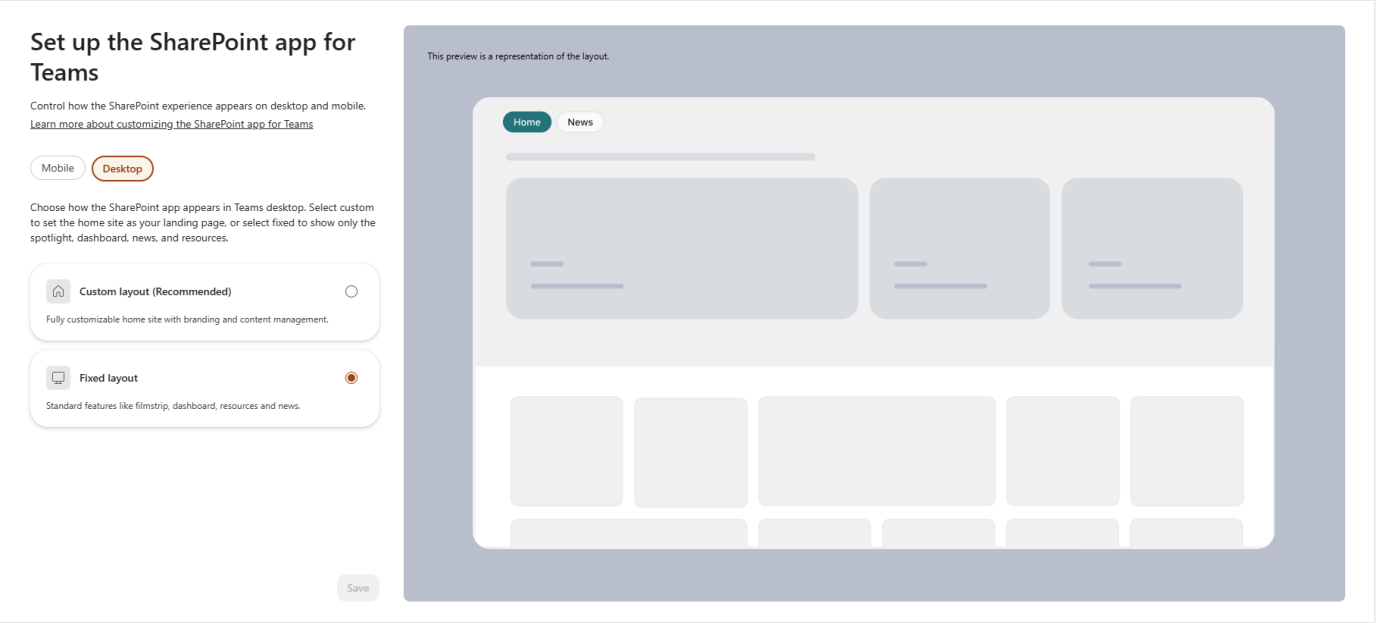
The desktop configuration controls how the SharePoint app in Teams appears on desktop and tablet devices. Choose between two layout options.

Custom layout (recommended)

The custom layout sets your **SharePoint home site as the landing experience** when users open the SharePoint app in Teams on desktop. Users arrive directly on the home site, giving them immediate access to organizational news, resources, and navigation from a familiar, branded experience.

Fixed layout

The fixed layout uses the predefined structured view that includes a Spotlight, Dashboard, News, and Resources panels as the default landing experience in Teams desktop.



ⓘ**Note:** The author created this article with assistance from AI. Learn more

---

Last updated on 09/21/2026

Use audience targeting to personalize the SharePoint app in Teams experience

Audience targeting can help you target content to specific Microsoft 365 Groups within your organization so your content is seen by the right people. Audience targeting can be applied to cards on the dashboard, SharePoint news posts, and links in the Resource section - along with numerous other web part and pages. For example, if a regional finance department has many specialized dashboard cards needed for their daily tasks, audience targeting ensures that only members of that group see those cards.

Depending on the size of your organization, and the information to communicate, you might decide to create a separate experience for each audience you wish to target. Consider creating a separate SharePoint app in Teams experience if you have subsidiaries that need their own content. Or if you have international legal entities that need control over the content. Or a common use case when you want to present unique content specific to frontline workers (for example, dashboard and resources with the frontline worker focus such as tasks, shifts, approvals, and top news).

> **Note**
>
> - Audience targeting filters content and isn't a security measure. It isn't meant to manage permissions, access, or secure confidential content.
> - Microsoft Entra Groups (including security groups, Microsoft 365 Groups, and Microsoft Entra Dynamic Groups) are supported.
> - The author is able to view all content in Edit mode. In read-mode, the content is filtered based on the audiences selected.
> - Publish (or republish) to save changes made to existing page content, page metadata, and audience targeting settings for audience targeting features to take effect.

Apply audience targeting to cards in the dashboard

Create a personalized experience by targeting dashboard cards to specific audiences to ensure only the most relevant cards are seen. You can then create a mix of corporate- and department-specific content (for example, centralized HR or corporate communications). It, too, helps

declutter the dashboard to prevent cards from appearing to users who wouldn't use them frequently. Use audience targeting:

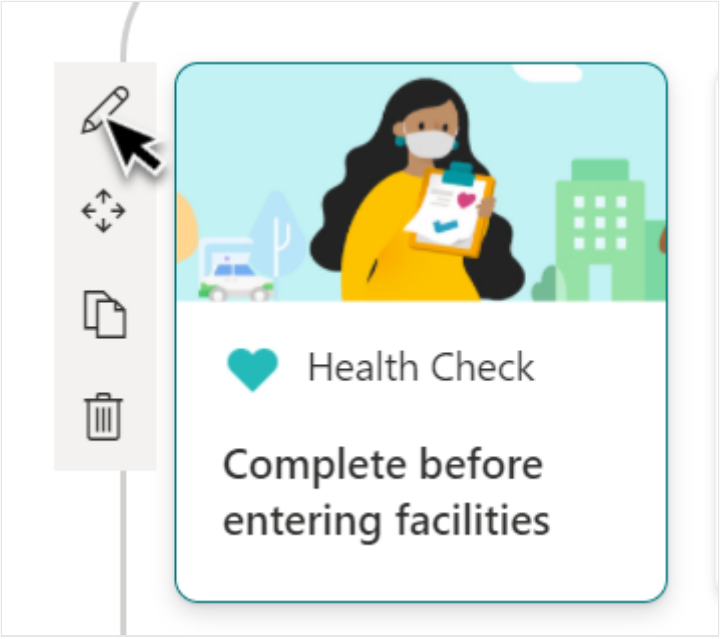
- To create custom views for distinct roles and regions,
- To generate as many different views as needed to create unique experiences, and
- To ensure the most important content is seen by the intended audience.

When you're using card-level targeting, consider testing your dashboard with different audience groups to ensure your audiences are seeing the content you want them to.

> **Note**
>
> - Site owner permissions to the SharePoint home site are required to edit the SharePoint app in Teams dashboard.
> - Site owners should review creating a SharePoint app in Teams dashboard and adding cards for more information.

To apply audience targeting to a dashboard card:

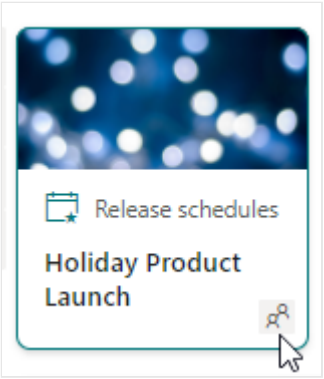
1. From the dashboard, select **Edit**.
2. Select **Edit** on the card you want to apply audience targeting to.



3. At the bottom of the edit pane, enter the Groups to the **Audience to target** field. Exit the edit pane when you're done.

4. Preview the viewing experience for different audiences and devices by selecting **Preview** from the command bar.

5. Publish the dashboard when you're done for the audience targeting to take effect. An icon appears on the card indicating audience targeting is applied.



> **Note**
>
> If an audience group that you recently created or changed was selected, it might take some time to see targeting applied for that group.

Preview your SharePoint app in Teams dashboard to see how it displays for different audiences

After creating or editing cards on your SharePoint app in Teams dashboard, make sure you preview the experience for each audience and on both desktop and mobile devices.

What you see in *preview mode* approximates how the dashboard displays for certain audiences and devices. When you apply audience targeting to cards, you can preview how different people view the dashboard depending on the audience or device.

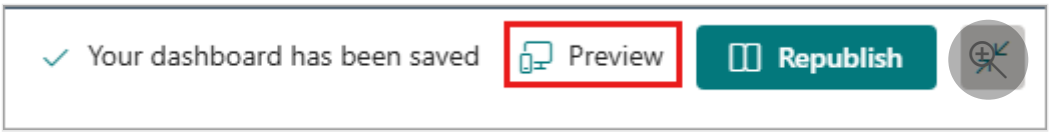
While in preview-mode, make sure:

- Physical gaps aren't present between cards that might appear while previewing different audiences and devices. If you see gaps, rearrange cards so that every audience and device has a high-quality viewing experience.
- Icons, graphics, and images are easy to identify and understand.
- Buttons and links are active and go to their intended destinations.

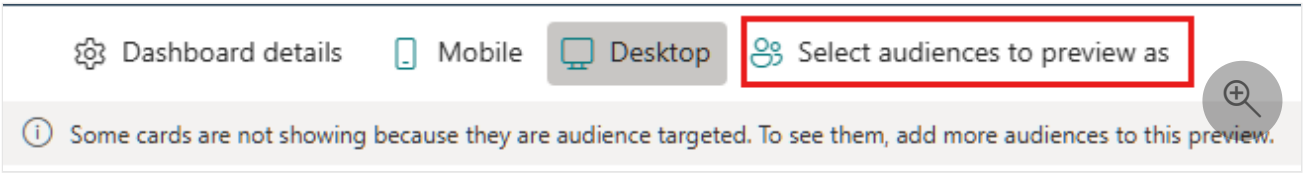
- Labels and description text are helpful, easy to read, and make sense for the intended audience.

To preview different audiences:

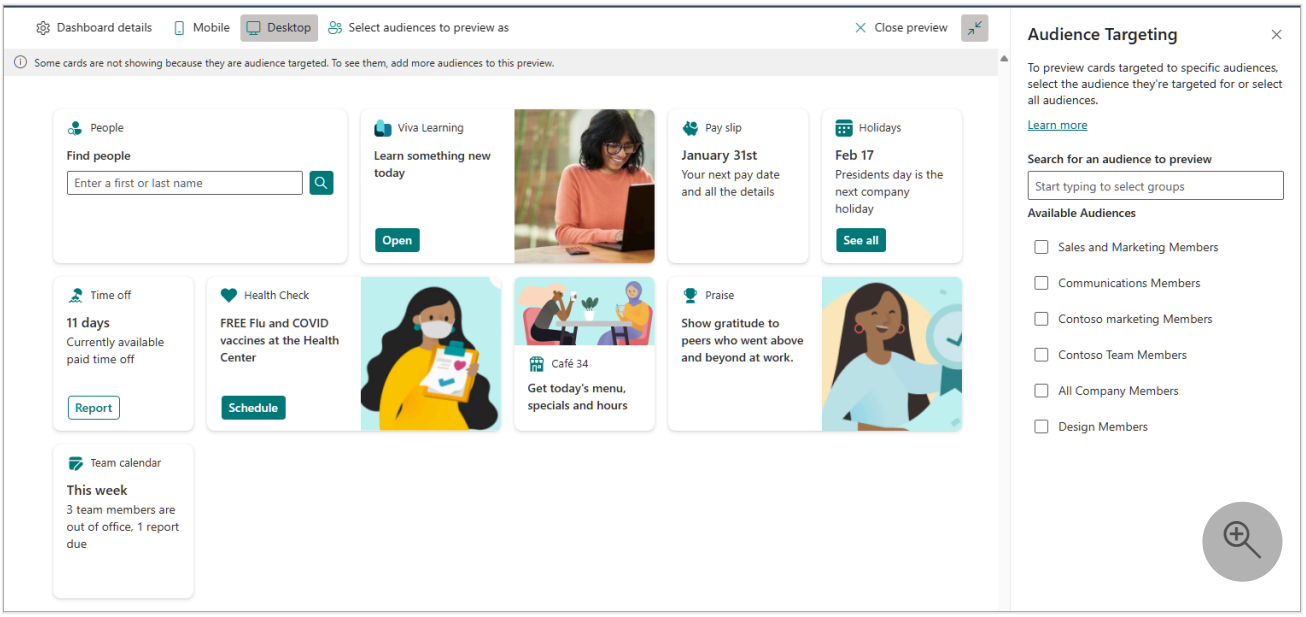
1. While in edit mode, select **Preview** on the top right.



2. Open the **Select audiences to preview as** drop-down list. (if no cards are audience targeted, you'll see a disabled **Audience targeting** label).

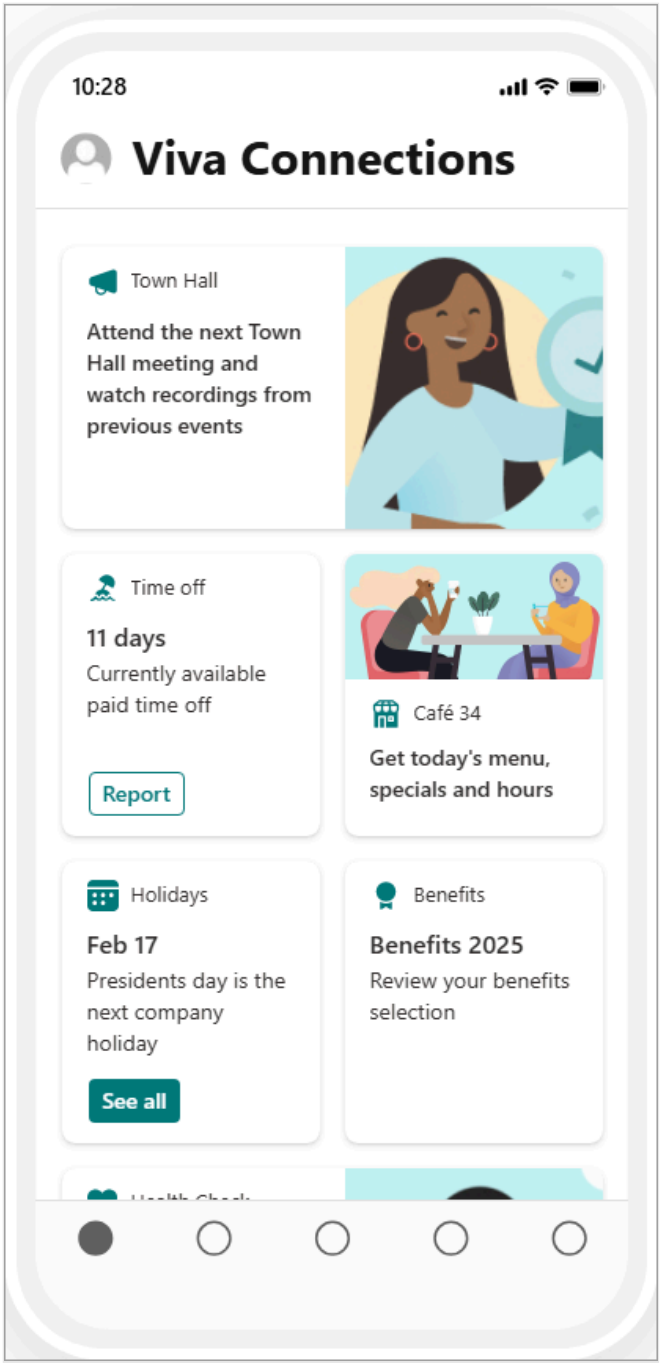
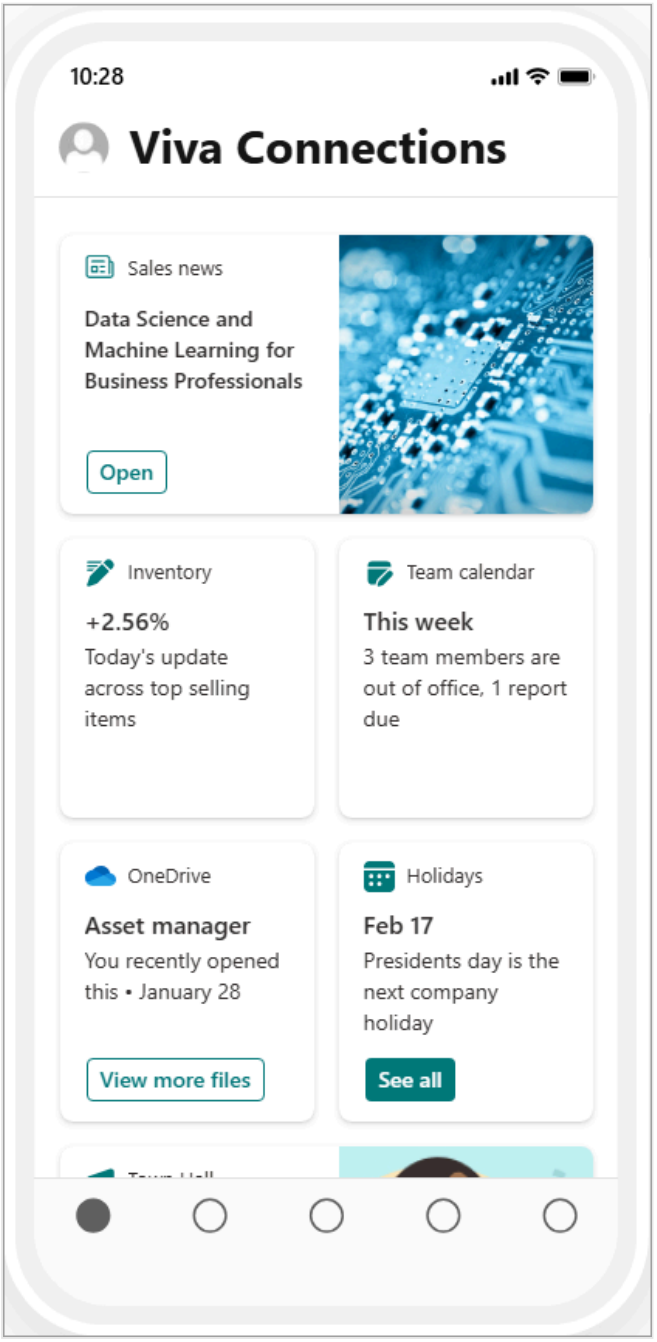


   - Search for and select a group. Once added, the group is selected by default. You can select the group again in the **Select audiences to preview as** drop-down list to deselect it. Cards targeted to a specific group display.
   - When one or more audiences are selected, cards that don't have audience targeting applied also display.
   - If no audiences are targeted, only cards that aren't audience targeted display. If there aren't any cards with audience targeting applied, none display.
   - If you aren't part of one of the selected audiences, you'll only see cards that aren't audience targeted. If none of the cards are audience targeted, you won't see any cards.



In the following example, the preview is set for mobile devices and highlights the different views that can be created from a single dashboard using audience targeting.

Expand table

View 1 (General User)	View 2 (Users in Sales)
	

Apply audience targeting to news posts that display in the News web part

Audience targeting is useful when you want to present information that is relevant only to a particular group of people. For example, you can target news stories about a specific project to only team members and stakeholders of the project.

To use audience targeting, you must first enable audience targeting for each pages library that contains the news stories you wish to target. For more information, see the article on enabling audience targeting for your pages library.

Apply audience targeting to news posts from SharePoint

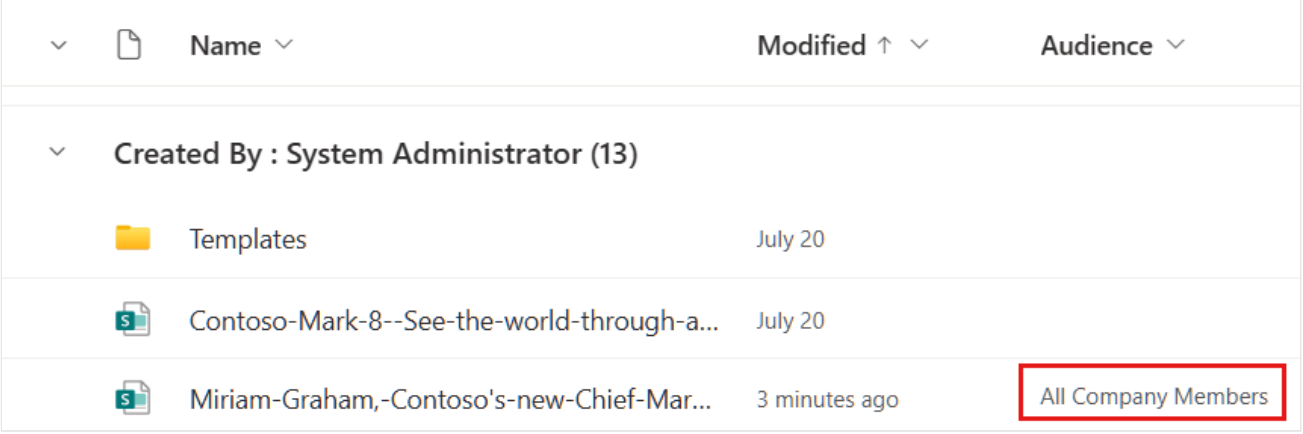
To apply audience targeting to news posts (site pages) from your SharePoint site:

1. Access **Settings** from the SharePoint site where the news is published and select **Site contents**.

2. Navigate to the news post you want to apply audiences to and select **Properties** from the command bar.

3. Under Audience, enter the Groups you wish to target the news post to. Close the Properties panel when done.

4. **Republish** the news post for the audience targeting to take effect. News posts that are targeted to specific audiences list the groups in the Audience column.



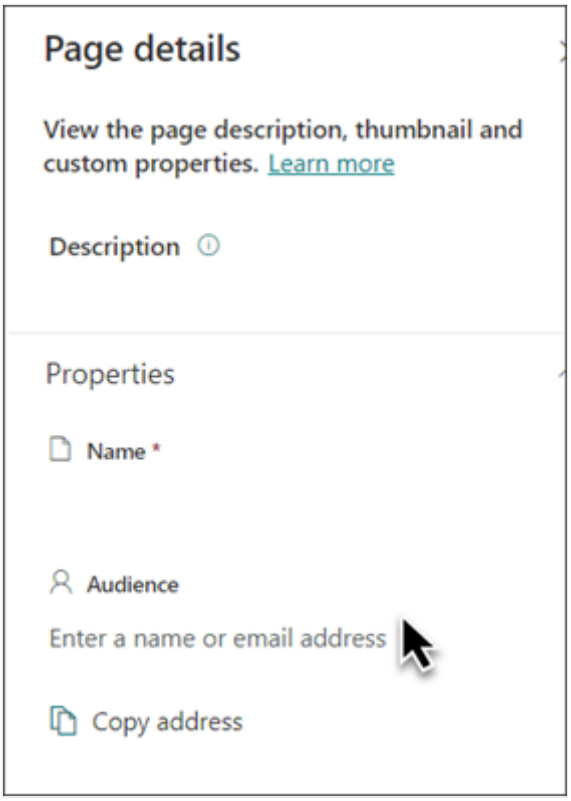
Apply audience targeting to news posts from the SharePoint app in Teams

To apply audience targeting to news posts from the SharePoint app in Teams:

1. Navigate to the news post you want to apply audiences to and select **Edit**.

2. Select **Page details** from the command bar.

3. Under Audience, enter the Groups you wish to target the news post to. Close the Properties panel when done.



4. Select **Update news** for the audience targeting to take effect.

Apply audience targeting to links in the Resources web part

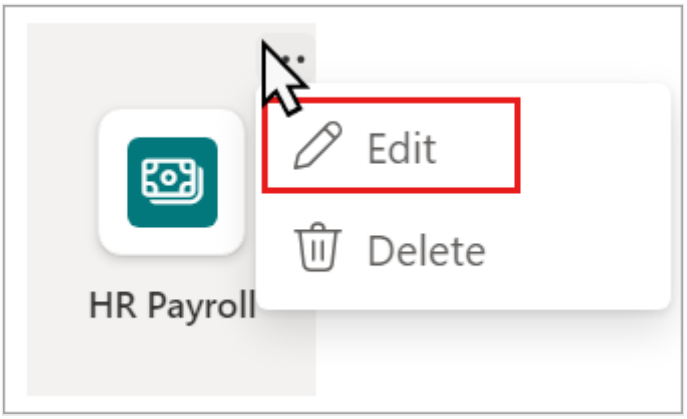
Resources are the navigation links that display beneath the dashboard. You can provide another level of customization to your Resource links by applying audience targeting. Resource links that have audience targeting applied only appear to users who are part of the selected audience.

For example, an organization could use audience targeting to provide a set of resource links for users working in Human Resources that would only be seen by those users.

1. Start by selecting **Edit** in the Resources section of your SharePoint app in Teams experience.

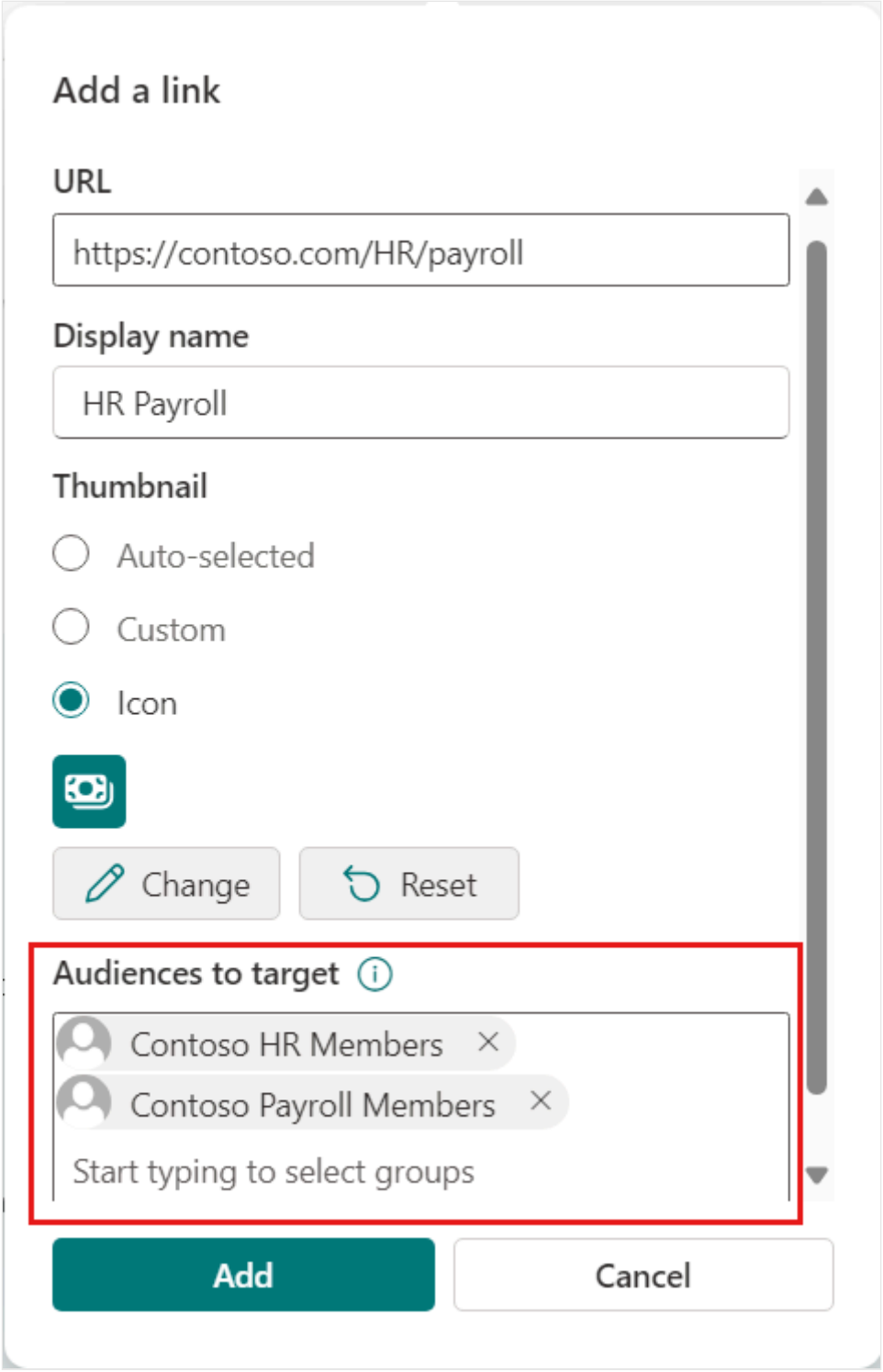
2. Hover over the resource link and select the **ellipsis**.

3. Select **Edit**.

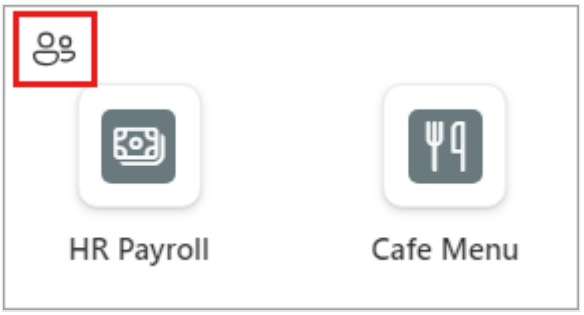


4. Under **Audiences to target**, enter the Groups that you want to see the resource link. Up to 10 audiences can be targeted.

5. Select **Save**.



6. Links targeted to specific audiences display an audience targeting icon in the upper left of the resource link.



For more information, see the article on using the Resources web part.

More resources

Overview: SharePoint app in Teams

Create the SharePoint app in Teams dashboard

Using web parts to display content on your SharePoint site

Set up global navigation in the SharePoint app bar

Last updated on 09/20/2026

Set up the SharePoint app in Teams experience in a specific language

The SharePoint app in Teams experience is available in most major languages used in Microsoft 365. Use this article to learn more about how to create and deploy the SharePoint app in Teams experience in a specific language, other than your organization's default language.

> **Note**
>
> Teams and SharePoint can individually support more than the following languages.

Available languages

English
Japanese
German
Chinese (Simplified)
Spanish
French
Portuguese (Brazil)
Russian
Italian

Chinese (Traditional)
Korean
Dutch
Polish
Swedish
Turkish
Czech
Portuguese (Portugal)
Thai

Danish
Hungarian

Finnish
Indonesian
Greek
Romanian
Ukrainian
Catalan
Norwegian Bokmål

Broadly, the SharePoint app in Teams has four components that influence the end user's overall language experience - the dashboard, news, resources, and announcements. This experience is also supported across desktop and web, and on mobile and tablet devices through the Teams mobile app.

The following steps use English as an example, but the steps apply for any one of the 27 languages specified in the available languages.

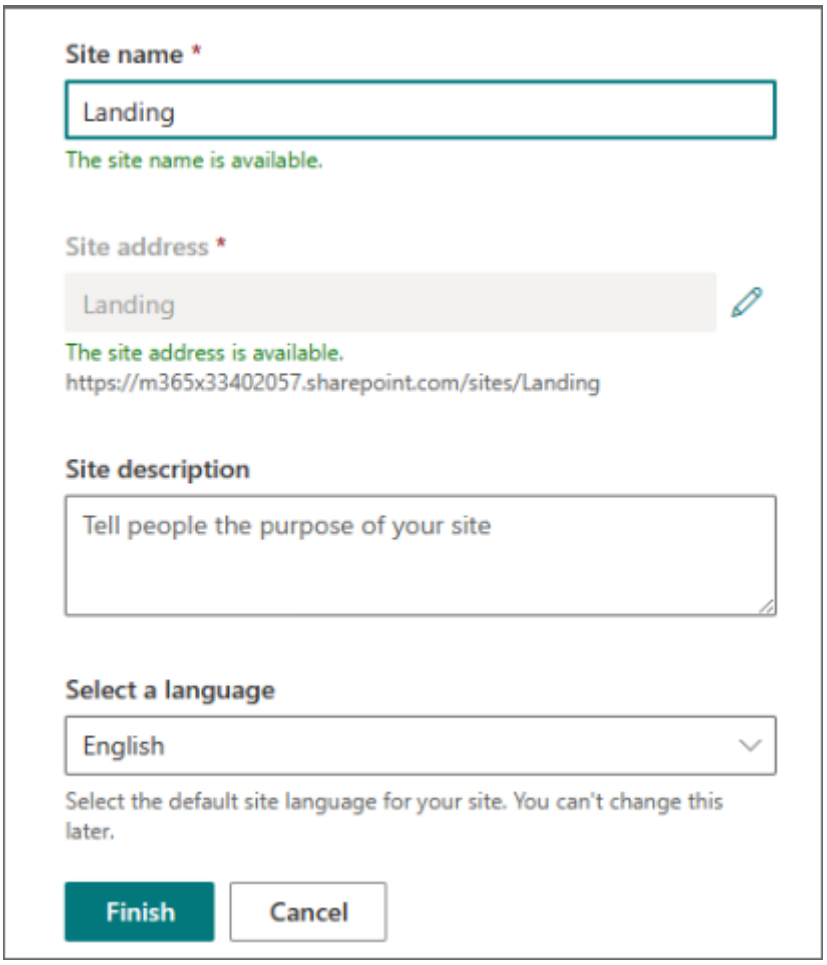
The SharePoint app in Teams dashboard

The dashboard is intended to provide quick access to content and tasks from various sources including:

- Intranet content,
- Line-of-business applications,
- HR tools,
- Frontline worker tools, and
- Internal or partner applications.

For organizations using an intranet portal (SharePoint home site)

1. Create a communication site and make sure to select English as the default language at site creation time.



2. Create the SharePoint app in Teams experience using this site as your existing intranet portal.

3. When creating the dashboard, make sure the dashboard author is typing the content in the English language for details like card titles and descriptions – even if their own preferred language setting in Microsoft 365 isn't English.

4. Then, you can create dashboards in more than one language using the SharePoint multilingual feature.

> **Note**
>
> For custom cards on the dashboard, ask your card developer to include content localized in the English language.

News for the SharePoint app in Teams

You can configure the News web part to display SharePoint news posted from:

- SharePoint Home sites,

- SharePoint sites users frequent and follow,
- Boosted SharePoint news, and
- Trending sites and news published by people the user works with.

Organizational news

Make sure that authoritative news sites (there can be more than one organization news site) are created with English as the default language and that authors of news post are creating the news posts in English language – even if their own preferred language setting in Microsoft 365 isn't English. In order for content in the news reader to display in a language other than your organization's default language, SharePoint news posts need to be available in more than one language.

All company Viva Engage

Announcement posts in the All-company group in Viva Engage should be created in English.

Resources web part

The Resources web part doesn't support multiple languages.

Microsoft Teams mobile app

In the Teams mobile app, SharePoint is displayed as another tab in the Teams app bar, representing the SharePoint app in Teams. The language experience of the mobile app is determined by the device language set by the user. Make sure to inform your users to set it to English for a cohesive experience – although it isn't required.

If a user has a device set to the French language, the Teams mobile app "system" strings (placeholder text Microsoft provides out-of-the-box) will be in French while the dashboard cards and news reader will appear in English if the French version of the SharePoint app in Teams experience isn't published. Resources content will also be in English.

More resources

- Overview of the SharePoint app in Teams
- Set up a Dashboard in more than one language

Last updated on 10/09/2026

View usage data for SharePoint app for Teams

Understand how and when users engage with components of the SharePoint app in Teams experience by using analytics. Review data on overall traffic, usage, and engagement across each of your organization's SharePoint app in Teams experiences. Data can be further filtered to view a specified range or downloaded as an analytics report in Excel.

> **Note**
>
> - Member level permissions (or higher) to the SharePoint Home site are required to view usage analytics for SharePoint app in Teams.
> - Usage analytics data is aggregated and can't be tracked to an individual user.
> - Users with a Microsoft 365 subscription (E, F, or A license) are limited to creating and using one experience. If you want to create or use two or more experiences (up to 50), then every user in your tenant must have a Microsoft Viva Suite or Viva Communications and Communities license. See Microsoft Viva plans and pricing for more info.
> - For tenants that are set up for more than one region, the option to access analytics will have to be disabled for each region using PowerShell commands. For more information, see how to disable analytics features.
> - The analytics feature is unavailable in GCC, GCC High, and DoD environments. For more information, see the list of platform features.

How to access the report

Users need member level permissions (or higher) for their SharePoint app in Teams experience to access and view the analytics data for that experience. For organizations that have more than one experience, you can view the analytics report for each experience by going to that experience and opening the report. Analytics data for SharePoint app in Teams can be accessed from your SharePoint home site or the SharePoint app in Teams.

Access analytics data from a SharePoint home site

1. Navigate to your organization’s SharePoint home site.

2. Select the **Settings** icon.

3. Select **Manage home site**.

4. Go to the **SharePoint app in Teams analytics** section and select **View analytics**.

Manage home site

Choose how the SharePoint app appears in Teams. Organize information, and track activity.

Learn more about managing a home site.

SharePoint app for Teams

Manage how the SharePoint app appears to users in Teams on desktop and mobile.

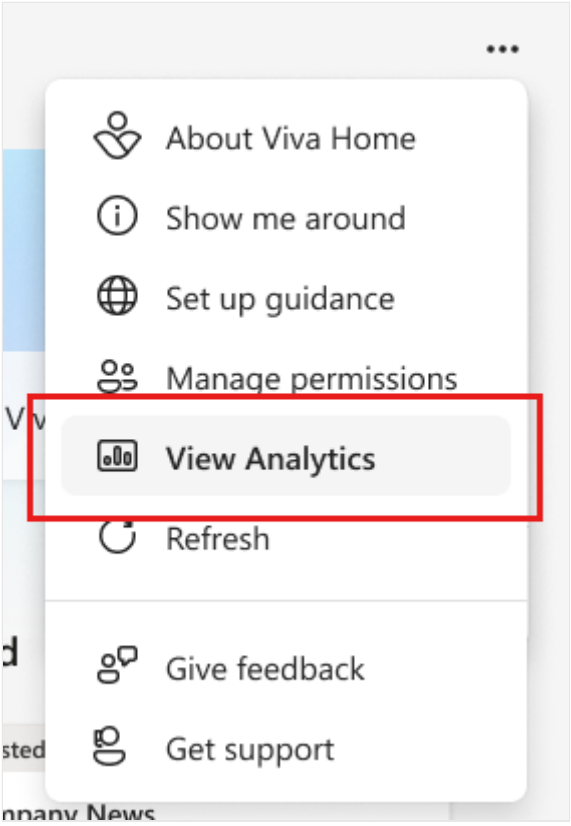
Set up experience

SharePoint app for Teams analytics

View usage of the SharePoint app for Teams and home site dashboard, including traffic and usage breakdowns.

Access analytics data from Microsoft Teams

1. Navigate to your organization's SharePoint app in Teams.
2. Select the **ellipsis** in the top-right corner.
3. Select **View Analytics**



What's in the usage report

The Analytics page contains charts and graphs providing data on overall traffic, usage, and engagement for your accessed SharePoint app for Teams experience. Data can be filtered down to the last 7, 30, or 90 days. Overall traffic data can be filtered to the last 12 months.

> **Note**
>
> - A Microsoft Viva suite or Viva Communications and Communities license is required to view data beyond 30 days. For more information, see Microsoft Viva plans and

pricing .

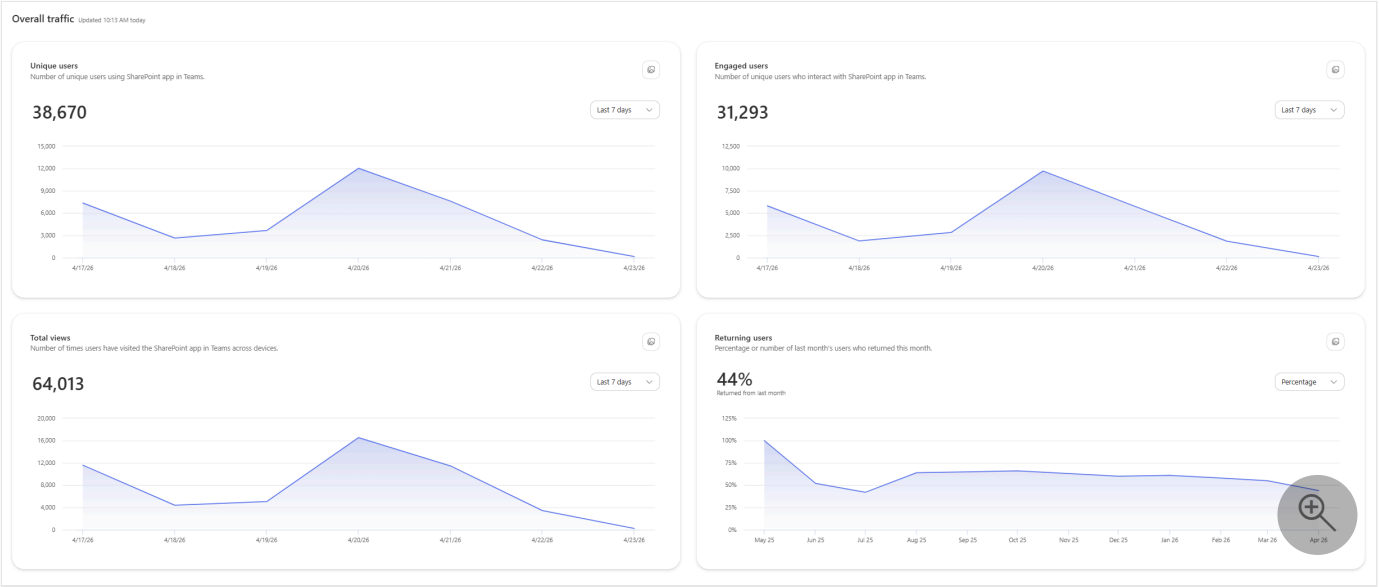
- Data filtered to the previous 90 days and 12 months will be available in mid-June 2024. Historical data for these new filters won't be available.

Overall traffic

This section provides usage data on unique users, engaged users, total views, and returning users. Activity for desktop, web, and mobile usage is combined in this section, regardless of the platform.

- **Unique users**: Total number of individual users regardless of how many times they visited across all platforms and devices.
- **Engaged users**: Total number of individual viewers who interact with the SharePoint app in Teams.
- **Total views**: Total number of views across all platforms and devices.
- **Returning users**: Can view by the percentage or number of users who engaged with SharePoint app in Teams content since the last month over a 12-month view. Select the dropdown to switch viewing data on returning users by percentage and individual user.

> **Note**
>
> A Microsoft Viva suite or Viva Communications and Communities license is required to view data on returning users. For more information, see Microsoft Viva plans and pricing .



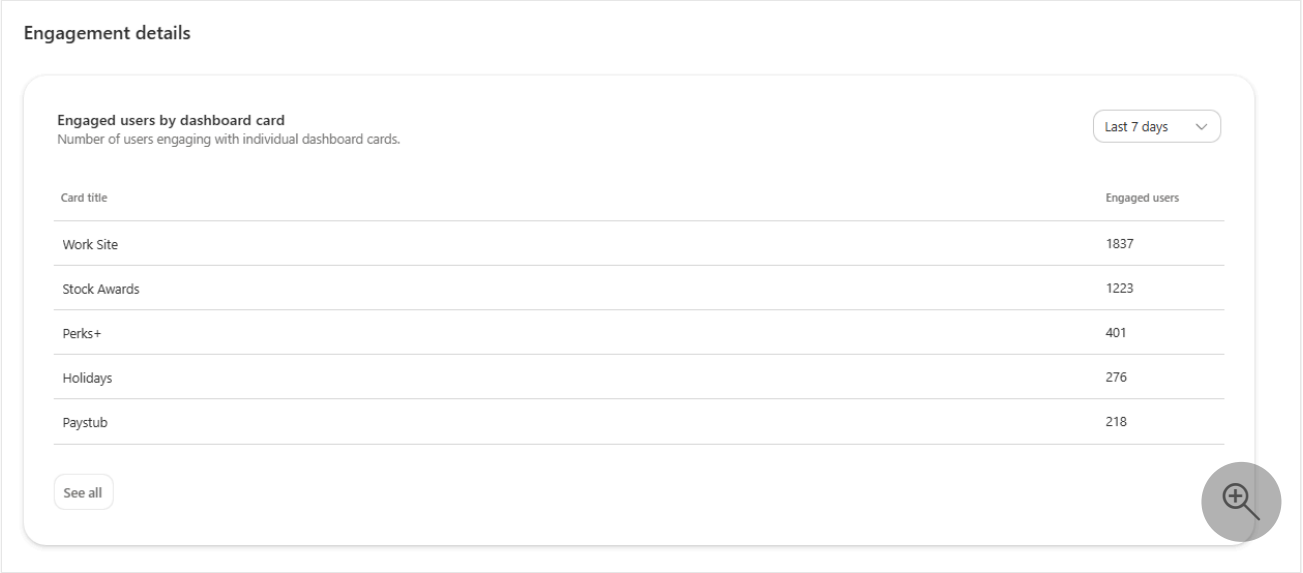
Usage details

This section breaks down usage data across the types of devices and apps used to access the SharePoint app in Teams experience, including activity from the Dashboard, News, and Resources web parts.

- **Total views by apps and devices**: Includes views for desktop, web, and mobile usage.
- **Engaged users by component**: Includes number of engaged users for the Dashboard, News and Resources web parts.
  - **Dashboard**: Includes usage from the Dashboard cards.
  - **News**: Includes usage from the News component.
  - **Resources**: Includes usage from the tab in the mobile app and the desktop app (The global navigation bar in SharePoint isn't included).

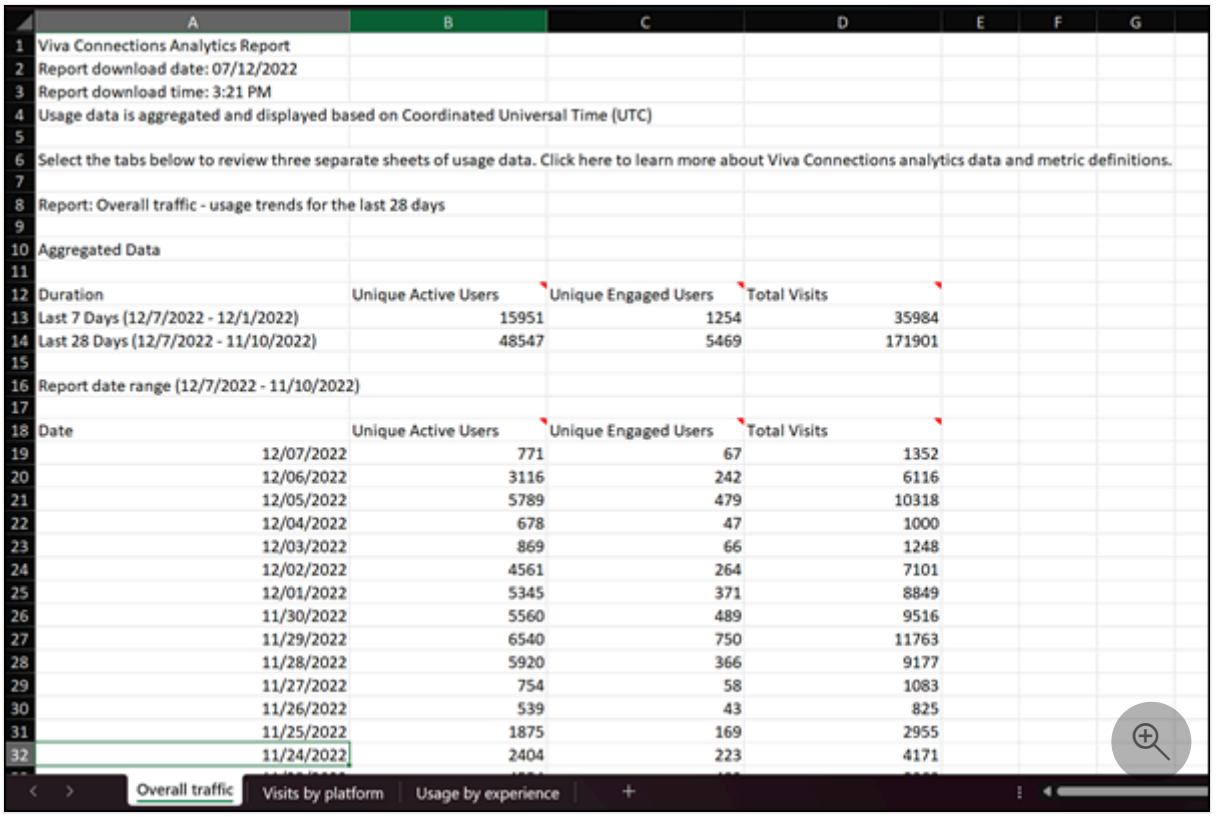
Engagement details

- **Engaged users by dashboard card**: Includes usage data for each dashboard card on your dashboard, indicating how often each user engages with a card.



Download report

Select **Download report** at the top of the analytics page to download an Excel spreadsheet that contains all the information on the analytics page across three separate tabs and sheets of data. The spreadsheet contains all data available that the account has access to (based on license).



	A	B	C	D
1	Viva Connections Analytics Report			
2	Report download date: 07/12/2022			
3	Report download time: 3:21 PM			
4	Usage data is aggregated and displayed based on Coordinated Universal Time (UTC)			
5				
6	Select the tabs below to review three separate sheets of usage data. Click here to learn more about Viva Connections analytics data and metric definitions.			
7				
8	Report: Overall traffic - usage trends for the last 28 days			
9				
10	Aggregated Data			
11				
12	Duration	Unique Active Users	Unique Engaged Users	Total Visits
13	Last 7 Days (12/7/2022 - 12/1/2022)	15951	1254	35984
14	Last 28 Days (12/7/2022 - 11/10/2022)	48547	5469	171901
15				
16	Report date range (12/7/2022 - 11/10/2022)			
17				
18	Date	Unique Active Users	Unique Engaged Users	Total Visits
19	12/07/2022	771	67	1352
20	12/06/2022	3116	242	6116
21	12/05/2022	5789	479	10318
22	12/04/2022	678	47	1000
23	12/03/2022	869	66	1248
24	12/02/2022	4561	264	7101
25	12/01/2022	5345	371	8849
26	11/30/2022	5560	489	9516
27	11/29/2022	6540	750	11763
28	11/28/2022	5920	366	9177
29	11/27/2022	754	58	1083
30	11/26/2022	539	43	825
31	11/25/2022	1875	169	2955
32	11/24/2022	2404	223	4171

Overall traffic | Visits by platform | Usage by experience

How to disable analytics features

Your organization might not want to see analytics data due to local data and compliance regulations or other reasons. Use the following steps to disable the SharePoint app in Teams analytics feature using PowerShell. For tenants that are set up for more than one region, the option to access analytics needs to be disabled for each region using the PowerShell command. Note: The SharePoint app in Teams was previously branded as "Viva Connections", thus you will see the former name still in these PowerShell commands.

1. Make sure any previous versions of SharePoint Online Management Shell are uninstalled on your device (Settings > Apps > Installed apps > uninstall "SharePoint Online Management Shell").

2. Download the latest SharePoint Online Management Shell.

3. Connect to SharePoint as a SharePoint Administrator in Microsoft 365. To learn how, see Getting started with SharePoint Online Management Shell.

4. Connect to the tenant's SharePoint service by running the following command:

   Run `Connect-SPOService -Url <sharepoint admin URL> -Credential <credentials>`

5. Enter the password in the password field.

6. Run `Get-SPOTenant` to view the tenant admin Settings.

7. Locate the "DisableVivaConnectionsAnalytics" setting.

8. Enable or disable the setting by running the following command:

   Run `Set-SPOTenant -DisableVivaConnectionsAnalytics $True`

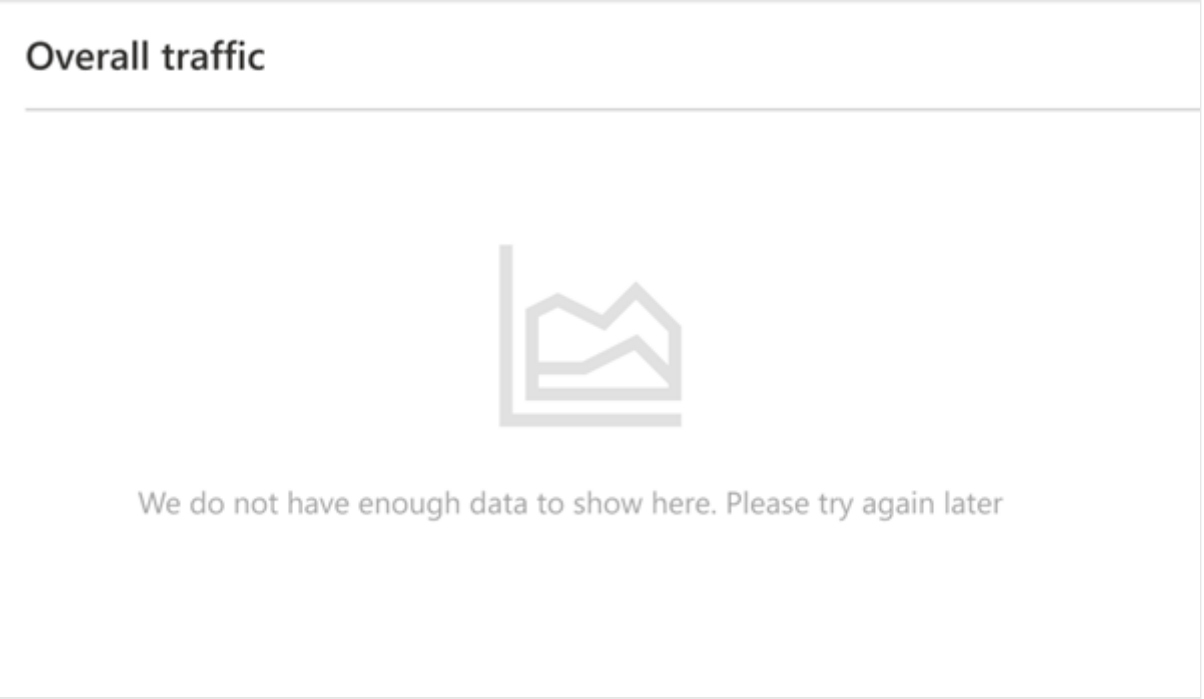
9. Run `Get-SPOTenant` to confirm the setting is updated.

Explanations for common report errors

You might see an error in the Analytics section. Review common errors to learn more about how to resolve them so you can download reports.

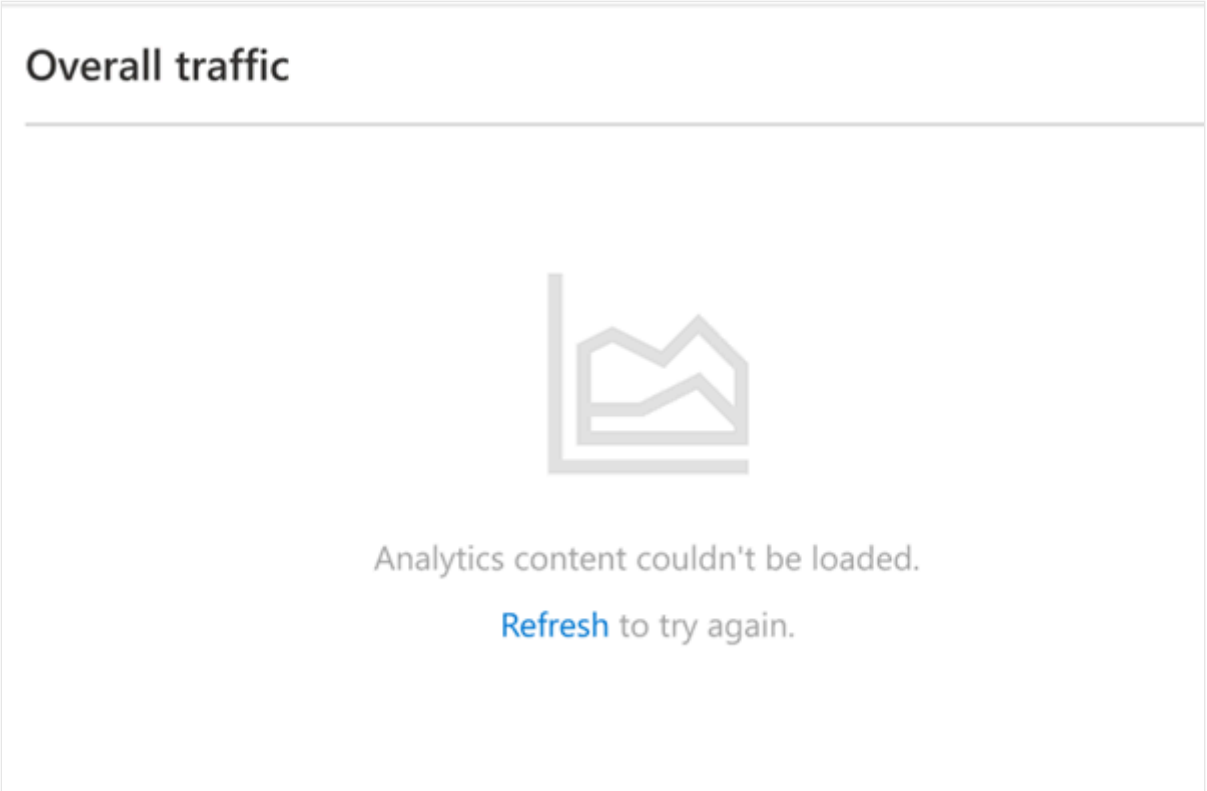
Not enough data to generate a report

This message displays if there isn't enough usage data to generate a report. Finish setting up SharePoint app for Teams and try to access the report again.



General error

Sometimes due to connectivity issues or other technical problems, the analytics report might not be available. Check your network connection, refresh the page, and try loading the report again.



Errors within the downloaded report

Within the downloaded Excel report, you might notice that certain sections aren't available due to insufficient usage data.

The report is disabled

You might get the following message: "Viva Connections usage data has been disabled for your organization by your administrator." This message means you can't access usage reports unless your admin enables the feature for your organization.

Overall traffic

Viva Connections usage data has been disabled for your organization by your administrator

Last updated on 10/09/2026

Microsoft Viva: Privacy, Security, and Compliance

Article • 05/05/2025

Privacy, security, and compliance are essential aspects of your organization. Microsoft Viva takes advantage of Microsoft 365 tools and services, which are governed under the Microsoft Product Terms and the Data Protection Agreement (DPA). For more information, see the Microsoft Trust Center.

For a more detailed look at security, compliance, and privacy for the Microsoft Viva suite, see the following articles:

Viva Privacy

Understand how privacy works in Microsoft Viva.

Viva Security

Learn how security works in Microsoft Viva.

Viva Compliance

Understand how compliance works in Microsoft Viva.

Understand how privacy works in Microsoft Viva

Article • 05/05/2025

Microsoft is transparent about the specific policies, operational practices, and technologies that help you ensure the privacy of your data across Microsoft Viva.

- You control your data.
- We're transparent about where data is located and how it's used.
- We secure data at rest and in transit.
- We defend your data.

Privacy is built into all Microsoft Viva experiences. Microsoft Viva and the Viva apps adhere to the Microsoft Privacy Statement and follow Microsoft's compliance with General Data Protection Regulation and the Microsoft EU Data Boundary.

Microsoft Viva inherits privacy features and settings from Microsoft 365, Teams, SharePoint, and Viva Engage, where applicable.

In addition to the inherited controls, each Viva app has its own set of privacy controls that lets you customize the information you share. The following information describes how the Viva apps handle and store data, who can access it, and, if applicable, how you can manage it.

GDPR compliance

Microsoft Viva and the Viva apps support compliance with General Data Protection Regulation (GDPR) requirements.

Additionally, see the following GDPR information for specific apps:

- Viva Connections and Viva Learning (SharePoint): Safeguarding your SharePoint data
- Viva Engage: Manage GDPR data subject requests in Viva Engage
- Viva Glint: Set up a successful Works Council program
- Viva Insights: Personal Insights privacy guide

Data residency

Data residency refers to the geographic location where data is stored at rest. The way that data is transferred and stored in Microsoft Viva is defined in the Microsoft Products and Services Data Protection Addendum (DPA).

If you are using Viva Connections, you can purchase the Advanced Data Residency add-on in Microsoft 365, which provides more tools to address data residency requirements.

All data within Viva is stored within the customer tenant for any given Viva application and follows the standard Microsoft 365 data storage guidelines by available geography. The following table provides information about where the data for each app resides, along with links to more information.

Expand table

Viva app	Where the data resides	More information
Viva Amplify	Data is stored in the data center where the associated Microsoft 365 tenant resides. If your organization is using SharePoint, Amplify follows the SharePoint data residency policy.	Privacy and security in Microsoft Viva Amplify
Viva Connections	Data is stored in the data center where the associated Microsoft 365 tenant resides. For tenants located in Germany or the EU, none of the data is transferred to a third country. **Note:** Data from third-party apps is governed by the data and privacy agreements for those apps. This information applies to data from Microsoft apps.	Data Residency for Viva Connections
Viva Engage	Committed to storing message bodies and files attached to messages at rest within a specific geographical area (Geo). Data is stored in either Engage cloud storage or SharePoint. Files saved in SharePoint are stored in SharePoint per your SharePoint data residency policy. Mobile push notifications require sending data to a third party notification service (Apple or Google), which might be outside your Geo.	Data residency for Viva Engage
Viva Glint	The data region for Viva Glint is determined by the default geography of the tenant, not individual users, and is stored in US or EU data centers based on central tenant location.	
Viva Insights	**Personal insights** - Processed and stored in the employee's Exchange Online mailbox. Data residency is based on the employee's mailbox location. **Manager/Leader/Advanced Insights** - The data region for Manager/Leader and Advanced is determined by the Default Geography of the tenant, not individual users. Data at Rest (header info and metadata sourced from	Viva Insights - Advanced/Manager/Leader Viva Insights - Personal

Viva app	Where the data resides	More information
	Exchange Online and Teams, but not message content or attachments) is stored in US, EU, EMEA, APAC based on central tenant location.	
Viva Learning	Integration with SharePoint is currently only supported for sites hosted from the home geography of the tenant. For example, a French tenant can only link SharePoint sites hosted in France to Viva Learning.	Viva Learning data residency
Viva Pulse	Data for customers located in the European Union Data Boundary (EUDB) is stored in data centers located in the EU. The data for all other tenants is stored in data centers located in the United States	Data residency for Viva Pulse

For more information, see:

- Microsoft 365 data locations
- Microsoft Privacy - Where is Your Data Located
- Licensing Documents (microsoft.com)

App-specific data information

Each of the Viva apps collects and stores data in different ways, based on the intent of the app. You control your data, but how you control it differs depending on the app.

Viva Amplify

Viva Amplify campaigns are set as private by default because campaigns are designed to be a private collaborative space for campaign team members to work and build their communications. Changing this setting is not recommended.

For more information about Viva Amplify, see Overview of Microsoft Viva Amplify.

Viva Connections

Privacy and security controls:

- You control what content is available through the app.
- Privacy settings inherited from SharePoint, Teams, Viva Engage/Viva

Expand table

What info is available?	Who can access it?	How is it managed?
Conversations, resources, and apps from Microsoft services (like Teams and SharePoint) and third-party apps (by using the SharePoint Framework) For users with elevated permissions, aggregated analytics data about traffic, usage by experience, and usage by platform.	Users with access to the SharePoint resources For analytics, users with site member or higher access to the SharePoint home site that supports the Connections instance.	Information is visible to users based on the setting and their role in the organization Different permission levels are required based on the content creator role (for example Home site or Dashboard). Dashboard authors can target the cards to specific audiences by using Microsoft Entra groups.

For more information about Viva Connections, see Overview of Viva Connections.

Viva Engage

Privacy and security controls:

- Security and privacy settings are managed as a part of Viva Engage.
- Role-based access

Expand table

What info is available?	Who can access it?	How is it managed?
Public announcements, private messages, posts, polls, and videos shared in communities, the inbox, and the Storyline. User profiles (through Viva Engage) Questions and answers Rewards and recognition Sentiment/usage analysis (personal analytics, audience analytics, campaign analytics, Answers analytics)	All users with a paid Microsoft or Office 365 subscription (as part of the Viva Engage license) and accessible through Microsoft Teams. By default, private content is restricted to the participants in the content (for example, the sender and recipient of a private message); however, admins can be temporarily granted access to private content. (You'll need to manually remove this access as well.)	The Engage admin can set up and configure Viva Engage through the Engage admin center (present in the Teams app).

For more information about privacy in Viva Engage, see Overview of security and compliance in Viva Engage.

Viva Insights

Privacy and security controls:

- Role-based access
- Everyone's data is kept private
- Mailbox security through Exchange

Expand table

What info is available?	Who can access it?	How is it managed?
Personal insights (visible only to the individual) Manager and leader insights (always aggregated and deidentified) Organization insights (aggregated and deidentified, with data access restricted to assigned analysts) **Note:** A manager or leader needs to have nine direct reports for the data to be aggregated. The admin can increase this threshold.	Insights only available to licensed users (Personal Insights) and assigned analysts or managers (Manager / Leader / Organization insights)	Admins can configure what information to include in insights, set access levels, and opt individual users in or out by using the Microsoft 365 admin center. Individual users can opt in or out by going to the Settings > Privacy menu in the Viva Insights app in Teams or on the web.

For more information on how to manage access to data in Viva Insights, see Managing who has access to data.

For more information about privacy and data protection in Viva Insights, see the following articles:

- Privacy guide for the Insights app
- Privacy guide for admins
- Technical privacy guide for organization insights and advanced insights

Viva Learning

Privacy and security controls:

- SharePoint integration supports local content
- Role-based access

Expand table

What info is available?	Who can access it?	How is it managed?
Training content from Microsoft, third party providers, and customer-owned content. Learning object content metadata, such as title, description, author, and language User data, such as bookmarks, recently viewed, recommended courses, assigned courses, and completion records Required service data, such as error logs Diagnostic data	The Viva Learning app is discoverable to all users with a paid Microsoft or Office 365 subscription and access to Microsoft Teams. Individual completion data and recommendations are available to those individuals and anyone that they share recommendations with.	Admins can control whether individual users can use Viva Learning and what they can do by changing user and group settings in the Teams admin center. Admins can also turn on or off the storage of diagnostic data.

For more information about Viva Learning, see Microsoft Viva Learning.

More resources

- Microsoft Viva compliance
- Microsoft Viva security
- Viva admin roles and tasks

Understand how security works in Microsoft Viva

Article • 05/05/2025

Microsoft Viva and the Viva apps work with and integrate into Microsoft 365. This means that the Microsoft 365 security capabilities—like role-based access, identity and app management, and others—apply to Microsoft Viva. The Viva apps can also use specific settings and policies of the apps that Viva interacts with. For example, while all users can access Viva Learning in Microsoft Teams by default, you can use app permissions policies in Teams to allow or block access for specific users.

Before setting up Microsoft Viva, consider the following security recommendations:

- Protect data by implementing appropriate access controls and role-based access controls so only authorized users have access to certain data and features. Use Microsoft Entra ID to handle user authentication and authorization.
- Provide another layer of security for users by setting up multifactor authentication (MFA).
- Make sure that you have a plan for incident response to tackle any security breaches that may occur.

> **Note**
>
> All the scenarios and suggestions provided are general in nature and may vary depending on the type of business and organization. It's important to consult with security experts and conduct your own risk assessments to ensure that you have adequate security measures in place for your specific environment.

Understand Teams and SharePoint security

Depending on which Viva app you're using, you may inherit much of your security configuration and options from Teams and SharePoint, which in turn rely on identity management through Microsoft 365 users and groups. Check out Settings interactions between Microsoft 365 Groups, Teams and SharePoint for information about how changes to one area can affect other services. For more information about configuring secure access and collaboration in Microsoft 365, see Set up secure file and document sharing and collaboration with Teams in Microsoft 365.

Viva apps security options and controls

In addition to the security capabilities available to Microsoft Viva through Microsoft 365, SharePoint, and Teams, each app has its own security controls and considerations.

Viva Amplify

Viva Amplify uses SharePoint and Microsoft 365 roles to control access and security of your content.

For more information about security in Microsoft Amplify, see Learn about roles and permissions in Viva Amplify.

Viva Connections

Viva Connections integrates your organization's SharePoint intranet into Microsoft Teams, providing employees with relevant news, information, and resources accessible from desktop or mobile devices.

Security for Viva Connections is largely inherited from Microsoft 365, SharePoint, and Teams. For example, if you configure Viva Connections to include content from Viva Engage in the Feed, your users only see community content from the Engage communities that they already have access to.

> **Important**
>
> This applies to content and cards sourced from Microsoft apps.

When you're setting up Viva Connections, be sure to confirm who has access to certain sites within SharePoint to ensure only authorized users have access to certain data and features.

For more information about Viva Connections, see Overview of Viva Connections.

Viva Engage

The admin tools in Viva Engage help protect your Engage data and determine who can access your Engage network, along with controlling access, managing users, providing secure access on mobile devices via Microsoft Intune, assigning roles, and limiting file uploads. The Engage admin can set up and configure Engage for your organization and manage data, network-related settings, and the various core or premium features within the application. To make someone an Engage admin, make them a Viva Engage administrators in Microsoft Entra ID.

For more information about security in Viva Engage, see Configure and review privacy and security settings.

Viva Glint

Microsoft Glint is a people-driven platform that provides visibility into the health of your organization and guides effective action.

This happens through the analysis of Microsoft 365 collaborative data and organizational (HR) data that you provide or that's used in Microsoft Entra ID. Because of the potential sensitivity about how data could be used, Viva Glint uses role-based access to control who has access. Learn about assigning roles for viewing feedback in reporting.

Viva Insights

Microsoft Viva Insights produces useful insights about how your organization and employees function by analyzing Microsoft 365 collaboration data and organizational (HR) data that you provide or that's used in Microsoft Entra ID.

Because of the potential sensitivity about how data could be used, Viva Insights uses role-based access to control who has access.

The Personal Insights feature is built on Microsoft Graph, which includes a set of REST-based API calls that enable developers to interact with the Microsoft technologies used by your organization. To use these API calls, developers must have specific permissions to access any data they request. Admins control both the deployment of any Microsoft Graph application and permissions to access these applications. You can't turn access to Microsoft Graph on or off globally in the Microsoft 365 Admin Center; instead you can achieve the same effect by blocking employees' ability to install third-party apps or by restricting developer access permissions. For more information, see Microsoft Graph and Microsoft Graph security API.

For more information about Viva Insights, see Introducing Viva Insights.

Viva Learning

Viva Learning is a centralized learning hub in Microsoft Teams that brings in content from different sources including Microsoft Learn, your organization's SharePoint sites, LinkedIn Learning, and third-party content providers and learning management systems. Non-Microsoft content that is accessible through Viva Learning is subject to terms other than the Microsoft product terms. Learn more about Viva Learning content terms and conditions.

Viva Learning is enabled by default for all Microsoft Teams users in your organization.

You can turn off or turn on Viva Learning at the organization level on the Manage apps page in the Microsoft Teams admin center. For more information, see Manage your apps in the Microsoft Teams admin center. To control whether specific users have access to Viva Learning,

create a custom app permission policy and assign it to those users. For more information, see Manage app permission policies in Teams.

For more information about Viva Learning, see Microsoft Viva Learning.

Viva Pulse

Viva Pulse enables team leads to send brief surveys using research-backed templates to get a snapshot of team sentiment and act on feedback. Additionally, Viva Pulse reporting enables analysis of results and trends so leads can pinpoint what's working well and which areas to focus on over time.

Security for Viva Pulse is largely inherited from Teams. Viva Pulse also supports using access control policies to grant or restrict access to specific features for users and groups. For more information about access control at the feature level in Viva Pulse, see Granular access controls for Viva Pulse.

Microsoft Viva - Compliance

Microsoft offers a comprehensive set of compliance offerings to help your organization comply with national, regional, and industry-specific requirements governing the collection and use and data. Microsoft Viva is also covered under the Microsoft Product Terms and Data Protection Agreement (DPA).

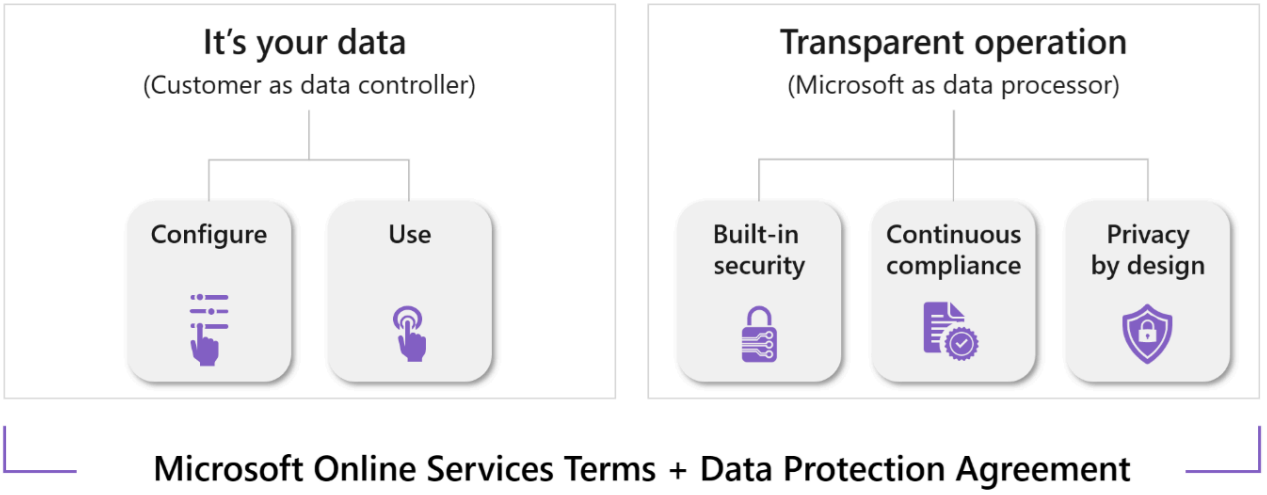
For more information, see the Microsoft Trust Center.

This article covers the following information:

- Microsoft Viva - Compliance
  - Shared responsibility model
  - Inheritance of compliance features and settings
  - System and Organization Controls (SOC) 2
  - General Data Protection Regulation (GDPR)
  - Data residency
  - Microsoft Purview
  - More resources

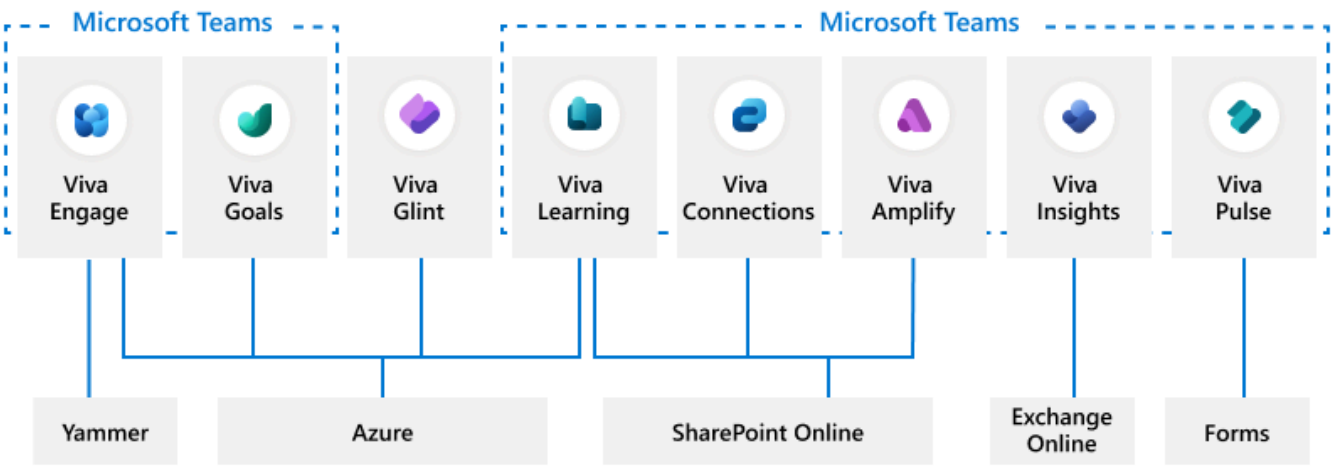
Shared responsibility model

Microsoft works to ensure that we are compliant with industry and international standards, and customers are responsible for ensuring their data within the Microsoft Cloud is protected in a manner that is compliant with the standards and regulations imposed on the customer.



Inheritance of compliance features and settings

Microsoft Viva apps are built on your existing infrastructure and, depending on the app, inherit compliance features and settings from Microsoft Teams, Exchange Online, SharePoint, Azure, and Viva Engage. In addition, all Viva modules are built on the Microsoft Graph API.



For detailed information on each service, see:

Microsoft 365 Plan for security and compliance

Microsoft Teams Overview of security and compliance in Microsoft Teams

Microsoft SharePoint Plan compliance requirements for SharePoint and OneDrive

Microsoft Graph Use the Microsoft Graph compliance and privacy APIs

Viva Engage Overview of security and compliance in Viva Engage

Microsoft Entra ID Microsoft Entra security baseline for Microsoft Entra ID

Azure Azure, Dynamics 365, Microsoft 365, and Power Platform compliance offerings

System and Organization Controls (SOC) 2

A SOC 2 report is an independent assessment of a service organization's systems and processes that are relevant to the trust services criteria. The report is conducted by a third-party auditor and evaluates the effectiveness of the controls in place to meet these criteria. Following is the SOC 2 audit report status for each Viva app:

Expand table

Viva app	SOC 2 report
Viva Connections	Covered within scope of Microsoft 365 - Central Services - SOC 2 report.

Viva app	SOC 2 report
	Excludes third-party content.
Viva Glint, Insights, Learning, Pulse	Covered by Microsoft 365 - Microservices Type 2 SOC 1 Report
Viva Engage	Covered by Microsoft 365 - Viva Engage - SOC 2 Type 2 (2024)

General Data Protection Regulation (GDPR)

All Viva apps built on your Microsoft 365 infrastructure support compliance with EU General Data Protection Regulation (GDPR) requirements. For detailed information, see Microsoft Viva privacy.

Data residency

Data residency refers to the geographic location where data is stored at rest. Many customers, particularly in the public sector and regulated industries, have distinct requirements around protecting personal or sensitive information. In addition, in certain countries/regions, customers are expected to comply with laws and regulations that explicitly govern data storage location.

For information about data residency for Viva apps, see Microsoft Viva privacy.

Microsoft Purview

Microsoft Purview is a family of data governance, risk, and compliance solutions that can help your organization govern, protect, and manage your entire data estate.

Currently, certain features in Viva Engage and Viva Connections (through SharePoint) are supported by Microsoft Purview.

The Viva Engage features eDiscovery and Data Retention are supported by Microsoft Purview; sensitivity labels and data loss prevention aren't supported. Viva Engage supports eDiscovery and the Microsoft Purview portal.

Viva Connections inherits eDiscovery and Data Retention support from SharePoint for files involved in each service.

More resources

Microsoft Viva privacy

Microsoft Viva security

Viva admin roles and tasks

Last updated on 12/22/2025

Plan, build, and launch a SharePoint home site for your organization

A SharePoint home site provides a customized landing experience that reflects the organization's brand, voice, and priorities. A SharePoint home site also serves as the gateway to other portals in your organization's intranet. It is the base SharePoint component when designing and implementing for the SharePoint app in Teams (formerly Viva Connections). Think of SharePoint home sites as an *add-on* to your intranet design. SharePoint home sites are communication sites that have special capabilities such as being marked as an official source of news in the organization. Consider making your organization's root site the SharePoint home site.

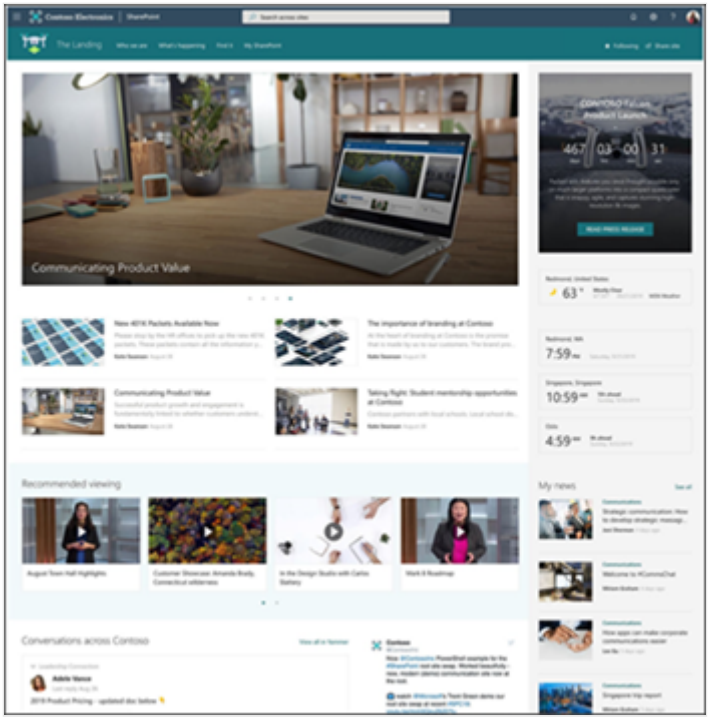
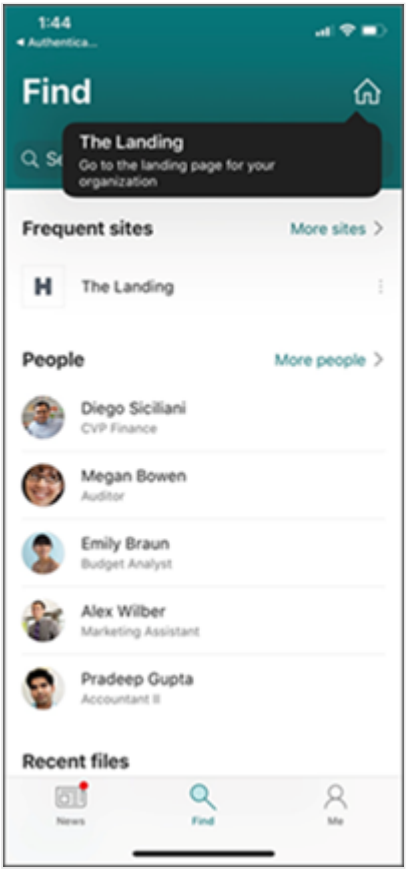
If you've already created the communication site and are ready to specify it as your home site now, learn how to configure the SharePoint app in Teams.

> **Note**
>
> - You must have an Enterprise (E), Frontline (F), or Academic (A) license type to create a Connections experience.
> - Users with a Microsoft 365 subscription (E, F, or A license) are limited to creating and using one experience. If you want to create or use two or more experiences (up to 50), then every user in your organization must have a Microsoft Viva Suite or Viva Communications and Communities license. See Microsoft Viva plans and pricing for more info.
> - You must have SharePoint admin permissions to access the SharePoint admin center.

Use a SharePoint home site to:

- Provide a gateway to other high-traffic portals.
- Connect people with an intranet-wide search experience.
- Showcase targeted news and content.
- Use the SharePoint app in Teams to integrate your intranet into Microsoft Teams.

Expand table

Example of a SharePoint home site:	View in the SharePoint mobile app:
	

SharePoint home site features explained:

SharePoint home sites are unlike any other site in SharePoint. When you set a SharePoint communication site as a home site, you'll automatically apply special capabilities that make the SharePoint home site an ideal landing destination for your organization's intranet.

Search for content across the entire intranet

SharePoint home sites allow users to search for content (such as sites, news, and files) across the entire intranet rather than searching just the site like typical SharePoint sites. The search scope for the SharePoint home site searches the entire intranet instead of just the site collection like a typical site.

Official source of organizational news

By default, a SharePoint home site is set as the organizational news source. News posts that are created from the SharePoint home site automatically become official organizational news and take priority on the SharePoint start page. Administrators can set additional sites as official organizations news sources in the SharePoint admin center.

Enable and customize global navigation in the SharePoint app bar

The SharePoint app bar features a global navigation option that displays intranet navigational nodes and resources no matter where users are in SharePoint. To take full advantage of this feature, you must have a SharePoint home site. Learn more about how to enable and customize global navigation in the SharePoint app bar.

Before getting started

Before you get started planning and building your SharePoint home site, review best practices and considerations.

Best practices for creating SharePoint home sites

- A SharePoint home site that will be used by the entire organization needs to be inclusive and easily accessible on all devices.
- The site needs to be inclusive and easily accessible on all devices, consider other languages that might be needed.
- The SharePoint home site will be viewed by a high volume of users. Make sure you manage site performance through the planning and building phases.
- Links in the SharePoint home site's navigation can direct users to content in addition to global navigation, which can be used to lead users to universally used resources and portals.
- The SharePoint home site should be discoverable by adding an entry point to Microsoft 365 Copilot and a featured link on the SharePoint start page.
- News published from the SharePoint home site should be relevant to the entire organization.

Considerations

- Align the branding on the SharePoint home site to the overall intranet brand where possible.
- Organizations with many portals and resources should consider making your SharePoint home site a hub site to expand navigational options and easily sync permissions and branding across many sites.

- Use a SharePoint home site template like the Organization home template when creating a new site to jump-start the design process.

Summary of how to get a SharePoint home site for your organization

Since SharePoint home sites are the gateway to your intranet, you want to prioritize content and resources that are relevant to most users. Work with business owners and stakeholders to organize and align the flow of information and the navigational design. Then, use the Page diagnostics for SharePoint tool to ensure to best viewing experience. Next, set your SharePoint communication site as a home site in the SharePoint admin center. Finally, use the Portal launch scheduler to plan the launch of your new site and make the site discoverable by adding links to key entry-points in the Microsoft 365 experience.

Expand table

Plan	Build	Launch and manage
- Align objectives with partners and business owners - Organize priority content - Design way finding for the SharePoint home site and global navigation - Think about branding - Use audience targeting on navigational links, news, and web parts	- Upload and organize site assets and content like files and logos (64x64px). - Customize the site to align with the rest of the intranet - Apply audience targeting - Turn on a content approval flow - Use PowerShell to turn the SharePoint comm site into a home site - Swap the root site location with the SharePoint home site - Measure site health and performance - Test on all devices	- Share the site with your organization - Use the Portal launch scheduler to release the new site in phases - Make the SharePoint home site discoverable - Announce the launch of the SharePoint home site using various communication channels - Monitor site usage and analytics

Plan your SharePoint home site

A great SharePoint home site starts with a plan. Because your SharePoint home site is essentially the gateway to your intranet, you want to collaborate with other business owners such as human resources, leadership teams, and even your legal team to ensure the most important and universal resources are accessible for everyone in the organization.

Expand table

Icon	Action	Get started
	Get organized	Start by aligning objectives with stakeholders and organizing priority content and resources. Consider details specific to your organization like if the SharePoint home page needs to be available in more than one language. Use modern SharePoint sites for the home site. Learn more about how modern SharePoint sites and how to create a multi-lingual site and pages.
	Plan navigation	Then, organize the navigational structure for the SharePoint home site itself and global navigation. Consider making the SharePoint home site a hub site if you need to add an extra layer of navigation and make it easier to sync associated site permissions and branding. Learn more about planning site navigation and how to make your SharePoint home site a hub site. Then, review guidance on how to set up global navigation on the SharePoint home site.
	Personalize content	Next, think about the different audiences that your organization serves. Consider how elements on your SharePoint home site like navigational links and certain web parts could benefit from audience targeting to specific audiences. Learn more about audience targeting.
	Gather branding assets	Finally, start gathering assets needed to apply custom branding and other details to your SharePoint home site, like logo files (64x64px recommended), color themes, and any custom solutions. Learn more about how to change the look of your site.
	Consider site performance	Even before you build your site, understand the main elements that make sure your SharePoint home site is healthy. A healthy SharePoint home site optimizes performance to ensure the best possible viewing experience. Use the Page diagnostics for SharePoint tool to make sure the SharePoint home page is healthy before sharing with end users. Learn more about healthy portals and using the Page diagnostics tool for SharePoint.

Build your SharePoint home site

When you've prepared a plan, you're ready to start creating the home site in SharePoint. Start with a communication site, and after you have the general layout finalized, create a SharePoint app in Teams experience from your existing SharePoint home site in the Connections admin center.

Expand table

Icon	Action	Get started
	Create a modern communication site	Start by creating a SharePoint communication site and build out the site by using sections, web parts, and pages. Consider using a mega menu and footer to enhance way finding. See the article on Using web parts to display

Icon	Action	Get started
		content on your SharePoint site for information on creating personalized content for users. Learn how to create a communication site, use modern web parts, and customize your site.
	Apply audience targeting	Next, turn on audience targeting on for the SharePoint home site. By enabling audience targeting, specific content is prioritized to specific audiences in navigational links, news, and certain web parts. Learn more about how audience targeting works and how to apply it to navigational links, news, and web parts.
	Set up a page approval flow	Then, make sure the SharePoint home site is set up for regular content updates. Turn on content approval to ensure only high-quality content is published on the SharePoint home site. Learn how to turn on a page approval flow.
	Swap the root site location with the SharePoint home site	Before you set a communication site as the SharePoint home site, swap the communication site in place of the root site of your tenant as a best practice. The root site for your organization is one of the sites that's provisioned automatically when you purchase and set up a Microsoft 365 plan. If you set up a SharePoint home site first, and then swap locations with your root site, you might lose SharePoint home site settings and need to reapply them. Learn how to swap the root site with the SharePoint home site.
	Set the SharePoint home site	Next, build a SharePoint app in Teams experience from an existing intranet portal.
	Set up global navigation	Then, enable global navigation to allow users to easily navigate to important intranet resources anywhere in SharePoint. Global navigation can only be customized from the SharePoint home site's home page. Learn how to enable and customize global navigation.
	Test site health and the viewing experience	Finally, review portal launch guidance and understand the main elements that make sure your SharePoint home site is healthy. A healthy SharePoint home site optimizes performance to ensure the best possible viewing experience. Use the Page diagnostics for SharePoint tool to make sure the SharePoint home page is healthy before sharing with end users. Learn more about healthy portals and using the Page diagnostics tool for SharePoint.

Launch your SharePoint home site

After you've set your SharePoint home site, it's time to plan the launch and make sure the rest of the organization can find and use the SharePoint home site.

Expand table

Icon	Action	Get started
	Share the site and schedule the portal launch	Start by ensuring your SharePoint home site is healthy, and then its time to share the site with the rest of the organization and schedule the launch. Use the Portal launch scheduler tool to gradually roll out the SharePoint home site to batches of end users. Using a phased approach is ideal to manage any performance issues that might arise and to ensure a positive viewing experience. Learn how about how to use the Portal launch scheduler tool.
	Improve discoverability	Next, make sure people in your organization can easily find the SharePoint home site through a few different entry points in the Microsoft 365 experience. Add a link to the SharePoint home site in the Microsoft app launcher (sometimes called the waffle) and on the SharePoint start page. Learn more about how to add a custom tile to the app launcher and how to add a featured link to the SharePoint start page.
	Engage your audience	Then, let your organization know about the new SharePoint home site resource, and other new elements like global navigation. Consider multiple communication options like a SharePoint news post that can also be shared in email and in Microsoft Teams. Learn more about how to create and post SharePoint news and share it in an email.
	Manage and maintain your SharePoint home site	Finally, when the site is healthy, launched, and being used by the organization, monitor site usage and maintain the site. Site maintenance should include making sure site content is relevant, there aren't any broken links, and that the site stays healthy and performant. Learn how to view usage data and analytics for your site and how to maintain your site over time.
	(Optional) Integrate the SharePoint home site into Microsoft Teams using the SharePoint app in Teams	Expand the reach of the SharePoint home site and help meet users where they're already working by making it easy to access and share content all in one place. After you have a SharePoint home site and the global navigation enabled and customized in the SharePoint app bar, you can integrate the SharePoint home site into Microsoft Teams.

SharePoint home site FAQs

Q: Are SharePoint home sites set in the Microsoft 365 admin center of SharePoint admin center? Starting in July 2026, use the SharePoint admin center to set a SharePoint home site to establish the SharePoint app in Teams experience.

Q: What's the difference between a SharePoint home site and the SharePoint start page?
The content on the SharePoint start page is driven and managed by Microsoft Graph. Content is personalized to the individual users' recent activity, followed sites, and content that is saved for later. The SharePoint home site is a landing experience for your entire organization. It displays

universally relevant content and directs users to other important portals like Human Resources and company directories.

Q: Can I integrate the SharePoint start page with my SharePoint home site?
Integration between the SharePoint home site and SharePoint start page isn't available at this time. However you can add a featured link to the SharePoint start page to increase SharePoint home site discovery.

Watch for updates in the Microsoft 365 public roadmap.

Resources

Planning your SharePoint hub sites

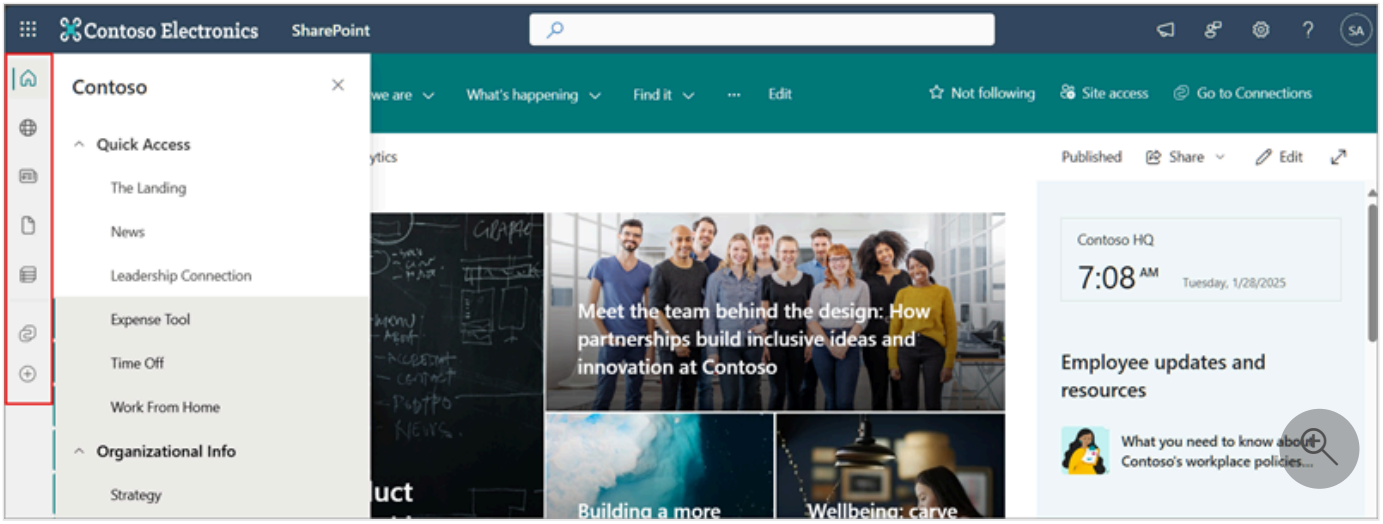
Creating and launching a healthy SharePoint portal

Apply and customize SharePoint site templates

Last updated on 09/20/2026

Introduction to the SharePoint app bar

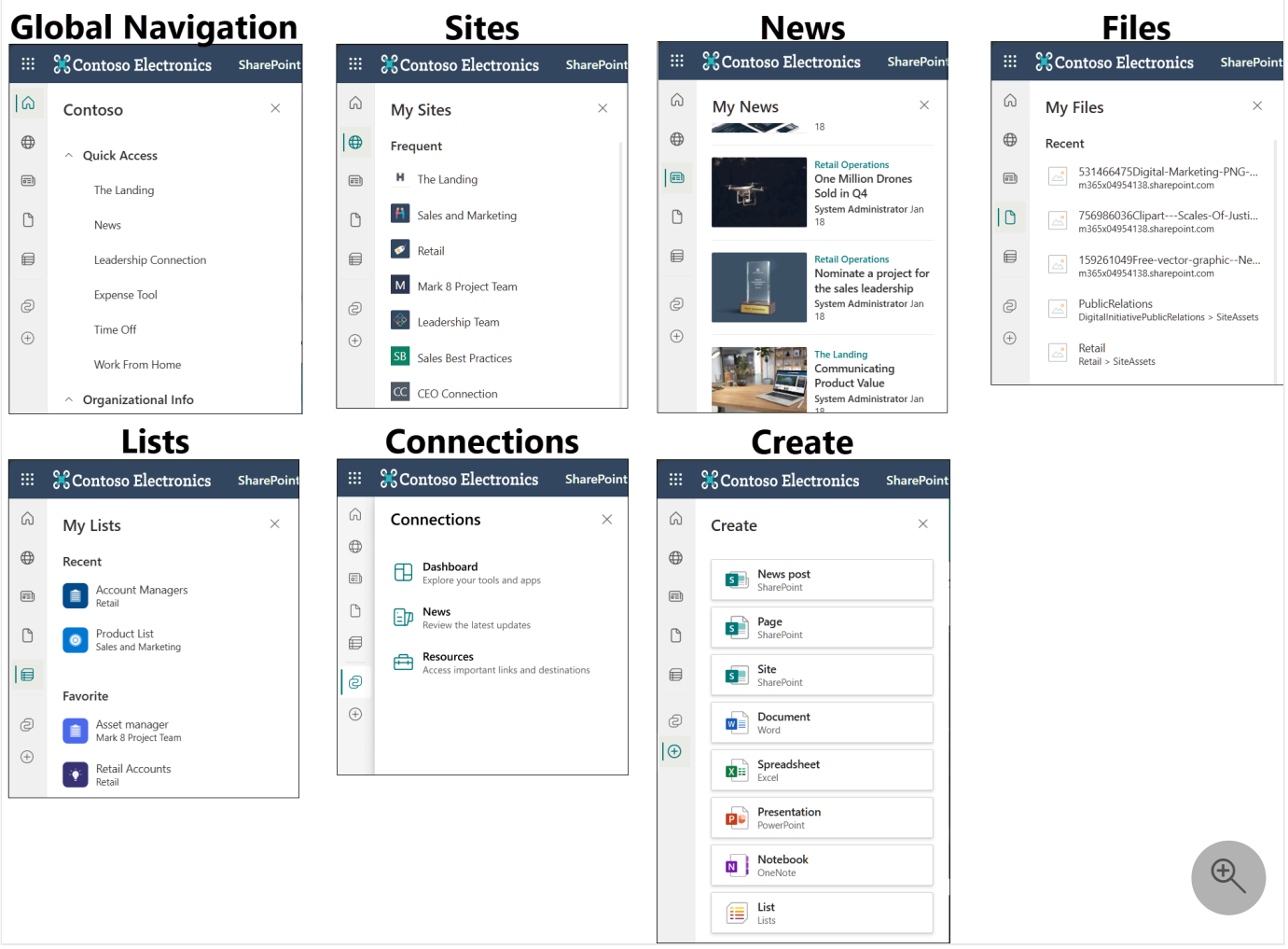
Help users find important content and resources no matter where they are in SharePoint. The SharePoint app bar improves the global way-finding and creation experiences while dynamically displaying personalized sites, news, files, and lists. The app bar is on the left-hand side anywhere in modern SharePoint sites.



The SharePoint app bar experience

The SharePoint app bar brings together intranet resources and personalized content like sites, news, files, and lists. Enable global navigation to allow users to easily navigate to important intranet resources anywhere in SharePoint. Customize global navigation details and the rest of the content will dynamically display and update personalized content for sites, news, and files. Access your SharePoint app in Teams. Create sites, files, and lists easily from anywhere in SharePoint.

> **Note**
>
> - The SharePoint icon will only show to customers who have enabled the SharePoint app in Teams experience with a configured and published dashboard.



Note

- Global navigation is the only app bar tab that can be customized.
- If global navigation is disabled or not configured, the home icon links to the SharePoint start page.
- Specific SharePoint app bar tabs can't be disabled.
- The SharePoint app bar can't be disabled on specific sites.
- The SharePoint app bar isn't available on classic SharePoint sites.
- The SharePoint app bar might affect current page customizations, specifically customizations that appear on the left side.
- The SharePoint app bar won't display in SharePoint for guests outside of your organization.
- In GCC High and DoD environments users might experience a degraded experience for the My sites panel in the app bar.
- Extra restrictions might apply to tenants within the GCC High and DoD environments when using My News in the SharePoint app bar.

- Global navigation in the SharePoint app bar must be enabled for SharePoint resources to display in the Microsoft Teams app bar for the SharePoint app in Teams.

The SharePoint app bar is a significant change to the user experience and your organization's intranet information architecture. To ensure a seamless experience, Microsoft created specific guidance on how to design current navigation to compliment the global navigation feature. There's also end-user guidance to help onboard the rest of your organization.

Customize global navigation in the app bar

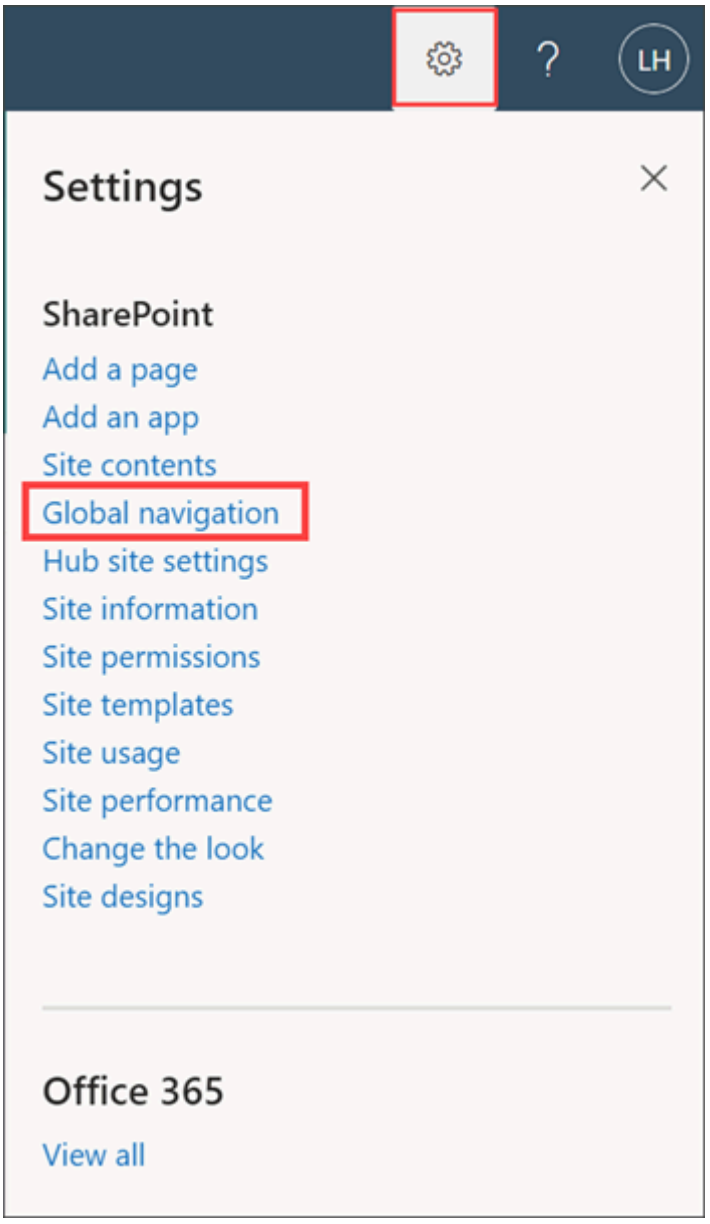
Global navigation can be enabled and customized in the SharePoint app bar. Customize the global navigation logo, title, and source depending on your users' and organization's needs.

If you choose to keep global navigation disabled, the home icon links to the SharePoint start page.

> **Note**
>
> - Site owner permissions (or higher) to the SharePoint home site are required to enable global navigation.
> - Users need read access (or higher) to the SharePoint home site to view the global navigation links.
> - Audience targeting can be applied to menu links in global navigation.
> - If you get an error after editing links to sites, try deleting the link and adding it again.
> - Implementing global navigation might take up to 24 hours for the changes to take effect for users.

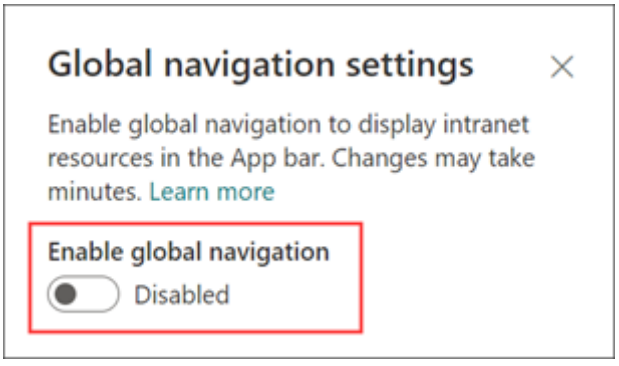
Get started customizing the global navigation tab

1. Set up a SharePoint home site if your organization doesn't already have one.
2. Share the SharePoint home site with everyone in your organization to ensure all users can access the global navigation links.
3. Navigate to your organization's SharePoint home site.
4. Select **Settings** and then select **Global navigation** settings.



> **Note**
>
> If you don't see **Global navigation** in the **Settings** pane on the SharePoint home site, you might not have site owner permissions (or higher) to the SharePoint home site.

5. Switch the **Enable global navigation** toggle to **On**.



6. Next, add the **Logo** to represent global navigation for your organization (organization or custom logo). No action is needed if you choose to keep the default home icon.

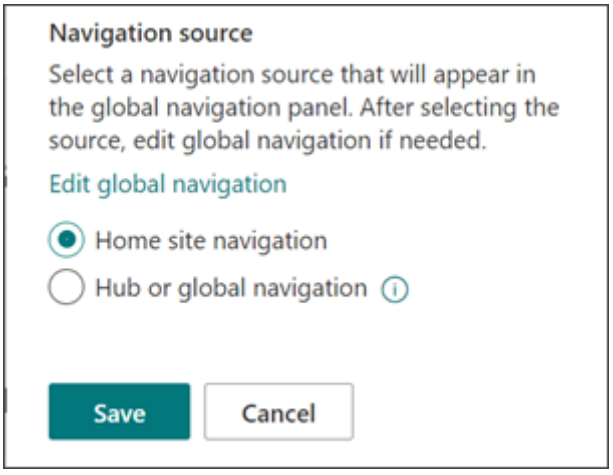
   Global navigation logo specifications:

   - The logo size should be 20x20 pixels
   - PNG file type
   - Transparent background recommended

7. Then, enter a **Title** that's to be displayed at the top of the global navigation pane.

8. Under **Navigation source** make edits to the selected global navigation source if needed by selecting **Edit global navigation**.

9. Select **Save** when you're done. Updates to global navigation might take several minutes before they appear.

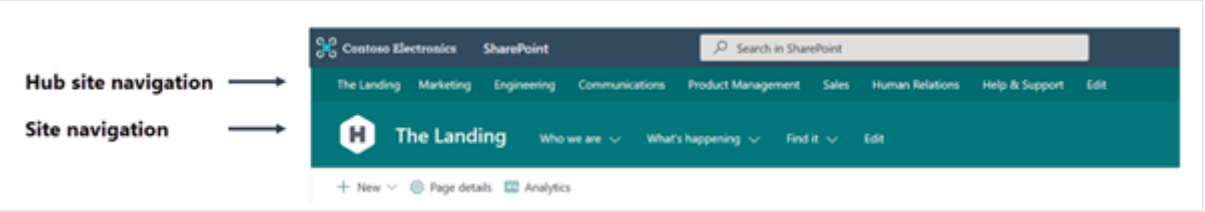


> **Note**
>
> - The global navigation source can be edited at any time by site owners or admins of the SharePoint home site.
> - The site and global navigation links and labels can be edited at any time by editors of the SharePoint home site.
> - Implementing global navigation might take up to 24 hours for the changes to take effect.
> - If you get an error after editing links to sites, try deleting the link and adding it again.

Determine the global navigation source depending on your SharePoint home site's configuration

If you haven't set up your SharePoint home site, do that first and if you're setting up a SharePoint home site specifically to implement global navigation, review this guidance.

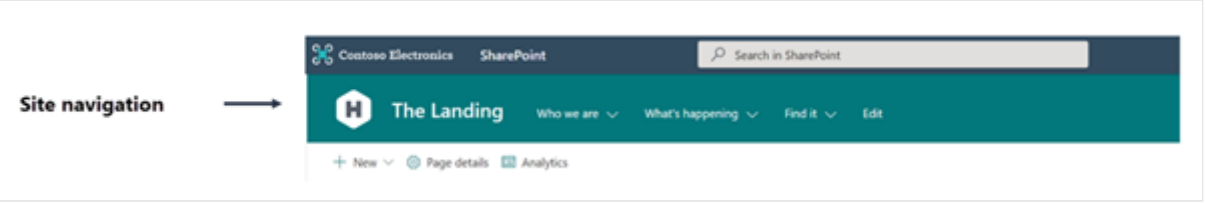
For SharePoint home sites that are a hub, you have two source options



- Select the site navigation source to display the SharePoint home site's navigation.
- Select the Hub or global navigation source to display the SharePoint home site's hub navigation.

> ⓘ **Note**
>
> When you apply the extended header layout to the site, you'll no longer see the site navigation.

For SharePoint home sites that aren't a hub, you have two source options



- Select the site navigation source to display the SharePoint home site navigation.
- Create a secondary set of navigation nodes specifically for the global navigation panel by selecting **Hub or global navigation**. Then, select **Edit global navigation** to create the new global navigation menu. Select **Save** when you're done.

> ⓘ **Note**
>
> For SharePoint home sites that aren't a hub site and choose to create a secondary set of navigational nodes for the global navigation pane - if you decide to make your SharePoint home site a hub in the future, the new hub site navigation inherits the current navigational nodes for global navigation and can be edited at any time.

See all the different ways you can set up global navigation

Depending on the content you want to make available in the global navigation, you can configure your SharePoint home site navigation and global navigation in three different ways.

Display the SharePoint home site's navigation in global navigation

Display hub and site navigation on the SharePoint home page, and the home site navigation in the global navigation panel.

1. Navigate to the SharePoint home site's **Settings** and then **Global navigation**.
2. **Enable** global navigation, enter a **Title**, and then select **Home site navigation** as the source.
3. Select **Save**. Changes might take a few minutes to reflect.

Display the SharePoint home site's hub navigation in global navigation

Display hub and site navigation on the SharePoint home page, and the hub navigation in the global navigation panel.

1. Navigate to the SharePoint home site's **Settings** and then **Global navigation**.
2. **Enable** global navigation, enter a **Title**, and then select **Hub or global navigation** as the source.
3. Select **Save**. Changes might take a few minutes to reflect.

Hide the site navigation and display it in the global navigation

Display just the hub navigation on the SharePoint home page, and the site navigation in the global navigation panel.

1. Start by hiding the site navigation by going to **Settings**, then **Change the look**, then **Navigation** and toggle the **Site navigation visibility** to **Off**.
2. Then, navigate to the SharePoint home site's **Settings** and then **Global navigation**.
3. **Enable** global navigation, enter a **Title**, and then select **Home site navigation** as the source.

4. Select **Save**. Changes might take a few minutes to reflect.

Set up a SharePoint home site for the first time

A SharePoint home site is a SharePoint communication site that you create and set as the top landing page for all users in your intranet. The home site brings together news, events, conversations, and other resources to deliver an engaging experience that reflects your organization's voice, priorities, and brand.

It's recommended that you set up a SharePoint home site for your organization to take full advantage of SharePoint's communication and collaboration features and is required to enable and customize global navigation in the SharePoint app bar.

Set up a SharePoint home site just for global navigation

If you're creating a SharePoint home site for the main purpose of setting up global navigation, you can simplify the steps recommended to plan and launch a SharePoint home site.

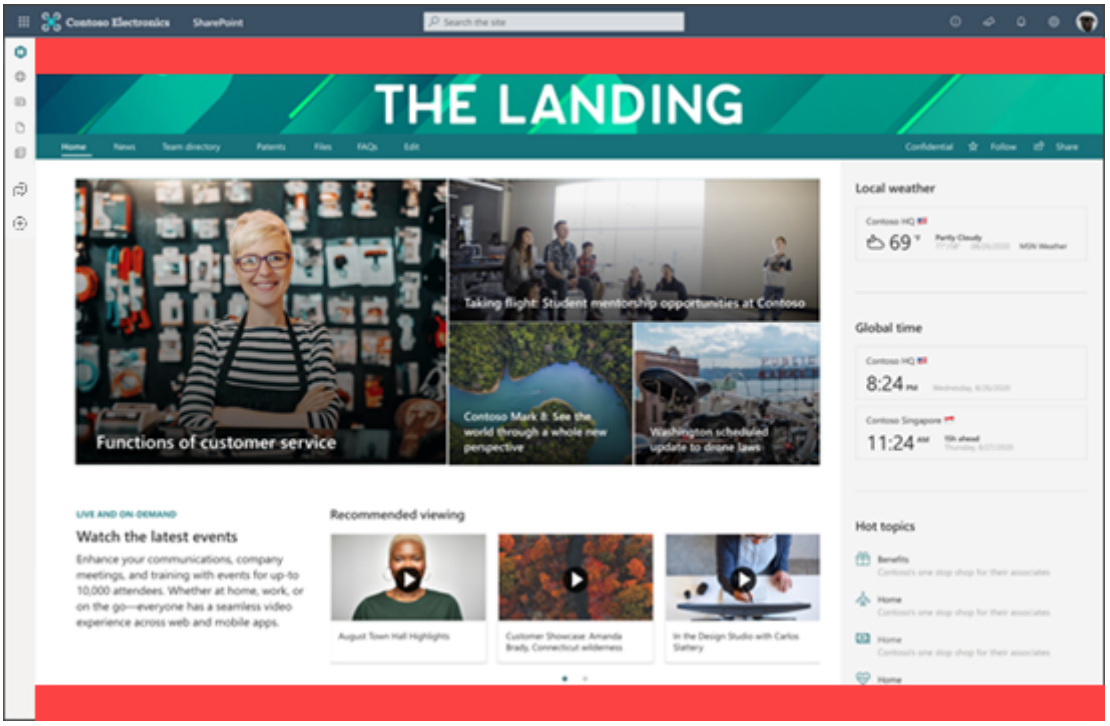
Learn more about planning navigation in SharePoint and apply information architecture principles to your new SharePoint home site's navigational design.

> **Note**
>
> - Only one communication site can be set as the SharePoint home site.
> - The first time you set up a SharePoint home site, it might take up to several minutes for the changes to take effect.
> - SharePoint admin credentials are required to transform a communication site into a SharePoint home site.

1. Start by creating a SharePoint communication site.
2. Customize the communication site navigation to reflect the view you'd like to see in the global navigation pane. You can make edits to the navigation source and individual labels and links at any time.
3. Set this communication site as a SharePoint home site within the SharePoint admin center.
4. Share the SharePoint home site with users so they can access the global navigation links.
5. On the SharePoint home site, select **Settings** and then **Global navigation** to **enable** and customize.
6. For the global navigation source, select **Home site navigation** to display the SharePoint home site navigation that you created in the global navigation panel, then select **Save**.

Understand how the app bar might affect page customizations

The SharePoint app bar might affect current page customizations, specifically customizations positioned to the left of your page. For organizations using page placeholders, the SharePoint app bar will cover parts of both the header and footer page placeholder. In the following image, the placeholder footprint is in red:



Modernize classic SharePoint sites to display the SharePoint app bar

The SharePoint app bar only appears in modern SharePoint sites and pages.

We highly recommend modernizing classic sites not only to display the SharePoint app bar but for a more consistent user experience. Learn more about how to modernize classic SharePoint sites and pages using the open-source SharePoint PnP Page Transformation solution.

Teach end users about this feature

Help end users understand how the new SharePoint app bar works.

Resources

- Learn more about SharePoint home sites

- Learn more about planning and creating hub sites
- Learn more about navigation and information architecture in SharePoint
- Learn more about sharing and permissions in SharePoint

Last updated on 10/06/2026

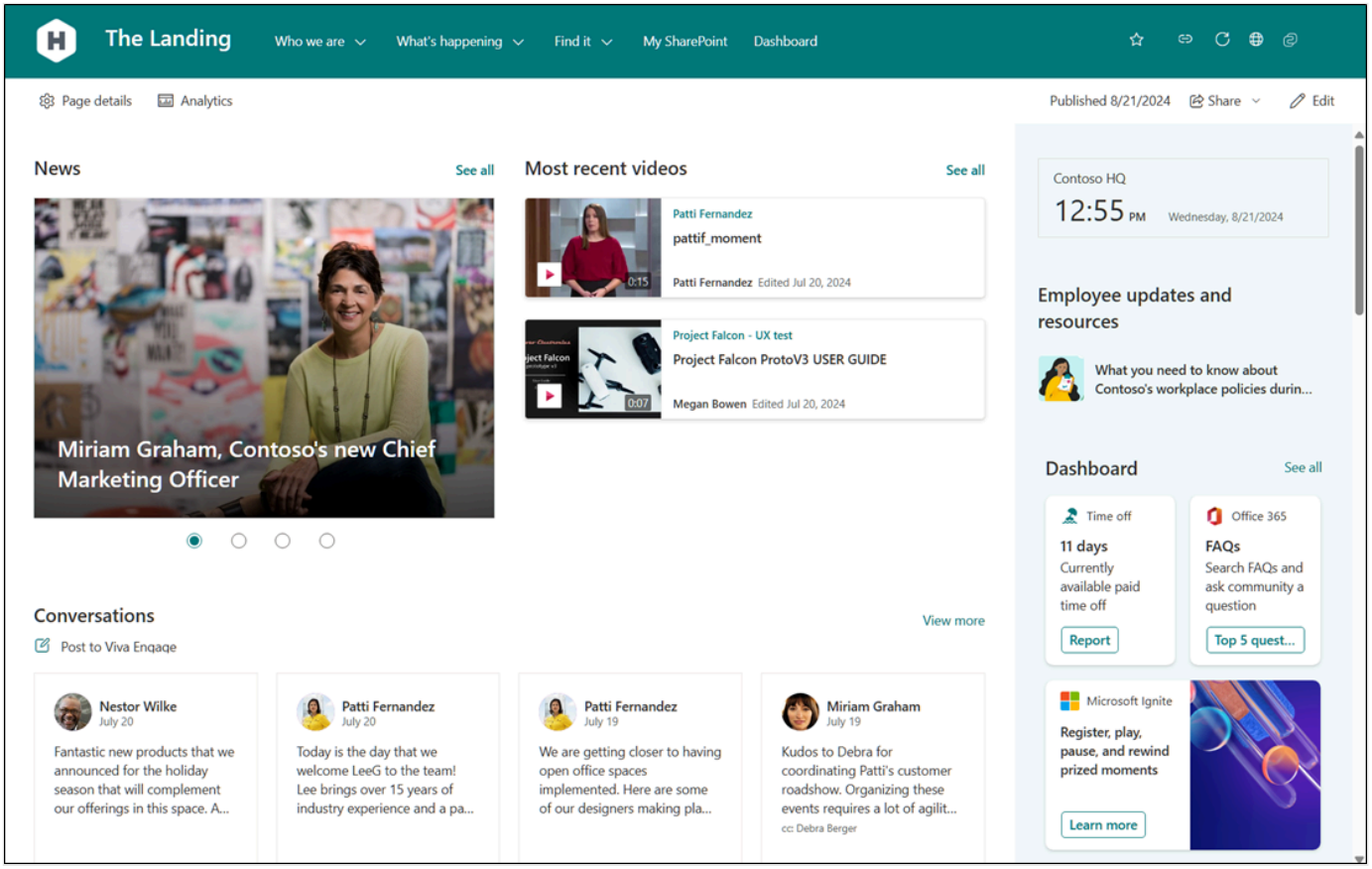
Using web parts to display content on your SharePoint site

Use the News, Viva Engage, File and Media, Highlighted content, and Video web parts to display content, videos, and files from sources across SharePoint, Viva Engage, and Clipchamp (videos stored in SharePoint) to keep users informed and engaged with news posts, conversations, and video feeds.

Each user's experience will look different because content displayed in the web parts is personalized to the viewer based on the SharePoint sites and Viva Engage communities that they follow. The tools described in this article are a good way to surface content on your SharePoint site to provide users with a steady stream of information.

Note

> - You need site member permissions (or higher) to add and edit web parts to a SharePoint site.

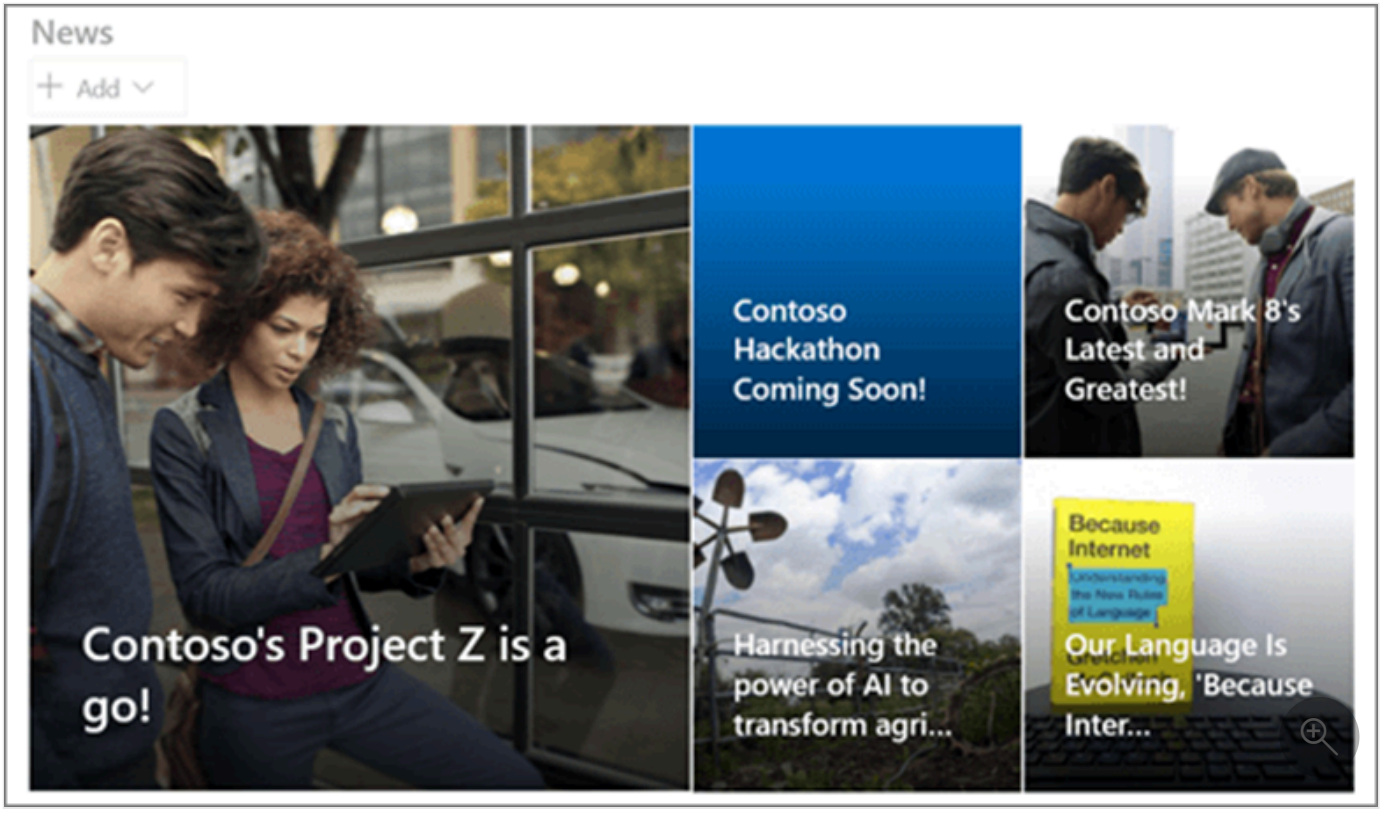


Display news posts with the News web part

Keep users in the loop and engage your audience with important or interesting stories by using the News web part on your page or site to display a collection of news posts from various SharePoint sources.

Create eye-catching posts like announcements, organizational news, people news, status updates, and more that can include graphics and rich formatting. Boost news posts so it appears in a prominent position to be seen by your organization. You can also customize the web part to change the layout, order of appearance, or target posts to specific audiences.

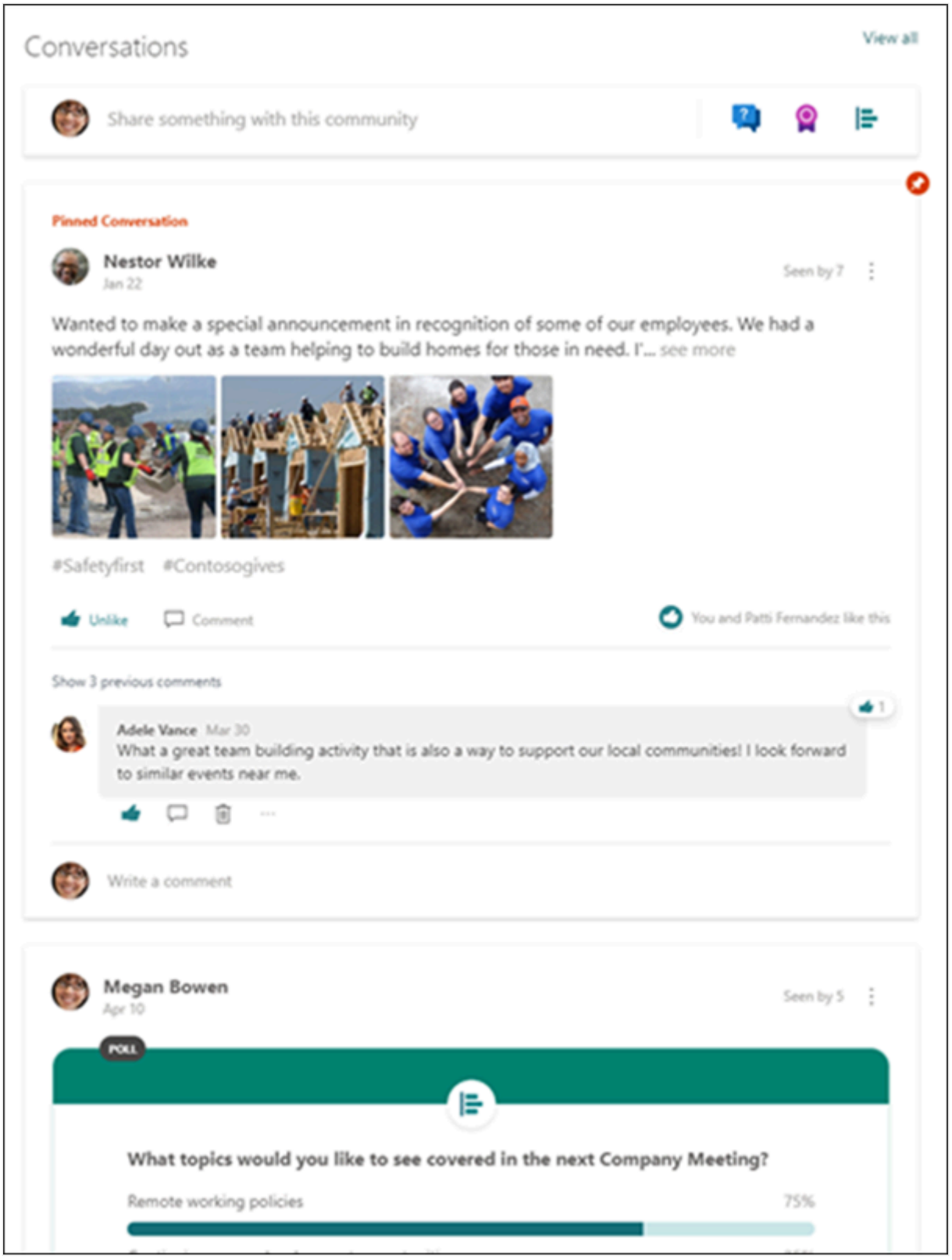
> **Note**
>
> Boosted news displays for up to four days in the News web part.



Show Viva Engage conversations and highlights with the Viva Engage web parts

Use the Viva Engage web parts, Conversations or Highlights, to help users participate in conversations with your organization's leadership, IT, Human Resources, or other internal departments without leaving your SharePoint page, or provide a quick overview of active

conversations and a targeted portal to specific groups or conversations in Viva Engage where users can start a post to ask a question, poll others, or send praise.



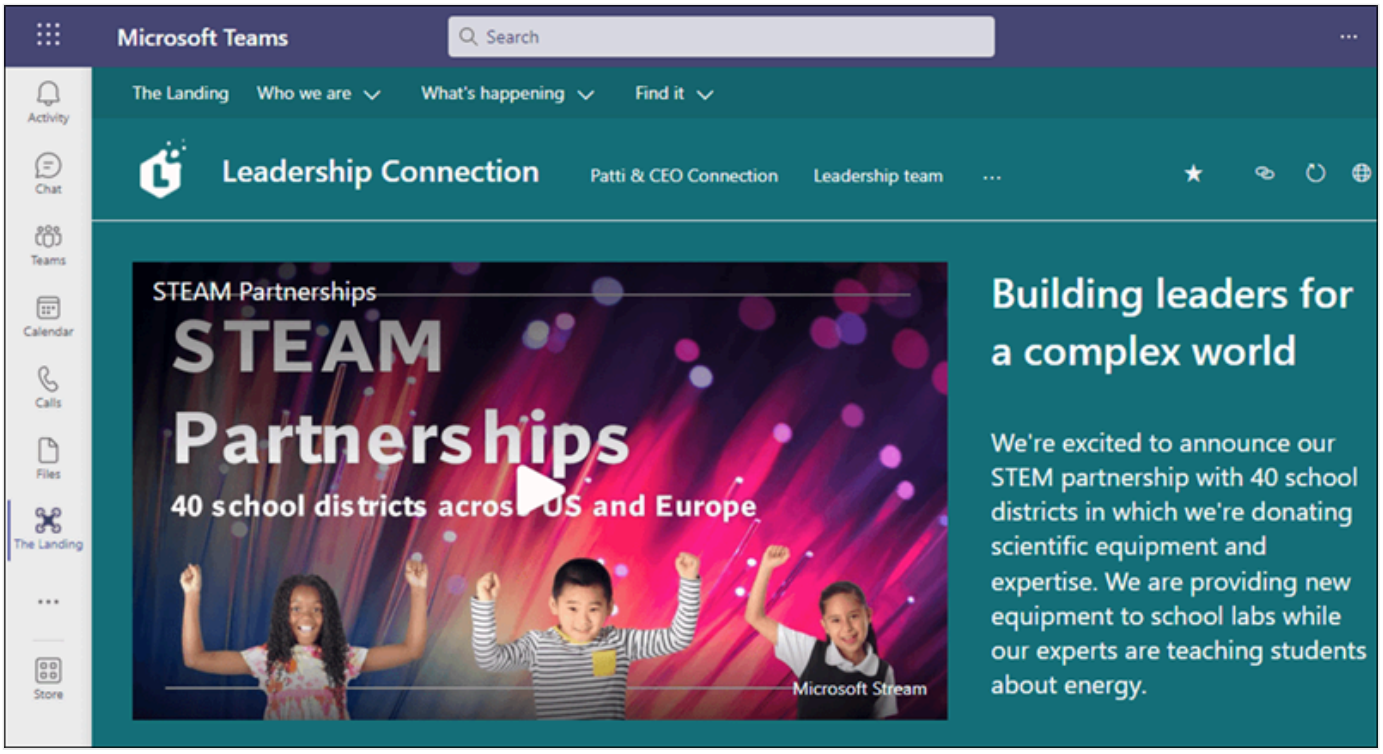
Feature videos hosted on a SharePoint site and Clipchamp

Feature a single video on a SharePoint page with the File and media web part or Video web part

If you want to feature a single video on a SharePoint page and be able to play the embedded video inline, you can use the File and Media web part.

After adding the File and Media web part to your page, you can select a video file from your site, another site, or from a link. Visitors to your page will be able to play the video directly on the page.

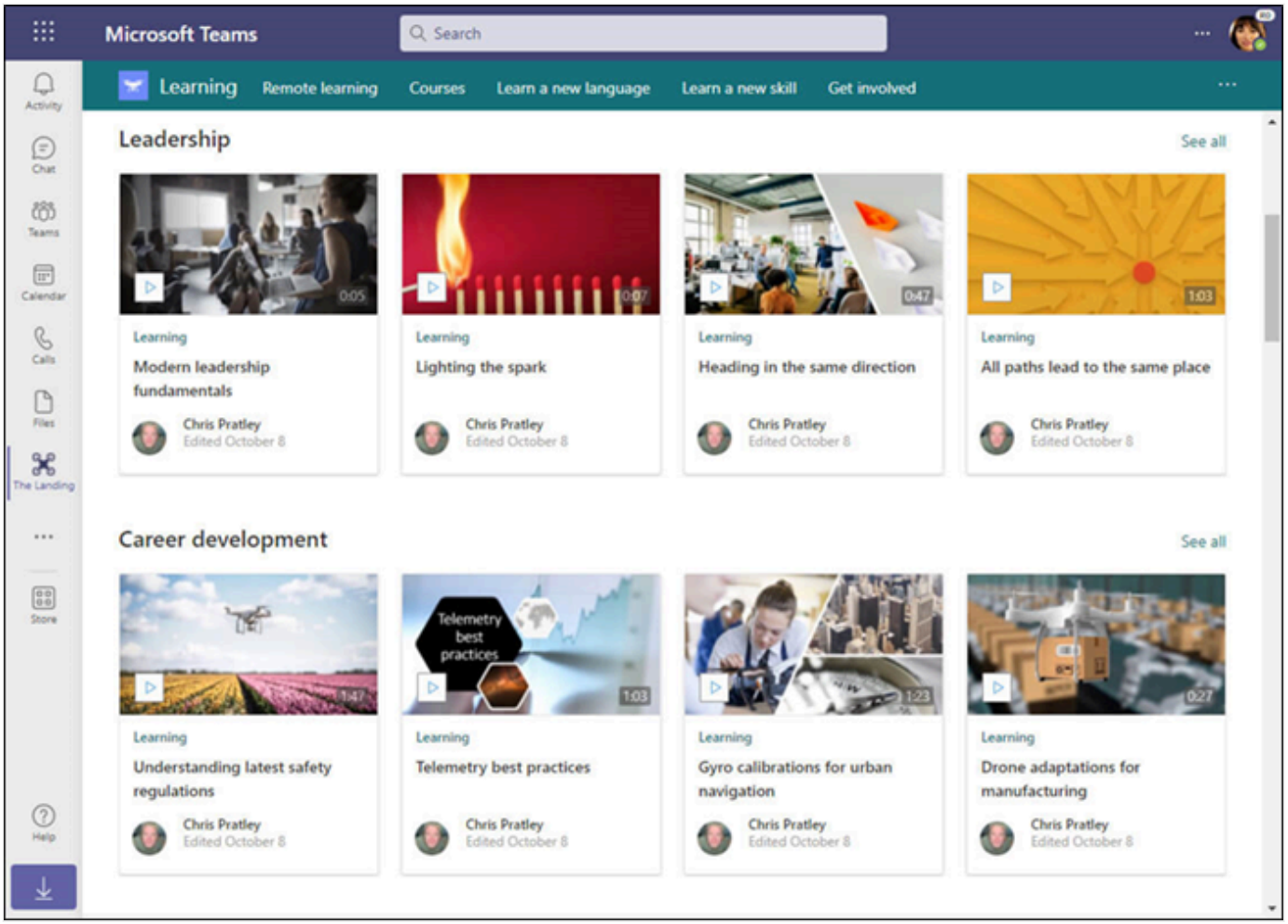
The File and Media web part can also be used to add a file on your page like an Excel spreadsheet, PowerPoint presentation, Word document, PDF, and more.



For more information, see the article on using videos on SharePoint pages.

Feature a list of videos on a SharePoint page with the Highlighted content web part

When you want to display a list of videos on a page, you can use the Highlighted content web part. You'll be able to configure how the list is filtered, sorted, and displayed. Visitors to your page will be able to select a video in the list to watch it. Using the web part, you can filter, choose sources, and sort videos that help you build a customized experience that will highlight videos to your viewers.



Additionally, you can review how to feature videos in Microsoft 365 with pages, sites, and portals.

Create video centric page content with Video Pages

Create video centric page content with video page templates. These templates are available in both SharePoint and Stream, making it easy to showcase video with customized and branded pages experience from either application.

For more information, see the article on creating video pages on SharePoint.

More Resources

Plan, build, and launch a SharePoint home site for your organization

Review using web parts on SharePoint pages

Last updated on 10/09/2026

Performance in the modern SharePoint experience

Article • 10/03/2022

The modern experience in Microsoft SharePoint is designed to be compelling, flexible and – importantly - more performant. Both SharePoint performance as a whole and the performance of individual SharePoint components such as search, lists and document libraries are affected by many factors, all of which contribute to the decisive performance metric: perceived end user latency, or the speed with which pages are rendered in the client browser. The SharePoint modern experience incorporates key performance improvements that help to minimize latency and improve SharePoint page responsiveness:

- Client-side processing and data requests
- Microsoft 365 Content Delivery Network (CDN)

More powerful computers and modern advancements in network architectures and web browsers have made it possible to improve the overall SharePoint user experience by shifting much of the data caching and processing from the server to the client machine. In this article, you will learn about how the SharePoint modern experience leverages client-side processing and the Microsoft 365 CDN to improve performance.

Client-side processing and data requests

In the classic SharePoint architecture, the SharePoint server farm executes data requests and other processing operations, returning results and rendered pages to the client. This model was intended to reduce the load on the client machine and browser, and also to reduce network traffic between the client and server farm, factors which were critical performance bottlenecks in legacy environments.

The SharePoint modern experience is designed to take advantage of the computing power of user computers and modern web browser capabilities to allow the client computer to directly perform certain data requests and processor-intensive operations such as page rendering.

The SharePoint modern experience client-side processing model can provide dramatic improvement in perceived end user latency over the classic SharePoint architecture. Keep in mind that there may be a greater dependency on the client-side execution environment as compared to the classic SharePoint architecture. As with any change to your network architecture, you should conduct a limited pilot to identify and resolve

potential bottlenecks before rolling the SharePoint modern experience into your production environment.

Microsoft 365 Content Delivery Network (CDN)

SharePoint latency is affected in part by the physical distance between your users and the location of your SharePoint environment (tenant). This consideration is particularly important for organizations that have a global presence where a site may be hosted on one continent while users on the other side of the world are accessing its content.

You can use the built-in Microsoft 365 Content Delivery Network (CDN) to host static assets to provide better performance for your SharePoint sites. The Microsoft 365 CDN improves performance by caching static assets closer to the browsers requesting them, which helps to speed up downloads and reduce latency. Also, the Microsoft 365 CDN uses the HTTP/2 protocol for improved compression and download speeds.

The Microsoft 365 CDN is composed of multiple CDNs that allow you to host static assets in multiple locations, or *origins*, and serve them from global high-speed networks. Depending on the kind of content you want to host in the Microsoft 365 CDN, you can add **public** origins, **private** origins or both.

Content in **public** origins within the Microsoft 365 CDN is accessible anonymously, and can be accessed by anyone who has URLs to hosted assets. Because access to content in public origins is anonymous, you should only use them to cache non-sensitive generic content such as JavaScript files, scripts, icons and images. The Microsoft 365 CDN is used by default for downloading generic resource assets like the Microsoft 365 client applications from a public origin.

Private origins within the Microsoft 365 CDN provide private access to user content such as SharePoint document libraries, sites and media such as videos. Access to content in private origins is secured with dynamically generated tokens so it can only be accessed by users with permissions to the original document library or storage location. Private origins in the Microsoft 365 CDN can only be used for SharePoint content, and you can only access assets through redirection from your SharePoint environment.

The Microsoft 365 CDN service is included as part of your SharePoint subscription.

For info about how to use the Microsoft 365 CDN, see Use the Microsoft 365 Content Delivery Network (CDN) with SharePoint.

For more info about the Microsoft 365 CDN, see Microsoft 365 CDN.

Related topics

Performance guidance for SharePoint portals

Tune SharePoint performance

Content Delivery Networks

Use the Microsoft 365 Content Delivery Network (CDN) with SharePoint

---

Feedback

Was this page helpful? Yes No

Provide product feedback

Creating and launching a healthy SharePoint portal

A **portal** is a Microsoft SharePoint site on your intranet with many site viewers who consume the content. In large organizations, you could have several, such as a company portal and an HR portal.

Typically portals have relatively few people who create and author the site and its content. Most visitors to the portal only read and consume the content. We don't recommend using SharePoint portals to host a town hall or live event.

> **Tip**
>
> Are you wanting to host a live event or town hall? Here are the options we recommend:
>
> - Learn about Microsoft Teams live events
> - Learn about hosting events with Viva Engage
> - Link directly to the live event you are streaming (**not** through your portal)

What type of site should I use as my portal?

SharePoint Online has several types of sites and page types. **For portals, we highly recommend using a communication site with a site page for the home page**, the default configuration when you create a communication site. Site pages allow you to use out-of-the-box web parts, custom web parts, and extensions.

To learn more, see Create communication sites in SharePoint.

> **Important**
>
> **Modern Team sites** are designed for use on collaboration sites, like projects / interest groups / focus areas or when you would like to collaborate with other team members. To learn more, see Create team sites in SharePoint.

The **App page type** was designed to be used for specific business applications within SharePoint Online. It was not designed to be used as a SharePoint Team site or a SharePoint Portal. To learn more, see [Creating application pages in SharePoint].

Guidance

This set of guidance will walk you through best practices and recommendations before you launch your portal and how to keep your portal healthy.

Expand table

Icon	What to do	Follow this
	Plan the rollout of your portal	Launch in waves
	Portal design guidance	Review the guidance while designing your sites
	Run the Page Diagnostics for SharePoint tool	Validate your pages and follow the guidance
	Optimize your Performance	Follow the guidance below and run the Page Diagnostics for SharePoint tool
	Use CDN for better performance	Implement Public and Private Content Delivery Networks (CDN)
	Batch REST API calls to SharePoint	Combine operations into fewer requests
	Improve performance for slow web parts	Follow guidance to remediate common issues
	Review page weight	Follow guidance to reduce page weight in your site pages
	Limit the number of requests to a page	Limit the number of web parts and calls into SharePoint
	Limit the number of search requests on a page	Follow the guidance to limit the number of search requests on a page.
	Optimize your images	Follow basic image optimization for the web
	Limit and use Iframes carefully	Don't use more than two Iframes on a page

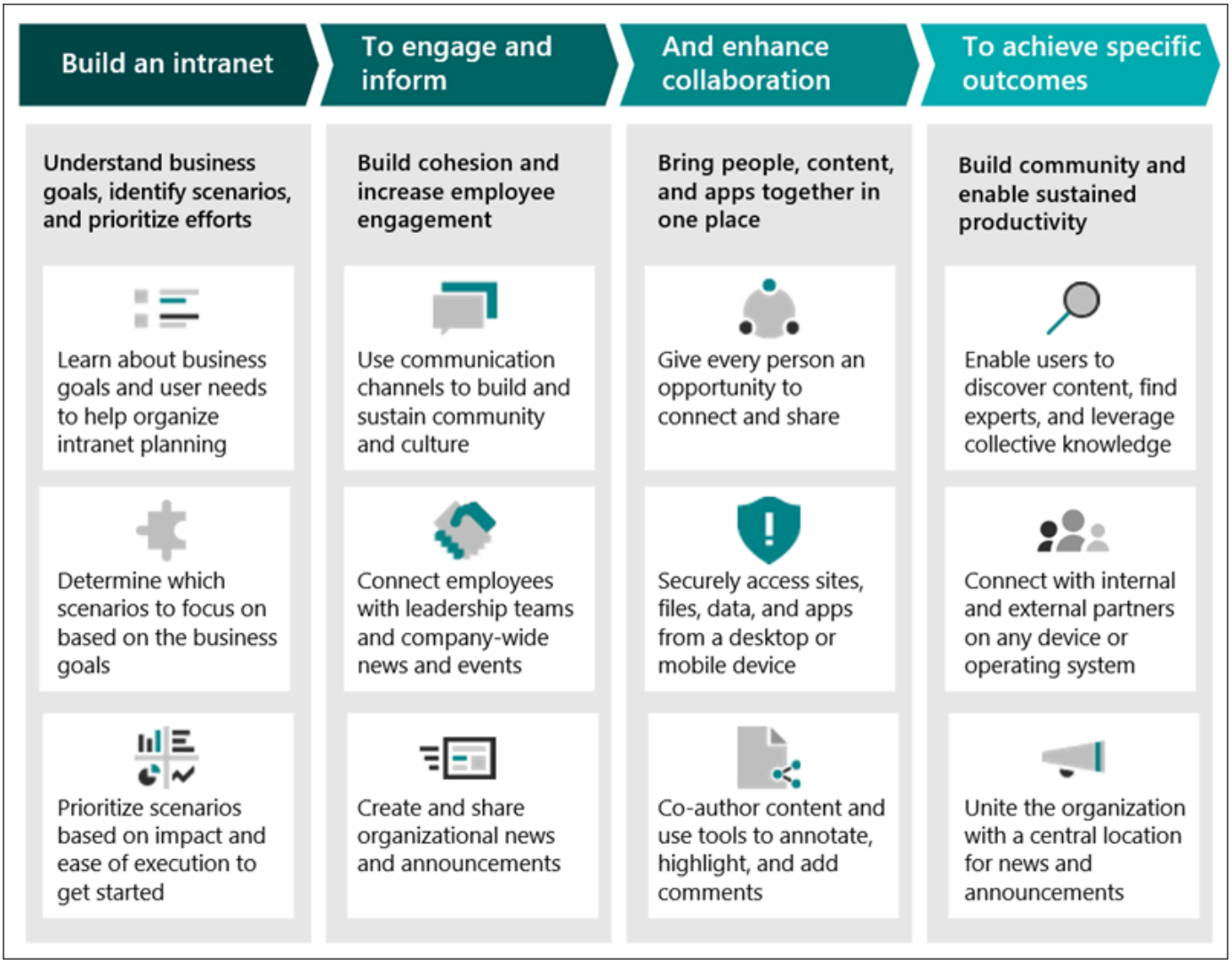
Icon	What to do	Follow this
	Optimize extensions	Follow the guidance to optimize and limit your custom extensions
	Modern portal limits	Follow the limits for modern portals to further optimize performance
	Network optimization	Configure your URLs and IP endpoints

Last updated on 06/25/2026

Intelligent intranet overview

Keep employees informed and engaged by providing a shared place to securely view and collaborate on content, and to connect and communicate with colleagues. Build community and culture within your organization by bringing people together through events, networking opportunities, and strategic communication channels. Personalize, share, and manage organizational news and shared content to drive organizational efficiencies securely on any device.

In this solution



Build an intelligent intranet

Learn how to move through the process of creating an intranet for your organization. Get familiar with common intranet planning and creation roles, design stages, and the intranet lifecycle. Learn how to align goals into priority scenarios that you can get started

implementing quickly. Then, learn how to engage with viewers and maintain your intranet over time as the organization changes and scales.

Help your organization engage and inform

Use SharePoint and other Microsoft 365 products to create communication channels that serve specific audiences. Learn how to create and share organizational news and use the News web part into key landing pages and portals.

Integrate Viva Engage and the Viva Engage web parts to embed conversations and highlights in sites. Use the power of video to share pre-recorded messages and record organizational events for later viewing. Use content services like audience targeting to make sure key audience are targeted specific content.

Enhance collaboration and sharing

Create and increase opportunities to collaborate across your organization. Use Microsoft Lists and document libraries to securely store and dynamically display content that can be accessed on any device. Then, users can view, share, and coauthor content in real time.

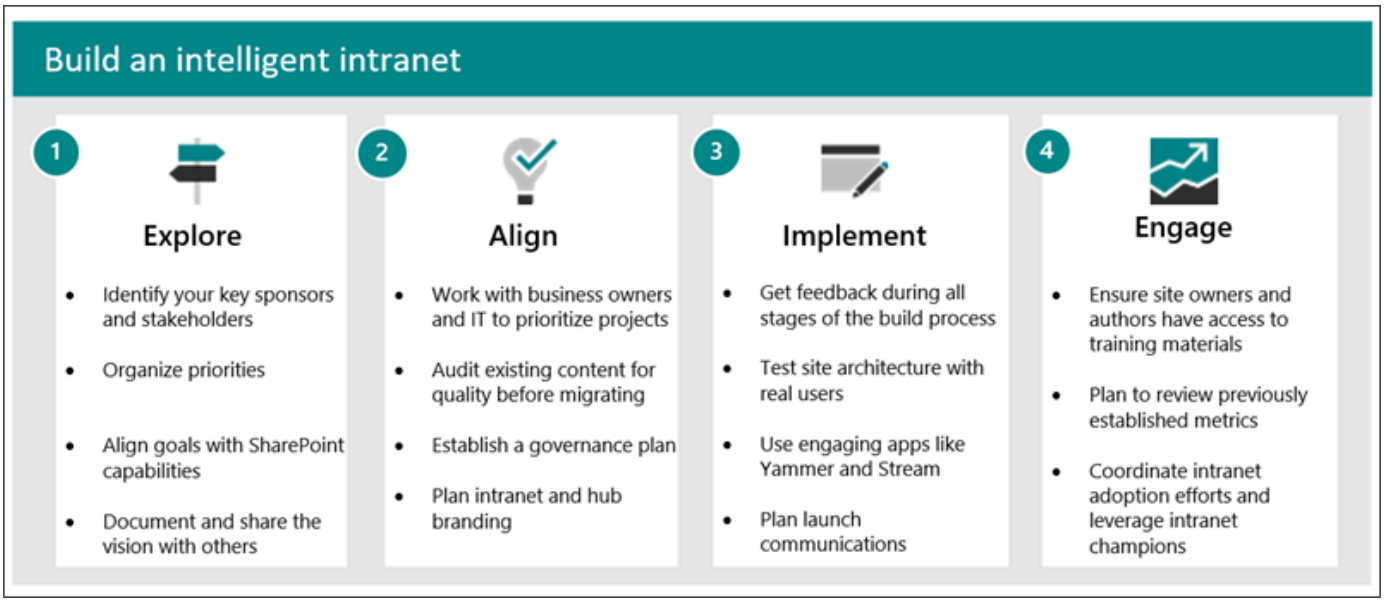
Use SharePoint team sites to create secure collaboration spaces for teams to share content, get updates, and news. Consider adding Microsoft Teams to your team site to add real-time chat and virtual meetings.

Achieve specific outcomes

Use SharePoint to achieve specific business outcomes like narrowing the distance between leadership teams and individual contributors by creating a leadership site that encourages sharing news and starting conversations. Use SharePoint to unite and inform groups of people with related interests by setting up news for a hub site. View custom solutions in the SharePoint Look Book to help inspire your next site design or simply navigate to the custom PnP site templates and select the template you need from the available templates.

Overview of how to set up an intelligent intranet

Harness the power of the intelligent intranet to communicate effectively across the organization, engage employees, and connect with relevant information and knowledge. Learn more about intranet planning and implementation phases and how to get started, and considerations like how to design your home site and use multi-lingual features. Then, use the intranet roadmap to prepare business owners, stakeholders, site owners, and content authors.



1 - Explore what's possible

Start by getting inspired by what you can accomplish with SharePoint by viewing compelling business scenarios, the SharePoint Look Book, and guided walkthroughs.

- Identify your key sponsors and stakeholders
- Organize priorities
- Align goals with SharePoint capabilities
- Document and share the vision with others

Learn more about how to think about your intelligent intranet.

2 - Understand and align

Get started planning your intelligent intranet. Learn more about intranet governance before you start building and ensure you have a plan in place to manage intranet governance. Explore various opportunities to engage viewers in workplace communications using Viva Engage, Teams, live events, and site templates.

- Work with business owners and IT to prioritize projects
- Audit existing content before migrating
- Establish a governance plan
- Plan intranet hubs and branding

Get familiar with the intranet lifecycle and site building blocks.

3 - Implement plans and start building

Start building the home site, hubs, sites, and pages that will make up the framework of your intranet. Consider using Microsoft Purview Information Barriers to ensure confidential content is seen by the right users or use audience targeting to target specific content to certain groups of users.

- Get feedback from stakeholders and users along the way
- Test site architecture with real users
- Use engaging communication apps like Viva Engage and Stream
- Plan launch communications

Learn more about intranet way finding and how to implement multi-geo features if needed.

4 - Engage and manage

Measure intranet effectiveness by reviewing Microsoft 365 usage analytics and SharePoint hub and page usage analytics. Make sure site owners and authors have appropriate training to create, build, and maintain sites.

- Ensure site owners have access to SharePoint training materials
- Plan to review site and hub metrics
- Consider using Microsoft Learning Pathways to surface training content on SharePoint pages

Expand table

Design process	Learn more
Plan sites - Help site owners understand how to plan to create high impact sites that meet objectives.	Plan your SharePoint communication site Get inspired with the SharePoint Look Book Guided Walkthroughs: Creating sites for your organization
Build sites - Learn how to create and customize sites that align with your organization.	Create and use modern pages on a SharePoint site Customize your SharePoint site Customize the navigation on your SharePoint site Using web parts on SharePoint pages
Manage sites - Show site owners how to maintain site content and use site analytics to engage viewers.	Management and life cycle of a SharePoint modern page

Design process	Learn more
	Manage your SharePoint site settings View usage data for your SharePoint site

Learn more about forming a site owner or intranet champions community to ensure that site owners stay up to date of new capabilities and guidance. Learn more about how to improve SharePoint adoption.

SharePoint intranet key capabilities by enterprise product license

Expand table

Capability or feature	Description	Licensing
Office apps	Office client apps – Word, Excel, PowerPoint, OneNote, Publisher, and Access on up to 5 PC/Macs, tablets, or mobile devices per person.	Microsoft 365 E5 Microsoft 365 E3
Social and intranet	Use SharePoint and Viva Engage to connect and engage across your organization with an intelligent, mobile intranet and enterprise social networking.	Microsoft 365 E5 Microsoft 365 E3
Files and content	OneDrive helps you work on a file and save it directly to OneDrive or SharePoint and changes are updated across synced devices. Stream lets you easily create engaging video content. Access and sync files on PC or Mac and mobile devices. Share files with external contacts by providing access or guest links.	Microsoft 365 E5 Microsoft 365 E3
Work management	Efficiently manage work across individuals, teams, and organizations. Create and automate business processes.	Microsoft 365 E5 Microsoft 365 E3

Learn more about Microsoft licensing

Get more information about Microsoft 365 for enterprise

Microsoft 365 small business license options

More intelligent intranet resources

How to think about your intelligent intranet

Plan an intelligent SharePoint intranet

Introduction to SharePoint information architecture

Planning intranet governance

Branding your SharePoint site

SharePoint adoption resources

Last updated on 06/25/2026

What's new for SharePoint home sites

This article highlights SharePoint home site updates rolling out starting May 2026 and details the specific changes due to the rename of Viva Connections to SharePoint app.

> **Note**
>
> SharePoint home site technology fully powers the Connections experience in Teams, now branded as the **SharePoint app in Teams.** Targeted Release rollout of all these updates is planned for early May 2026 with GA by end of June 2026. You can track progress on the related Microsoft 365 public roadmap: ID 557983.

A SharePoint home site provides a customized landing experience that reflects the organization's brand, voice, and priorities. A SharePoint home site also serves as the gateway to other portals in your organization's intranet. It's simply a special communication site in your organization. You can either create a new home site or set an existing communication site as your home site. An admin can do this action in the SharePoint admin center.

Viva Connections is a customizable employee engagement experience app in Teams. It is how your SharePoint intranet can be deployed within Teams desktop and mobile. With the rename of Viva Connections to SharePoint app in Teams, this functionality becomes a prominent feature of a SharePoint home site.

With this update, you can:

- Create or set a Home site in SharePoint admin center.
- Configure your home site with web parts and deploy it to your organization, just like any portal launch.
- In the home site, under **Settings**, set up the SharePoint app for Teams.

SharePoint home site updates - May-June 2026

What's not changing

- Existing home sites, site content, branding, and overall look and feel stay the same.
- Existing Viva Connections configurations, including customized app names and logos, keep working as configured.

- Existing Viva Connections deployments stay available as a branded employee experience within SharePoint.
- Organizations that require multiple home sites still need the appropriate licensing.

What's new

- SharePoint administrators can now create and designate home sites directly from the SharePoint admin center.
- A new Resources web part is available for curated links and employee resources.
- A new Announcements web part is available. We have also removed the extra Viva license requirement for using Announcements feature.
- New filmstrip layout options are available for the News web part.
- A simplified experience for configuring SharePoint app in Teams is now available directly from the home site experience.

What's changing in the user experience

- The Teams desktop and mobile branding change from the default Viva Connections to SharePoint for noncustomized experiences.
- The default app experience aligns with SharePoint branding and removes Viva-specific default content, including the "Go to Connections" UX in the default app experience. Users can get back to the default experience by double clicking the app logo in Teams left navigation and clicking on the app name in the panel.
- The global navigation experience within the SharePoint app in Teams desktop displays either SharePoint or your organization's customized app name.
- The Dashboard web part "See all" experience now supports end-user personalization and customization.

Create and designate home sites directly from the SharePoint admin center

You can now create and establish a communication site as a SharePoint home site directly within your organization's SharePoint admin center. Previously, you needed to go to the Viva Connections management console within Microsoft 365 admin center. Use the following step-by-step instructions to help set up your SharePoint home site. You must be assigned the role of SharePoint admin to accomplish these steps.

Once established, you can configure and manage your site content like any other SharePoint site - choosing your preferred theme, layouts, pages, navigation, and more.

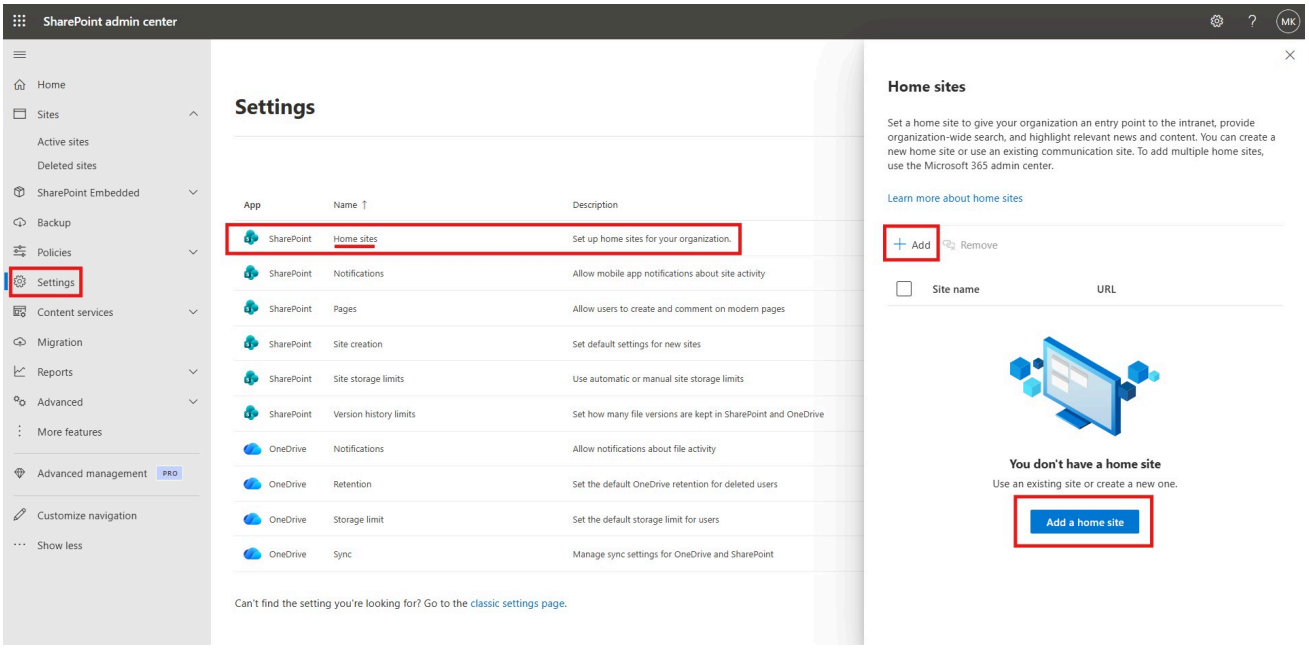
To create a SharePoint home site, follow these steps:

1. Go to your SharePoint admin center and sign in. (The URL resembles `https://tenantname-admin.sharepoint.com/`.)

2. In the navigation pane, select **Settings**.

3. Under **SharePoint apps**, select **Home sites** to open a configuration panel called **Home sites**.

4. Select either + **Add** or **Add a home site**.



5. Select the type of home site you want to add. To create a new site, go to *step 6*. To use an existing communication site, go to *step 7*.

6. To create a new site to use as your home site:

   a. Select **Create a new site**, and then select **Next**.

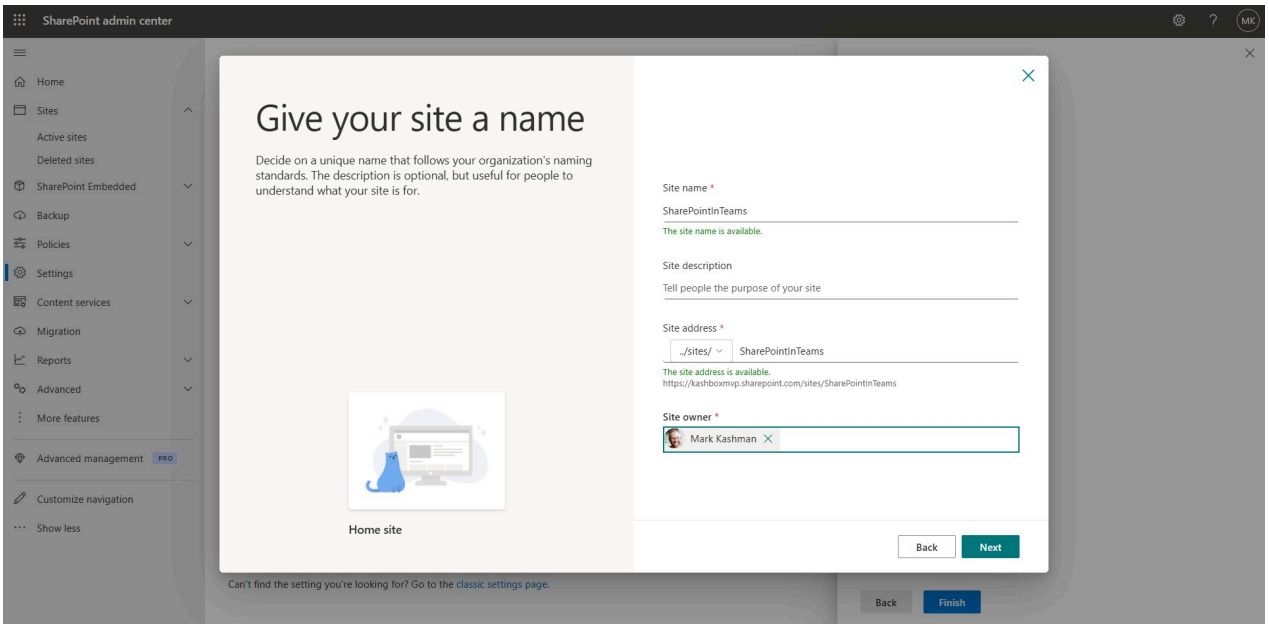
   b. On the **Preview and use 'Home site' template** page, select **Use template**.

   c. Give your site a unique name in the text box under **Site name**.

   d. Validate your site name and URL, add a site owner, and then select **Next**.

   e. Set your language and time zone, and then select **Create site**.

   The site gets created as a home site, with Site name and URL.



7. To use an existing communication site:

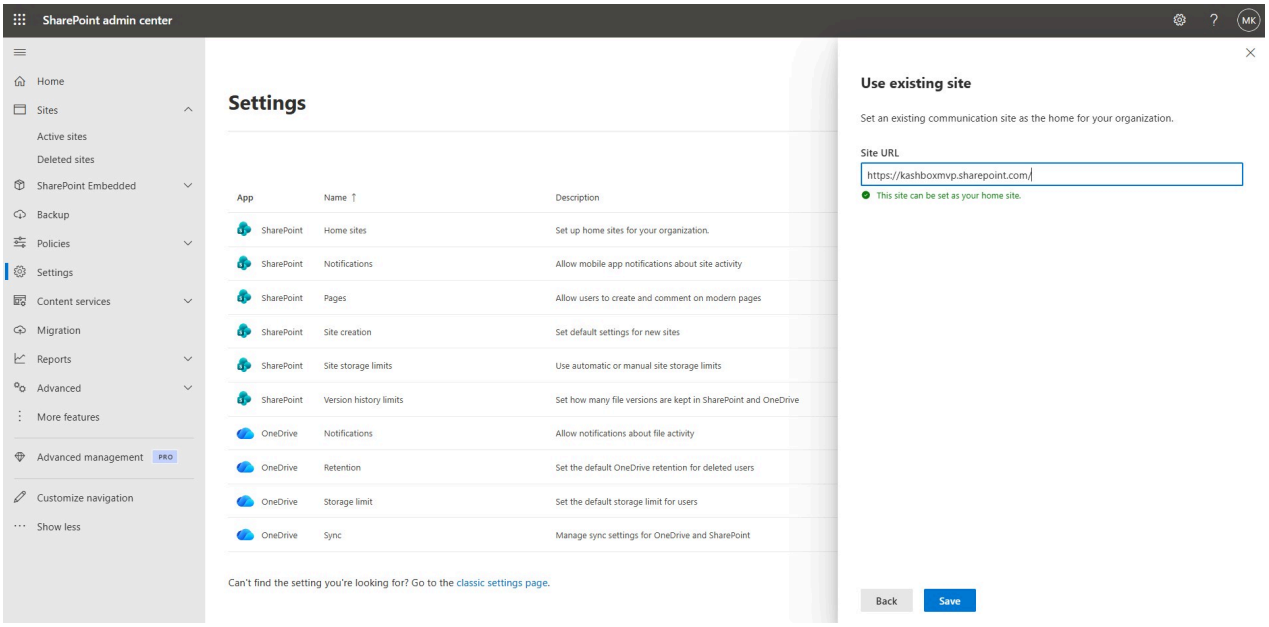
   a. Select **Use an existing communication site**, and then select **Next**.

   b. Specify the site URL of the existing communication site you want to set as your home site.

   c. Validate that this site can be set as your home site. Green text indicates that the site meets the criteria.

   d. Select **Save**.

   The specified site is assigned as a home site, with its site name and URL.



Note

To add multiple home sites, you must still go to Viva Connections in the Microsoft 365 admin center.

Last updated on 09/28/2026

How to think about your intelligent intranet

These days, there's an abundance of discussions about best practices to modernize your intranet - designing an intranet the new way, in the “modern” way, in the intelligent way - and so on. There aren't many discussions about what modern means as a concept, how modern thinking relates to technology, and how to apply modern principals to your organization's intranet.

Use this guide to understand how to leverage SharePoint to meet your organization's needs through integrating modern concepts into the design of your intranet, portals, and sites.

What does intelligent mean?

In the modern world, the intranet should be the center of your workplace. An intelligent SharePoint intranet is engaging, informative, personalized, and integrated with the other portals and sites in your intranet as well as other Microsoft 365 apps like Microsoft Teams and Viva Engage. Modern intranets take many shapes and sizes depending on the ever-evolving needs of the business.

Hallmarks of what constitutes an intelligent intranet:

- **Rapid deployment**: Adaptable designs can be built using out of the box pages and web parts and no longer solely depends on IT to deploy.
- **Built with the UX in mind**: Accessible design principals are built into the modern experience enabling viewers to securely access the intranet on any device.
- **Personalized experience**: Features like audience targeting, news, the Highlighted Content web part, and the My Feed web part make it easy to dynamically display personalized content.
- **Software as a service**: Updates are automatic, ensuring you are using the latest technology.

Why invest in the modern approach?

Investing in the modern approach looks different depending on the condition of your current intranet but no matter the path it will require strategic planning and a team to implement changes. By spending resources modernizing your intranet now, you will enable your organization to move faster and more efficiently than before.

What makes modernizing your intranet worth the effort:

- **Move at the speed of your business**: Display content dynamically using flexible designs that scale as your business grows.
- **Meet employees where they are**: Target relevant content to specific viewers on any device.
- **Reduce the cost of technical resources**: Security, permissions, sharing, and other governance components can be centrally managed across Microsoft 365 apps.
- **Improves the likelihood of intranet success**: Viewers are more likely to use the intranet when content is relevant, easy to navigate, and mobile.

How to think about intelligent intranets

Secure and accessible

Expand table

Traditional	New	How to get started
Deployed solely by IT	Relies on a collaborative approach with several stakeholders across departments of the organization	Instead of assigning intranet tasks to a few IT members, assemble a team that represents the needs of your viewers and business to create intranet solutions. Learn more about modern intranet teams
Manually governed by IT	Uses governance models that provide flexibility for users in a compliant way based of the organization's goals - sharing, provisioning, risk mitigation	Instead of asking for permission to create a site from IT, site owners can create their own sites using SharePoint's out-of-the-box responsive designs and custom theming. Learn more about managing site creation
Resources can only be accessed in the office or on a computer	Work anytime, anywhere, any place, on any device	Instead of limiting access to content, use SharePoint security and compliance features to make sure viewers have access to the right information on any device. SharePoint works by default on mobile devices.

Informs and engages

Expand table

Traditional	New	How to get started
Communication primarily through email	Communicate primarily through SharePoint news, community portals, and Viva Engage	Instead of sharing a project update in a newsletter, announce your update on your project's site and in the Viva Engage feed to start an engaging conversation. Learn more about using the Viva Engage web part
Outdated news is shared in a corporate news feed or newsletter	SharePoint news posts transform news into a visually engaging experience that can be created quickly and distributed to specific audiences in real-time	Instead of communicating big announcements through an org-wide email, create a news post that will dynamically display to your relevant audience. Learn more about creating a news site
Disjointed experience for international organizations	Multi-lingual and audience targeting features ensure users relate to relevant information	Instead of creating separate experiences for unique viewers, target navigational links to specific audiences. Learn more about targeting content to specific audiences

Builds community and culture

Expand table

Traditional	New	How to get started
Intranet structure is based on organization structure	Role and task-based portals house community initiative-driven projects	Instead of separating content by organizational structure, use hubs to organize content based on business initiatives. Learn more about planning hubs
In-person gatherings to build team and organizational culture	Frequent engagement through online events that showcase people, celebrate milestones, and maintain consistent conversation using Viva Engage and Microsoft Stream	Instead of semi-annual gatherings, record online events and embed the event recording using Microsoft stream in a news post. Learn more about using the Stream web part.
Infrequent interaction between the organization and leadership	Aligns organizations with leadership through live events, dynamic content like news, and social connection	Instead of formal engagements with leadership, create accessible outlets in the form of live events in Viva Engage. Learn more about organizing a live event in Viva Engage

Creates and extends knowledge

Expand table

Traditional	New	How to get started
Static information like FAQ	Dynamic information that's community generated in Viva Engage	Instead of creating a FAQ page, embed a Viva Engage web part that connects viewers to subject matter experts and provides insights into previous conversations. Learn more about using the Viva Engage web part
Browse to find	Search *and* browse to find	Instead of limiting viewers access to content, use SharePoint modern search features that protect sensitive content while increasing search success. Learn more about search in SharePoint
Collection of websites	Collection of experiences	Instead of organizing your internet by area of business, organize by business outcomes and initiatives. Learn more about planning hubs
Limited number and access to subject matter experts	Find subject matter experts and communities of expertise	Instead of relying on finding subject matter experts in siloed organizations, surface expertise in social communities like Viva Engage and Teams. Learn more about organizing a live event in Viva Engage

Moving in the modern direction

Understand that your intranet is an ever-evolving component of your business that will need to grow and scale alongside your organization. Focus on incorporating modern changes that will have the greatest impact to your business first. Plan and schedule when changes will be incorporated and how you will track progress. Use site analytics to understand user behavior and collect feedback from users along the way.

Signals your intranet is moving in the modern direction:

- It's where you start your workday
- It's always with you
- Promotes collaboration
- It makes your job easier
- Everything is in one place

Signals your organization can benefit from modern:

- Currently sharing documents in shared folders on a server
- It's difficult to be productive on-the-go
- Your business is growing faster than you can keep up with
- Unmanageable volume of emails
- Your organization has offices in multiple locations

More modern resources

Modern inspiration in the SharePoint Look Book

Information architecture in modern SharePoint

Modernize your classic SharePoint sites

Modernize your classic SharePoint pages

SharePoint modernization scanner

Last updated on 06/25/2026

Intelligent intranet introduction and roadmap

Your intranet might include your organization's main landing page, portals for corporate communications, and individual sites for departments or divisions (like IT or HR). In this article, we look at the high-level tasks needed to create and maintain a successful intranet with SharePoint in Microsoft 365.

Whether you're the organization intranet owners, an IT Professional or administrator, a site owner, or a content creator you're in the right place. Use this article as a guide to help you find the resources that you need for your role and the goals that you have for your intranet. As you read the sections below, follow the links for more detailed information on the areas that you're working on.

Roadmap contents:

- Introduction to key success factors and considerations
- Review of the different roles and tasks
- How to get started

Who should use this roadmap?

- **Organization intranet owners** — This is the person managing the overall direction and coordination of your organization's intranet.
- **IT pros and admins**—One or more IT and SharePoint Administrators who are responsible for managing the backend configuration and implementation for your organization's intranet.
- **Business owners and site owners**—The various stakeholders who are responsible for creating and maintaining portions of the intranet.
- **Content authors** — The people creating and managing content on sites and pages.

What you'll learn:

- Understand, at a high level, the various roles, and responsibilities of creating an intelligent intranet.
- See what you can do with SharePoint out-of-the-box sites and web parts.
- Framework for planning and aligning your intranet around strategic business outcomes.

- Known success factors for creating engaging intranet experiences.

Keep in mind:

Intranets are a constant work in progress and are never really considered done. Make sure you have a plan to keep your content relevant, otherwise your intranet starts losing value on the day that you launch. Celebrate your initial launch, plan to monitor and maintain your intranet and its content over time as the organization changes and business goals evolve.

How to think about an intelligent vs traditional intranet design

The new, modern experience in SharePoint is designed to be compelling, flexible, and more performant. The modern experience makes it easier for anyone to create beautiful, dynamic sites and pages that are accessible and mobile-ready. Modern SharePoint supports intelligent workplaces — those that apply the collective knowledge of current users, share and collaborate easily, and engage audiences with targeted content and news.

Expand table

Traditional intranet	Intelligent intranet
Communication primarily through email	Communication primarily through SharePoint sites and community portals
Static information like FAQ	Dynamic information that's community generated in Viva Engage
Corporate news dominates the newsfeed	Personalized news and content is targeted to specific audiences
Hierarchical collection of websites	Dynamic collection of experiences and services provided by independent site collections

Key success factors

Over the years, we have learned about what makes an intranet successful. These factors can help accelerate the creation, adoption, and overall success of your intranet:

- Ensure that your intranet goals are directly tied to key business outcomes.
- Have an executive sponsor and identify intranet champions.
- Establish KPIs that are regularly communicated from the project's start to finish.
- Design for simplicity and longevity.

- Involve your business owners and users to get feedback during all stages of the design process.
- Establish a governance plan that defines roles and responsibilities, guidelines, and best practices, compliance and retention, provisioning sites, and expectations for content management.
- Audit existing content to ensure quality and relevancy before migrating to a new intranet.
- Align your intranet with your organization brand and culture.
- Enable social connection that encourages communication, engagement, and collaboration.
- Train your content creators and your users.

Up next

Review the different roles and responsibilities when creating your intelligent intranet.

Related articles

Create and launch healthy portals

Ways to work with SharePoint

Guide to the Modern experience in SharePoint

Last updated on 06/25/2026

Introduction to roles, tasks, and timelines

When planning to create, or update, your organization's intranet, there will be several people involved. The best intranet teams aren't large but contain the right partners and stakeholder who can make decisions that serve the entire organization.

Roles and tasks at-a-glance

Expand table

Your role	Aligning tasks	Implementation tasks	Management tasks
Organization intranet owners	Strategy, branding, adoption, governance, information architecture, and change management		
IT pros / Admins	Platform integration, content migration, performance, scalability, user training	Site creation, navigation, search, branding, publishing	
Business owners / site owners	Business objectives, permissions, content audit, and migration	Site creation, navigation, branding, audience targeting	Site management, scheduled content audits
Content authors	Content best practices, content, and site design	Create and maintain content, content collaboration	Update existing content, publish new content

See what the intranet lifecycle looks like.

Learn more about basic site building blocks.

Organization intranet owners

The intranet owners work with business owners and IT to prioritize the intranet projects in your portfolio for the greatest business benefit.

Start by getting inspired with the SharePoint Look Book. The look book provides examples of intranet pages that you can build in SharePoint and will give you an idea of the possibilities. Keep these in mind as you proceed through the planning and implementation process.

Next, start to plan your intelligent SharePoint intranet by working with your key stakeholders to understand your key business and intranet goals. Do research with intranet users to discover key personas and scenarios. Review your existing intranet and determine which initiative to start with for your best return on investment. As you prioritize your intranet initiatives, consider how to get the best performance and scalability from the portals that you build. If your existing intranet is using SharePoint server, consider how migrating your content to SharePoint fits into your overall plan. To troubleshoot page performance issues, use the page diagnostics tool.

Choose one or more opportunities to start with and meet with the business owners in that area of your organization to plan the solution. Some solutions may require coordination among different parts of the organization.

As you plan and implement your intranet, keep in mind these key success factors:

- For your intranet, as a whole:
  - Have a sponsor for each initiative and an executive sponsor from the business for the intranet as a whole.
  - Ensure that your intranet goals are directly tied to key business goals.
  - Get a core team together to think about governance—make sure you align your governance decisions to business goals.
  - Align your intranet with your organization brand and culture.
  - Don't assume you have to launch with a "big bang"—align communications and training with your launch plan.

- For each initiative:
  - Gather outcomes, not requirements—be sure to talk to site users, not just owners.
  - Design to align to your organization standards—but allow the site "story" to dictate the navigation and page layouts.
  - Establish success goals for each site and review them regularly.
  - Test your proposed navigation with site visitors—make sure that visitors can easily get to their top tasks.

Key tasks

Organize your intranet

A critical part of your SharePoint intranet is your site architecture. By using a series of communication sites and hubs, you can create an intuitive intranet with common navigation across related sites and an easy-to-manage permissions structure. For a detailed look at site navigation in SharePoint, see Planning navigation for the modern SharePoint experience.

*Start by—Developing an understanding about what you need your intranet to accomplish and start organizing content assets to align with key outcome goals. Organize depending on the needs of the business—by region, department, or function—and by the topics that your users care about.

You know you're done when — Business owners and users confirm they can find and have access to the content that makes their jobs more productive.

Brand your intranet

Branding provides a way to align your intranet with your organizational culture. With SharePoint, you can add branding to your SharePoint site, and also customize the Microsoft 365 theme for your organization.

*Start by—Answer, do you need a consistent brand across all sites or will different divisions, departments, or groups in your organization have their own look and feel? Then, collect approved brand assets like brand colors, logos, and images depending on your organization's branding requirements.

You know you're done when — You've determined the end-to-end look of the intranet from the home page to hubs to individual sites.

IT pros and admins

IT Pros and admins implement the needed platform integration steps needed by your business owners for their intranet portals—such as with databases or line-of-business applications. This may include content migration from existing systems. They also work with other stakeholders and the business to determine a governance strategy for the intranet and train people in the organization to use SharePoint and other tools to manage the intranet.

As you plan and implement your intranet, keep in mind these key success factors:

- Establish a governance plan that supports business needs and your retention, security, and compliance goals.
- Make sure all site owners, content authors, and visitors understand how governance applies to their roles.
- Clean up existing content prior to migration. Only migrate content that is relevant, current, and supports the outcome goals of each site.
- Enable social connection that encourages communication, engagement, and collaboration.
- Train your content authors and your users.

Key tasks

Plan and align the governance strategy

Governance is the set of policies, roles, and processes that control how your organization's business divisions and IT teams work together to achieve its goal—ensuring organization content and communications are secure and viewers benefit from a consistent experience. Every organization has unique needs and goals that influence its approach to governance. Some details to consider when planning your governance strategy: naming conventions, guest access, classification of sites, groups, and files.

Start by — Understanding the rules and requirements of your organization, in combination with the needs of business owners and site owners. Then, develop a plan alongside IT, HR, and senior leadership that allows employees to maximize the value of SharePoint with minimal oversight in a way that's compliant.

You know you're done when — When governance stakeholders, business owners, and content creators can work effortlessly in SharePoint without slowing the rhythm of business.

Migrate content from your existing intranet

Your existing intranet may contain content from various sources located on different platforms. A key task in creating your intelligent SharePoint intranet is determining the state of your existing content and deciding which content to migrate to the new intranet.

Your current business owners and site owners may be best suited to evaluate if content should be migrated and you may want to have them perform the actual migration, depending on what's involved. They may need your assistance depending on the quantity and location of the content to be moved. Learn about options for migrating from file shares, SharePoint Server, and other cloud providers.

Start by — Working with business leaders and other content stakeholders to review your existing content for relevance and accuracy.

You know you're done when — A curated set of content has been migrated to SharePoint.

Customize SharePoint to meet your business needs

With the SharePoint intelligent experience, you can create an engaging, easy to maintain intranet without the need for customization. We highly recommend using SharePoint default experiences where possible. This will provide easier change management over time.

If you do need to customize SharePoint, SharePoint provides Framework solutions, apps, add-ins, and solutions to help you meet your business needs. For more info, see SharePoint development.

Train your content authors

Depending on their background, the people in your organization may need some help getting started with SharePoint. Microsoft 365 learning pathways provides a way to bring a curated set of Microsoft content to your users. Other references that can help your content creators manage updates to the site include:

- Create a document library in SharePoint
- Create a list in SharePoint
- Add text and tables to your page
- Add content to your page using the Embed web part
- Use the image web part
- Use the News web part on a SharePoint page

Start by — Determining your users' needs for training on SharePoint and making these references known.

You know you're done when — Questions about SharePoint intranet usage on organization social media channels and through the help desk have decreased to a modest level.

Business owners and site owners

As a business owner, you may be responsible for intranet content for a specific area of your organization such as HR or operations. You may also be the site owner, the person who has the permissions in SharePoint to create and maintain the content and experiences on the site. Before you start configuring individual sites, for some ideas, look over the SharePoint Look Book. As part of your overall governance plan, you may decide that sites need to follow consistent patterns to ensure that readers to not have to spend too much time orienting themselves as they go from site to site or topic to topic in the intranet.

Keep in mind these key success factors as you plan and implement your intranet:

- Have a relentless focus on user experiences as you implement your site — check labels for relevance, ensure images relate to the content, don't assume — test!
- Clean up existing content prior to migration. Only migrate content that is relevant, current, and supports the outcome goals of the site.
- Involve your users to get feedback during all stages of the build process.

- Make sure the site owner or contact is visible in a consistent place on the home page of the site so that visitors know to whom they should reach out for feedback.
- Plan launch communications, which might include a launch event or activity. Celebrate your success!

Key tasks

Migrate your data

One of the largest tasks in creating a new intranet site is migrating your existing data to SharePoint. We highly recommend doing a content audit to see what's being used, what's up to date, and what's no longer needed and can be deleted or archived.

Look for opportunities to eliminate prior versions of documents that you no longer need. If you migrate files ending .v1, .v2, and so on, you create confusion for your users who won't be able to rely on search to consistently find the latest version of documents.

Train your users to take advantage of SharePoint's automated versioning — and remove version IDs and dates from file names wherever possible, migrating only the latest and most accurate version. Better still, see if you can convert legacy documents to modern pages to create more engaging and easier to consume content. You get better search experiences and achieve higher user satisfaction and easier maintenance by removing content that's no longer needed prior to migration.

Learn about options for migrating from file shares, SharePoint Server, and other cloud providers.

Video is a great way to communicate to the people in your organization for executive briefings or when sharing ideas through video can lead to greater engagement. Use Microsoft Stream to deliver live and on-demand meetings, events, and training. If you have existing video content that you want to make available on your new intranet site, upload it to Stream as part of your content migration process.

Start by — Understanding the full scope of content that might need to be migrated and then define the criteria used to target content that should be migrated, should be edited and then migrated, and should be retired.

You know you're done when — You've got the minimum amount of content necessary to create and launch an effective SharePoint site.

Determine your permissions and sharing strategy

SharePoint permissions are managed through a set of roles within a site — owners, members, and visitors. Depending on the type of site, there may be more permission and sharing options available like using Microsoft 365 groups.

Start by — Determining who needs access, who shouldn't have access, and how you grant access requests.

You know you're done when - All site owners and users have access to the content they need, while securing confidential content when appropriate.

Design the intranet portal page, also known as the home site

The main intranet portal for your organization is a large part of your new SharePoint intranet. You can create this page at any time during your intranet development project. You can still point to your legacy intranet sites with an intelligent portal home page. If you have an existing communication site that you want to use as your main portal page, you can move it to the root site.

The mega menu, news web part, and Viva Engage feeds can all be used to make your main portal page an engaging and productive destination for your users. For an end-to-end look at creating this page, read Guided walkthrough: Creating an Enterprise Landing site for your organization.

Start by — Considering the goals from the perspective of your organization's communications team, your executive sponsor, your IT department, and end users. Design the portal home page with simplicity and scalability in mind.

You know you're done when — You've created a launch plan using the Portal launch scheduler for redirecting from your current portal page to the new page and have shared this plan with all stakeholders and users.

Design your business, or topic-specific intranet site

As you start designing the intranet sites for your services and functions, make sure you have done research with your users to better understand their needs and how they currently interact with your content. To create custom surveys and questionnaires and spend time observing users and meeting with them, you can use Forms.

We recommend developing your intranet pages using communication sites. With communication sites, you can share news, reports, statuses, and other information through various templates and web parts. For an end-to-end look at setting up a communication site, see

Guided walkthrough: Creating a communication site for your organization. Learn more about how to plan your sites.

To post important or interesting stories, announcements, people news, status updates, and more that can include graphics and rich formatting, you can use the news web part. Within the news web part, to prioritize specific content for specific audiences, you can set up audience targeting. For an end-to-end look at using news in SharePoint, see Guided walkthrough: setting up news for your organization.

To align your organization's branding requirements, you can change the look of your site.

Start by — Prioritizing business objectives, and then decide the type of sites and web parts that are needed initially.

You know you're done when — Business and site owners have dedicated areas in SharePoint that can be owned and maintained with little oversight.

Content authors

Content authors are the people who create content on sites. Content authors can take on many responsibilities such as creating and publishing news, creating topic-specific pages, or serving as subject matter experts and thought leaders for special projects and initiatives. Content authors should get familiar with SharePoint design fundamentals.

As you create and manage content for your intranet, keep in mind these key success factors:

- Consider whether content is best presented as a page or a document. Use pages when your content is dynamic and most easily communicated with engaging web parts such as images, video, or links. Use documents when your content is designed to be downloaded or printed.
- Summarize up front — place the information readers must have for your communication to be successful at the top of the page before you focus on the design.
- Use sections and heading styles to visually separate topics and concepts to make your pages more readable and accessible.
- Create custom page templates to drive consistency and simplify page creation.
- Ensure you follow image and video guidelines to keep page performance high.

Key tasks:

Inform and engage

Collect and manage content using SharePoint pages. Use lists for information you might collect in Excel. Lists enable you and your audience to gather, track, and share information. Improve the display of lists with column and list view formatting using the List web part. Use libraries to store documents. Easily add, reorder, sort, filter, and create custom views of libraries using the Document library web part.

Dynamically display content from a document library, a site, a site collection, or all sites using the Highlighted content web part.

Create and curate news relevant to your audience using the News web part. Quickly create eye-catching posts like announcements, people news, status updates, and more that can include graphics and rich formatting.

Customize the way your users view content and news by using audience targeting. Audience targeting enables specific content to be prioritized to specific audiences on the SharePoint start page, news on the mobile app, and in News web part when audience targeting is enabled.

Enable users to work on any device. When users keep files on their local device or on a network share, they're out of luck when they don't have the device with them or don't have a connection to your network. If something happens to a user's device, the data might not be recoverable. Get the SharePoint mobile app.

Start by — Organizing content into topics, creating pages for each topic. Determine whether the page content should include text, links, list, or libraries. Align the content to the story to ensure that the reader can get the information that they need efficiently by quickly scanning or skimming the page.

You know you're done when — You can confirm users have access to the right information at the right time by using site usage and analytics, and asking users for feedback.

Build culture and community

Help work groups connect and engage across your organization using Viva Engage. Learn more about the Viva Engage Highlights and Viva Engage Conversations web parts. Sometimes content needs to be delivered through video - like when organization-wide announcements are made or when senior leaders host a live event or when you want to provide examples on pages that provide instructions. Microsoft Stream is your organization's own video site. To display video content, use the Stream web part.

Start by — Finding news, announcements, and events to amplify on your site.

You know you're done when — You're regularly promoting news and events that start conversations and engage and connect wide audiences.

Up next

Learn more about how you can get started creating or updating your organization's intranet.

Related topics

Create and launch healthy portals

Guide to the Modern experience in SharePoint

Intelligent Intranet Envisioning Workshop PowerPoint deck

Plan your intranet

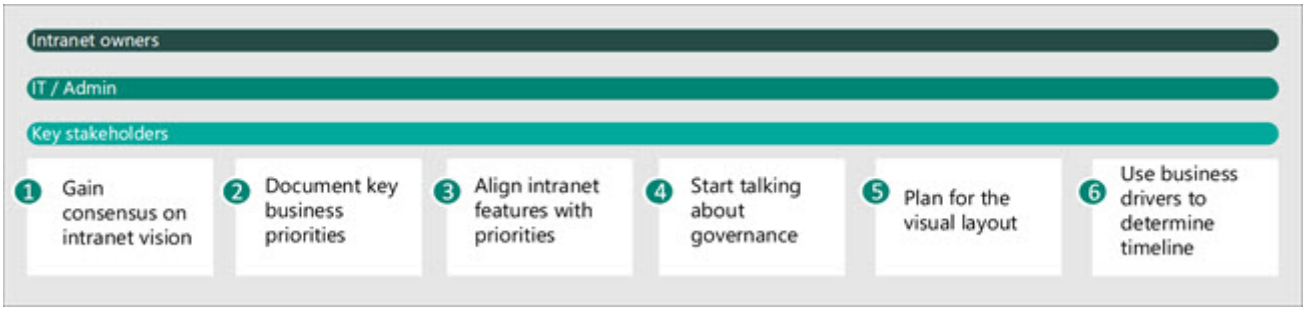
Plan your communication site — get started

Last updated on 06/25/2026

Get started creating your intelligent intranet

Now that you are familiar with the key success factors, phases, roles, and tasks needed to create an intelligent intranet, review next steps and get started planning.

Explore

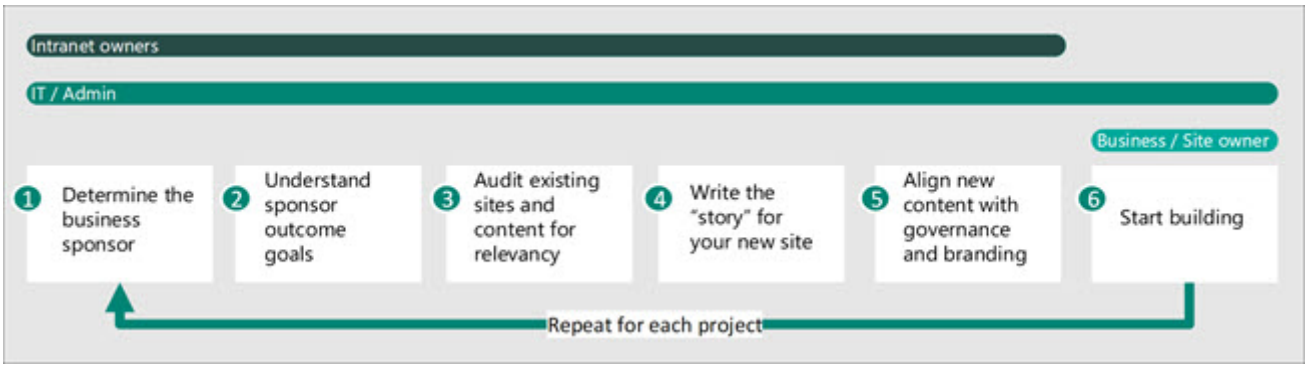


- Identify your key sponsors and stakeholders and review key organizational priorities. Document a vision that will help provide direction and help you prioritize opportunities.
- Align key outcome goals with SharePoint capabilities to identify where you may need to invest in customization. Consider whether an "intranet in a box" solution might be appropriate for your organization.
- Think about governance. What processes will you need to create to provision, manage, and maintain sites and content? Do you have security, retention, or compliance goals that need to be considered?
- Think about branding and architecture—do you want all sites to share a common look and feel?
- Analyze possible opportunities to identify priorities.

Expand table

Role	Exploration tasks
Organization intranet owners	Identify your key sponsors and stakeholders and review key organizational priorities. Document a vision that will help provide direction and help you prioritize opportunities.
IT pros / Admins	Organize a core team to plan governance—make sure you align your governance decisions to business goals.
Business owners / site owners	Help identify key organizational opportunities and priorities.

Align and plan

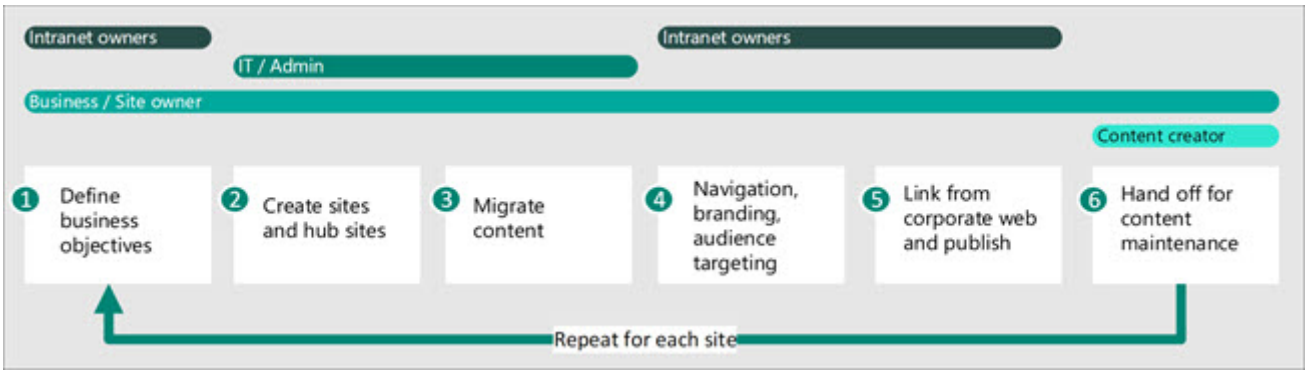


- Work with business owners and IT to prioritize the intranet projects in your portfolio for the greatest business benefit in the shortest time.
- Start by developing an understanding about what you need your intranet to accomplish and start organizing content assets and business outcomes. Organize depending on the needs of the business—by region, department, or function—and by the topics that your users care about.
- As you prioritize your intranet projects, consider how to get the best performance and scalability from the portals that you build.

Expand table

Role	Aligning tasks
Organization intranet owners	Communicate goals and progress from project start to finish. Director of the branding direction, governance strategy, information architecture, change management, and product adoption.
IT pros / Admins	Responsible for platform integration, content migration, performance, scalability, and user training.
Business owners / site owners]	Develop and plan solutions to business objectives. Responsible for site permissions, content audit, and content migration.
Content authors	Authority on content best practices, content creation, content management, and page design.

Create and implement

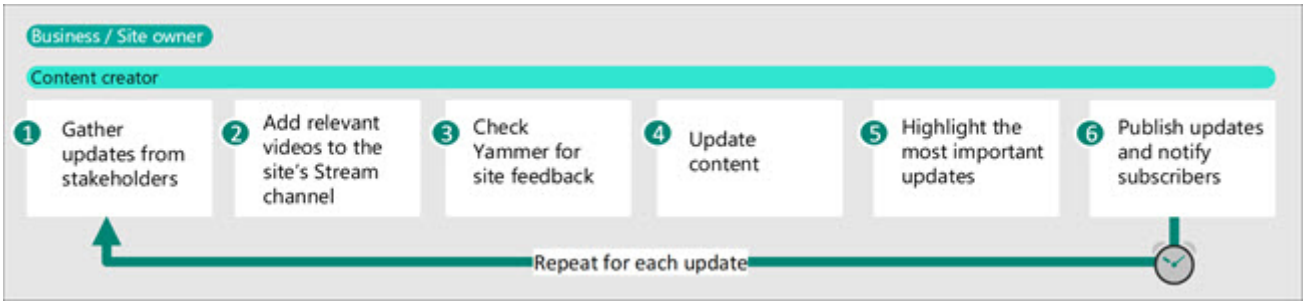


- Communicate goals progress regularly
- Measure, learn, and pivot as you go
- Get feedback regularly

Expand table

Role	Implementation tasks
Organization intranet owners	Get user feedback along the way. Use findings from user feedback to learn and pivot your intranet plan.
IT pros / Admins	Implement decisions made by the intranet stakeholders regarding site creation, navigation, search, branding, and publishing.
Business owners / site owners	Use business objectives to drive decisions around site creation, navigation, branding, and audience targeting.
Content authors	Create solutions to business objectives by creating and sharing relevant content with the right audiences.

Engage, manage, and maintain



- Celebrate the launch of your new intranet
- Use metrics to measure progress
- Communicate what's new
- Maintain high-quality content
- Educate users

Expand table

Role	Management tasks
Organization intranet owners	Celebrate the launch of your new intranet. Communicate goals and progress regularly after the launch.
IT pros / Admins	Communicate what's new with intranet stakeholders and business owners. Educate users about publishing rules like site creation and content retention policies.
Business owners / site owners	Schedule content audits and use site usage metrics to measure progress.
Content authors	Refresh existing content, publish new content and participate in scheduled content audits to keep content up-to-date and compliant.

Up next

Get started planning your intranet around initiatives that solve specific problems, can be implemented quickly, and will yield a high return on investment.

Related topics

Create and launch healthy portals

SharePoint adoption resources

Intelligent Intranet Envisioning Workshop PowerPoint deck

Plan your intranet

Plan your communication sites

Last updated on 06/25/2026

Plan an intelligent SharePoint intranet

Microsoft SharePoint offers a wide variety of options and tools to create intranet sites for your organization. Moving your intranet to SharePoint in Microsoft 365 might take a while, particularly if you already have extensive intranet content. In this article, we look at how to plan a new SharePoint intranet with a focus on quickly bringing sites online and getting a return on your investment.

We cover how to:

- Understand your key organizational priorities
- Understand your audience
- Plan for governance
- Review your current intranet
- Identify and prioritize your business initiatives
- Identify one key scenario to prototype and pilot
- Launch the pilot and engage with your users

What's possible with SharePoint?

With SharePoint, any user can create highly functional intranet pages quickly without the need for writing code or other difficult customizations. These sites look great on any device or screen and provide deeply engaging experiences for your users.

If you're currently using SharePoint Server for your intranet, you'll find SharePoint in Microsoft 365 to be easier to work with. Responsive, dynamic pages are easy for anyone to create, and the requirements for IT to build and maintain custom solutions are much less.

As a first step, to see examples of what's possible with SharePoint, we recommend that you review the SharePoint Look Book. The look book provides various examples about how to include news, events, resources, and personalized content in SharePoint sites that anyone can create and maintain.

For an understanding about how the different component parts work together, review the Guide to the Modern experience in SharePoint.

For inspirations and demonstrations on adopting the intelligent intranet, visit the The intelligent intranet - Microsoft Adoption.

In the following sections, we look at how to find the best starting point for your SharePoint intranet and how to prioritize the different intranet solutions that you may need for your organization. Keep these references handy as you work with your stakeholders - they can help you get the most value and best time to value for your intranet solutions.

Understand current business goals and key stakeholders

The most successful intranets don't just look good, they're primarily focused on helping people get work done and often on promoting engagement. The look book can help inspire you to think about how your content might appear, but your business outcome goals are important to understand what content and functionality are most important for your users and your organization.

All organizations have important strategic goals that drive behavior and investments. If you want to be sure that your intranet is successful – and gets the right level of funding – you need to ensure that it's aligned with these goals. You can also use these goals to help prioritize your intranet initiatives. Unlike many technology projects, an intranet project is never 'done' because your organization priorities and interests will change over time. But, at any given time, you want to focus on the intranet initiatives that are most closely aligned with your organizational priorities and key business stakeholders.

In addition, take a look at recent employee satisfaction survey data. A good way to become more informed about the information and tools that your employees need are to look at the pain points identified in these surveys.

Understand your audience

A good place to start thinking about your new intranet is what it is like when the intranet is in place. What will people be able to accomplish? How will they start their day? What will people say about the intranet? One potentially helpful exercise to frame the overall objectives for the intranet is to engage your key intranet stakeholders in a cover story exercise. This is an exercise in imagination. The purpose is to think broadly about an ideal future state by imagining a magazine cover story about the new intranet, including the key headlines, sidebars, and quotes from users.

With the end in mind, it can also be helpful to create personas for your key users. A persona is a fictional but realistic description of a typical intranet user (for example, new starter/new employee, knowledge worker, field worker, sales rep, people manager, or content author). You'll

want to do some research to engage with people who represent these different personas to understand their information requirements. You can't build an intranet without an understanding of the people for whom you are building it. Site owners alone aren't enough – their perspective is what they want to publish. That is often not the same thing as what their users want to consume.

Think about governance

If your users complain that search isn't successful because too much irrelevant content is discovered, this can indicate a governance problem. Before you think about your new intranet project, think about how you'll govern the architecture and the content. These are decisions that are a lot easier to make and enforce if they're decided early in your intranet project. For example, you'll want to think about:

- Who can provision new sites and when they're provisioned, what is the process to ensure that sites are discovered in navigation or as key bookmarks in search?
- Do you want all sites to follow a similar pattern so that users can easily find key content as they move from site to site?
- Who is accountable and responsible for the content on sites? How often does content need to be reviewed?
- Is content management for intranet sites in the performance goals or job descriptions for people with edit or owner permissions?
- Does intranet content need to be retained based on your retention policies or classified based on its sensitivity?

You don't need to make every governance decision up front, but if you don't have a plan for how you'll govern your new, intelligent intranet, it can quickly become a wasteland of information that fails to achieve your critical business goals.

Review your existing intranet

Your current intranet may be composed of sites from different business groups, such as HR, IT, Facilities, Engineering, and others. As a first step to planning your new SharePoint intranet, we recommend taking an inventory of your existing sites and meeting with the owners of each to determine their business outcome goals for new sites. Take stock of where your content is located and how much content you would need to move when creating a new intranet site. Look at your current content to understand if it's current or needs to be updated prior to moving to a new site. It's not unusual to find a migration strategy where existing content is left behind. You don't have to migrate anything – you may find that it's more effective to create new content that

is optimized for the modern SharePoint experience rather than migrate existing, out-of-date content to the new location.

As part of these meetings, you can identify the business needs that are addressed by each existing site and any requirements you might have for new sites.

In addition to meeting with current site owners, you may also want to convene a focus group of new employees. New employees are a key audience for the intranet and people who have joined the organization in the past two to three months can provide some valuable insights about what is missing or hard to learn in your current intranet, or resources they wish they had when they first started. They may also provide you with some valuable ideas from the organizations where they previously worked to help you think about new and important capabilities to incorporate.

Think of this step as an opportunity to learn. You're learning about what is important to your users and to the business. You'll use this information to identify initiatives for your intranet.

Identify initiatives

Using the information you gathered during your research, work with your key intranet stakeholders to identify initiatives that reflect your organizational priorities – and any barriers that might exist when you're implementing them.

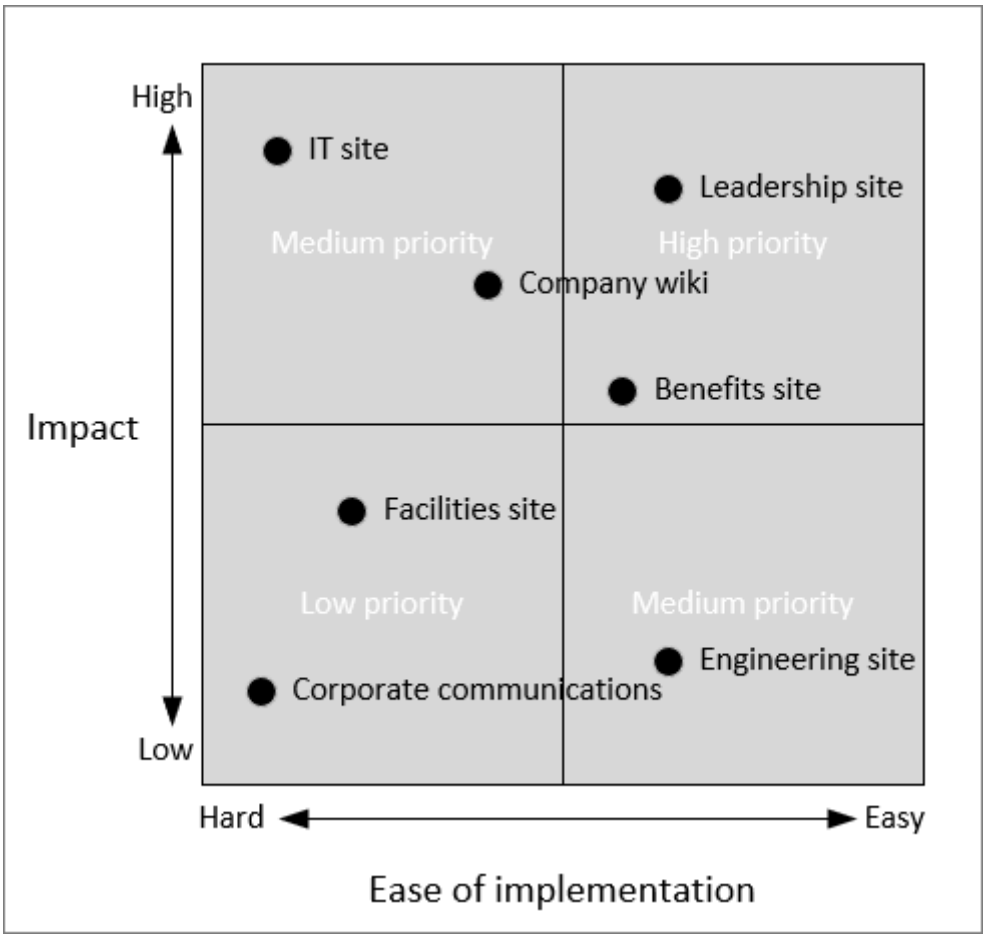
While you may ultimately implement solutions to address all of the identified initiatives, prioritizing which project to do first will help you achieve early success and user engagement as efficiently as possible.

Review each initiative you have identified for the following criteria:

- Does it solve a real problem?
- How many people will use it?
- Can it be built in a reasonable time frame?
- What's the return on investment?

Analyze each initiative for its positive impact on your users with respect to the ease of implementation. A high impact initiative that can be built with a minimum of customization can be an ideal first project.

Consider plotting your business initiatives on a grid, like the following, and review with your intranet stakeholders and IT department to choose the best option to start with.



To help decide which initiative to address first, work with the business leaders for that area to work out the objectives for the solution, who will be responsible for driving success in this area, and the metrics that you'll use to measure success. Don't just focus on system metrics. Think about actual business impact. For example:

Expand table

Initiative	Key content	Business owner	System success metric	Business success metric
Educate employees about benefits (Benefits site)	- Announcements - Training videos	HR	- News post views - Training video views	Help requests are reduced by x%
Weekly news post by a senior leader	- Streaming events - Formal training	Engineering	- Training content produced for all aspects of coding excellence - Monthly streaming events	Training completed successfully by x% of engineering staff
Foster positive employee agreement about company strategy (Executive	News posts - Streaming events	HR	Ongoing monthly activity posts by leadership and	- Viva Engage conversations show positive sentiment - Comments addressed

Initiative	Key content	Business owner	System success metric	Business success metric
Leadership Viva Engage Community)	- Viva Engage conversations		comments by employees	within 24 hours – "no question/comment left behind" - x% increase in employee satisfaction scores for executive communications
Improve timeliness consistency in proposal development (Marketing site)	- Company business value slides - Proposal templates	Marketing	- Slide downloads - Sales team alignment	x% reduction in the time to create proposals

Choose pilot scenarios

Work with the owner of each scenario to determine what an ideal solution would look like to them:

- Who are your visitors?
- What do the visitors to the site want to accomplish or learn?
- What tools or technology do they use today?
- What information do you want to promote?
- What tools or technology do you want visitors to use to accomplish their key tasks?
- Who are the champions who will help them transition to the new site or solution?
- How will you know if your solution is successful?

For example, create a table like the following to list business scenarios that you want to address with intranet sites across your organization:

Expand table

As an...	I need to...	So that...	I know this is successful when...
Employee	Understand and be able to update my benefits	I can take advantage of a key lifecycle benefit	Help requests are reduced
Employee	Learn about how to use the self-service benefits portal	Make updates on my own	Help requests are reduced

As an...	I need to...	So that...	I know this is successful when...
HR employee	Promote the use of the self-service benefits portal	I can spend more time working with employees on unique benefits questions and scenarios	All of my employee interactions are about individual critical scenarios

From the high priority scenarios, identify which ones meet these three key criteria:

- Can you build a prototype quickly (a few days)?
- Is there a committed sponsor?
- Is there enough up-to-date content to demonstrate key capabilities?
- Is there a specific audience for a pilot?

After you have compiled this information, create a design brief to help map out the user journey about how you want the site to operate. For example:

Expand table

User journey component	Description
Scenario	Leadership site: One-stop site for employees to hear from company leadership, learn the company's goals, and hear the latest news from customer meetings and industry events.
Users	All company employees.
Value	Increase employee awareness and alignment with company strategy and business initiatives.
User journey	- News post is sent to the company announcing a leadership Q&A meeting - Allan goes to the leadership portal to watch the event live - Allan uses Viva Engage to ask a question at the meeting - Allan shares the recording link with coworkers.
Metrics	- Live event views - Event recording views - Viva Engage engagement
Stretch goals	- Continued Viva Engage engagement - Improving employee sentiment (survey)

Choose solution components

SharePoint offers various building blocks that you can use to create an intranet:

- **Communication sites** - Use communication sites to share news, reports, statuses, and other information through various templates and web parts.
- **Home site** - A home site is a communication site that you set as the intranet landing page for your organization.
- **Hub sites** - Use hub sites to organize related sites and teams and centralize news, search, and content management.
- **SharePoint news** - Use the news web part to post important or interesting stories, announcements, people news, status updates, and more that can include graphics and rich formatting.
- **Viva Engage** - Use Viva Engage to connect with people across your organization beyond the boundaries of projects, functions, and departments.
- **Dynamics 365 Customer Voice** - Use Dynamics 365 Customer Voice to create custom quizzes, surveys, questionnaires, registrations, and more.
- **Stream** - Use Stream to deliver live and on-demand meetings, events, and training.

For the scenario that you've decided to build, choose the components that you'll need to use to meet the site's business objectives. We recommend creating a rapid prototype, and granting access to your key stakeholders. This provides a substantive framework for further discussions and revisions of the design.

At this stage, we recommend that you involve your help desk so that they're prepared to answer questions after the site rolls out to a larger audience.

For best practices for launching an intranet site, review Creating and launching a healthy SharePoint portal.

Roll out the pilot

When the prototype has evolved to a point where you want to share it more broadly, you can roll it out to a pilot group, or even to the whole organization. User adoption is a critical part of success for a new intranet site. To drive site usage, we recommend that you use down both a top and bottom up approach:

- Recruit executive sponsors who can ensure that the intranet project is funded, and can help message the importance of the new site to others in the organization.
- Empower champions throughout the organization to promote the new site on a grass roots level.

Other things you can do to drive success include:

- Have launch events and communications campaigns.
- Provide formal training.
- Hold regular office hours where users can ask questions.

As the site rolls out and more users engage, watch your success metrics and make adjustments as needed to drive more engagement and user satisfaction.

When the site is on its way to success, take stock of any lessons learned in the process and proceed on to the next intranet project that you want to undertake.

Related articles

SharePoint Look Book

Last updated on 06/25/2026

Considerations when planning for a global intranet

If your organization has team members in multiple locations around the world, you have additional considerations and options as you plan for your SharePoint intelligent intranet. For example, you may want different branding for individual regions. You may want to target content to team members in certain countries/regions. You may want to provide sites in multiple languages. Or you may need to comply with data residency requirements in certain countries/regions. Here are options to consider which can be used independently or in combination to meet the needs of your global intranet and create the best experience for your users.

Hub sites

Multilingual sites and pages

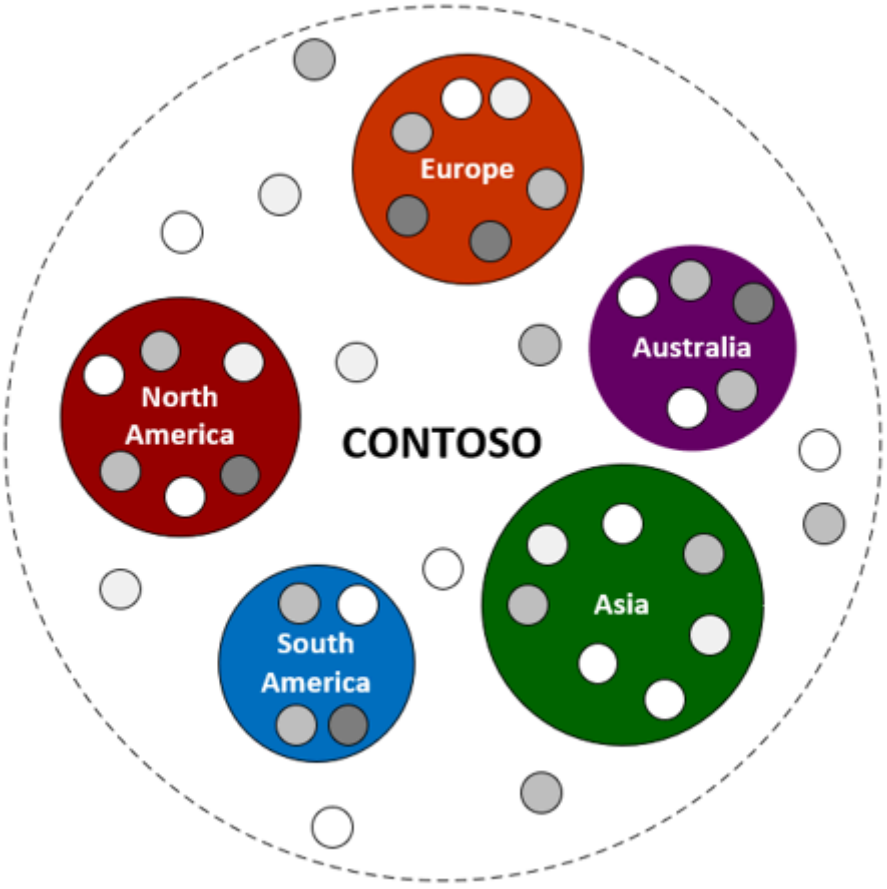
Regional settings

Audience targeting

Multi-Geo for data residency requirements

Hub sites

The advantage to using hub sites is that they provide a flat architecture that is flexible and carries branding and navigation across multiple sites connected to the hub.



If you have subsidiaries in different regions that have their own branding and navigation, an option for you is to create a hub site for each region.

Learn how to plan for hub sites

Multilingual sites and pages

A separate consideration for a global or regional intranet is whether you want to set up sites on your intranet to be multilingual so that users can read and work with content in their preferred languages.

User interface elements like site navigation, site title, and site description can be shown in the user's preferred language. Additionally, you can provide pages and news posts on communication sites that you translate to users' preferred languages. For example, you may have provisioned your site with a default language of English, but you have users who have set their language preference to Spanish, and users who have set their language preference to French. You can set up your site(s) to view in the site default language as well as in French and Spanish.

> **Note**

User interface elements and pages are not translated automatically. Each page created in your default language can have a corresponding page in a chosen target language that you, or someone you assign, manually translates. After you translate such a page and publish it, it will automatically be displayed to users who have set a preferred language in their Office personal profile.

Next steps for multilingual sites and pages

- Site owners determine which languages to support on their sites
- Site owners enable multilingual features and choose languages
- Create multilingual communication sites, pages, and news
- Set up a multilingual site name, navigation and footer

Regional settings for sites

Site owners can change regional settings for a site to specify calendar settings and how numbers, dates, and times are shown for all users of a site. Individual users can choose to specify their own personal settings.

Audience targeting

Audience targeting helps the most relevant content get to the right audiences. By enabling audience targeting, specific content will be prioritized to specific audiences through SharePoint web parts, page libraries, and navigational links.

For example, you might want to prominently display news about a sales meeting in Asia to users in that region rather than display it prominently to all regions.

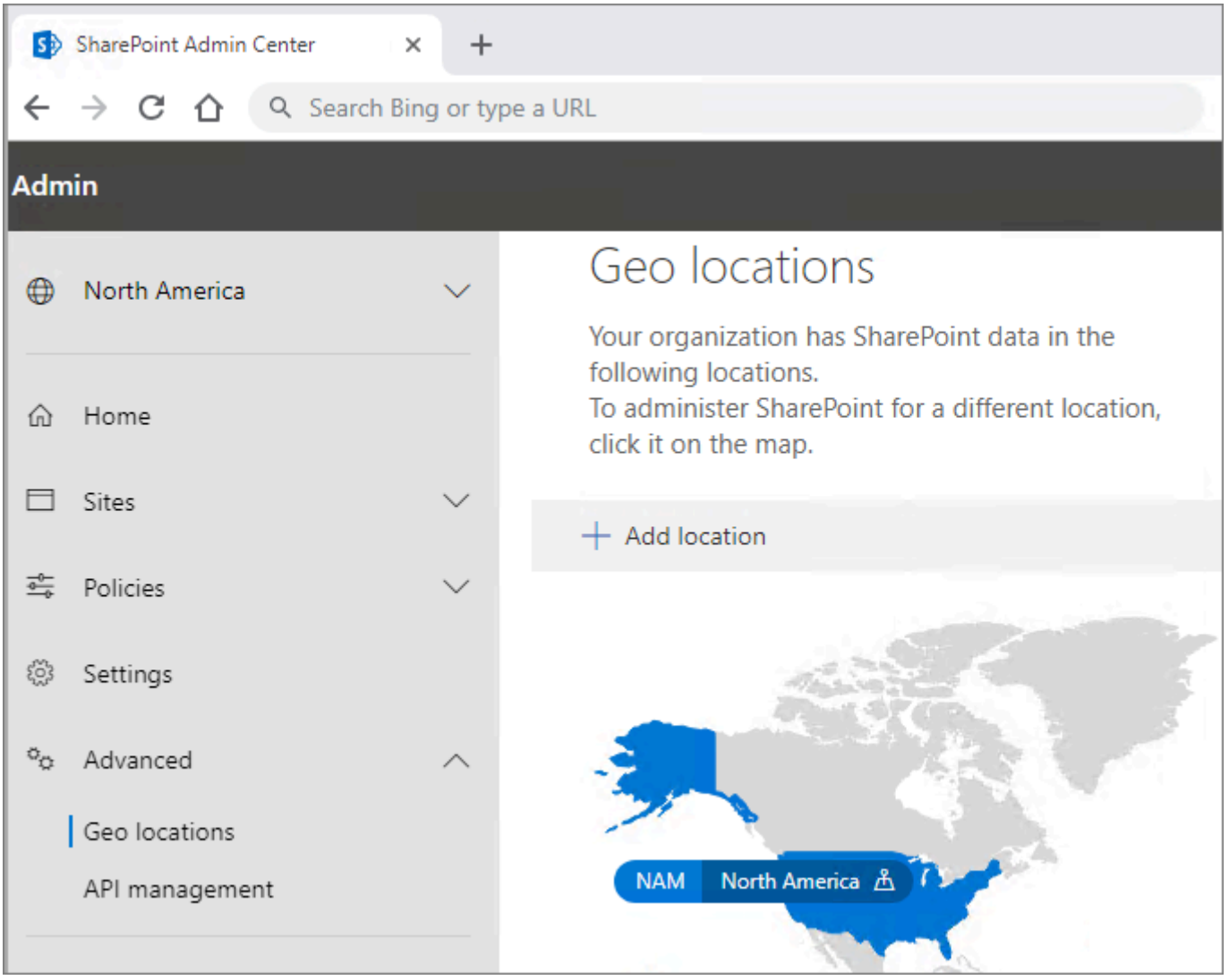
Next steps for audience targeting

- Learn how to set up audience targeting
- Learn more about creating groups for audience targeting

Microsoft 365 Multi-Geo

Some countries/regions have laws requiring that user data be stored within that country. To accommodate these requirements, you can set up a Microsoft 365 Multi-Geo tenant. With a Multi-Geo tenant, your tenant may be provisioned in one country, but user data for SharePoint, OneDrive, and Exchange can be stored in other countries/regions. For example, you may have 5,000 employees in Europe and 8,000 employees in North America. All the users are working within the same tenant, but data for the 5,000 employees are stored in Europe while data for the 8,000 employees is stored in North America. This allows for seamless collaboration across your organization while still meeting data residency requirements.

After Multi-Geo is enabled for your tenant, you can set up and manage geo locations on the Geo locations page in the SharePoint admin center.



> **Note**
>
> Due to the unique nature of data requirements in China, a differentiated version of Office 365 is available and operated by a partner from datacenters inside China. This service is not considered a Multi-Geo service. It is powered by technology that Microsoft has licensed to

21Vianet. For more information, see Office 365 operated by 21Vianet - Service Descriptions.

A differentiated service called Microsoft Cloud Germany is being migrated to Office 365 services in the new German datacenter. For more information, see Migration from Microsoft Cloud Deutschland to Office 365 services in the new German datacenter regions.

Next steps for Microsoft 365 Multi-Geo

- Learn how to plan and set up Multi-Geo for your organization
- Learn how to set up Multi-Geo in the SharePoint admin center to enable Multi-Geo features across the user experience

---

Last updated on 06/25/2026

Planning intranet governance

Article • 07/19/2024

As you plan your new intranet project, think about how you govern the site architecture and the content. Your intranet governance plan should be created in the context of the overall governance plan for Microsoft 365. As a key business solution in your digital workplace, your intranet has its own unique governance requirements and expectations, especially because of its organization-wide focus and impact.

Planning intranet governance should happen during the exploration phase - to ensure that all stakeholders have shared vision and goals. Envisioning is only the beginning. Your intranet governance plan evolves as your organization evolves and as new capabilities are added to SharePoint and Microsoft 365.

A good governance plan helps define the priorities for the intranet and helps to prevent content sprawl. It also ensures that roles and responsibilities are clearly defined and communicated – and ideally, incorporated into job descriptions or performance goals. One aspect that often separates your intranet from other solutions is the number of people who are involved in creating and maintaining content. To ensure ongoing success, it's important to make sure that each of your intranet stakeholders and users understands their roles and responsibilities.

Intranet governance also includes policies and procedures but it's so much more than that. Intranet governances should include a plan for user training, monitoring usage, user behavior, and communicating expectations to all of the diverse stakeholders involved. This is what makes creating a governance plan document is challenging. It's difficult to create a single document that addresses these multiple audiences and can be communicated in a way that encourages adherence and adoption.

Instead of creating a document or series of documents, consider creating a resource site that incorporates training and governance in a single place. Think about how you can combine “how to” (training) with “how should” (governance) so that when your intranet users visit your user resource destination, they understand both “why” and “how” your intranet is designed and governed the way you have implemented.

You can consider using the Microsoft 365 Learning Pathways site as a possible starting point or create your own user resource center that integrates with or complements the Learning Pathways content.

Having an effective governance plan in place enables the decision-making process for the intranet. By reviewing and revising the governance plan regularly, you can help ensure that your intranet remains a critical asset for your organization.

Governance Team

As a key business asset, intranet governance needs to reflect the goals of business stakeholders and the legal and regulatory environment for your organization – not just the expectations of your IT department. Create a governance team that includes core members from key business stakeholder groups in your organization in addition to IT.

There's no magic size for the governance team, but it should be small enough to make it easy to make decisions and representative enough to incorporate the “voice of the business” and IT. When you have specific topics to review that extend beyond the expertise of the team, you can bring in outside members (such as legal or records management) to ensure that your decisions are aligned with organizational constraints.

Your governance team may meet on a frequent basis during intranet planning and then less frequently over time. The goal is to establish a rhythm that works for your intranet and team members. Since governance has an ongoing role for your intranet success, the governance team shouldn't be disbanded when you launch.

Governance Plan Elements

There's no “one size fits all” model when it comes to intranet governance. In fact, your intranet governance plan may be different for different types of content. For example, you may want to have more formal policies and stricter governance guidelines for sites that face the entire organization and less strict policies for content that is more targeted, such as content for an individual department or a one-time event (see Figure 1). The best approach is to look at the different elements and thinks about what is critical or necessary for your organization. Consider your audience and the culture of your organization to guide your decisions and approach, as well as your overall Microsoft 365 governance expectations.

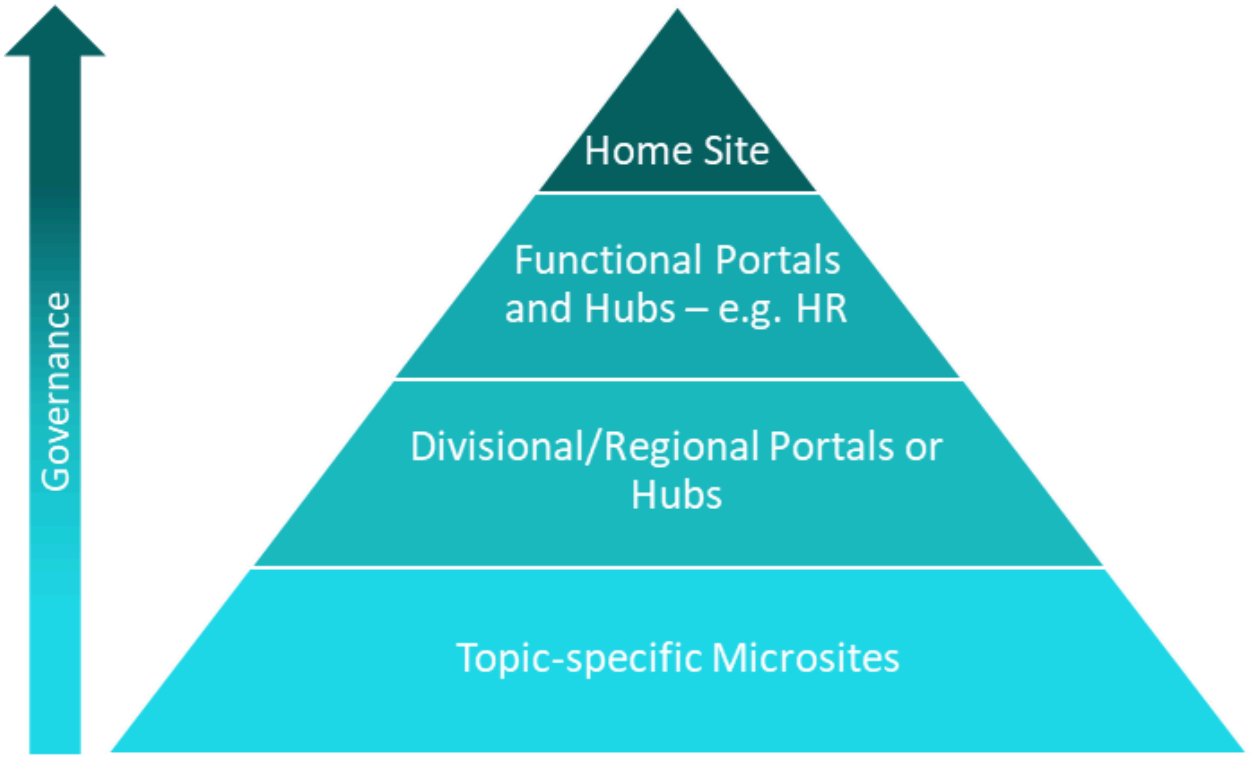


Figure 1. Your governance decisions may be different (and stricter) based on the "reach" of your content.

At a minimum, consider each of these elements as part of your intranet governance planning effort.

- Vision
- Policies and guidelines
- Site provisioning and decommissioning
- Information architecture and search
- Branding
- Content management
- Security and information management
- Roles and responsibilities
- Feedback
- Training and support
- Measurement

Vision

The vision statement describes, at a high level, what you want to achieve with your intranet - essentially how the solution delivers value to the organization and to each individual employee. Use the intranet vision statement to guide your governance plan. Be sure that the vision is clear because the degree of formality and the depth to which you need to document the governance plan should align with the outcomes you want to achieve.

A clear vision statement provides critical guidance to the inevitable decision tradeoffs you need to make for your governance plan. For example, you probably don't want a completely uncontrolled environment with unstructured and “unfindable” content if your intranet vision is to provide a key source of organizational knowledge and information. In this case, the unstructured environment with no controls is unpredictable and will likely misalign with desired business outcomes. In a different scenario, some users may have a goal to create an experimental place where new site owners can create “practice” sites to try out new skills or test alternative approaches to solve specific business problems. For this use case, an overly restrictive governance plan may not make much sense. You may determine that you don’t want to support an unlimited number of “practice” sites, so you may want a governance policy that says that all “test” sites are deleted after a specific period of time. But, for these practice or test sites, the unstructured environment is fine. You can only know what is level of governance is ideal because you have a clear vision. The vision provides a framework for both the context and your investment in governance. Once you're clear about your intranet vision, your governance team can use that vision to guide the governance decisions.

Your intranet vision includes defining ownership. There's no right answer about which organizational entity should “own” the intranet – and often, intranet ownership is shared by more than one organizational unit. However, most intranet professionals agree that there's one organization that shouldn't be the exclusive intranet owner – IT. IT can't build an intranet for the business. IT can only build an intranet with the business and with a commitment from the business. Successful intranets have a champion and owner from the business, ideally at an executive level.

Policies and guidelines

Policies define the rules and guidelines for your intranet. From a governance perspective, policies are usually driven by statutory, regulatory, or organizational requirements. Users are expected to meet policies without deviation. If your organization is subject to regulatory oversight, be sure you can enforce your policies as a failure to do so may target your organization as being “non-compliant.” Guidelines are usually established to encourage consistent practices. In many cases, guidelines are more recommendations, but policies are requirements.

For example, consider the site ownership. A policy might state, “All SharePoint sites have a primary and secondary contact responsible for the site and its content.” A related guideline might state, “The site contact is listed in a web part in the lower left-hand corner of the site home page.” The guideline might become a policy for major functional sites but remain a guideline or recommendation for topic-specific microsites. Another example of a policy is whether people outside the organization can have access to the

intranet as a whole or only to individual sites. The policy might have a default value of no external access but there could be a process that allows for exceptions to allow specific partner users to have access to some intranet sites.

Each organization has its own set of policies and guidelines. General topics should include content oversight, site design, branding and user experience, site management, and security.

Steps to ensure success:

- Verify that your intranet policies and guidelines don't conflict with broader organizational policies and your overall governance decisions for Microsoft 365.
- Publish policies and guidelines where users can easily find and follow them. Some policies may need to be published for "all users," while others may need to be secured to protect the integrity of the application. Consider creating a governance site rather than a document to facilitate publishing and "consuming" governance policies and guidelines.
- Use capabilities to automatically apply policies and guidelines wherever you can. For example, you can enforce content management and retention policies with information protection capabilities in Microsoft 365. You can encourage following design guidelines by using site designs to embed best practices in sites as they're created. The best way to ensure that your policies are followed is to ensure that site owners and authors don't have to think about them. Try to automate as much as you can and where you can't automate, plan to provide training to ensure that site owners and content authors clearly understand governance expectations.
- Regularly review and revise policies and guidelines to keep them aligned to organizational needs.

Consider these topics for your intranet policies and guidelines:

- External sharing – can people outside the organization access intranet sites?
- Default sharing links for intranet documents - consider setting the default for all intranet sites to be "People with existing access" to ensure that site owners don't accidentally create links that allow visitors to edit key intranet documents.
- Site navigation – for individual sites and the intranet as a whole.
- Site designs - including guidance for items like the positions of key web parts on departmental home pages. Do you want all sites to follow a similar pattern so that users can easily find key content as they move from site to site? If so, then you may want to apply site designs to ensure that it's easy for site owners to follow your design patterns.

- Metadata architecture and content types - for example, policies for enterprise content types and organization-wide metadata).
- Guidelines for Teams chat and Viva Engage conversations - including more than just messaging policies for Teams and how to participate in a Viva Engage conversation, but also conversation guidelines (such as using @mentions sparingly and organization-specific "do's and don'ts").
- User profiles – including expectations for the About me statement and expectations for skills and expertise (for example, how well do you have to know a topic to list it in the skills and expertise area of your profile?).
- Organizational policies and guidelines for intranet site names, file names, Microsoft 365 group names, etc.

Site provisioning and decommissioning

A key intranet governance decision involves determining who can create a new intranet site. Your modern intranet architecture is "flat" which means that your intranet contains many sites. Do you want to provide a self-service model for new intranet sites or do you want to manage site creation through a form submission and workflow? There's no right answer to this question – but no matter which approach you choose, you need to think about governance. There are two popular solutions to governing new site creation:

Implement a site request process for intranet sites

You can easily hide the option to create a new site in the SharePoint admin center. If you do so, you want to create a process for users to request a new intranet site. Having a request process makes it easy to review and track site requests and ensures that your environment remains "tidy," but if your review and approval process takes too long, it could be frustrating for your users. Your provisioning process can use a site design to ensure consistency or you can manually create sites to follow your design patterns. A key part of your provisioning process will be to ensure that new site owners have the appropriate guidance and training that they need to be successful when you fulfill their site requests.

Allow self-service site creation

If you enable self-service site provisioning, you want to consider providing site designs that embed your best practices so that new site owners start with a "template" that aligns to your governance guidelines. You'll also want to track new sites in the Admin Center so that you can follow up with new site owners to provide the information that they need to be successful after the site has been created.

In addition to providing a process to provision new sites, you'll also want to think about a process to provision new hubs and associated hubs. Hubs must be provisioned by a SharePoint Administrator and above, so you need to think about how you'll plan and govern the creation of new hubs.

When an intranet site is no longer needed, there may be cases where your records management process prohibits deletion of the site and/or content. Another key governance decision is planning how you'll delete or decommission intranet sites in the context of both legal holds and records management requirements. Learn more about Microsoft Purview compliance documentation, including records management and eDiscovery (Premium).

Information architecture and search

Well-planned information architecture is a prerequisite for a successful and well-performing intranet. It's difficult to separate planning your intranet information architecture from planning your intranet governance. These two planning tasks go together and you'll likely find that you're thinking about the two aspects of your intranet iteratively and simultaneously. Intranet governance should cover several key aspects of your information architecture:

- **Navigation architecture** – how your sites and hubs are associated to support users who navigate or browse for content.
- **Page architecture** – guidelines for pages, especially site home pages, to help create consistent experiences across all intranet sites.
- **Metadata architecture** – columns and content type planning to support consistent approaches for organizing content and pages.
- **Search experiences** – understanding how users find content when they don’t know where it might be in the architecture and how they discover content. You can help users discover content and improve search outcomes by using several features in search, including acronyms, bookmarks, Q&A, floor plans, and locations. For more information, learn how to make content easy to find and how search experiences work in SharePoint. Your governance plan should include how you'll support and manage the creation of the search discovery attributes.

Branding

Brand standards help to define the look and feel of your intranet. These standards are reflected in site and page designs. Your brand standards can include standards for the

use of imagery, including requirements to use only brand-compliant images or icons from an organization assets library on intranet pages, and requirements to use only brand-compliant custom themes for sites. Your standards might prescribe a specific theme for different types of sites or sites with different access levels. Your standards might also include content authoring standards such as tone of voice, spelling conventions, accessibility standards, and other guidelines that support your organizational brand. Learn more about branding in SharePoint.

Content management

Content management is one of the most important parts of your intranet governance plan. Many intranet users complain about intranet search – that they can't find what they're looking for. Most often, the problem isn't with search; the problem is that there's no content management in the governance plan!

Some common content issues include: Files are often duplicated rather than linked – so search finds multiple copies of the same document and the searcher doesn't know which one is the correct version. File names often include version numbers instead of allowing SharePoint to manage versions – so search finds all the various versions of a document and not just the most recent, making it harder for the searcher to find the current version of a file.

Your governance plan should include these key content management concepts:
Content creation

- Where should content be published? For example, if I'm not the "owner" of a document, should I publish it to my intranet site? Or instead, should I find the owner and ask them to publish it so that I can add a link?
- Are there guidelines for creating intranet content? For example, what is the appropriate tone of voice and are there specific guidelines organizing content on pages? When should content authors create documents for the intranet and when should they create pages?
- Are there accessibility standards that content authors need to follow? Consider these 8 tips to create accessible SharePoint pages (from the Humans of IT Blog on the Microsoft Tech Community).
- How should files be named? Should your governance content include file naming recommendations such as not including version numbers in file names?

Information protection

- Does your organization have a requirement to protect certain types of sensitive information? If so, can your governance plan (and deployment) use Microsoft 365

information protection capabilities such as sensitivity labels and retention policies?

Content review

- Do you want to set up flows using Power Automate to trigger intranet content review at a specific time interval?
- Who is accountable to review content and at what frequency? Is it the site owner or the content author or another role? Is the expectation different for different types of sites or different types of content?

Content disposition

- Do you have requirements to implement records retention policies on some or all content to prevent accidental deletion?

Security and information management

Your governance plan shouldn't only include what *should* be posted on the intranet – but it should also include guidelines for content that *shouldn't* be posted on the intranet. You may be able to enforce some policies using automated information protection capabilities, but you want to provide training and guidance for site owners and content authors to ensure that they understand their responsibilities when it comes to security and information management for both sites and content.

Roles and responsibilities

Roles and responsibilities describe how each employee as an individual or in a role (such as Site Owner) is responsible for ensuring success of the intranet. Documenting roles and responsibilities is a critical aspect of your intranet governance plan. To ensure that intranet responsibilities are treated seriously, it's helpful to partner with your human resources organization to ensure that intranet responsibilities are part of job descriptions or performance goals.

It “takes a village” to successfully support an intranet in any organization. You need a team - and the team may include specialized roles that you use on an occasional basis, such as developers to create a custom web part, permanent roles such as site owners for whom intranet site management is a small part of their job, and other permanent roles for people whose entire job responsibilities involve intranet management. Some organizations find it helpful to organize their intranet resources in a center of excellence, which may include full time members of the IT staff supplemented with virtual members who work in different business groups around the organization. Others extend their centralized staff to include “intranet champions,” who extend the support team into

various departments and geographic locations by volunteering to help ensure intranet success.

No matter who is in your “village,” it's critically important that everyone understands their role and for which aspects of the intranet they're responsible. Figure 2 shows an example of a role and responsibilities description for an intranet Site Owner.

Some of the key roles to consider for your intranet governance plan include:

- Intranet Steering Committee
- Intranet Business Owner
- Intranet Technology Owner
- Corporate Communications
- Training
- Intranet Governance Team
- Site Owners
- Hub Owners
- Site Members/Editors
- Site Visitors
- Viva Engage Community Owners
- Viva Engage Community Members
- Team Owners
- Team Members
- Intranet/SharePoint/Microsoft 365 Champions

Feedback channel

Your intranet governance plan should incorporate a mechanism to collect feedback from intranet users. This includes a vehicle to collect feedback – for example, a Microsoft Form linked from the footer of your home site – but also mechanisms to gather and process the feedback and take actions based on the feedback. It's a good idea to acknowledge all feedback, even if you don’t plan to take an immediate action.

Training and support

Your intranet won't be successful if you don’t incorporate a way to provide training and support for all users, but most especially, Site Owners. The best way to reinforce your governance policies and guidelines is to build them in to your training. In other words, don’t provide training that only shows “how to” – make sure that your training also

includes your policies and guidelines – the “how should” aspect of your governance plan.

It's helpful to provide a dedicated site where Site Owners and other intranet users can find training and governance information. You can create your own “user resource center” as described earlier or use a third-party or Microsoft-provided training environment. To ensure that your training content is always current, you can link to content at Microsoft’s training platforms such as Microsoft Office Help and Training and Microsoft Learn. You can also embed the support.office.com training into your own environment by deploying Microsoft 365 Learning Pathways in your tenant and adapting the content to include your governance policies and guidelines.

You can help your intranet users find your training content by adding a custom tile to your Organization Profile or adding a custom help link directly in Microsoft 365.

Measurement

Your intranet measurement plan should be aligned to the criteria for success defined for the intranet vision. It should define the metrics and analytics used to track success, any associated KPIs, and processes for evaluating metrics and taking action to make improvements.

Look for metrics that are more than just page views. Just because a page is viewed doesn't mean it's adding value to users. Instead, look at metrics that measure business value. For example, are you seeing fewer support tickets related to expense processing because your intranet was updated to include better and more up-to-date content about expense reports? Are you seeing fewer help desk calls regarding how to upload documents because you have updated your training content and made it more accessible? Are HR representatives spending more time on unique issues because the HR content is organized more effectively?

If your initial design plan identified key business outcomes or surveyed users to ensure they had easy access to the information they need for their job, repeat the process after you have deployed or updated your intranet to identify the business impact of your intranet update or investment. Supplement this data with qualitative feedback from site owners and users to create a comprehensive assessment of the effectiveness of your intranet and your governance plan. Don't be afraid to decommission content or sites that are no longer relevant. You can optimize your intranet value by using metrics to identify duplicate, outdated, and irrelevant content and sites.

More intranet governance resources:

SharePoint governance overview

How to think about your modern intranet

Feedback

Was this page helpful? Yes No

Provide product feedback

New SharePoint Experience

SharePoint is redesigned for simplicity and clarity, centered on discovering, publishing, and building—now with flexible workflows and AI-first capabilities built in.

What is in the new SharePoint experience?

The new SharePoint experience consists of the following changes:

1. The SharePoint home page is replaced with a *Discover* experience.
2. The SharePoint app bar is refreshed with a newer experience.
3. The new app bar has two new destinations, *Publish* and *Build* destinations.
4. The new app bar will show global navigation at the top with the logo and name, if it is enabled and configured in your Home site.
5. The visual updates include neutral app theming that applies a consistent, neutral palette to SharePoint UI surfaces and elevating content forward across key surfaces (including SPFx placeholders). Together, these changes reduce visual noise, improve readability, and bring clearer structure and visual focus to customer branding and content as users view and edit pages.

Last updated on 07/31/2026

Introduction to SharePoint information architecture

Well-planned and executed information architecture is a prerequisite for an intelligent and high-performing intranet, hub, or site. The most important first step in planning an effective information architecture is understanding your users and helping them find what they need to complete tasks in a way that makes the most sense to them.

Information architecture also helps improve user adoption, satisfaction, and productivity while reducing IT costs, information overload, and minimize compliance and security risks.

> **Note**
>
> All navigation types (site, hub, global, and footer) are limited to 500 child links at each level. Additional nodes added after the limit has been reached will receive an error.

In this article:

- Learn the main elements of information architecture
- Review the different roles involved in implementing information architecture
- Understand the different levels of information architecture – global, hub, and local
- Explore SharePoint information architecture building blocks

Information architecture elements in SharePoint

Information architecture is about how you organize and label your content and how your visitors interact with the content to get work done. On websites, information architecture includes elements like navigation, search, site hierarchy, taxonomy, and security. Modern SharePoint information architecture is also about how to ensure the right content gets to the right people and follows your organization's content compliance regulations.

Information architecture covers six main elements that relate to way finding in SharePoint:

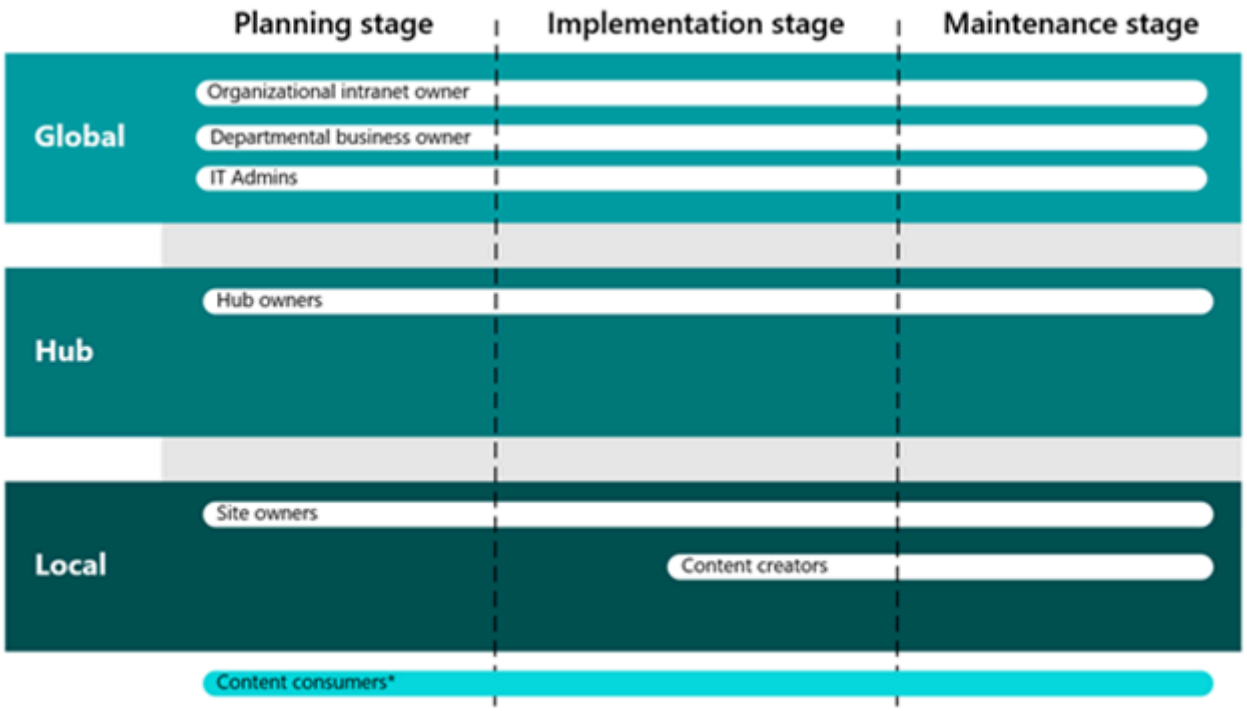
- **Global navigational structure** – Considered the top level of navigation across your SharePoint tenant and how you structure your sites so that users can find content including the home site of your intranet.

- **Hub structure and organization** – Hubs enable you to group together similar articles, tasks, and content.
- **Local site and page navigational structure** – How content is organized on each site and page so that users can further navigate or consume content effectively.
- **Metadata architecture** – Metadata impacts search and browsing structure as well as compliance and retention policies.
- **Search experiences** – How your users "consume" information architecture in addition to browsing.
- **Personalized content experiences** – How specific content is targeted to certain users and groups of users.

Designing the optimal structure for hubs, sites, and pages requires sufficient planning. It also requires knowledge of the domain, content, understanding the user experience, awareness of design approaches, and best practices in Microsoft SharePoint. Even with a good plan, information architecture is a continuous process. Over time, organizations change, people change, and projects change. Over time you'll learn about your users, which will allow for adjustments that make content more discoverable.

Understand your role and how to collaborate

Information architecture for your organization is most effective when many types of roles collaborate on your intranet, such as: intranet owners, departmental business owners, IT administrators, and hub owners just to name a few. Learn more about how each role plays a part in planning, implementing, and managing ongoing maintenance for organizational information architecture.



Organization intranet owner(s) – The organizational intranet owners consist of a mix of decision-makers and job functions to manage the overall direction and coordination of your organization's intranet. Organizational intranet owners work with business owners (departments) and IT admins to establish global and hub level navigation. Organizational intranet owners spend most of their time working on planning and implementing global and hub level navigation.

Departmental business owners – Departmental business owners represent large areas of the organization, like human resources, marketing, and engineering. Departmental business owners work with organizational intranet owners to ensure their area of the business is well-represented in global and hub navigation. Departmental business owners should be included early in the planning stage to ensure business and user needs are met.

IT Admins – IT admins partner with organizational intranet owners and departmental business owners to implement high level navigational structure like implementing the start page and hubs. IT admins also help implement certain governance policies around site creation and usage. IT admins are involved in planning, implementing, and maintaining information architecture as the business changes and scales.

Hub owners – Hub owners manage hub-level content, branding, permissions, and navigational elements for hubs in your organization's intranet. Hub owners partner with departmental business owners and IT admins to plan, create, and manage hubs throughout the lifecycle of your organization's intranet architecture.

Site owners – Site owners manage site-level content, branding, permissions, and navigation. Depending on the needs of the business and users, site owners can associate their sites to

hubs if the hub owner allows.

Content creators – Content creators are responsible for keeping site content updated and publishing news. Content creators should be given a site member permission level to make changes to sites and pages. Content creators partner with site owners during the implementation and management stages.

Content consumers – Content consumers aren't represented in the counts as anyone who is using and viewing content throughout the three levels of navigation. Intranet owners, departmental business owners, hub owners, and site owners should regularly engage with content consumer – especially during the planning process – to ensure the right content is findable and usable.

Guiding principle: the world is flat

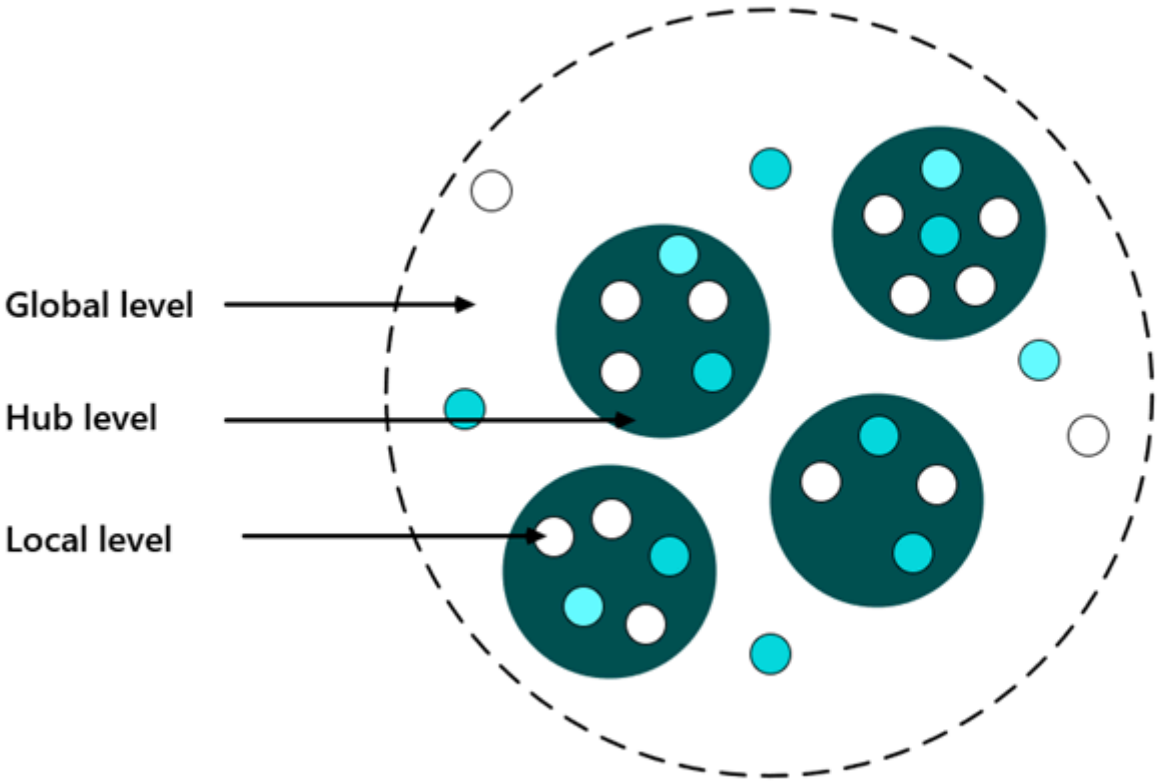
Classic SharePoint architecture is typically built using a hierarchical system of site collections and subsites, with inherited navigation, permissions, and site designs. Once built, this structure can be inflexible and difficult to maintain. In the modern SharePoint experience, subsites aren't recommended. In the new "flat" world of modern SharePoint, plan to create one site for each discrete topic, task, or unit of work. This allows you to easily distribute management and accountability for each content collection and support your ability to move sites around in your navigational architecture without breaking links. Moreover, when a topic is no longer needed, you can easily archive or delete a site with minimal impact.

In the new flat world, you have several ways to connect sites and content to each other as part of your information architecture toolkit:

- Use "roll up" web parts such as News, Highlighted content, or Sites to dynamically surface content from other sites in an existing site.
- Use inline hyperlinks to provide more detail about a topic to provide more information to your reader (as demonstrated in the previous bullet).
- Add explicit links to related sites in your site navigation.
- Connect families of related sites using hubs.

Levels of navigation

There are three levels of navigation to think about for modern SharePoint experiences:



- Global navigation for the entire collection of sites that comprise your intranet
- Hub navigation for groups of related sites
- Local navigation of an individual site

Global navigation

Many intranets include top navigation that persists on every site. Global navigation allows you to create an overall navigation story for your intranet that visually connects all the sites, content, and tools your viewers need to get work done. Every organization has a different requirement for what goes in global navigation, but some of the category labels often used include concepts such as:

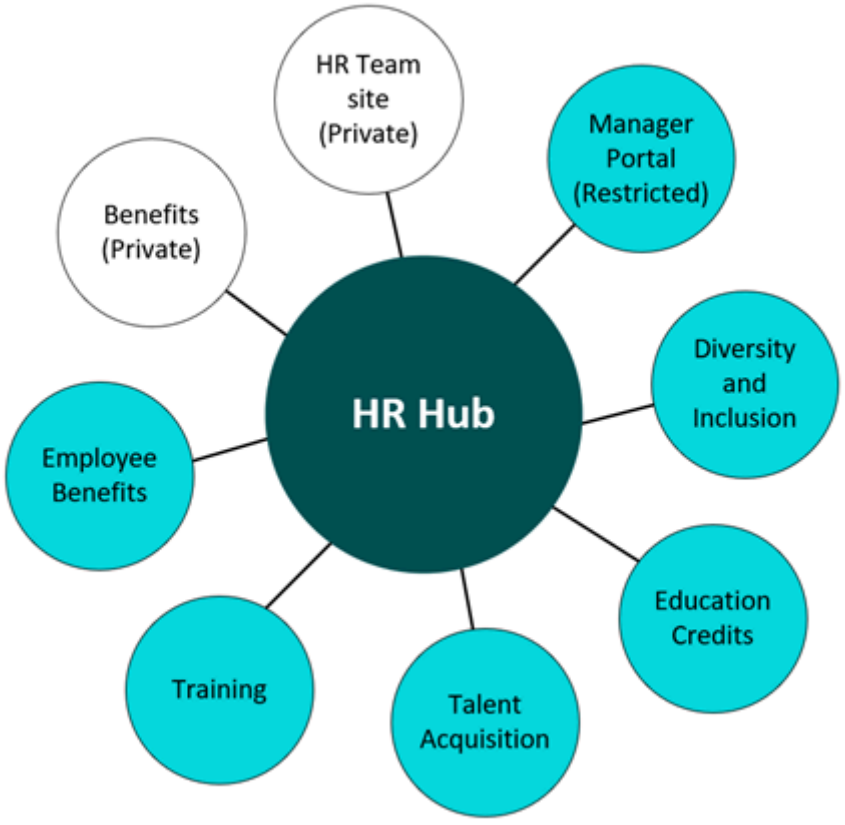
- Home
- About Us
- News
- Working Here/Work Resources/Administrative Services/Administration
- Operations/Operations Services
- Pay & Benefits
- Life & Career
- Locations
- Policies & Procedures/Tools & Resources/Safety & Security

The goal of global navigation is to support browsing to content. Since there's limited real estate available for global navigation links, global links generally point to major category navigation pages, sublinks, or a mega menu experience to provide enough information to help viewers find the content they need. Because the context for global navigation must be broad, it's challenging to make the labels both comprehensive and useful. If you plan to implement global navigation, you want to test your proposed navigation to make sure that it resonates with users.

Global navigation is enabled with the SharePoint app bar on your home site. You need to have a home site to enable global navigation. Global navigation appears on the left side of every site and page.

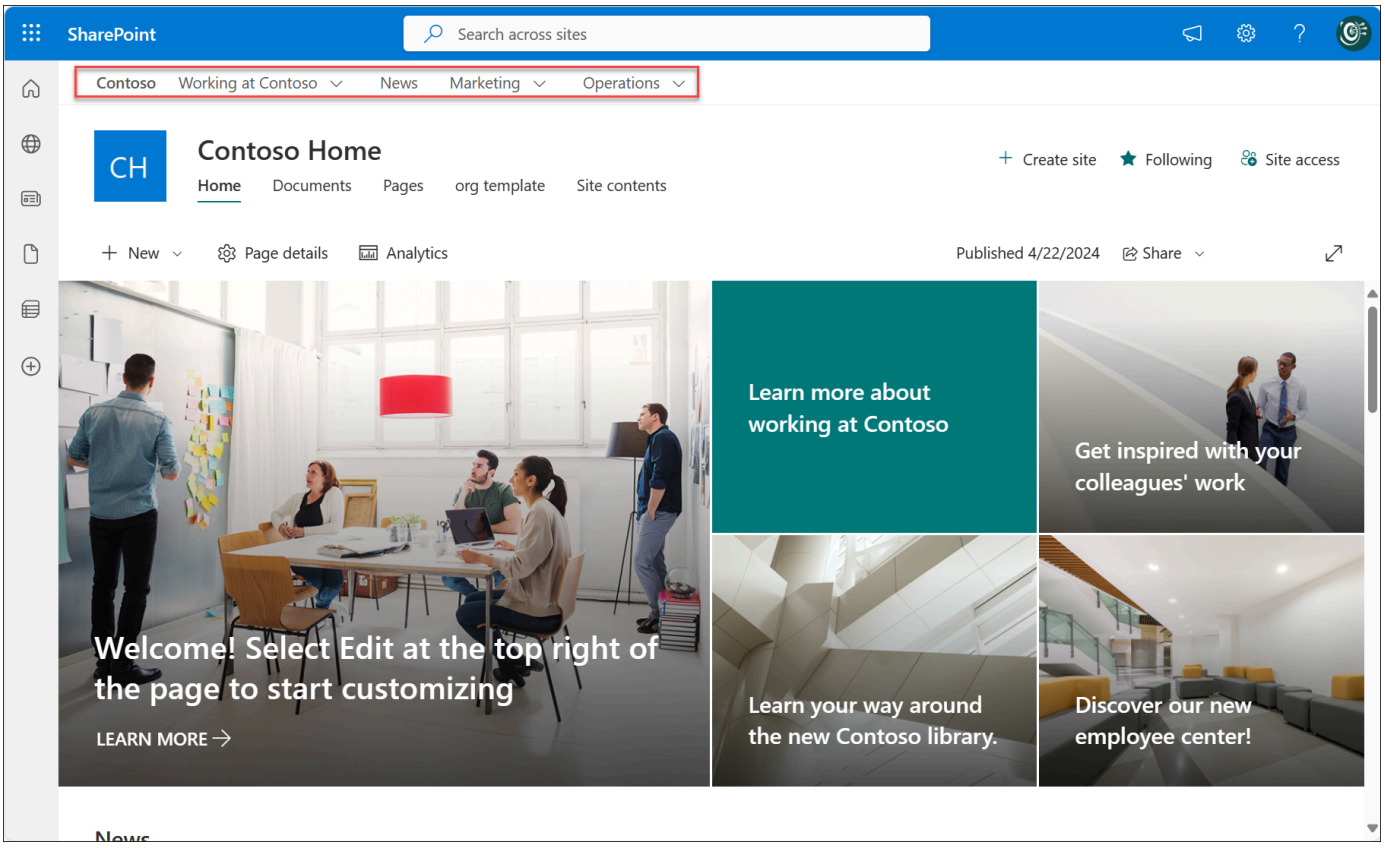
Hub navigation

SharePoint hubs help organize related sites based on project, department, division, region, or concept. Hubs make it easier to discover related content such as news and other site activities, apply common navigation, branding, site structure across associated sites and search across all associated sites. One of the important planning decisions for hubs is planning the hub navigation.



Hub navigation appears above the local navigation on each site, just below the suite bar, as shown in the image earlier in this article. Hub navigation is established in the site that is declared

to be the hub. It's defined by the hub owner and is shared by all the associated sites.



Each site can belong to only one hub at a time, but you can associate hubs together in a combination of navigation links and associated hubs as part of your navigation experience. For more information, see Planning your SharePoint hubs.

Local navigation

Local navigation is the static navigation that viewers see on every page of your site. For team sites, local navigation shows up on the left side of the page in the area referred to as the "quick launch". For communication sites, local navigation shows up at the top of the page. Local navigation is on every page in your site. It creates a persistent experience to allow site visitors to move back and forth among the pages and content on each site. Think about how viewers might explore your content and use local navigation to support that exploration.

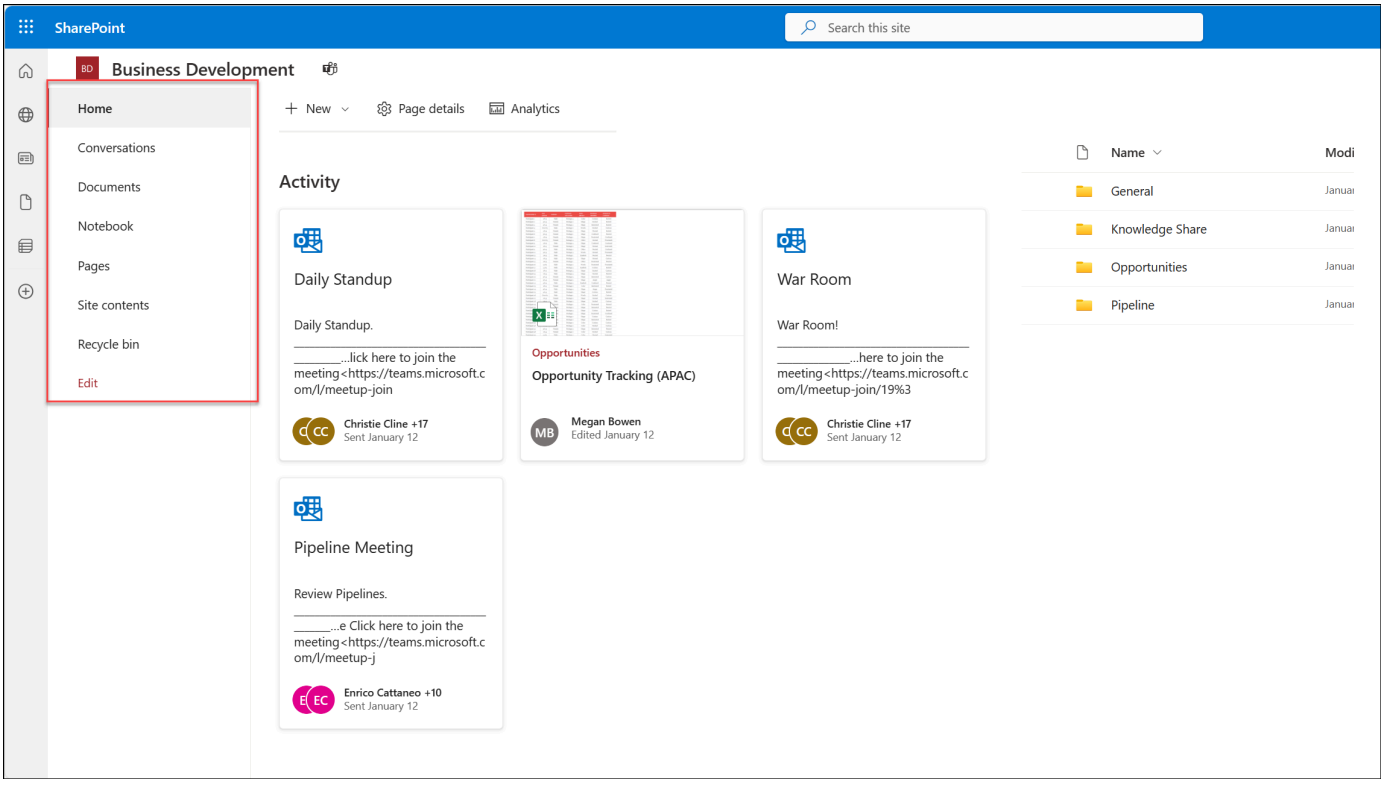
Example: A travel site might have the following local navigation links that support viewers who are exploring the travel site from the perspective of "what am I allowed to do?" and viewers who are exploring the travel site from the perspective of the travel process – before, during, and after their trip.

- Travel guidelines
  - Air
  - Car

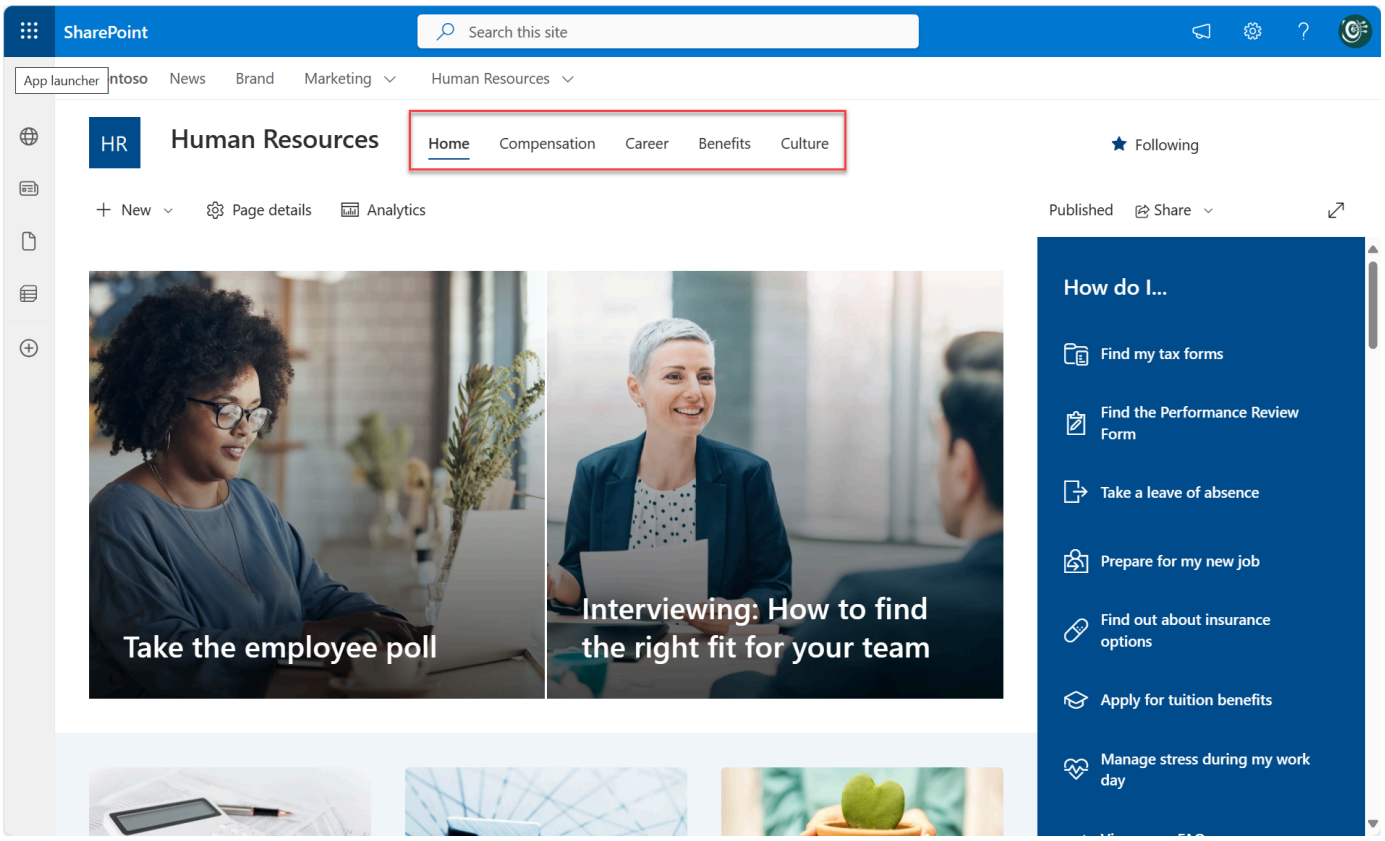
    - Ground transportation
    - Hotel
    - Train
- Before you go
    - Travel approval
    - Booking service
- During your trip
    - Travel safety
    - Itinerary changes
- After you return
    - Expense reporting
    - Trip reports

Where you see local navigation elements:

Team site navigation



Communication site navigation



Sites

Your intranet and portals are comprised of team sites and communication sites that provide further access into the site's pages, lists, and libraries.

One component to modern SharePoint team sites that makes information architecture easier to implement and maintain are Microsoft 365 groups. Microsoft 365 groups provide a membership service that allows for easy hub and site permissions as well as other functionality for SharePoint team sites and Microsoft Teams. With Microsoft 365 groups, you can give a group of people access to a collection of collaboration resources like Planner, OneNote, SharePoint team sites, and more. Microsoft 365 groups can only be used on SharePoint team sites.

Pages

Pages within team or communication sites provide an opportunity to use dynamic web parts that automatically update content from other sites and pages like News, Highlighted content, or Sites web parts. Every page in each site tells a story for the reader.

Your sites generally include three types of pages:

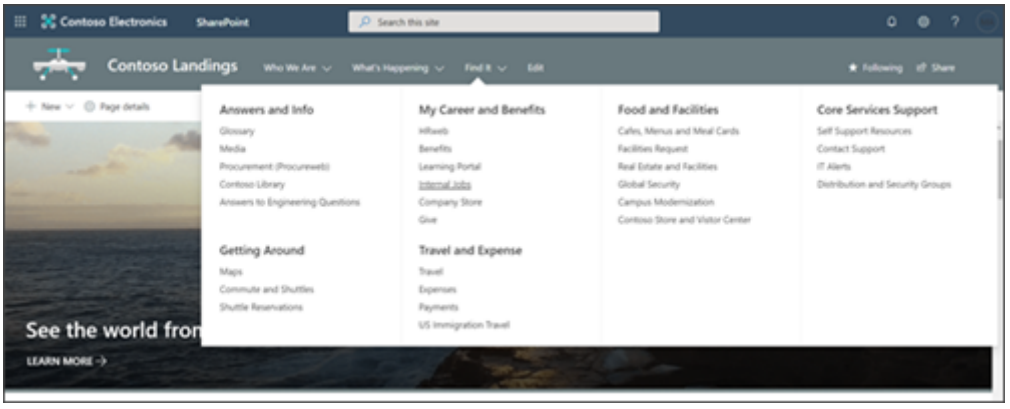
- The **home page** where you provide an overview of your content and introduce the reader to what they find on the site.

- **Navigation pages** that provide options or summary information for the reader and help them get to a decision point about where they want to go next.
- **Destination pages** that are the end point of the reader's journey. This is where you present information to read, print, or download. If you have a lot of information on your destination page or you want to provide supplemental explanations for detailed topics, you can create an ancillary page.

Since we know that most readers don't read every word on a web page or even scroll to the bottom, you need to pay attention to how you present information on each page. Make sure that you put the most important information – the information that your readers must have for your communication to be successful – at the top of the page. As the page continues, you can add additional information that is helpful, but not crucial. Think of this as writing with your summary or conclusion up front, instead of at the end. Use sections, headings, and bullets to make your pages easier to read. For more info, see Add sections and columns on SharePoint modern page.

Navigational elements

Navigational elements are menu styles like the mega menu, cascade menu, and footer menus. Secondary navigational elements include inline links and buttons.



Personalization elements

Audience targeting - Audience targeting helps the most relevant content get to the right audiences. By enabling audience targeting, specific content is prioritized to specific audiences through SharePoint web parts, page libraries, and navigational links.

Information barriers - Information barriers are policies in Microsoft 365 that a compliance admin can configure to prevent users from communicating and collaborating with each other. This is useful if, for example, one division is handling information that shouldn't be shared with specific other divisions, or a division needs to be prevented, or isolated, from collaborating with all users outside of the division. Information barriers are often used in highly regulated industries and those with compliance requirements, such as finance, legal, and government.

Multilingual considerations - If your organization spans a diverse population, you may want to make content in your intranet sites available in multiple languages. User interface elements like site navigation, site title, and site description can be shown in the user's preferred language. Additionally, you can provide pages and news posts on communication sites that you translate and that are shown in the user's preferred language.

To show the site name, navigation, and footer of your site in the different languages you've made available, each must be translated manually. For example, let's say you've created a communication site with an English default language, and you've enabled the site for Spanish

and German languages. When you create a site, you set up the site name and description in the default language (in this case, English). You can also update the site name and description after site creation. Then you create the navigation nodes and footer content in English.

After the site is set up in English, a user with Spanish as their preferred personal language manually edits and translates the title, description, navigation, and footer content into Spanish. A user with German as their preferred personal language does the same for German. Once the content is translated, it displays for all users of those preferred languages.

Metadata architecture

Columns and content types are the two most important metadata elements that you can use to organize documents and pages in your SharePoint site. Metadata helps your users filter and sort content within a list or library – but also helps with search. Use columns in your Site Pages library as well so that you can use highlighted content web parts to dynamically connect related pages based on shared metadata.

Folders are another way to organize document content, but folders are a physical construct with limited flexibility. Folders aren't necessarily bad – they can help you manage performance and security in your document libraries – but folder structures with more than one or two levels of nesting create a significant discoverability burden for users and should be avoided. Every site comes with one document library – but you aren't limited to just one library. Instead of using the one default Documents library on your intranet sites, consider adding topic-specific libraries and add site columns to organize your content within the libraries to avoid creating multiple levels of nested folders.

Search experiences

Search uses your information architecture investments to help users find content when they don't know where it might be in your architecture. It also helps users discover content that they may not have known about.

You can help users discover content and improve search outcomes by using several features in search, including acronyms, bookmarks, Q&A, floor plans, and locations. For more info, see Make content easy to find and Search experiences in SharePoint.

Next: learn about SharePoint information architecture principles

---

Last updated on 06/25/2026

Information architecture in modern SharePoint

The most effective SharePoint sites help viewers find what they need quickly so that they can use the information they need to make decisions, learn about what is going on, access frequently used tools, and engage with colleagues to help solve specific problems.

Even when search is available, most viewers start their web experiences by browsing. That pattern persists on internal web sites as well. Good navigation experiences present viewers with a complete picture of what is available, and combined with the home page, provide a comprehensive "story."

In this article:

- Understand basic information architecture principles
- Learn more about how to write effective labels and links
- See how to ensure frequently used tools and content are findable

Information architecture goals

Navigation should always be planned from the perspective of the user. Planning effective navigation involves considering not just the information you want to present, but also thinking about the information your viewers want or need to consume. Therefore, organizing and labeling your navigation links is critical for the purposes of usability and findability.

Successful intranet and site navigation experiences enable users to:

- **Find information** – Users need to find documents, files, and links most relevant to the work they do without spending time sifting through content. Make sure to present only the most relevant and high-priority information first.
- **Take action** – Users typically have a specific task in mind when they visit a site. Make sure common tasks are built-in to navigational structure as labels and links so that they can be easily identified and accessed.
- **Understand company structure** – When viewed at-a-glance, users should be able to get a sense of how the organization is structured. Make sure you incorporate hierarchy and structure into site and intranet navigation.

Get organized

There is no one right way to organize your navigation links. You will make different choices based on the type of site you are creating and your viewers. Organizing concepts might include:

- Services
- Products
- Activities
- Audiences (if your viewers can clearly identify the audience to which they belong – such as student or teacher)
- Expertise areas or functions

As you organize user needs and business needs, consider the following:

- **How can information architecture reduce the cognitive load for your viewers?** - Cognitive load is the amount of information that a person can process at any given time. Managing the user's cognitive load helps prevent information overload and time wasted finding resources. Ensure you understand your viewers needs prior to implementing information architecture.
- **What is the current mental model of your users?** - Mental models are the existing models people use while interacting with a website or application. Information is easier to discover when it is in a place that matches the user's mental model of where it should be.
- **How can information architecture help users make better and more efficient decisions?** - Decision making can be incredibly taxing. Information architects can help us make decisions by providing certain information at key moments.

The default navigation for all SharePoint sites primarily includes type of content. For communication sites, the default navigation includes Documents, Pages, and Site Contents. These categories are helpful as you are building your site, but they are not typically going to add value to your viewers once your site is ready to launch. This is because the consumer of a communication site typically doesn't care about the type of content – they care about the purpose or subject of the content. For communication sites, plan to delete the "out of the box" navigation when you are ready to launch and replace it with something that aligns with the guidance provided in the local navigation section of this guide.

The default navigation for team sites includes links to the related services provided by Microsoft 365 for modern teams – including a link to the shared team notebook and the conversations for the team in Outlook. These represent the typical features that teams need to effectively collaborate and might be hard for people to find without the experience provided by

the navigation. You may choose to supplement or refine these links for your team sites, but you will also likely find that the default navigation experience is a good starting point. You may be more likely to keep most of these links than you would with a communication site.

Prioritize usability and findability

The key goal when we plan navigation is to make our sites useable and our content findable. The best way to ensure that your navigation meets these goals is to test it. There are several cost-effective approaches that you can use to ensure that your navigation design is effective, including:

- **Card Sorting** - Primarily helpful for planning navigation.
- **Tree Testing** - Helpful for testing suggested navigation paths.
- **Usability Testing** - Task-based scenarios that are helpful for comprehensive testing of site and page navigation.

These two resources provide an overview of techniques and tools for testing the usability and findability of your navigational strategy:

- Usability Analysis
- Overview of Testing Approaches

Write clear and intuitive labels

The words you use for navigation matter – not just because the real estate for navigation is limited – but also because your labels are what guide your viewers to the content. Each label makes a promise: if you select this link, you should get the information you expect to find.

To ensure that your labels keep their promises, make sure they are:

- **Specific** - Tell the viewer exactly what they will find when they select the link. If the target for your link includes Policies and Procedures, make sure the label includes both terms.
- **Comprehensive** - Describe content with your collection of labels. You should not plan to link to every single page or document in your navigation, but your navigation should provide a complete picture of the content on your site.
- **Concise** - Keep your labels short and to the point.
- **Familiar** - Don't make up terms in your labels. Keep your viewers in mind – if you use an unfamiliar term, your viewers will be confused and unable to find what they need.
- **Front-loaded** - Make sure that your labels are "scannable." For example, Company Information is better than Information About our Company.

- **Clear** - As much as possible, you want your navigation labels to be mutually exclusive – at least for the major categories. It is perfectly fine to have a sub-link display in multiple categories – especially if viewers might expect to find it in more than one place – but the major categories need to be easily distinguished from one another.
- **Targeted** - It's not a good idea to show people links to private sites that they don't have access to. Where appropriate, use the audience targeting features for SharePoint to target navigation links to viewers for whom the link will work. Note that there are exceptions to this guideline. For example, you may want to use your navigation to help people discover sites that they may not have access to today but could be approved to join. If you do provide links in navigation to private sites, be sure that the owner of the site knows that they may be getting a lot of access requests!

Think about link target interactions

Many usability guidelines recommend limiting the number of new windows that are automatically opened for site viewers. Most of the time, opening a link in the same window allows site viewers to use the back button when they want to return to your site. When a viewer wants to open a link in a new window, the guidelines recommend that the viewer be allowed to choose this outcome by "right clicking" the link. An exception to this guideline is the recommendation to always open documents in a new window to prevent users from accidentally closing the browser window when they close the document.

By default, navigation links on modern SharePoint sites open to a link that points to:

- **A page or site in the same tenant** (same site or another site) - Links open in the same tab.
- **A document** (same site or different site) - Links open in a new tab.
- **An external site or document** (internet site) - Links open in a new tab.

In classic SharePoint sites with publishing features, you can choose to open navigation links in a new window. This allows you to consider the context for your site viewers and determine whether it might be helpful to open a link in a new window. There is no way to select how navigation links open in modern SharePoint sites. This means that your navigation links will follow the default guidelines, but you still need to be especially careful about the labels for navigation links to make sure that your viewers know that they are leaving the site when they select the link.

Make sure that the navigation label accurately describes the destination – a place on a completely different site or an application – and if you know that the back button may not work, consider using an alternative way to present the link, such as the text web part where you can elect to open a link in a new window.

At the current time, only the Text web part lets you create a hyperlink and choose how the link opens. When you add a hyperlink to text, you have the option to choose to open the link in a new tab.

Test usability and findability with real users

Once you have established a basic working structure for global, hub, or local level navigation experiences, you should test your design with real-life users. Create tasks and ask users to complete the tasks. Ask users to "think out loud" as they are looking for information and resources. Note where improvements can be made and then implement and test the changes again. Plan to review basic global, hub, and local navigation experiences as your business changes and grows.

Learn more about navigation basics like how to write effective labels, how to test findability, and how to use menu styles.

Next: learn about SharePoint information architecture models and examples

---

Last updated on 06/25/2026

Information architecture models and examples

Navigation design defines the visual way of finding components (menus, links, sites, and pages). Navigation design aims to help users understand how to interact with SharePoint sites and portals and what types of information are available. Options for implementing navigation differ based on the framework for your sites and intranet.

In this article:

- Learn about information architecture elements
- Explore common information architecture models and scenarios
- Use the models and scenarios as a starting point for navigational design

Information architecture modeling elements

Information architecture elements are secondary components to navigation design that compliment building blocks. The following components should be considered when selecting, planning, and implementing navigational design for global, hub, or local navigation.

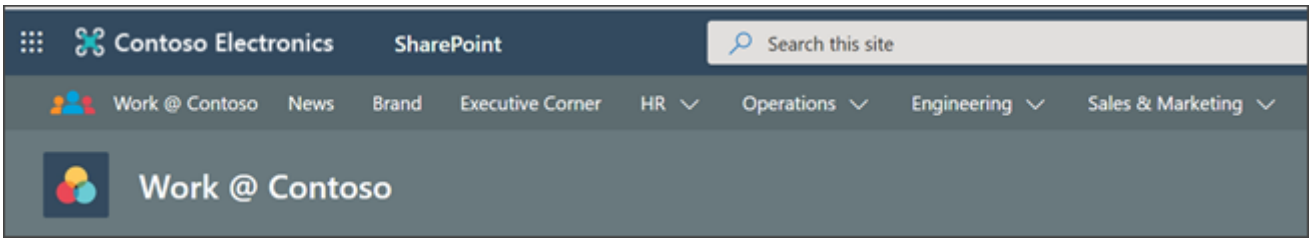
- **Site hierarchy** – Use hubs and visual layouts to establish visual hierarchy
- **Security** – Data governance, administration, and editing privileges
- **Taxonomy** – Record management, compliance requirements

Common models for navigation design

The way you organize sites and content depend on the composition of your organization and the needs and goals of your users. For example, if your goal is to enable front-line workers with specific sites and documents, you may decide to optimize navigation for a mobile device. Another example, if your goal is to create a collaboration space for your team, you may decide to design your SharePoint team site to align with Microsoft Teams.

Common methods of organizing navigational design:

By department

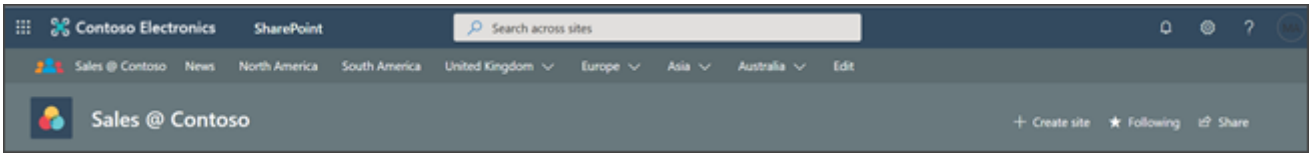


Benefits - Most users already have a well-established mental model for navigation broken down by department. This model scales many sizes and types of organizations and is a common method for organizing and planning hubs.

Governance considerations - For large organizations, especially with international offices, it can be challenging to make sure the right people have access to the right content for security and compliance purposes. Consider using personalization elements like information barriers and audience targeting to help surface content the specific audiences.

Maintenance considerations - As the business grows and departments and team move, you need to update global, hub, and local navigation to reflect organizational changes.

By geographic location

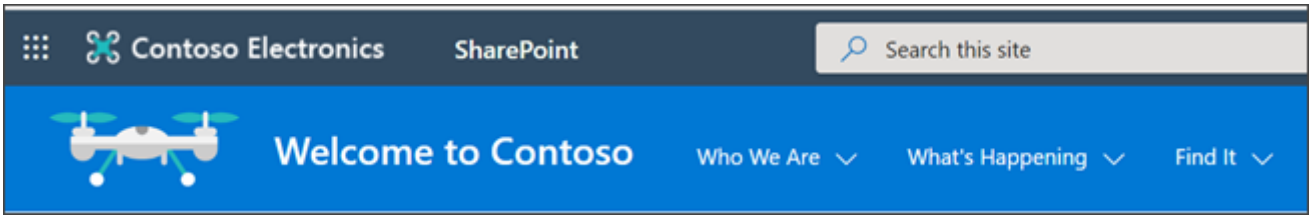


Benefits - Organizing by geographic location is an effective way to bring people of similar disciplines together to collaborate and build community. For large organizations, and international organizations, location can be an important decision-making factor for users. Organizing by region may be important when certain topics have different laws and mandates depending on the region. For example, crisis management sites or human resource guidelines.

Governance considerations - Many governance details may vary by region, for example site creation policies, data retention, and data storage policies. Learn more about the multi-geo user experience and multi-geo configuration.

Maintenance considerations - When the organization moves locations, navigation needs to be updated to reflect those changes. There are other multi-geo considerations to plan when enabling SharePoint, Microsoft 365 groups, and other Microsoft 365 apps globally. Multi-geo enables global businesses to control the country or region where shared resources like SharePoint Team Sites, Office 365 Groups content (associated SharePoint Sites and shared mailboxes) are stored and managed.

By task or scenario

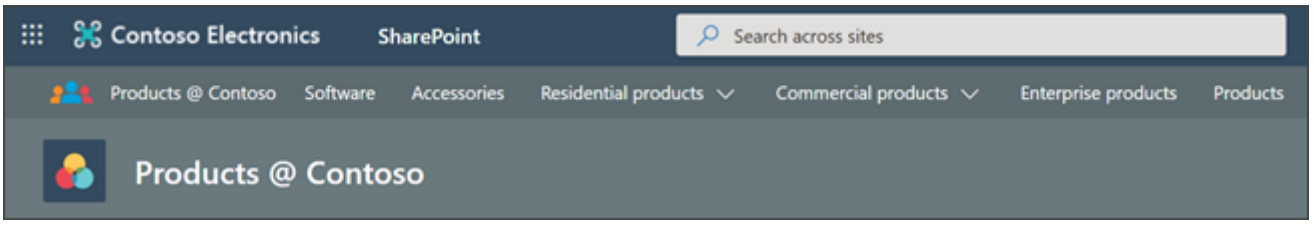


Benefits - Organizing by scenario within navigation helps users learn about a general concept, for example "about us" pages. Organizing by common and frequently used tasks is helpful in the same way, for example tasks like "get reimbursed" or "pick a healthcare plan."

Governance considerations - This style of navigation could attract a broad and high-volume audience depending on the rest of your navigation design. High volume sites should take extra care in ensuring page performance is managed by optimizing image sizes and other details. Consider using tactics like creating hubs to organize tasks by departmental needs, which will make it easier to manage page access and organization.

Maintenance considerations - When organizational information (leadership, locations, etc.) becomes outdated, navigation needs to be updated.

By portfolio



Benefits - Sometimes content is best organized by type, or portfolio, to display content in natural groupings or for specific audiences. Organizing your navigation by portfolio offers flexibility as your business scales and grows.

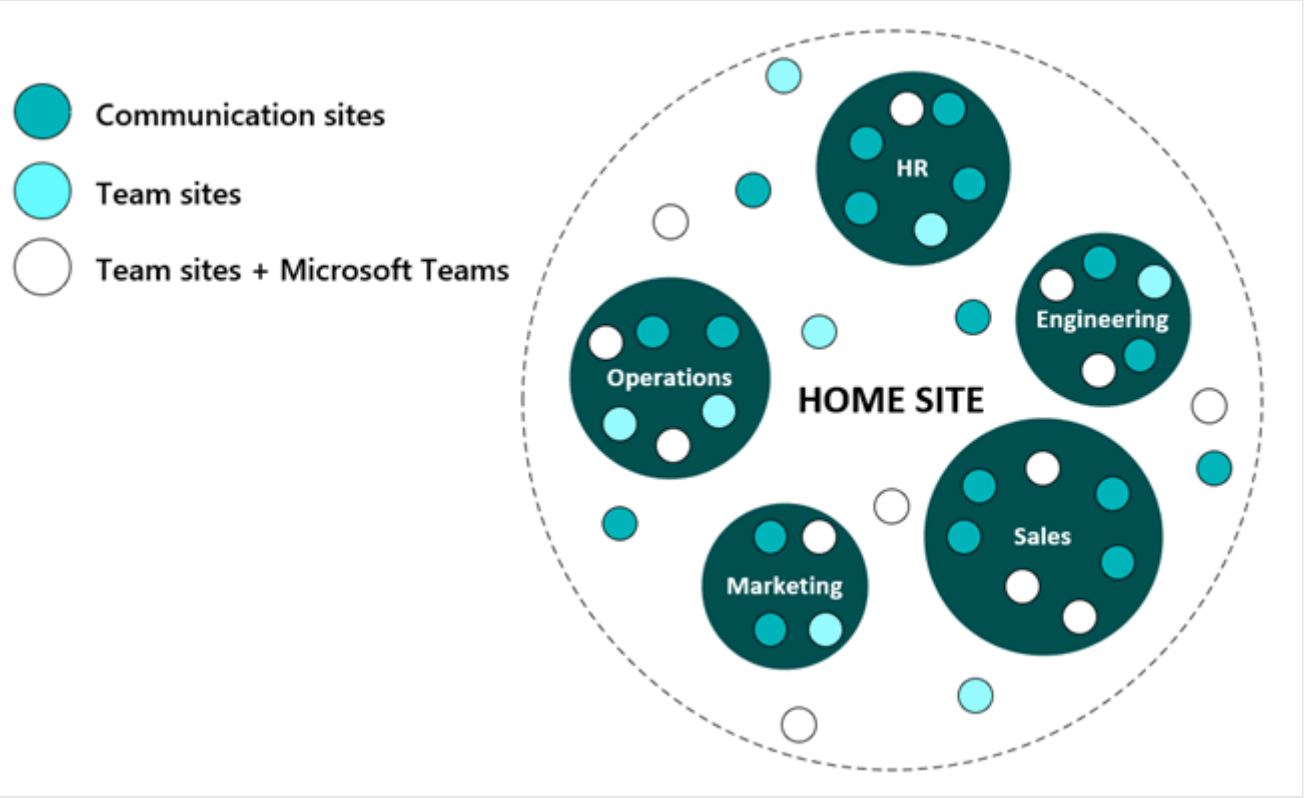
Governance considerations - For large organizations, especially with international offices, it can be challenging to make sure the right people have access to the right content for security and compliance purposes. Consider using personalization elements like information barriers and audience targeting to help surface content the specific audiences.

Maintenance considerations - As the business and portfolios grow, the navigation needs to reflect organizational changes.

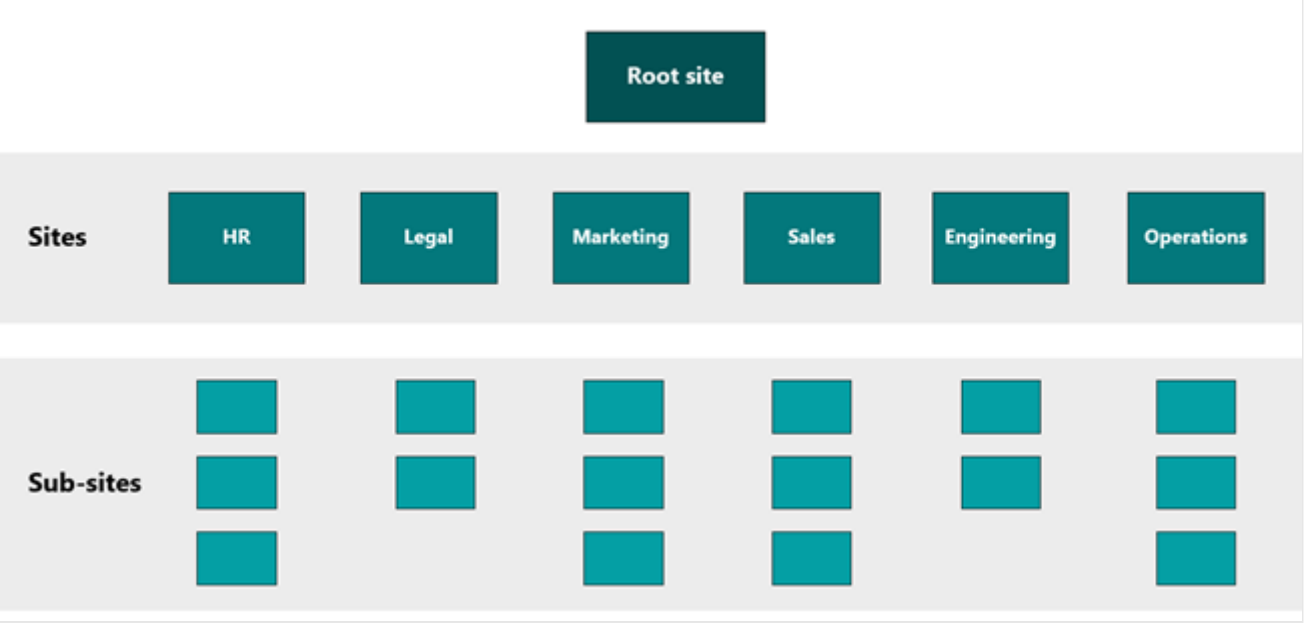
Scenarios

Scenario 1: Move to modern navigation from classic navigation

Modern navigation



Classic navigation



Your intranet is an ever-evolving component of your business that will need to grow and scale alongside your organization. Modern intranet navigation differs from classic navigation in the sense that it is “flat”--in the modern SharePoint experience, sub-sites are not recommended. In the new “flat” world of modern SharePoint, plan to create one site for each discrete topic or unit of work. Classic SharePoint architecture is typically built using a hierarchical system of site

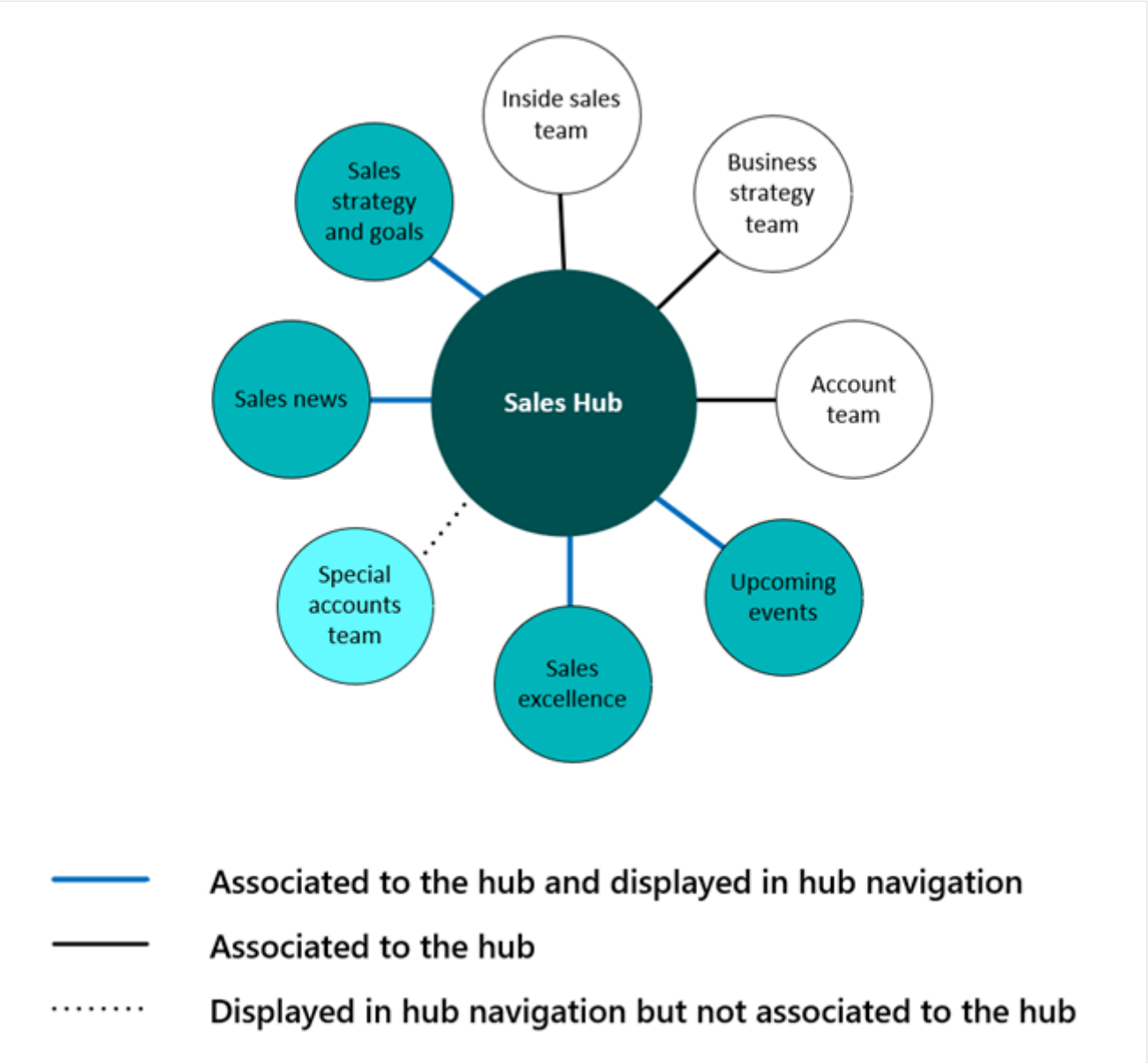
collections and sub-sites, with inherited navigation, permissions, and site designs. Once built, this structure can be inflexible and difficult to maintain.

Focus on incorporating modern changes that have the greatest impact to your business first. Plan and schedule when changes are incorporated and how you'll track progress. Use site analytics to understand user behavior and collect feedback from users along the way. How to get started

Moving to modern navigation from classic SharePoint navigation is a process that depends on the size of your organization and the complexity of your tenant's configuration. Below are general guidelines and tools you can use to get started:

- Define new intranet business objectives and choose pilot scenarios
- Get organized and find methods to test potential designs
- Take an inventory of your current sites and subsites
- Start planning hubs and your home site by grouping high priority tasks and content
- Release hubs and associated sites in phases
- Regularly review hub and site analytics to track page traffic and popular content
- Make navigation changes based on your learning from user testing and analytics

Scenario 2: Consider modern hub navigation configuration



These are special considerations for planning hub navigation. A site can be:

- In the hub navigation and be associated to the hub
- Associated to a hub and not be in the hub navigation
- In the hub navigation and not associated to the hub

Example 1 - Site is in the hub navigation and associated to the hub.

Showcasing sites associated to the hub allows viewers to discover the sites within the hub family and easily navigate among and across the “family members.” Adding an associated site to the hub navigation displays the organizational framework for the collection of sites in the hub navigation. All sites in the hub share a common theme and navigation helps to establish the identity of the hub family both visually and via viewer interaction. Your hub links can go to sites or content pages or a combination of both – but use the practices described for link labeling to ensure that you're providing clear and consistent experiences.

When you choose to show all associated sites (and associate hubs) in the hub navigation, think about whether all the people who have access to the hub will also have access to each of the sites associated to the hub. For example, if you add links to private sites in the navigation, you're increasing their "discoverability," which can be a good thing – if the site owners for those private sites are prepared to get access requests. However, you may not want to show restricted sites in the navigation if the site owner doesn't want the site or the content to be discovered.

To ensure that your hub navigation links keep their promises, consider the following options:

- For links that shouldn't be discoverable to all viewers, target the link so that it only shows up for audiences who have access to the content.
- For "discoverable" but restricted links, consider adding the word restricted, or request access, or private to the label. Have a conversation with those site owners to make sure that they're prepared for potentially more frequent access requests. In addition, you could consider adding the “lock” emoji to your private or restricted sites.

Example 2 - Site is associated to the hub and not shown in the hub navigation.

If the use case for your hub is primarily about sharing a common theme or for rolling up content for people who are members of private sites, you may want to associate a site to a hub but not showcase the site in the shared hub navigation. One reason that this might be OK is that the members of the private sites already know about the sites and don't need the hub to provide links to the site. However, these same site members would find it useful to see the news and activity rolled up from their private sites on the hub (via the Highlighted Content and News web parts.

Another reason not to show associated sites is that the owners of one or more private sites don't want the sites to be discovered in the hub navigation or they are not prepared to manage unexpected access requests.

Example 3 - Site is added to hub navigation but not associated to the hub.

One of the nice features of hub navigation is that it allows you to plan a shared navigation experience for all the sites associated to the hub – including links to frequently needed sites that are not part of the hub.

If a site is associated to a hub, it's reflected in the hub navigation. You may not want all sites that are related to the hub "family" to be associated to the hub. For example, consider a scenario when you're collaborating with external partners on a team site. You may not want to associate external sites to your hub because you may not want to display the shared navigation for the hub

to external partners. But, you may want to add links to the external sites to the hub navigation to make it easier for internal viewers to discover these related external sites.

This presents a convenient way to showcase links to all the external sites managed by the business group without having to worry about exposing navigation links to external viewers. When internal viewers navigate to the external sites, they'll no longer see the hub context and theme – but this is the desired outcome.

A site can only be associated to one hub. However, you can increase discovery by adding navigational links to other hubs or other sites in your hub navigation.

Next: learn how to get started planning and implementing SharePoint navigational design

---

Last updated on 06/25/2026

Get started planning and implementing SharePoint navigation design

To begin, understand that no two organizations will build identical architecture structures in SharePoint. This is because your architecture design stems from the unique needs of your organization and users. Also, remember that architectural structure will change over time as you learn more about user needs and as the business scales and grows.

Similar to SharePoint intranet content, SharePoint architecture should be reviewed and revised as often as needed to ensure users have easy access to relevant content and resources.

In this article:

- Explore how to understand users' needs, content requirements, and scope
- Learn how to think about planning, implementing, and managing global, hub, and local navigation

First: Understand your users

The most important step in planning an effective information architecture is understanding your users:

- Who are your users? What key roles do they have?
- What vocabulary do they have? What terms do they use to look for content?
- What do they want to learn?
- What do they want to do? What are their top tasks?

Next: Understand your content

In addition to understanding your users and their experiences, you also need to understand your content. Think about how content is distributed across current intranet sites, libraries, and folders. Look at usage data to understand what content is accessed most and least frequently.

Think about the categories of information in your organization, such as services, products, areas of expertise, and functions. Don't just think about the organization chart. Think about the information people need in their daily work and the key business outcomes you want to achieve. Use this information, and your knowledge of your users, to organize groups of related

information, such as key business processes, major projects or initiatives, key business roles, frequent tasks, services, as well as organizational units.

Then: Understand your scope

Information architecture includes five primary elements:

- **Portal navigational structure** – How you structure your sites so that users can find content including the home site of your intranet.
- **Hub structure and organization** – How you group together similar topics, tasks, and content.
- **Site and page architecture** – How content is organized on each site and page so that users can further navigate or consume content effectively.
- **Metadata architecture** – How to structure and label your individual content items for browsing and searching as well as compliance and retention.
- **Search experiences** – How your users "consume" information architecture in addition to browsing.

Finally: Decide which navigational model works and start to plan and implement

New navigational design for a site:

> **Note**
>
> To edit site navigation, you must be a site owner.

Expand table

Plan	Build	Manage
1. Ensure you understand your users needs and the site goals. 2. Learn about designing for local navigation.	1. Customize the navigation of your site. 2. Consider joining a hub site to increase viewership. 3. Target navigational links to specific audiences.	1. Use site analytics to understand how users are engaging with your site. 2. Review site navigation as needed to ensure all links are active, relevant, and up to date.

New navigational design for a hub:

> **Note**
>
> To edit hub navigation, you must be the hub owner or tenant administrator. The default navigation menu style for team sites hub navigation will be cascading.

Expand table

Plan	Build	Manage
1. Ensure you understand your users needs and the site goals. 2. Learn about designing for global navigation. 3. Consider using a hub site to group similar sites together. 4. Learn about multi-lingual considerations.	1. Decide on a menu style. 2. Customize the navigation for individual sites. 3. Set up associations and permissions for hub sites.	1. Use hub analytics to understand how users are engaging with your site. 2. Review site navigation as needed to ensure all links are active, relevant, and up to date.

New navigational design for an intranet site:

> **Note**
>
> To edit intranet site navigation, you must be the hub owner or tenant administrator.

Expand table

Plan	Build	Manage
1. Define new intranet business objectives and choose pilot scenarios. 2. Learn about user needs and find methods to test potential designs. 3. Take an inventory of your current sites and subsites 4. Plan the home site.	1. Start planning hubs and your home site by grouping high priority tasks and content. 2. Set up associations and permissions for hub sites. 3. Release hubs and associated sites in phases.	1. Establish an intranet review team that ensures navigation and content are up to date and aligned with your organization. 2. Regularly review hub and site analytics to track page traffic and popular content. 3. Make navigation changes based on your learning from user testing and analytics.

Next: learn how to get started planning and implementing SharePoint site navigation

Last updated on 06/25/2026

Plan and implement SharePoint site navigation

The fundamental principles and practices for site and page navigation apply to classic and modern SharePoint architectures. However, your options for implementing navigation differ based on the framework for your sites and intranet. For example, the default navigation experiences available in classic SharePoint site hierarchies - sites with subsites - aren't available in the modern experience.

Instead, hubs provide a great way to achieve the cross-site navigation features previously available in managed navigation and site hierarchies in classic SharePoint. No matter which framework you're using, you can use the guidance in this document to help you create the right navigation for your organization.

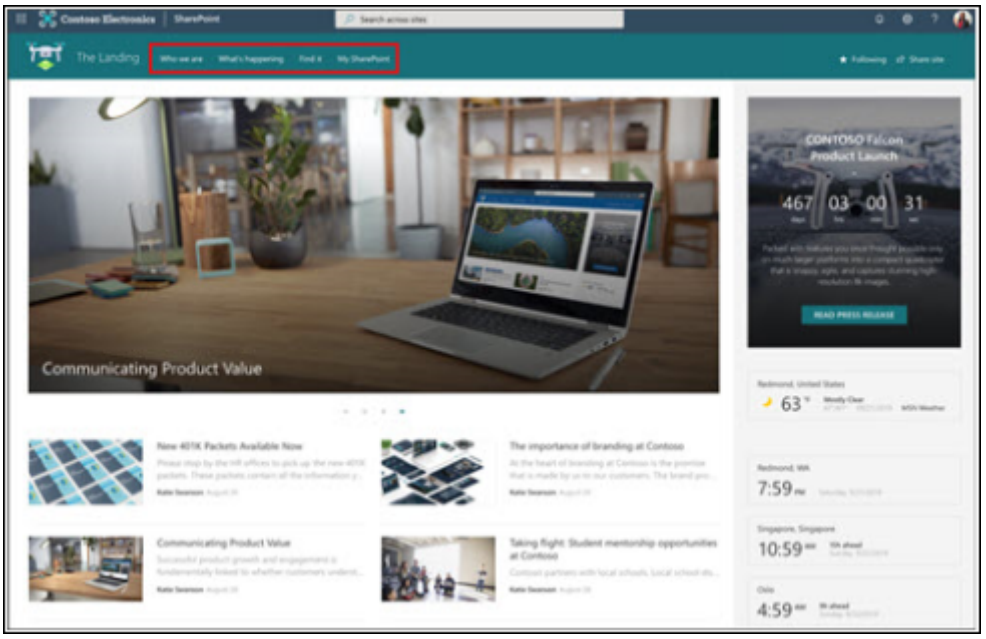
In this article:

- Explore considerations and best practices for site and page navigation design
- Learn about site navigation best practices
- Learn about menu styles and experiences

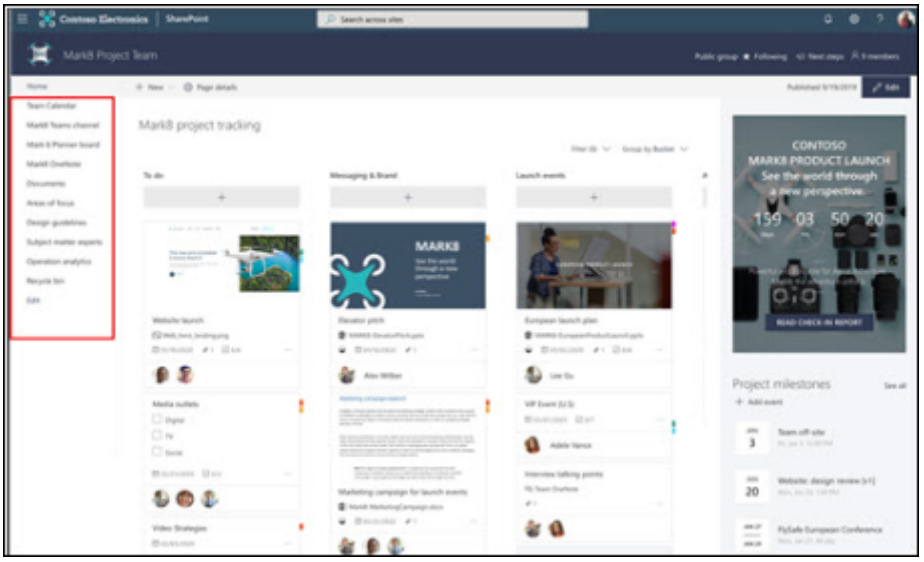
SharePoint site navigation

This planning guide primarily addresses *site* navigation: the top (team and communication sites and hubs) and left (team sites only) navigation experiences.

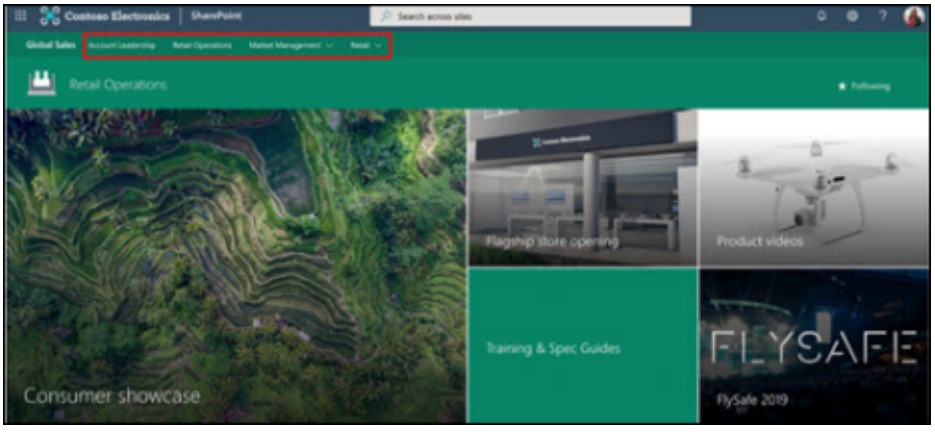
Top site navigation



Left site navigation



Hub navigation (top site)



"When we're observing customers carrying out tasks on websites we notice certain common patterns. For example, we find that when people arrive at a particular site they start by ***navigating***

***about 70% of the time**. When people get stuck navigating, they may resort to using site search.*" -- Gerry McGovern

Why navigation is important

The most effective SharePoint sites help viewers find what they need quickly so that they can use the information they need to make decisions, learn about what is going on, access the tools they need, or engage with colleagues to help solve a problem.

Even when search is available, most viewers start their web experiences by browsing. That pattern persists on internal web sites as well. Good navigation experiences present viewers with a complete picture of what is available on the site and, combined with the home page, provide a comprehensive "story" for the site.

Page navigation and site navigation display differently. The links in site navigation are static on every page in the site. The navigation links on individual pages are accessed only when the viewer lands on the page. A benefit to on-page links is that they can be different from page to page. Both types of navigational links guide your viewers by providing *wayfinding* experiences.

The key advantage of site navigation links is that they're always visible in the context of the site. Because site navigation links are persistent, they provide an opportunity to provide significant value for site viewers as they traverse the site and address their goals: to find and do what they came for. Hub navigation links extend this wayfinding experience to other sites in the hub "family." This supports navigating to related content not just on the site, but on related sites as well. Setting site navigation links to open in a new tab can help site viewers find the information they want, without navigating away from the current page that they are on.

Site and page navigation fundamentals

When you plan site and page navigation, you want to think about:

- **Organizing** – Grouping logical and similar intents
- **Labeling** – Writing clear labels your users will immediately understand
- **Usability** – Users' ability to easily navigate the end to end experience
- **Findability** – Users' ability to quickly find what they need

Navigation should always be planned from the perspective of the user of information – the viewers to your site. Planning effective navigation involves considering not just the information you want to *present*, but also thinking about the information your viewers want or need to *consume*.

Therefore, organizing and labeling your navigation links is critical for the purposes of usability and findability. If 70% of viewers come to your sites expecting to browse for information, the usability of your site depends on creating a great browsing experience. To learn more, see Information architecture principles in SharePoint.

Organizing

There is no one right way to organize your navigation links. You will make different choices based on the type of site you're creating and your viewers. Organizing concepts might include:

- Services
- Products
- Activities
- Audiences (if your viewers can clearly identify the audience to which they belong – such as student or teacher)
- Expertise areas or functions

The default navigation for all SharePoint sites primarily includes *type* of content. For **communication sites**, the default navigation includes Documents, Pages, and Site Contents. These categories are helpful as you're building your site, but they are not typically going to add value to your viewers once your site is ready to launch.

This is because the consumer of a communication site typically doesn't care about the *type* of content – they care about the *purpose* or *subject* of the content. For communication sites, plan to delete the "out of the box" navigation when you're ready to launch and replace it with something that aligns with the guidance provided in the local navigation section of this guide.

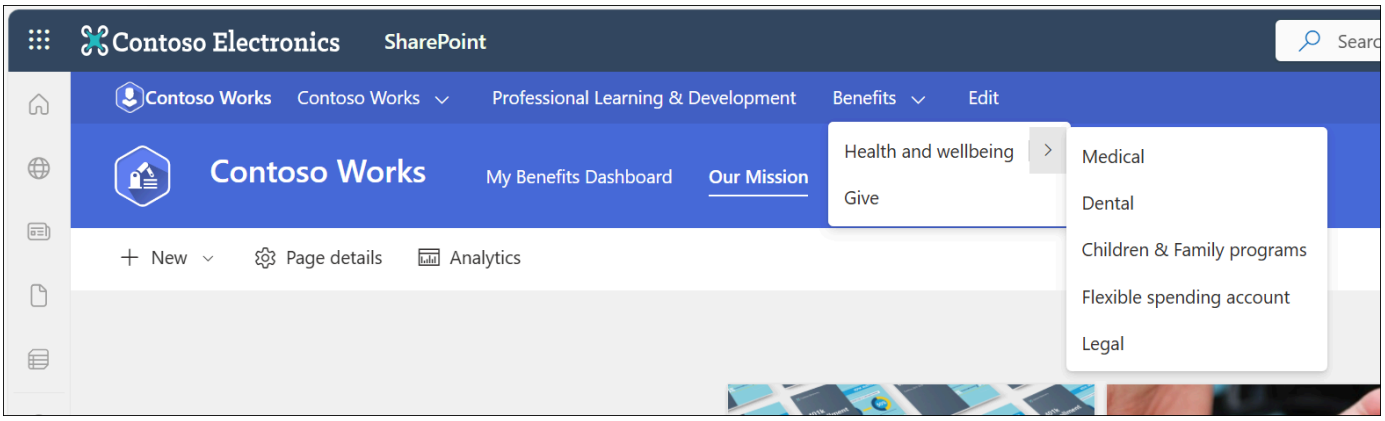
The default navigation for **team sites** includes links to the related services provided by Microsoft 365 for modern teams – including a link to the shared team notebook and the conversations for the team in Outlook. These represent the typical features that teams need to effectively collaborate and might be hard for people to find without the experience provided by the navigation.

You may choose to supplement or refine these links for your team sites, but you will also likely find that the default navigation experience is a good starting point. You may be more likely to keep most of these links than you would with a communication site.

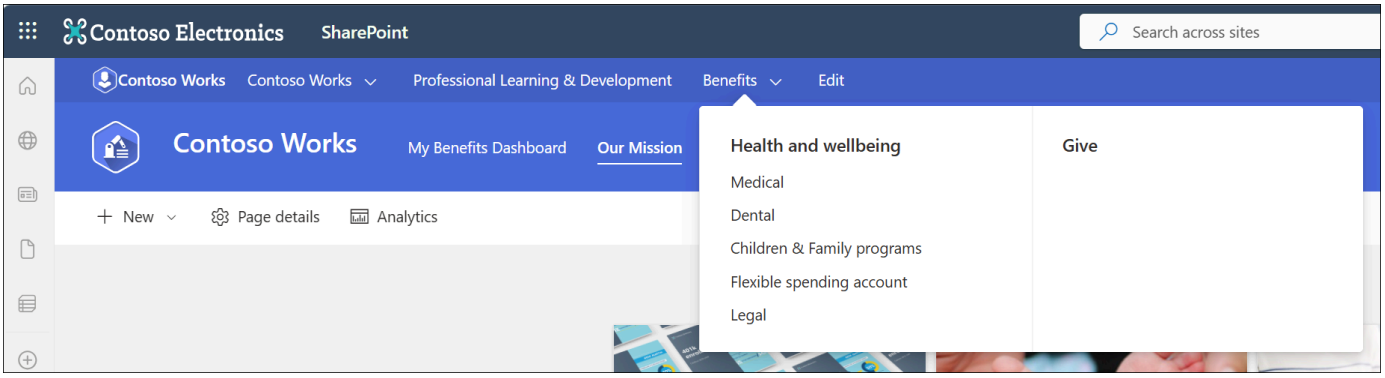
Navigation menus in SharePoint

There are two types of navigation menu styles for SharePoint sites - cascading and mega menu. Team sites and communication sites support both mega menus and cascading menus. Hubs, whether they are team sites or communication sites, add an additional mega menu to the site. Mega menus are not available in on-premises sites. Learn about how to customize the navigation on your SharePoint site.

Cascading menu



Mega menu



Menu links

There are two types of navigation links: a label and a link. A label is simply a category link – it lets you group related links but is not a link itself. A link requires a hyperlink and presents a "clickable" experience for the user. A label should always have at least one link below.

Both cascading and mega menus support up to three levels of navigation in your menu. The first level represents the tabs you see across the top. The second level is the next level below the tab and the third level is indented or below the second level. Mega menus work best when you're using all three levels of navigation experiences. If you use a mega menu, the second level of links will appear in **bold**. If you only need two levels in your menu, consider using the cascading style.

Menu experiences

There are two types navigation experiences – targeted and not targeted. With targeted navigation, you can choose who sees navigation links to create more personal navigation experiences. With non-targeted links, all users see the link, even if they don't have access to the target location. Learn about how to target navigation links in menus.

Menu symbols

All types of menu links support some decoration with emojis. Emojis can be used at the beginning or end of a link label to add some visual interest to your links.

Choose an emoji that relates to the label topic. You can search for emojis at emojipedia.org, or use the Windows key + period (.). Copy the emoji and add it to the label when you're editing your navigation.

Link to pages, not individual documents

Document links open in a new window, which is helpful if someone wants to close the document after reading, but document links take viewers to a new context. In some cases, this may be the experience you want. But when navigation points to a page with an embedded document instead of directly to a document, you have an opportunity to provide *context* for the document and retain the navigational context for the site. Think about the following alternatives if you want to use a navigation link to open to a single document:

- Can you re-create the document content as a page instead of a document? Pages are easier to read online and provide opportunities to create rich, dynamic experiences for your viewers. Modern pages are easier to read on mobile devices. Documents are great when viewers need to download or print – but when all they need to do is read, a short, well-crafted page is a better way to present and maintain information.
- Embed the document or a link to the document on a page. When a visitor clicks the link to a page, the site navigation remains visible. The page allows you to provide context for the document and it also keeps the viewer in the context of your site.

Practice progressive disclosure

Navigation should answer the question, "What can I do on this site or from this location?" But, limited real estate on the navigation bar or quick launch means you need to apply the principle of progressive disclosure. This approach suggests that you group your content into logical categories and provide a limited set of choices for your viewers to allow them to explore each content category to learn more.

Progressive disclosure applies to all types of navigation and not just top or site navigation. It also applies to page content. You don't need to have a link to every bit of content on your site or in your portal in the navigation – but your viewers should be able to get a sense of the entire site by exploring your navigation options. Great navigation experiences help viewers understand:

- Where am I?
- What can I do here?
- Where can I go next?

Plan to optimize the navigation experiences for your viewers by combining navigation and page links to answer these three questions.

Managing navigation expectations

Navigation enhances the story of your digital workplace by making it easy for users to browse the content they need. On the internet, we expect to have to search for the content we need. Yet on the intranet, viewers expect a navigation experience that is carefully curated to help them understand and find the content they need.

Curating a navigation experience for intranets and digital workplaces comprised of even just a few hundred sites can be a daunting task – especially your goal (or the goal assigned to you) is to make sure that all content is findable in "three clicks." Contrary to popular belief, your viewers will not leave your site or give up if they are unable to find what they are looking for in three clicks! More or fewer clicks do not make viewers happier or perceive that the site is faster.

What really matters in navigation experiences is "information scent" – whether the label for the link provides an adequate clue about where the "click" will go. It is the quality of the label and whether the label fulfills its promise that has the highest impact on usability. Viewers are willing to click to find information if they are confident that with each click, they are headed in the right direction – closer to their goal.

"Information scent" on SharePoint sites can be achieved with **clear, mutually exclusive labels** for links and labels lists and libraries that clearly tell viewers what they will find. You can improve your navigation by spending time testing to make sure that the navigation labels resonate with your viewers and following the guidance for labels recommended in this document. Your navigation outcomes will be most successful if you take the time to understand your viewers, their key "tasks and asks," and design navigation experiences that keep their promises.

Last updated on 06/25/2026

Planning your SharePoint hub sites

Hub sites help you organize your intranet. Getting the most value from hub sites requires some up-front planning. Read on to find out more about hub sites and how you can plan for them.

Setting the stage

SharePoint hub sites provide an important building block for your intranet. They're the "connective tissue" you use when organizing families of team sites and communication sites together.

One of the key principles of modern intranets based on Microsoft SharePoint is that each unit of work should get a separate site collection. This helps you to manage governance and growth over time. Each communication site and Microsoft 365 group-connected team site is created as a site collection that can have its own permissions. A hub site (most commonly created from a communication site) should also be considered its own unit of work that brings together many other sites.

In the past, many organizations used subsites to create connective tissue for their intranets. They used the site collection's shared navigation to connect sites and the hierarchical structure of subsite relationships to nest sites within sites. However, subsites don't give any room for flexibility and change. Since subsites are a physical construct reflected in the URL for content, if you reorganize your business relationships, you break all the intranet relationships in your content. Subsites can also create challenges when it comes to governance because many features (including policy features like retention and classification) in SharePoint apply to all sites within the site collection, whether you want them to or not. This means that you must frequently enable a feature for the entire site collection, even if it's only applicable to one subsite.

What is the one thing that we can guarantee is going to happen in every business? Change! As your organization evolves, you need intranets that make it easy to align experiences with the way you work and that can adapt to the inevitable changes in the way you work. This is a key benefit provided by SharePoint hub sites; they model relationships as links, rather than hierarchy or ownership, so that you can adapt to the changes in the way you work in a dynamic, changing world.

Getting started

Before you start making hubs sites, let's recap the three things hub sites give you:

- Shared navigation and brand
- Roll-up of content and search
- A home destination for the hub

Now let's think about the information you're trying to share throughout your intranet, and consider the business outcomes you're trying to enable.

An intranet can play many roles in an organization. It's an internally facing site, a place to communicate important news, and a collaboration platform. It's also a way to showcase your corporate culture. It can be the foundation of your digital workplace. An intranet lets you tell stories and share information. Empowering employees with a voice on your intranet can provide a way to move to a culture of collaboration that enables your organization to transform and adapt to change.

Many successful intranets include the following elements:

- **Communication**: For example, a home page that includes news from around the organization to keep employees informed, overall navigation, links to key tools and

information, internal marketing promotions, and a place to engage employees around important topics.

- **Content**: A place for the functional parts of the organization, such as Human Resources (HR), Legal, and Information Technology (IT), to offer their services to the rest of the organization. For example, the HR part of the intranet could be where employees can find out how many vacation days they have left, whether their benefits program offers vision or dental coverage, or what training is available for individual roles. The Legal area might be where employees can find a sample non-disclosure agreement they can execute prior to having a conversation with a prospective vendor.

- **Actions and activities**: Links to the time-tracking system or the expense report form and a place where managers can approve expenses or timesheets.

- **Collaboration**: Places where teams can get work done and where role or topic-based communities can share knowledge and leverage expertise across the organization and with external partners in the extended enterprise.

- **Culture**: Stories and places that allow employees to engage or learn, including profiles, communities and clubs, and even images and branding that reflect the organizational structure. Sometimes even the intranet name embodies the culture. For example, an electric utility has an intranet called "The Grid" with messaging and promotions to make sure that "no one works off The Grid."

- **Mobility**: The ability for employees to get work done from any device while they're on the go.

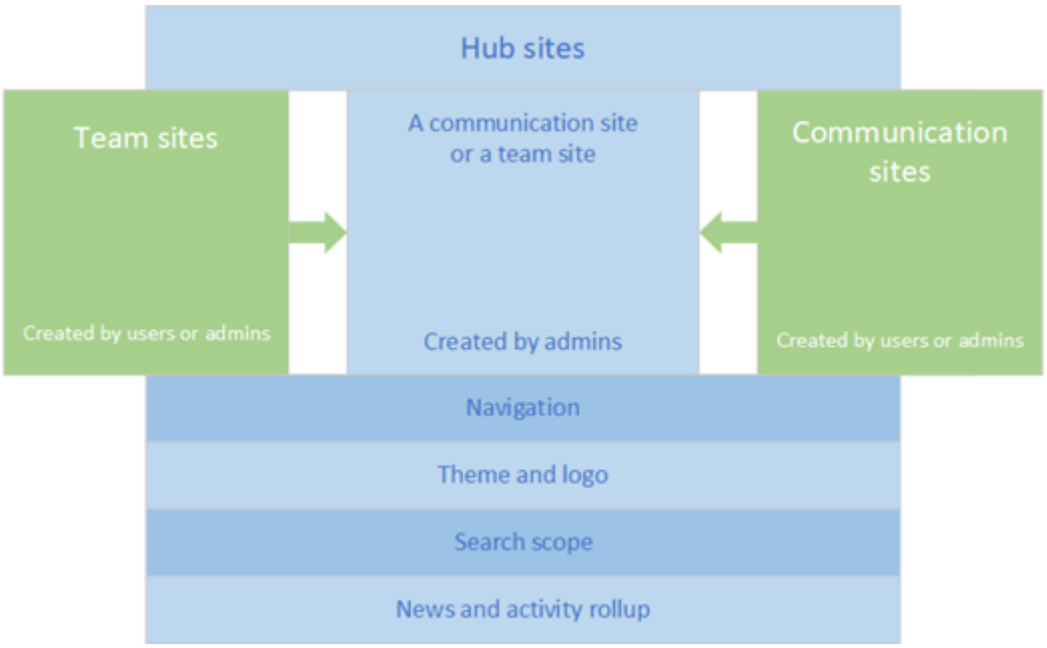
- **Search**: The ability for employees to find content even if they don't know where it lives.

The emphasis for each of these elements can vary based on organizational priorities and to some extent, the digital maturity of the organization. Microsoft 365 provides three main building blocks to help you create your intranet in a way that allows you to configure experiences that align with your organization, your employees, and your readiness. Different organizations will use the building blocks in different ways, but the building blocks themselves reflect common patterns that organizations use to get work done:

- Team sites (collaboration)

- Communication sites (communication)

- Hub sites (connection)



At their core, the three types of building blocks share a common structure. For example, they share the same set of internal web parts. However, there are some fundamental differences in intent, usage expectations, governance (including how they are created), and how and which web parts you might use on each type of site.

Expand table

	Team site	Communication site	Hub site
Primary business objective	**Collaborate** When you want to create a place where the members of a work group or project team can work together on project deliverables, plan an event, track status, or exchange ideas, you want a team site. Team sites are connected by default to a Microsoft 365 group to deliver a full range of communication and collaboration tools, including Microsoft Teams and Planner.	**Communicate** When you want to broadcast a message, tell a story, share content for viewing (but not editing), or showcase services or people, you want a communication site. Communication site owners often want to include an engagement component - for example an "Ask Business Development" area on a site communicating information about business development. This is a great place to connect a Viva Engage community.	**Connect** When you want to create a shared experience for a family of related sites—to discover related content by rolling up site activity and news, organize related sites so that they share a common navigation, and apply a common look and feel.
Content authors	**All members are content authors** who jointly create and edit content.	**Small number of content authors** and a much larger number of content readers or consumers.	**Hub site owner** defines the shared experiences for hub navigation and theme. **Hub site members** create content on the hub site as with

	Team site	Communication site	Hub site
			any other SharePoint site. Owners and members of the sites associated with the parent hub create content on individual sites.
Governance (as allowed for your organization based on the settings in the Security & Compliance center)	Norms typically **determined by the team**. Practices are aligned in the best way to get work done.	Policies often **determined by the organization** to ensure consistency of experience and effective management of organizational information.	Governance **determined by each owner of the associated site based on the type of site and organizational policies**. The best experience for visitors is achieved when everyone has at least read permissions for associated sites (but this is not required).
Permissions	Microsoft 365 group, plus SharePoint groups and permission levels	SharePoint group	Same as original site type. Hub sites do not alter an associated site's permissions - but you may add a "reader" group to the hub to make it easier to provide read access to associated sites. For more information, see: Hub permissions.
Created by	**Site owner** (unless this has been disabled in your organization) or **admin**.	**Site owner** (unless this has been disabled in your organization)	SharePoint site administrators and above in Microsoft 365
Examples	- Project team working together to complete deliverables and manage tasks. - Holiday party planning committee planning the annual get-together. - HR performance management team. - Executive committee—different leadership groups within the organization.	- Travel team publishing guidelines about corporate travel. - Policies and procedures. - Micro-site for a new corporate initiative. - Resources for the sales team for a product or service.	- HR hub that provides a connection and roll-up for all HR functions, such as benefits, compensation, performance management, talent acquisition, and a manager portal. - Sales hub providing enterprise resources for the Sales organization

	Team site	Communication site	Hub site
	- Extranet site to work with Partner A.		and connecting regional sales team and communication sites. - Location-specific hub that groups the communication and team sites for a specific location (for example, the New York office).

What should be a hub site?

Hub sites complement the search experience by helping you discover information in context.

One of the biggest challenges with intranet design is figuring out how the intranet navigation should be organized. In the new world where all team and communication sites are peer site collections, information architects must think about creating experiences that will allow intranet users to find what they need in multiple "find" scenarios:

- I know it exists, and I know where it is
- I know it exists, but I don't know where it is
- I don't know if it exists

These scenarios are enabled with a combination of navigation, search, and discovery (or serendipity) and should be a factor in how you design and organize your hub sites. One of the important capabilities that hub sites enable is the serendipitous discovery of information because they can surface contextually relevant content from sites you may not follow but are associated with the hub. The SharePoint start page was built to support discovery and search across the entire organization's content, but if you already have a particular context in mind, hub sites can be very helpful in narrowing those experiences down to a handful of related sites.

As a starting point in your hub planning, think about hub sites for key functions that your users need to get work done—for example: HR, Finance, Communications or Public Relations, Legal, and IT. These functions may be represented in different organizational departments or business units in large organizations or combined into the role of a few people in smaller organizations.

Let's take HR as an example. HR often encompasses the following sub-functions:

- Benefits

- Pay and compensation
- Talent acquisition or recruiting
- Performance management
- Professional development or training
- Manager portal

Using the guiding principle of creating a site for each unit of work, you can think about an HR family of sites that could include six functional sites for each of these functions plus an HR hub that connects the related sites to provide an overall HR experience. This is another way to think about the value of hub sites: they allow you to create an experience that improves information discovery for a specific context (in our example, for employees looking for HR information).

In the classic intranet model, you might have created an HR site and used subsites to support each HR function. In the flat world of modern SharePoint, the HR family is connected using the HR hub to provide the connective tissue for navigation within the family and to provide an opportunity to serendipitously discover content on a related member of the family when users navigate to the HR home. For example, if you're on the HR hub reading a news announcement about open enrollment because you're in the process of onboarding a new employee, you might be happy to know that a new version of the "Welcome to the Company" onboarding toolkit was just released on the Talent Acquisition site. Likewise, if you're trying to find the HR team's office sharing policy, you'll appreciate being able to limit your search to only the HR-affiliated sites, rather than the entire organization.

You don't have to have a hub site for every function. However, when a function provides multiple logically different services (as in the HR example), it's a good practice to create a hub site to provide a single starting place for your users. Often, intranet users start their exploration with browsing. Hub sites help combine the benefits of browsing ("I know this is an HR topic") with the benefits of a more narrowly scoped search ("I want to find information about vision benefits, not the company's strategic vision."). Even if the users don't know which sub-function provides a service, they can navigate to the HR hub and then, using the search scope provided by the hub, search (or navigate) within the HR hub to quickly find what they need.

Some organizational functions have an enterprise-wide scope but a regional or product execution. For example, think about a Sales department that may have sites for sales regions and sites for location-based offices. This type of function has always presented a challenge to hierarchical intranet content organization using subsites. Do we make the Southeast Sales site a subsite of the Southeast Region site or the Global Sales site? And, what happens when a state within the southeast region is allocated to a new region; for example, from the southeast region to the northeast region? This type of dynamic organizational movement creates a nightmare for intranet organization if you use subsites, but not with hub sites. Picking a hub may create some angst because an individual site can be associated with only one hub, but keep in mind that content from a site can appear on multiple hubs. You can customize sources for the following web parts on a hub:

- News
- Highlighted content
- Sites
- Events

> **Note**
>
> An organization can have up to 2,000 hub sites. You might not need a hub site for every function and it's important to do some planning before you create hubs.

There is no "one size fits all" way to determine how to align sites to a hub in this scenario. Always start by answering these questions:

- Who is your audience and what do they need to accomplish?
- How do the people who need the information get their work done?

Align your hub to create experiences that enable the user first. You may want to think about how people in each work group think about the work they do by aligning regional sites with the *function*, since sales content for the northeast is more likely to be organized similarly to sales content for the southeast than it will be for the southeast regional office. But this is very much an "it depends" situation. In some organizations, it will make much more sense to organize all functions around a regional hub than a functional hub. With hub sites multi-geo capabilities, you can create a better user experience associating Austria Sales with the Austria hub and not the global Sales hub. In this type of scenario, you can use a link on the Austria sales site to connect it to the global Sales hub and add each regional sales site to the Hub navigation for global sales.

> **Note**
>
> A site can only associate with a hub family. However, hub families can be connected to one another using links either on the page or in hub navigation. In addition, hubs can also be associated to other hubs to create an extended search scope for your hub families. For example, you may have a hub called Northeast Region Sales that you want to "connect" to a Global Sales hub. You can now **associate a hub to another hub** to expand search results across multiple hubs in your organization.

A good practice is to start with a consistent approach for all functions that have a pattern, such as Sales. If you align region-specific functions to the regional hub, do that for all functions. Either approach is valid, but from a usability perspective, it helps to be consistent.

How should I organize my hub site?

Hub sites provide two primary organizational experiences that you should think about as part of the hub planning process. Though creating a hub site must be done by SharePoint site administrators and [above] in Microsoft 365, planning, managing, and organizing the hub site is the responsibility of the hub site owner. The organizing concepts for hubs are:

- Association
- Navigation

Association

A site becomes part of a hub family by Associating a SharePoint site with a hub site. When creating a hub site, SharePoint Administrators can allow only certain site owners to associate sites with the hub.

After a SharePoint Administrator gives a site owner permission to associate their sites with a hub site, the site owner can then choose to associate the sites with the hub. When they do, the site inherits the hub site theme and shared navigation. Content from their site will roll up to the hub site in web parts where the source is "all sites in the hub," and the site will be included in the hub site search scope.

Associating with the hub does not automatically add the site to the hub navigation. Hub site owners determine which sites are included in the navigation. They can also configure the News, Sites, Events, and Highlighted content to roll up activity from all associated sites or only selected sites.

> **Note**
>
> Association with a hub does not change the permissions on a site. If you associate a site that has restricted access with a hub, only users who have access to the restricted site will see content rolled up on the hub. Information surfaced on the hub site is security trimmed: if you don't have access to the content, you won't see it. Something you may want to consider is adjusting permissions on the associated sites after you have assembled your hub family or adding a hub "read" permission group to the hub and adding that permission group to associated sites.

Navigation

The hub site owner determines which sites are reflected in the shared navigation and can also include links to other resources. This navigation appears at the top, below the suite bar. Most of the time, you will want to add associated sites to your hub navigation. That's one of the benefits of the experiences that you can enable with a hub. Your hub navigation can have up to three levels, which lets you organize your hub family in a way that helps users discover and find relevant content.

> **Note**
>
> The default navigation menu style for team sites hub navigation will be cascading.

However, you may not want to add every associated site to your navigation and you may want to consider adding sites that aren't associated to the navigation. Consider the following as you plan your hub navigation.

- **Do you want to add private or restricted access sites to the navigation?** Maybe. For example, HR may want to associate their private team site with the HR hub to make it more convenient for HR team members. But, the HR hub owner may not want to display a link to the HR team site in the shared navigation for the HR hub because this would make the private HR site more discoverable by everyone in the organization, who will get an access challenge when they click the link to the HR team site. If you add private sites to hub navigation, consider using audience targeting so that the link only appears for members of the private site. In another scenario, there may be a site that is "semi-private" that you want interested people to discover. For example, you might have a community that wants to restrict membership to people with a specific expertise, but also wants to discover experts across the organization. In this scenario, users might get an access denied/request access message, but the site owner is prepared and wants to grant access to interested people.

  > **Tip**
  >
  > If you add links to private sites in your hub navigation and don't plan to use audience targeting, consider adding (restricted) or (private) or (external) to the link name to help users understand that they may not have access to the navigation link.

- **Do you want to add sites that are not associated with the hub to the navigation?** Maybe. Since an individual site can only be associated with one hub, adding sites that aren't associated with your hub helps provide a way to connect your hub to related sites. For example, if you choose to associate functions within a region with a regional hub instead of the global function hub, you could add navigation links from the function hub to each of the region sites. For example, if you have a function hub for HR, you could add the regional HR sites (Northeast HR, Southeast HR, and so on) to the navigation of the HR hub to create a comprehensive HR experience. Note that when you do this, the news and activity in the regional HR sites will not show up on the HR hub (but they will show up on the regional hub). And, when you navigate from the HR hub to the regional HR site, you will be on a site that has the regional hub navigation and theme, not the HR navigation and theme. There is nothing inherently wrong or bad about this scenario, but you should be aware of the implications when you plan your hub navigation experiences

  > **Tip**
  >
  > Don't associate extranet sites with the hub if you don't want extranet users to see the shared navigation. Consider just adding the external sites to the hub navigation so that

internal users have quick access to relevant extranet sites.

Can I make just one hub site for my whole organization?

There is no requirement to have more than one hub for your organization, but you should think about what this means for information organization and discovery. An advantage to having just one hub is that every site in the intranet will share a consistent top navigation. However, since every site can also share consistent global navigation in the App Bar, you may want to consider taking advantage of more than one hub.

If you have only one hub, you'll miss the ability to easily surface related information in context and the ability to easily define a search scope for related content. For example, if you have a single enterprise hub, it will be harder to surface just HR-related news on the HR site. Even small organizations may find that restricting the context in which users find information is helpful in managing information overload. We now have the ability to create a hierarchy of hubs to create hub to hub associations. This allows you to create a network of hubs that roll-up to each other to create connections and additional search scopes. When hubs are associated with each other, content can be searched for and displayed on hubs up to three levels of association.

How many sites should I associate to a hub?

Though there is technically no limit to the number of sites you can associate to a hub, there are practical guidelines to consider so that you will get the optimal benefit of using hubs in your information architecture (IA).

As with most IA decisions, you should first focus on the outcomes you are trying to achieve by using hubs and then use that goal to help determine a practical number of sites to associate to a hub. A good place to start is to focus on the key benefits of using a hub to organize sites.

Expand table

Key Benefit/Outcome Goal	Practical Guidance
Share a common theme across all sites	In general, you would not establish a hub when the only outcome goal is to share a consistent theme for all sites. For more information about SharePoint site themes, see: SharePoint site theming - PowerShell cmdlets | Microsoft Learn.
Display links to all sites in the hub in site	**Technically no more than 500, practically and from a performance perspective, no more than 100.** There is a technical limit to the number of navigation nodes

Key Benefit/Outcome Goal	Practical Guidance
navigation	that you can have in a SharePoint site. However, unless you are using audience targeting to limit the number of sites that a given user sees, showing 500 navigation links would create a very challenging user experience to read. From a user experience and performance perspective, the recommended number of links is no more than 100. If you want to display all sites in your hub in your navigation, the recommended maximum number of sites per hub is 100.
Display a security trimmed, dynamic list of all sites in the hub without written code.	**No more than 99.** The sites web part can be set to filter for "all sites in the hub" up to a maximum of 99 sites.
Shared search scope for all sites in the hub.	**Approximately 2,000.** Technically, there is no hard limit to the number of sites you can associate to a hub from a search perspective. However, you could experience performance issues when you have large numbers of sites associated to a hub. Consider your outcome goal - do you really need a site for each "topic", or would a document library achieve your goals? You can have 2000 lists and libraries in a site collection and within each library, you can have up to 30 million files and folders. You may find that using multiple document libraries in a site may achieve your outcome goals if the primary purpose of your hub is to search across related files. If you need a site for each topic, you should consider the challenges of managing large number of site collections associated to a single hub and whether there may be an alternative approach to get the outcome goals you want.

Additional important considerations

- **Finding hubs if you have more than one**. Hubs are an important building block for your intranet. Here are some ways you can make your hub sites discoverable:
  - **Add hubs to global navigation**. Add your hubs to the global navigation for your tenant in the SharePoint app bar.
  - **Add key hubs to the SharePoint start page**. Pin your hub sites to the Featured links area of the SharePoint start page. Encourage all users to "follow" hub sites.
- **Reaching the right audience for news**. Hub sites help you bring news to the right people at the right time and in the right context. News doesn't flow down to associated sites, only up from the associated site to the hub. If you want the broadest reach for your news, publish it to the hub site. To make hub news more visible, you may want to have two news web parts on your home page: one for news published on the hub home and another that includes news rolled up from associated sites (all or only selected sites).

- **Hub naming conventions**. Think about naming conventions for hub sites to make them more discoverable. Some options include names such as HR Central, HR Hub, HR Portal. Try to choose a consistent naming convention for all hub sites.

- **Getting ready to hub**. Once you have planned your hubs, you can transform an existing site (preferably a communication site) to become a hub site or create a new communication site and make it a hub site. Then, you can add and configure the web parts and navigation on the hub site to emphasize the hub capabilities.

- **Subsites**. Hub sites solve many or most of the use cases for which you previously used subsites. We recommend using hub sites going forward to organize the sites in your intranet. However, subsites will continue to be supported as a classic feature, and we'll add the new team site template as a subsite option.

- **Should your home site be a hub?** It depends. Consider making your home site a hub if you have a unique set of sites that represent your "official" intranet where you want a distinct brand and search scope that you want to distinguish from other sites in the tenant. Consider leaving your home site as a "regular" site if you plan to have multiple hubs and you want your users to leverage the SharePoint app bar for global navigation. Every site in the intranet does not have to be connected to a hub if your home site is not a hub. Some sites may be part of a hub and have both local and hub navigation but other sites may only have local navigation. In this scenario, your intranet global navigation is provided by the app bar, not a hub.

Use hub sites when they align with your business outcomes and solve a need for your users.

Need more help?

If you have technical questions about this topic, you might find it helpful to post them on the SharePoint discussion forum. It's a great resource for finding others who have worked with similar issues or who have encountered the same situation.

Principal author: Susan Hanley, MVP

- LinkedIn: http://www.linkedin.com/in/susanhanley
- Website: www.susanhanley.com

Last updated on 06/25/2026

Create a hub site in SharePoint

If you have the permissions of a SharePoint Administrator or higher in Microsoft 365, you can transform any existing site into a hub site.

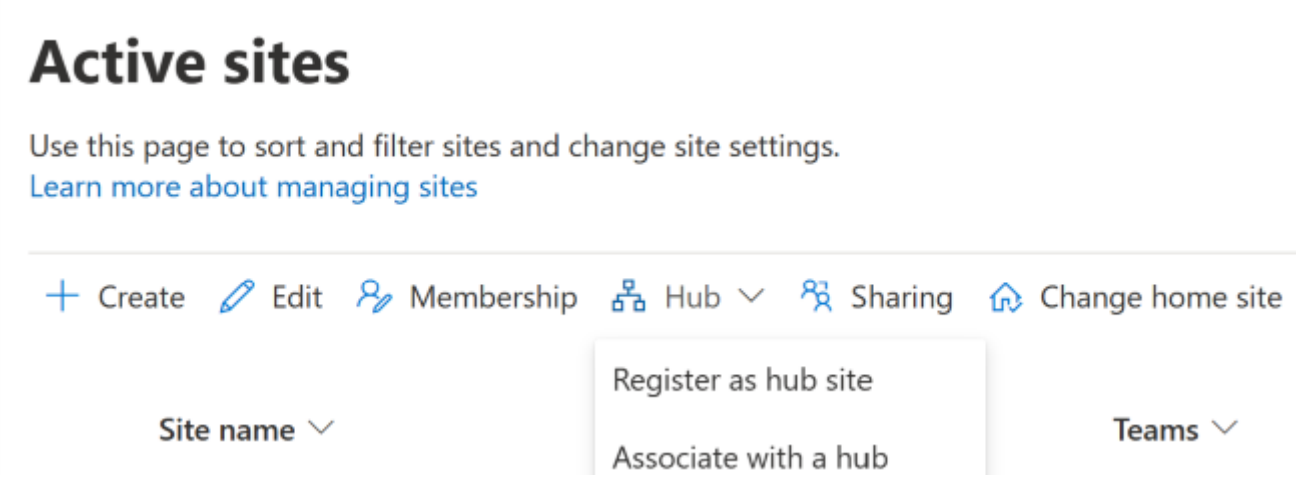
> **Note**
>
> We recommend selecting a communication site, or a team site that uses the new template. If you use a classic team site, the hub navigation appears only on modern pages, and hub site settings will only appear on modern pages.
> Sites that are already associated with another hub can't be converted to a hub site.
> You can create up to 2,000 hub sites for an organization. This applies to hub-to-hub associations as well. Any site labeled as a hub site counts against this limit. There's no limit on the number of sites that can be associated with a hub site.
> When users associate their sites with a hub, it doesn't impact the permissions of either the hub site or the associated sites. It's important to make sure all users you allow to associate sites to the hub have permission to the hub.

Create a hub site in the new SharePoint admin center

1. Go to **Active sites** in the SharePoint admin center, and sign in with an account that has admin permissions for your organization.

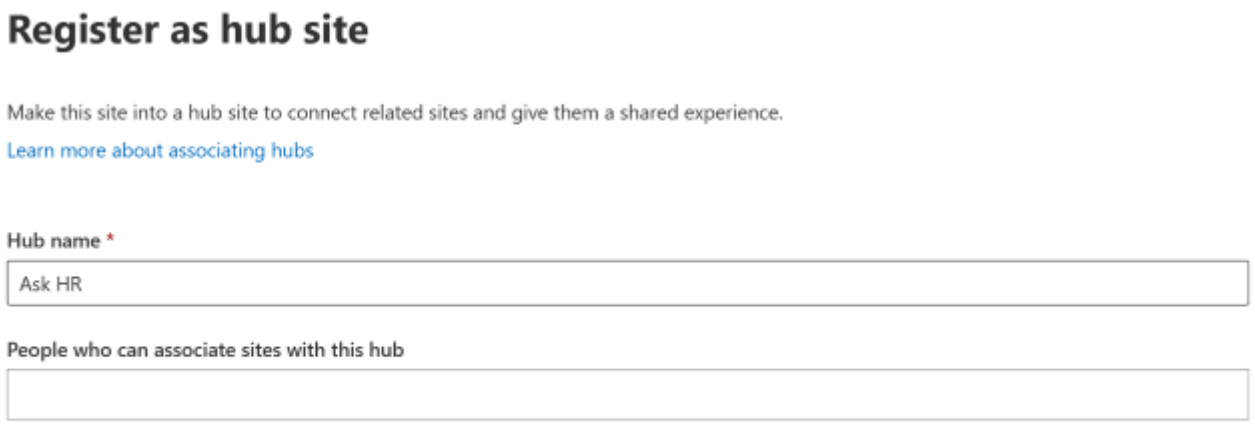
> **Note**
>
> If you have Office 365 operated by 21Vianet (China), sign in to the Microsoft 365 admin center, then browse to the SharePoint admin center and open the Active sites page.

2. Select the site, select **Hub** on the command bar, and then select **Register as hub site**.



> **Tip**
>
> Using the Hub site menu, you can also associate a site with the hub site, change a site's association to a different hub site, or disassociate a site from a hub site.

3. Enter a display name for the hub site, and specify the individual users or security groups you want to allow to associate sites with the hub.



> **Important**
>
> If you leave the **People who can associate sites with this hub** box empty, any user can associate their site with the hub.
> If you later want to change the hub site display name or the list of people who can associate sites with the hub, you need to use PowerShell or go to hub site settings on the hub site.

4. Select **Save**.

Related articles

- For info about using a site design that gets applied when sites join the hub, see Set up a site design for your hub site. For more info about site designs and site scripts, see SharePoint site design and site script overview.
- To learn how to use Microsoft PowerShell to create and manage hub sites, see Manage SharePoint hub sites.
- For info about how site owners can customize hub sites, see Set up your SharePoint hub site.
- For info about removing a hub site, see Remove a hub site.

Last updated on 06/24/2026

Unregister a site as a hub site

Article • 07/19/2024

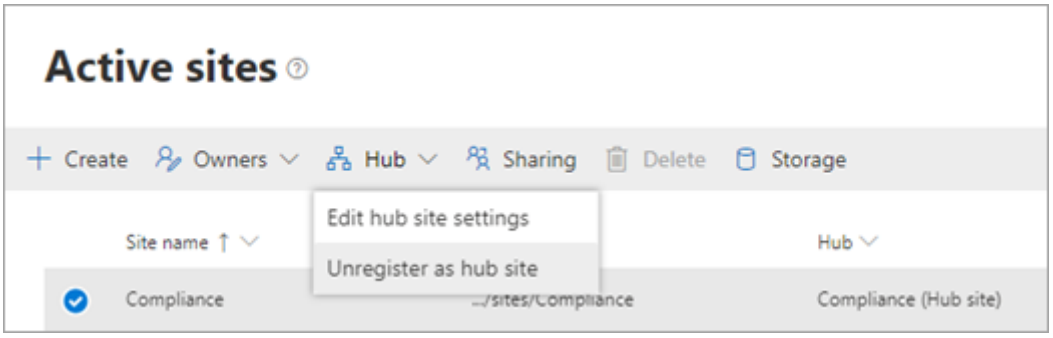
If you're a user who has SharePoint administrator or above permissions in Microsoft 365, you can make a hub site no longer a hub site (unregister it as a hub site). Make sure you do this before you delete the hub site. When you unregister a hub site, the associated sites won't automatically disassociate from the hub site. Disassociating a site removes the hub site navigation bar from the top of the site. The look that the site inherited from the hub site stays the same and features such as additional navigation links, applications, or custom lists with specific columns that were added as part of the inherited hub site design will remain. Any hub-site-related web parts added to the home page will only show information from the site instead of from sites associated with the hub.

Unregister a hub site in the new SharePoint admin center

1. Go to **Active sites** in the SharePoint admin center, and sign in with an account that has admin permissions for your organization.

   > **Note**
   >
   > If you have Office 365 operated by 21Vianet (China), sign in to the Microsoft 365 admin center, then browse to the SharePoint admin center and open the Active sites page.

2. Select the site, select **Hub** on the command bar, and then select **Unregister as hub site**.



3. Select **OK**.

Related articles

To learn how to use Microsoft PowerShell to manage and delete hub sites, see Manage SharePoint hub sites.

Feedback

Was this page helpful? Yes No

Provide product feedback

Set up a site template for your hub site

A site template is one or more site scripts that Microsoft SharePoint runs when a site is associated with a hub site. Actions describe changes to apply to the new site, such as creating a new list or adding nodes to the site navigation. Site templates provide reusable lists and custom actions so your users can quickly get started with the features they need.

> **Note**
>
> For organizations using Multi-Geo Capabilities in Microsoft 365, hub site templates work only when sites are in the same geo location as the hub site.

> **Note**
>
> These instructions require a SharePoint Administrator or above in Microsoft 365.

1. Create a JSON script, add it, and create the site template

Follow the steps in Get started creating site templates and site scripts. For the full list of supported actions, see Site template JSON schema. Note that when you create the site template, the site template you provide ("64" for team site or "68" for communication site) doesn't matter.

2. Scope access to the hub site template

When a site template is first created, it is available to everyone. You can grant View rights to the site template. After rights are granted, only the users or groups (principals) specified have access. We recommend granting access to the same principal used to scope the hub site.

PowerShell

```
Grant-SPOSiteDesignRights
  -Identity <ID>
  -Principals ("HR@contoso.sharepoint.com")
  -Rights View
```

Replace <ID> with the site design ID from when you added the site script.

3. Set your site template for the hub site

You can set the hub site template in two ways. You can do it using the following PowerShell command:

PowerShell

```
Set-SPOHubSite https://contoso.sharepoint.com/sites/Marketing
-Title "Marketing Hub"
-LogoUrl https://contoso.sharepoint.com/sites/Marketing/SiteAssets/hublogo.png
-Description "Hub for the Marketing division"
-SiteDesignId "<ID>"
```

Replace <ID> with the site script ID from when you added the site script.

You can also let hub site owners set the hub site template by using a new option available in the UI. For info about the hub site settings available to site owners, see Set up your SharePoint hub site.

Last updated on 06/25/2026

Control settings for Microsoft Lists

Article • 04/22/2025

As at least a SharePoint Administrator in Microsoft 365, you can control settings for Microsoft Lists. You can:

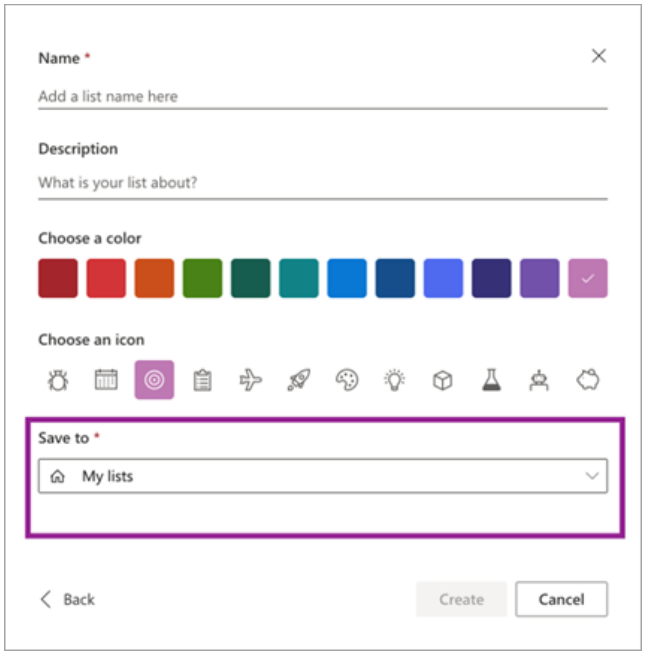
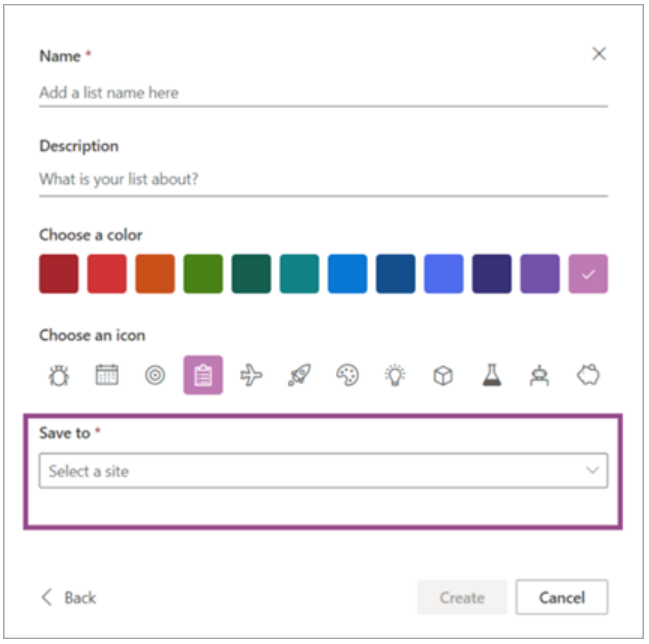
- Disable the creation of personal lists (prevent users from saving new lists to "My lists").
- Disable built-in list templates that aren't relevant for your organization.

You control both of these settings by using Microsoft PowerShell.

Disable creation of personal lists

If you change this setting, when users create a list, they must select a SharePoint site for saving the list. The "Save to" setting doesn't include the "My lists" option.

Expand table

Default	Personal list creation disabled
	

1. Download the latest SharePoint Online Management Shell.

> **Note**
>
> If you installed a previous version of the SharePoint Online Management Shell, go to Add or remove programs and uninstall "SharePoint Online Management Shell."

2. Connect to SharePoint as at least a SharePoint Administrator in Microsoft 365. To learn how, see Getting started with SharePoint Online Management Shell.

3. Run the following command:

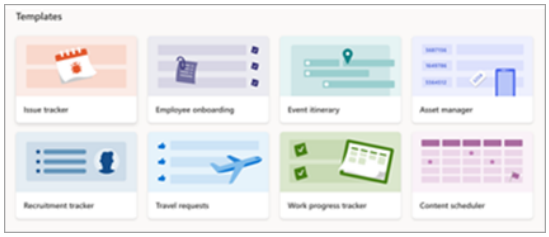
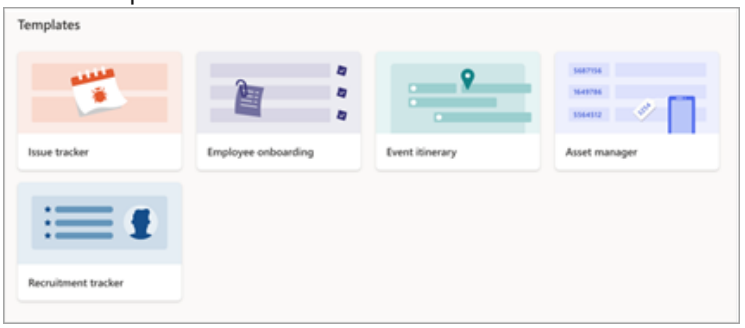
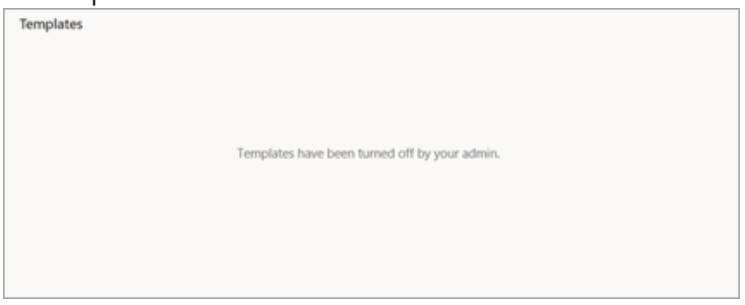
```
PowerShell

Set-SPOTenant -DisablePersonalListCreation $true
```

To re-enable the creation of personal lists, set the parameter to `$false`.

Disable built-in list templates

Disabling these templates removes them from all places users create lists (the Lists app, Microsoft Teams, and SharePoint sites).

Expand table

Default	Built-in list templates disabled
	Some templates disabled  All templates disabled 

1. Download the latest SharePoint Online Management Shell.

> **Note**
>
> If you installed a previous version of the SharePoint Online Management Shell, go to Add or remove programs and uninstall "SharePoint Online Management Shell."

2. Connect to SharePoint as at least a SharePoint Administrator in Microsoft 365. To learn how, see Getting started with SharePoint Online Management Shell.

3. Run the following command:

```
PowerShell
Set-SPOTenant -DisableModernListTemplateIds '<template ID>'
```

Where the template ID is:

- Issue tracker: 'C147E310-FFB3-0CDF-B9A3-F427EE0FF1CE'
- Employee onboarding: 'D4C4DAA7-1A90-00C6-8D20-242ACB0FF1CE'
- Event itinerary: '3465A758-99E6-048B-AB94-7E24CA0FF1CE'
- Asset manager: 'D2EDA86E-6F3C-0700-BE3B-A408F10FF1CE'
- Recruitment tracker: '3A7C53BE-A128-0FF9-9F97-7B6F700FF1CE'
- Travel requests: 'C51CF376-87CF-0E8F-97FF-546BC60FF1CE'
- Work progress tracker: 'B117A022-9F8B-002D-BDA8-FA266F0FF1CE'
- Content scheduler: '9A429811-2AB5-07BC-B5A0-2DE9590FF1CE'
- Incidents: 'E3BEEF0B-B3B5-0698-ABB2-6A8E910FF1CE'
- Patient care coordination: '0134C13D-E537-065B-97D1-6BC46D0FF1CE'
- Loans: '7C920B56-2D7A-02DA-94B2-57B46E0FF1CE'
- Gift ideas: '008F8143-9644-0238-B4B5-C03E4F0FF1CE'
- Recipe tracker: 'A1755E7D-8E3A-4141-89FC-6C77EB0FF1CE'
- Expense tracker: '96D6DBE5-D7C3-030A-867A-0B72EB0FF1CE'
- Travel requests with approvals: '4EB20749-6360-417C-83DD-06135C0FF1CE'
- Content scheduler with approvals: 'C381BD64-C1A1-4D9E-BE9C-0571900FF1CE'
- Playlist: '3A867B4A-7429-0E1A-B02E-BF4B240FF1CE'
- Resume repository: 'F6AEF3EE-EC97-433C-A662-E9170B0FF1CE'

To re-enable a built-in template, use the parameter `EnableModernListTemplateIds`.

Disable extra features on a built-in template

Some built-in list templates include extra features such as automations and custom formatting. If you wish to keep only the base schema of a built-in list template but not the rest of its features included in that template:

1. Create a list from the built-in list template.

2. Create a custom list template based off of that list. The custom list template doesn't include any extra features by default.

3. Disable the original built-in list template.

> **Note**
>
> Users in your organization see the custom list template on the **From your organization** tab rather than on the **From Microsoft** tab.

Creating custom list templates

As a SharePoint Administrator and above in Microsoft 365, you can provide custom list templates for users in your organization. When users create new lists, they can select from these templates alongside the built-in templates from Microsoft. This feature enables your organization to create repeatable list solutions (in SharePoint, Teams, and within the Lists app itself).

You can create and manage custom list templates using Microsoft PowerShell:

1. Download the latest SharePoint Online Management Shell.

   > **Note**
   >
   > If you installed a previous version of the SharePoint Online Management Shell, go to Add or remove programs and uninstall "SharePoint Online Management Shell."

2. Connect to SharePoint as a Global Administrator or SharePoint Administrator in Microsoft 365. To learn how, see Getting started with SharePoint Online Management Shell.

Add a custom template

Follow these steps to create a custom list template.

1. Run the following command to extract the site script output from an existing list and write it to a variable:

   PowerShell

   ```
   $extracted = Get-SPOSiteScriptFromList -ListUrl
   "https://contoso.sharepoint.com/sites/strategy/customer-contacts"
   ```

2. Reference the variable in the following command to upload a site script that can be used with a list design.

   PowerShell

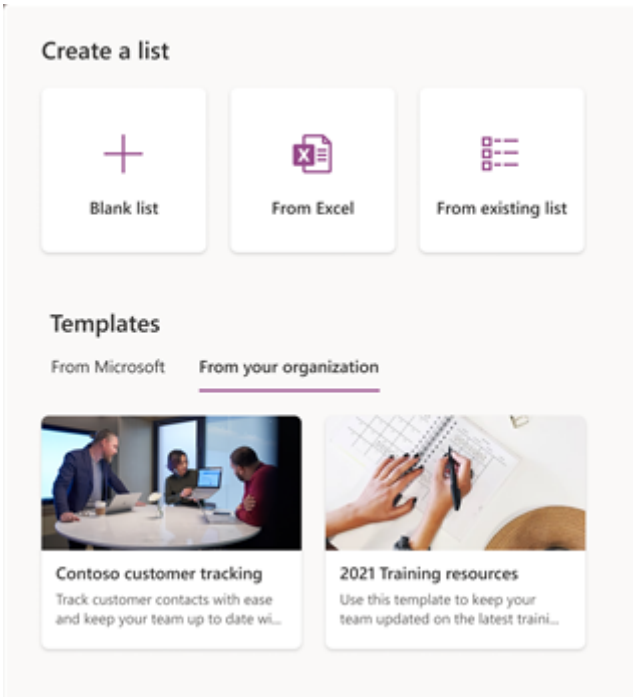
   ```
   Add-SPOSiteScript
     -Title "Contoso Customer Tracker"
     -Description "This creates a customer contact list"
     -Content $extracted
   ```

3. Create your list design using the site script ID returned from the step above:

PowerShell

```
Add-SPOListDesign
  -Title "Contoso customer tracking"
  -Description "Tracks key customer data in a list"
  -SiteScripts "<ID from previous step>"
  -ListColor Orange
  -ListIcon BullseyeTarget
  -Thumbnail "https://contoso.sharepoint.com/SiteAssets/site-thumbnail.png"
```

When users in your organization create a list (in SharePoint, Teams, or the Lists app), they see the template on the "From your organization" tab.



> ⓘ **Note**
>
> List templates can't be updated after you add them. Instead, remove the existing template and add the updated version.

Scope the permissions to a custom template

By default, the custom list template is available to everyone in your organization. If you want, you can limit access to specific users or a security group. The following example shows how to grant an individual user view rights to a template.

PowerShell

```
Grant-SPOSiteDesignRights
  -Identity <List design ID to apply rights to>
  -Principals "nestorw@contoso.onmicrosoft.com"
  -Rights View
```

Get templates

The following example retrieves all custom list templates.

PowerShell

```
Get-SPOListDesign <List design ID>
```

Remove a custom template

The following example shows how to remove a custom list template so that it's no longer available to users when they create lists.

PowerShell

```
Remove-SPOListDesign <List design ID>
```

You can also remove the associated site scripts that the list design is referencing using:

PowerShell

```
Remove-SPOSiteScript <Site script ID>
```

Last updated on 06/25/2026

Package biz apps into organizational list templates

There are a number of steps by which you can create a packaged SharePoint list template that contains in-built custom flows. The objective is to assemble and register a packaged file that contains the site script actions needed to create the list and the flows, and a Dataverse solution archive (zip) that contains the flow definitions.

Once you have your source SharePoint list set up and are ready to work on integrating flows with it, and on assembling a template with these components, perform the following the steps:

Obtaining solution zip file

1. Sign in to Power Automate portal by launching https://flow.microsoft.com/ (or choose **Integrate** > **Power Automate** > **See your flows**" in the SharePoint Portal).

2. Create a new Dataverse solution by referring to Overview of solution-aware flows.

   For an introduction to Dataverse solutions, see Solution concepts.

3. Add a new flow or customize existing flows to this solution by referring to Create a cloud flow in a solution.

4. Ensure that your flows use connection references for each trigger and action that you use. For more information on how to use a connection reference, see Use a connection reference in a solution.

5. Once you're satisfied with the contents of your solution (including any connection references or environment variables you wish to set up), export and download it to a disk.

6. Extract all files from the zip file into a separate folder.

7. Browse into the folder's **Workflows** subfolder.

8. Open each flow-related .json file and then search and replace all instances of the following elements:
   a. **The URL of the SharePoint site that the original list resided in**: Replace with **{ContextSharePointSiteUrl}**.
   b. **The ID of the original SharePoint list**: Replace with **{ContextSharePointListId}**.

For example:

[Before replacements]

```
PowerShell
"parameters": {
   "dataset": "https://microsoft.sharepoint-df.com/teams/AlinTest ",
   "table": "d6ac2804-7a1c-4cd4-98c8-56b85a9294b7"
            }
```

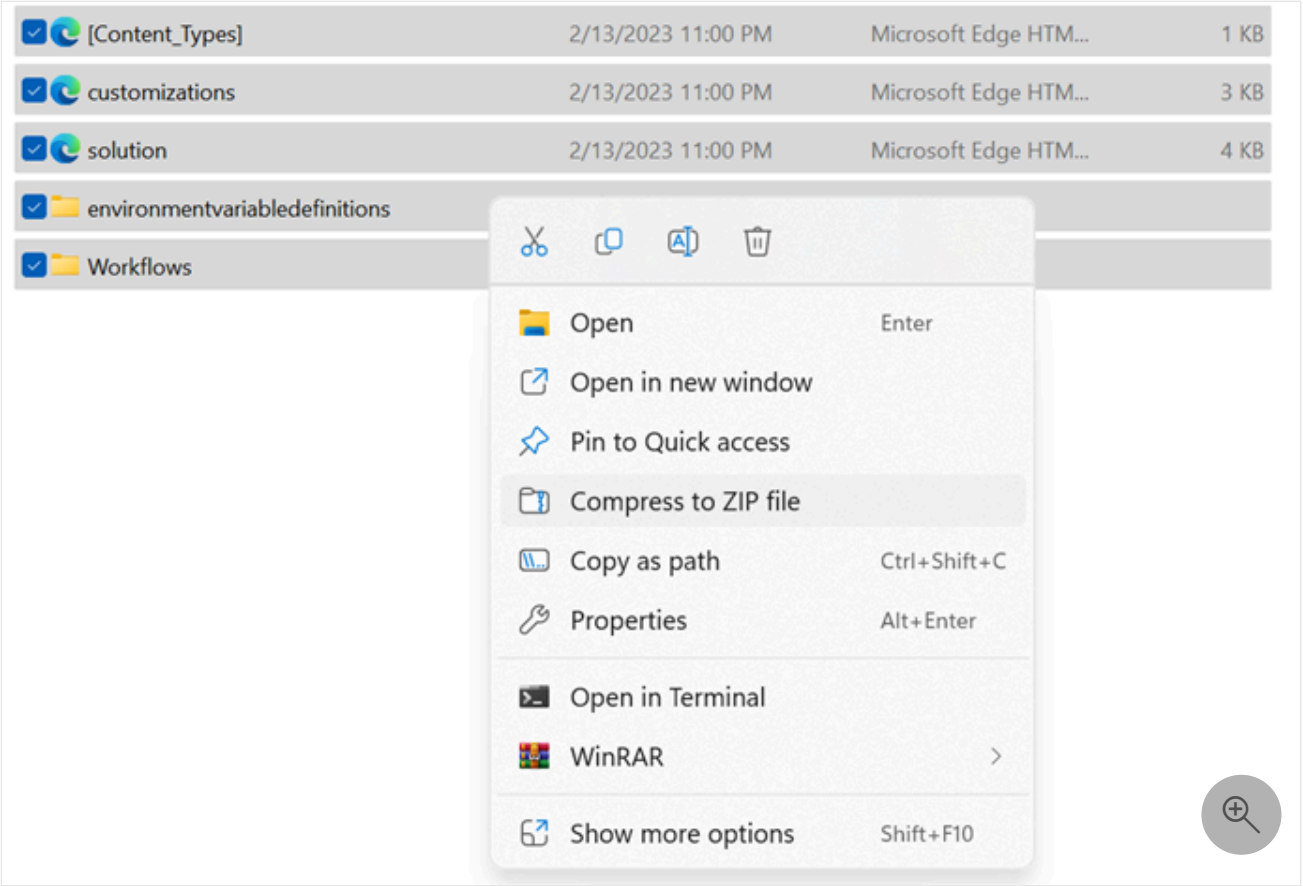
For example:

[After replacements]

```
PowerShell
"parameters": {
   "dataset": "{ContextSharePointSiteUrl}",
   "table": "{ContextSharePointListId}"
            }
```

9. Save the changes and close all file editors that you've opened for these files.

10. Go back to the root folder of the solution; select all files (solution.xml, customizations.xml, and so on) and folders; right-click and choose **Compress to ZIP file** from the context menu.



You can keep this resulting zip file, and you can also choose to discard the original solution zip file that earlier downloaded (as specified in Step 6 of this procedure).

Obtaining the site script action file (manifest.json)

> **Important**
>
> Prior to performing the steps in this section, ensure that you've tested your prototype list and flows to your satisfaction.

1. Ensure you've installed SharePoint Online Management Shell on your computer.

2. Launch SharePoint Online Management Shell.

3. Run the following command to connect to the tenant's admin service:

```
[Connect-SPOService](/powershell/module/sharepoint-online/connect-sposervice) -Url <Link to SPO admin portal> -Credential <full username of the admin user>
```

4. Run the following command to extract a site script file from the target list:

```
[Get-SPOSiteScriptFromList](/powershell/module/sharepoint-online/get-spositescriptfromlist) -ListUrl <full URL of the target list> | Out-File manifest.json
```

5. Open the *manifest.json* file in your favorite text (or code) editor and manually add an action with the verb "importBusinessApps," the relative path of your solution file inside the overall template package and the target listName (in this case, the title of the listName binding). This value should be the same as the *listName* property of the "CreateSPList" action.

   For example:

```
1   {
2     "$schema": "https://developer.microsoft.com/json-schemas/sp/site-design-script-actions.schema.json",
3     "actions": [
4       {
5         "verb": "createSPList",
6         "listName": "[[AdventureWorksTemplates_listName]]",
7         "identity": "AdventureWorksTemplates",
8         "templateType": 100,
9         "color": "5",
10        "icon": "7",
11 >      "subactions": [ ···
55        ]
56      },
57      {
58        "verb": "importBusinessApps",
59        "listName": "[[AdventureWorksTemplates_listName]]",
60        "solutionFileRelativePath": "solution.zip"
61      }
62    ],
63    "bindings": {
64      "AdventureWorksTemplates_listName": {
65        "source": "Input",
66        "defaultValue": "Cake Counter"
67      }
68    }
69  }
70
```

Assembling the final SharePoint package zip file

1. Ensure that the solution zip file and the *manifest.json* file (from previous step) are in the same folder location.
2. Select these two files; right-click and then select **Compress to ZIP file** (or **Send to** > **ZIP file**, depending on the OS).

Registering the new template as a list design

1. To upload the zip file (created in Assembling the final SharePoint package zip file) as a site script package, run the following command in the same management shell window:

```
$pkg = Add-SPOSiteScriptPackage -Title "<script title>" -Description "<script description>" -ContentPath '<relative path to zip file from previous step>'
```

> **Note**
>
> Inclusion of the *Description* property in the command is optional.

2. Take a peek at the new package by printing out its properties through the following command:

   `"$pkg"`

   The output should contain an *Id* property which is needed in the following steps.

   > **Note**
   >
   > (Optional) Run `Get-SPOListDesign` to ensure you're not adding a duplicate with the same title/description, or to inspect what's already there.

3. Run the following command:

   `Add-SPOListDesign -Title "<list design title>" -Description "<list design description>" -SiteScripts $pkg.Id`

   If the list design was successfully created, you should be able to view it in the **From your organization**" area of the **Create List** dialog.

Last updated on 06/25/2026

Use Group Policy to control Lists sync settings

This article describes the Group Policy objects (GPOs) for Microsoft Lists (and SharePoint lists) that administrators can configure by using Group Policy. Use the registry key information to confirm that a setting is enabled. Lists sync policies are listed under OneDrive because Lists sync gets packaged, installed, and updated through the OneDrive sync app's existing update mechanism. For information about controlling OneDrive sync settings by Group Policy, see OneDrive policies.

> **Note**
>
> To preserve Lists performance acceleration when the Chromium-based browser restrictions on local network access take effect, deploy the browser policy `LocalNetworkAccessAllowedForUrls` now.
> Add your tenant's SharePoint Online and OneDrive endpoints (for example:
>
> - `https://YOURTENANT-my.sharepoint.com`
> - `https://YOURTENANT.sharepoint.com`
>
> Policy reference (Edge): https://learn.microsoft.com/deployedge/microsoft-edge-browser-policies/localnetworkaccessallowedforurls
>
> Policy reference (Chrome): https://chromeenterprise.google/policies/#LocalNetworkAccessAllowedForUrls

List of policies by string ID

- (DisableListSync) Prevent Lists sync from running on this device
- (BlockExternalListSync) Prevent users from syncing lists shared from other organizations
- (DisableNucleusSilentConfig) Prevent users from getting silently signed in to offline experiences on the web

Prevent Lists sync from running on this device

By default, Lists sync is turned on for users of Microsoft Lists, which allows users to access and edit their lists even when offline. If you enable this policy, Lists sync will be blocked from running on the device.

Prevent Lists sync from running on the device:

```
[HKLM\SOFTWARE\Policies\Microsoft\OneDrive] "DisableNucleusSync" = "dword:1"
```

Re-enable Lists sync on the device:

```
[HKLM\SOFTWARE\Policies\Microsoft\OneDrive] "DisableNucleusSync" = "dword:0"
```

> **Note**
>
> This policy's registry value name `DisableNucleusSync` differs from the policy name `DisableListSync`. When verifying this policy is applied, look for `DisableNucleusSync` in the registry.

Prevent users from syncing lists shared from other organizations

Enabling this setting prevents users at your organization from syncing lists that are shared from other organizations. After the setting is enabled (by entering value **1**) on a computer, lists shared from other organizations won't sync. Disable the setting (by entering value **0**) to allow your users to sync external lists.

Prevent external List sync with:

```
[HKLM\SOFTWARE\Policies\Microsoft\OneDrive] "BlockExternalListSync" = "dword:1"
```

Restore external List sync with:

```
[HKLM\SOFTWARE\Policies\Microsoft\OneDrive] "BlockExternalListSync" = "dword:0"
```

Prevent users from getting silently signed in to offline experiences on the web

Offline experiences in Microsoft Lists and OneDrive on the web are set up to automatically sign in users with their Microsoft Entra account credentials. If you enable this setting, people who used offline experiences in Microsoft Lists and OneDrive on the web previously and who are signed in on a Microsoft Entra-joined PC will no longer be able to set up offline experiences without entering their account credentials.

> **Important**
>
> If the M365 browser extension isn't installed on users' Chromium-based browsers (Microsoft Edge, Google Chrome, and so on), we recommend leaving silent account

configuration enabled to ensure the seamless operation of List sync.

Enabling this policy sets the following registry key value to 1:

```
[HKLM\SOFTWARE\Policies\Microsoft\OneDrive] "DisableNucleusSilentConfig" =
"dword:00000001"
```

For more information about this feature, including troubleshooting steps, see Silently configure user accounts.

Control Lists sync on unmanaged devices and based on location

You can use the following settings to control access to Lists sync from unmanaged devices and configure network location-based access to List sync.

Control access from unmanaged devices

Control access to SharePoint and OneDrive based on network location

---

Last updated on 03/27/2026

Use macOS preferences to control Lists sync settings

Article • 03/03/2023

This article describes macOS preferences for Microsoft Lists (and SharePoint lists). For info about controlling OneDrive sync settings on macOS, see Deploy and configure OneDrive on macOS.

Manage Lists sync settings on macOS using property list files

Lists sync gets packaged, installed, and updated through the OneDrive sync standalone (non-App Store) app's existing update mechanism. As a result, some Lists sync preferences are listed under the OneDrive group domain. After the OneDrive sync app for Mac is installed, users can configure settings for Lists sync. As an administrator, you might want to provide users in your organization with a standard set of preferences. Preferences for the Lists sync app for Mac are stored in property list `.plist` files.

Expand table

	Lists sync preferences	OneDrive group preferences
.plist location	~/Library/Preferences/com.microsoft.SharePoint-mac.plist	~/Library/Group Containers/UBF8T346G9.OneDriveStandaloneSuite/Library/Preferences/UBF8T346G9.OneDriveStandalo

List of policies by string ID

- `DisableNucleusSync` - Prevent Lists sync from running on the device
- `BlockExternalListSync` - Prevent users from syncing lists shared from other organizations
- `DisableNucleusSilentConfig` - Prevent users from getting silently signed in to Lists sync with existing Microsoft account credentials being used across Microsoft apps on macOS

Prevent Lists sync from running on the device

By default, Lists sync is turned on for users of Microsoft Lists. If you set this preference, Lists sync will be blocked from running on the device.

Location: Lists Sync preferences

Prevent Lists sync from running on the device:

```XML
<key>DisableNucleusSync</key>
<integer>1</integer>
```

Re-enable Lists sync on the device:

```XML
<key>DisableNucleusSync</key>
<integer>0</integer>
```

Prevent users from syncing lists shared from other organizations

Enabling this setting prevents users at your organization from syncing lists that are shared from other organizations. After the setting is enabled (value 1) on a computer, lists shared from other organizations won't sync. Disable the setting (value 0) to allow your users to sync external lists.

Location: Lists Sync preferences

Prevent external List sync with:

```XML
```

```
<key>BlockExternalListSync</key>
<integer>1</integer>
```

Restore external List sync with:

```XML
<key>BlockExternalListSync</key>
<integer>0</integer>
```

Prevent users from getting silently signed in to Lists sync with existing Microsoft account credentials being used across Microsoft apps on macOS

Lists sync is set up to automatically sign users in with credentials being used across other Microsoft apps on macOS like OneDrive. If you enable this setting, automatic sign-in and Lists sync setup wouldn't occur.

Location: OneDrive group preferences

Prevent Lists sync silent configuration:

```XML
<key>DisableNucleusSilentConfig</key>
<integer>1</integer>
```

Restore Lists sync silent configuration with:

```XML
<key>DisableNucleusSilentConfig</key>
<integer>0</integer>
```

Feedback

Was this page helpful? Yes No

Provide product feedback

Add a sample site to your organization

Discover the modern experiences you can build with Microsoft SharePoint.

Use the SharePoint Look Book adoption page to find inspiring samples of communication sites and team sites that look great on the web and on mobile devices. Then, add one or more sample sites to your organization. You can customize the sample to use for your own site or use the site for learning or showing to your colleagues. You can add a sample site by first browsing and selecting templates then applying the custom PnP site templates.

https://learn-video.azurefd.net/vod/player?id=c91087f4-d17d-4f5e-87fe-ff199e2e32fc&locale=en-us&embedUrl=%2FSharePoint%2Fadd-sample-site

What's included in a sample? You get:

- A modern communication or team site, depending on the sample you choose
- A site home page with sample branding, web parts, content, and images
- Sample news posts and pages
- Sample navigation

Get started

Select a sample you like

Browse the samples in the online SharePoint Look Book adoption page.

Or, navigate to the custom PnP site templates and select the template you need.

Provision a template

Follow steps described in Provisioning a template to provision a template.

To use this service, you need to be signed in as a SharePoint Administrator in Microsoft 365.

Additional resources

Create a communication site

Create a team site

Using web parts

Create and use modern pages

Last updated on 06/24/2026

Overview of the Microsoft New Employee Onboarding sites

There are three (3) templates for New Employee Onboarding (NEO) to help organizations improve their onboarding process. The NEO sites are designed to deliver a flexible and consistent experience. The NEO sites can be used on their own, or together.

The NEO sites help organizations by:

- Providing new employees a place to get started
- Connecting new employees to people and culture
- Helping stakeholders easily contribute to new employee onboarding
- Generating data and usage reports that help measure NEO content effectiveness

Why invest in new employee onboarding sites?

New employee onboarding (NEO) should be a strategic process that integrates new employees into an organization and its culture while providing the knowledge and tools needed to become fully contributing team members. NEO processes often fall short for both the new hires and the organization. Only 12% of employees strongly agree their organization does a great job of onboarding new employees. An engaging and well-organized NEO process can make all the difference in helping a new hire navigate through an exciting – but stressful - career journey, and it can have major organizational benefits.

A strategically planned NEO experience can:

Improve new hire performance and time to productivity - Organizations with a standard onboarding process report 50% greater new-hire productivity.*

Improve new employee retention - Based on our research, 69% of employees are more likely to stay with a company for three years if they had a great onboarding experience. Employees who have a negative onboarding experience are twice as likely to look for new opportunities.**

The NEO experience process

Expand table

Provide new employees a place to get started	Connect new employees to people and culture	Help stakeholders easily contribute to new employee onboarding	Measure effectiveness of new employee onboarding
Sense of place	Preonboarding	Departmental and team onboarding	Value realization
Onboarding journey	Social connections and live events	Easy to create and maintain compelling content experiences	Example model for KPIs

NEO site template features

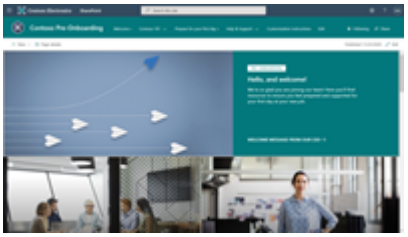
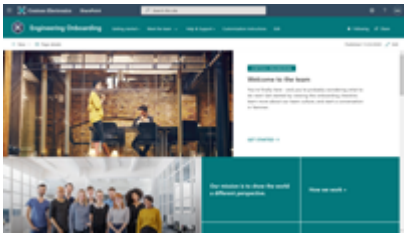
- **A fully configured and customizable set of new hire sites built on SharePoint communication sites:** NEO sites include: the site, information architecture, design, and prepopulated content and web parts. There are three NEO sites available that must be provisioned separately and can be customized or added to your organization's new hire content.
- **Onboarding journey:** Onboarding can be an overwhelming experience for new hires with everything the new hire is typically expected to do and learn in a short period of time. Avoid overwhelming your new employees by providing them with a curated onboarding journey that paces the new hire through a configurable activity list of administrative, technology, culture, training, and connection-related to-do's. The onboarding journey comes with a preconfigured list of new employee onboarding activities for you to customize for your processes.
- **Sample site pages:** To inspire and provide design templates for arranging your content, the NEO site includes sample inner site pages. Use these site pages as templates for your content.
- **Easy provisioning:** Provision NEO sites from the SharePoint look book with just a few steps.
- **Mobile ready:** NEO sites can be easily accessed on a mobile device when you get the SharePoint mobile app.

NEO site template options

New employee onboarding involves multiple levels within an organization, including preonboarding, corporate onboarding, and departmental onboarding. Each onboarding level provides its own unique value, contributing to a comprehensive onboarding experience each new employee should experience.

Research has shown preonboarding new hires, after they sign their acceptance letter but before they officially join the company, can lead to higher performance and better retention rates. To deliver a flexible and consistent onboarding experience, NEO sites consist of three different SharePoint site templates that are designed to work alone or as one cohesive and familiar experience for new hires.

Expand table

Preonboarding site	Corporate onboarding site	Departmental onboarding site
		
Share the Preonboarding site with new hires as soon as the job offer has been accepted	Share the Corporate onboarding site with new hires on their first day	Managers and onboarding buddies should share their respective Departmental onboarding site

1. **New employee pre-onboarding site:** A site for new hires, who have yet to officially join the company, to learn more about the company they have joined and to get ready for their official start date. External guest access can be used for providing prestart hires, with no corporate credentials, access to the Preonboarding site only.

2. **New employee corporate onboarding site:** A place for new hires to visit to get the information and connections they need to successfully onboard to the organization.

3. **New employee departmental onboarding site:** A place for new hires to visit to learn more about the department they're joining, its people, culture, and priorities. The Departmental onboarding site can be associated to an existing departmental hub.

> **Note**
>
> To deliver a flexible and consistent new hire onboarding experience the NEO sites consists of **three different SharePoint site templates**, that are designed to work alone or as one cohesive and familiar experience for new hires. Sites must be provisioned individually, and then can be configured to create a hub or add a site to an existing hub.
>
> You must have site collection administrator permissions or higher to provision the New Employee Onboarding sites.

Step 1: Provision NEO sites

The New Employee Onboarding (NEO) sites can be provisioned from the custom PnP site templates and selecting the template you need. A **site collection administrator** can start the provisioning process with a few steps. Each site takes about 20 minutes to provision. Before starting the provisioning process, make sure you have met the prerequisites for provisioning.

Prerequisites

To successfully provision the NEO sites via the SharePoint look book, the person doing the provisioning must be a site collection admin of the tenant where the NEO sites will be provisioned. If you have never provisioned a template from the Look book, review overview guidance.

Provision the NEO sites

1. Navigate to the custom PnP site templates and select the template you need. Learn more on how to apply the PnP templates here.

2. Navigate to the site you want to provision and select **Add to your tenant**. If you are not signed into to your tenant, the SharePoint look book will ask for your site collection admin credentials.

3. From the permissions requested dialog box, select **Consent on behalf of your organization** and then select **Accept**.

   > ⓘ **Important**
   >
   > The provisioning service requires these permissions to provision the site template. There is no overall impact on your tenant and these permissions are explicitly used for the purpose of the solution installation. You must accept these permissions to proceed with the installation.

4. Complete the fields on the provisioning information page as appropriate for your installation. At a minimum, enter the email address where you wish to get notifications about the provisioning process and the URL prefix for your site to be provisioned to.

5. Select **Provision** when ready to install the NEO sites into your tenant environment. The provisioning process will take up to 20 minutes for each site. You will be notified via email

(to the notification email address you entered on the Provisioning page) when the site is ready for access.

> **Note**
>
> Have provisioning questions? Need to report an issue? Post your questions and comments about the provisioning of the NEO sites to the SharePoint provisioning service forum.

Add owners to all sites

As the site collection admin, you may not be the person customizing the sites, so you'll need to assign a few site owners to the sites. Owners have administrative privileges on the site so they can modify site pages, content, and branding.

1. Select **Share** in the right-hand corner of the site.
2. Add users, Office 365 Groups, or security groups to give them access to the site.
3. Assign users as a **Site owner** to allow permission to customize the site.
4. Include the site URL in the Share message, and then select **Share**.

Step 2: Customize the onboarding experience

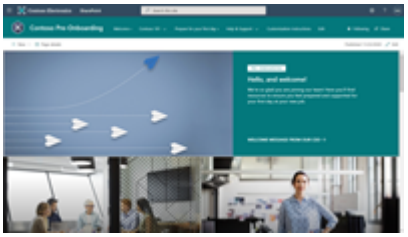
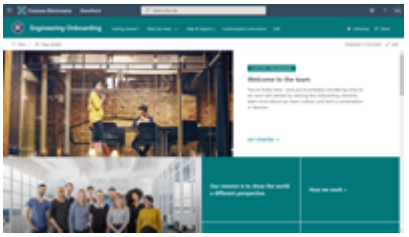
The New Employee Onboarding (NEO) sites consist of three SharePoint site templates that can be customized to fit the needs of your users and organization. Many of the core pages are already built and prepopulated with content. Review content on sites and pages, then plan on customizing content, images, branding, web parts, and pages.

Before you customize NEO site content, ensure you understand the needs of your users and the business objectives of your organization. New hires will need different kinds of support and resources depending on the onboarding phase and culture of your organization. Begin by signing into your account and reviewing prepopulated content. Then, customize content and prepare to share the site with new hires.

It's important to make sure the right content is available to users at the right time. It's also important to make new employees feel welcome before their first day. Organizations with a standardized onboarding process report 50% greater new-hire productivity. Alternatively, employees who have a negative onboarding experience are twice as likely to look for new opportunities shortly after starting a new job.

NEO site options:

Expand table

Preonboarding site	Corporate onboarding site	Departmental onboarding site
		
Share the Preonboarding site with new hires as soon as the job offer has been accepted	Share the Corporate onboarding site with new hires on their first day	Managers and onboarding buddies should share their respective Departmental onboarding site

> **Note**
>
> There are three NEO site templates that can be used alone or all together. Check with your site collection administrator to confirm which NEO sites were provisioned and are available for customizations.

1. **New employee pre-onboarding site:** A site for new hires, who have yet to officially join the company, to learn more about the company they have joined and to get ready for their official start date. External guest access can be used for prestart hires who don't already have corporate credentials to give them access to the Preonboarding site only.

   > **Important**
   >
   > Enable external sharing for the Pre-onboarding site. The Pre-onboarding site is intended to be shared with new hires as soon as they sign their offer letter, but before they start their first day at work. Therefore, this site needs to be shared with external users. External sharing is off by default for SharePoint communication sites. In order for site owners to share externally, turn on external sharing for the Pre-onboarding site.

2. **New employee corporate onboarding site:** A place for new hires to visit to get the information and connections they need to successfully onboard to the organization.

3. **New employee departmental onboarding site:** A place for new hires to visit to learn more about the department they're joining, its people, culture, and priorities. Consider associating departmental onboarding sites with existing department portals if you have them.

Get started - Sign into your Microsoft 365 account

> **Note**
>
> You need to be a site owner to customize and share the NEO sites. Work with your SharePoint Administrator if you don't already have access.

1. Open your web browser and navigate to office.com or your organization's sign-in location.
2. **Sign in** with your username and password.
3. Navigate to the location of the site using the URL supplied by your site collection admin, or select SharePoint from the Microsoft 365 home page, and then select the site.

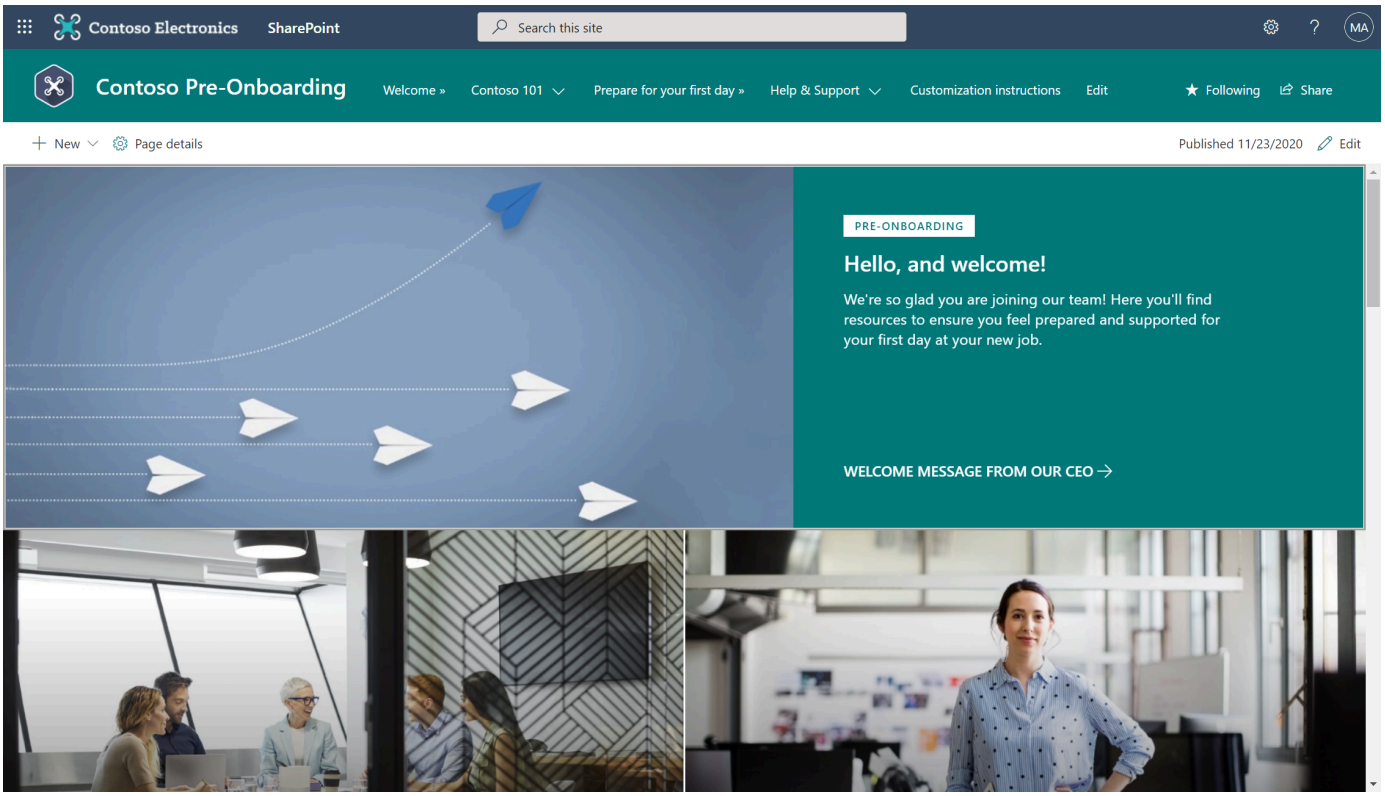
Explore and review prepopulated content

To deliver a flexible and consistent new hire onboarding experience the NEO sites consists of three different SharePoint site templates, that are designed to work alone or as one cohesive and familiar experience for new hires. Check with your site collection administrator to confirm which NEO sites were provisioned and are available for customizations.

- Review content in the Preonboarding site
- Review content in the Corporate onboarding site
- Review content in the Department onboarding site

> **Note**
>
> The NEO sites come with many pre-built pages that can be identified in the site navigation with this symbol ">>." Determine which pages and content to keep, edit, or delete based on the needs of your organization.

New employee preonboarding site



The preonboarding site is where a new hire starts their onboarding journey. This site is for new hires who have accepted their job offer but have not officially joined the company yet. In this stage, new hires will be interested in learning more about the company, how to get ready for their official start date, and who to go to for questions.

Pre-populated site content

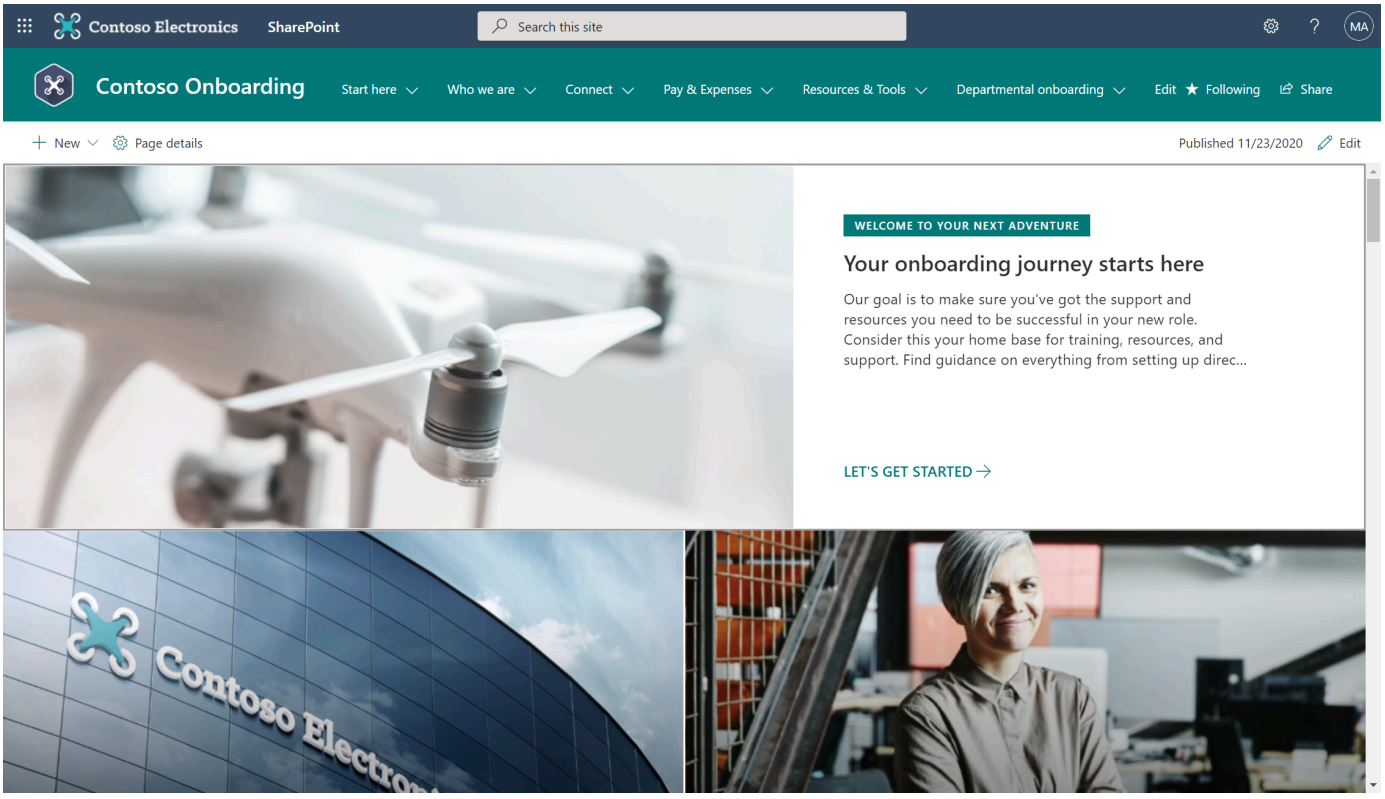
- **Home page** – The home page is the first site your user will see after they agree to accept the job. Use this landing page as an opportunity to highlight significant concepts and get new employees excited about starting their new job. Provide content for topics like organization leaders, values, communities of interest, benefits, and career planning resources.

  > **Important**
  >
  > Plan to connect social media accounts to the Hero web part and the Twitter web part.

- **Welcome** – Give new hires a warm welcome and place to start understanding onboarding tasks and how to prepare for their first day. This is a good opportunity to include a video message from leadership. Use the YouTube web part, or Embed web part to display the video.

- **Contoso 101** – Provide high-level information about the organization that engages and excites. Share more about leadership and values in Our leadership team and Our values pages.
- **Prepare for your first day** – Ensure new hires feel prepared and supported on their first day by providing details on what to bring and where to go.
- **Help & Support** – Highlight where to go for support and customize questions and answers for the FAQ page.

New employee corporate onboarding site



The corporate onboarding site is the landing place for the new employee onboarding experience and is designed to provide a high-level view of organizational goals, leadership, team structure, and resources. In this phase, users are looking for guidance, support, and clarity. Use this site to outline onboarding details and expectations during the first months of onboarding. Ensure users have access to support channels like Viva Engage, write FAQs relevant to your organization, and customize the onboarding checklist to include the activities you want all new hires to do in their first 30, 60, 90 days.

Pre-populated site contents:

- **Home page** – Provide a high-level view of significant concepts that will be relevant to new users. This page is a great location to help new employees build their network and learn

from more experienced and knowledgeable employees with Microsoft Teams live events

- **Start here** – Specify what new hires should do in their first 30, 60, and 90 days of onboarding by creating an onboarding process in on the Start your journey here page. The new hire checklist found in this section comes prepopulated with a set of generic onboarding activities. Customize list content to meet your needs. Learn more about working with SharePoint lists .

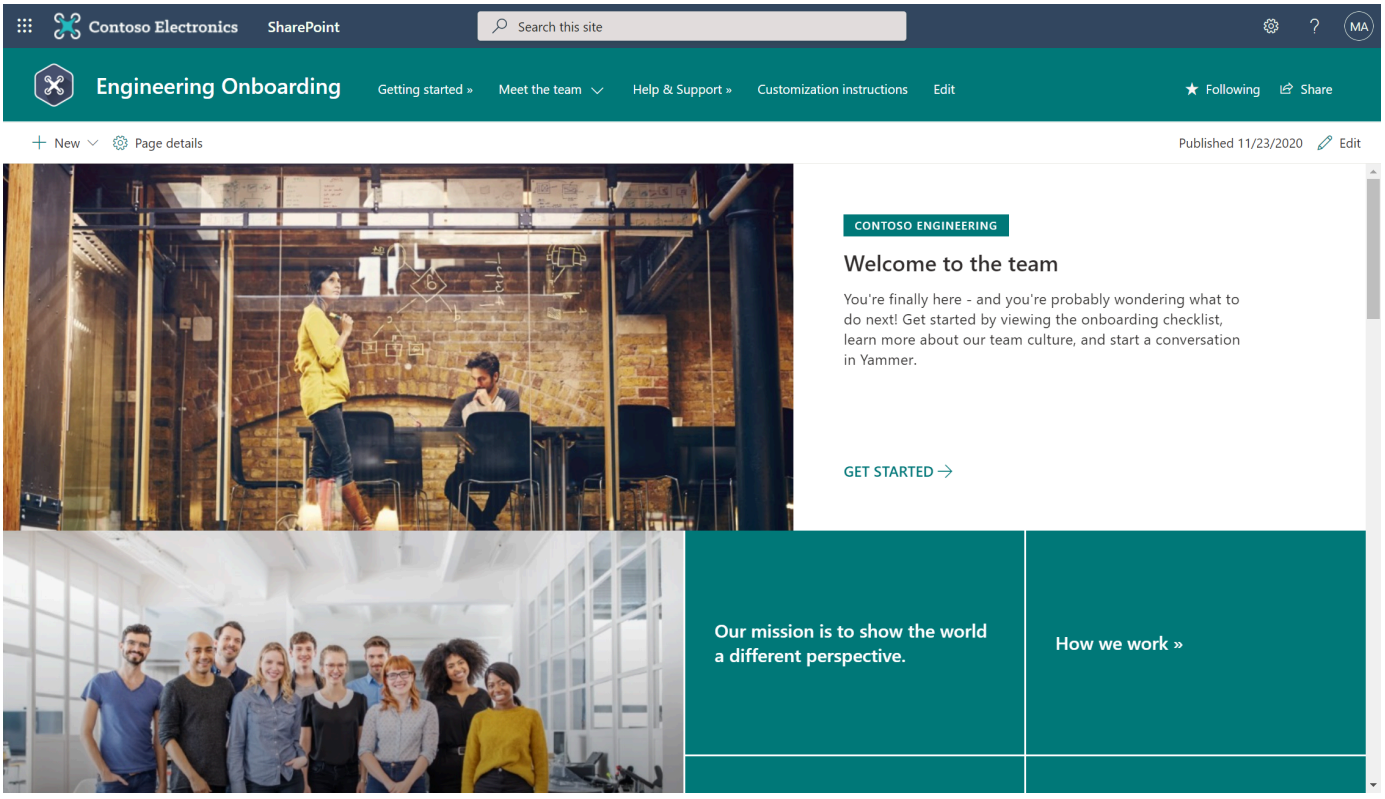
- **Who we are** – Introduce users to more detail about the organization in the Our story, Our leadership, Our teams pages. Customize these pages and the Office locations page for your organization. Or, link to an existing leadership page instead.

- **Help & Support** - Highlight where to go for support and customize questions and answers for the FAQ page.

- **Community** – Help new hires start building community right away and make sure new hires are aware of Employee resource groups and other connection channels.

- **Departmental onboarding** – Provide an entry point to departmental-level information from the site navigation where users can access departmental onboarding sites. Consider provisioning the Department site template.

New employee departmental onboarding site



Here, users need to learn about departmental leadership, culture, goals, and resources. Use the departmental onboarding site to provide access to communication channels, training guides, and events relevant to new hires. Consider associating departmental onboarding sites with existing department portals if you have them.

Pre-populated site contents

- **Home page** - Provide a high-level view of significant concepts that will be relevant to new hires.
- **Getting started** – Help users quickly understand onboarding tasks, departmental procedures, and anything else that will help new hires be successful.
- **Meet the team** – Introduce new hires to people, the organization structure and goals on the Leadership, The organization, and Our priorities pages. Edit the Call to Action web part to include links and images. Or, link to an existing team page instead.
- **Help and support** - Highlight where to go for support and consider creating a FAQ section.

Next steps: Customize place-holder content, edit the site navigation, add pages as needed, and hook up social media accounts in web parts.

Customize the content and look of your NEO sites

Now that you've reviewed the pre-built pages and prepopulated content, you are ready to customize the NEO experience for your organization.

Navigation

Site navigation is important because it helps users immediately understand what can be accomplished on a given site. The most effective SharePoint sites help viewers find what they need quickly so that they can use the information to make decisions, learn about what is going on, access the tools they need, or engage with colleagues to help solve a problem. Edit site navigation for all NEO site templates to meet the needs of your audience and organization. Learn how to edit site navigation.

Web parts

Customize web parts with images, labels, links, and content that aligns with your organization's mission. Keep images and descriptions simple and easy to understand for your new-hire audience.

- **Hero web part** - Bring focus and visual interest to your page with the Hero web part. You can display up to five items in the Hero web part and use compelling images, text, and links to draw attention to each.
- **Text web part** - Use the Text web part to add paragraphs to your page. Formatting options like styles, bullets, indentations, highlighting, and links are available.
- **Image web part** – Use the Image web part to add an image to a page.
- **Quick links web part** – Organize and display links to other resources with the Quick links web part.
- **People web part** – Use the People web part to display profile photos, contact information, and organizational information for people at work.
- **Twitter web part** - Use the Twitter web part to highlight topics and conversations on SharePoint pages.
- **YouTube web part** - Use the YouTube web part to embed YouTube videos right on your page.

Site theme and branding

Edit the look of your SharePoint sites to align with your organization's brand. Customize the site display name, logo, theme, header layout, navigation style, and more in the Change the look panel.

Hub site settings

SharePoint hub sites help connect and organize sites based on project, department, division, region, etc. making it easier to:

- Discover related content such as news and other site activities
- Apply common navigation, branding, and site structure across associated sites
- Search across all associated sites.

Considering associating the departmental onboarding site to an existing corporate onboarding site or departmental hub. Learn how hub site associations work and how to manage hub settings for your organization. Learn more about SharePoint hub sites.

More customization resources

- Add a page to a SharePoint site
- How to use web parts on SharePoint pages
- Use the Events web part
- Use the News web part

Step 3: Share the NEO sites with end users

After customizing content, get ready to share the new onboarding experience with new hires. Different permissions will apply to the Preonboarding site since users will be external guests. Once new hires start working, use internal permissions sharing instructions to give access to the corporate onboarding site.

Share the Preonboarding site

> **Note**
>
> If you are unable to add visitors (external users, also referred to as guests) to the pre-boarding site, work with your SharePoint Administrator to turn on external sharing for a SharePoint site.

As a site owner, you can give external people access to the site by adding them as a **visitor**.

1. Select **Share site** from the right-hand corner.
2. In the Share site pane, enter the names of people to add them to the site. The permission level will be read only.
3. Enter an optional message to send to the person, or clear the Send email box if you don't want to send an email.
4. Select **Share.**

Share the Corporate and Departmental onboarding sites

1. Select **Share site** from the right-hand corner.
2. In the **Share site** pane, enter the names of people or groups to add them to the site, or enter "Everyone except external users" to share the site with everyone in your organization.
3. Change the permission level (Read, Edit, or Full control) as needed.

4. Enter an optional message to send to the person or clear the Send email box if you don't want to send an email.

5. Select **Share**.

Step 4: Measure the impact of your NEO sites

Define NEO success metrics

Define site success metrics to measure and optimize your organization's onboarding process. This is an example of possible metrics for a new employee onboarding site experience in the form of an onboarding hub:

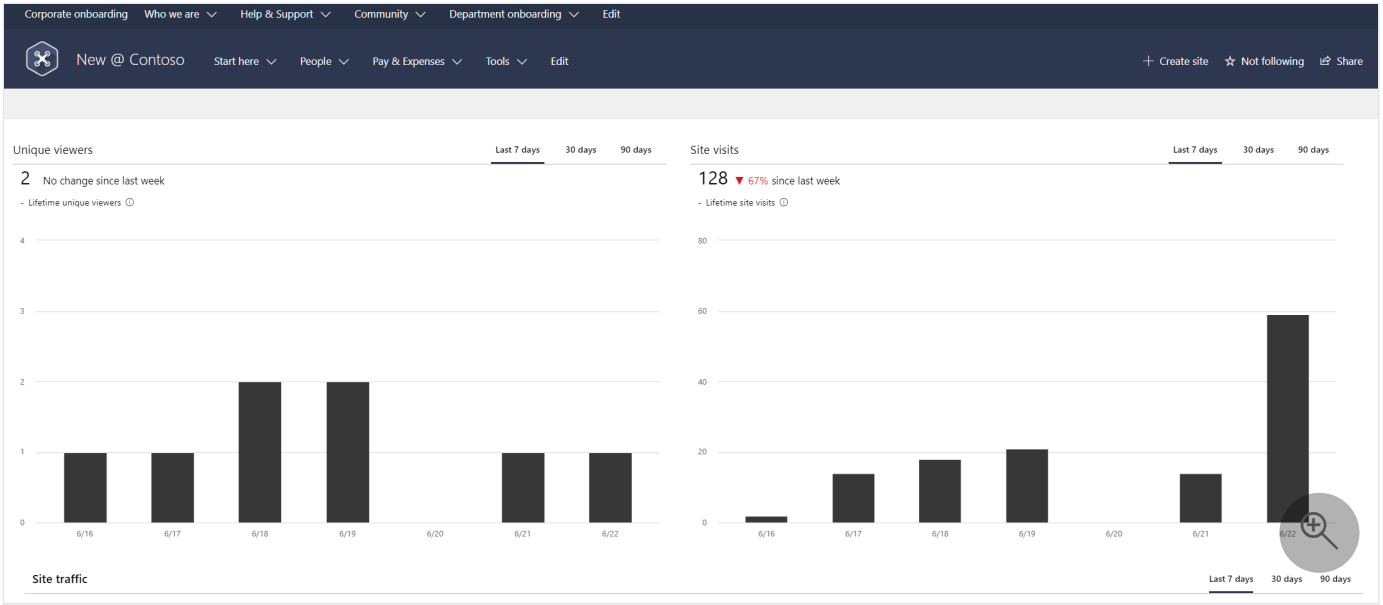
Expand table

Objective	Business owner	KPI measure	Data source	KPI formula	KPI baseline	KPI target
Help onboard new employees more effectively	Diego Siciliani	New employee satisfaction	Survey data	Average score of new employee satisfaction with NEO Hub	N/A	4.25
Help onboard new employees more effectively	Diego Siciliani	NEO hub usage	Site usage report	Number of unique viewers and visits	N/A	500 unique viewers/month and 1,500 views/month
Increase new employee retention	Alexandre Levesque	New employee retention	HR system retention data	% of new employee cohort that remains with the company after one year	75%	90%
Improve new employee engagement	Diego Siciliani	New employee engagement score	Survey data	Average score of new employee engagement question	3.75	4.25

Use site usage data

As a SharePoint site owner, you can view site usage data that shows you how users are interacting with your site. For example, you can see the number of people who have visited the site, how many times people have visited the site, and a list of files that have received the most views. Site owners should utilize SharePoint's built-in site usage reporting capabilities to measure the impact of the NEO sites and hub. Learn how to view usage analytics for your site.

Example of site usage data:



Step 5: Manage and maintain your NEO sites

NEO sites should present the most up-to-date content your organization has to offer, so you'll need to commit to maintaining relevant content throughout the experience. Develop a plan to audit content and refresh web parts as needed to ensure contact information, FAQs, the onboarding checklist, and People web parts are up to date. Learn more about managing communication sites.

- Train site owners and authors. Make sure all site owners and authors have appropriate training and access to maintain the site.
- Update content in web parts. Keep web parts like the People web part updated to ensure you are using the full value of the NEO sites.
- Review previously established metrics after the launch. Use insights from site analytics to promote content on the home page, update navigation, or rewrite content for clarity.
- Establish a schedule to audit content. Plan when site owners should audit content in advance to make sure your sites are always up to date.
- Periodically review your site settings. Make changes to the settings, site information, and permissions for the site as needed.

NEO site FAQs

Question: What are the requirements for installing the New Employee Onboarding (NEO) sites into my tenant environment?

Answer:

- SharePoint and communication sites enabled.
- The individual that will be provisioning CLO365 must be the site collection administrator of the target tenant for install.

Question: How long will it take to install the site in our tenant environment?

Answer: Based on our testing of the installation, it should take less than 15 minutes. This does not include time required to customize the site to your requirements.

Question: Where can I ask questions or report an issue with the SharePoint provisioning service?

Answer: Post your questions and comments about the provisioning of the NEO sites to the SharePoint provisioning service forum.

Question: Where can I share feedback for ideas on how to improve the SharePoint site experience?

Answer: Post your ideas and comments about SharePoint sites in the Site and Collaboration User Voice Forum

> **Note**
>
> Microsoft will be moving from UserVoice to our own customer feedback solution on a product-by-product basis during 2021. Learn more.

Question: Where can I ask questions or report an issue with the SharePoint provisioning service?

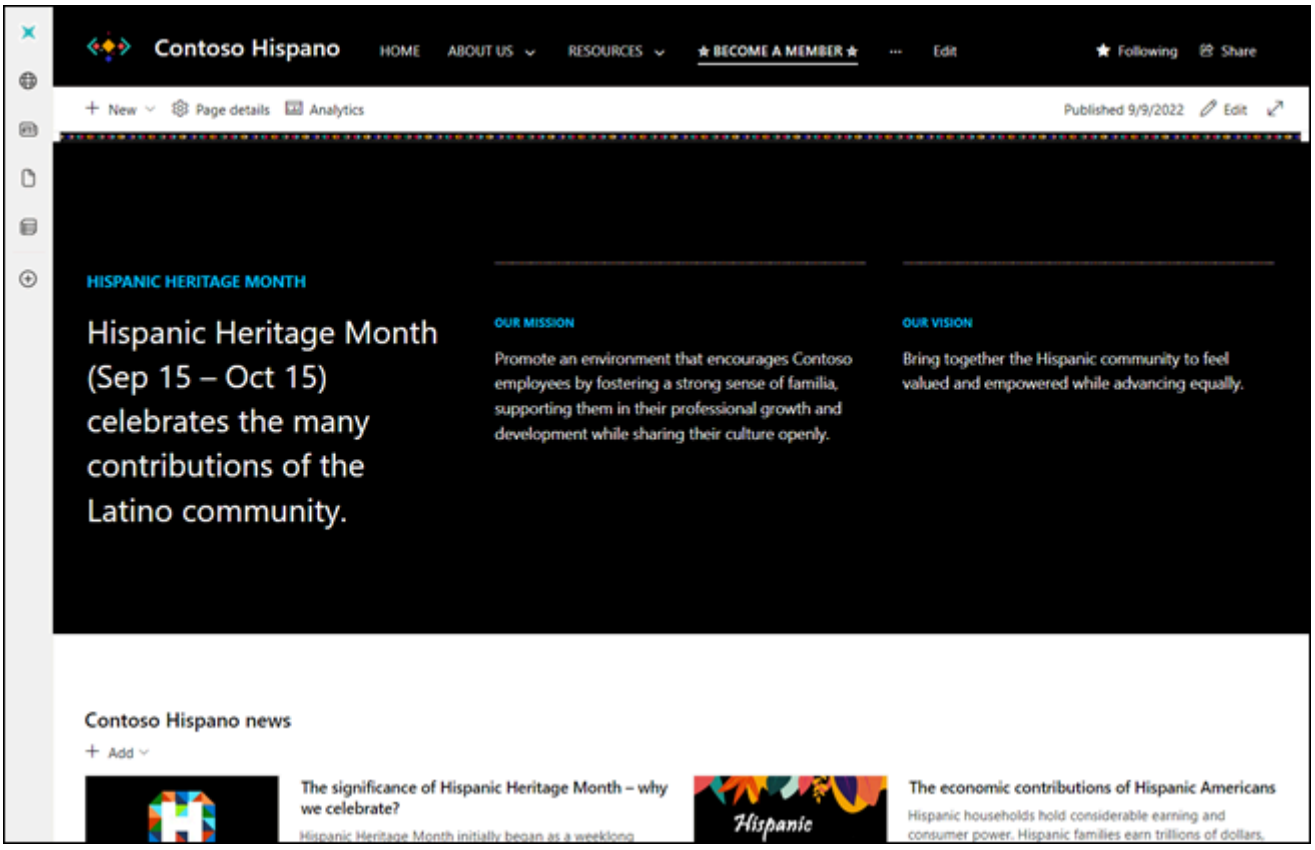
Answer: Post your questions and comments about the provisioning of the NEO sites to the SharePoint provisioning service forum.

Sources:

- Gallup, State of the American Workplace, 2017*
- SHRM, Don't Underestimate the Importance of Good Onboarding, 2017**
- Source: Digitate, Super CIO: What the CIO sees—that other people don't, 2018

Last updated on 06/25/2026

Overview of the Hispanic Heritage Employee Resource Group site template



Use the Hispanic Heritage Employee Resource Group site template to quickly create a communication site from the SharePoint Look Book to uplift employee resource groups, support the career growth of people in your organization, and to help advance equality and allyship for all.

This template features content focused on a Hispanic and Latinx employee resource group but can be adapted to fit various other employee groups at your organization.

The Hispanic Heritage Employee Resource Group site features:

- **Home page with a unique theme:** The site's landing page features Hispanic heritage branding, inclusive content, and example news posts and events.
- **Page template:** Use the page template to create news posts and more pages for the site.
- **Pre-populated content and web parts:** Includes inspirational and inclusive content to make customizing the site easier.
- **Easy provisioning:** Provision the Hispanic Heritage Employee Resource Group site from the SharePoint Look Book with just a few steps.

- **Mobile ready:** The Employee Resource Group site can be easily accessed on a mobile device when you get the SharePoint mobile app.

How to get the Hispanic Heritage Employee Resource Group site:

Expand table

Step 1: Provision	Step 2: Customize	Step 3: Share
Navigate to the custom PnP site templates and select the template you need	Follow guidance on this page to customize the site	Share the site with the rest of your organization

Step 1: Provision the site

1. Go to the Hispanic Heritage Employee Resource Group template page.
2. Select **Add to your tenant**. If you aren't signed into to your tenant, the SharePoint Look Book asks for your site collection admin credentials.
3. From the permissions requested dialog box, select **Consent on behalf of your organization** and then select **Accept.**

   > **Note**
   >
   > The provisioning service requires these permissions to provision the site template. There is no overall impact on your tenant, and these permissions are used for the solution installation. You must accept these permissions to proceed with the installation.

4. Complete the fields on the provisioning information page as appropriate for your installation. At a minimum, enter the email address where you wish to get notifications about the provisioning process and the URL prefix for your site to be provisioned to.
5. Select **Provision** when ready to install the site into your tenant environment.
   - The provisioning process takes up to 20 minutes.
   - You'll be notified via email (to the notification email address you entered on the Provisioning page) when the site is ready for access.

Next, add owners to the site

As the site collection admin, you may not be the person customizing the site, so you need to assign a few site owners. Owners have administrative privileges on the site so they can modify site pages, content, and branding.

1. Select **Share** in the right-hand corner of the site.
2. Add users, Microsoft 365 Groups, or security groups to give them access to the site.
3. Assign users as a Site owner to allow permission to customize the site.
4. Include the site URL in the Share message, and then select **Share.**

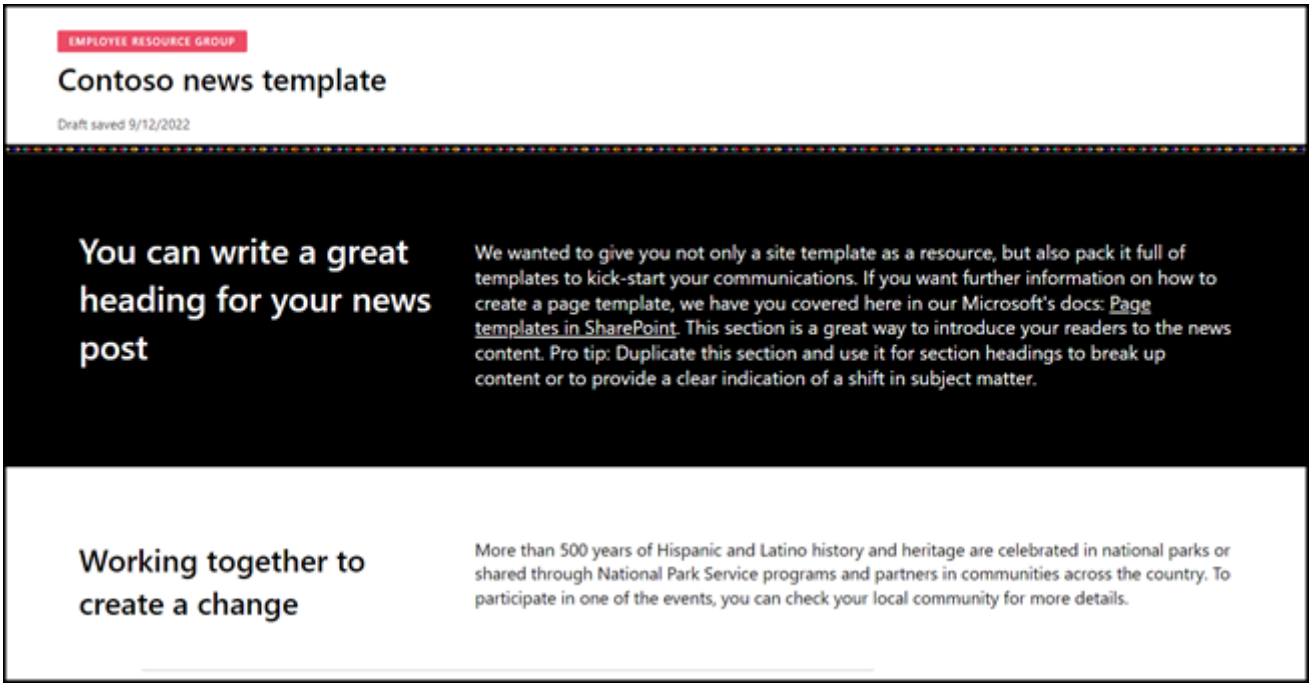
Step 2: Customize the site

After the site has been provisioned and site owners have been added, it's time to customize the site to make it your own. Customize the site's look, navigation, and content like news posts and events.

Start by signing into Microsoft 365 and navigating to the site

1. Open your web browser and navigate to office.com or your organization's sign-in location.
2. Sign in with your username and password.
3. Navigate to the site's location using the URL supplied by your site collection admin, or select SharePoint from the Microsoft 365 home page, and then select the site.

Next, explore prepopulated content:



- **Home page –** The landing page features a unique theme, colorful images, and more inspirational content that is relevant and engaging. Content here's inspired by Hispanic and Latinx employee resource groups but can be adapted to other types of groups. Customize the Text, News, Events, and Quick Links web parts to make this site your own.
- **Page template –** A page template with a unique theme can be found in the site's contents to help create news posts and pages for the site more quickly.
- **News web part –** Prepopulated news posts were created using the page template.
- **Events web part –** Prepopulated events from different employee resource groups highlight more opportunities to learn and practice allyship.

Then, customize the site

1. **Add your organization's logo and review more site design details:** Edit the look of your SharePoint sites to align with your organization's brand. Customize the site display name, logo, header layout, navigation style, and more in the Change the look panel.

2. **Customize the site's navigation:** Edit site navigation to include links to other relevant resources. Learn how to edit site navigation. Start by selecting **Edit** next to the navigation panel to start editing labels and links.

3. **Edit web part content:** Select **Edit** in the right-hand corner to begin customizing web parts and content. Select the **Edit** (pencil icon) next to each web part to customize the layout and to edit content.

   - Text web part – Replace prepopulated content with your own.

   - News web part - Use the Page template that can be found in **Settings** > **Site content** > **Pages** > **Templates** to create branded news posts that populate the News web part. Delete the prepopulated news posts before sharing the site with others.

   - Events web part - Edit events in the Events web part to include events from your organization's employee resource groups. Delete the prepopulated events before

sharing with others.

- Quick Links web part – Edit links to connect to more resources and employee resource groups sites.

Step 3: Share the site

Once you are done customizing and proof-reading the site, you're ready to share it with others. Run a health check before sharing and consider using the Portal launch scheduler tool if you expect a high amount of site traffic (10k individual visits per day or higher) to ensure a high-quality viewing experience.

1. Select **Share** from the right-hand corner.
2. In the Share site pane, enter the names of people to add to the site. The permission level is read only.
3. Enter an optional message to send to the person or clear the Send email box if you don't want to send an email.
4. Select **Share.**

More resources

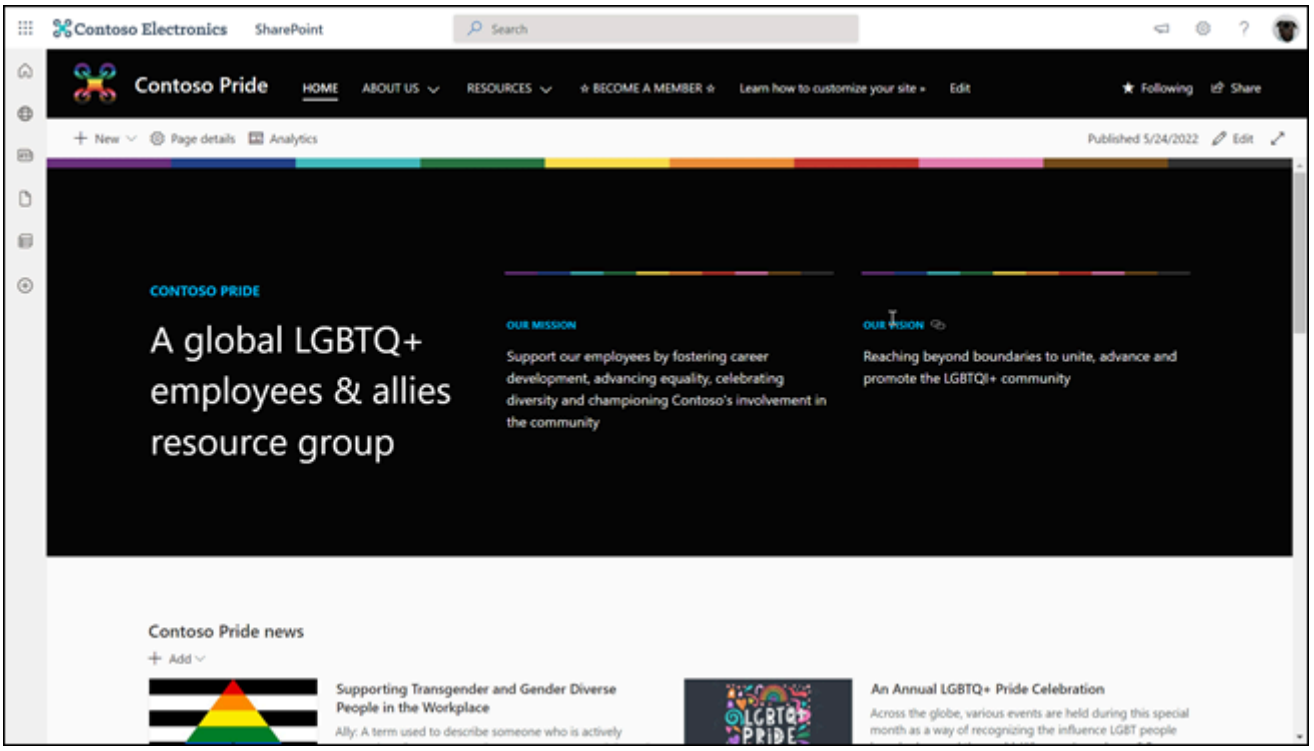
Add a page to a communication site

Using web parts on SharePoint pages

Customize your SharePoint site

Last updated on 06/24/2026

Overview of the LGBTQ+ Employee Resource Group site template



Use the LGBTQ+ Employee Resource Group site template to quickly create a communication site from the SharePoint Look Book. You can use this site template to uplift employee resource groups, support the career growth of people in your organization, and to help advance equality and allyship for all.

This template features content focused on an LGBTQ+ employee resource group but can be adapted to fit various other employee groups at your organization.

The LGBTQ+ Employee Resource Group site features:

- **Home page with a unique theme:** The site's landing page features Pride branding, inclusive content, and example news posts and events.
- **Page template:** Use the page template to create news posts and more pages for the site.
- **Pre-populated content and web parts:** Includes inspirational and inclusive content to make customizing the site easier.
- **Easy provisioning:** Provision the LGBTQ+ Employee Resource Group site from the SharePoint Look Book with just a few steps.
- **Mobile ready:** The LGBTQ+ Employee Resource Group site can be easily accessed on a mobile device when you get the SharePoint mobile app.

How to get the LGBTQ+ Employee Resource Group site:

Expand table

Step 1: Provision	Step 2: Customize	Step 3: Share
Navigate to the custom PnP site templates and select the template you need	Follow the guidance to customize the site	Share the site with the rest of your organization

Step 1: Provision the site

1. Go to the LGBTQ+ Employee Resource Group template page.
2. Select **Add to your tenant**. If you aren't signed into to your tenant, the SharePoint look book will ask for your site collection admin credentials.
3. From the permissions requested dialog box, select **Consent on behalf of your organization** and then select **Accept.**

> **Note**
>
> The provisioning service requires these permissions to provision the site template. There is no overall impact on your tenant, and these permissions are used for the solution installation. You must accept these permissions to proceed with the installation.

4. Complete the fields on the provisioning information page as appropriate for your installation. At a minimum, enter the email address where you wish to get notifications about the provisioning process and the URL prefix for your site to be provisioned to.
5. Select **Provision** when ready to install the site into your tenant environment.

    - The provisioning process takes up to 20 minutes.
    - You'll be notified via email (to the notification email address you entered on the Provisioning page) when the site is ready for access.

Next, add owners to the site

As the site collection admin, you may not be the person customizing the site, so you need to assign a few site owners. Owners have administrative privileges on the site so they can modify site pages, content, and branding.

1. Select **Share** in the right-hand corner of the site.
2. Add users, Microsoft 365 Groups, or security groups to give them access to the site.

3. Assign users as a Site owner to allow permission to customize the site.
4. Include the site URL in the Share message, and then select **Share.**

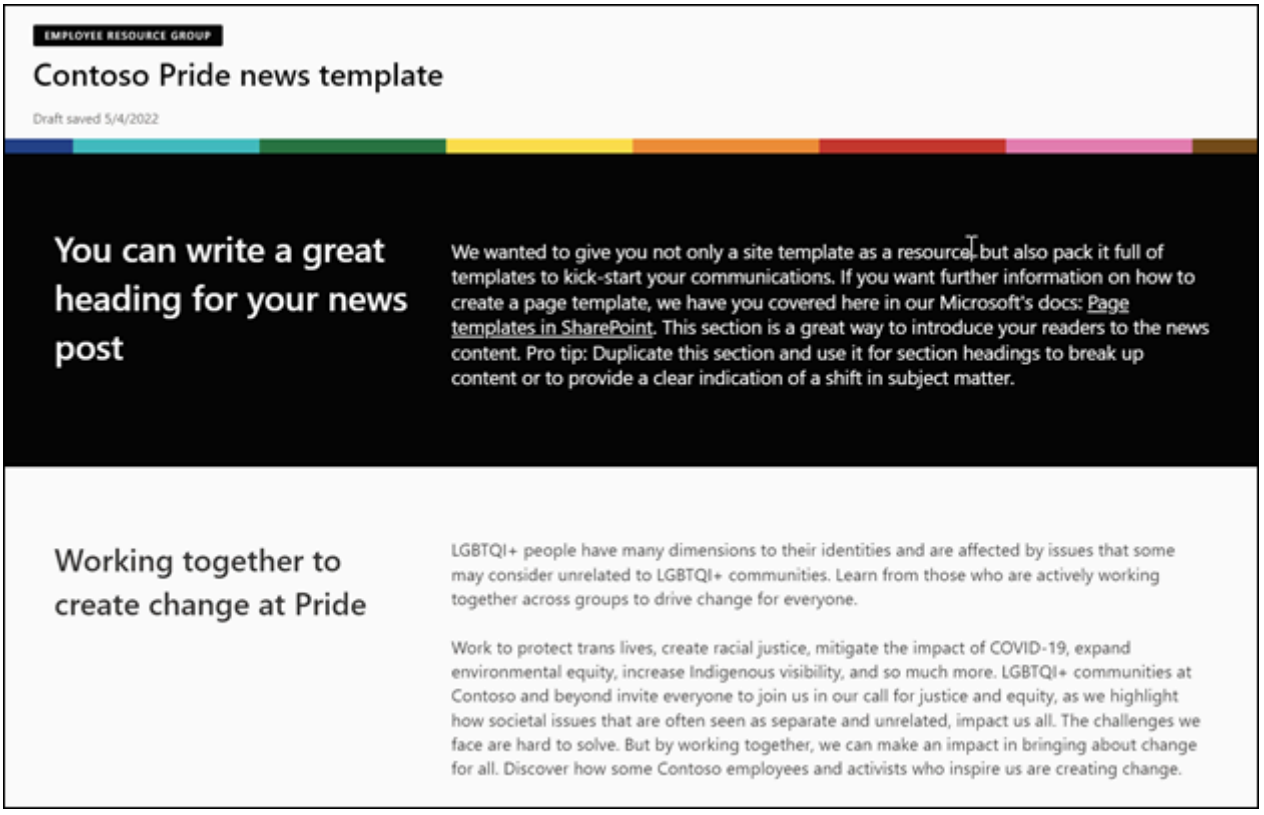
Step 2: Customize the site

After the site has been provisioned and site owners have been added, it's time to customize the site to make it your own. Customize the site's look, navigation, and content like news posts and events.

Start by signing into Microsoft 365 and navigating to the site:

1. Open your web browser and navigate to office.com or your organization's sign-in location.
2. Sign in with your username and password.
3. Navigate to the site's location using the URL supplied by your site collection admin, or select SharePoint from the Microsoft 365 home page, and then select the site.

Next, explore prepopulated content:



- **Home page –** The landing page features a unique theme, colorful images, and more inspirational content that is relevant and engaging. Content here's inspired by an LGBTQ+ employee resource group but can be adapted to other types of groups. Customize the Text, News, Events, and Quick Links web parts to make this site your own.

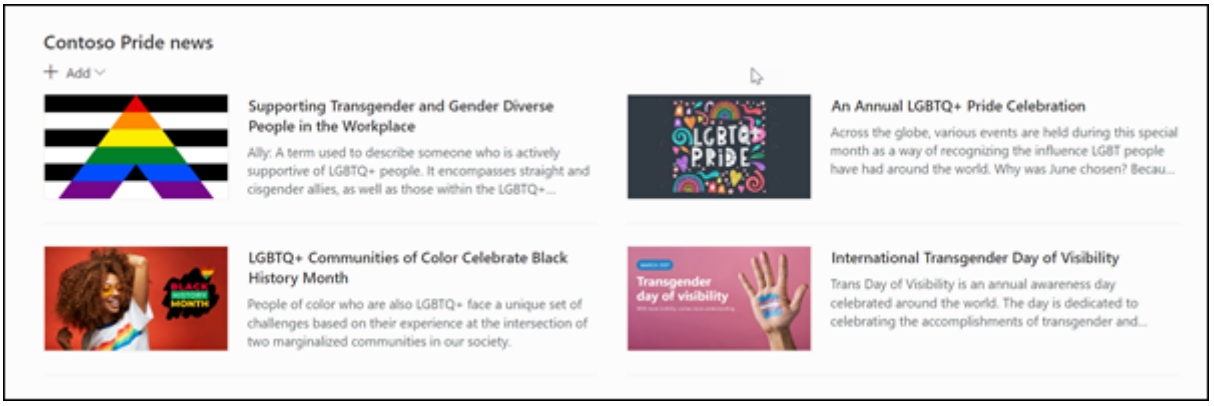
- **Page template –** A page template with a unique theme can be found in the site's contents to help create news posts and pages for the site more quickly.
- **News web part –** Prepopulated news posts were created using the page template.
- **Events web part –** Prepopulated events from different employee resource groups highlight more opportunities to learn and practice allyship.

Then, customize the site:

1. **Add your organization's logo and review more site design details:** Edit the look of your SharePoint sites to align with your organization's brand. Customize the site display name, logo, header layout, navigation style, and more in the Change the look panel.

2. **Customize the site's navigation:** Edit site navigation to include links to other relevant resources. Learn how to edit site navigation. Start by selecting **Edit** next to the navigation panel to start editing labels and links.

3. **Edit web part content:** Select **Edit** in the right-hand corner to begin customizing web parts and content. Select the **Edit** (pencil icon) next to each web part to customize the layout and to edit content.



   - Text web part – Replace prepopulated content with your own.

   - News web part - Use the Page template that can be found in **Settings** > **Site content** > **Pages** > **Templates** to create branded news posts that populate the News web part. Delete the prepopulated news posts before sharing the site with others.

   - Events web part - Edit events in the Events web part to include events from your organization's employee resource groups. Delete the prepopulated events before sharing with others.

   - Quick Links web part – Edit links to connect to more resources and employee resource groups sites.

Step 3: Share the site

Once you're done customizing and proof-reading the site, you're ready to share it with others. Run a health check before sharing and consider using the Portal launch scheduler tool if you expect a high amount of site traffic (10k individual visits per day or higher) to ensure a high-quality viewing experience.

1. Select **Share** from the right-hand corner.
2. In the Share site pane, enter the names of people to add to the site. The permission level is read only.
3. Enter an optional message to send to the person or clear the Send email box if you don't want to send an email.
4. Select **Share.**

More resources

Add a page to a communication site

Using web parts on SharePoint pages

Customize your SharePoint site

Last updated on 06/24/2026

Introduction to the SharePoint Success Site

The SharePoint Success Site is a ready to deploy and customizable SharePoint communication site that helps your organization maximize the adoption of SharePoint. The SharePoint Success Site is designed to support new SharePoint Site owners in creating high-impact sites to meet the goals of your organization.

The SharePoint Success Site builds on the power of Microsoft 365 learning pathways which allows you to use Microsoft-maintained playlists for training purposes. You can also create custom playlists to meet the unique training requirements of your organization. If you are already using M365 learning pathways and don't want to provision the SharePoint Success Site, you can enable the SharePoint Success Site playlist into learning pathways.

Install the SharePoint Success Site in your tenant environment, customize the pre-populated training and site content, and then make it available to end users.

Ready to get started right away? Next, review the prerequisites and provisioning guidance.

Why invest in a SharePoint Success Site?

The SharePoint Success Site helps Site owners improve the quality and impact of the sites they build in SharePoint for internal audiences, while helping ensure they follow your organization's site usage guidelines.

Use the SharePoint Success Site to:

- **Get more out of SharePoint** - Show new Site owners how to leverage the value behind SharePoint's communication and collaboration features. Help new Site owners understand the ways to work with SharePoint to meet specific business outcomes. Then, show users how to utilize the power behind SharePoint's communication and collaboration features with step-by-step guidance.
- **Enable Site owners to create high-impact sites** - Ensure Site owners have the right information and support to create purposeful sites that are widely adopted by the intended audience.
- **Ensure Site owners follow site creation policies** - Customize the site usage and creation policies page in your SharePoint Success site to communicate organizational policy expectations during the training experience.

- **Provide the most up-to-date content** - Equip Site owners with SharePoint self-help content that is maintained by Microsoft and published as SharePoint evolves.

SharePoint Success Site features

The SharePoint Success Site is designed to reduce the amount of work needed to plan, build, and manage new SharePoint sites for Site owners and content authors.

SharePoint Success Site features:

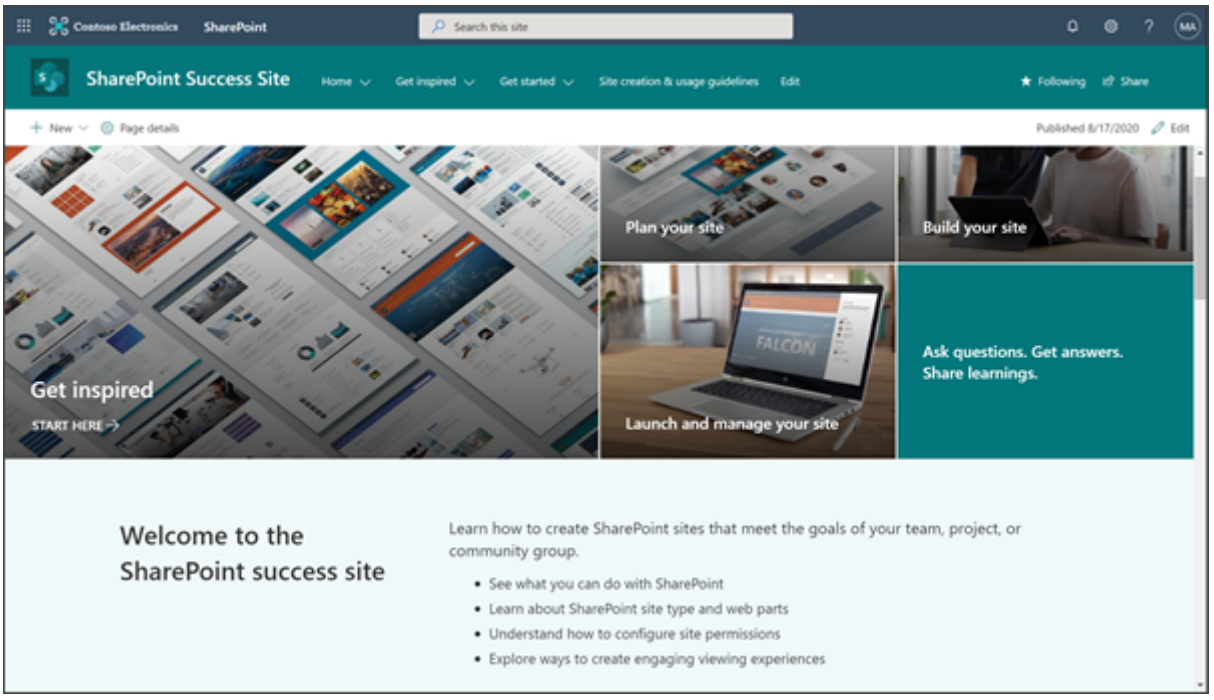
- **Fast provisioning:** Provision the SharePoint Success Site with just a few steps.
- **Easily customizable:** Edit the site layout, branding, and Microsoft-provided playlist content to align with how you have set up SharePoint in your tenant.
- **Comprehensive Site owner training content:** Training on what makes an effective site and how to build and maintain the site.
- **Site creation guidelines:** Create SharePoint usage guidelines that fit policy requirements for your organization.
- **Create your own training playlists:** Add your own custom training content and playlists specific to your organization's desired business outcomes outside of SharePoint.

What comes with a SharePoint Success Site

The SharePoint Success Site comes pre-populated with web parts and content to guide your users through the most up-to-date site creation training. There are several opportunities to customize the experience to better suit your organization's goals, tenant configuration, and usage policy.

SharePoint communication site

The SharePoint Success Site is a SharePoint communication site that includes pre-populated pages, web parts, and site navigation. The site can be customized to incorporate your organization's existing branding, support, and training content.



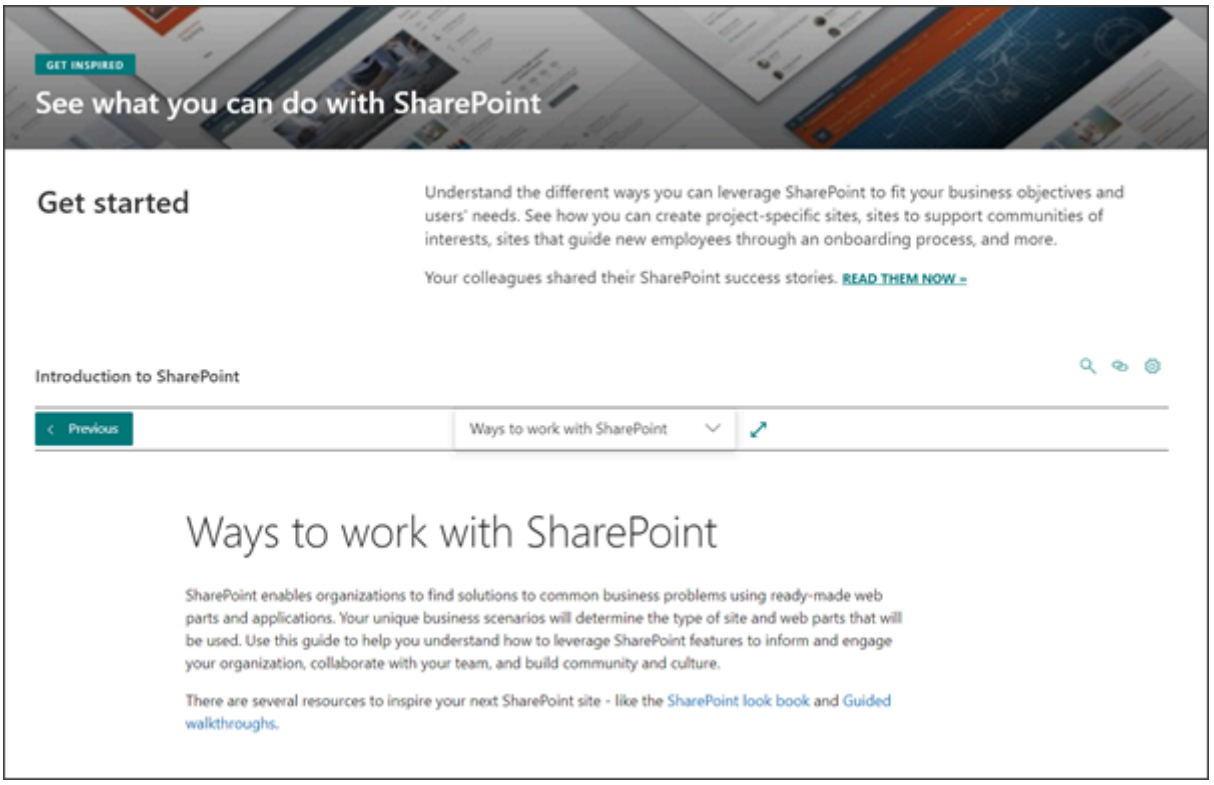
Microsoft-maintained content feed

The SharePoint Success Site's up-to-date content feed includes a range of content that helps new users and existing site owners plan, build, and manage SharePoint sites:

- **Plan your site:** Guidance on the ways to work with SharePoint, how to plan a site, including what type of SharePoint site to use and how to manage site access and permission strategy.
- **Create your site:** Content that helps new Site owners create their site, add content, customize web parts, and apply brand elements.
- **Share and manage your site:** Guidance to help launch, share, and manage the new site.
- **Advanced site creation:** Content for Site owners who want to learn more about SharePoint beyond site creation basics.

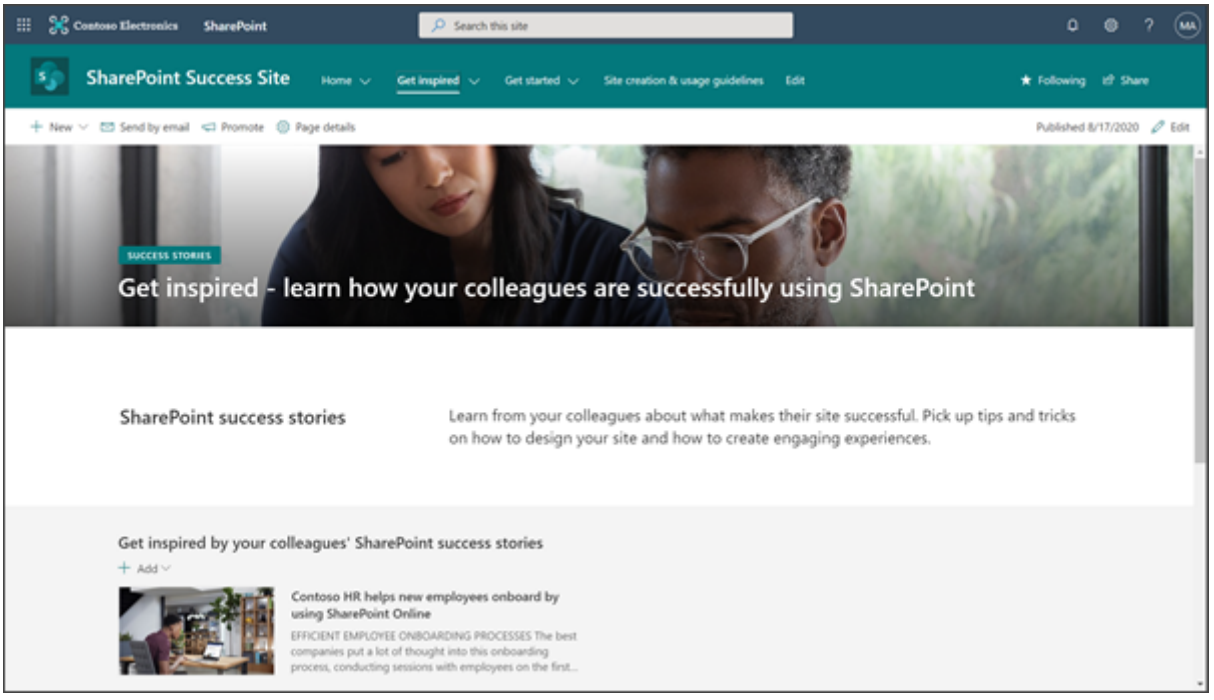
Site inspiration

The introductory content helps new site owners understand the different ways you can leverage SharePoint to meet common business objective through fictional stories that help establish an understanding about the site creation stages and common tasks. Users will have access to stories that illustrate how to build an onboarding site, a project management site, a site that supports a community of interest, and a team collaboration site. These scenarios provide guidance on how to think about the planning, building, and launching phases.



Success stories

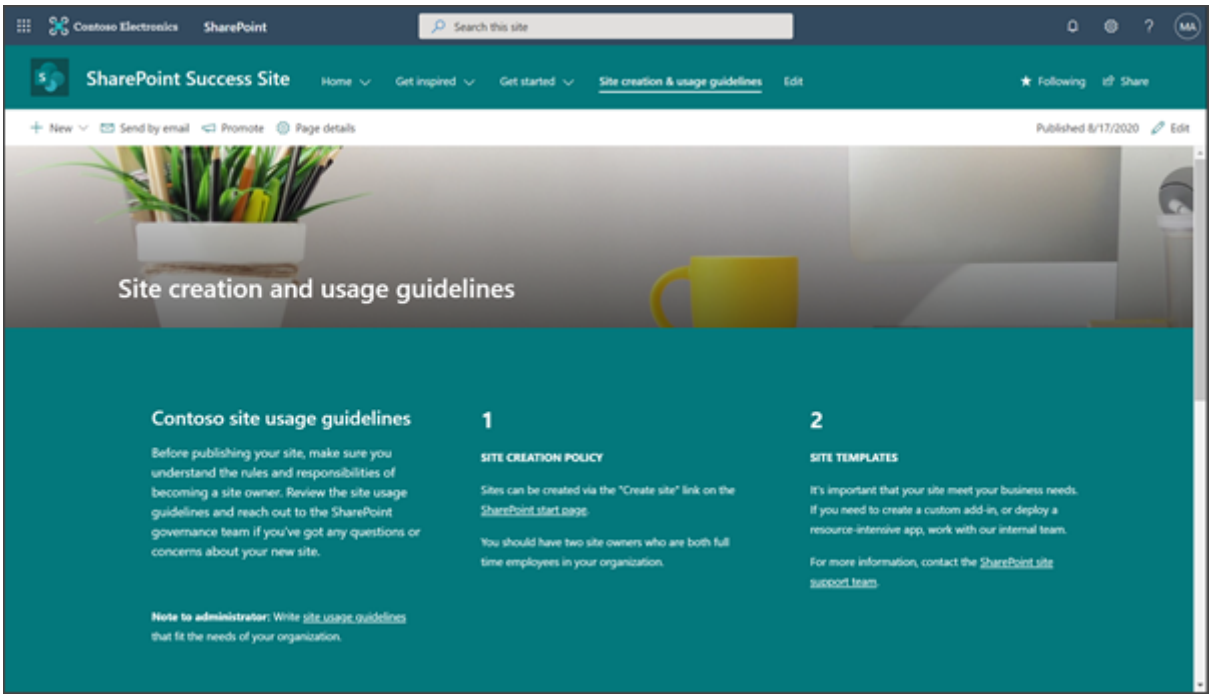
The success stories section is a gallery to showcase internal SharePoint site success stories that inspire others in the organization. Learn how to create a Microsoft Form to solicit success stories from site owners and authors, and publish on your SharePoint Success Site to inspire.



Site creation guidelines

The site creation guidelines page provides a starting point to educate new Site owners about SharePoint creation policies for your organization. The guidelines include suggested usage policy

topics and questions to prompt consideration of usage policies within your organization. Customize the content in your SharePoint Success Site site creation guidelines page to serve your organization's governance needs.



Summary of how to launch a SharePoint Success Site

Step 1: Meet the prerequisites and then provision the SharePoint Success Site

Step 2: Customize the site design, playlists, success stories, and site creation guidelines

Step 3: Launch and share the site with others

Next steps - provision the SharePoint Success Site

Review and implement SharePoint Success Site provisioning requirements and instructions.

Frequently asked questions

Question: Who has permission to provision the SharePoint Success Site?

Answer: The Global Administrator (formerly called the Tenant admin) are required.

Question: Who has permission to customize the site template?

Answer: The SharePoint site owner and above (./site-permissions).

Question: Who can create custom playlists and hide or show content in M365 learning pathways?

Answer: The SharePoint site owner and above (./site-permissions). M365 learning pathways.

Question: Who has permissions to use the SharePoint Success Site as a user?

Answer: Microsoft 365 user permissions or SharePoint Site visitor permissions or higher.

Last updated on 06/25/2026

Provision the SharePoint Success Site

Article • 03/18/2024

Start the SharePoint Success Site provisioning process by understanding the prerequisites. We recommend provisioning the SharePoint Success Site from the Microsoft 365 learning pathways administration page by following the instructions in this article. Global Administrator (sometimes called tenant administrator) credentials are required to start the provisioning process for the SharePoint Success Site.

> **Important**
>
> Microsoft recommends that you use roles with the fewest permissions. Using lower permissioned accounts helps improve security for your organization. Global Administrator is a highly privileged role that should be limited to emergency scenarios when you can't use an existing role.

Before getting started, watch the provisioning instructional video, follow all steps in the process, and make sure you've met the requirements for provisioning.

Meet the requirements

Before provisioning the SharePoint Success Site, meet the requirements for both the **person** provisioning and the **tenant.** Your tenant's configuration determines what path you need to take to install the SharePoint Success Site. Start by reviewing the SharePoint Success Site requirements below to prepare your tenant.

Expand table

Admin role requirements	+	Tenant requirements	=	Ready to provision

Admin requirements

The **person** doing the provisioning must be a Global Administrator (sometimes called a tenant admin) where the SharePoint Success Site is provisioned *and must also be* a site admin for the App Catalog.

Expand table

Global Administrator role	+	Admin of the App Catalog	=	Admin role requirements met

Are you a Global Administrator?

- **Yes** - Next, confirm your tenant has already enabled the App Catalog.
- **No** - Partner with your global admin to get the site provisioned. Learn more about admin roles.

If you aren't sure, you can confirm your role by signing in to office.com. If you're a Global Administrator, you see an Admin center app icon in the app launcher next to your Microsoft 365 apps.

Are you a site administrator for the App Catalog?

- **Yes** - Next, confirm your tenant has Microsoft 365 learning pathways provisioned.
- **No** - Next, ask your Global Administrator to add you as an App Catalog administrator.

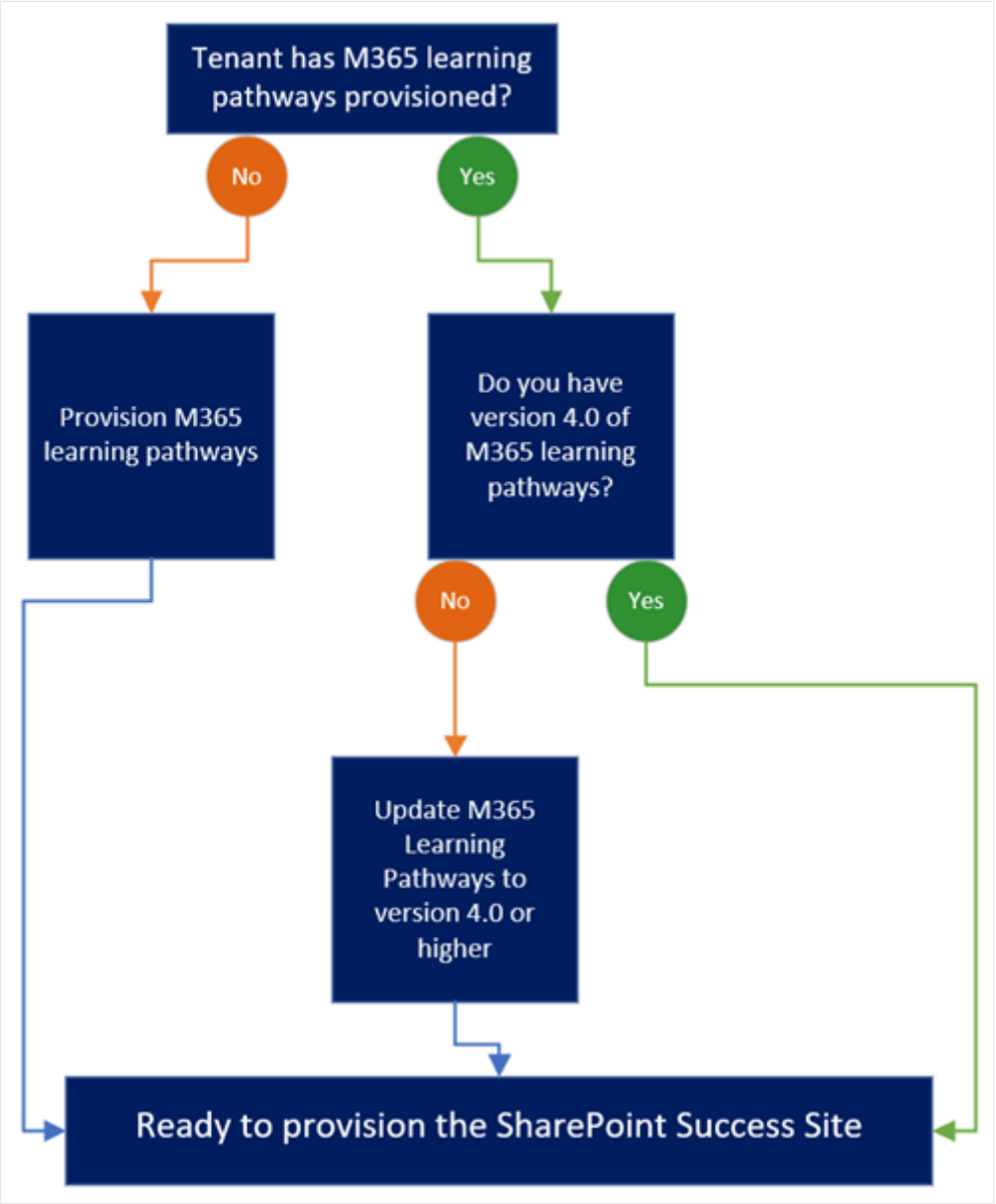
Tenant requirements

The **tenant** where the site is provisioned must have the App Catalog installed *and* have the latest version of Microsoft 365 learning pathways installed. Your tenant must have **version 4.0 or higher** of Microsoft 365 learning pathways.

Expand table

App Catalog installed	+	Microsoft 365 learning pathways 4.0 or higher installed	=	Tenant requirements met

Use this decision tree to determine your tenant's path to meeting the **tenant** requirements.



Ready to get started provisioning? Review the provisioning instructions.

Does your tenant have the App Catalog installed?

- **Yes** - Next, confirm you're an administrator of the App Catalog.
- **No** - Next, enable the App Catalog (this takes about 30 minutes).

If you're unsure, navigate to the SharePoint admin center, then select **Sites** > **Active sites**. The **App Catalog** appears in the list of sites.

> **Important**
>
> If you need to create a App Catalog, wait at least 30 minutes after creating before provisioning Microsoft 365 learning pathways and the SharePoint Success Site.

Does your tenant have Microsoft 365 learning pathways provisioned?

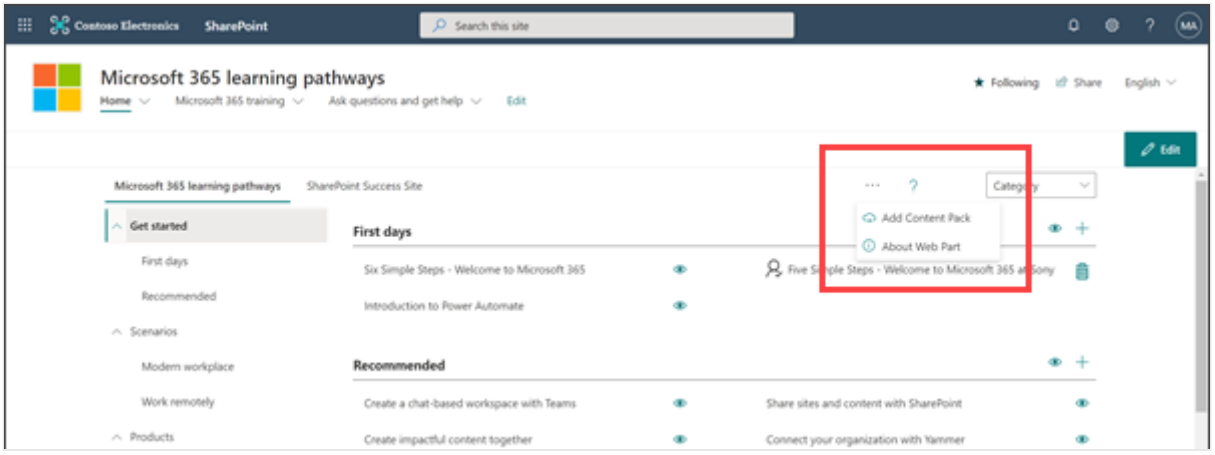
- **Yes** - Next, confirm you're using version 4.0 or higher.
- **No** - Provision Microsoft 365 learning pathways for the first time.

If you're unsure, navigate to the SharePoint admin center, then select **Sites** > **Active sites**. **Microsoft 365 learning pathways** appear in the list of sites.

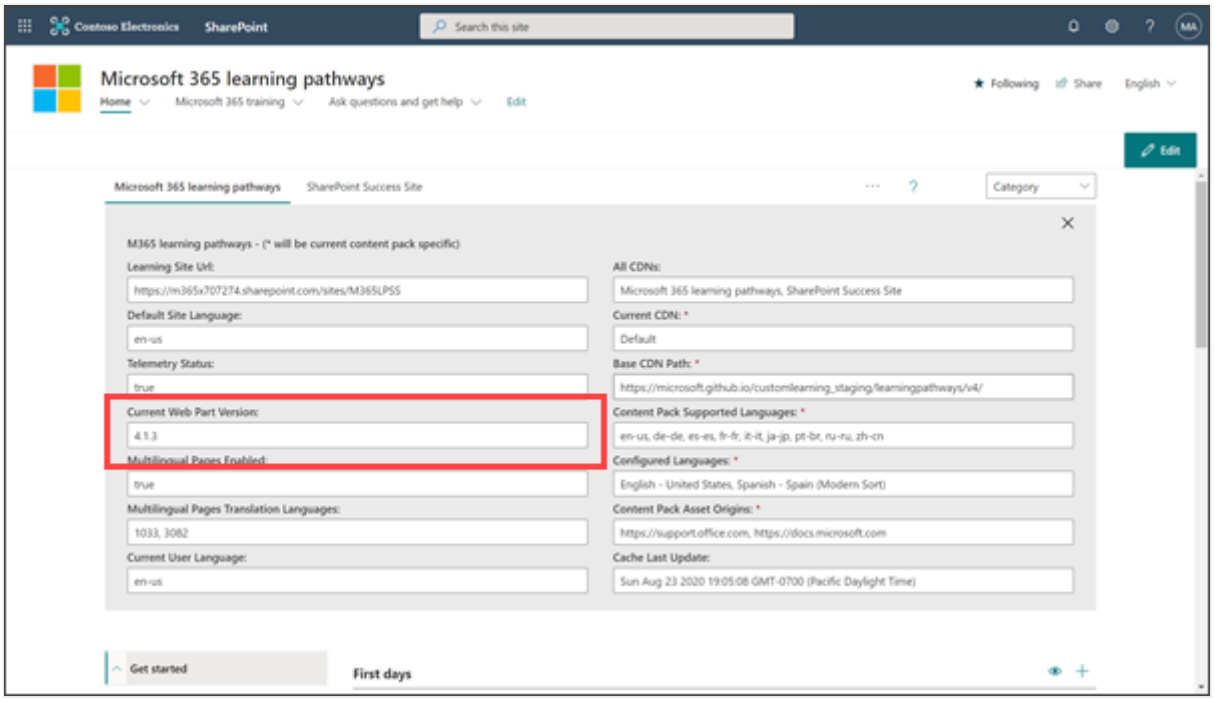
Is your tenant's version of learning pathways version 4.0 or higher?

- **Yes** - You're ready to provision the SharePoint Success Site.
- **No** - Update to version 4.0 or higher and then provision the SharePoint Success Site from the Microsoft 365 learning pathways administration page.

If you're unsure, navigate to your tenant's **Microsoft 365 learning pathways administration page** and select the ellipses **(...)**



Then, select **About web part** to confirm the current version.



If you need to, update Microsoft 365 learning pathways from version 3.0 to version 4.0 or higher

> **Important**
>
> The person updating Microsoft 365 learning pathways must be a site administrator for the App Catalog. If the person provisioning Microsoft 365 learning pathways isn't a site administrator for the App Catalog, add an administrator to the App Catalog and continue.

In this step, you upload the Microsoft 365 learning pathways 4.0 web part to the App Catalog, and then navigate to the Microsoft 365 learning pathways Administration page to start the update process.

Upload the web part package:

1. Go to the GitHub custom learning repository, and then download customlearning.sppkg to a local drive on your PC.
2. If you're not already signed in, sign into your tenant with a Global Administrator credentials.
3. Select **Admin** > **Show All** > **SharePoint** > **More Features**.
4. Under **Apps**, select **Open**.
5. Select **App Catalog** > **Distribute Apps for SharePoint**.
6. Select **Upload** > **Choose Files**.
7. Select the customlearning.sppkg file you downloaded, then select **OK** > **Deploy**.

8. From the Learning Pathways site, select Learning pathways administration from the Home menu.
9. You see a prompt asking if you want to update, then select **Start**.
10. When the update is complete, select **Close**.

Provision the SharePoint Success Site

Once you've confirmed the following, you're ready to provision:

- You're signed in as a Global Administrator.
- Your tenant has the App Catalog enabled.
- You're a site administrator for the App Catalog.
- Your tenant has version 4.0 or higher of Microsoft 365 learning pathways provisioned.

We recommend that you install the SharePoint Success Site by using the following steps. As an alternative, you can install the SharePoint Success Site from the look book, just make sure you follow all instructions. Before getting started, watch the provisioning instructions video.

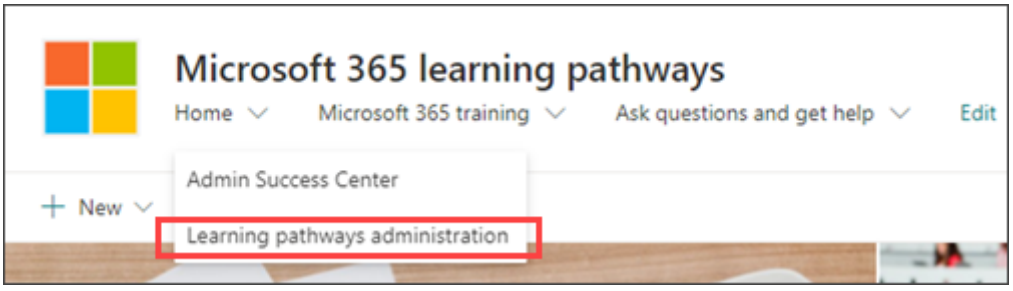
Provision the SharePoint Success Site to your tenant from the Learning pathways administrative page

1. Navigate to office.com or your organization's sign-in location.

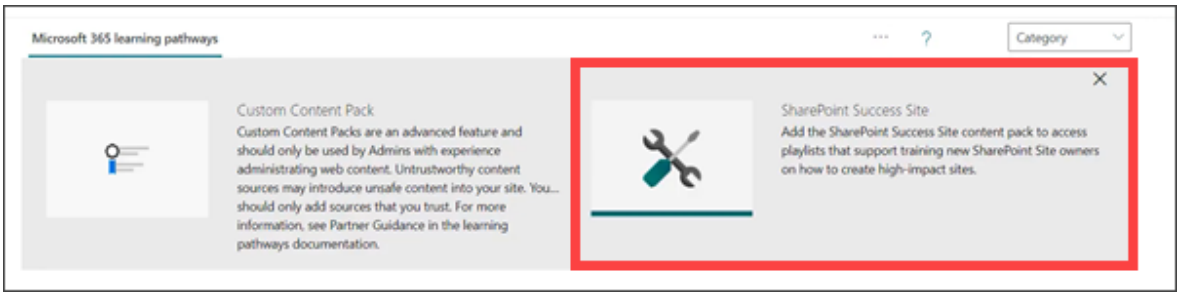
2. Sign in with your username and password.

3. Navigate to the location of the site using the URL supplied by your SharePoint Administrator or select SharePoint from the Microsoft 365 home page, and then select the **Microsoft 365 learning pathways** site.

4. From the learning pathways Home menu, select **Learning Pathways Administration**.



5. Select the ellipses **(...)** and then select **Add Content Pack**.



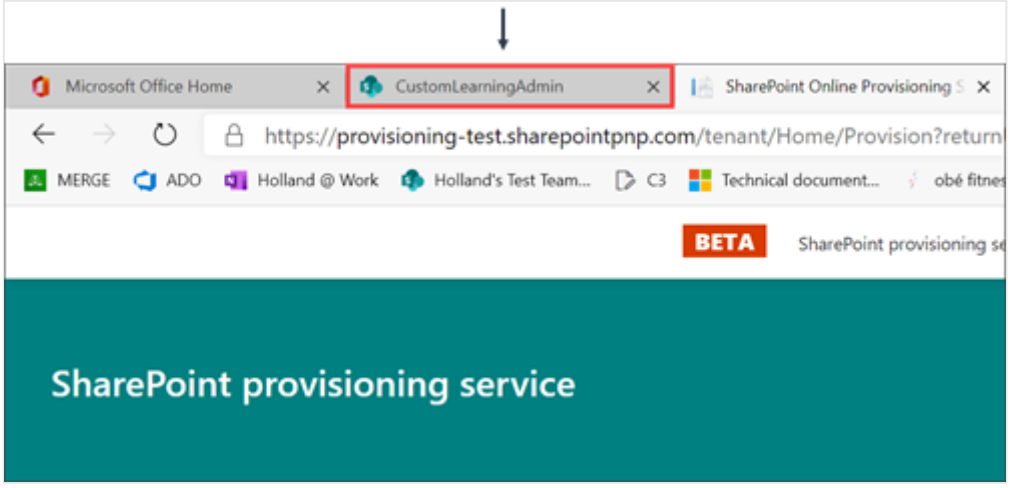
6. Select SharePoint Success Site to open the SharePoint Success Site provisioning page.

7. Select **Add to your tenant**.

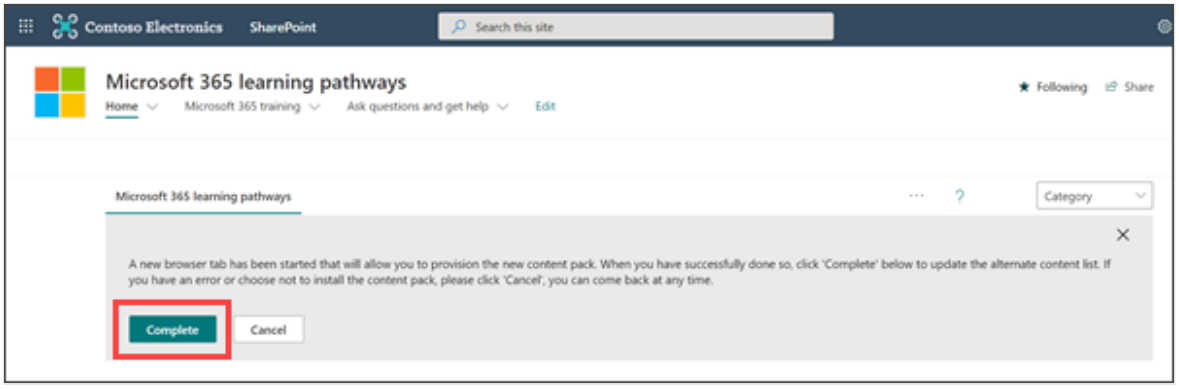
8. Fill out the email address and URL details and then select **Provision**.

9. Select **Complete**.

10. When you see **Provisioning completed** on the provisioning page, you see a new tab appear in your browser called **CustomLearningAdmin**. Select the **CustomLearningAdmin** tab as shown in the following image:



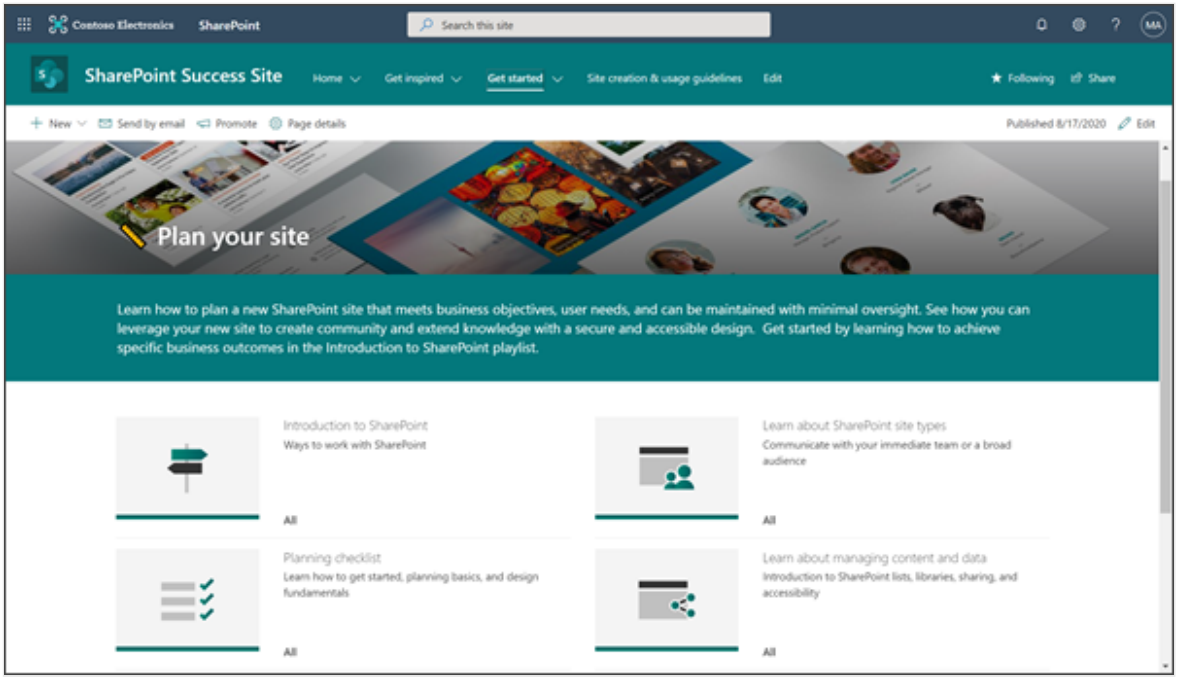
11. Then, select **Complete** as shown in the following image to complete the provisioning process:



> ⓘ **Important**

Make sure to select **Complete** to complete the provisioning process.

12. To confirm the SharePoint Success Site has been successfully provisioned, go to the SharePoint site you provisioned, select **Get Started** > **Plan your site.** You should see the web part on the page as shown in the following image:



Add Site owners

Assign a few Site owners to grant administrative privileges to customize the site and training content. In order to hide, show, or enable playlists, users need Site owner or Site member permissions to the Microsoft 365 learning pathways site. In order to edit the look, navigation, and site content, users need Site owner or Site member permissions to the SharePoint Success Site.

Add Site owners or members to both sites:

1. From the site select **Settings**, then select **Site permissions**.
2. Select **Advanced Permission Settings**.
3. Select **Site owners** or **Site members**
4. Select **New** > **Add users to this group**, and then add the people you want to be Site owners or Site members.
5. Include a link to **Explore the site** in the sharing message, and then select **Share**.

Next steps - customize the SharePoint Success Site

Share the URLs for the Microsoft 365 learning pathways administration site and the SharePoint Success site with the Site owners and members who are responsible for

customizing the site. Then, customize Microsoft 365 learning pathways playlist content and the look and feel of your SharePoint Success Site to meet the needs of your organization.

Site provisioning help

- Reference troubleshooting for provisioning help
- See Microsoft 365 learning pathways FAQs
- Share your feedback with us

Frequently asked questions

Question: What are the requirements for installing the SharePoint Success Site into my tenant environment?

Answer:

- Ensure SharePoint Online is enabled in your environment.
- The individual that provisions the SharePoint Success Site must be the Global Administrator of the target tenant for install.
- The tenant where the site is provisioned must have:
  - The App Catalog installed
  - Version 4.0 or higher of Microsoft 365 learning pathways installed

Question: Can I provision the site from the look book?

Answer: Yes, follow the guidance on how to provision from the look book.

Question: Who has permission to provision the SharePoint Success Site?

Answer: A Global Administrator.

Question: I have installed the SharePoint Success Site successfully, but I'm not able to get the Success Site content from the Microsoft 365 learning pathways web part loaded on my site. What should I do?

Answer:

It's likely that the content pack hasn't been fully installed. You must return to the **CustomLearningAdmin** page that will appear when site provisioning is done to complete the installation. Confirm you have followed steps 10 through 12 above. Review the provisioning video for more detail.

Question: Who has permission to customize the site template?

Answer: A SharePoint site owner and above.

Question: Who can create custom playlists and hide or show content in Microsoft 365 learning pathways?

Answer: A site collection administrator or site owner of Microsoft 365 learning pathways.

Question: Who has permissions to use the SharePoint Success Site as a user?

Answer: Any user or guest who has SharePoint site visitor permissions or higher.

Feedback

Was this page helpful? Yes No

Provide product feedback

Customize the SharePoint Success Site

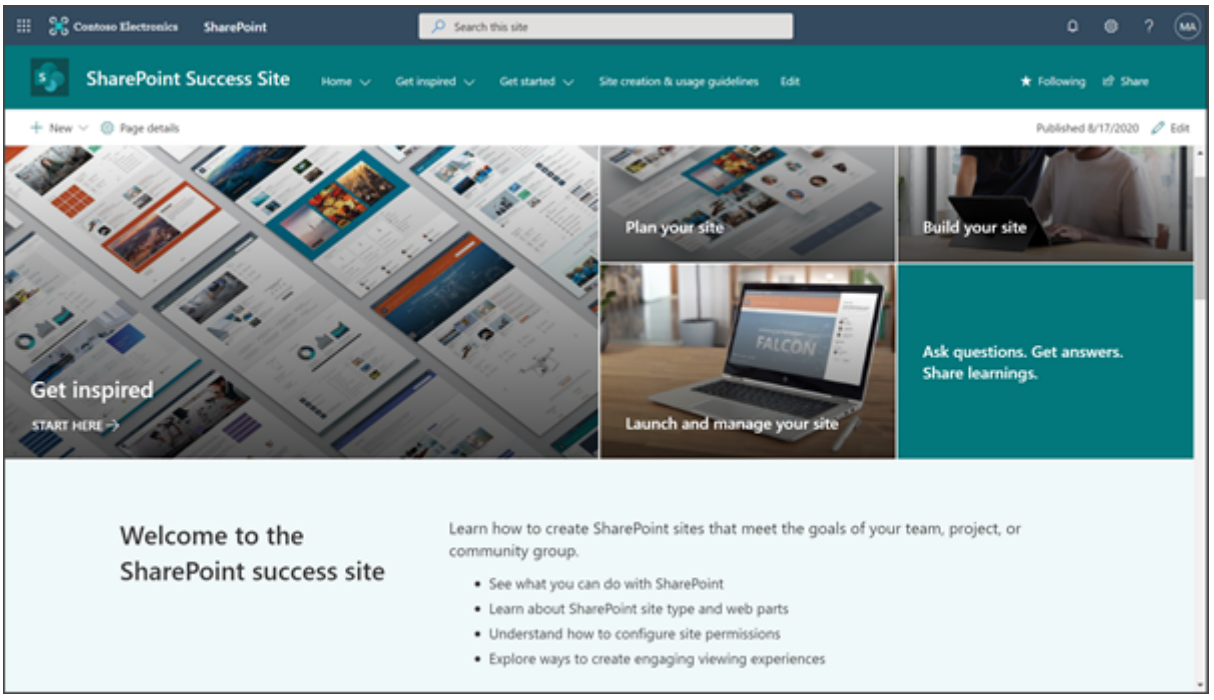
The SharePoint Success Site is a ready to deploy, up-to-date, and customizable SharePoint communication site that helps your organization maximize the adoption of SharePoint. The SharePoint Success Site helps end users improve the quality and impact of the sites they build for internal audiences, while helping ensure they follow your organization's site usage guidelines.

The SharePoint Success Site is prepopulated with web parts and content to guide your viewers through the most up-to-date SharePoint site creation training content. However, there are several opportunities to customize the experience to better suit your organization's goals and usage policy. Learn about what's included in a SharePoint Success Site, and then get started customizing.

> ⓘ **Important**
>
> You must have Site owner or Site member permissions to the SharePoint Success Site and the M365 learning pathways administrative page in order to make customizations..

The SharePoint Success Site consists of three parts:

1. **SharePoint communication site** - The site comes prepopulated with content and web parts that can be further customized to fit the needs of your organization.
2. **Microsoft 365 learning pathways** - Microsoft 365 learning pathways is a solution that enables you to use existing content produced by Microsoft, and the ability to create and enable your own training playlists.
3. **Up-to-date SharePoint training content feed** - Content in the SharePoint Success Site is updated by Microsoft as SharePoint evolves and can be customized to align with your organization's site creation policy.



Before you share the site with end-users

There are several customization opportunities to align the site content, look, and feel with your organization. Before you publish your site and share it with users, review and customize the following elements:

- Training content in Microsoft 365 learning pathways
- The SharePoint Success Site template
- The Viva Engage conversation, People, and Forms web parts
- Content in the site usage guidelines page
- Content in the success story page
- Branding details like the site logo and theme
- Navigational elements

Summary of site requirements and permissions

Before getting started customizing, ensure that the SharePoint Success Site has been set up by your SharePoint administrator. You need to be a Site owner or Site member for **both** Microsoft 365 learning pathways *and* the SharePoint Success Site in order to have permission to make site customizations.

If you're not sure your tenant has the site, contact your SharePoint administrator to verify that the SharePoint Success Site has been provisioned and ask for the Microsoft 365 learning pathways and SharePoint Success Site URLs. If you're the Global Administrator (formerly called the Tenant

admin) and Microsoft 365 learning pathways hasn't been provisioned, see the provisioning guidance.

Who has permissions to customize the site template?

Site member level permissions and above can customize the site template.

Who can create custom playlists and hide or show content in M365 learning pathways?

Site member level permissions and above can create custom playlists and hide or show content in M365 learning pathways.

Who has permissions to use the SharePoint Success Site as a user?

- Office 365 user permissions or SharePoint Site visitor permissions or higher

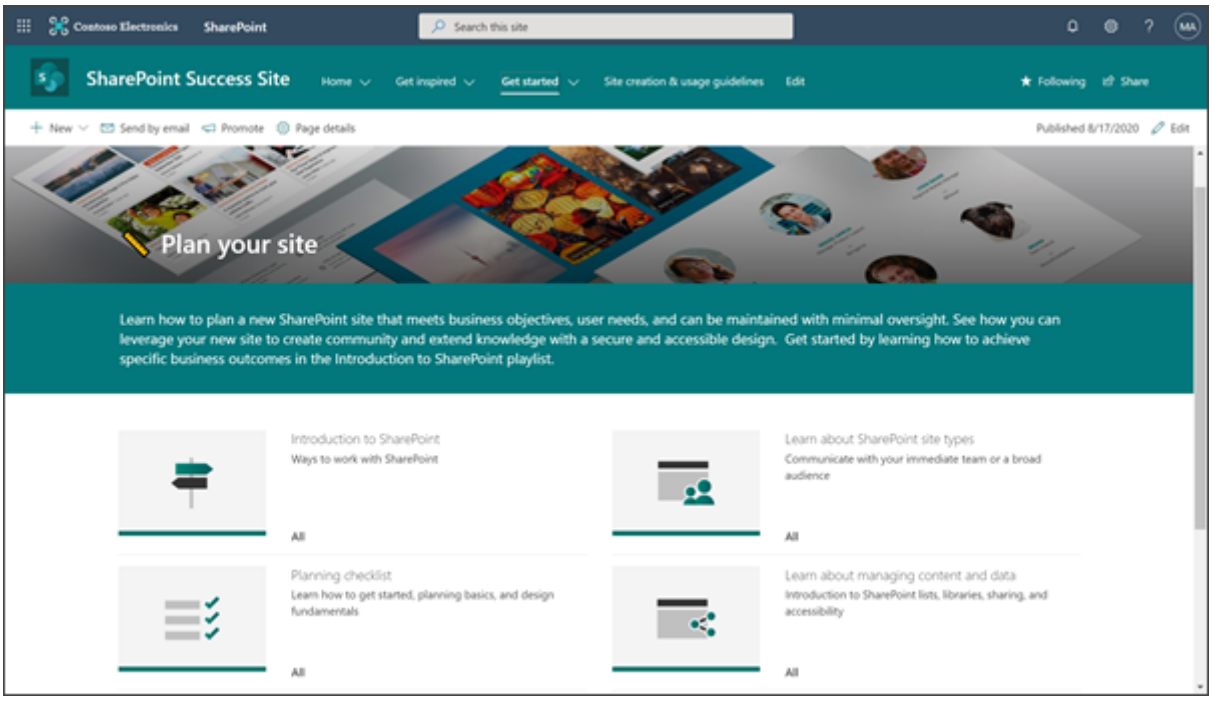
Get started customizing

Once you confirm the necessary access and permission to customize the site, you're ready to get started with the customization process. The SharePoint Success Site is hosted in your Microsoft 365 tenant, so you need to sign into Microsoft 365 and then navigate to the site.

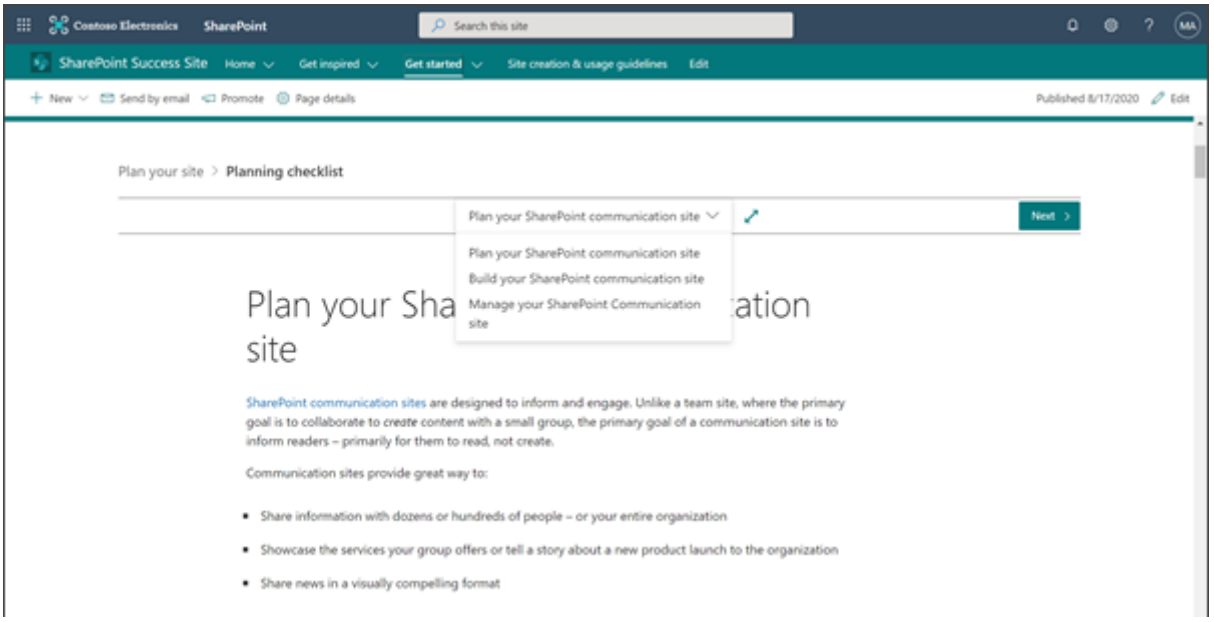
Sign in

1. Open a web browser and navigate to office.com or your organization's sign-in location.
2. Sign in with your username and password.
3. Navigate to the location of the site using the URL supplied by your tenant administrator or select SharePoint from the Microsoft 365 home page, and then select the **SharePoint Success Site**.

Explore and review the prepopulated training content



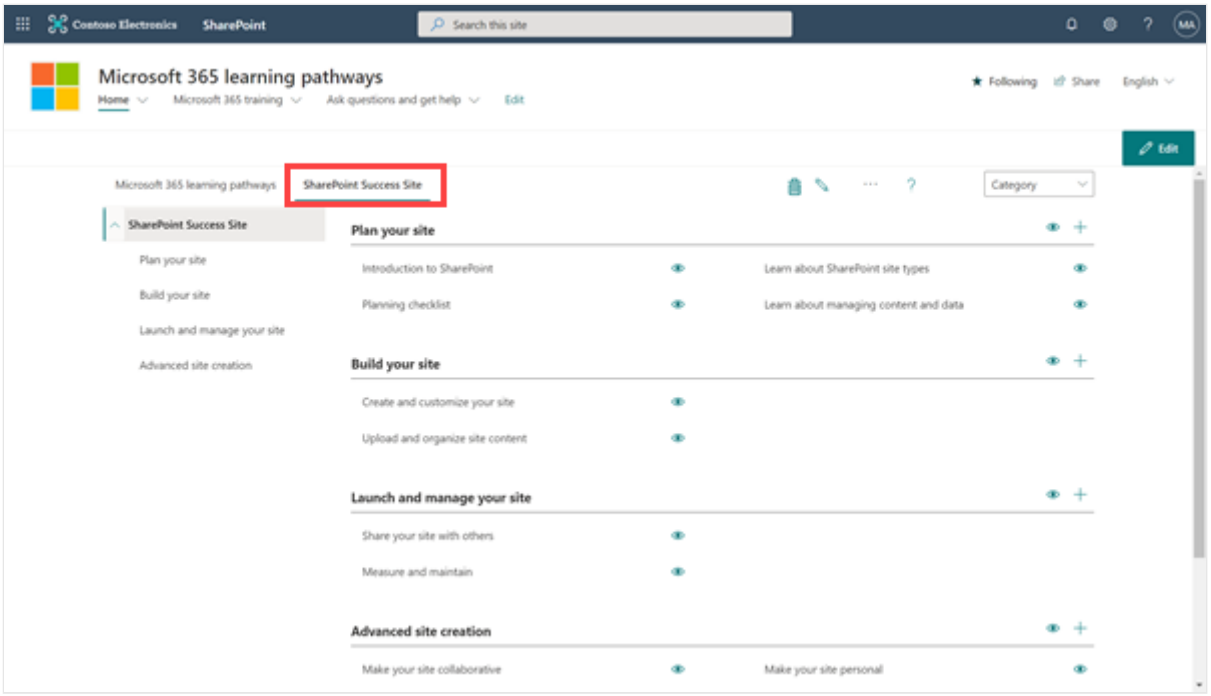
Review the **Plan, Build, Launch and manage, and Advanced** playlist sections to see the full suite of Microsoft curated content available in the SharePoint Success Site.



Select a topic, and navigate through content using controls at the top of the article

Select content categories and subcategories, and then navigate through the playlist using arrows and bread crumbs in the control bar to get a sense for how the SharePoint Success Site content is organized and displayed.

Customize playlist content



Navigate to the Microsoft 365 learning pathways admin page

1. Navigate to the Microsoft 365 learning pathways by selecting **Home** > **Administration**.
2. Next, select the **gear icon** in the web part.
3. Then, select **Home** > **Learning pathways administration**.
4. Select the **SharePoint Success Site** tab.

Show or hide sections to the playlist content

Select which content to display in your SharePoint Success Site by hiding and showing subcategories of content. For example, if you don't want users to have access to the Advanced site creation section, you can hide that subcategory so it won't be visible to end-users. Decide which content is appropriate for your SharePoint Success Site.

> **Important**
>
> Hiding playlists does not hide the associated page in the SharePoint Success Site, nor will adding custom playlists automatically create site pages for them. Add or delete pages within the site as needed.

Add your own custom playlists

With Microsoft 365 learning pathways, you can create custom playlists that are tailored to the unique needs of your organization. For example, create a playlist for team site integration with Microsoft Teams.

Customize the look and feel of your site

The following sections of the SharePoint Success Site can be customized to meet your requirements, prior to sharing with end users. There are several different ways you can make the SharePoint Success Site template your own. Customize the following elements of your site to fit the need of your organization:

- Update the SharePoint Success Site branding to align with your organization.
- Customize the Hero web part to include images of real sites in your organization where possible.
- Add web parts to your site as needed.
- Customize the page layouts as needed.
- Add new pages to more support or training resources.

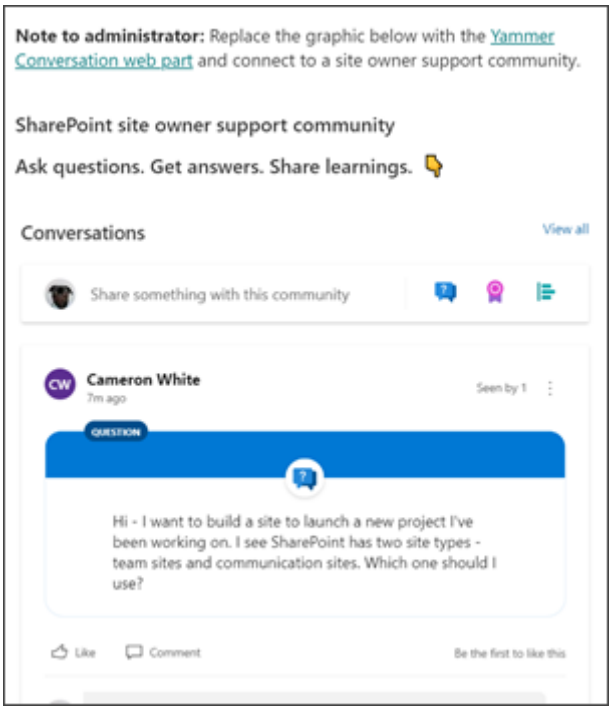
Customize the site navigation

As a Site owner you have full control of the site navigation. Use the following resources to help you make changes that align with business outcomes:

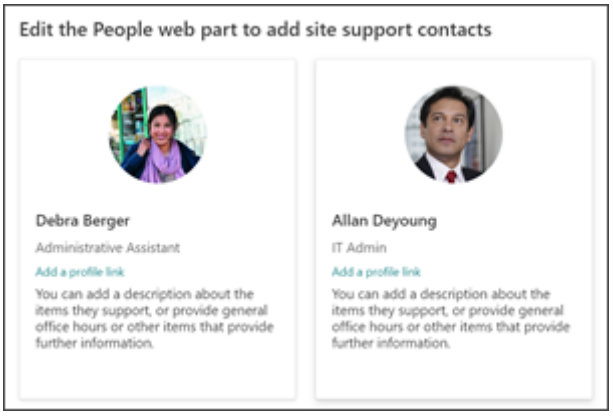
- Customize the site navigation.
- Associate this site with a hub.
- Use audience targeting to target specific navigational links to specific users. For example, in the **Home** navigation drop-down you see a shortcut to the Microsoft 365 learning pathways administration page. Target that page to Site owners for the SharePoint Success Site to prevent end-users from seeing it.
- Delete unwanted pages if you need to.

Customize specific web parts

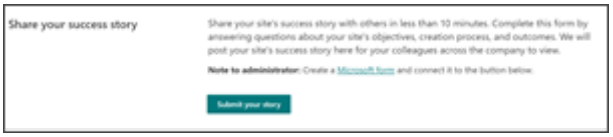
1. **Viva Engage conversations web part** - Use a Viva Engage web part to connect new SharePoint Site owners with extra support from current SharePoint Site owners and admins. Connect your Viva Engage community to the Viva Engage conversations web part.



2. **People web part** - Edit the People web part to display contact information so new Site owners can reach out for help.

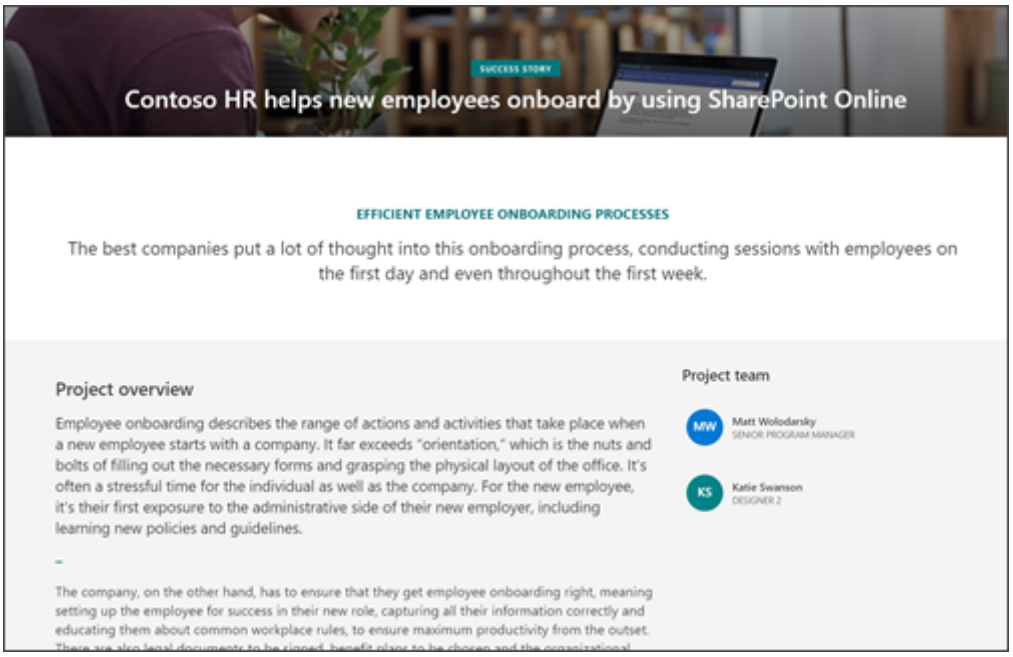


3. **Button web part** - Edit the Button web part to link to a Microsoft Form to collect success stories from Site owners. Consider using the Forms web part to embed a custom form that allows SharePoint Site owners to easily share their success stories.



Customize the Success stories page

The success stories section is a gallery for organizations to showcase internal SharePoint site success stories to inspire new Site owners with their site creation.



If available, add SharePoint success stories to your portal. If there are no ready-to-publish success stories, consider working with internal partners to create SharePoint successes by building high priority sites that align with business outcomes. Highlighting these "early wins" will help inspire others in the organization on the possibilities for using SharePoint themselves to achieve business outcomes.

Here are some sample questions to consider using in your form:

- Name of solution
- Project team members
- Who is the sponsor of the project?
- What Microsoft 365 technologies (for example, SharePoint, Viva Engage, Stream, Flow) were used as part of the solution?
- What were the reasons for building the SharePoint site?
- Provide a description of the solution
- What impact or results has the SharePoint site generated?
- What best practices for planning and implementing your solution would you recommend to other who are building their own SharePoint site?

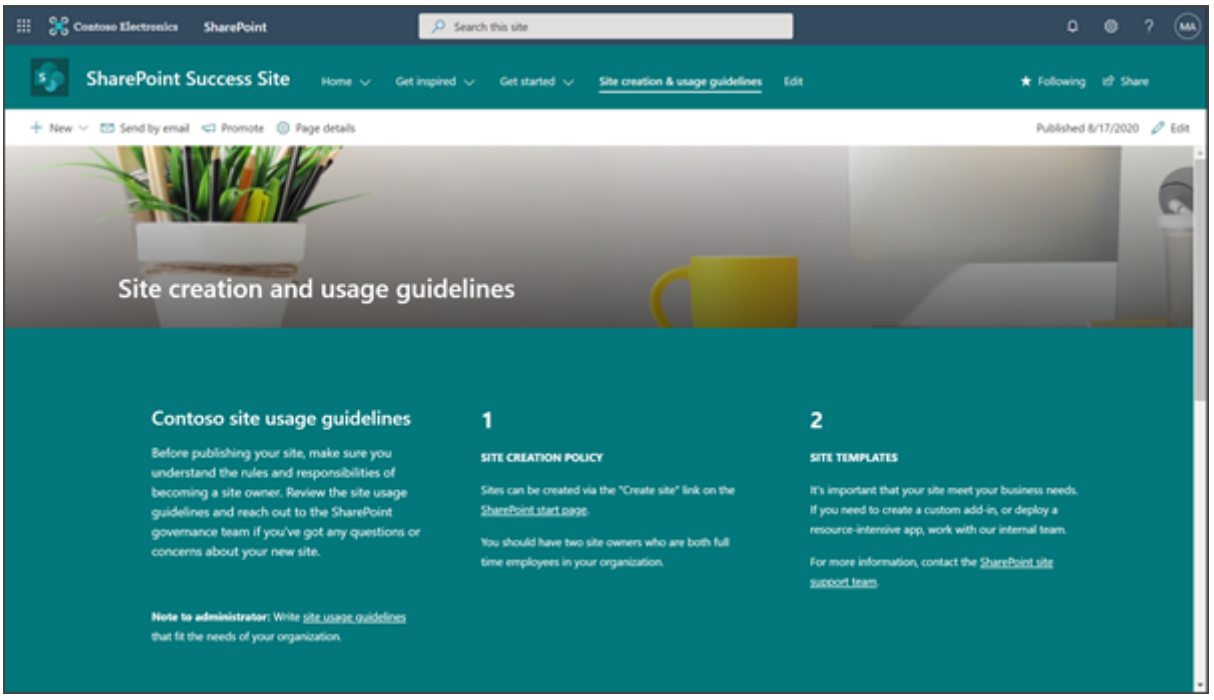
Learn more about how to create a form using Microsoft Forms.

Or, delete unwanted pages if you don't want to include this page in your site.

Customize the Site creation guidelines page

To ensure the proper use of SharePoint in your organization, it's important to communicate your site usage guidelines to new and existing site owners. This should include guidelines for how

people should create sites in your tenant, design standards, and how people should share information using SharePoint and Microsoft 365.



The example site creation and usage guidelines aren't intended to be a final policy document. Once you have created your own unique usage guidelines, remove the content from the Site usage guidelines page and replace it with your organization's usage guidelines. See how to create and use modern pages on a SharePoint site.

Create site usage guidelines that are appropriate for your organization by reviewing our site usage guidelines checklist that will help you create guidelines that:

- Inspire discussion and consideration among your stakeholders on important site usage policies.
- Provide links to resources that can help you better understand the options related to key policy decisions.
- Provide sample text to get you started in creating your own policies.

Here are some topics to consider as you create your own site creation and usage guidelines:

- How to get a new SharePoint site
- Guidelines for using site templates
- Site design, branding, and customization
- Rules for sharing and permissions
- Capacity guidelines
- Site lifecycle management policies

Provide contact information for SharePoint support

If your organization has an intranet team to support site owners, consider profiling the intranet team members on the SharePoint Success Site homepage using the People web part. The home page of the SharePoint Success Site has a People web part you can use to add your own Intranet team. If you don't a dedicated team supporting site owners, remove the current People web part.

Share the site with end-users

Share your site with others. Partner with others in your organization to ensure the SharePoint Success Site is widely known and adopted.

Key success factors to managing the SharePoint Success Site:

- Celebrate the launch of your SharePoint Success Site.
- Create and post news announcing the new resource.
- Ensure users have an outlet for questions and feedback.
- Plan to review the SharePoint Success site as needed to ensure content and site usage policies are still relevant.
- Build culture and community by integrating a Viva Engage web part.
- Integrate and customize your organization's high-value training content.

Adoption and awareness strategy

To help build, grow, and sustain your SharePoint adoption efforts, it's recommended to create a SharePoint user group community in Viva Engage. Your SharePoint champions and power users can answer SharePoint related questions posted in the Viva Engage group and encourage site owners to share their successes and best practices. See the champions guidance for more information on how to identify and build a successful champions program.

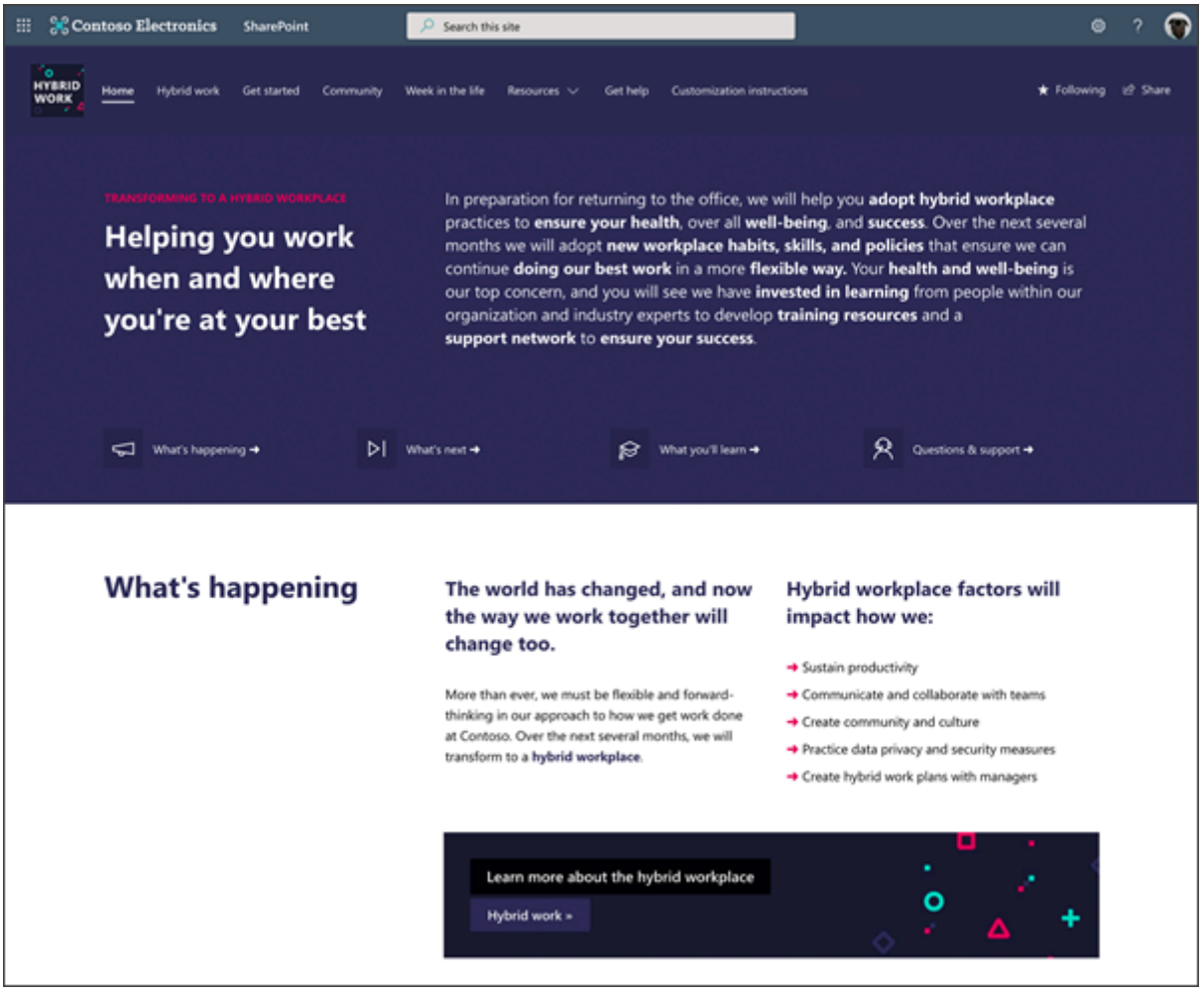
To increase visibility and engagement within your portal champions community, integrate the Viva Engage group hosting your community into the SharePoint Success Site using the Viva Engage conversations web part.

Last updated on 07/01/2026

Overview of the Workplace transformation site

Help your organization drive and manage change by using the Workplace transformation site template in SharePoint. The site template helps organizations to successfully manage the people side of their organization change management initiatives to ensure all impacted employees are informed, have support, and know where they can learn more about upcoming changes.

The Workplace transformation site template is designed help people in your organization understand and engage in the change management process by providing a landing place using a SharePoint communication site in combination with Microsoft Lists to help users see the big picture. The site design is based on change management research that is focused on helping organizations successfully adopt and sustain change.



The Workplace transformation site template helps organizations:

- Inspire employees on the new possibilities' your change management project offers

- Provide employees with the information, resources, and support they'll need to successfully adopt new ways of working
- Ready employees for a successful transition to new processes, tools, and expectations

The Workplace transformation site features:

- A landing place for people in your organization to get more information, news, and support
- Specialized support channels for many audiences like managers, teams, and champions
- Prepopulated content and web parts that can be customized to fit the needs of your organization and specific change management projects
- Opportunity to use the Microsoft 365 Learning pathways solution to display Microsoft-curated and maintained training playlists
- Integration with Microsoft 365 lists that let you customize and manage the change management journey
- Examples of micro-learning content that can be adapted to your change project

How to use the Workplace transformation site template

The Workplace transformation site can be used to drive any article or scope of organizational change. The site template helps organizations to successfully manage the people side of their organization change management to ensure all impacted employees are informed, have support, and know where they can learn more about upcoming changes.

Examples of the types of change projects that could benefit from the workplace transformation template:

- **New process –** Communicate and manage changes to data security policies, new contract management workflows, or project intake processes.

- **Merger and acquisition –** Onboard new employees and help current employees understand what to expect and how to work together.

- **New systems –** Roll out a new employee benefits program, or help employees adopt new tools and apps.

Site design is based on a proven change management model

Phases of change management:

1. Awareness and commitment – Start communicating details about upcoming changes with users and provide various support channels and opportunities to engage through events and Viva Engage community chats.

2. Learn – Build training content right into the site itself by using Microsoft 365 Learning pathways.

3. Practice and exploration – Use your organization's champion community in leading hand-on events and demonstrations in addition to 1:1 help.

4. Use and consult – Use Microsoft Lists to help your organization manage tasks and knowledge checks associated with training and change management objectives.

5. Sustain – Help users practice and sustain new skill set and habits by using micro-learning content like quick tips and publishing regular news posts sharing change management success stories.

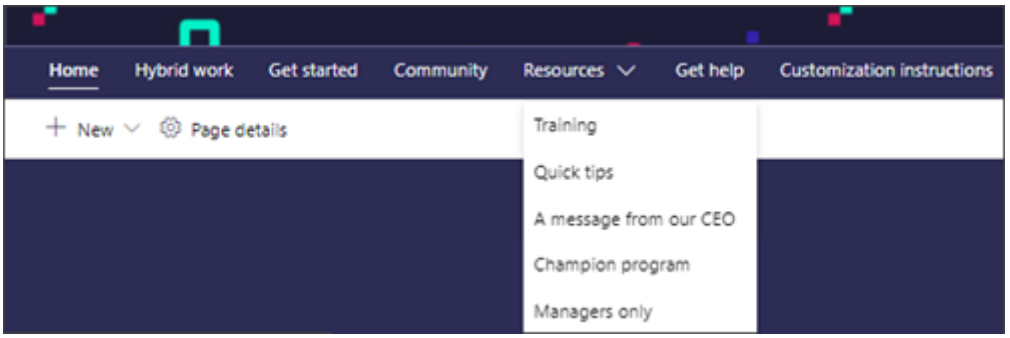
Prepopulated content focuses on the hybrid workplace

The workplace transformation site features prepopulated content that revolves around helping organizations transition to a hybrid workplace. The hybrid workplace is one that is flexible when and where people do their work. Many organizations plan to allow employees to work from home up to 50% of the time, which means the organization needs to adopt new ways of working to ensure wellbeing and productivity.

Learn more about the future of work and what we have learned about remote work so far.

Overview of the site contents

The workplace transformation site is full of prepopulated content, web parts, news templates, and a Microsoft List. Carefully review and customize prepopulated content before sharing broadly with end users.



- **Home page –** Help employees easily understand "what's in it for me?" right away by providing a landing place for employees to learn more right away about why the change is happening and how it impacts their day-to-day work.
- **Hybrid work –** Explain in more detail what is changing and what success will look like when change is adopted and sustained.
- **Get started –** Give employees a jumping-off place to dive into messages from leadership, view the change management checklist, and RSVP to an upcoming event.
- **Community –** Help recognize and celebrate success within the organization and give employees and opportunity to connect in a change management Viva Engage community.
- **Training –** Embed curated training playlist that can be easily viewed and bookmarked on any device.
- **Quick tips –** Create micro-learning opportunities to help employees adopt and sustain new skills.
- **A message from our CEO –** Unite the organization around a central change by sharing a recording or written message from leadership endorsing the change project.
- **Champions program –** Recruit subject matter experts into your champions program.
- **Managers only –** Provide special resources and support that managers may need around the change project that can be audience targeted to a specific security group.
- **Get help –** Make sure employees know where to go for support and have more than one option for getting 1:1 help or learning from others.

Considerations for Microsoft 365 Learning Pathways

Microsoft 365 learning pathways is a customizable, on-demand learning solution that displays playlists using the Microsoft 365 Learning pathways web part right onto SharePoint pages.

Consider using the Microsoft 365 Learning pathways solution in combination with the workplace transformation site to embed training playlists on SharePoint pages.

Learn more about how to provision the Microsoft 365 learning pathways solution for the first time, how to find Microsoft-maintained content packs, and how to customize learning pathways and playlists.

Step 1: Provision the Workplace transformation site template

> **Note**
>
> - Tenant administrators' credentials (or higher) are required to provision a template.
> - The workplace transformation site will take about 15 minutes to provision.

Start by navigating to the custom PnP site templates and select the Hybrid work PnP template. Follow the instructions to provision the PnP template.

Learn more about provisioning site templates.

Share the site with site owners and members to customize

Once the site has been provisioned and you're ready to customize. If other people from your organization are making site customizations, make sure you share the site add them as site owners and site members to ensure they have access and the right permissions to make edits to site content, theme, navigation, settings, and permissions.

Step 2: Customize the Workplace transformation site

Customize the workplace transformation site to fit the needs of your organization's change management project. Customize the theme, logo, navigation, web parts, and prepopulated content.

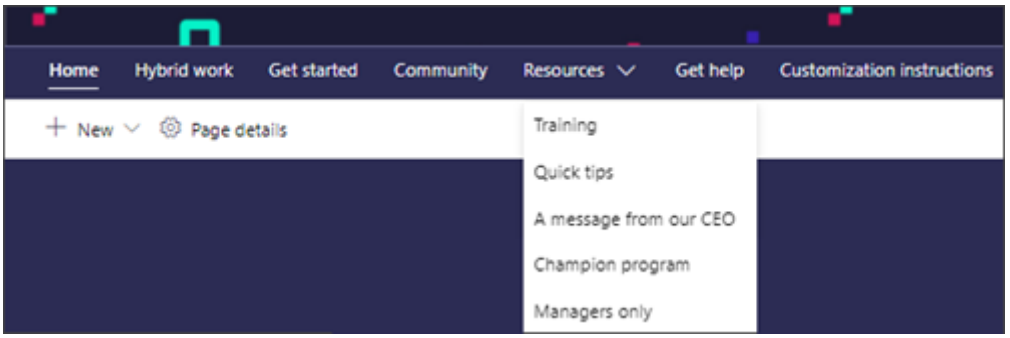
> **Note**
>
> You need site member (or higher) permissions to the Workplace transformation site template in order to make customizations.

Sign in

1. Open your web browser and navigate to office.com or your organization's sign in location.
2. **Sign in** with your username and password.
3. Navigate to the location of the site using the URL supplied by your tenant admin, or select SharePoint from the Microsoft 365 home page, and then select the **Workplace transformation site**.

Review prepopulated content

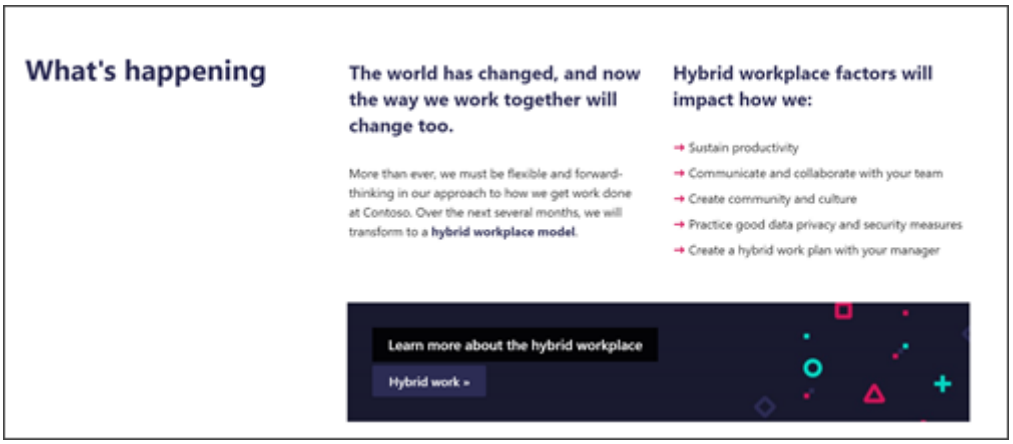
The workplace transformation site is full of prepopulated content, web parts, news templates, and a Microsoft list. Carefully review and customize prepopulated content before sharing broadly with end users.



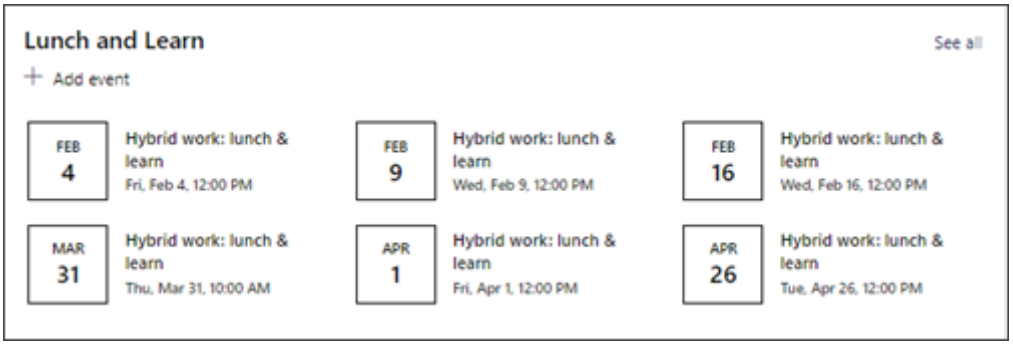
The workplace transformation site features prepopulated content that helps organizations transition to a hybrid workplace. However, the workplace transformation site can be customized for any change management project. Learn more about the workplace transformation site features and contents.

Customize web parts and content

Learn how to customize web parts and content that will appear on certain pages or throughout the site.

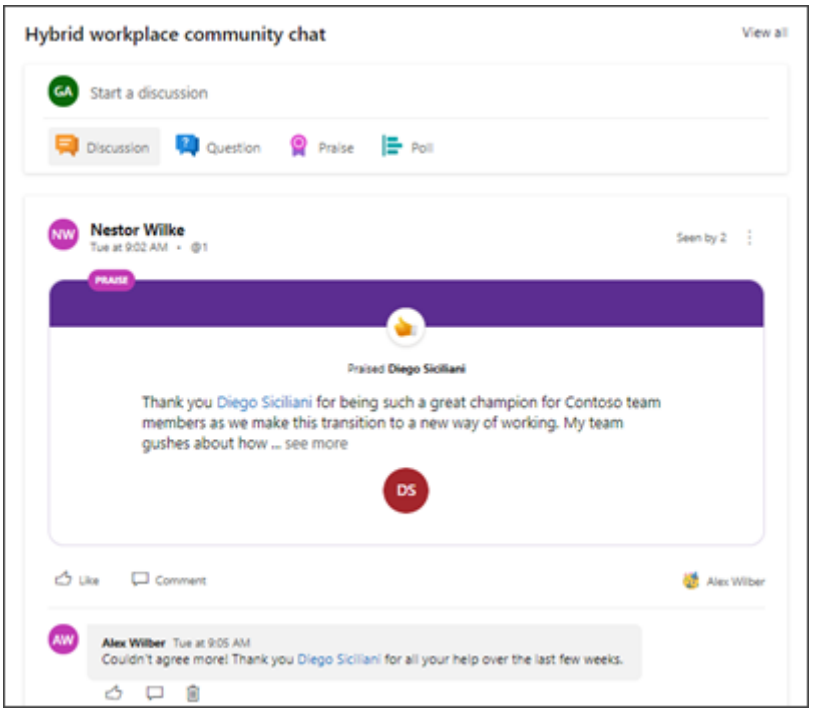


Text, labels, and buttons - Edit the labels and links in the Text web parts and Call to Action web parts throughout the site.

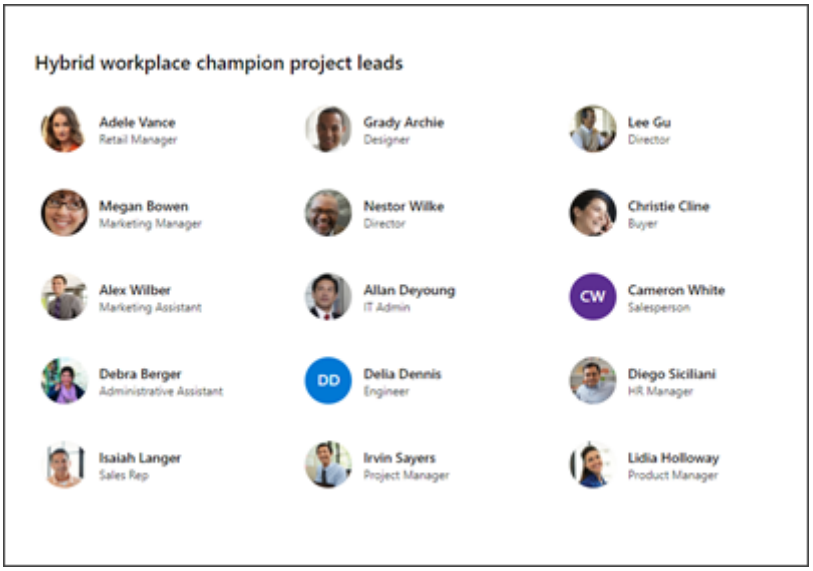


Events- Add, edit, and delete events in the Events web parts on the **Home** and **Get help pages**.

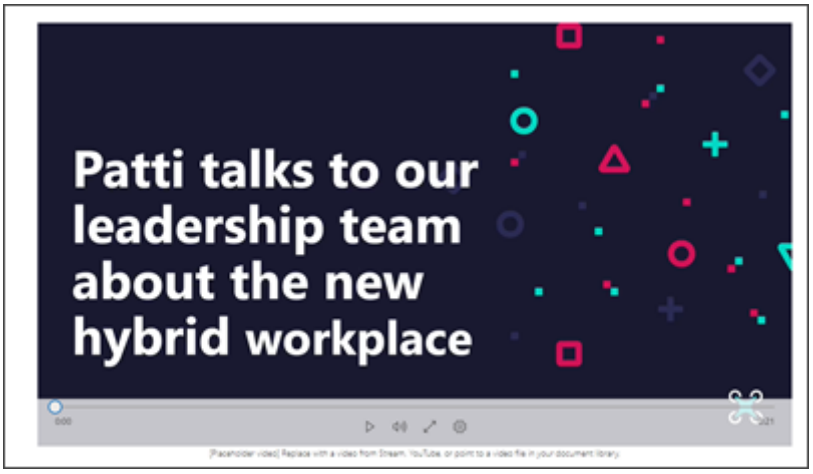
News and news post templates - Use prepopulated news templates to create news posts in the News web part on the **Community page**. Find the templates by navigating to **Setting** > **Site Content** > **Site pages** > **Templates**.



Viva Engage - Replace the graphic and connect the Viva Engage conversations web part on the **Community** page with an existing Viva Engage community.

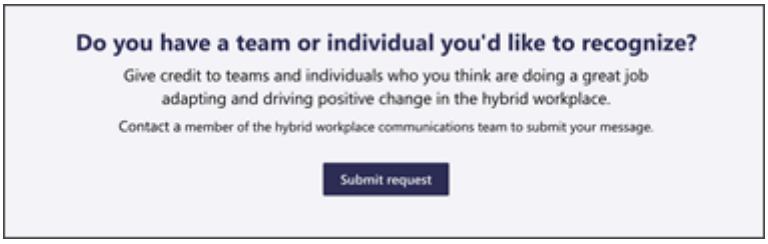


People - Edit People web parts in news post templates and on the **Get help** page.



Video - Edit the Embed web part on the **Message from our CEO** page to point to a YouTube video or an intranet video link. Use the Stream web part to display an existing Stream video.

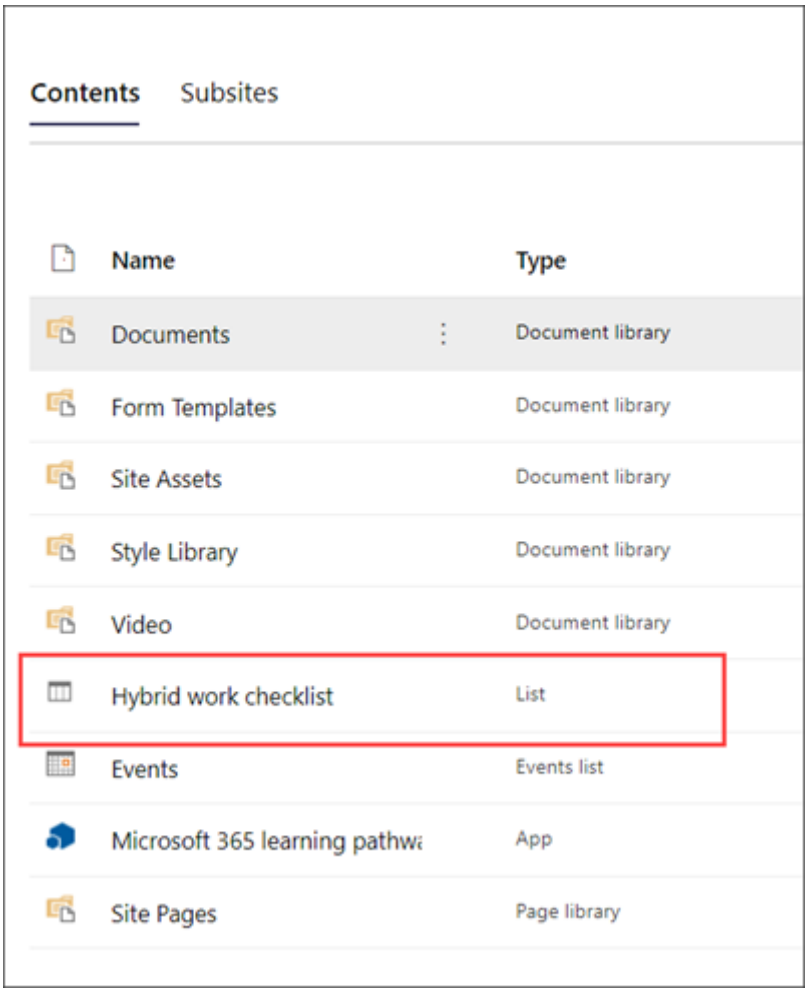
Use Microsoft Forms to facilitate news post requests



Edit the Button web part on bottom of the **Community** page to give users an opportunity to engage and acknowledge others. Connect the Button web part to a Microsoft Form where users can submit nominations. Then, use the prepopulated news post templates in **Settings** > **Site contents** to publish news.

Edit the change management checklist

The Workplace transformation site contains a Microsoft List in **Site contents** that is displayed in a List web part on the **Get started page**. This list is intended to give end users a high-level view of what to expect through the change management journey. Edit the list to meet the need of your change management project.



1. Start by navigating to **Setting** > **Site contents**, and then select **Hybrid workplace checklist**.
2. Then you can edit list items, change columns and labels, the theme and more. Or, you can create a new list based on an existing Excel spreadsheet or use a list template.
3. Finally, edit the view of your list to make sure users see the most important information in the List web part on the **Get started page**.

Learn more about Microsoft 365 lists.

Use Microsoft 365 learning pathways to embed training content on a page

If your tenant admin has set up Microsoft 365 Learning pathways, you can add pages to the site and use the Learning pathways web part to display custom training playlists. Then, use Learning pathways reporting capabilities to measure content impact.

Use tools to help target content to specific audiences or protect content from specific audiences

Consider using audience targeting to surface important content to specific groups or use information barriers to protect sensitive information that may appear in the **Managers** section under **Resources**.

Update the site theme and branding

Edit the look of your site to align with your organization's brand. Customize the site display name, logo, theme, header layout, navigation style, and more in the Change the look panel.

Customize site navigation

Site navigation is important because it helps users immediately understand what can be accomplished on a given site. The most effective SharePoint sites help viewers find what they need quickly so that they can use the information to make decisions, learn about what is going on, access the tools they need, or engage with colleagues to help solve a problem. Learn how to edit site navigation.

Step 3: Share the Workplace transformation site with end users

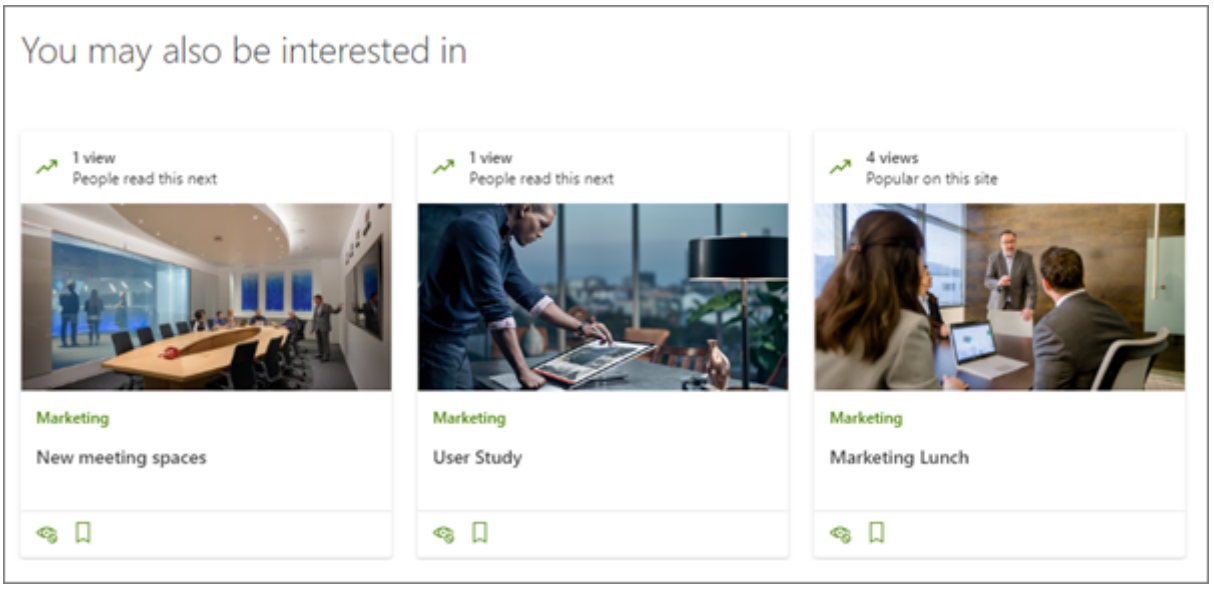
Once the site has been customized and republished, it's ready to share with end users.

1. Select **Share site** from the right-hand corner.
2. In the **Share site** pane, enter the names of people or groups to add them to the site, or enter "Everyone except external users" to share the site with everyone in your organization.
3. Change the permission level (Read, Edit, or Full control) as needed.
4. Enter an optional message to send to the person or clear the **Send email box** if you don't want to send an email.
5. Select **Share**.

Last updated on 06/24/2026

How SharePoint page recommendations work

SharePoint recommendations on modern pages help you and your users discover pages and news in your organization. At the bottom of news posts and pages, you see recommendations especially for you or your users. Recommendations show below the heading **You may also be interested in**.



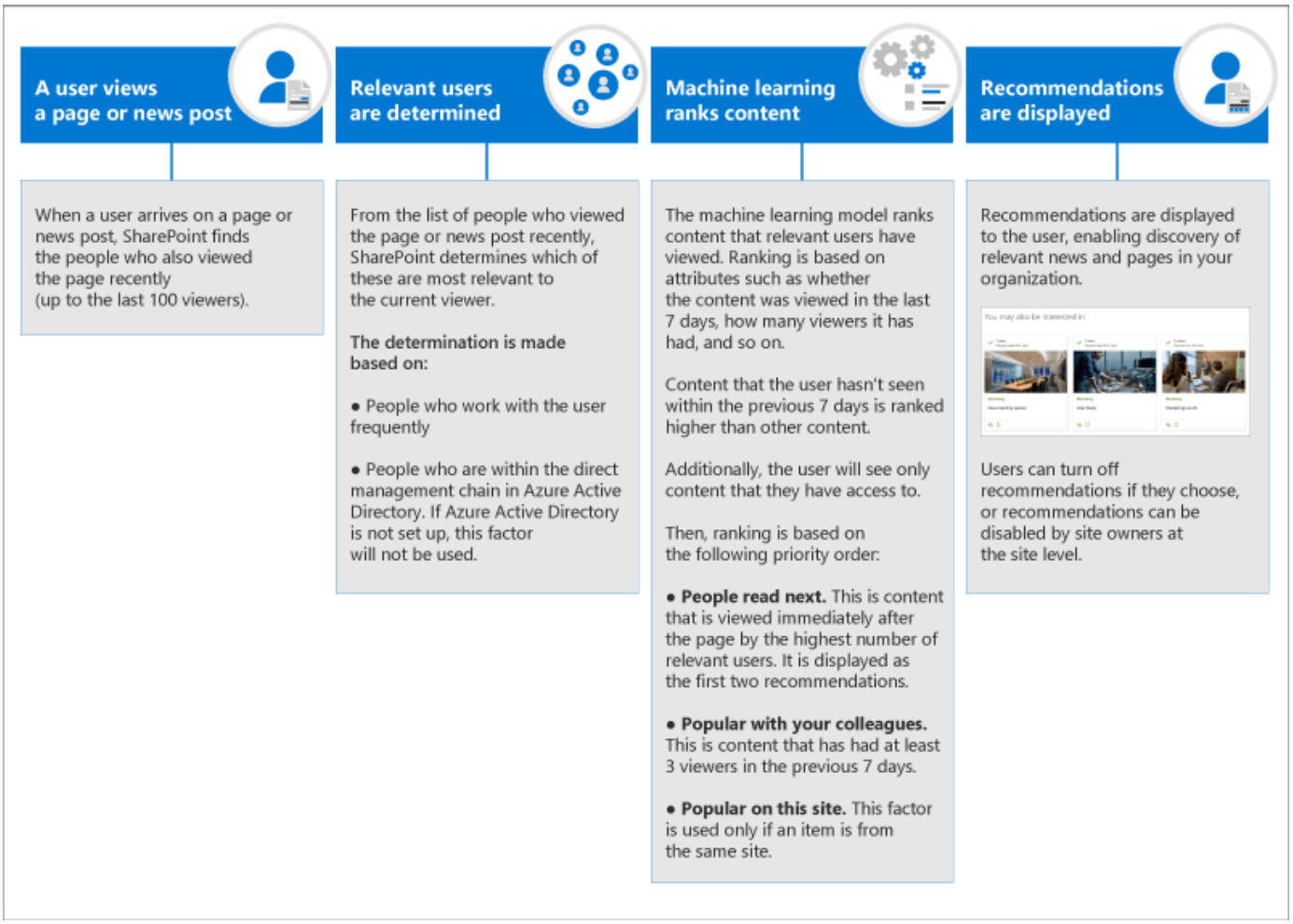
> **Note**
>
> This feature is in an early release phase, and is not yet available to all users.

Recommendations are shown on all newly created pages and news posts by default.

How are recommendations determined for each user?

The recommendations that users see on their pages are based on what their colleagues have read next; what is popular with their colleagues; and what is popular on the site. Only pages and posts that users have access to are shown.

Here's a diagram that shows how recommendations are determined in more detail (scroll down for a text version of this diagram):



How to disable recommendations

To learn how to disable at the page and site level, see SharePoint page recommendations.

In the article linked above, you'll learn the three different ways to hide or disable recommendations:

- Users can hide individual recommendations
- Page authors can turn off recommendations for the pages they create
- Site owners can disable recommendations at the site level

Recommendations can't be disabled for an entire tenant.

How are recommendations determined for each user? (Text version)

This is a text version of the diagram above.

A user views a page or news post When a user arrives on a page or news post, SharePoint finds the people who also viewed the page recently (up to the last 100 viewers).

Relevant users are determined From the list of people who viewed the page or news post recently, SharePoint determines which of these are most relevant to the current viewer. The determination is made based on:

- People who work with the user frequently
- People who are within the direct management chain in Microsoft Entra ID. If Microsoft Entra ID isn't set up, this factor won't be used.

Machine learning ranks content

The machine learning model ranks content that relevant users have consumed according to various attributes, such as whether the content was viewed in the last seven days, how many viewers it has had, and so on. Content that the user hasn’t seen within the previous seven days is ranked higher than other content. Additionally, the user sees only content that they have access to Then, ranking is based on the following priority order:

People read next. This is content that is viewed immediately after the page by the highest number of relevant users. It's displayed as the first two recommendations.

Popular with your colleagues. This is content that has had at least three viewers in the previous seven days.

Popular on this site. This factor is used only if an item is from the same site.

Last updated on 06/25/2026

SharePoint brand center

Article • 04/18/2025

The SharePoint brand center offers a centralized branding management application that empowers your brand managers or designated brand owners to help your organization to customize the look and feel of their experiences.

With this new brand asset management system, you can handle your colors, fonts, and images, and other assets all in one place.

What is the brand center?

The brand center uses the SharePoint Organization Asset Library (OAL) to store and manage assets in the background. The brand center app is located in a designated site within your tenant.

> **Note**
>
> The SharePoint brand center currently only allows one brand center for your organization, and the Global Administrator sets it up.

The brand center app lets you access and manage your organization's brand assets from one central place. By using the brand center app, you can make sure that your organization's brand identity is coherent and professional in all your communication channels. You can also save time and resources by avoiding duplication and confusion of brand assets, and by empowering your employees to create high-quality branded content.

Setting up the brand center

To enable the new brand center the global administrator needs to perform a set of simple steps in the Microsoft 365 admin center to create/activate the Brand center app. The brand center app requires the use of Public CDN.

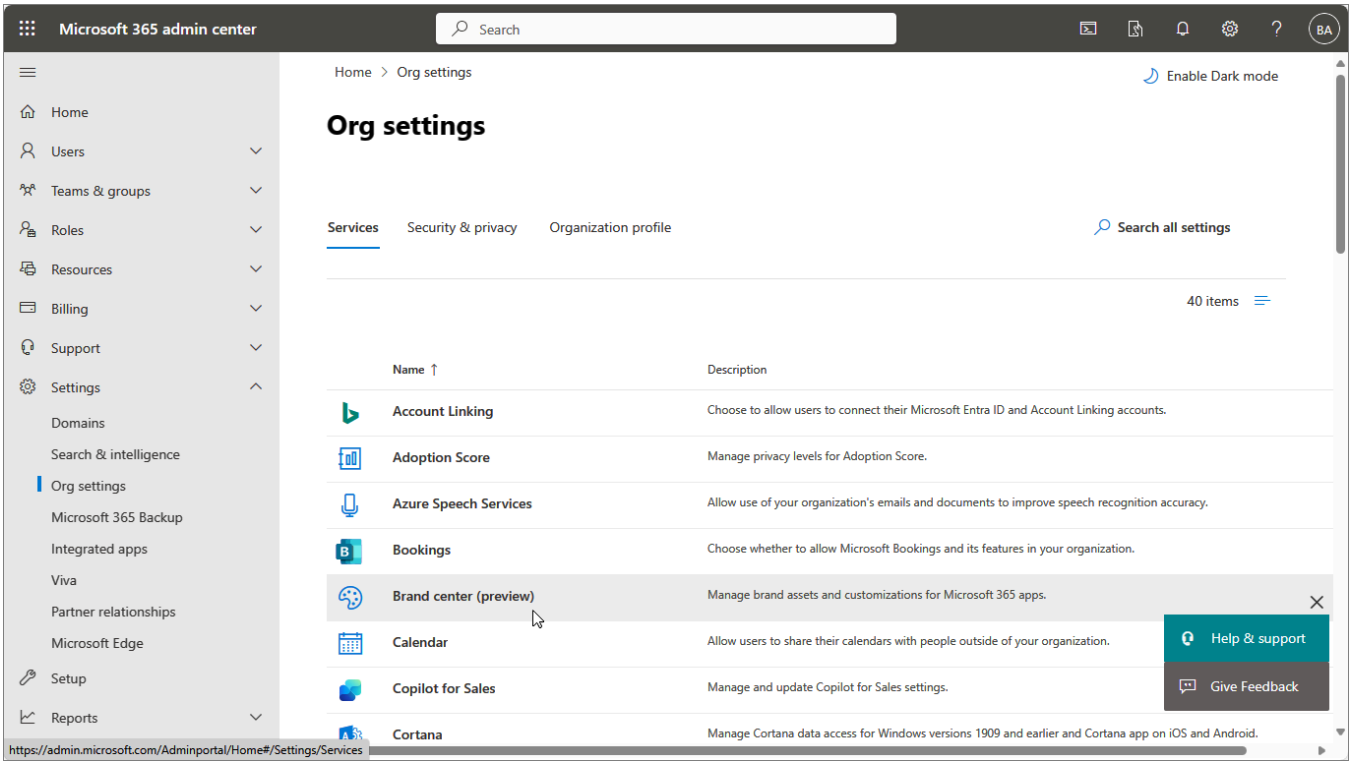
The brand center administrative experience finds the site that has your organization’s existing organization asset libraries if you're using them and base your brand center on this site. If you aren't using the organization asset library feature, we'll prompt you to make a new site to be your brand center.

When you turn on the SharePoint brand center for your organization, this lets you use the custom fonts feature in SharePoint and Viva Connections. You can find more details in the Message Center post for Custom Fonts.

To enable the SharePoint brand center, the global administrator needs to perform a few simple steps in the Microsoft 365 admin center to create/activate the Brand center app.

The steps required depend on your current tenant configuration. The following describes steps you need to do for each of the three scenarios:

- Scenario 1: Your tenant doesn't currently utilize the SharePoint Organization Assets feature.
- Scenario 2: Your tenant uses the SharePoint Organization Assets feature with Private CDN.
- Scenario 3: Your tenant uses the SharePoint Organization Assets feature with Public CDN.



Scenario 1: Your tenant doesn't currently utilize the SharePoint Organization Assets feature.

For this scenario, the global administrator performs the following steps to create the Brand center app.

1. In the admin center, go to **Settings** > **Org settings**.
2. Select **Brand center**.
3. Choose site name for the Brand Center site – Suggested “Brand Guide”.
4. Read and give consent to the use of Public CDN in your tenant for the Brand center.
5. Create the site and configure Public CDN in your tenant.

6. Add site owners to the Brand center site you created and share the link to the site to those owners to unlock the Brand center app.

Scenario 2: Your tenant uses the SharePoint Organization Assets feature with Private CDN.

For this scenario, the global administrator performs the following steps to create the Brand center app.

1. In the admin center, go to **Settings** > **Org settings**.
2. Select **Brand center**.
3. The Brand center recognizes your existing organization assets site location and will utilize this as the location for the Brand center app.
4. Read and give consent to the use of Public CDN in your tenant for the Brand center.
5. Activate Public CDN in your tenant.
6. Copy and share the link to the Brand center site/app to your site owners to unlock the Brand center app.

Scenario 3: Your tenant uses the SharePoint Organization Assets feature with Public CDN.

For this scenario, the global administrator needs to perform the following steps to create the Brand center app.

1. In the admin center, go to **Settings** > **Org settings**.
2. Select **Brand center**.
3. The Brand center recognizes your existing organization assets site location and will utilize this as the location for the Brand center app.
4. Activate the Brand center app for your organization.
5. Copy and share the link to the Brand center site/app to your site owners to unlock the Brand center app.

After you finish setting up your SharePoint brand center, you can control who can access the brand center app by customizing the site permissions of the brand center site. Site owners of the brand center site will be able to use the brand center app.

Managing the brand center

The SharePoint brand center includes two levels of management: the Microsoft 365 Admin Center and the Brand Center associated SharePoint site. Within the Microsoft 365 Admin Center, the global administrator has control over the enablement of the Brand Center and easy access to the associated site with management in the SharePoint Admin Center.

From the Brand center associated site, SharePoint site owners and above can update the site permissions in the SharePoint Admin Center such as adding more brand managers to the experience. You can do this by adding members to the site owners' group. Within the app itself, the brand managers are able to upload and manage their organization's brand assets.

Expand table

Who?	Where?	What?
Global administrator	Microsoft 365 Admin Center	- Enablement of the brand center -Access to the SharePoint Admin Center of the brand center site
- Global administrator - Site administrator - Site owner	SharePoint Admin Center	Update permissions

Managing brands in Multi-geo organizations

One of the challenges of managing brand assets across geographies is ensuring consistency and compliance with local regulations and cultural preferences. Brand managers need to be able to adapt their brand assets to different markets and languages, while still maintaining a unified and recognizable brand identity.

The SharePoint brand center currently only creates a single brand center app in the primary geo of a tenant. We haven't changed anything about how this impacts the current multi-geo operations for Organization Asset Image or Template Libraries. However, for custom fonts to work across geographies, the following requirements must be met:

> Each additional geography where custom fonts are wanted must have an organization asset library set up in a site that uses the Public CDN. Once these requirements are met, custom fonts show up in the **Change the Look** panel and will work in that geography.

> **Note**
>
> This does not impact Organization Asset Image Libraries and Template Libraries.

Brand Assets

Every organization has a set of brand assets that are important for expressing its brand identity. Brand assets are the things that give your brand its distinctive look, sound, and feel. They include your logo, colors, fonts, images, voice, and guidelines. You use your brand assets to show your brand personality and style in all the places where you communicate with your customers, such as websites, social media, marketing materials, presentations, and products. When you use your brand assets well, you make your brand more memorable, trustworthy, and unique.

One of the challenges of managing brand assets is to ensure consistency and quality across different platforms and devices. You want your brand to look sharp and professional everywhere, without spending too much time and effort on resizing, formatting, or providing appropriate access to your users.

The SharePoint brand center makes the management of brand assets simple across the Microsoft 365 product ecosystem. This centralized management system enables both asset management along with customization for how the assets are utilized within each product.

Brand Images

SharePoint offers a feature called the organization asset library (OAL), which allows you to store and access your brand images from a central location. You can upload and manage your organization's logos, icons, backgrounds, and other images in a centralized library that can be accessed by all your users. This way, you can ensure that your team members have access to the latest and most relevant images that reflect your brand identity and message. You can also use organization assets to create templates and themes that incorporate your images and fonts, making it easy to create professional and consistent slides and documents.

Learn more about image asset management.

Brand Fonts

A font isn't just a way of writing. It's a visual feature that connects your content to your brand and expresses your tone and character. A font can give your content a professional, creative, friendly, or authoritative appearance, depending on the typeface, size, color, and spacing you use.

For SharePoint and Viva Connections experiences, an organization uses the SharePoint brand center to control your organization’s fonts. This helps you make sure that your font selections are coherent and match your brand identity and guidelines.

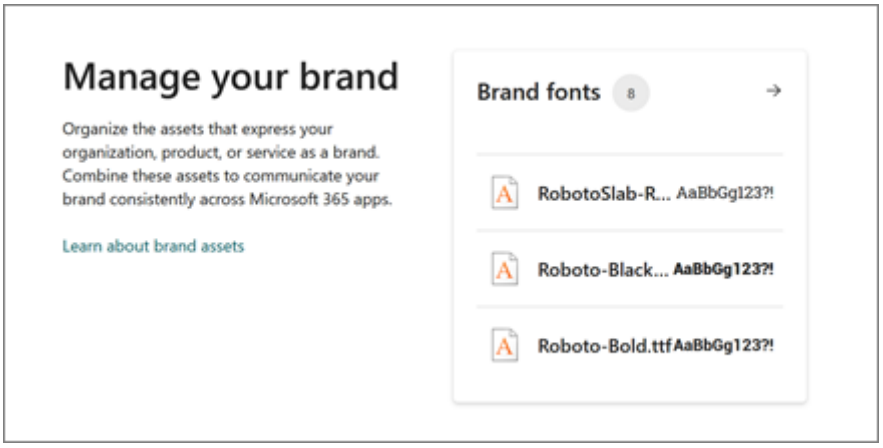
Learn more about brand fonts in the SharePoint brand center.

Organization font support for PowerPoint for the web is also available utilizing the organization assets infrastructure. Customers with E3 or E5 licenses can take advantage of Organization Font Support in PowerPoint for the web to edit and display their fonts.

Learn more about brand organization fonts for PowerPoint for the web.

Brand Fonts

The choice of font can have a significant impact on the look and feel of your content. A font can convey your brand personality, tone, and style, as well as enhance the readability and aesthetics of your text. Whether you want to create a professional, elegant, playful, or creative impression, using a font that matches your brand identity can help you stand out from the crowd and connect with your audience.



Brand fonts are your organization's fonts that are uploaded and managed within the SharePoint brand center. In this article, we talk about how to manage your brand fonts so you can use them in Microsoft 365.

There are different types of font format types and font file types. The way a font is used, digital, or printed, can change the font file type needed.

Web-safe fonts

Web-safe fonts are a set of fonts that are widely used and available on most devices by default. They're designed to be compatible with different browsers and operating systems, and to reduce the risk of font substitution or distortion.

Adding brand fonts to the brand center

SharePoint and Viva Connections include a set of font options that are available for use within Microsoft web products.

However, sometimes you may want to use a custom font that you've created, purchased, or downloaded from somewhere else. These custom fonts might be more accurate to how you

would like to represent your brand within Microsoft 365 applications like SharePoint and Viva Connections.

Locate custom fonts on the Web

You can also get and use fonts that are installed with other applications, or download fonts from the Internet. Some fonts on the Internet are sold commercially, some are shareware, and some are free. The Microsoft Typography site site provides links to other font foundries (the people or businesses outside of Microsoft who make and offer fonts) where you can find more fonts.

Install a custom brand font

After choosing your custom brand font, you'll need to upload it into the SharePoint brand center so that it can be part of your font packages. You'll go to the Brand Fonts library from the Brand center app.

1. Download or locate your custom brand font files. These often come in .zip folders.
2. If the font files are zipped, unzip them by right-clicking the .zip folder and then clicking **Extract**.
3. Navigate to the Brand fonts library in the SharePoint brand center app. Using the upload button

After the brand font files are uploaded our system extracts the needed metadata from the font files for use in the Brand center.

> **Note**
>
> There's a slight delay in the time from upload until this metadata is populated into the library and the font is available for use.

Supported font file types:

Expand table

Font file type	File extension
True Type fonts	.ttf
Open Type fonts	.otf

Font file type	File extension
Web Open Format Font	.woff
Web Open Format Font	.woff2

The Web Open Format file is a web-only font format that compresses the fonts to make them load faster on websites. This format can't be used for other purposes, such as installing the fonts on your computer. WOFF 2.0 is the ideal format for web fonts being used on SharePoint and Viva Connections. These fonts work well on the web but not in graphics software.

Font file Size Limit: 10 MB

Manage your custom brand fonts

To manage your custom brand fonts, you'll need to navigate to the Brand Fonts library in the Brand center app.

1. Select your custom font file from the library.
2. Edit the Visible property on your font file to control the availability of the font for experiences.
3. To remove a custom font file from the tenant's brand fonts library across all geo locations, use Remove-SPOFontFile.

Last updated on 09/05/2026

Font packages

A font package is a collection of fonts that are packaged together. Font packages are used in SharePoint and Viva Connections to control how the fonts look in different areas within each product.

Typography provides the visual framework for presenting text. It's an important part of expressing a brand or creating a beautiful design. You'll often see multiple terms mixed or used interchangeably when referring to typography, such as typeface and fonts A typeface is the entire font family while a font is an individual font style. We often use these terms interchangeably. We refer to fonts to cover both scenarios for the SharePoint brand center.

> **Note**
>
> Known Limitations:
>
> - Custom fonts are set at the site or Viva Connections experience level.
> - A font package applied to the Homesite backing the Viva Connections desktop experience also applies to the Viva Connections desktop experience.
> - A font package applied to the Viva Connections desktop experience also applies to the attached/associated SharePoint homesite.
> - Font packages cannot be deleted from the brand center app, they can be edited or made not visible to remove from selection experiences.

You have the option to select from the standard font packages or a custom font package for your organization to modify the fonts of your SharePoint site or Viva Connections experience. The font packages that Microsoft offers are created to build on the Microsoft brand, while also enabling versatility to invigorate our partnerships without overpowering them. They show our shared goals and personality, and they represent our diversity and ability to optimize your experiences.

Default font packages

- Microsoft default: Segoe UI
- Amasis Pro
- Aptos-Aptos Serif

- Georgia Pro Condensed-Verdana Pro Condensed
- Office: Aptos Display-Aptos
- Sitka Heading-Sitka Text
- Verdana Pro-Georgia Pro
- Walbaum-Trade Gothic Next

These font packages have been designed for readability, so you might find them useful starting points for creating custom font packages.

Anatomy of a font package

Each font package is composed of two font families. We consider these to be our Display and Content fonts.

Display font

The display font is a more decorative or eccentric typeface that is used for larger and more prominent elements of text. A display font is often used to express the feel of a brand. These are often slab serif, script, decorative, uppercase only typefaces.

Content font

The content font is used more widely to ensure consistency and legibility at all sizes. A content font should be identified and ideally have a range of weights and styles to fit a wide range of scenarios. This font should be considered as the baseline for most of your content and should be the most legible font from your brand.

Font slot mappings

Font packages use four font slots that correspond to different parts of the experience. For each part, you pick a font and font style that will change the fonts of different components based on these chosen font styles. These include:

Title

The title font is used to identify the most distinct items for your experience. Consider using your display font.

Headline

The headline font is used for a variety of headings and titles in the experience. Consider your content font in a bold or semibold style.

Body

The body font is used in more versatile ways and should be easy to read. Consider your content font in a normal or regular style.

Interactive

The interactive font is used for items that trigger action, such as buttons. Consider using your content font with a bold or semibold style.

Create your own font packages

In the SharePoint brand center, a brand manager is able to create custom font packages for your organization. These font packages are available in the Change the Look experience for site owners and Viva Connections operators to apply to their sites and experiences.

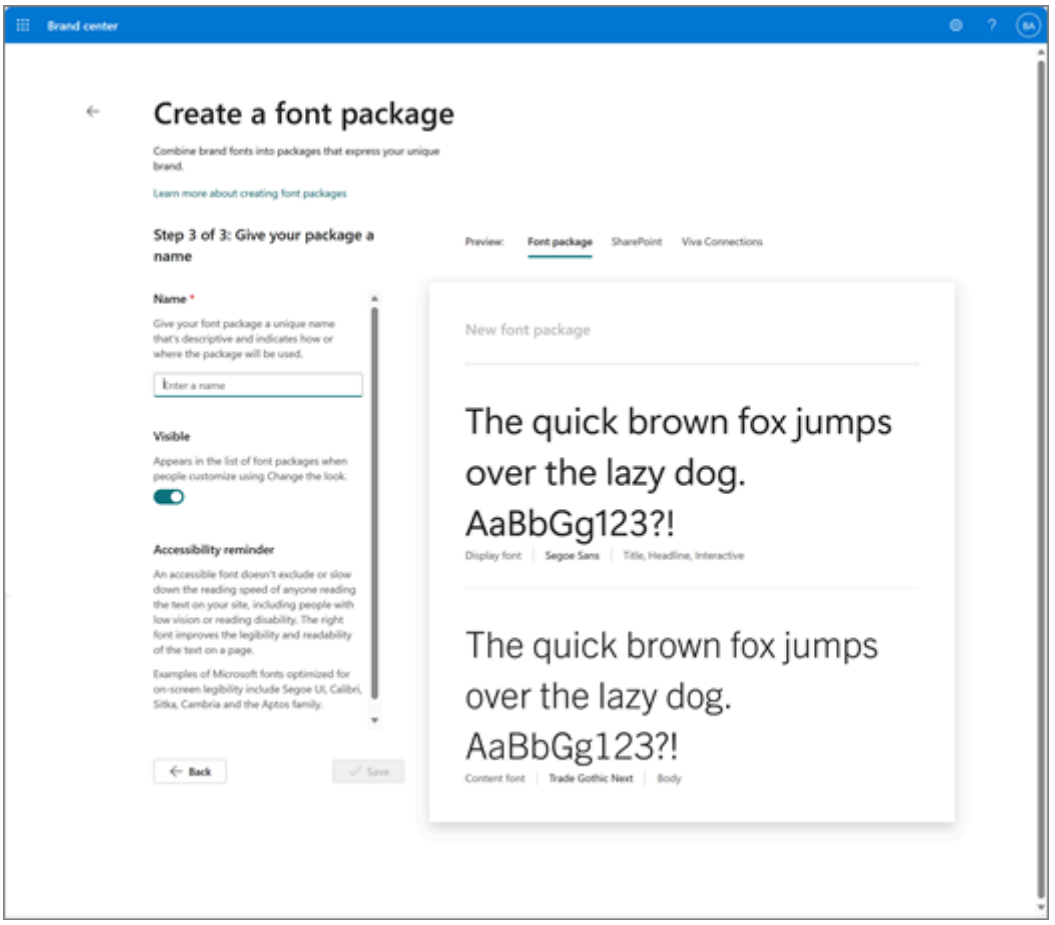
> ⓘ **Note**
>
> To create a custom font package, you must upload your organization's fonts to the brand fonts library.

Visit the SharePoint or Viva Connections branding experiences and select **New Font Package**

Step 1: Select display and content fonts using the font families visible in your Brand fonts library. You can select up to two different font families, you can select the same font family for both display and content fonts if desired.

Step 2: Select your font family and font style for each of the four font slot mappings.

Step 3: Name your font package and preview in different experiences. Determine the Visible setting for your font package.



Pay attention to Accessibility

An accessible font doesn't exclude or slow down the reading speed of anyone reading the text on your site, including people with low vision, or reading disability. The right font improves the legibility and readability of the text on a page.

To reduce the reading load, select familiar fonts such as Segoe UI or Aptos. Avoid using all capital letters and excessive italics or underlines.

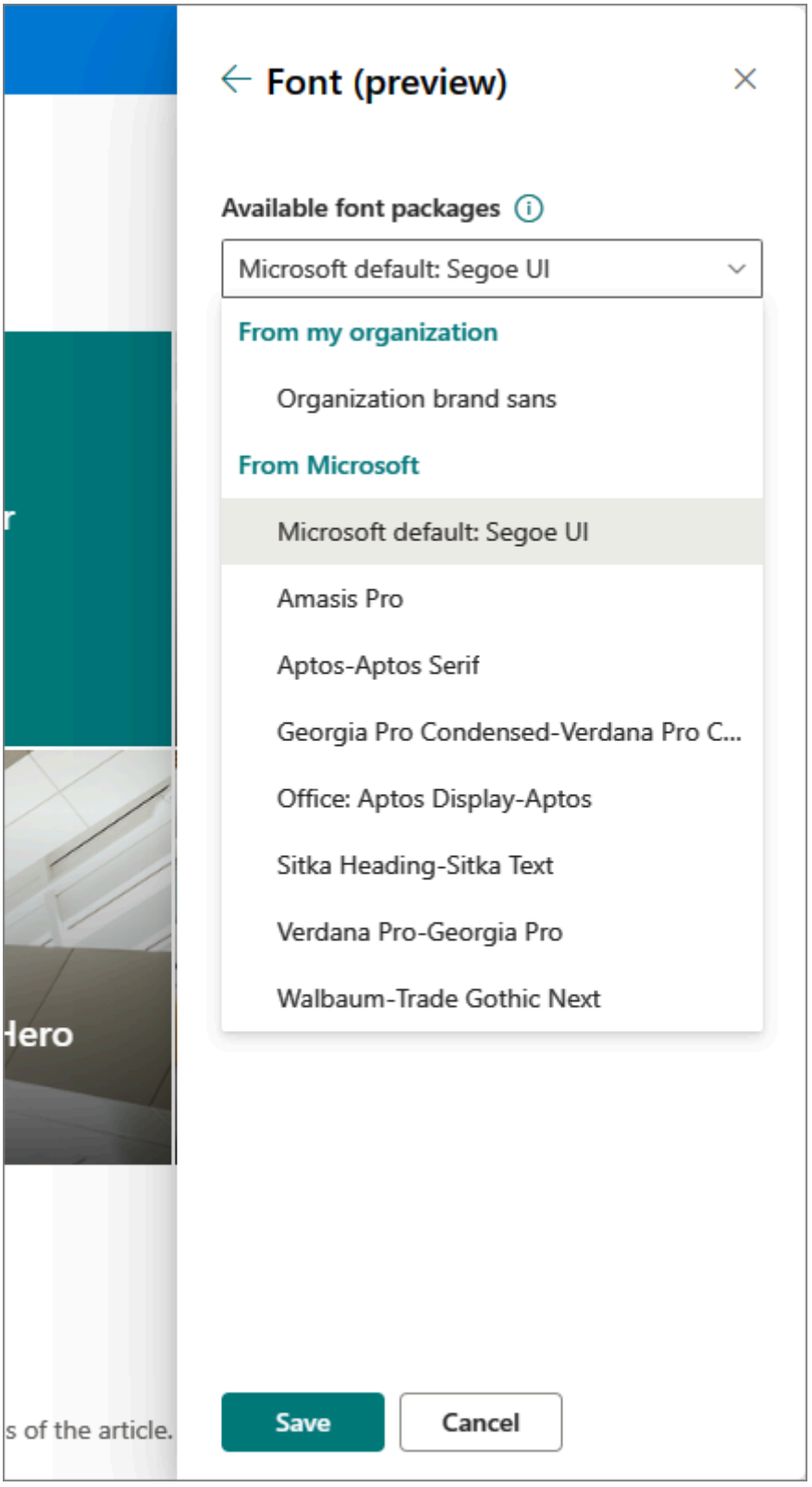
A person with a vision disability might miss out on the meaning conveyed by particular colors. For example, add an underline to color-coded hyperlink text so that people who are color-blind know that the text is linked even if they can't see the color. For headings, consider adding bold or using a larger font.

The text on your site should be readable in a high contrast mode. For example, use bright colors or high-contrast color schemes on opposite ends of the color spectrum. White and black schemes make it easier for people who are color-blind to distinguish text and shapes.

For instructions on how to work with fonts and text, go to Add accessible content and links to a SharePoint Online site and Add text to a SharePoint space.

Use a font package to change the fonts in your experience

With the introduction of the brand center app, custom fonts become available to Site owners to use from the **Change the Look panel** to customize the look and feel of their content. Once you have created a font package for your organization the “From my organization” section of the Font packages dropdown to the **Change the Look** > **Font** panel.



Learn more about Change the Look.

Font Packages in SharePoint

Supported custom fonts components in SharePoint

Custom fonts are currently supported in the following areas:

1. Site header - site title
2. Hub header – hub title
3. Navigation (hub and site) – links and labels
4. News web part
5. Page title region
6. Quick links web part
7. Button
8. Dashboard for Viva Connections
9. Image web part
10. Site header - finish
11. Section heading
12. Hero web part
13. Sites web part
14. People web part
15. Call to action web part
16. Text web part (RTE)
17. All web part titles (from Microsoft)

Font packages in Viva Connections

Supported custom fonts components in Viva Connections

Custom fonts are currently supported in the following areas:

1. Welcome/Greeting text
2. Section Headings
3. Dashboard cards Level 1
4. Resources

Last updated on 06/24/2026

Font Licensing for the brand center

Article • 04/22/2024

Fonts are a kind of software. Like many other kinds of software, you get a license to use font files instead of buying them. Different vendors have different licenses for their fonts, but most licenses, including the ones for the fonts Microsoft provides with applications and Windows, don't let you put the fonts in applications or share them with others.

Any font used in Microsoft 365 applications requires a font license that covers the conditions of font usage for the intended product. This could include a webfont license, application license, desktop license, server license, or several other license types.

> ⚠ **Warning**
>
> By using this feature and publishing font files, a font catalog is created. The newly created font catalog files are publicly stored, along with the fonts, in the cloud and won't respect the site classification guidelines if the Organization Asset Library is hosted in Restricted SharePoint Site. The font catalog files contain font names and other font related metadata. The files are accessible to anyone, even people outside of your organization, who can get the URLs that link to them.

Don't use this feature if your fonts contain proprietary information, or if they have license usage restrictions, such as restrictions on cloud hosting, or your organization isn't comfortable making the fonts publicly available.

Microsoft provided fonts

Microsoft provides a set of fonts for usage in Microsoft 365 applications. A Microsoft 365 application can use the fonts to render content to a screen, allow that content to be edited, and allow that content to be output to a device, like a printer.

Some of the fonts supplied with the Brand center were created specifically for Microsoft by leading type designers and type design companies (known as font foundries). Other fonts were licensed to Microsoft from font foundries for inclusion with Microsoft 365 applications.

Reference: Cloud fonts in Office - Microsoft Support

> ⓘ **Note**

Microsoft provided fonts are available to Microsoft 365 subscribers.

Custom brand fonts

For fonts obtained elsewhere or supplied with other apps, you'll need to review the license agreements that accompany those applications.

Why must I dig up and read those agreements?

We're sorry, but Microsoft can't provide guidance to fonts that we didn't supply.

The rights we provide you for Windows supplied fonts are considered quite broad, and it's possible that other font licenses, even some free ones, may be more restrictive.

Some font foundries may give away "free" versions of fonts with limited licenses and make their money selling extended rights.

Some font licenses may restrict commercial use, require attribution, and restrict redistribution or commercial redistribution of documents that include embedded versions of the font.

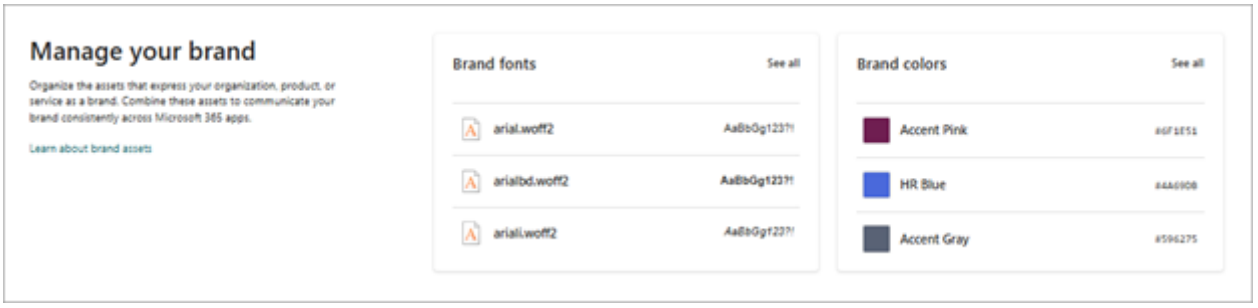
Feedback

Was this page helpful? Yes No

Provide product feedback

Brand Colors

By strategically incorporating brand colors throughout your content, you can create a cohesive visual identity that resonates with your audience. These colors are more than mere aesthetic choices; they are powerful tools that evoke emotions, convey messages, and build recognition. Whether it's through a striking website, engaging social media graphics, or compelling marketing materials, the thoughtful use of color can transform ordinary content into an extraordinary experience that authentically expresses your organization's values and essence.



Brand colors are your organization's colors that are uploaded and managed within the SharePoint brand center. In this article, we talk about how to manage your brand colors so you can use them in Microsoft 365.

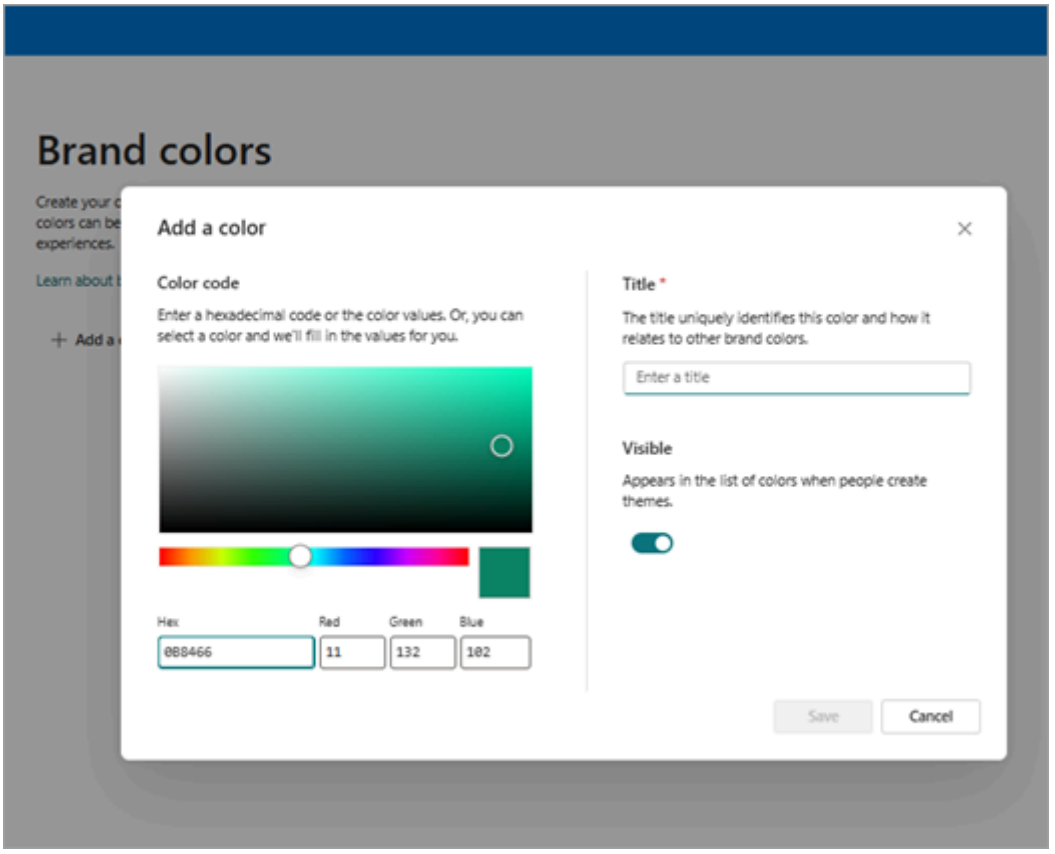
Adding brand colors to the brand center

Once the brand center is enabled, brand managers can create, update, and manage their organization's brand colors easily through the app.

In the brand color library, you can add a new color to create a full list of available standard colors to be used in various experiences.

> ⓘ **Note**
>
> Brand colors are currently supported for use in the SharePoint and Viva Connections theme experiences>

Step 1: Select Brand color from the SharePoint brand center app.



Step 2: Create your brand color by selecting and customizing your color.

You can create a new color using multiple methods:

Use the color pickers to move around and select a color

Enter a Hexadecimal code value into the Hex box

Enter Red, Green, Blue values into the text boxes

Step 3: Name your brand color. Determine the visible setting for your brand color.

> **Note**
>
> This name will appear in picker experiences where you would like to select colors to use and should provide the appropriate information to guide users when selecting.>

Manage your brand colors

To manage your brand colors, you'll need to navigate to the Brand colors library in the Brand center app.

1. Select your color from the library.
2. Edit the Name, Color, or Visible property for your color.

> **Note**
>
> Deletion of brand colors is not allowed from the Brand center app at this time.

See also:

How to choose the perfect colors for your brand

Fundamentals of color: What is color theory?

Last updated on 06/24/2026

Site theme

The theme is a powerful tool that allows SharePoint site owners and Viva Connections operators to apply cohesive and visually appealing colors to their web spaces. By leveraging these themes, organizations can create a unified look and feel across their sites, ensuring both aesthetic harmony and brand consistency. The customization options provided by themes enable users to tailor their site designs to reflect their unique brand identities while maintaining functionality and accessibility.

Principles of SharePoint themes

Guided

Our theming system works at a global level so that updates can be made consistently across each site, allowing users to optimize their websites effortlessly.

Smart and efficient

Our theming system expedites the site creation process by using smart algorithms to generate options that maximize aesthetic choices.

Professional

Our themes embody a professional look and feel that ensures coherency and conveys the brand of our enterprise audiences

Accessible

Our built-in accessibility checker ensures universal design at all levels of themes. For users who decide to customize, we provide helpful guidance to design for accessibility.

Default themes from Microsoft

- Teal
- Blue
- Orange
- Red
- Purple

- Green
- Periwinkle
- Cobalt
- Dark Teal
- Dark Blue

This collection of themes have been designed for accessibility and reflect colors from the Microsoft brand revealing our shared goals and personality.

Anatomy of a theme

Color Combinations

Color combinations are the foundation of your theme, enabling multiple brand colors to reflect your organization's brand identity and personality. Each theme supports up to 16 color pairs, with each pair consisting of an accent color and a background color. To ensure readability, the text color is automatically set to black or white based on the contrast ratio of the background color.

Application Zones

Theme colors are applied across key areas of the SharePoint site:

- Site Header and Footer: Managed by site owners to establish consistent branding.
- Section Design: Page authors can apply color combinations to individual sections for visual distinction.
- Text Web Part (Rich Text Editor): Theme colors enhance text formatting and styling.
- Design Ideas: Color combinations are reflected in suggested layouts and visual enhancements.

Create your own theme

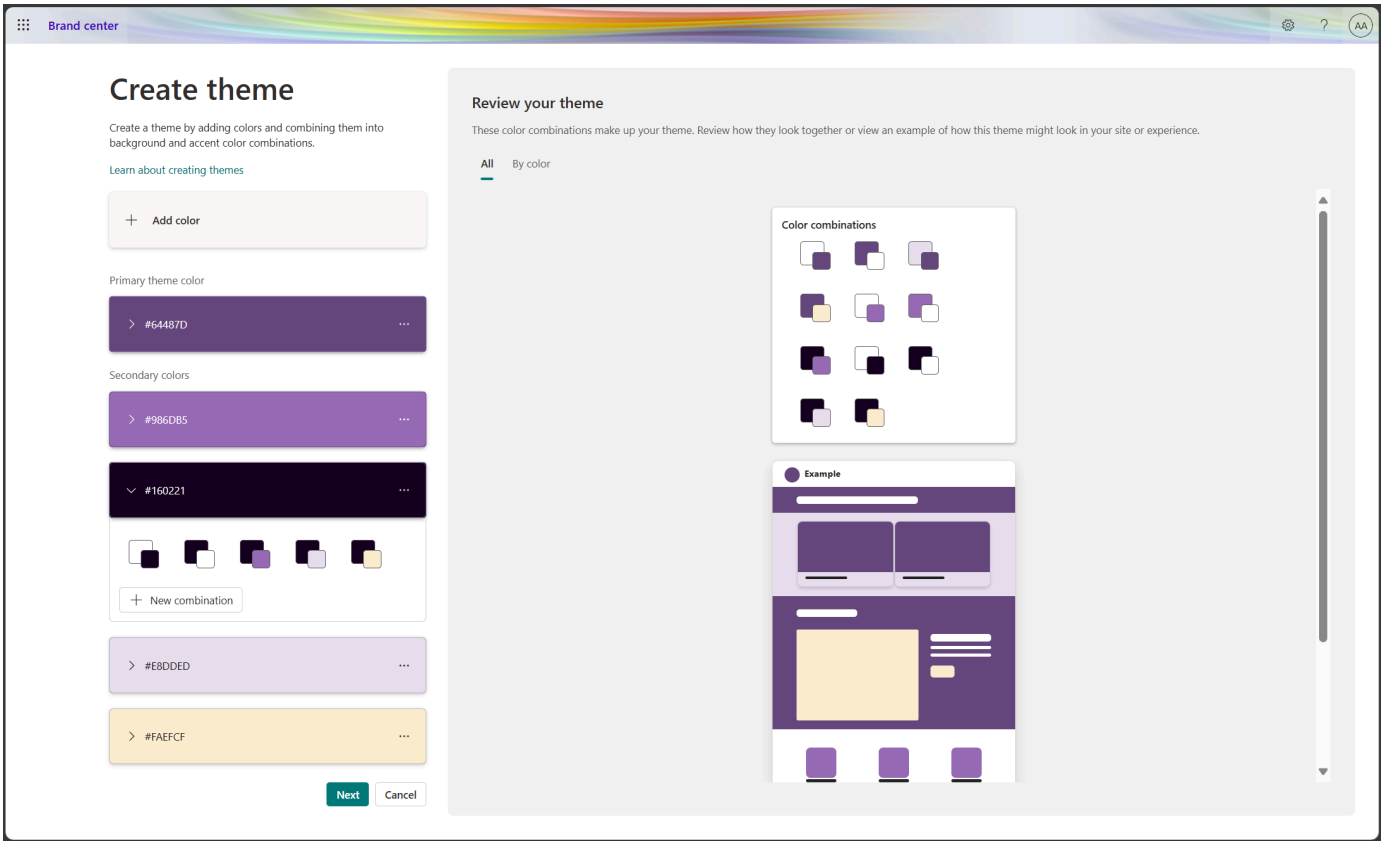
In the SharePoint brand center, a brand manager can create custom themes for your organization. These themes are available in the Change the Look experience for site owners and Viva Connections operators to apply to their sites and experiences.

> **Note**
>
> To create custom themes in the Brand center, your administrator must have enabled the Brand center from the Microsoft 365 Admin center. You can only read or delete a legacy

custom theme which consists of primary color, text color, background color, accent color. The legacy custom theme won't be automatically upgrade to the new custom theme format.

Visit the SharePoint or Viva Connections branding experiences and select **New theme**.

- **Step 1**: Select your primary, secondary colors using your brand colors or by adding a custom color. Add up to 16 combinations within the primary and secondary colors. In each color combination, you can switch around the background/accent color.
- **Step 2**: Name your theme and preview in SharePoint experiences.



Pay attention to accessibility

Color and contrast are important for accessibility. People with low vision, such as those with macular degeneration, need a certain amount of contrast to be able to see what's on the screen. It's also important to be careful with color selection, because color blind people can't tell the differences between certain colors. For example, someone who has red-green color-blindness sees red and green as the same color. In this theme creation experience we provide a color contrast checker built into the UI Elements preview to guide you towards creating accessible themes.

See also

SharePoint site theming

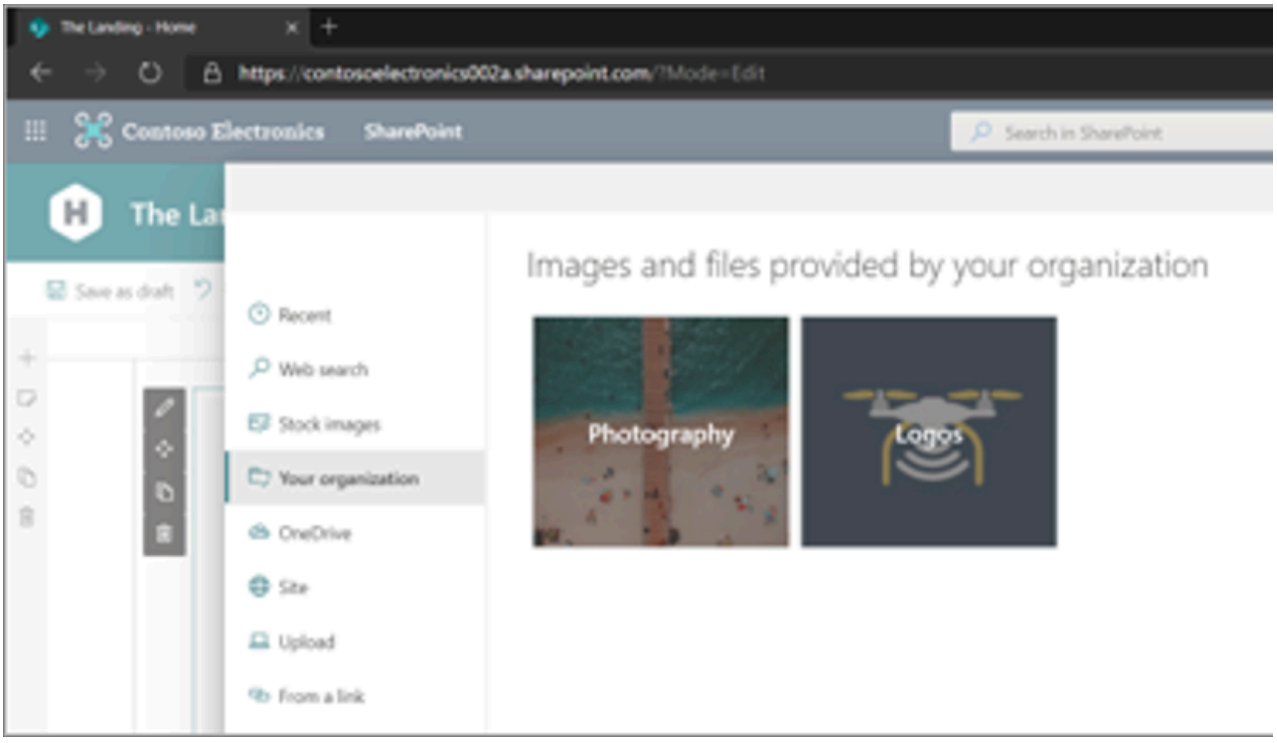
Last updated on 06/25/2026

Create an organization assets library

> **Note**
>
> This feature is not available for Office 365 operated by 21Vianet (China) or Microsoft 365 US Government plans.
>
> You can specify up to 30 organization asset libraries for a single organization. All of these libraries (regardless of type) must be on the same site. Only libraries (not folders) can be set as organization asset libraries.

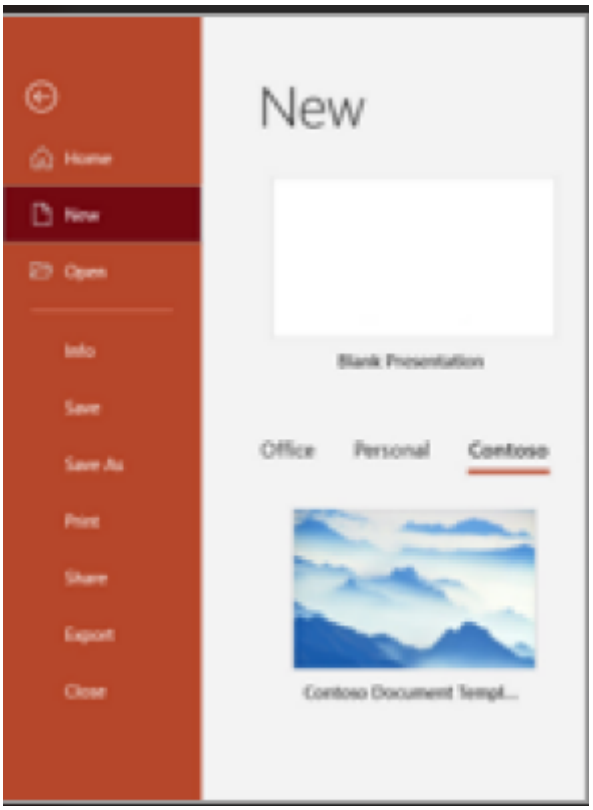
If your organization needs to store and manage files for all your users to use, you can specify one or more document libraries on a SharePoint site as an "organization assets library." You can create two types of organization assets:

- **Images such as photos and logos**: When a user adds a web part to any modern page in SharePoint and that web part opens the file picker, the user can select "Your organization" in the left pane to browse the libraries you've specified.



- **Office templates**: When a user creates a new Office document, they can select the tab for your organization to see the available templates. The following Office apps are supported:

- Word, Excel, or PowerPoint desktop apps. Microsoft 365 Apps Version 2002 or later is also required.



- PowerPoint on the web. Templates aren't available from the **New** menu. Instead, users need to go to the PowerPoint start page and select **Office Template Library**. For the organization assets library to appear to a user in PowerPoint on the web, the user must be assigned a license to Office 365 E3 or E5.

> **Note**
>
> - For the organization assets library to appear to a user in PowerPoint on the web, the user must be assigned a license to Office 365 E3 or E5. Users who use the Word, Excel, or PowerPoint desktop app also need Microsoft 365 Apps Version 2002 or later. (The organization assets library is not available in Word on the web or Excel on the web.)
> - Allow up to 24 hours for the organization assets library to appear to a user in the desktop apps.
> - Uploaded template files must be in the following formats:
> - **Excel**: .xltx. Learn how to save an Excel workbook as a template.
> - **Word**: .dotx. Learn how to save a Word document in this format.
> - **PowerPoint**: .potx. Learn how to save a PowerPoint file in this format.

- Users need at least read permissions on the root site for your organization for the organization assets library to appear in the desktop apps.

Organization fonts are supported on PowerPoint for the web. Learn more about support for your organization fonts here.

Use Microsoft PowerShell to specify a library as an organization assets library

1. Select an existing site or create a new site for the organization assets. This can be any type of site, such as a communication site, a team site that's connected to a Microsoft 365 Group, or a modern team site that isn't connected to a Microsoft 365 Group.

   > **Note**
   >
   > All organization asset libraries must be on the same site.

2. **Set the permissions on the site**. Add the people you want to be able to upload files as members or owners of the site or Microsoft 365 Group.

   > **Note**
   >
   > Adding "Everyone except external users" as visitors is required. If necessary, customize the permissions for the library. You can customize the permissions of up to 100 files and folders in the library.

3. Upload the images or Office templates to a document library.

4. Download the latest SharePoint Online Management Shell.

   > **Note**
   >
   > If you installed a previous version of the SharePoint Online Management Shell, go to Add or remove programs and uninstall "SharePoint Online Management Shell."

5. Connect to SharePoint as at least a SharePoint Administrator in Microsoft 365. To learn how, see Getting started with SharePoint Online Management Shell.

6. Run the following command to designate the document library as an organization assets library:

PowerShell

```
Add-SPOOrgAssetsLibrary -LibraryUrl <URL> [-ThumbnailUrl <URL>] [-OrgAssetType
<ImageDocumentLibrary or OfficeTemplateLibrary>] [-CdnType <Private or
Public>]
```

- *LibraryURL* is the absolute URL of the library to be designated as a central location for organization assets.
- *ThumbnailURL* is the URL for the image file that you want to appear in the card's background in the file picker; this image must be on the same site as the library. The name publicly displayed for the library will be the organization's name.
- *OrgAssetType* is either `ImageDocumentLibrary` or `OfficeTemplateLibrary`. If you don't specify the *OrgAssetType*, the library will be designated as an image library by default.
- *CdnType* needs to be specified only if you want to create a public CDN. If you don't specify the *CdnType*, it enables a private CDN by default.

  Learn more about the Add-SPOOrgAssetsLibrary cmdlet.

Example:

PowerShell

```
 Add-SPOOrgAssetsLibrary -LibraryURL
https://contoso.sharepoint.com/sites/branding/Assets -ThumbnailURL
https://contoso.sharepoint.com/sites/branding/Assets/contosologo.jpg -
OrgAssetType         ImageDocumentLibrary
```

> **Note**
>
> Adding an organization assets library will enable a content delivery network (CDN) for your organization to provide fast and reliable performance for shared assets. You'll be prompted to enable a CDN for each organization asset library you add. For more information, see Content Delivery Networks (CDNs).

Related commands

- See information about all organization asset libraries on the site:

  `Get-SPOOrgAssetsLibrary`

  Learn more about this cmdlet.

- Update thumbnail URL:

  `Set-SPOOrgAssetsLibrary -LibraryUrl <String> -ThumbnailUrl <String>`

  Learn more about this cmdlet.

- Remove a library:

  `Remove-SPOOrgAssetsLibrary -LibraryUrl <String>`

  Learn more about this cmdlet.

Last updated on 04/04/2026

Support for organization fonts in PowerPoint and Word

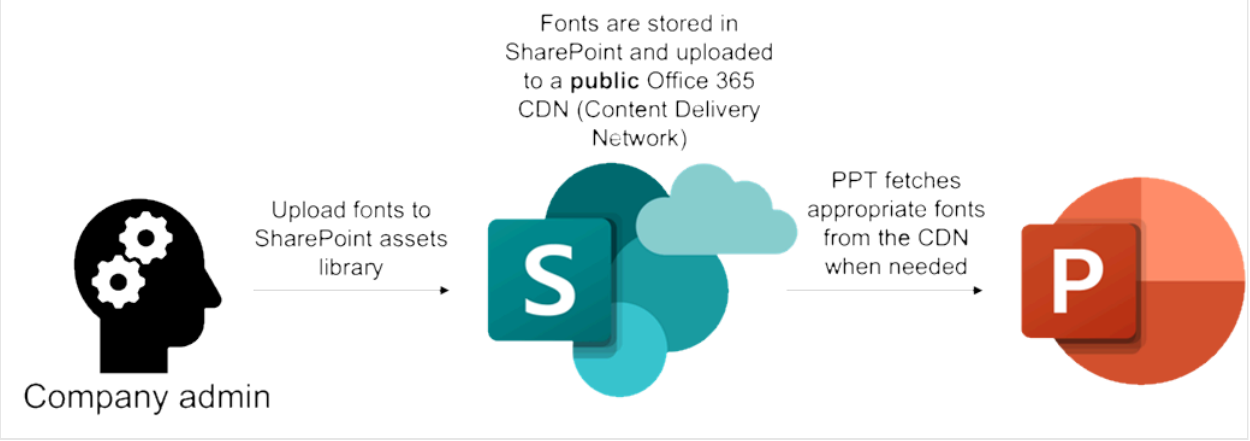
Article • 06/24/2024

Organization fonts allow customers to create a brand for their organizations and encourage consistency in documents and presentations. Earlier, organization users could only see and use organization fonts when they were installed locally on their desktops. Now, customers with E3 or E5 licenses can take advantage of Organization Font Support in PowerPoint for the web to edit and display their fonts. When you upload your font as a SharePoint Organization Asset Library (OAL), you'll see that your organization font now renders properly on PowerPoint and Word.

> **Note**
>
> Organization font support on PowerPoint and Word is not available for Office 365 Germany, Office 365 operated by 21Vianet (China), or Microsoft 365 US Government plans.

How does this work?

The following diagram outlines the key steps in making our solution work (PPT is used as an example in this diagram):



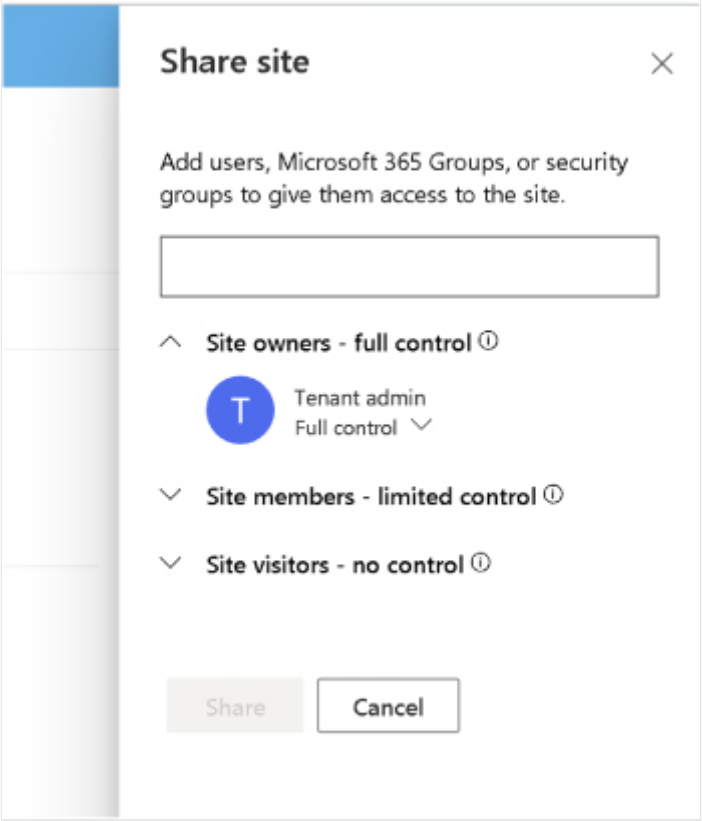
1. Organization administrator uploads their fonts to their organization's SharePoint site using the **SharePoint Online Management Shell.**
2. SharePoint stores the assets in a public Office 365 Content Delivery Network.
3. When a user opens a PowerPoint or Word file on the web platform, the web Application will access the Content Delivery Network (CDN) and fetch appropriate fonts.

Adding organization fonts to SharePoint as an organization asset library

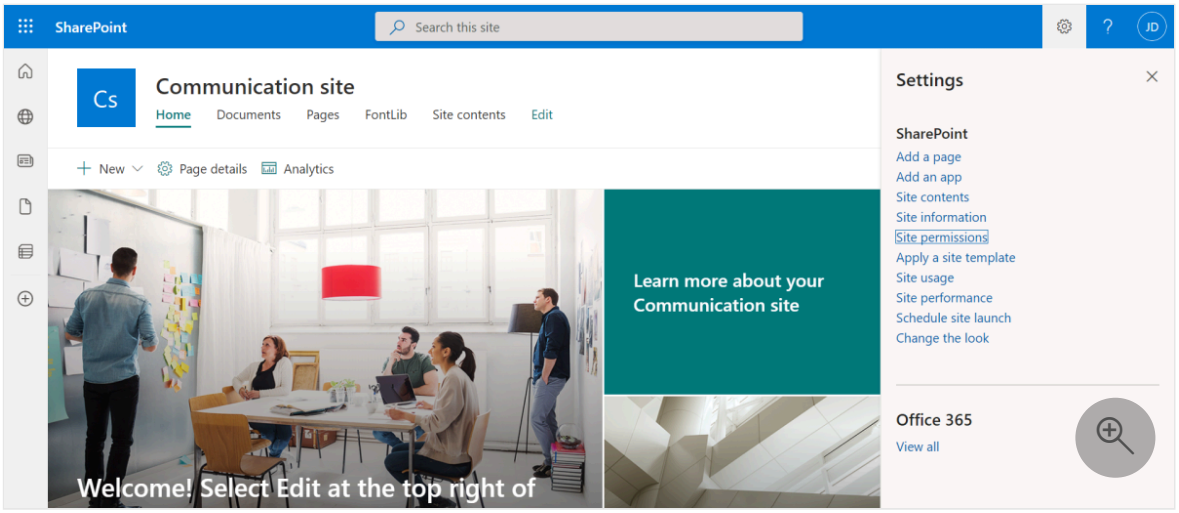
1. Create a new SharePoint site or use your existing site for Organization Asset Libraries.

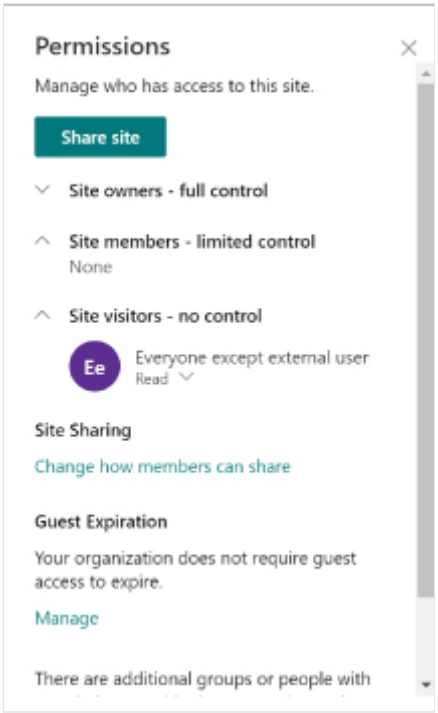
   > **Note**
   >
   > You cannot customize the permissions of font organization asset libraries as the fonts are hosted in a public CDN. When uploaded, font asset libraries are available across your entire tenant. Currently, sub-group permissioning of font asset libraries are not supported.

2. Ensure that your administrator account has **Full control** permissions to the SharePoint site you are using for your Organization Asset Libraries.

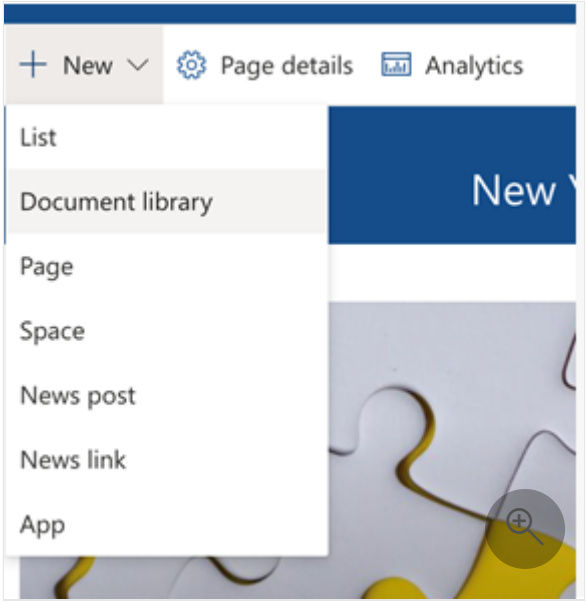


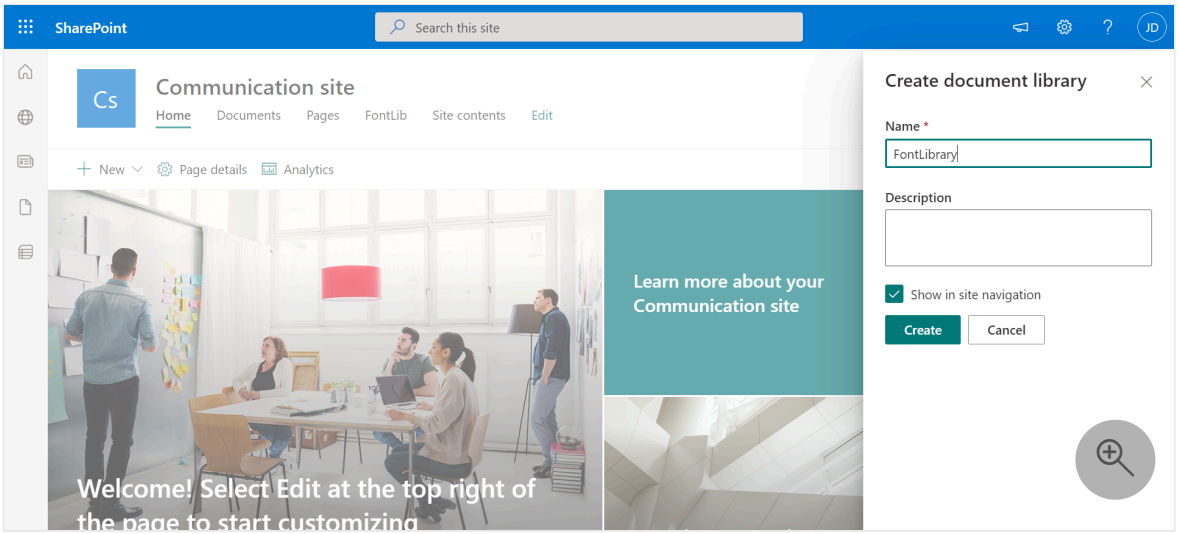
3. Ensure the site permissions for **Everyone except external user** are set to **Read** or **Edit**.





4. Navigate to your site's home page. From the **New** dropdown menu, select **Create a Document Library** and name your new font library.





5. Download the latest version of the SharePoint Online Management Shell.

6. Connect your SharePoint Management Shell with your administrator username and password.

7. Using the **SharePoint Online Management Shell**, run the following command as an administrator to designate the library as custom fonts asset library.

   `Add-SPOOrgAssetsLibrary -LibraryUrl <New Document Library SharePoint URL> -OrgAssetType OfficeFontLibrary -CdnType Public`

   For example:

   `Add-SPOOrgAssetsLibrary -LibraryUrl https://constosofonts.sharepoint.com/FontLibrary -OrgAssetType OfficeFontLibrary -CdnType Public`

   > **Note**
   >
   > - Only include the direct path of your font library. The trailing `/AllItems.aspx` should not be included in your Library URL.
   > - Font asset libraries must be designated with `-CdnType Public`.

8. Using the **SharePoint Online Management Shell**, run the following command as an administrator to upload your custom font(s) to the document library location.

   PowerShell

   ```
   Set-SPOCustomFontCatalog -FontFolder <Local Font Folder Location> -LibraryUrl <Document Library SharePoint URL>
   ```

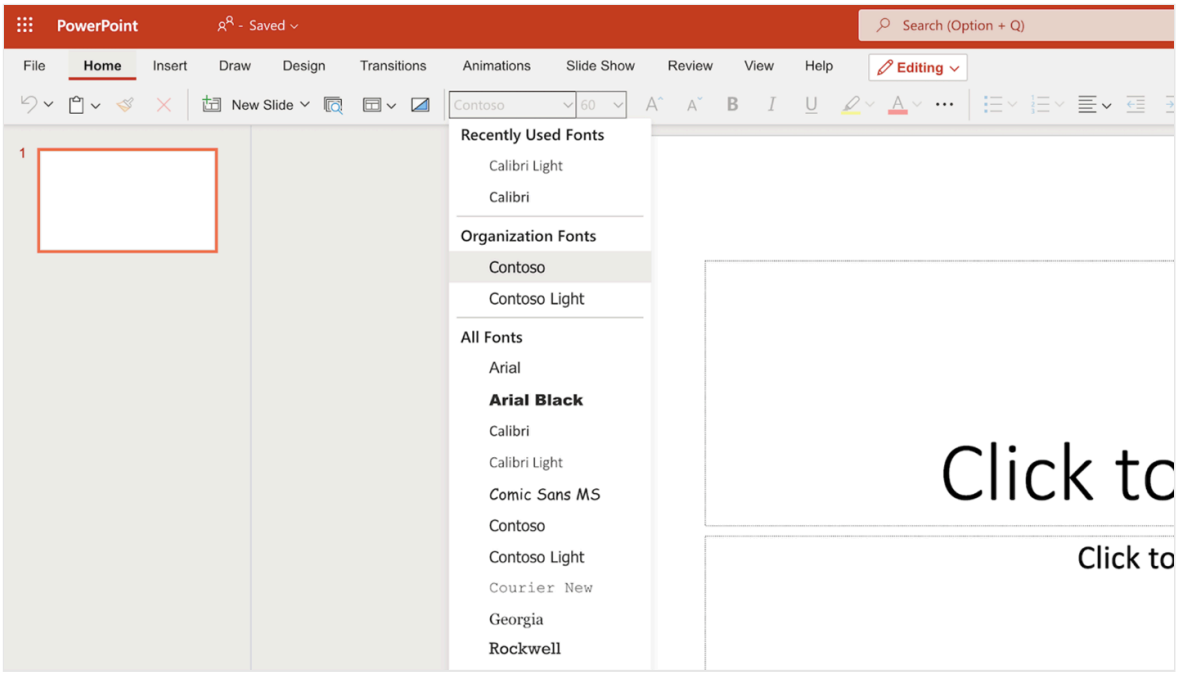
For example:

```
PowerShell

Set-SPOCustomFontCatalog -FontFolder "C:\ProgramData\Fonts" -LibraryUrl
https://contosofonts.sharepoint.com/FontLibrary
```

> **Note**
>
> - Your font folder should be the directory holding all your font files and should not include any non-font files.
> - You may be re-prompted to enter your credentials at this step.

Allow 24-hours for the SharePoint servers to update and for the users in your organization to see their organization fonts when using the **Font** dropdown menu in PowerPoint and Word for the web.



Important notes on features and its release

Feature notes

- Updates to organization font asset libraries can take up to 24 hours to propagate and become broadly available.
- If you need to change your font asset library, you will need to remove the font asset library using the Remove-SPOOrgAssetsLibrary command. Repeat the

process above to upload your updates in the font files. Changes made to the Document Library on the SharePoint web platform may affect font availability and feature functionality.

- The uploaded organization fonts will only be usable and viewable within your organization. To share them externally, you need to embed fonts into your PowerPoint presentations.
- This feature is only available on PowerPoint and Word on Web, Windows, Mac, and Mobile.

Licensing considerations

> ⚠ **Warning**
>
> By using this feature and publishing font files, a font catalog file will be created. The newly created font catalog files will be publicly stored, along with the fonts, in the cloud and will not respect the site classification guidelines if the Organization Asset Library is hosted in Restricted SharePoint Site. The font catalog files will contain font names and other font related metadata. Please note that the files will be accessible to anyone, including persons external to your organization, who are able to extract the URLs that point to them.
>
> These newly created files can be deleted by you. If deleted, the feature will not work as expected.
>
> Do not use this feature if your fonts contain proprietary information, or if they have license usage restrictions, such as restrictions on cloud hosting, or your organization isn't comfortable making the fonts publicly available.

Feedback

Was this page helpful? Yes No

Provide product feedback

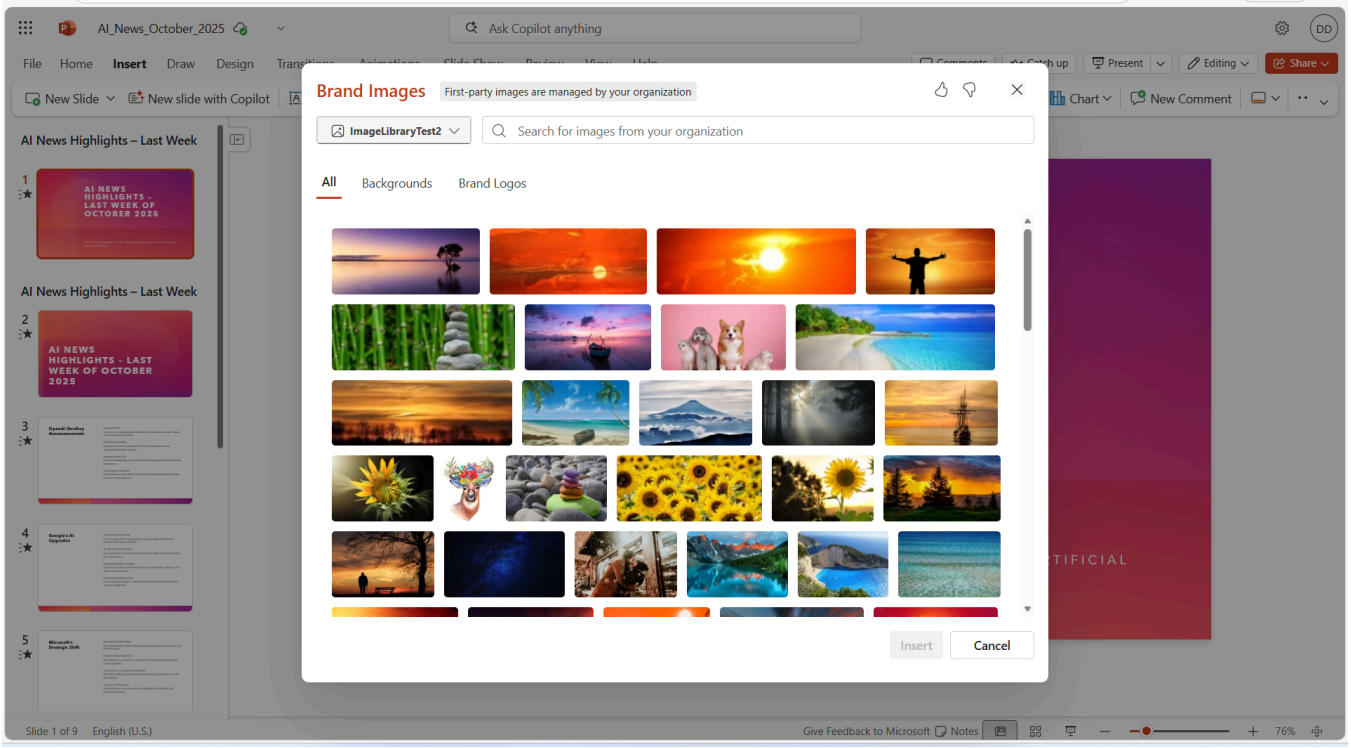
Connect organizational asset libraries to PowerPoint for an on-brand experience

Summarize this article for me

PowerPoint can now search and retrieve enterprise assets directly from your organizational asset libraries (OALs). This new workflow helps organizations democratize access of approved brand assets and simplifies retrieval through “Brand Images” feature. Create on-brand documents with quick access to company stock images, logos, icons, and illustrations.

How does it work?

- Assigning an organization image library allows PowerPoint to search and download content directly from the library.
- Instantly access your Brand Images right inside PowerPoint by going to **Insert** → **Pictures** → **Brand Images**
- Search in Brand Images utilizes image metadata stored within the OAL. Image tags, file name, description, and location are used to help users find the most relevant results.



Use Microsoft PowerShell to specify an organization image document library to be searchable

First, if you haven't, download the latest SharePoint Online Management Shell.

> **Note**
>
> If you installed a previous version of the SharePoint Online Management Shell, go to Add or remove programs and uninstall "SharePoint Online Management Shell."

Connect to SharePoint as a SharePoint Administrator or higher in Microsoft 365. To learn how, see Getting started with SharePoint Online Management Shell.

Run the following command to designate a document library as an organization image library and enable Brand Images in PowerPoint.

PowerShell

```
Add-SPOOrgAssetsLibrary -LibraryUrl <URL> [-ThumbnailUrl <URL>] [-OrgAssetType
ImageDocumentLibrary] [-CdnType <Public or Private>]
```

- *LibraryURL* is the absolute URL of the library to be designated as a central location for organizational assets.
- *ThumbnailURL* is the URL for the image file that you want to appear in the card's background in the file picker; this image must be on the same site as the library. The name publicly displayed for the library is the organization's name.
- *OrgAssetType* must be ImageDocumentLibrary. For now, search functionality only supports ImageDocumentLibrary.
- *CdnType* needs to be specified only if you want to create a public CDN. If you don't specify the *CdnType*, it enables a private CDN by default.

Example:

PowerShell

```
Add-SPOOrgAssetsLibrary -LibraryURL
https://contoso.sharepoint.com/sites/branding/Assets -ThumbnailURL
https://contoso.sharepoint.com/sites/branding/Assets/contosologo.jpg -OrgAssetType
ImageDocumentLibrary
```

> **Note**
>
> - You can only use image document libraries.
> - Ensure SharePoint Management Shell version is 16.0.24915.12000 or later.

- Brand Images feature is currently available on PowerPoint on both desktop and web.
- If you don't already have an organization asset library created, use Microsoft PowerShell to specify an existing library as an organization asset library.
- For a user to see the organization's asset library in PowerPoint for the web, they must have an Office 365 E3 or E5 license.
- Allow up to 24 hours for the organization assets library to appear to a user in the desktop apps.
- Users need at least read permissions on the root site for your organization for the organization assets library to appear in the desktop apps.

Best Practices

Follow these guidelines to improve the organization asset library image search experience:

- Avoid Multiple formats and resolutions of the same image. Search may return multiple versions of the same image reducing the breadth of search results.
- Avoid exceptionally large images. Images over 10 MB result in search latency and slow downloads, host application limits may also apply.
- Remove any files that aren't image based. Non-image files may be included in search results but fail on insertion.
- Insufficient tagging and descriptions. Successful search results require meaningful file names, image tags, location, and descriptions to be included with the content in the organization image asset library. Insufficient metadata reduces search hit rates and lower result relevancy.
- The following image formats are supported: JPEG, PNG, SVG, BMP, GIF, TIFF, WEB P, HEIF, ICO.

Reference

- Create an organization assets library
- Add-SPOOrgAssetsLibrary
- Set-SPOOrgAssetsLibrary

Last updated on 03/03/2026

How to Enable Enterprise Brand Images with PowerPoint Copilot

Copilot in PowerPoint can now create on-brand presentations using your company-approved images stored in Brand Kit in Microsoft 365. Here's how you can set up Copilot in PowerPoint to use your brand images.

Option 1: Brand Kit in Microsoft 365.

Copilot in PowerPoint can create on-brand presentations using images from your organization's Brand Kits.

Steps to Enable:

1. Ensure your Brand Kit contains a significant image set (ideally 1,000+ images) to achieve the best results in Copilot scenarios.
2. Publish your organization's Brand Kit to make approved brand assets available to users. Learn how to create and publish in, Create and manage official Brand Kits in the Microsoft 365 Copilot app.
3. A user in your organization can then include branded images from Brand Kit when creating or editing presentations with Copilot in PowerPoint.

Option 2: SharePoint Organizational Asset Library (OAL)

If your organization stores approved images in a SharePoint Organizational Asset Library (OAL), you can link those images to a Brand Kit in Microsoft 365. Once connected, users can access those assets through Brand Kits when creating presentations with Copilot in PowerPoint.

Option 3: Templafy Image Library

If your organization stores approved images in Templafy, you can link those images to a Brand Kit in Microsoft 365. Once connected, users can access those assets through Brand Kits when creating presentations with Copilot in PowerPoint.

Note: Your administrator should enable the Microsoft Graph Connector for Templafy in order to be able to link Images from Templafy in Brand Kit.

Tips for Success

- Use Copilot to generate on-brand presentations. To use images from your organization's Brand Kit, select the + button in the Copilot prompt box, then choose Select brand and pick the desired Brand Kit. Copilot will use brand assets from the selected Brand Kit when creating your presentation.
- Ensure your Brand Kit image asset library contains at least 1,000 brand-approved images with robust metadata (name, description, and tags) to improve Copilot's ability to retrieve relevant visuals.
- To further enhance image relevancy, consider expanding the quantity of images provided to Copilot and refining your image tags to optimize search results.

Related Articles

- Keep your presentation on-brand with Copilot - Microsoft Support

Templafy Connector

- About the Templafy connector
- How to Enable Microsoft Graph connector for Templafy Image Library for administrators
- How to include branded images from Templafy when creating presentations with Copilot for users in your organization

---

Last updated on 07/24/2026

Create a site

This article explains how users with at least SharePoint Administrator permissions in Microsoft 365 can create sites (formerly known as "site collections") in the SharePoint admin center. To learn about creating sites and managing users and groups using Microsoft PowerShell, see Create SharePoint sites and add users with PowerShell.

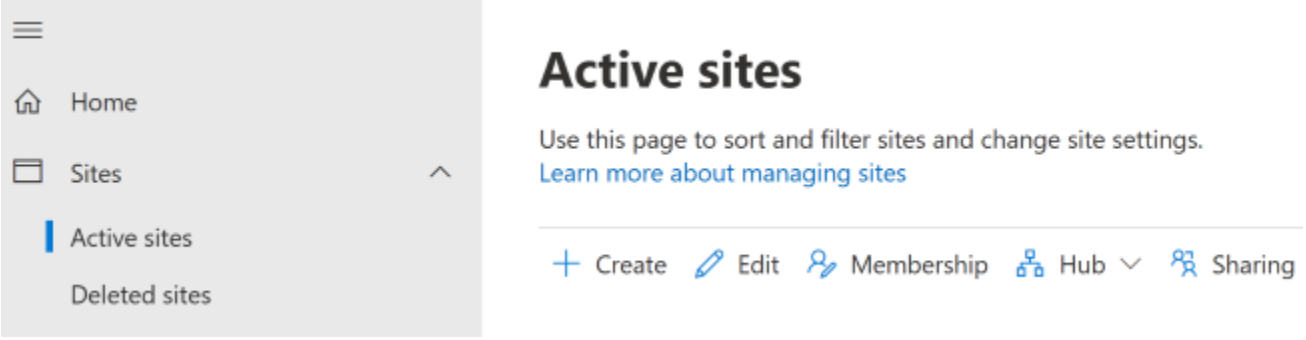
For info about creating site collections in SharePoint Server, see Create a site collection in SharePoint Server.

Create a team site or communication site

1. Go to **Active sites** in the SharePoint admin center, and sign in with an account that has admin permissions for your organization.

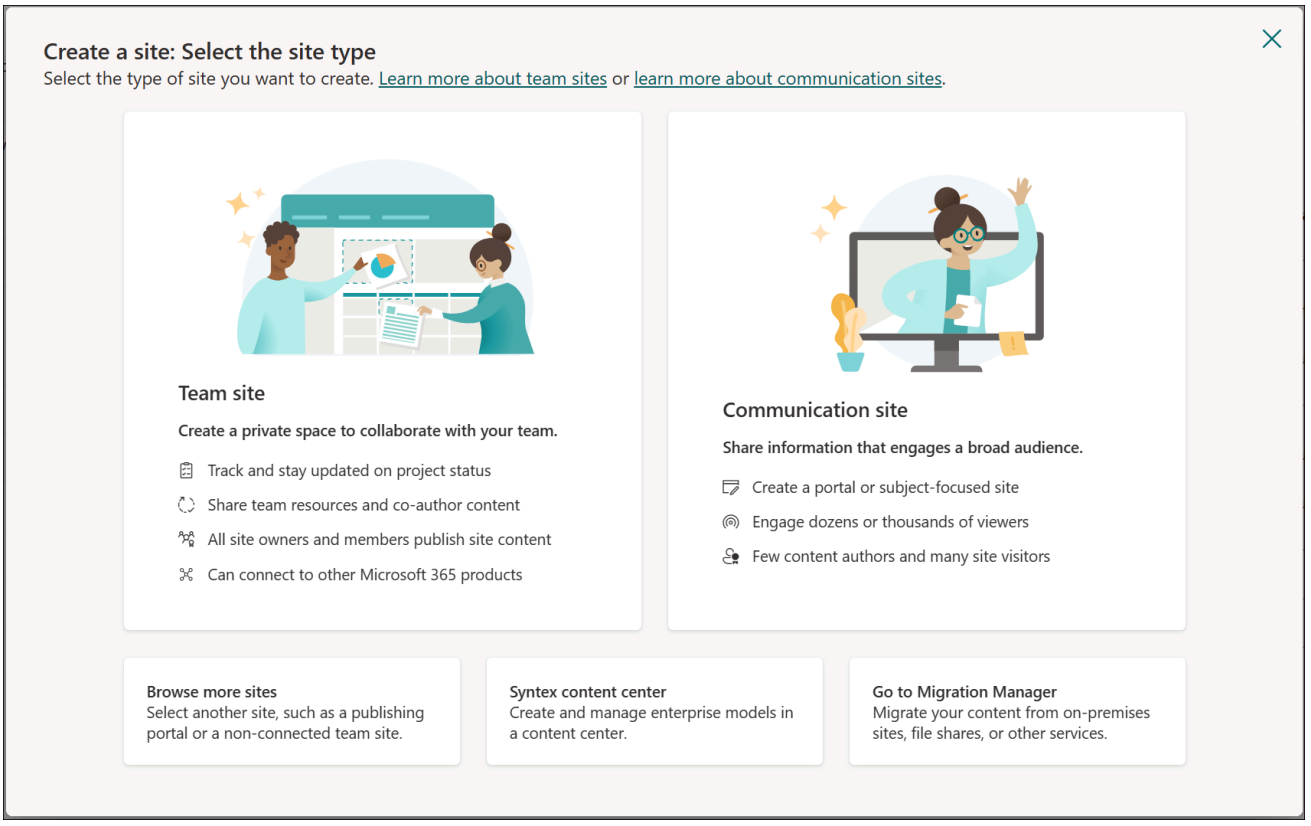
> **Note**
>
> If you have Office 365 operated by 21Vianet (China), sign in to the Microsoft 365 admin center, then browse to the SharePoint admin center and open the Active sites page.

2. Select **Create**.



> **Tip**
>
> If you go to **Resources** > **Sites** in the Microsoft 365 admin center and select **Add a site**, it opens Active sites in the SharePoint admin center in a new tab, and opens the Create a site panel.

3. Select **Team site** (to create a Microsoft 365 group-connected team site), **Communication site**, or **Browse more sites**.



4. Browse and select a template. Select **Use template**.

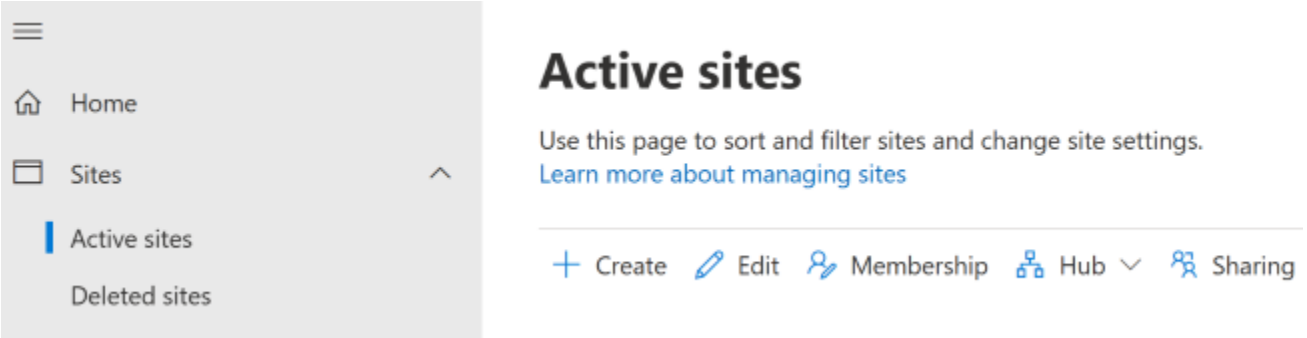
5. Follow the steps to specify a site name, owner, language, and other settings. When you're done, select **Create site**.

> **Note**
>
> If you enter a site name and another site already exists at the default address for that name, the site address is automatically changed to an available address. For example, if you enter "Marketing" as the site name, and you already have a site at /sites/marketing, you'll receive a warning ***This site address is available with modification*** and will be offered a new URL automatically at /sites/marketing2. If you want to reuse the URL "marketing" for the new site, you need to permanently delete the existing site or delete the redirect at that address.

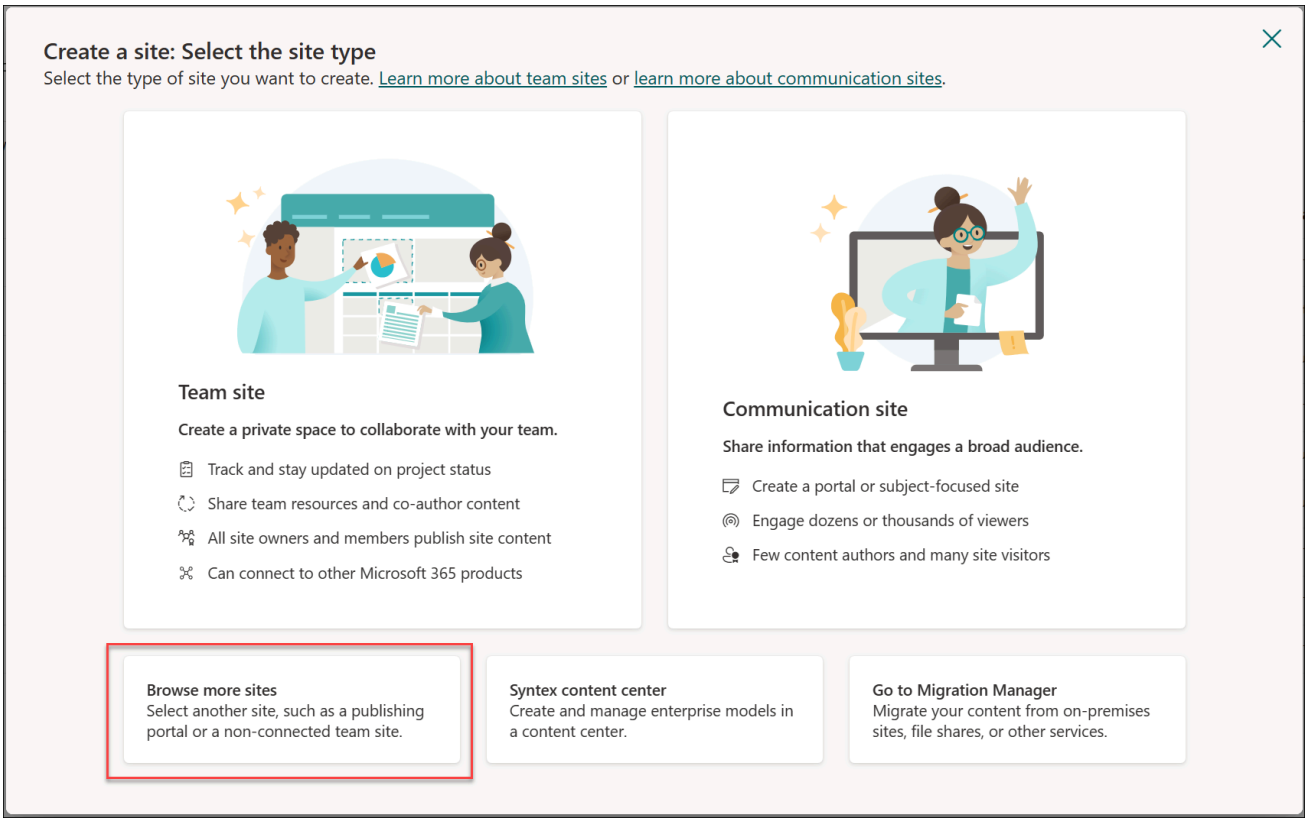
Create a classic site

We recommend using the new site templates for all your new sites. However, if you need to create a site that uses a classic template, you can do so using the following steps:

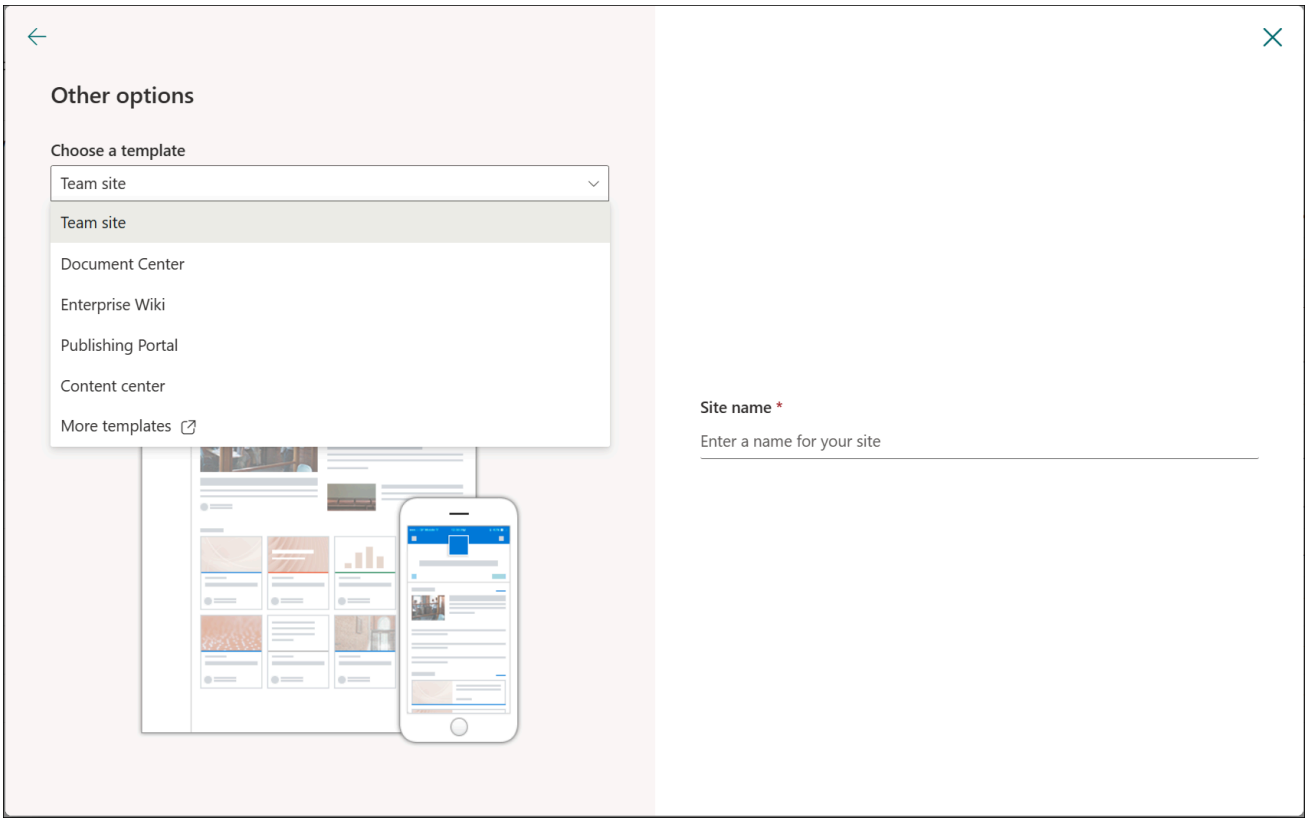
1. Go to **Active sites** in the SharePoint admin center, and select **Create**.



2. At the bottom of the panel, select **Brose more sites**.



3. Under **Choose a template**, select **More templates**.



- In the **Title** box, enter a name for the site.
- In the **Web Site Address** drop-down lists, select a domain name and a URL path—either **/sites/** or **/teams/—and then type a URL name for the site.
- In the **Template Selection** section, in the **Select a language** drop-down list, select a language for the site. You can enable the SharePoint multiple language interface on your sites, but the primary language for the site remains the one you select here.

> **Note**
>
> It's important to select the appropriate language for the site, because once it's set, it can't be changed. After creating a site, verify the locale and regional settings are accurate. (For example, a site created for Chinese will have its locale set to China.)

- In the **Template Selection** section, under **Select a template**, select the template that most closely describes the purpose of your site.

> **Tip**

For more information about the classic templates, see **Using templates to create different kinds of SharePoint sites**.

- In the **Time Zone** box, select the time zone that's appropriate for the location of the site.
- In the **Administrator** box, enter the user name of the person you want to be the site administrator. You can also use the **Check Names** or **Browse** button to find a user to make site administrator.
- In the **Storage Quota** box, enter the number of megabytes (MB) you want to allocate to this site. Don't exceed the available amount that is displayed next to the box.
- In the **Server Resource Quota** box, accept the resource quota default. This setting no longer affects the resource amounts available for the site.

4. Select **OK**.

Last updated on 06/24/2026

Delete a site

Article • 07/19/2024

When you, as a SharePoint Administrator and above in Microsoft 365, delete a site (previously called a "site collection"), it's retained as a deleted site for 93 days. Deleting a site deletes everything within it, including:

- Document libraries and files.
- Lists and list data.
- Site settings and history.
- Any subsites and their contents.

You should notify the site admins and any subsite owners before you delete a site so they can move their data to another location, and also tell users when the sites will be deleted.

> ⚠ **Warning**
>
> We do not recommend deleting the root site for your organization. If you do, all your SharePoint sites will be inaccessible until you restore the site or create a new root site. Instead of deleting the root site, we recommend replacing it. Learn more about the root site and how to replace it

> ⓘ **Note**
>
> Deleted sites in the Recycle Bin do not count toward the organization's total storage usage. It will take up to 48 hours for the storage usage to update.

Delete a site in the new SharePoint admin center

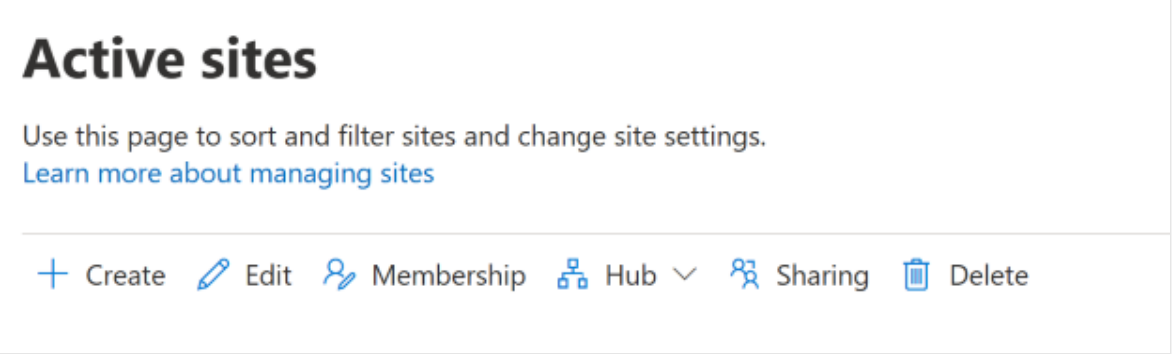
By using the SharePoint admin center, you can delete both classic and modern sites. As a a SharePoint Administrator and above in Microsoft 365, you can now delete sites that belong to Microsoft 365 groups. Deleting these sites will delete the group and all its resources, including the Outlook mailbox and calendar, and any Teams channels.

1. Go to **Active sites** in the SharePoint admin center, and sign in with an account that has admin permissions for your organization.

> **Note**
>
> If you have Office 365 operated by 21Vianet (China), sign in to the Microsoft 365 admin center, then browse to the SharePoint admin center and open the Active sites page.

2. In the left column, select a site.

3. Select **Delete**, and to confirm, select **Delete**.



> **Note**
>
> To delete a hub site, you first need to unregister it as a hub site.
>
> Deleted Microsoft 365 groups are retained for only 30 days.
>
> For info about deleting a site by using PowerShell, see Remove-SPOSite.

Permanently delete a site

To reuse a URL from a deleted site (recreate a site), you need to permanently delete the site. After the site is permanently deleted, it might take up to 24 hours for the URL to become available. On the Deleted sites page of the new SharePoint admin center, you can permanently delete all sites except those that belong to Microsoft 365 groups.

1. Go to **Deleted sites** in the SharePoint admin center, and sign in with an account that has admin permissions for your organization.

> **Note**

If you have Office 365 operated by 21Vianet (China), sign in to the Microsoft 365 admin center, then browse to the SharePoint admin center and open the Deleted sites page.

2. In the left column, select a site.

3. Select **Delete**, and to confirm, select **Delete**.

To permanently delete sites (including Microsoft 365 group-connected team sites) by using PowerShell, follow these steps:

1. Download the latest SharePoint Online Management Shell.

> **Note**
>
> If you installed a previous version of the SharePoint Online Management Shell, go to Add or remove programs and uninstall "SharePoint Online Management Shell."

2. Connect to SharePoint as a Global Administrator or SharePoint Administrator in Microsoft 365. To learn how, see Getting started with SharePoint Online Management Shell.

3. Run the following command:

```
PowerShell

Remove-SPODeletedSite -Identity
https://contoso.sharepoint.com/sites/sitetoremove
```

(Where `https://contoso.sharepoint.com/sites/sitetoremove` is the URL of the site you want to permanently delete). For more info about using this command, see Remove-SPODeletedSite.

Summary of options

Expand table

Site type	How to delete	How to permanently delete
Root site	Not recommended. Replace the root site with a different site. When the site is no longer a	From the Deleted sites page of the new

Site type	How to delete	How to permanently delete
	root site, its URL will be /sites/archive-*datetime*, and you can delete it from the Active sites page of the new SharePoint admin center or by using PowerShell	SharePoint admin center or by using PowerShell
Communication sites	Delete them from the Active sites page of the new SharePoint admin center or by using PowerShell	From the Deleted sites page of the new SharePoint admin center or by using PowerShell
Microsoft 365 group-connected team sites	Delete Microsoft 365 groups and all their resources from the Microsoft 365 admin center, the Active sites page of the new SharePoint admin center, or by using PowerShell	From PowerShell only
Hub sites (those designated with "(Hub site)" in the Hub column)	Unregister them as hub sites from the Active sites page of the new SharePoint admin center, or by using PowerShell, and then delete them based on their site type	Based on their site type
Classic sites	Delete them from the Active sites page of the new SharePoint admin center or by using PowerShell	From the Deleted sites page of the new SharePoint admin center or by using PowerShell

Note

Sites associated with a hub can be deleted like any other site based on their template.

See also

User instructions for deleting sites and subsites

Feedback

Was this page helpful? Yes No

Provide product feedback

Restore deleted sites

Article • 05/29/2025

Deleted SharePoint sites are retained for 93 days. After 93 days, sites and all their content and settings are permanently deleted, including lists, libraries, pages, and any subsites.

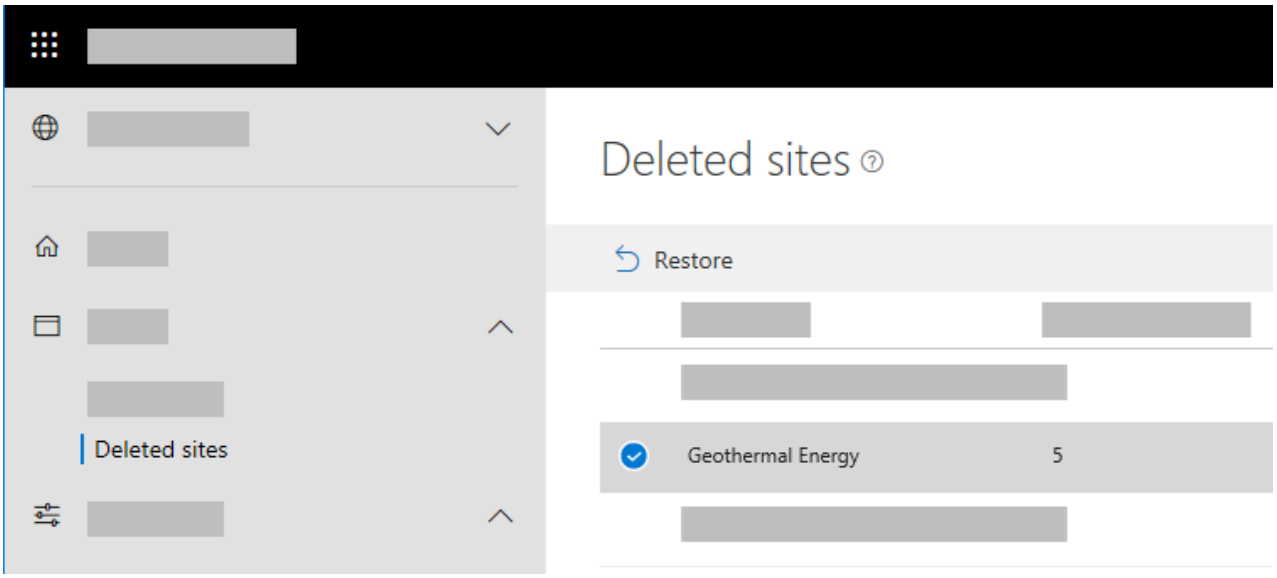
> **Note**
>
> If you need to retain content for a minimum period of time to comply with industry regulations or internal policies, you can create a retention policy to keep a copy of it in the Preservation Hold library. For info, see Overview of retention policies.
>
> For info about restoring items within a site, see Restore items in the Recycle Bin of a SharePoint site.
>
> For info about restoring deleted sites in SharePoint Server, see Restore deleted site collections using Microsoft PowerShell.

Restore a deleted site in the new SharePoint admin center

In the new SharePoint admin center, you can delete and restore all the new types of sites with the permissions of a SharePoint Administrator or more in Microsoft 365.

1. Go to **Deleted sites** in the SharePoint admin center, and sign in with an account that has admin permissions for your organization.

   > **Note**
   >
   > If you have Office 365 operated by 21Vianet (China), sign in to the Microsoft 365 admin center, then browse to the SharePoint admin center and open the Deleted sites page.



> **Note**
>
> You can sort and filter deleted sites the same way you sort and filter sites on the Active sites page. You can also sort and filter deleted sites by Time deleted.

2. Select the site you want to restore.

3. Select **Restore**. (If you don't see the **Restore** button, make sure only one site is selected. The button won't appear if multiple sites are selected.)

> **Note**
>
> Restoring a site that belongs to a Microsoft 365 group restores the Microsoft 365 group and all its resources. The other group resources are retained for only 30 days, whereas the site is retained for 93. If the other group resources have been deleted, you can use the PowerShell command Remove-SPODeletedSite to permanently delete the site.
> For info about permanently deleting sites from the Deleted sites page, see Permanently delete a deleted site.

Related articles

Restore deleted items from the site collection recycle bin

SharePoint data deletion in Microsoft 365

SharePoint stores objects as abstracted code within application databases. When a user uploads a file to SharePoint, SharePoint disassembles the file and translates it into application code. SharePoint stores the code in multiple tables across multiple databases. In SharePoint, all content that a customer uploads is broken into chunks, encrypted (potentially with multiple AES 256-bit keys), and distributed across the datacenter. For specific details about the chunking and encryption process, see Encryption in the Microsoft Cloud.

When you use the SharePoint application within a browser, any user who deletes an item retains the item in the site Recycle Bin for 93 days from the time they deleted it from its original location. The items stay in the site Recycle Bin the entire time, unless someone deletes them from the site Recycle Bin or empties that Recycle Bin. In that case, the items go to the site collection Recycle Bin, also known as the second-stage Recycle Bin, where they stay for the remainder of their retention period. Items deleted from the site collection Recycle Bin are purged immediately. If the item deleted causes the site collection Recycle Bin to exceed its quota, it starts purging the oldest items until there's space for the most recently deleted item. For info about restoring deleted items, see Restore items in the Recycle Bin of a SharePoint site and Restore deleted items from the site collection recycle bin.

When you delete a site collection, you also delete the hierarchy of sites in the collection, and all content within them:

- Documents and document libraries
- Lists and list data
- Site configuration settings
- Role and security information that is related to the site or its subsites
- Subsites of the top-level website, their contents, and user information

If you accidentally delete a site collection, a global or SharePoint admin can restore it by using the SharePoint admin center.

Deleted site collections are retained for 93 days. After 93 days, sites and all their content and settings are permanently deleted, including lists, libraries, pages, and any subsites.

Hard deletion occurs when a user purges deleted items from the site collection Recycle Bin, when the retention and backup periods expire, or when an administrator permanently deletes a site collection by using the Remove-SPODeletedSite cmdlet. When a user hard deletes (permanently

deletes, or purges) content from SharePoint, SharePoint also deletes all encryption keys for the deleted chunks. The blocks on the disks that previously stored the deleted chunks are marked as unused and available for reuse.

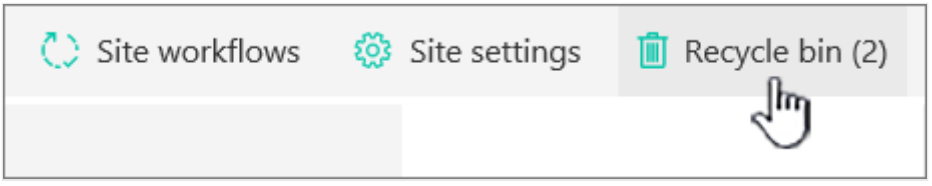
Users can also interact with the SharePoint platform by using CSOM/REST APIs. API calls can recycle or delete items on SharePoint such as files and folders. Recycling an item adds it to the Recycle Bin, similar to the browser application behavior described earlier in this article. However, deleting results in the item being immediately purged and it isn't recoverable from the site or site collection Recycle Bins. You can read more about SharePoint APIs here.

SharePoint retains backups of all content for 14 more days beyond actual deletion to facilitate a full site collection restore for customers. Customers can reach out to Microsoft support to initiate a full site collection or subsite point in time restore if files are hard deleted, corrupted, or infected with malware and are unrecoverable using the methods described earlier. After this 14 day period, Microsoft no longer retains the data and it isn't recoverable.

Delete an item from the site Recycle Bin

To delete items from the SharePoint site Recycle Bin

1. Click **Recycle Bin** in the Quick Launch bar on the left of the screen.
   If you don't see the **Recycle Bin** on the Quick Launch bar, follow these steps:
   a. Click **Settings** and then click **Site Contents**. The **Recycle bin** option is in the top-right portion of the **Site Contents** page.



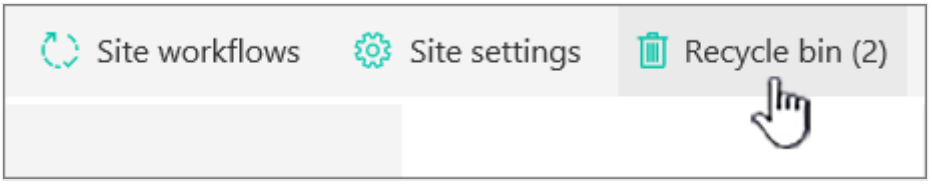
2. On the **Recycle Bin** page, click the box to the left of the items or files you want to delete or restore.

3. Click **Delete** to delete the selected files.

> **Note**
>
> If you don't see the item you're looking for, it might have already been deleted and already moved to the site collection Recycle Bin. Or it might have exceeded the holding time limit (93 days) and already been permanently deleted.

To delete all items from the SharePoint site Recycle Bin

1. Click **Recycle Bin** in the Quick Launch bar on the left of the screen.
   If you don't see the **Recycle Bin** on the Quick Launch bar, follow these steps:
   a. Click **Settings** and then click **Site Contents**. The **Recycle bin** option is in the top-right portion of the **Site Contents** page.

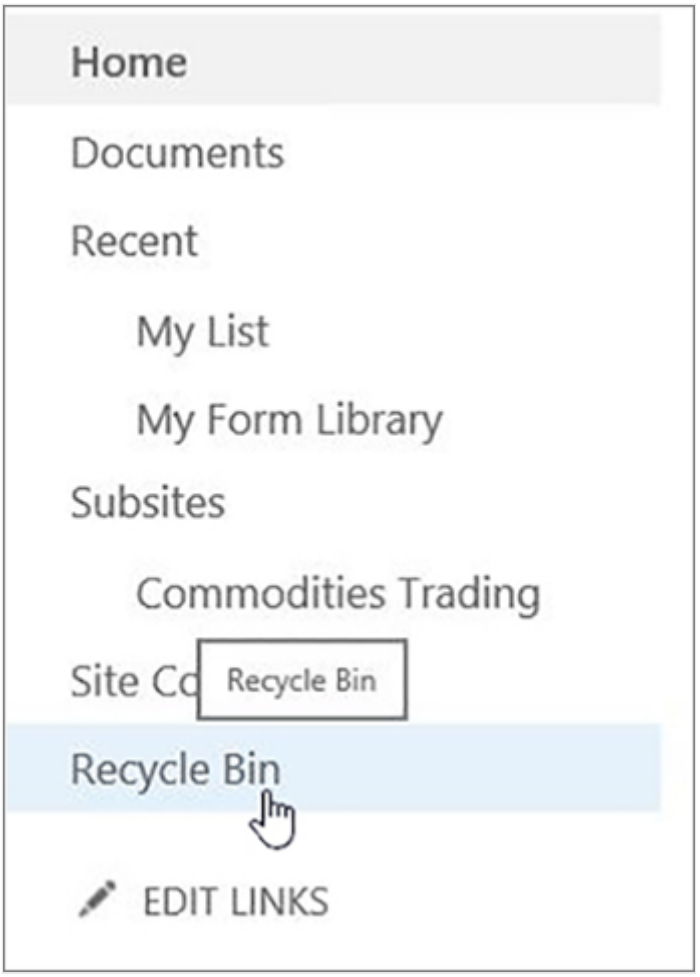


2. On the Recycle Bin page, click **Empty recycle bin** Empty recycle bin to delete all items.
   If **Empty recycle bin** isn't visible, make sure you unselect all items in the recycle bin.

Delete items or empty the Second-stage Recycle Bin in SharePoint

> **Caution**
>
> When you delete an item from the Second-stage or Site Collection Recycle Bin, it is permanently removed.

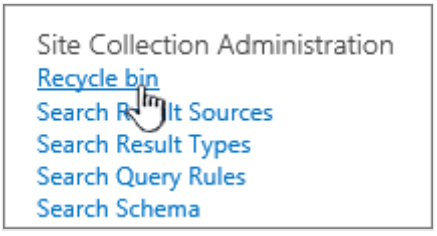
1. On modern team sites and classic sites (subsites) in the left pane, choose **Recycle bin**.



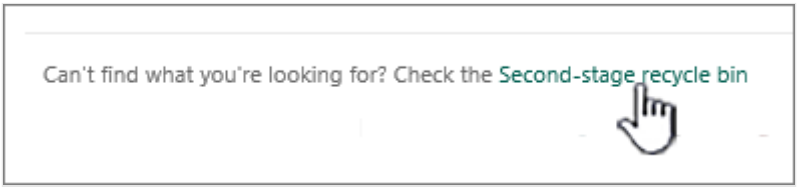
On modern communication sites, select **Site contents**, and then click **Recycle bin** in the top navigation bar. If you don't see the Recycle Bin, and you do have permissions, try the following steps.

a. Click **Settings** and then click **Site settings**. If you don't see **Site settings**, click **Site information** and then click **View all site settings**. Some pages might require you to select **Site contents**, and then **Site settings**.

b. On Site Settings, under **Site Collection Administration**, select **Recycle bin**.

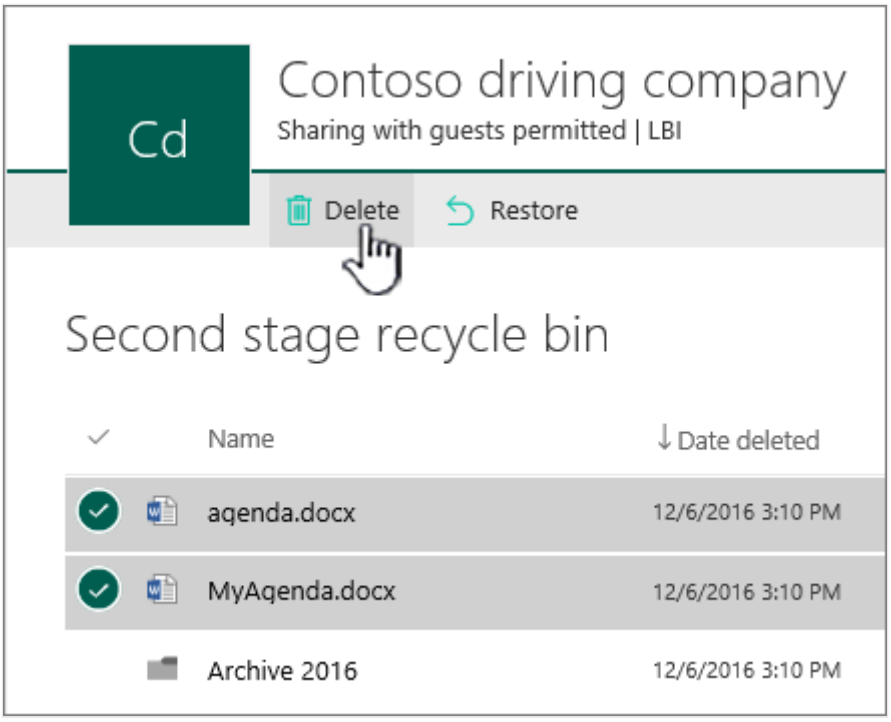


2. At the bottom of the **Recycle bin** page, click **Second-stage recycle bin**.

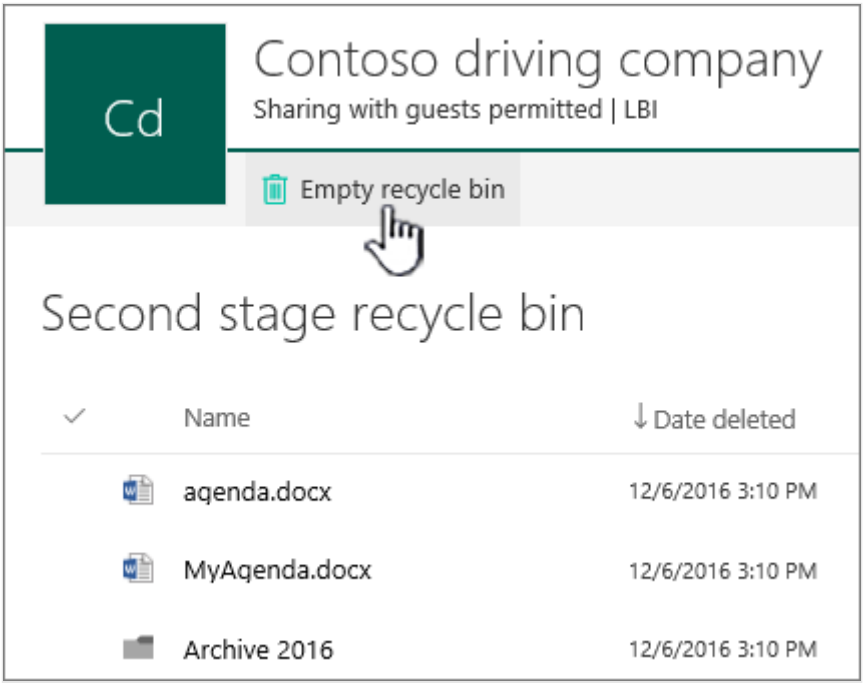


3. Do one of the following:

- **Delete one or more items** - Hover and click the circle next to the item(s) you want to delete and then click **Delete**.



- **Delete all items** - Clear all check marks and click **Empty recycle bin**.



4. In the confirmation box, click **Delete**.

Last updated on 08/31/2026

Restore deleted items from the site collection recycle bin

When you delete items (including OneDrive files) from a SharePoint site, they're sent to the site Recycle Bin (also called the first-stage Recycle Bin), from where you can restore them if you need to. When you delete items from a site Recycle Bin, they're sent to the site collection Recycle Bin (also called the second-stage Recycle Bin). The first-stage Recycle Bin contributes to the storage-used metric while the second-stage Recycle Bin does not.

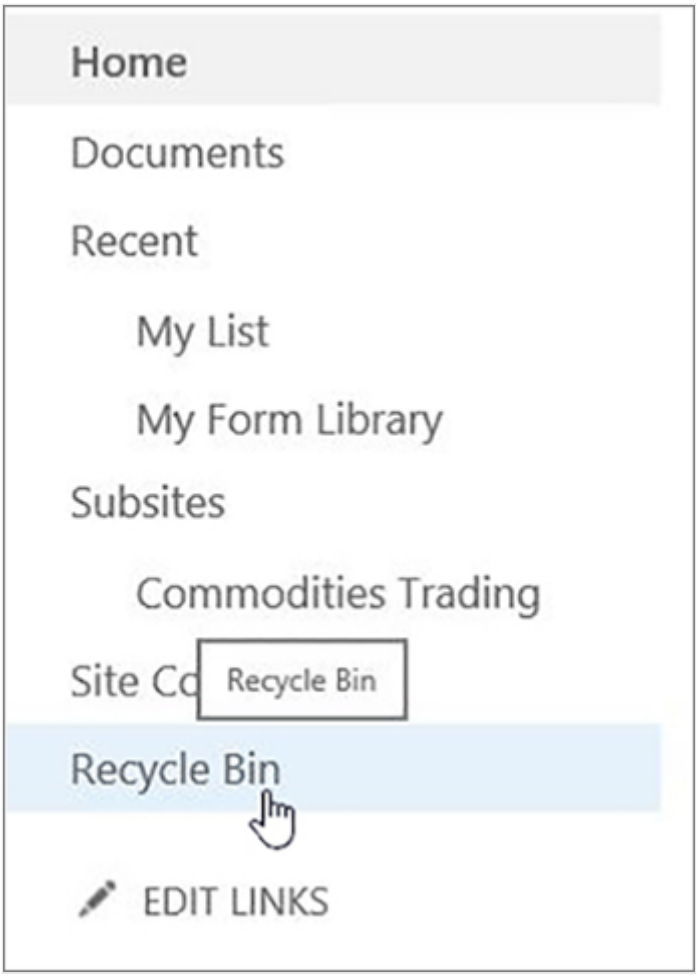
> **Note**
>
> Web items (subsites) go directly to the second-stage Recycle Bin and still count toward the storage-used metric. The quota is returned when the web items are purged from the second-stage Recycle Bin.

A SharePoint site collection administrator can view and restore deleted items from the site collection Recycle Bin to their original locations. If an item is deleted from the site collection Recycle Bin, or it exceeds the retention time, it is permanently deleted.

> **Important**
>
> The SharePoint Recycle Bin is different from the Recycle Bin in Windows. If you delete files or folders that you're syncing, you can restore them from the Windows Recycle Bin on your PC. To put your Windows Recycle Bin on your desktop, see Customize the Desktop Icons in Windows.

Restore an item from the SharePoint in Microsoft 365 site collection Recycle bin

1. On modern team sites and classic sites (subsites), in the left pane, select **Recycle bin**.

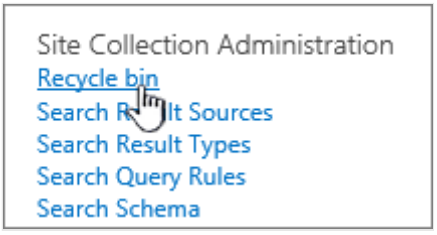


On modern communication sites, select **Site contents**, and then select **Recycle bin** in the top navigation bar. If you don't see the Recycle Bin, follow these steps:

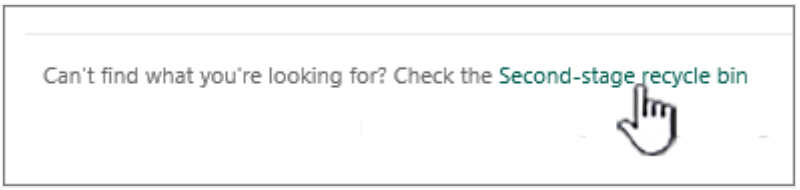
a. Select **Settings** and then select **Site settings**.

> ⓘ **Note**
>
> If you don't see Site settings, select **Site information** and then select **View all site settings**. Some pages might require you to select **Site contents** and select **Site settings**.

b. Under **Site Collection Administration**, select **Recycle bin**.

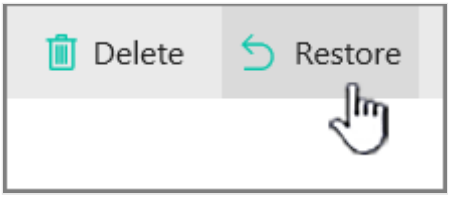


2. At the bottom of the **Recycle Bin** page, select **second-stage recycle bin**.



> **Note**
>
> You need administrator or owner permissions to use the site collection Recycle Bin. If you don't see it, it might have been disabled or you don't have permission to access it.

3. Point to the items you want to restore, select the check icon to the right of each one, and then select **Restore**.



> **Note**
>
> If you restore an item that was originally located in a deleted folder, the folder is recreated in its original location and the item is restored in that folder.

Restore an entire site collection

If you're a global admin or SharePoint admin in Microsoft 365, you can also restore entire site collections from the site collection Recycle Bin. For info, see Restore deleted sites.

How long are deleted items kept in the Recycle Bin?

In SharePoint in Microsoft 365, items are retained for 93 days from the time you delete them from their original location. They stay in the site Recycle Bin the entire time, unless someone deletes them from there or empties that Recycle Bin. In that case, the items go to the site collection Recycle Bin, where they stay for the remainder of the 93 days unless:

- The site collection Recycle Bin exceeds its quota and starts purging the oldest items.
- The items are manually deleted by the site collection administrator from the site collection Recycle Bin (for info about doing this, see SharePoint data deletion in Microsoft 365).

The site Recycle Bin storage counts against your site collection storage quota and the quota specified in Manage large lists and libraries. The amount of space allocated to the site collection Recycle Bin is 200% of the site collection quota. These values are not configurable.

SharePoint Online retains backups of all content for 14 additional days beyond actual deletion. If content can't be restored via the Recycle Bin or the feature specified in Restore your OneDrive, an administrator can contact Microsoft Support to request a restore any time inside the 14-day window.

> **Note**
>
> Restorations from backups can only be completed for site collections, not for specific files, lists, or libraries. If you need to recover a specific item, find it in the Recycle Bin, right-click it, and choose **Restore**.

In addition to the above, customers also have the option to utilize Microsoft 365 Backup for data recovery. Microsoft 365 Backup offers a longer protection time and provides uniquely fast recovery from common business continuity and disaster recovery (BCDR) scenarios like ransomware or accidental/malicious employee content overwrite/deletion. Additional BCDR scenario protections are also built directly into the service, offering an enhanced level of data protection.

A few basics about restoring from the Recycle Bin

- **Securable objects bring all their contents back with them** When you restore any securable object (any object to which access can be controlled), it is restored with all of the objects that it contained when it was deleted. For example, if you restore a list, library, folder, or Document Set, the restored version contains all the documents and other items that it contained when it was deleted. If you restore a file or other item that has multiple versions, the restored file or item includes all the versions it contained when it was deleted.
- **Most objects can't be restored if their container objects aren't present** If you delete an object and then delete the object that contained it, you must restore the container before you can restore the object. For example, if you delete a file and then delete the library in which it was stored, you must restore the library before you can restore the file. If you delete an earlier version of a file and then delete the current version of the file itself, you must restore the file itself before you can restore the earlier version.
- **Exception: An object deleted from a folder can be restored without first restoring the folder** The folder is automatically re-created in its former location, but now contains *only*

the object that you restored. (Alternatively, you can also restore the folder manually from the Recycle Bin, in which case it's restored with all the contents that it had when it was deleted.)

Last updated on 08/31/2026

Manage site admins

Article • 11/14/2024

This article describes how a SharePoint Administrator and above in Microsoft 365 can add and remove site admins (previously called "site collection admins"). If you're an owner of a communication site, or a site that belongs to a Microsoft 365 group, see Manage your SharePoint site settings for info about giving people access to your site. If you're an admin for a classic site, see Manage your SharePoint site settings.

> **Note**
>
> If you're a Global Administrator and want info about assigning other users the SharePoint Administrator role in Microsoft 365, see Assigning admin permissions.Microsoft recommends that you use roles with the fewest permissions. Using lower permissioned accounts helps improve security for your organization. Global Administrator is a highly privileged role that should be limited to emergency scenarios when you can't use an existing role.

Add or remove site admins in the new SharePoint admin center

By using the new SharePoint admin center, you can change the owners for sites that use the new team site and communication site templates. You can also add and remove group members in the Microsoft 365 admin center. For info, see Add or remove members from Microsoft 365 groups.

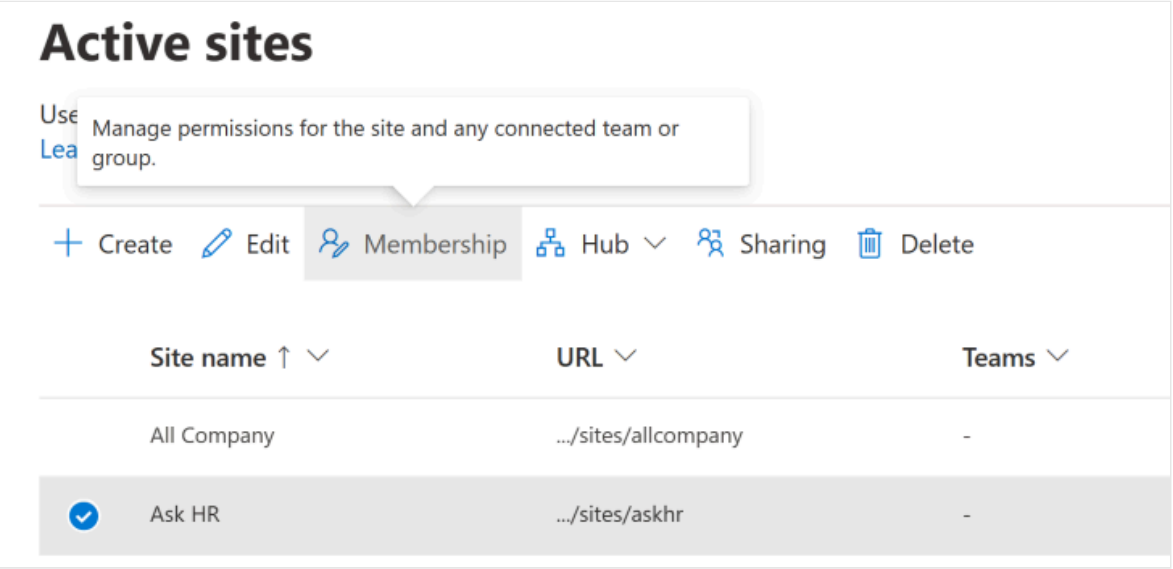
1. Go to **Active sites** in the SharePoint admin center, and sign in with an account that has admin permissions for your organization.

   > **Note**
   >
   > If you have Office 365 operated by 21Vianet (China), sign in to the Microsoft 365 admin center, then browse to the SharePoint admin center and open the Active sites page.

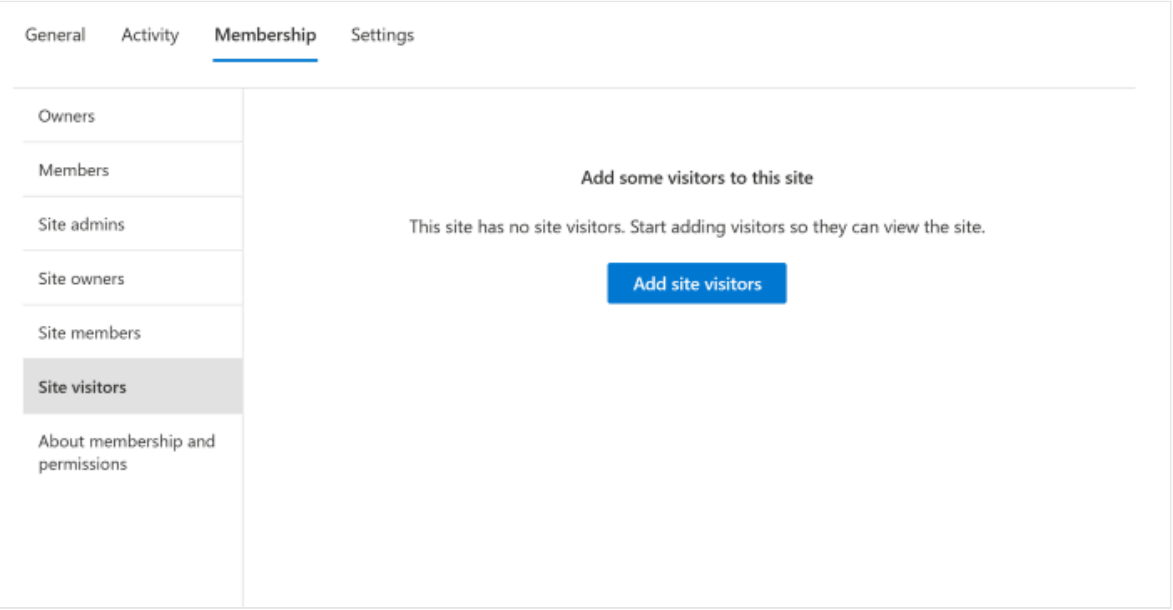
2. In the left column, select a site.

3. Select **Membership** on the command bar to open the details panel. For a group-connected team site, you can add and remove group owners and additional site

admins. For other sites, you can add and remove site admins and change the primary admin. Note that if you remove a person as a primary admin, they will still be listed as an additional admin. For info about each role, see About site permissions.



4. In the details panel, you can add or remove the owners, members, site admins, site owners, site members, and site visitors.



Feedback

Was this page helpful? Yes No

Provide product feedback

Manage site creation in SharePoint

Article • 05/29/2025

As a SharePoint Administrator and above in Microsoft 365, you can let your users create and administer their own SharePoint sites, determine what kind of sites they can create, and specify the location of the sites. By default, users can create communication sites and Microsoft 365 group-connected team sites.

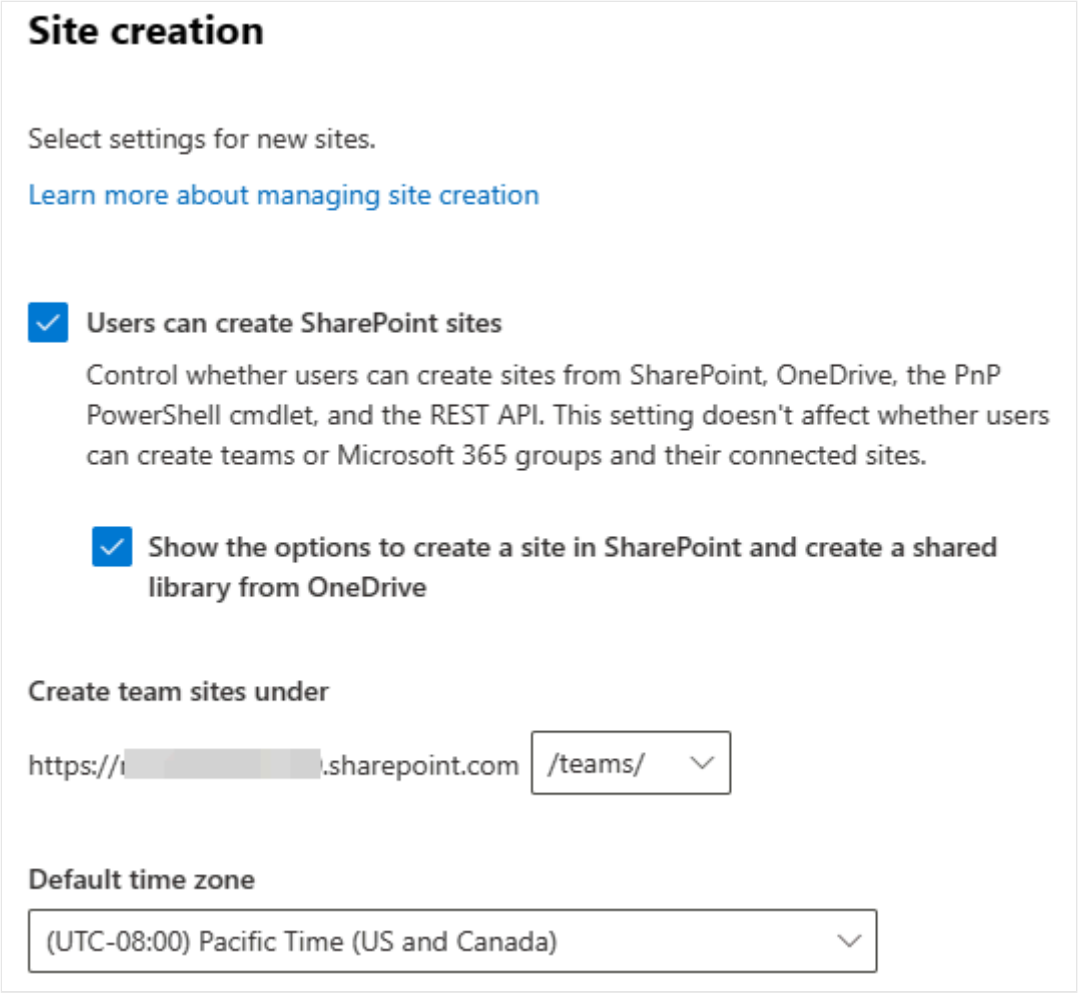
> **Note**
>
> Disabling site creation for users doesn't remove their ability to create Microsoft 365 groups or resources, such as Microsoft Teams, which rely on a group. When a Microsoft 365 group is created, a SharePoint site is also created. To restrict creation of Microsoft 365 groups and the resources that rely on groups see Manage who can create Microsoft 365 Groups.

Manage site creation in the new SharePoint admin center

1. Go to **Settings** in the SharePoint admin center, and sign in with an account that has admin permissions for your organization.

   > **Note**
   >
   > If you have Office 365 operated by 21Vianet (China), sign in to the Microsoft 365 admin center, then browse to the SharePoint admin center and open the Settings page.

2. Select **Site creation**. The **Site creation** page appears.



3. If you want users to be able to create sites, select **Users can create SharePoint sites**. This setting controls whether users can create sites from SharePoint, OneDrive, the PnP PowerShell cmdlet, and the REST API. This setting doesn't affect whether users can create teams or Microsoft 365 groups and their connected sites.

4. If you want users to be able to create sites from these services, select **Show the options to create a site in SharePoint and create a shared library from OneDrive**.

> ⓘ **Note**
>
> Even if you clear these checkboxes, users may be able to create Microsoft 365 groups from other places in Microsoft 365. Each group always comes with a team site. Learn how to manage who can create Microsoft 365 groups

5. Under /sites or /teams, select to create Microsoft 365 group-connected team sites, and then select the default time zone and storage limit for new sites.

6. Select **Save**.

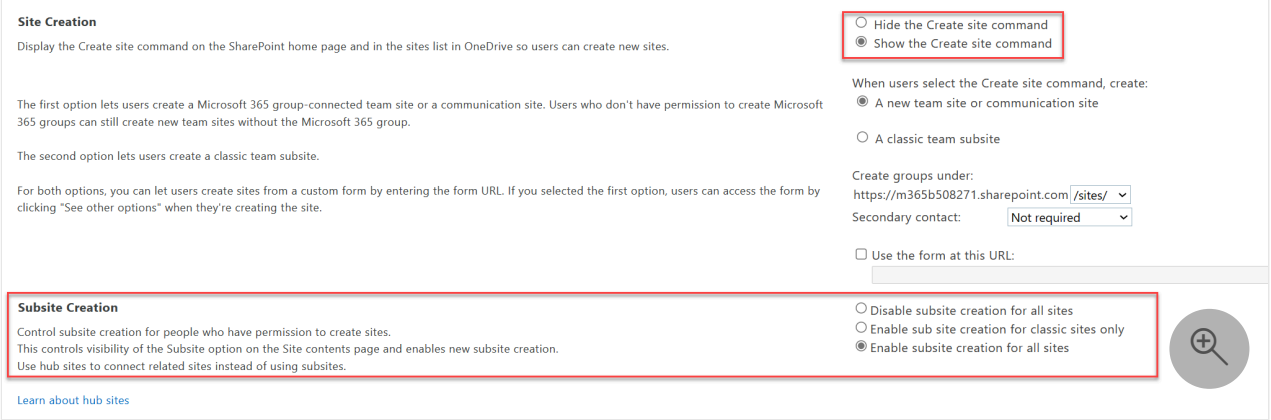
Manage detailed site and subsite creation settings in the classic SharePoint admin center

Admins in the SharePoint admin center can choose to either enable or disable subsite creation across sites or enable for classic sites only. When subsite creation is being disabled, not only will the subsite option be hidden from the command bar including classic, but also users won't be able to create new subsites directly through a URL or API.

> **Note**
>
> For information about classifying Microsoft 365 groups, see Manage Microsoft 365 Groups with PowerShell.

1. In the left pane of the new SharePoint admin center, select **Settings**. At the bottom of the page, select **classic settings page**.

2. Under **Site Creation**, select to show or hide the **Create site** command.



   - If you choose **Disable subsite creation for all sites**, it hides the subsite creation command (including classic) and disable users from being able to create new subsites through a URL or API.
   - If you choose **Enable subsite creation for classic sites only**, users are able to create new subsites for classic sites.
   - If you choose **Enable subsite creation for all sites**, users are able to create new subsites from any SharePoint site.

3. Select **OK** when you're done.

> **Note**

Creating a subsite in OneDrive isn't supported. You'll see an error, “New subsites aren't available in this site. Create a new site instead.”

Tip

Instead of using subsites, we recommend that you use hub sites. SharePoint hub sites allow you to group similar articles and content together using modern architecture design. Plan to create hub sites.

Restrict OneDrive and SharePoint site creation by users

The restricted site creation feature IT administrators use SharePoint Online Management Shell to designate which Microsoft Entra security groups in their tenant can create OneDrive and SharePoint sites.

You can choose between two ways to manage site creation within your tenant: deny mode (the specified groups can't create sites) and allow mode (only the specified groups can create sites). When you enable this feature for your tenant, restricted site creation defaults to **deny** mode.

Restricted site creation policies only control site provisioning capabilities and not site access permissions.

Prerequisites

Your organization needs **SharePoint Advanced Management Plan 1**. See Prerequisites: SharePoint Advanced Management Plan 1 add-on.

Also see the requirements for the SharePoint Online PowerShell module.

Site types for restricted site creation by users

Each restricted site creation policy includes a *site type* specifying the types of sites users in the specified groups are either allowed or denied from creating.

Expand table

Site type	Applies to
All	OneDrive and all SharePoint sites
SharePoint	All SharePoint sites (but not OneDrive)
OneDrive	Only OneDrive
Team	Only SharePoint team sites (classic)
Communication	Only SharePoint communication sites

You can specify up to 10 Microsoft Entra security groups for each site type.

How do restricted site creation deny and allow modes work?

The restricted site creation by users mode is shared across all site type policies. You can't use deny mode for one site type and allow mode for a different site type.

When you set restricted site creation by users to **deny** mode, users can't create a site if they belong to any security group configured for a site type that matches the site they want to create. For example, if a user is in a group listed under the All, SharePoint, or Communication site types, they can't create a SharePoint communication site.

When you set restricted site creation by users to **allow** mode, users can only create a site if they belong to a security group configured for a site type that matches the site they want to create. For example, a user can create a OneDrive site only if they're in a group listed under the All or OneDrive site types.

Current limitations of restricted site creation by users

- Only Microsoft Entra security groups (mail-enabled or non-mail-enabled) are supported at this time.
- You can configure up to 10 security groups per site type.
- This feature isn't currently available for Microsoft 365 government cloud environments, such as GCC, GCC-High, DoD, or Microsoft 365 operated by 21Vianet.

Manage restricted site creation by users

The Set-SPORestrictedSiteCreation and Get-SPORestrictedSiteCreation commands allow administrators to configure and view the restricted site creation feature and policies for the tenant.

> **Important**
>
> You must use version 16.0.25513.12000 (published November 2024) or later of the SharePoint Online Management Shell for these commands to function properly. Earlier versions don't have the current list of site types and don't operate correctly.

Enable restricted site creation by users

To enable restricted site creation by users, run the following command in the SharePoint Online Management Shell:

PowerShell

```
Set-SPORestrictedSiteCreation -Enabled $true
```

Restricted site creation by users starts in deny mode without any policies, and doesn't affect any users by default.

Set Allow or Deny mode for restricted site creation by users

After you turn on the restricted site creation by users feature, decide whether you want to deny certain groups of users from creating sites or allow certain groups to create sites.

For example, the following command sets restricted site creation to deny mode:

PowerShell

```
Set-SPORestrictedSiteCreation -Mode Deny
```

> **Important**
>
> Swapping between the two modes removes all existing site type configurations. The restricted site creation feature only supports either all deny or all allow configurations.

Configure policies for site types

You can specify a comma-separated list of up to 10 Microsoft Entra security groups for each site type. For example, if restricted site creation is in deny mode, the following command creates a policy blocking users in either of the following two groups from creating any SharePoint site.

PowerShell

```
Set-SPORestrictedSiteCreation -SiteType SharePoint -RestrictedSiteCreationGroups
"00aa00aa-bb11-cc22-dd33-44ee44ee44ee,11bb11bb-cc22-dd33-ee44-55ff55ff55ff"
```

> **Note**

> You must specify Microsoft Entra security groups by using the Object ID shown in the Microsoft Entra admin center.

To clear the configuration for a site type, specify "" for the RestrictedSiteCreationGroups:

PowerShell

```
Set-SPORestrictedSiteCreation -SiteType All -RestrictedSiteCreationGroups ""
```

View configuration

Use the following command to view the existing restricted site creation configurations:

PowerShell

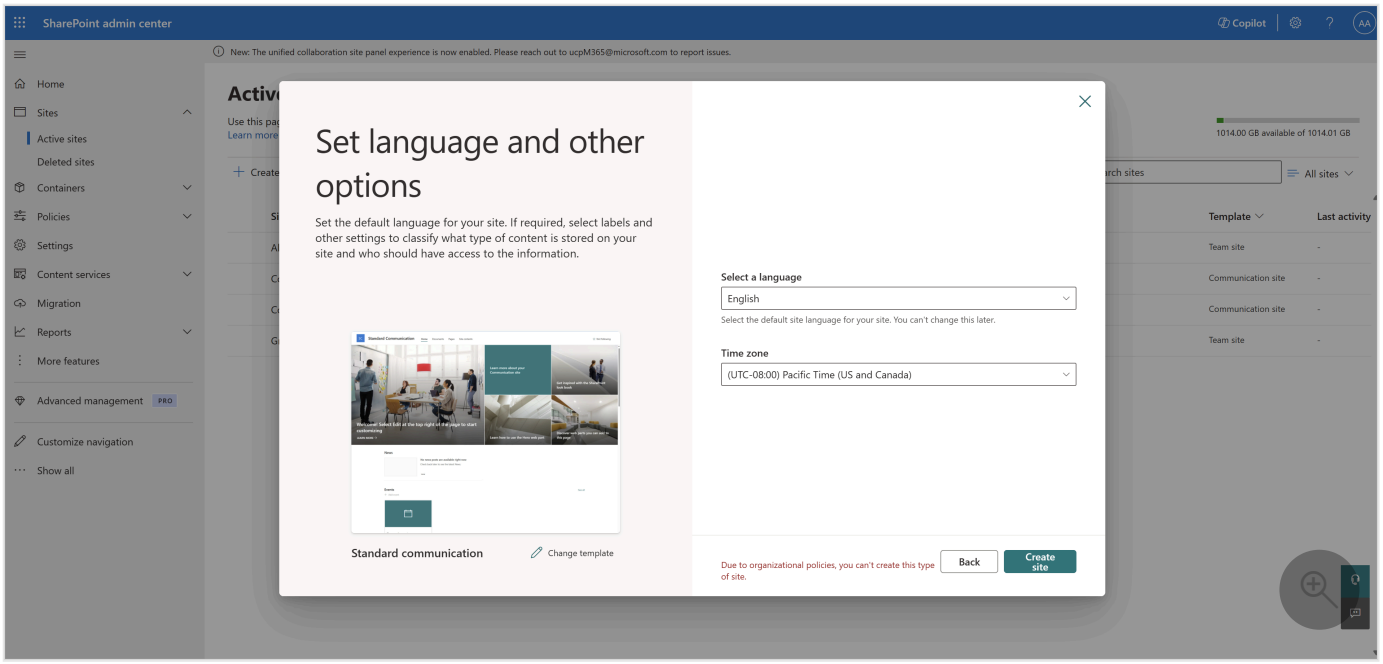
```
Get-SPORestrictedSiteCreation
```

What messages do users see when restricted from site creation?

When a user is blocked from creating a site by a restricted site creation by users policy, they receive a message depending on the type of site they're creating and how they're creating it. See the following examples for reference:

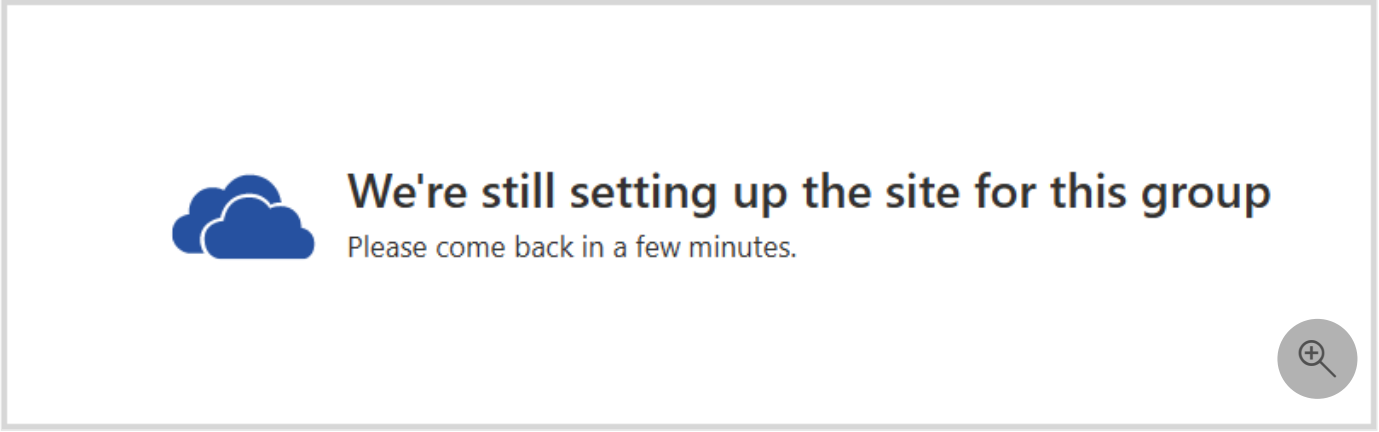
Example 1: User can't create a communication site

When a user creates a communication site from the web, they see the error message "Due to organizational policies, you can't create this type of site."



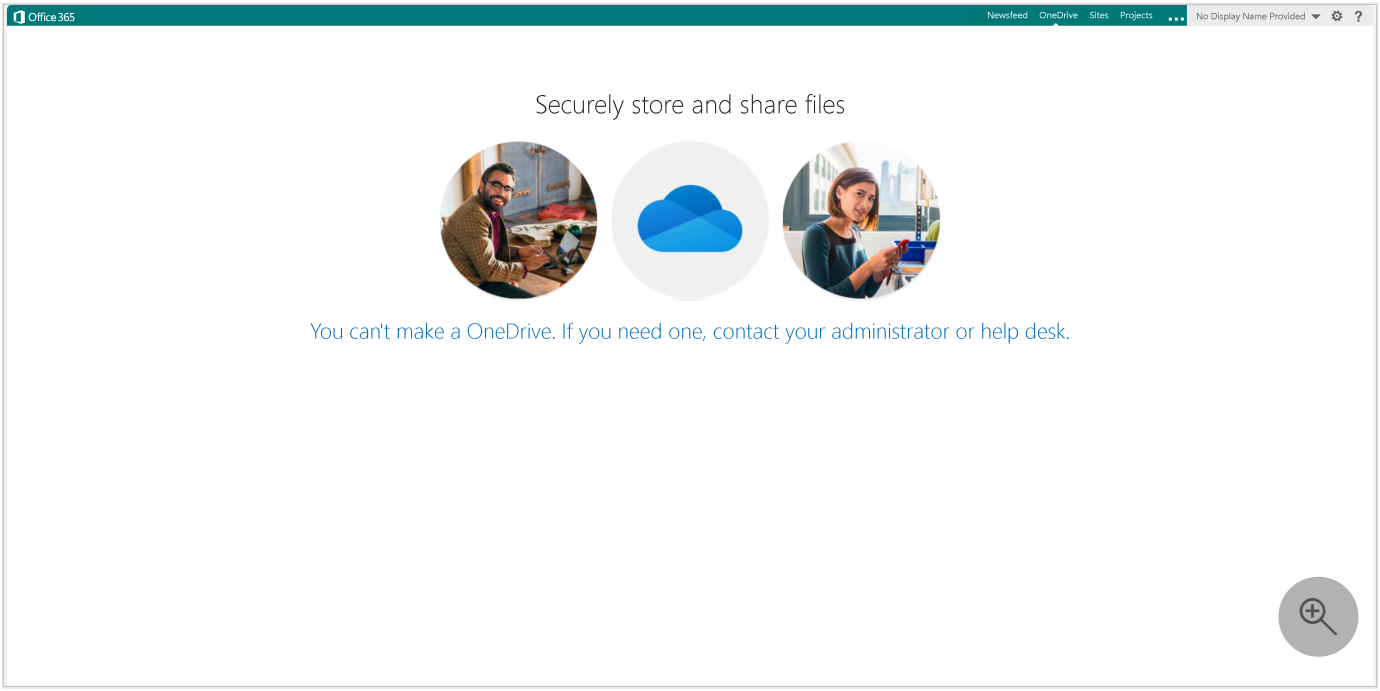
Example 2: User can't create a team site

When a user creates a team site from the web, the user sees the message "We're still setting up the site for this group," but the site isn't created.



Example 3: User can't access OneDrive

When first signing in to their OneDrive from the web, the user sees the error message "You can't make a OneDrive. If you need one, contact your administrator or help desk."



Example 4: User can't create a site using PowerShell

When creating sites through the SharePoint Online Management Shell, the cmdlet fails with the exception "Due to organizational policies, you can't create this type of site."

Related articles

- Microsoft SharePoint Premium – SharePoint Advanced Management overview
- Set-SPORestrictedSiteCreation
- Get-SPORestrictedSiteCreation

Last updated on 09/02/2026

Manage site storage limits in SharePoint in Microsoft 365

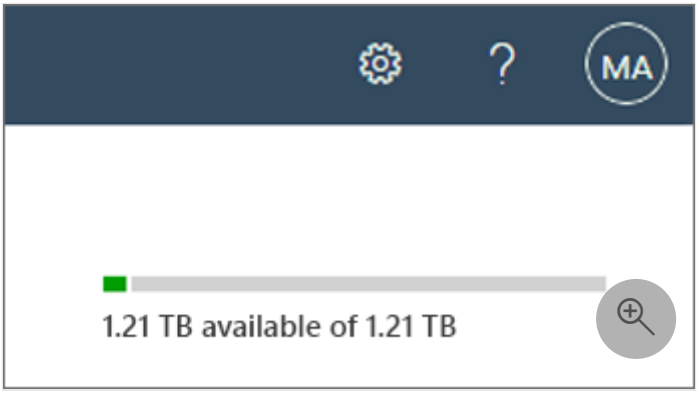
The amount of SharePoint space your organization has is based on the number of licenses (see SharePoint Limits) you have. If you're a Global Administrator in Microsoft 365, you can Add storage space for your subscription if you run out of storage space.

> **Important**
>
> Microsoft recommends that you use roles with the fewest permissions. Using lower permissioned accounts helps improve security for your organization. Global Administrator is a highly privileged role that should be limited to emergency scenarios when you can't use an existing role.

View the total and available storage space for your organization

1. Go to Active sites in the SharePoint admin center, and sign in with an account that has admin permissions for your organization.

2. In the upper right of the page, see the amount of storage available and the total storage for your subscription. (If your organization has configured Multi-Geo in Microsoft 365, you can point to the bar to see the amount of storage used in the current geo location and all other geo locations.)



> **Note**

Storage usage doesn't include changes made within the last 24-48 hours. SharePoint storage is calculated in binary Gigabytes (GB), where 1 GB = 2^{30}. Deleted sites in the Recycle Bin do not count toward the organization's total storage usage.

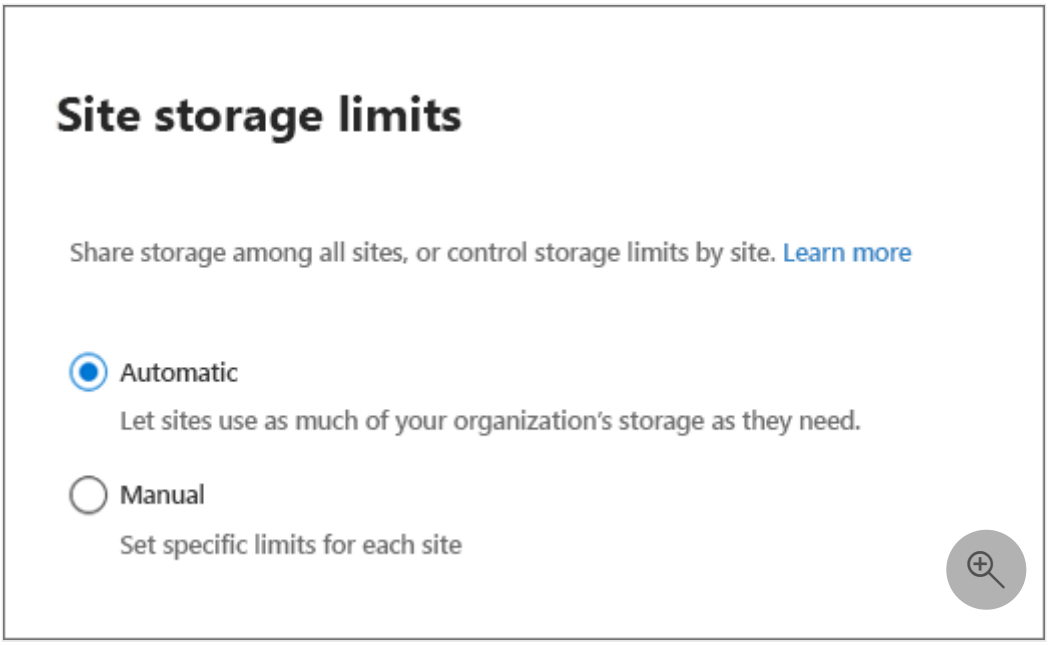
Set automatic or manual site storage limits

By default, your SharePoint storage is available in a central pool from which all sites can draw. You, as a SharePoint Administrator and above, don't need to divvy up storage space or reallocate space based on usage. That's all handled automatically: sites use what they need when they need it. If you previously set storage limits manually and switch to using pooled storage, SharePoint resets all the limits to 25 TB (25600 GB). (Note that the total storage for your organization might be less than 25 TB.)

If you prefer to fine-tune the storage space allocated to each site, you can set your storage management option to "manual" and specify individual site storage limits.

> **Note**
>
> Some functionality is introduced gradually to organizations that have opted in to the Targeted release option in Microsoft 365. This means that you might not yet see some features described in this article, or that some of the features (described in this article) might look different.

1. Go to Settings in the SharePoint admin center, and sign in with an account that has admin permissions for your organization.
2. Select **Site storage limits**.



3. Select **Automatic** or **Manual**, and then select **Save**.

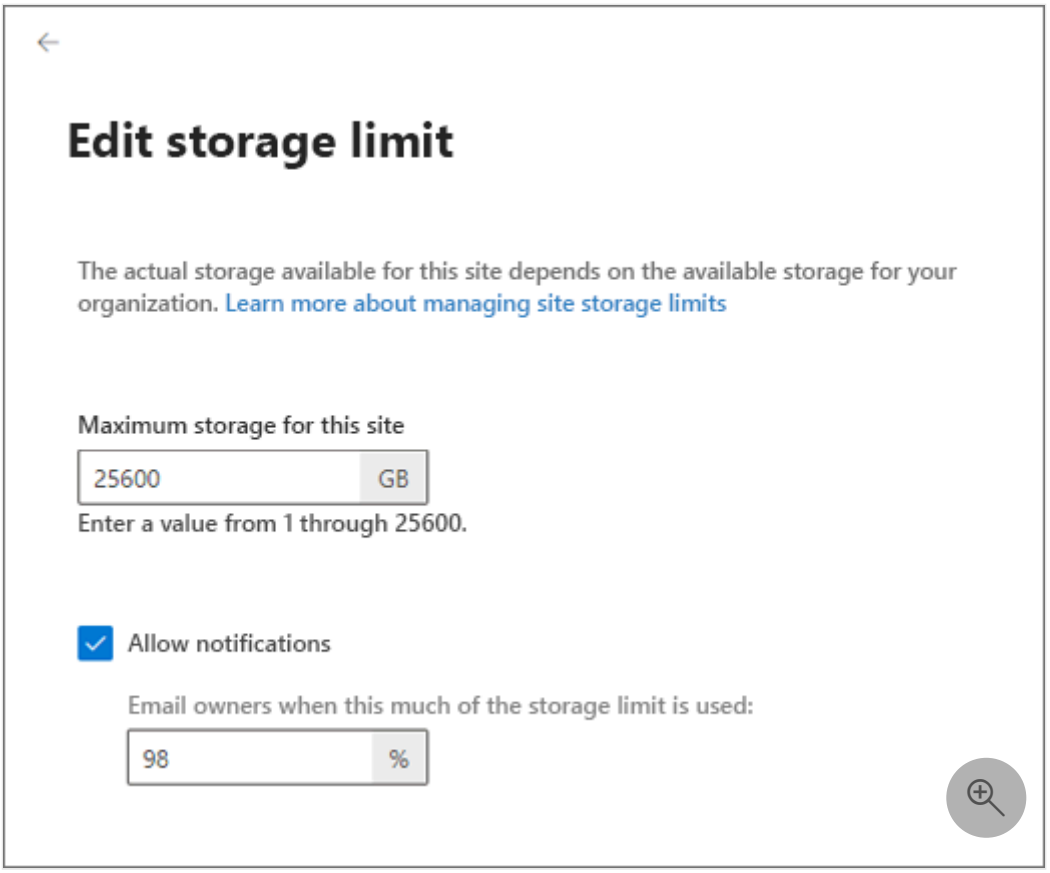
Manage individual site storage limits

Follow these steps to specify individual site storage limits *when your storage management option is set to "manual."* We recommend that you also set an email alert so that you and the site owners can be notified when sites are nearing the storage limit. To learn how to set the default storage limit for new sites, see Manage site creation.

1. Go to Active sites in the SharePoint admin center, and sign in with an account that has admin permissions for your organization.

2. In the left column, select the site, or for a channel site, select the link in the **Channel sites** column.

3. On the **General** tab, under **Storage limit**, select **Edit** to open the edit storage limit panel.



4. Enter the maximum storage in GB for the site.

> ⓘ **Note**
>
> The maximum value you can enter is 25600 GB, although this may be more space than your organization has. To learn how your total storage is calculated, see SharePoint Limits.

5. Make sure **Notifications** is turned on to send an email to site owners when the site approaches the storage limit. Then, enter a value as a percent for how full you want the storage to be when the email is sent.

6. Select **Save**.

If a site runs out of storage, site admins can request for more by performing the following steps:

1. Go to the Site Settings page.

2. Under **Site Collection Administration**, select **Storage Metrics**.

> ⓘ **Note**

Depending on your site, you may need to perform the following steps to see the **Site Collection Administration** section:

On the upper right corner of your site, select **Settings** and then select **Site Settings**. If you don't see **Site settings**, select **Site information** and then select **View all site settings**.

3. Select **Request more quota** in the upper right.

This step sends a storage request email to the Global Administrators in the organization.

Last updated on 07/30/2026

Change a site address

> **Important**
>
> There is currently a known issue caused by the retirement of BCS that is affecting changing of site addresses. The fix is currently being worked on. Currently, if you are facing issues, please try changing the site address using the PowerShell cmdlet while using the -SuppressBcsCheck parameter.

> **Note**
>
> This feature isn't supported for Microsoft 365 Sovereign Cloud customers, except GCC Low.

As a SharePoint Administrator in your organization, you can change the URL for the following types of SharePoint sites (previously called "site collections"):

- Microsoft 365 group-connected team sites
- Modern team sites that don't belong to a Microsoft 365 group
- Communication sites
- Classic team sites

Changing the site address isn't supported in the following situations:

- The Publishing feature is currently activated or was previously activated for the site.
- The site contains more than 15 million documents.

You can change only the address of the site within the URL, for example:

https://contoso.sharepoint.com/sites/*project-x*
to https://contoso.sharepoint.com/sites/*project-y*

You can't move the site from "/sites" to "/teams." For info about changing your SharePoint domain name, see Change your SharePoint domain name.

It can take about 10 minutes to change the site address (depending on the size of the site), and the site is read-only during this time. We recommend changing addresses during times when site usage is low.

You can change the address of up to 100 sites at a time. To change another site address, wait for ongoing changes to finish.

> **Note**
>
> If you need to revert a site address change, follow the steps in Revert a site address change.

How do I communicate the address change to users?

Before you change the address of a site, it's important to communicate the change to site users (generally anyone with the ability to edit or view the site). This can help reduce user confusion and calls to your help desk. Review the effects of changing a site address and let users know the following information:

- The planned date of the change
- The planned URL
- Users should close their files and not make edits during the address change
- Users should check the site recycle bin to make sure it contains no files they want to keep
- File permissions and sharing stay the same

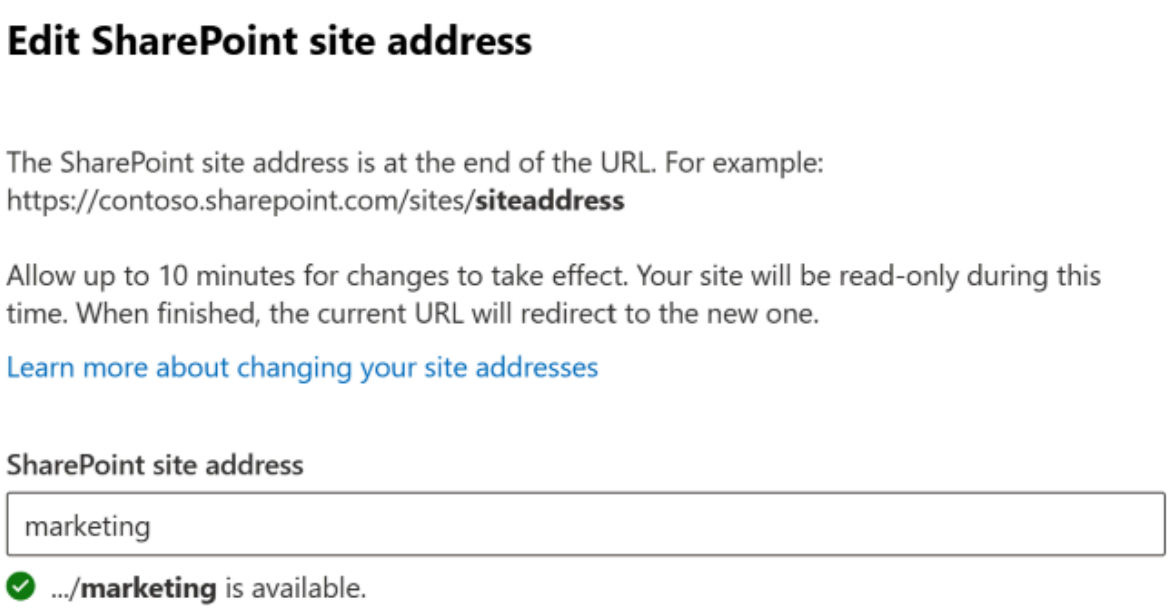
How do I change a site address in the SharePoint admin center?

1. Go to **Active sites** in the new SharePoint admin center, and sign in with an account that has admin permissions for your organization.

   > **Note**
   >
   > If you have Office 365 operated by 21Vianet (China), sign in to the Microsoft 365 admin center, then browse to the SharePoint admin center and open the Active sites page.

2. Select the site name to open the details panel.

3. On the **General** tab, under **Site address**, select **Edit**.



4. Enter the new site address, and then select **Save**.

> ⓘ **Note**
>
> You can't change the address of hub sites, sites that are locked or on hold, Project Web App (PWA) sites, or sites that have BCS connections.
>
> When you change a site address, we create a redirect at the previous address. If you want to reuse the previous address, you need to delete the redirect. Learn how

How do I change site addresses by using PowerShell?

1. Download the latest SharePoint Online Management Shell.

> ⓘ **Note**
>
> If you installed a previous version of the SharePoint Online Management Shell, go to Add or remove programs and uninstall "SharePoint Online Management Shell."

2. Connect to SharePoint as at least a SharePoint Administrator in Microsoft 365. To learn how, see Getting started with SharePoint Online Management Shell.

3. Run the following command to verify that the site address can be changed:

PowerShell

```
Start-SPOSiteRename -Identity https://contoso.sharepoint.com/sites/project-x -
NewSiteUrl https://contoso.sharepoint.com/sites/project-y -ValidationOnly
```

4. Run the following command to change the site address:

PowerShell

```
Start-SPOSiteRename -Identity https://contoso.sharepoint.com/sites/project-x -
NewSiteUrl https://contoso.sharepoint.com/sites/project-y
```

For more information about this cmdlet, see Start-SPOSiteRename.

What are the effects of changing a site address?

While the change is in progress, the site is set to read-only, and a redirect is created. After the change is complete, users are redirected to the new URL if they've saved the site as a favorite, or if they select a link to the site.

Apps
If apps in your organization refer to the site's URL, you might need to republish the apps when you change the site's address.

Custom Forms Created in Power Apps
You need to recreate the Custom Form after the site address change.

Hub sites
If the site is associated with a hub, you must reassociate it after the site address is changed.

InfoPath forms
InfoPath forms that refer to URLs might not work after the site address is changed.

List View web part
If a List View web part on a page is scoped to a specific folder in that list, the web part might display an error after the site URL is changed. To fix this issue, either edit the web part and reset the folder path or remove the web part from the page, and then add it again.

Microsoft Forms If the site is a Microsoft 365 group-connected site that has forms in Microsoft Forms, any File Upload questions in forms break. To fix this issue, recreate the file upload questions to allow responders to upload files again.

OneNote If users have a notebook open during the site address change, they see a notebook sync error. After the address is changed, the following OneNote apps will automatically detect and seamlessly sync notebooks to the new site URL:

- OneNote desktop app – Version 16.0.8326.2096 and later
- OneNote for Windows 10 – Version 16.0.8431.1006 and later
- OneNote mobile app – Version 16.0.8431.1011 and later

Users don't need to sign in again or take any other action.

Permissions People who have permission to access the site can access the site during and after the site address change.

Recent lists inside Office apps The Word, Excel, and PowerPoint desktop apps and apps for the web will show the new URL after the change.

Recycle bin You can restore files in the recycle bin according to the usual deletion timeframe.

SharePoint mobile apps for Android and iOS The SharePoint mobile apps detect the site's new URL. Make sure that users have updated their apps to the latest version.

SharePoint web parts Any embedded URLs in any SharePoint web parts (News, List, etc.) won't be updated and may break. This includes page thumbnail images in news posts existing on the site. After the site address is changed, you might need to update individual web parts to use the new URL.

SharePoint workflow 2013 SharePoint workflow 2013 will need to be republished after the site address is changed.

Sharing links
After the site address is changed, sharing links will automatically redirect to the new URL.

Site customizations and embedded code You might need to fix site customizations and embedded code that refer to URLs after the site address change. Changing the site address preserves data stored in SharePoint but won't change URL dependencies in custom solutions.

Synced locations The OneDrive sync app will automatically detect and seamlessly transfer syncing to the new site URL after the site address has been changed. Users don't need to sign in again or take any other action. (Version 17.3.6943.0625 or later of the sync app required.) If a user updates a file while the site address is being changed, they see a message that file uploads are pending during the change.

Microsoft 365 groups The email address of the group won't be renamed. The group name is updated only if the site name is updated during the rename process.

Teams (for Microsoft 365 group-connected sites) When the site address change is complete, users are able to access their SharePoint files in the Teams app, with the following limitations.

Expand table

Functionality	Limitation
Viewing files in Teams	Files shared in channels before the address were changed can be viewed in the Teams app on the channel's Files tab. They can also be viewed in Office apps for the web from the channel's Files tab or the conversation. To view Word, Excel, and PowerPoint files in the desktop apps: Select the "Open in Desktop" option from the channel's Files tab. Open the file in the Office app for the web, and then select "Open in Desktop".
Uploading files to channels	Uploading files from a computer or OneDrive to a channel conversation will work after a user visits the Files tab for any channel in the site.
File app – Microsoft Teams page	The Microsoft Teams page in the Teams File app will work after a user visits the Files tab for any channel in the site.
Teams mobile app	Open and download will continue to work. To edit a Word, Excel, or PowerPoint file in the site, use the Office app for the web or the desktop app. Files shared after the site address was changed can be edited in the Office mobile apps.

How do I revert a site address change?

If you need to change the address of a site that was previously changed, we recommend not renaming the site again. This can cause issues if you later want to use the current address for another site. Instead, we recommend that you return the site to its original address. To do so, use an additional site rename and delete certain redirect sites. Learn how to delete redirect sites.

For a case where you changed https://contoso.sharepoint.com/sites/*project-x* to https://contoso.sharepoint.com/sites/*project-y* and want to revert back, the steps to follow are:

1. Delete the redirect from *project-x* to *project-y* by using the Remove-SPOSite cmdlet on the *project-x* address.

2. Initiate a new site address change from *project-y* to *project-x*.

3. Delete the redirect from *project-y* to *project-x* by using the Remove-SPOSite cmdlet on the *project-y* address.

   After following these steps, you should be back to the original state before the site address change.

Last updated on 12/22/2025

Manage site redirects

When you change a SharePoint site address, such as moving a site to a different geo location, or swapping a site, we automatically create redirects to ensure that prior URLs continue to work. These redirects are sites that use a special site template at the prior site URL.

For example, if you changed a site address from https://contoso.sharepoint.com/sites/*OldSiteName* to https://contoso.sharepoint.com/sites/*NewSiteName*, or if you moved a site from https://*contoso*.sharepoint.com/sites/SiteName to https://*contosoEUR*.sharepoint.com/sites/SiteName, we place a redirect (Template type REDIRECTSITE#0) at the old URL. This redirect contains special headers and logic to redirect your browser requests to the new site.

In some cases, you might want to free up the old URL to use it for a new site. To free up the old URL, you need to delete the redirect.

> **Note**
>
> After you delete a redirect, any request to that URL won't get redirected. This means that any bookmarks, links, or Shared With Me references aren't routed to the new URL.

How do I remove a redirect?

1. Download the latest SharePoint Online Management Shell.

   > **Note**
   >
   > If you installed a previous version of the SharePoint Online Management Shell, go to Add or remove programs and uninstall "SharePoint Online Management Shell."

2. Connect to SharePoint as a Global Administrator or SharePoint Administrator in Microsoft 365. To learn how, see Getting started with SharePoint Online Management Shell.

3. Run the following command:

   PowerShell

   ```
   Remove-SPOSite -Identity https://contoso.sharepoint.com/sites/OldSiteName
   ```

   > **Note**

If you get an error message "The operation is not supported for the site," make sure a retention policy isn't applied to the old or new URL for the site. You might need to remove the retention policy to delete the redirect.

4. When prompted, confirm that you want to delete the redirect.

You can confirm that the redirect is deleted by browsing to the URL. It should return a 404 error. You can also run `Get-SPOSite -Identity https://contoso.sharepoint.com/sites/OldSiteName`. It returns "we cannot get the site."

> **Note**
>
> You might need to clear your browser history and cache before browsing to the URL. Otherwise, it may take longer for the redirect site deletion to reflect, depending on individual browser settings.

How do I get a list of all redirect sites?

To get a list of all redirect sites, run the following command:

PowerShell

```
Get-SPOSite -Template REDIRECTSITE
```

Last updated on 12/22/2025

Lock and unlock sites

By using the permissions of a SharePoint Administrator or more in Microsoft 365, you can block access to a site or make a site read-only. Use Microsoft PowerShell to change the lock state of the site.

> **Note**
>
> You can't set the lock state on the root site. If the SharePoint administrator changes the SharePoint domain, OneDrive and SharePoint sites in a locked state (excluding sites connected to Microsoft Teams channels or Microsoft 365 Groups) are updated to the new domain.

Change the lock state for a site

Follow these steps to change the lock state for a site by using PowerShell.

1. Install the SharePoint Online Management Shell by downloading and running the SharePoint Online Management Shell or installing the module from the PowerShell Gallery. If you installed a previous version of the SharePoint Online Management Shell, go to **Add or remove programs** and uninstall SharePoint Online Management Shell.

2. Connect to SharePoint as a SharePoint Administrator in Microsoft 365. To learn how, see Getting started with SharePoint Online Management Shell.

3. At the PowerShell command prompt, type the following command, and then press Enter.

   PowerShell

   ```
   Set-SPOSite -Identity "<SiteURL>" -LockState "<State>"
   ```

   Where:
   `SiteURL` is the URL of the site that you want to lock or unlock and `State` is one of the following values:

   - **Unlock** to unlock the site and make it available to users.
   - **ReadOnly** to prevent users from adding, updating, or deleting content. A message appears on the site stating that the site is under maintenance and is read-only.

- **NoAccess** to prevent users from accessing the site and its content. If you provided a `NoAccessRedirectUrl` value for your organization, traffic is redirected to the URL you specified. If you didn't set this URL, a 403 error is displayed.

> **Note**
>
> If the site was closed and made read-only through a site closure policy, the PowerShell command to unlock the site doesn't work.

PowerShell

```
Set-SPOTenant -NoAccessRedirectUrl 'https://www.contoso.com'
```

For more info about the `LockState` parameter, see Set-SPOSite. For more info about the NoAccessRedirectUrl parameter, see Set-SPOTenant.

Last updated on 06/17/2026

Modernize your root site

When Microsoft SharePoint is set up for an organization, a root (or top-level) site is created. Before April 2019, the site was created as a classic team site. Now, a communication site is set up as the root site for new organizations. If your environment was set up before April 2019, you can modernize your root site in three ways:

- If you have a different site that you want to use as your root site (a communication site or modern team site that isn't connected to a Microsoft 365 group), replace (swap) the root site with the other site.
- If you want to keep using the classic team site but add a new modern home page and enable full-width pages with horizontal navigation, enable the communication site experience on the site.
- If you want to continue using the classic team site, enable the modern site pages library experience and set a modern page as the home page of the root site. This gives users a modern team site experience with the left navigation.

> **Important**
>
> Before you launch an intranet landing page at your root site location, we strongly encourage you to review the guidance about launching healthy portals.
> Some functionality is introduced gradually to organizations that have opted in to the Targeted release option in Microsoft 365. This means that you might not yet see some features described in this article, or they might look different.

What's the root site?

The root site for your organization is one of the sites that's provisioned automatically when you purchase and set up a Microsoft 365 or Microsoft 365 plan that includes SharePoint. The URL of this site is typically *contoso*.sharepoint.com, the default name is "Communication site," and the owner is Company Administrator (all Global Administrators in the organization). The root site can't be connected to a Microsoft 365 group.

> **Warning**

The root (top-level) site for your organization can't be deleted. If you're a SharePoint Administrator and above in Microsoft 365, you can replace the root site with a different site.

Microsoft recommends that you use roles with the fewest permissions. Using lower permissioned accounts helps improve security for your organization. Global Administrator is a highly privileged role that should be limited to emergency scenarios when you can't use an existing role.

Replace your root site

Before you begin, make sure you:

1. Note any "Featured links" that have been added on the SharePoint start page. You'll need to add them again after you replace the root site. Learn how
2. Review your source site to make sure it has the same policies, permissions, and external sharing settings as your current root site.
3. Communicate the upcoming change to users. This can help reduce user confusion and calls to your help desk. If users are using files on the sites you're replacing, ask them to close the files and check the site recycle bin to make sure it contains no files they want to keep.

By default, a site redirect will be created that will redirect traffic from the source site to the root site. For info about site redirects, see Manage site redirects.

If you've turned on audit log search, the following events can be recorded:

- Scheduled site swap: A site replacement (swap) was scheduled at this time
- Swapped site: A site replacement (swap) completed successfully at this time
- Failed site swap: A site replacement (swap) failed at this time and won't be tried again

Limitations

- The site you select as the new root site must be a communication site (SITEPAGEPUBLISHING#0) or a modern team site that isn't connected to a Microsoft 365 group (STS#3) and where **the publishing feature has never been activated.**
- When you replace the root site, both the current site and the new site can't be hub sites or associated with a hub. If either site is a hub site, unregister it as a hub site, replace the root site, and then re-register the site as a hub site. If either site is associated with a hub, disassociate the site, replace the root site, and then reassociate the site. Learn how to manage hubs in the new SharePoint admin center

- Replacing the root site with another site replaces the entire site collection with the new site collection. If your current root site has subsites, they'll be archived.
- The site you select as the new root site must be within the same domain as the current root site.
- If the site is on hold, you'll receive an informative error and you can't replace the site.
- You as the admin must also be a member of the site that you are replacing.

Use the new SharePoint admin center

We recommend replacing the root site at a time when site usage is low.

1. Go to **Active sites** in the SharePoint admin center, and sign in with an account that has admin permissions for your organization.

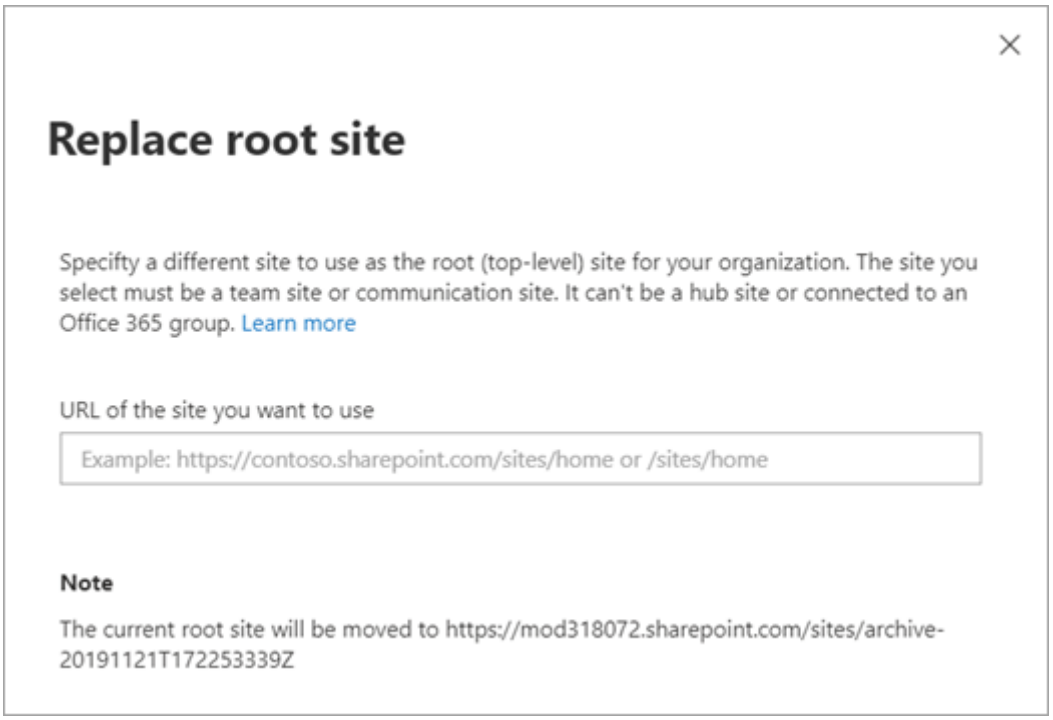
   > **Note**
   >
   > If you have Office 365 operated by 21Vianet (China), sign in to the Microsoft 365 admin center, then browse to the SharePoint admin center and open the Active sites page.

2. In the upper right, make sure the **All sites** view is selected.

3. In the URL column, select to sort A to Z so the current root site appears at the top of the list.

4. Select the root site (https://contoso.sharepoint.com).

5. Select **Replace site** on the command bar.



6. In the **URL of the site you want to use** box, enter the full or relative URL of the site that you want to become the new root site.

7. Select **Save**.

   While the root site is being replaced, it might return a "not found" (HTTP 404) error for few minutes.

   After you replace the root site, content must be recrawled to update the search index. This might take some time depending on factors such as the amount of content in these sites. Anything dependent on the search index might return incomplete results until the sites have been recrawled.

8. If the new root site was an organization news site, update the URL. Get a list of all organizational news sites

9. If you disabled site redirects, you'll need to update sharing links and any apps or files (like the OneDrive sync app and OneNote files) to refer to the new URL.

> ⓘ **Note**
>
> For info about using PowerShell to replace (swap) the root site, see Invoke-SPOSiteSwap.
>
> Project Server sites might need to be validated to make sure they're still associated correctly.

Last updated on 06/25/2026

Plan, build, and launch a SharePoint home site for your organization

A SharePoint home site provides a customized landing experience that reflects the organization's brand, voice, and priorities. A SharePoint home site also serves as the gateway to other portals in your organization's intranet. It is the base SharePoint component when designing and implementing for the SharePoint app in Teams (formerly Viva Connections). Think of SharePoint home sites as an *add-on* to your intranet design. SharePoint home sites are communication sites that have special capabilities such as being marked as an official source of news in the organization. Consider making your organization's root site the SharePoint home site.

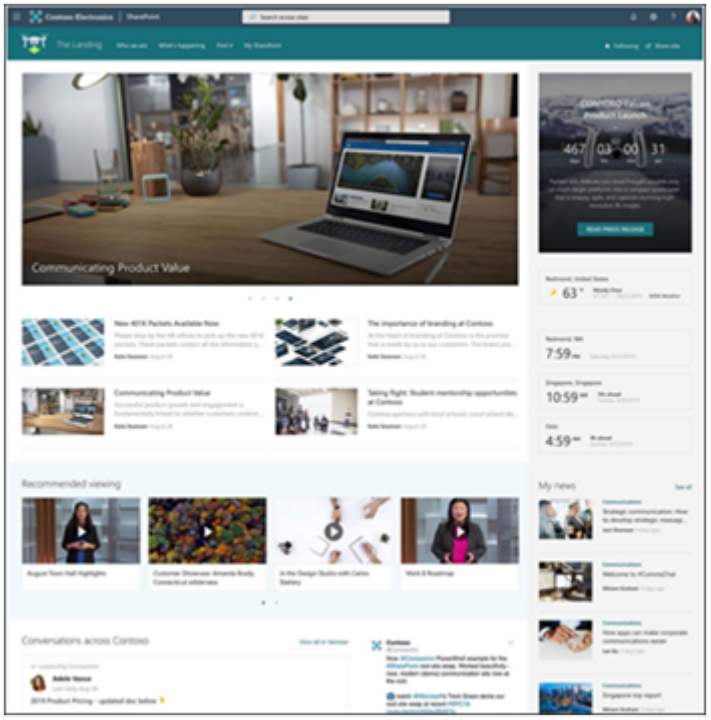
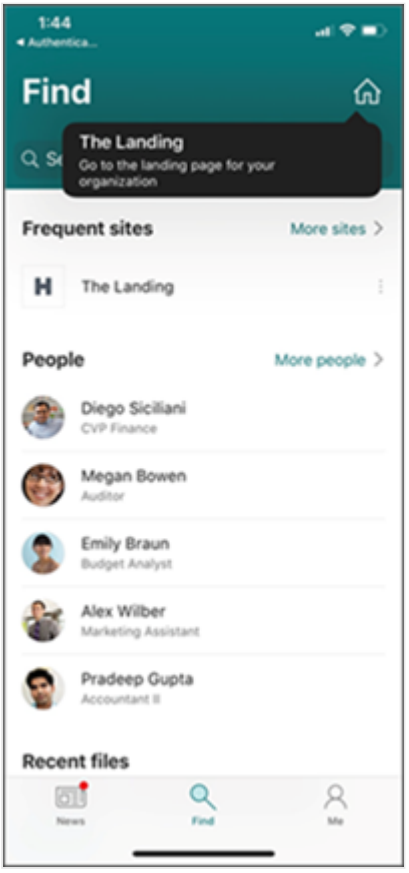
If you've already created the communication site and are ready to specify it as your home site now, learn how to configure the SharePoint app in Teams.

> **Note**
>
> - You must have an Enterprise (E), Frontline (F), or Academic (A) license type to create a Connections experience.
> - Users with a Microsoft 365 subscription (E, F, or A license) are limited to creating and using one experience. If you want to create or use two or more experiences (up to 50), then every user in your organization must have a Microsoft Viva Suite or Viva Communications and Communities license. See Microsoft Viva plans and pricing for more info.
> - You must have SharePoint admin permissions to access the SharePoint admin center.

Use a SharePoint home site to:

- Provide a gateway to other high-traffic portals.
- Connect people with an intranet-wide search experience.
- Showcase targeted news and content.
- Use the SharePoint app in Teams to integrate your intranet into Microsoft Teams.

Expand table

Example of a SharePoint home site:	View in the SharePoint mobile app:
	

SharePoint home site features explained:

SharePoint home sites are unlike any other site in SharePoint. When you set a SharePoint communication site as a home site, you'll automatically apply special capabilities that make the SharePoint home site an ideal landing destination for your organization's intranet.

Search for content across the entire intranet

SharePoint home sites allow users to search for content (such as sites, news, and files) across the entire intranet rather than searching just the site like typical SharePoint sites. The search scope for the SharePoint home site searches the entire intranet instead of just the site collection like a typical site.

Official source of organizational news

By default, a SharePoint home site is set as the organizational news source. News posts that are created from the SharePoint home site automatically become official organizational news and take priority on the SharePoint start page. Administrators can set additional sites as official organizations news sources in the SharePoint admin center.

Enable and customize global navigation in the SharePoint app bar

The SharePoint app bar features a global navigation option that displays intranet navigational nodes and resources no matter where users are in SharePoint. To take full advantage of this feature, you must have a SharePoint home site. Learn more about how to enable and customize global navigation in the SharePoint app bar.

Before getting started

Before you get started planning and building your SharePoint home site, review best practices and considerations.

Best practices for creating SharePoint home sites

- A SharePoint home site that will be used by the entire organization needs to be inclusive and easily accessible on all devices.
- The site needs to be inclusive and easily accessible on all devices, consider other languages that might be needed.
- The SharePoint home site will be viewed by a high volume of users. Make sure you manage site performance through the planning and building phases.
- Links in the SharePoint home site's navigation can direct users to content in addition to global navigation, which can be used to lead users to universally used resources and portals.
- The SharePoint home site should be discoverable by adding an entry point to Microsoft 365 Copilot and a featured link on the SharePoint start page.
- News published from the SharePoint home site should be relevant to the entire organization.

Considerations

- Align the branding on the SharePoint home site to the overall intranet brand where possible.
- Organizations with many portals and resources should consider making your SharePoint home site a hub site to expand navigational options and easily sync permissions and branding across many sites.

- Use a SharePoint home site template like the Organization home template when creating a new site to jump-start the design process.

Summary of how to get a SharePoint home site for your organization

Since SharePoint home sites are the gateway to your intranet, you want to prioritize content and resources that are relevant to most users. Work with business owners and stakeholders to organize and align the flow of information and the navigational design. Then, use the Page diagnostics for SharePoint tool to ensure to best viewing experience. Next, set your SharePoint communication site as a home site in the SharePoint admin center. Finally, use the Portal launch scheduler to plan the launch of your new site and make the site discoverable by adding links to key entry-points in the Microsoft 365 experience.

Expand table

Plan	Build	Launch and manage
- Align objectives with partners and business owners - Organize priority content - Design way finding for the SharePoint home site and global navigation - Think about branding - Use audience targeting on navigational links, news, and web parts	- Upload and organize site assets and content like files and logos (64x64px). - Customize the site to align with the rest of the intranet - Apply audience targeting - Turn on a content approval flow - Use PowerShell to turn the SharePoint comm site into a home site - Swap the root site location with the SharePoint home site - Measure site health and performance - Test on all devices	- Share the site with your organization - Use the Portal launch scheduler to release the new site in phases - Make the SharePoint home site discoverable - Announce the launch of the SharePoint home site using various communication channels - Monitor site usage and analytics

Plan your SharePoint home site

A great SharePoint home site starts with a plan. Because your SharePoint home site is essentially the gateway to your intranet, you want to collaborate with other business owners such as human resources, leadership teams, and even your legal team to ensure the most important and universal resources are accessible for everyone in the organization.

Expand table

Icon	Action	Get started
	Get organized	Start by aligning objectives with stakeholders and organizing priority content and resources. Consider details specific to your organization like if the SharePoint home page needs to be available in more than one language. Use modern SharePoint sites for the home site. Learn more about how modern SharePoint sites and how to create a multi-lingual site and pages.
	Plan navigation	Then, organize the navigational structure for the SharePoint home site itself and global navigation. Consider making the SharePoint home site a hub site if you need to add an extra layer of navigation and make it easier to sync associated site permissions and branding. Learn more about planning site navigation and how to make your SharePoint home site a hub site. Then, review guidance on how to set up global navigation on the SharePoint home site.
	Personalize content	Next, think about the different audiences that your organization serves. Consider how elements on your SharePoint home site like navigational links and certain web parts could benefit from audience targeting to specific audiences. Learn more about audience targeting.
	Gather branding assets	Finally, start gathering assets needed to apply custom branding and other details to your SharePoint home site, like logo files (64x64px recommended), color themes, and any custom solutions. Learn more about how to change the look of your site.
	Consider site performance	Even before you build your site, understand the main elements that make sure your SharePoint home site is healthy. A healthy SharePoint home site optimizes performance to ensure the best possible viewing experience. Use the Page diagnostics for SharePoint tool to make sure the SharePoint home page is healthy before sharing with end users. Learn more about healthy portals and using the Page diagnostics tool for SharePoint.

Build your SharePoint home site

When you've prepared a plan, you're ready to start creating the home site in SharePoint. Start with a communication site, and after you have the general layout finalized, create a SharePoint app in Teams experience from your existing SharePoint home site in the Connections admin center.

Expand table

Icon	Action	Get started
	Create a modern communication site	Start by creating a SharePoint communication site and build out the site by using sections, web parts, and pages. Consider using a mega menu and footer to enhance way finding. See the article on Using web parts to display

Icon	Action	Get started
		content on your SharePoint site for information on creating personalized content for users. Learn how to create a communication site, use modern web parts, and customize your site.
	Apply audience targeting	Next, turn on audience targeting on for the SharePoint home site. By enabling audience targeting, specific content is prioritized to specific audiences in navigational links, news, and certain web parts. Learn more about how audience targeting works and how to apply it to navigational links, news, and web parts.
	Set up a page approval flow	Then, make sure the SharePoint home site is set up for regular content updates. Turn on content approval to ensure only high-quality content is published on the SharePoint home site. Learn how to turn on a page approval flow.
	Swap the root site location with the SharePoint home site	Before you set a communication site as the SharePoint home site, swap the communication site in place of the root site of your tenant as a best practice. The root site for your organization is one of the sites that's provisioned automatically when you purchase and set up a Microsoft 365 plan. If you set up a SharePoint home site first, and then swap locations with your root site, you might lose SharePoint home site settings and need to reapply them. Learn how to swap the root site with the SharePoint home site.
	Set the SharePoint home site	Next, build a SharePoint app in Teams experience from an existing intranet portal.
	Set up global navigation	Then, enable global navigation to allow users to easily navigate to important intranet resources anywhere in SharePoint. Global navigation can only be customized from the SharePoint home site's home page. Learn how to enable and customize global navigation.
	Test site health and the viewing experience	Finally, review portal launch guidance and understand the main elements that make sure your SharePoint home site is healthy. A healthy SharePoint home site optimizes performance to ensure the best possible viewing experience. Use the Page diagnostics for SharePoint tool to make sure the SharePoint home page is healthy before sharing with end users. Learn more about healthy portals and using the Page diagnostics tool for SharePoint.

Launch your SharePoint home site

After you've set your SharePoint home site, it's time to plan the launch and make sure the rest of the organization can find and use the SharePoint home site.

Expand table

Icon	Action	Get started
	Share the site and schedule the portal launch	Start by ensuring your SharePoint home site is healthy, and then its time to share the site with the rest of the organization and schedule the launch. Use the Portal launch scheduler tool to gradually roll out the SharePoint home site to batches of end users. Using a phased approach is ideal to manage any performance issues that might arise and to ensure a positive viewing experience. Learn how about how to use the Portal launch scheduler tool.
	Improve discoverability	Next, make sure people in your organization can easily find the SharePoint home site through a few different entry points in the Microsoft 365 experience. Add a link to the SharePoint home site in the Microsoft app launcher (sometimes called the waffle) and on the SharePoint start page. Learn more about how to add a custom tile to the app launcher and how to add a featured link to the SharePoint start page.
	Engage your audience	Then, let your organization know about the new SharePoint home site resource, and other new elements like global navigation. Consider multiple communication options like a SharePoint news post that can also be shared in email and in Microsoft Teams. Learn more about how to create and post SharePoint news and share it in an email.
	Manage and maintain your SharePoint home site	Finally, when the site is healthy, launched, and being used by the organization, monitor site usage and maintain the site. Site maintenance should include making sure site content is relevant, there aren't any broken links, and that the site stays healthy and performant. Learn how to view usage data and analytics for your site and how to maintain your site over time.
	(Optional) Integrate the SharePoint home site into Microsoft Teams using the SharePoint app in Teams	Expand the reach of the SharePoint home site and help meet users where they're already working by making it easy to access and share content all in one place. After you have a SharePoint home site and the global navigation enabled and customized in the SharePoint app bar, you can integrate the SharePoint home site into Microsoft Teams.

SharePoint home site FAQs

Q: Are SharePoint home sites set in the Microsoft 365 admin center of SharePoint admin center? Starting in July 2026, use the SharePoint admin center to set a SharePoint home site to establish the SharePoint app in Teams experience.

Q: What's the difference between a SharePoint home site and the SharePoint start page?
The content on the SharePoint start page is driven and managed by Microsoft Graph. Content is personalized to the individual users' recent activity, followed sites, and content that is saved for later. The SharePoint home site is a landing experience for your entire organization. It displays

universally relevant content and directs users to other important portals like Human Resources and company directories.

Q: Can I integrate the SharePoint start page with my SharePoint home site?
Integration between the SharePoint home site and SharePoint start page isn't available at this time. However you can add a featured link to the SharePoint start page to increase SharePoint home site discovery.

Watch for updates in the Microsoft 365 public roadmap.

Resources

Planning your SharePoint hub sites

Creating and launching a healthy SharePoint portal

Apply and customize SharePoint site templates

Last updated on 09/20/2026

Change your SharePoint domain name

When you first sign up for Microsoft 365, you create an `onmicrosoft.com` domain. Even if you later add a custom domain, all your SharePoint and OneDrive URLs use the original `onmicrosoft.com` domain.

If your organization is going through a rebranding, merger, or acquisition and needs to change the domain in your SharePoint and OneDrive URLs, you can change the domain name by using PowerShell. For example, if your organization name changes from Contoso to Fabrikam, you can change your SharePoint URLs from `contoso.sharepoint.com` to `fabrikam.sharepoint.com`.

> **ⓘ Important**
>
> - When the rename operation begins, all sites in the tenant queue for individual renames to the new domain. While the renaming is happening, sites that are on the original domain are temporarily inaccessible. Once each site is renamed to the new domain, it becomes accessible again.
> - The standard version of the renaming feature is currently available to organizations that have no more than 10,000 total sites, which includes SharePoint sites, OneDrive accounts, and SharePoint Embedded containers combined.
> - Advanced Tenant Rename is available to organizations with any number of sites, provided they have SharePoint Advanced Management. See the section Advanced Tenant Rename in this article.
> - The domain name change affects only SharePoint and OneDrive URLs. It doesn't impact email addresses.
> - For information about changing a site address, like from `https://contoso.sharepoint.com/sites/sample1` to `https://contoso.sharepoint.com/sites/sample2`, see Change a site address.
> - The domain rename feature isn't available for organizations who have set up multigeo. This limitation includes tenants that were enabled during a trial or a paid offering in the past.
> - If your organization uses special clouds or government clouds (such as GCC, GCC High, DoD, and so on), or if you have a `.de` domain, you can't change your domain name.
> - When you rename your SharePoint domain, Microsoft creates a redirect at the previous address, which expires one year after the rename.

- You can only rename your SharePoint domain up to two times during the lifetime of your tenant. You can't schedule another SharePoint domain rename within 30 days after a previous rename completes.
- Changing your SharePoint domain name back to the original name after you rename it isn't supported. For example, if you change your SharePoint domain from `contoso.sharepoint.com` to `fabrikam.sharepoint.com`, changing it back to `contoso.sharepoint.com` isn't supported.
- Before starting a tenant rename, verify that no sites are blocked from being renamed. If more than 10% of sites fail to rename to the new domain, the tenant rename operation goes into a suspended state. To determine whether a tenant rename is suspended, see the section Monitor the status of the rename (in this article). If this occurs, submit a support request using Restore Tenant Rename Suspension to resume the operation.
- A redirect site is created for each site rename and each redirect takes 0.15 MB. So, an organization should readily have an amount of storage equal or greater than 0.15 MB times the number of sites on the tenant before renaming.

Limitations of changing a SharePoint domain name

Low impact

Expand table

App or feature	Limitation	Action required
Hub site menu items	Although the menu items continue to work, the process doesn't change items that contain absolute URLs.	Edit the menu items and if necessary, change the URLs to the new domain name.
Office "Recent" and "Pinned" lists	These lists update over time depending on usage.	None
Office.com	The URLs at `https://www.office.com` can take 24 hours to update.	None
OneDrive	Only the domain name portion in URLs is changed. The relative path based on the User Principal Name (UPN) isn't changed.	None
OneDrive sync app (OneDrive.exe)	Requires version 17.3.6943.0625 or later for all users.	Make sure the URLs "oneclient.sfx.ms" and "g.live.com." aren't blocked, and that all

App or feature	Limitation	Action required
		computers in your organization can reach them to apply updates.
OneDrive sync app (OneDrive.exe)	The organization name displayed in Office apps isn't changed. (For example, the app displays the old folder name C:\Users\Sophia\OneDrive – Contoso)	Users can disconnect and reconnect their account in the Office app.
OneNote	Requires a recent version of OneNote.	Make sure all users have the following versions installed: OneNote desktop app: Version 16.0.8326.2096 or later. OneNote for Windows 10: Version 16.0.8431.1006 or later. OneNote mobile app: Version 16.0.8431.1011 or later.
OneNote	While the domain name is being changed, users might receive a notebook sync error.	None
SharePoint mobile apps	Requires a recent version of the mobile app.	Make sure all users have the following versions installed: iOS: 4.20.0 or later. Android: 3.21.0 or later.
SharePoint mobile apps	While the domain name is being changed, users might receive a notebook sync error.	None
Search and Delve	The search index takes a while to reflect new URL changes.	None. As a benchmark, sites with under 100,000 documents are often updated in three days. For sites with over 100,000 documents, the updates can take a few weeks to months depending on traffic.
Search and Delve	Search results might not be complete or might return results for the original URLs until the search index is updated.	None
SharePoint content	Although content (such as text on pages) that includes the domain name continues to work, the process doesn't update it to display the new name.	Search for the old domain name and edit content to display the new domain name.

Medium impact

Expand table

App or feature	Limitation	Action required
Custom apps and Group Policy objects	Absolute URLs embedded in these apps and objects aren't changed.	Edit custom apps and Active Directory Group Policy objects that contain absolute URLs and, if necessary, change the URLs to the new domain name. Confirm with app publishers that apps don't contain absolute URLs.
Custom and non-Microsoft apps	Some apps might not process the HTTP 308 redirect correctly.	Edit custom apps and work with app publishers to ensure that they handle HTTP 308 responses correctly.
Delve	It can take 24 hours before people profiles can be viewed.	None
eDiscovery	Holds can't be removed until you update the URLs.	In the Microsoft Purview portal, change the eDiscovery hold URLs to the new domain name.
InfoPath forms	Forms that use a SharePoint connection as a data source don't work.	Reconnect these forms to SharePoint.
Loop	Existing workspaces can't be shared and new pages can't be added to them.	No action is available.
Microsoft 365 Archive	Archived OneDrive accounts and SharePoint sites are renamed to the new domain. However, archived SharePoint sites connected to Teams channels or Microsoft 365 groups aren't renamed.	Reactivate archived SharePoint sites connected to Teams channels or Microsoft 365 groups before the rename.
Microsoft Forms	Forms that have the option to upload attachments in responses don't work.	Remove the upload button and add it again in the form.
Office apps	While the domain name is being changed, users might experience an error when saving Word, Excel, and PowerPoint documents that are located in a site or OneDrive.	Attempt to save the document again and if necessary change the URL of the **Save** location.
OneDrive	The Quick access links in OneDrive and SharePoint don't work in some cases.	No action is available.
OneDrive app in Teams	Accessing the app returns a 404 error.	Until a fix is released, to resolve the error: 1. Create a 1:1 chat with another user. 2. In the message box, select **Actions and apps** > **Attach file** > **Upload from this device**. 3. Select a file you send to the other user, then select **Open**.

App or feature	Limitation	Action required
		4. Press **Enter** to send the file or select **Send**. After sending the file, navigate to the OneDrive app in Teams.
Power Automate	Request sign-off flows that use SharePoint as a connection don't work.	Remove and re-create the Request sign-off flow.
Power Automate	Any flows deployed as solutions with managed layers that use SharePoint as a connection don't work.	Remove and re-create the flows.
Power Automate	Some regular flows don't work after the rename.	As part of the rename operation, updates to Power Automate are attempted but a small subset might fail due to service issues. For any flows identified that don't work, manually update the URL.
Power BI	Power BI reports using SharePoint connections as a data source don't work.	Before changing your domain name, download the Power BI reports that are using SharePoint connections as a data source as a `.pbix` file. After you change the domain name, edit the connections in the Power BI Desktop app and republish the report. Power BI reports that aren't created or maintained in the Power BI Desktop app need to be recreated.
Project Online	Workflows that are in flight don't complete and are orphaned. New workflow instances can't be initiated. Association to previous workflow instances isn't available and are orphaned.	Before changing your domain name, make sure all in flight workflows are completed. After you change the domain name, republish the workflows. You can then reset them to in flight in Project Web App by going to **PWA Settings** > **Change or Restart Workflows**.
Project Online	URLs embedded in workflows aren't changed. For example, if a workflow contains the embedded URL `contoso.sharepoint.com`, it isn't changed. This might impact the functionality of the workflow.	Workflows that contain URLs referring to the original domain name might need to be updated to the new name.
Project Online	References to PWA sites in Project Online at `https://project.microsoft.com` don't work.	In Project Online at `https://project.microsoft.com`, change the URL of the PWA sites under **Settings** > **My PWA Site**.

App or feature	Limitation	Action required
Project Online	Custom Excel Reports that use Microsoft Project Data connections as a data source don't work.	These reports need to be reconnected.
Project Pro	The app doesn't work until you update the URL of the PWA site.	Before changing your domain name, make sure that all projects that are checked out in Project Pro are checked in. After you change the domain name, change the URL of the PWA site under **File** > **Info** > **Manage Accounts**.
SharePoint 2013 workflows	Workflows that are in flight don't complete and are orphaned. New 2013 Workflow instances can't be initiated. Association to previous workflow instances isn't available and these workflows are orphaned.	Before changing your domain name, make sure all in-flight workflows are completed. After you change the domain name, republish the workflows.
SharePoint 2013 workflows	URLs embedded in workflows aren't changed. For example, if a workflow contains the embedded URL `contoso.sharepoint.com`, it isn't changed. This configuration might impact the functionality of the workflow.	Workflows that contain URLs referring to the original domain name might need to be updated to the new name.
SharePoint add-ins	Add-ins might not function as expected.	The add-ins might need to be republished. Review the App configuration settings in Microsoft Entra ID for the add-in and update any URLs to the new domain name. For SPFx applications, in Microsoft Entra ID update the Authentication URLs to the new domain for the SharePoint Online Client Extensibility Web Application Principal.
SharePoint hub sites	Sites registered as hub sites don't work.	Unregister and register the affected sites as hub sites in the SharePoint admin center after the rename.
SharePoint web parts	Some web parts might not function as expected.	The web parts might rely on direct URL references. Update the web parts with the new URLs.
Site customizations and embedded code	Absolute URLs embedded in SharePoint customizations aren't updated.	Edit customizations that contain absolute URLs and if necessary, change the URLs to the new domain name.

App or feature	Limitation	Action required
Teams on the web and Teams desktop app	The first time someone tries to access the **Files** tab for a team or private channel, they receive an error. The tab works for all users afterwards.	None
Teams on the web and Teams desktop app	It can take 72 hours for meeting notes to work (for both current and previous meetings).	None
Teams on the web and Teams desktop app	On the **Files** tab, any folders added by using **Add cloud storage** (which point to another SharePoint site) don't work.	Remove and re-add the folders.
Teams on the web and Teams desktop app	Document libraries and SharePoint Lists added as tabs don't work.	Remove and re-add the tabs.
Teams on the web and Teams desktop app	Embedded images in Wikis aren't displayed.	Edit the `Wiki.mht` file located in the SharePoint Site Teams Wiki Data library and if necessary, change the URLs of the embedded images to the new domain name.
Teams on the web and Teams desktop app	Personal Wikis don't work.	In a one-on-one or group chat, attach and send a file to the chat.
Non-Microsoft apps including backup solutions	Absolute URLs embedded in non-Microsoft apps (including backup solutions) aren't changed.	Confirm with app publishers (including backup solutions) that they support tenant renames.
Isolated web parts and full page apps	Isolated components aren't updated and stop working.	Solutions that contain isolated components need to be republished in the tenant app catalog. The solution starts working again after republishing.

High impact

Expand table

App or feature	Limitation	Action required
Alternate URLs	If your tenant still has alternate URLs configured, you can't change your domain name.	Remove alternate URLs before you can schedule a rename. Contact Microsoft for support getting them removed.

App or feature	Limitation	Action required
Business Productivity Online Suite (BPOS) sites	If your tenant still has Microsoft Business Productivity Online Suite (BPOS) sites remaining in it, you can't change your domain name.	Remove BPOS sites and its configuration before scheduling tenant renaming. Submit a support request by selecting Rename a SharePoint Tenant with BPOS sites.
Deleted sites	You can't restore any sites that you deleted after the change.	Before changing your domain name, review the Deleted sites page in the SharePoint admin center and restore any sites that you want to keep.
Historical German cloud (.de) tenants	If your tenant was originally in the German cloud with a .de domain, you can't change your domain name. This limitation applies even if your tenant was later migrated to the regular cloud but still retains the .de domain.	No action available.
Locked sites and OneDrive accounts	Locked OneDrive and SharePoint sites (the LockState is NoAccess) are renamed to the new domain. However, locked SharePoint sites connected to Teams channels or Microsoft 365 groups aren't renamed.	Before changing your domain name, review any sites connected to Teams channels or Microsoft 365 groups that are locked to determine if the lock should be removed. Lock and unlock sites
Multi-Geo configurations	You can't change your SharePoint domain name if your organization is currently set up for Microsoft 365 Multi-Geo or was previously set up for it.	No action available.
Point-in-time restoration	You can't restore a site to a previous time before the domain name change.	No action available.
Root site replacement	You can't replace your root site (using either the SharePoint admin center or the PowerShell cmdlet Invoke-SPOSiteSwap) between the time you schedule your domain name change and when it completes.	Replace your root site before you schedule the domain name change or after it completes.
SharePoint public sites	If your tenant contains old SharePoint public sites, you can't change your SharePoint domain name.	Remove public sites on the tenant before scheduling tenant renaming. Submit a support request by selecting Rename a SharePoint Tenant with Public site.
Special and government	If your organization uses special clouds or government clouds (GCC, GCC High, DoD, and so	No action available.

App or feature	Limitation	Action required
clouds	on), you can't change your domain name.	
Vanity domain configurations	If your SharePoint domain is, for example, `teams.contoso.com` (versus `contoso.sharepoint.com`), you can't change your domain name.	No action available.
Licenses	Purchase or update to licensing doesn't take effect during Rename	Wait until Rename completes
Admin Roles	Creating or updating Admin Roles doesn't take effect during Rename	Wait until Rename completes
Storage	Purchase or update to Storage doesn't take effect during Rename	Wait until Rename completes

What is Advanced Tenant Rename?

If you want to rename an organization with more than 10,000 total sites or want greater control over the rename operation, you must use Advanced Tenant Rename. It supports changing the SharePoint domain on tenants with any number of sites and has the ability for admins to prioritize up to 4,000 sites in their organization for early execution within the overall rename. This priority execution allows select business-critical or high-visibility sites to complete first and reduces any risk or concerns with its impact on daily operations.

Advanced Tenant Rename is a part of SharePoint Advanced Management.

What are the prerequisites?

Advanced Tenant Rename currently supports tenants that meet the following conditions:

- Meet Prerequisites for SharePoint Advanced Management.
- Your organization doesn't have Microsoft 365 Multi Geo enabled.
- Your organization doesn't use government clouds, including GCC, GCC High, and DoD.
- Your organization doesn't use vanity domains (from an earlier MTE offering).

How do I prioritize sites when renaming domain?

By using Advanced Tenant Rename, you can prioritize up to 4,000 sites for early execution. This list can include both OneDrive and SharePoint sites, but it excludes root sites (for example, `contoso.sharepoint.com`, `contoso-admin.sharepoint.com`, `contoso-my.sharepoint.com`).

The prioritized sites are processed first among all the sites in your organization. This priority gives them the opportunity to complete their renames sooner. Plan your tenant rename to start at the beginning of a low-impact period (such as weekends or holidays) and prioritize those sites that you believe are important to have accessible at the start of the next business day.

To manage prioritization, use the following PowerShell cmdlets.

- Set-SPOTenantRenameSitePrioritization – Prioritize the specified site for early execution.
- Remove-SPOTenantRenameSitePrioritization – Remove prioritization for the specified site.
- Get-SPOTenantRenameSitePrioritization – View the current list of prioritized sites.

Use the PowerShell cmdlets for prioritization after you schedule the tenant rename. You can make changes to the list of prioritized sites up to two hours before the scheduled start time of the rename. Once the rename starts, the system doesn't accept further changes.

Step 1: How do I add the new domain name?

1. Check the availability of the new domain you want. For example, if you want your SharePoint and OneDrive URLs to begin with `fabrikam.sharepoint.com`, enter `https://fabrikam.sharepoint.com` in a browser. If you get a message that the address couldn't be found (404), it's probably available. If you get a sign-in screen or a message that your username couldn't be found in the fabrikam.sharepoint.com directory, the domain is taken and you need to try a different one. If another customer already registered the domain, Microsoft can't provide any information or contact the customer.

   -or-

   If you own the domain for another subscription, you need to delete that tenant in Microsoft Entra ID. Deleting a tenant typically takes three days to complete and to make the domain available.

   > ⚠ **Warning**
   >
   > Don't use the domain to test this procedure in a test environment first. If you do, you won't be able to use the domain for your production environment.

2. Add your new .onmicrosoft.com domain using the Domains page in the Microsoft 365 admin center.

- Don't use the **Add domain** option directly present in the Domains page, since that option doesn't create a `.onmicrosoft.com` domain. Use the steps in the specified link to correctly create one.
- Don't make this domain your fallback domain.

3. Go back to the Domains page and check that the newly added `.onmicrosoft.com` domain appears in a **Healthy** state.

Step 2: Use Microsoft PowerShell to rename your domain

> ⚠ **Warning**
>
> - When the change of the SharePoint domain starts, sites that remain on the original domain are temporarily inaccessible. As each site gets renamed to the new domain, it becomes accessible again.
> - Changing your SharePoint domain name might take several hours to days depending on the number of sites and OneDrive users that you have. Make this change during a period of low usage, such as a weekend, and tell users to avoid accessing SharePoint and OneDrive content during the change. In addition, any actions that create new OneDrive libraries and sites, such as creating a new team or private channel in Microsoft Teams, are temporarily blocked during the rename.
> - Don't plan any UPN changes or renames while the change of your SharePoint domain name is in progress. Wait until after the domain name change is complete.

1. **REQUIRED** - Download the latest SharePoint Online Management Shell. If you installed a previous version of the SharePoint Online Management Shell, go to **Add or remove programs** and uninstall SharePoint Online Management Shell. Review the System Requirements and Install Instructions. The app isn't supported on Mac.

2. Connect to SharePoint as at least a SharePoint Administrator in Microsoft 365. To learn how, see Getting started with SharePoint Online Management Shell.

   Run this command:

   PowerShell

   ```
   Connect-SPOService -Url "https://contoso-admin.sharepoint.com"
   ```

3. Run the following command to specify the new domain name:

```
PowerShell
Start-SPOTenantRename -DomainName <DomainName> -ScheduledDateTime <YYYY-MM-DDTHH:MM:SS> [-WhatIf] [-Confirm]
```

Where "DomainName" is the part before "sharepoint.com" or "onmicrosoft.com" and "ScheduledDateTime" is at least 24 hours in the future, but not more than 30 days. The time you enter is based on the current date and time of the computer you're using.

Here's an example:

```
PowerShell
Start-SPOTenantRename -DomainName "fabrikam" -ScheduledDateTime "2021-12-31T10:25:00"
```

If that PowerShell command isn't found or returns nothing, make sure you installed the latest SharePoint Online Management Shell. Before installing the latest version, you might need to uninstall all previous versions by running the following command:

```
PowerShell
Uninstall-Module Microsoft.Online.SharePoint.PowerShell -Force -AllVersions
```

For more information, see Start-SPOTenantRename.

To cancel a rename before it starts, you can run the following command:

```
PowerShell
Stop-SPOTenantRename
```

For more information, see Stop-SPOTenantRename.

Step 3: Prioritize sites (premium)

If you purchase SharePoint Advanced Management licenses for all users when you schedule your rename, the process automatically considers Advanced Tenant Rename and gives you the ability to prioritize sites.

Use the `Set-SPOTenantRenameSitePrioritization` cmdlet to prioritize individual sites. For example, to prioritize a site named *projectx*, run the following command:

PowerShell

```
Set-SPOTenantRenameSitePrioritization -SiteUrl
https://contoso.sharepoint.com/sites/projectx
```

If you already identified the list of sites you want prioritized and want to perform the Set operation in bulk, put the list in a CSV file and then use PowerShell to import it and iteratively execute the cmdlets. The file should have a single column with the title `SiteUrl`, and every subsequent row should be the full URL of the desired site.

Here's an example:

PowerShell

```
Import-Csv <Path> | ForEach-Object {Set-SPOTenantRenameSitePrioritization -SiteUrl
$_.SiteUrl}
```

If you attempt this operation with a file that has all 4,000 sites in it, the complete execution of this cmdlet can take approximately 4-6 hours. If you want shorter waiting times, split your list of sites and run the command in batches.

To view the list of sites currently prioritized, run the following command:

PowerShell

```
Get-SPOTenantRenameSitePrioritization
```

To remove prioritization for a site, run the following command:

PowerShell

```
Remove-SPOTenantRenameSitePrioritization
```

For example, to remove prioritization for the `projectx` site, run the following command:

PowerShell

```
Remove-SPOTenantRenameSitePrioritization -SiteUrl
https://contoso.sharepoint.com/sites/projectx
```

Prioritizing a site isn't a guarantee that the site rename finishes first. Several factors can affect processing times, and the system processes multiple site renames in parallel. Prioritized sites have a higher chance of completing first.

Step 4: Monitor the status of the rename

To check the status of the rename operation, run the following command:

PowerShell

```
Get-SPOTenantRenameStatus
```

Make sure you open a new PowerShell window to sign in again. The date and time shown with this command is in UTC time but follows the local format of the system where the cmdlet is run.

For more information, see Get-SPOTenantRenameStatus.

During and after the rename, you can get the state of a site by running the following command:

PowerShell

```
Get-SPOSiteRenameState
```

For more information about this cmdlet, see Get-SPOSiteRenameState.

To verify success of the rename operation, review the status of the rename operation, and the count of renamed sites in comparison to total sites. The count of sites that can't be renamed to the new domain is shown in the **Attention Required** field.

To get more information on these sites, run the following command:

PowerShell

```
Get-SPOSiteRenameState
``

Pass the `RenameJobID` listed in the tenant rename status as the `ParentOperationID`,
and the status (such as Success, Failed, or Suspended). If you want to export these
results to a CSV file, you can use the follownig cmdlet:

```powershell
Export-Csv
```
```

Here's an example:

PowerShell

```
Get-SPOSiteRenameState -ParentOperationID <RenameJobID> -State Failed | Export-Csv -
Path <Path>
```

Step 5: Review features and settings after the rename

1. Review any firewall rules that might block access to the new domain.
2. Review organization browser settings to make sure the new domain is a trusted location. This action includes reviewing any Group Policy settings that might control browser settings.
3. Review any non-Microsoft apps, custom apps, and scripts that access SharePoint. They might need to be modified to use the new domain.
4. If you have custom SharePoint Framework solutions that require access to an API, check the API access page in the SharePoint admin center to ensure that SharePoint Framework components can use the new domain name.

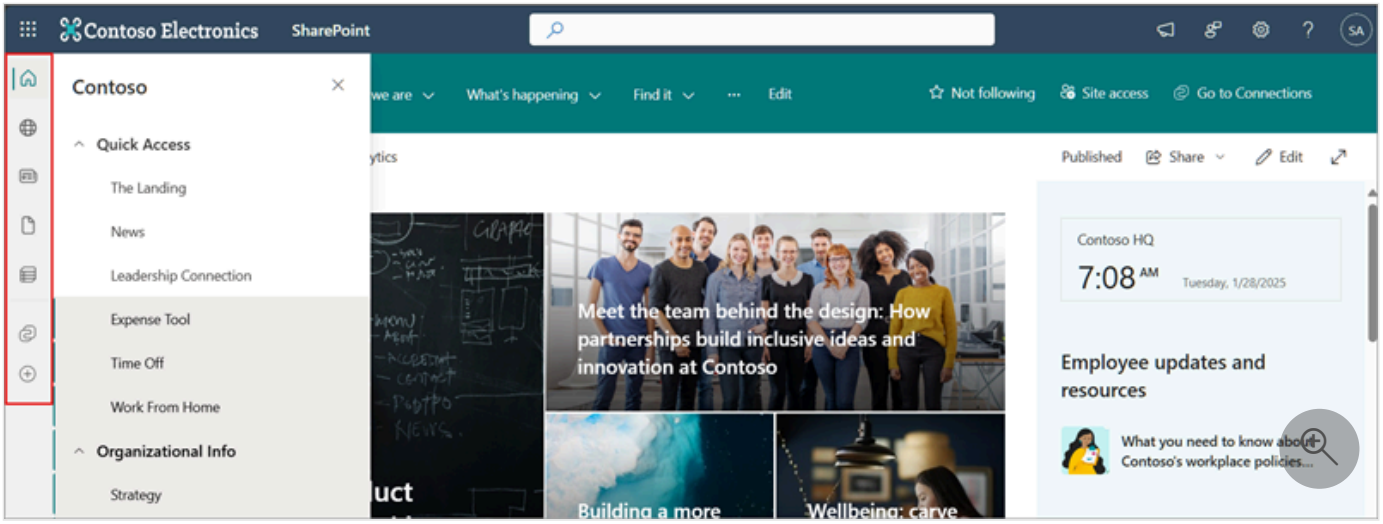
Troubleshooting

- Frequently asked questions
- Errors and how to fix them

Last updated on 07/29/2026

Introduction to the SharePoint app bar

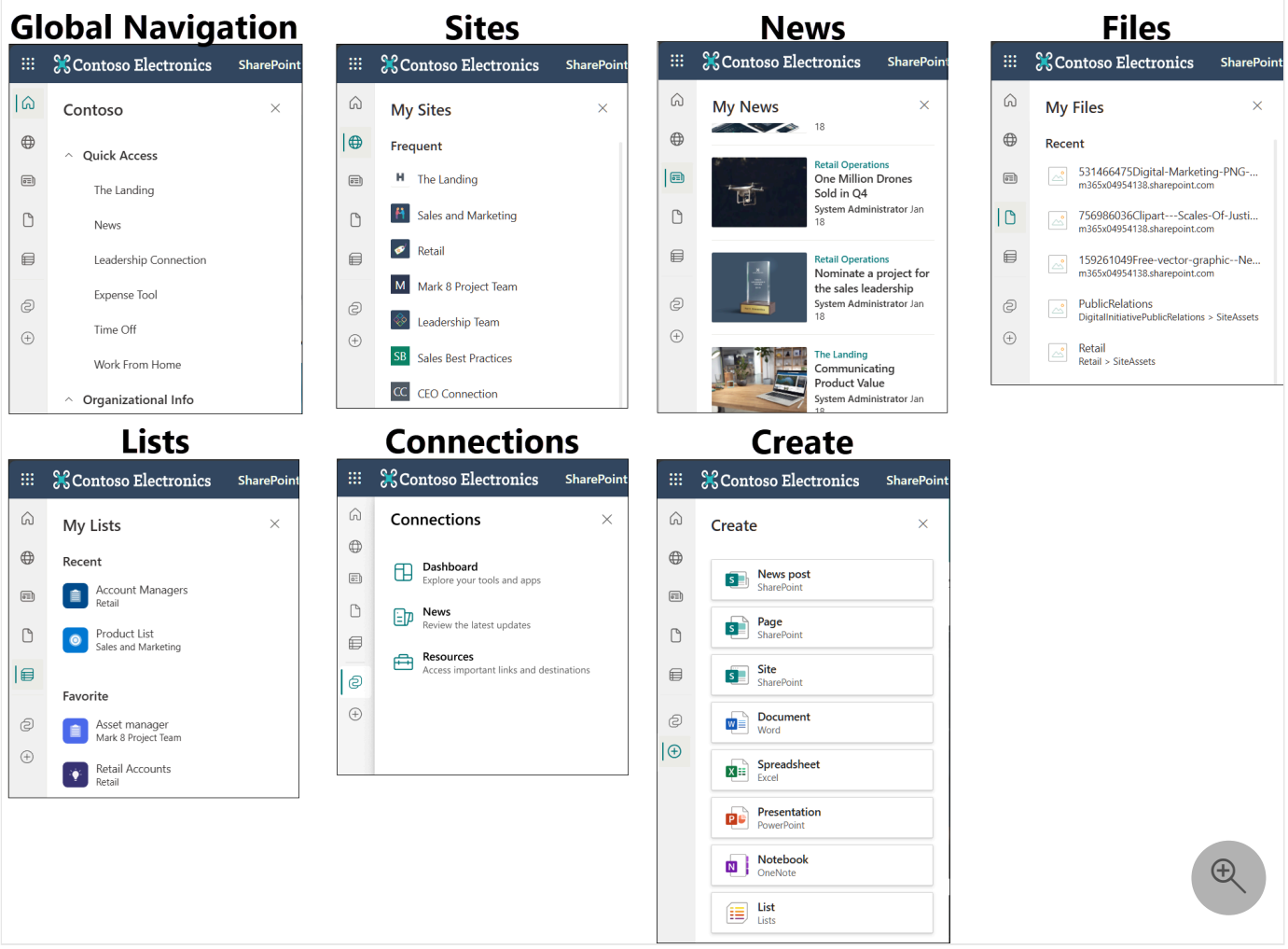
Help users find important content and resources no matter where they are in SharePoint. The SharePoint app bar improves the global way-finding and creation experiences while dynamically displaying personalized sites, news, files, and lists. The app bar is on the left-hand side anywhere in modern SharePoint sites.



The SharePoint app bar experience

The SharePoint app bar brings together intranet resources and personalized content like sites, news, files, and lists. Enable global navigation to allow users to easily navigate to important intranet resources anywhere in SharePoint. Customize global navigation details and the rest of the content will dynamically display and update personalized content for sites, news, and files. Access your SharePoint app in Teams. Create sites, files, and lists easily from anywhere in SharePoint.

> **Note**
>
> - The SharePoint icon will only show to customers who have enabled the SharePoint app in Teams experience with a configured and published dashboard.



Note

- Global navigation is the only app bar tab that can be customized.
- If global navigation is disabled or not configured, the home icon links to the SharePoint start page.
- Specific SharePoint app bar tabs can't be disabled.
- The SharePoint app bar can't be disabled on specific sites.
- The SharePoint app bar isn't available on classic SharePoint sites.
- The SharePoint app bar might affect current page customizations, specifically customizations that appear on the left side.
- The SharePoint app bar won't display in SharePoint for guests outside of your organization.
- In GCC High and DoD environments users might experience a degraded experience for the My sites panel in the app bar.
- Extra restrictions might apply to tenants within the GCC High and DoD environments when using My News in the SharePoint app bar.

- Global navigation in the SharePoint app bar must be enabled for SharePoint resources to display in the Microsoft Teams app bar for the SharePoint app in Teams.

The SharePoint app bar is a significant change to the user experience and your organization's intranet information architecture. To ensure a seamless experience, Microsoft created specific guidance on how to design current navigation to compliment the global navigation feature. There's also end-user guidance to help onboard the rest of your organization.

Customize global navigation in the app bar

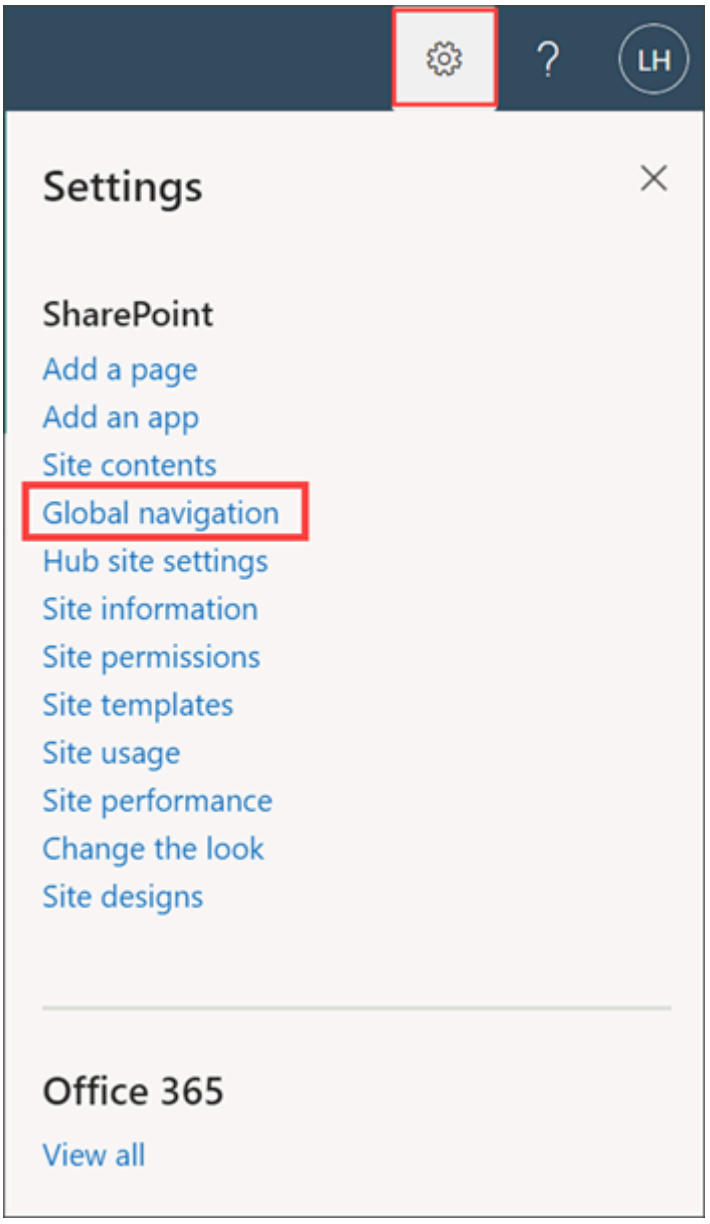
Global navigation can be enabled and customized in the SharePoint app bar. Customize the global navigation logo, title, and source depending on your users' and organization's needs.

If you choose to keep global navigation disabled, the home icon links to the SharePoint start page.

> **Note**
>
> - Site owner permissions (or higher) to the SharePoint home site are required to enable global navigation.
> - Users need read access (or higher) to the SharePoint home site to view the global navigation links.
> - Audience targeting can be applied to menu links in global navigation.
> - If you get an error after editing links to sites, try deleting the link and adding it again.
> - Implementing global navigation might take up to 24 hours for the changes to take effect for users.

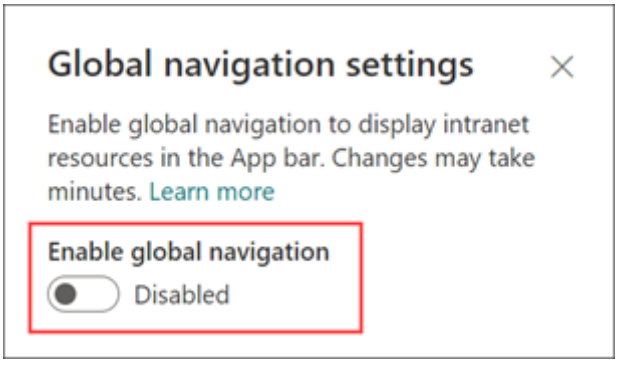
Get started customizing the global navigation tab

1. Set up a SharePoint home site if your organization doesn't already have one.
2. Share the SharePoint home site with everyone in your organization to ensure all users can access the global navigation links.
3. Navigate to your organization's SharePoint home site.
4. Select **Settings** and then select **Global navigation** settings.



> **Note**
>
> If you don't see **Global navigation** in the **Settings** pane on the SharePoint home site, you might not have site owner permissions (or higher) to the SharePoint home site.

5. Switch the **Enable global navigation** toggle to **On**.



6. Next, add the **Logo** to represent global navigation for your organization (organization or custom logo). No action is needed if you choose to keep the default home icon.

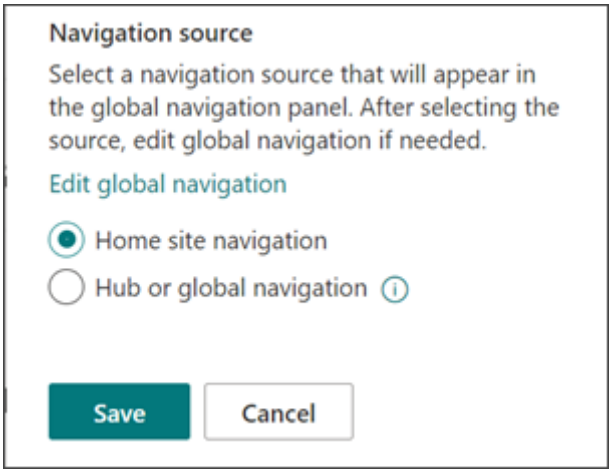
   Global navigation logo specifications:

   - The logo size should be 20x20 pixels
   - PNG file type
   - Transparent background recommended

7. Then, enter a **Title** that's to be displayed at the top of the global navigation pane.

8. Under **Navigation source** make edits to the selected global navigation source if needed by selecting **Edit global navigation**.

9. Select **Save** when you're done. Updates to global navigation might take several minutes before they appear.

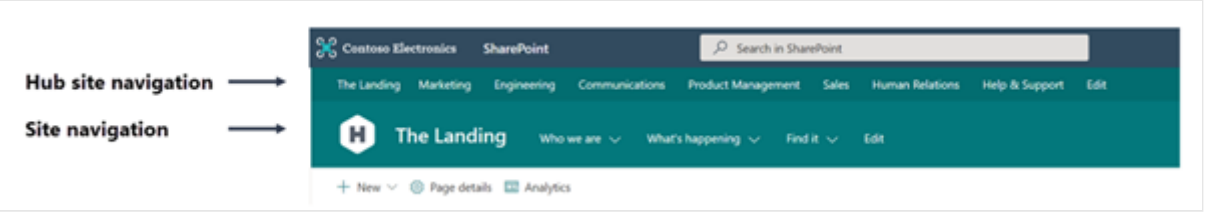


> **Note**
>
> - The global navigation source can be edited at any time by site owners or admins of the SharePoint home site.
> - The site and global navigation links and labels can be edited at any time by editors of the SharePoint home site.
> - Implementing global navigation might take up to 24 hours for the changes to take effect.
> - If you get an error after editing links to sites, try deleting the link and adding it again.

Determine the global navigation source depending on your SharePoint home site's configuration

If you haven't set up your SharePoint home site, do that first and if you're setting up a SharePoint home site specifically to implement global navigation, review this guidance.

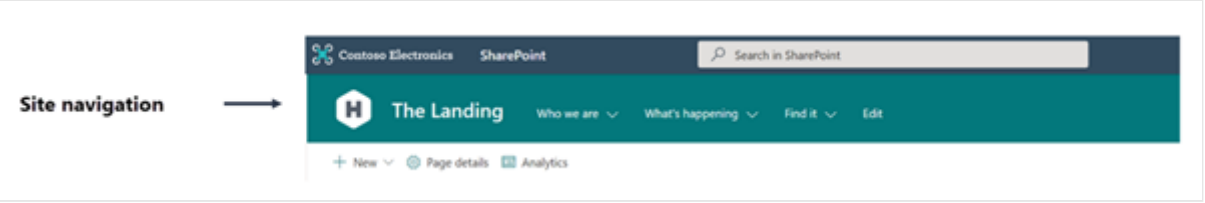
For SharePoint home sites that are a hub, you have two source options



- Select the site navigation source to display the SharePoint home site's navigation.
- Select the Hub or global navigation source to display the SharePoint home site's hub navigation.

> ⓘ **Note**
>
> When you apply the extended header layout to the site, you'll no longer see the site navigation.

For SharePoint home sites that aren't a hub, you have two source options



- Select the site navigation source to display the SharePoint home site navigation.
- Create a secondary set of navigation nodes specifically for the global navigation panel by selecting **Hub or global navigation**. Then, select **Edit global navigation** to create the new global navigation menu. Select **Save** when you're done.

> ⓘ **Note**
>
> For SharePoint home sites that aren't a hub site and choose to create a secondary set of navigational nodes for the global navigation pane - if you decide to make your SharePoint home site a hub in the future, the new hub site navigation inherits the current navigational nodes for global navigation and can be edited at any time.

See all the different ways you can set up global navigation

Depending on the content you want to make available in the global navigation, you can configure your SharePoint home site navigation and global navigation in three different ways.

Display the SharePoint home site's navigation in global navigation

Display hub and site navigation on the SharePoint home page, and the home site navigation in the global navigation panel.

1. Navigate to the SharePoint home site's **Settings** and then **Global navigation**.
2. **Enable** global navigation, enter a **Title**, and then select **Home site navigation** as the source.
3. Select **Save**. Changes might take a few minutes to reflect.

Display the SharePoint home site's hub navigation in global navigation

Display hub and site navigation on the SharePoint home page, and the hub navigation in the global navigation panel.

1. Navigate to the SharePoint home site's **Settings** and then **Global navigation**.
2. **Enable** global navigation, enter a **Title**, and then select **Hub or global navigation** as the source.
3. Select **Save**. Changes might take a few minutes to reflect.

Hide the site navigation and display it in the global navigation

Display just the hub navigation on the SharePoint home page, and the site navigation in the global navigation panel.

1. Start by hiding the site navigation by going to **Settings**, then **Change the look**, then **Navigation** and toggle the **Site navigation visibility** to **Off**.
2. Then, navigate to the SharePoint home site's **Settings** and then **Global navigation**.
3. **Enable** global navigation, enter a **Title**, and then select **Home site navigation** as the source.

4. Select **Save**. Changes might take a few minutes to reflect.

Set up a SharePoint home site for the first time

A SharePoint home site is a SharePoint communication site that you create and set as the top landing page for all users in your intranet. The home site brings together news, events, conversations, and other resources to deliver an engaging experience that reflects your organization's voice, priorities, and brand.

It's recommended that you set up a SharePoint home site for your organization to take full advantage of SharePoint's communication and collaboration features and is required to enable and customize global navigation in the SharePoint app bar.

Set up a SharePoint home site just for global navigation

If you're creating a SharePoint home site for the main purpose of setting up global navigation, you can simplify the steps recommended to plan and launch a SharePoint home site.

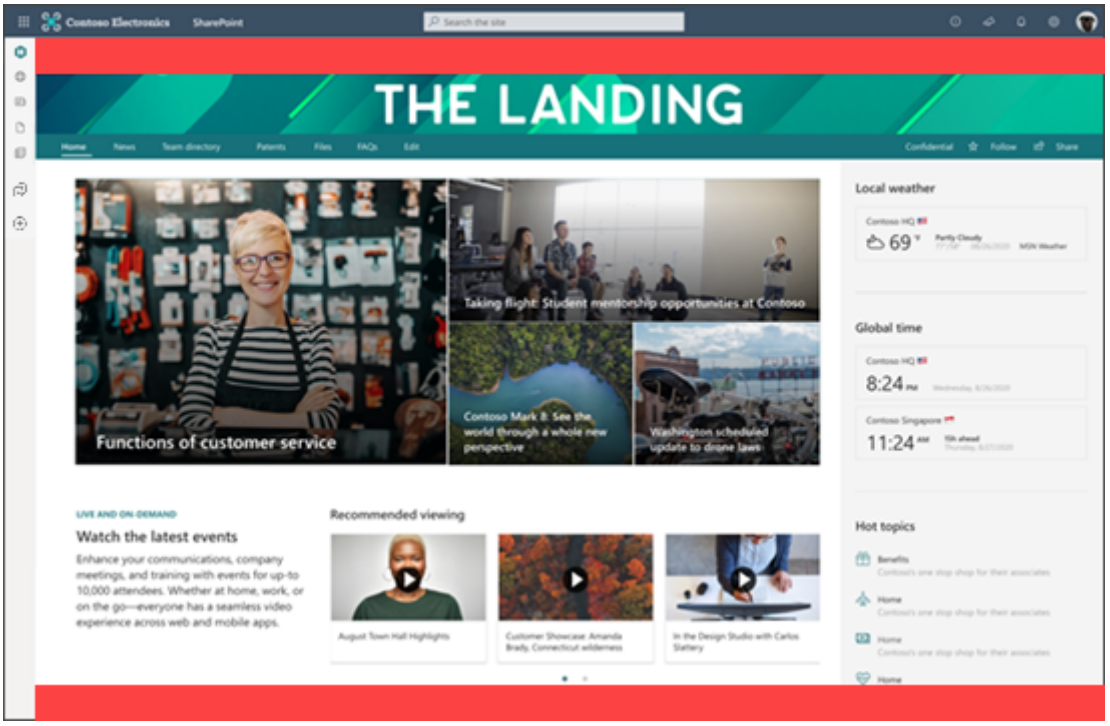
Learn more about planning navigation in SharePoint and apply information architecture principles to your new SharePoint home site's navigational design.

> **Note**
>
> - Only one communication site can be set as the SharePoint home site.
> - The first time you set up a SharePoint home site, it might take up to several minutes for the changes to take effect.
> - SharePoint admin credentials are required to transform a communication site into a SharePoint home site.

1. Start by creating a SharePoint communication site.
2. Customize the communication site navigation to reflect the view you'd like to see in the global navigation pane. You can make edits to the navigation source and individual labels and links at any time.
3. Set this communication site as a SharePoint home site within the SharePoint admin center.
4. Share the SharePoint home site with users so they can access the global navigation links.
5. On the SharePoint home site, select **Settings** and then **Global navigation** to **enable** and customize.
6. For the global navigation source, select **Home site navigation** to display the SharePoint home site navigation that you created in the global navigation panel, then select **Save**.

Understand how the app bar might affect page customizations

The SharePoint app bar might affect current page customizations, specifically customizations positioned to the left of your page. For organizations using page placeholders, the SharePoint app bar will cover parts of both the header and footer page placeholder. In the following image, the placeholder footprint is in red:



Modernize classic SharePoint sites to display the SharePoint app bar

The SharePoint app bar only appears in modern SharePoint sites and pages.

We highly recommend modernizing classic sites not only to display the SharePoint app bar but for a more consistent user experience. Learn more about how to modernize classic SharePoint sites and pages using the open-source SharePoint PnP Page Transformation solution.

Teach end users about this feature

Help end users understand how the new SharePoint app bar works.

Resources

- Learn more about SharePoint home sites

- Learn more about planning and creating hub sites
- Learn more about navigation and information architecture in SharePoint
- Learn more about sharing and permissions in SharePoint

Last updated on 10/06/2026

Create guidelines for site usage

Using the following steps as a template, create your own custom guidance for SharePoint site owners on how sites are set up and managed in your organization. Each section provides guidance about what to include, sample text to help you get started, and links to resources to learn more about each area.

Download the PDF

Introduction

Guidance:

- Provide a short introduction to frame your guidelines. If you have broader business or digital resource use policy, link to it if it applies to SharePoint sites as well.

Sample text:
A SharePoint site is designed to be a powerful tool for team collaboration and communication. [Enter your IT/productivity service org] administers the Microsoft 365 service your site is built on. The goal is to make it easy to accomplish your business goals.

General guidelines

Guidance:

- Provide general policy statements that you want your users to follow. These may include key business uses you have defined for sites, internal communication policies, or security and privacy guidelines.

Resources:

- Plan your SharePoint site
- Guide to the modern experience in SharePoint

Sample text:
*Here are some things to keep in mind as you work with your SharePoint sites. Refer to [**insert your organization's name**] business resource use policy. These policies apply to all SharePoint site usage.*

Guidelines for creating your site

Guidance:

- Provide basic procedural guidance. How does someone get a SharePoint site? It may be via the "Create site" link on the SharePoint start page or you may have a unique provisioning process for your organization.
- If you have specific site templates that you want your site owners to select when they create their own sites, include that info in this section.
- Include information on custom provisioning solutions.
- Are there any ownership or site classification requirements your organization implements?
- When you set up your site, it's important to select the appropriate site classification level. Include references or links to your organization's data classification guidelines.

Resources:

- Manage site creation in SharePoint
- Policy recommendations for securing SharePoint sites and files
- Branding and site provisioning solutions for SharePoint

Sample text:
*Sites can be created via the "Create site" link at [**insert your SharePoint link**].*

You should have two site owners who are both full time employees at your org.

*When you set up your site, it's important to select the appropriate site classification level. [**Insert link to your organization's data classification guidelines**].*

Your site designs and customizations

Guidance:

- Provide information on design guidelines. Does your organization have or allow custom themes? Or do you stick with out-of-the-box options?
- Do you have specific templates or web parts you want site owners to use? Explain those so they understand why and how.
- Does your organization allow custom scripts and add-ins?
- We recommend creating a way for site owners to engage with your team when they want to customize a site. Set up a service ticket category or form to make it easy to contact you.

Resources:

- Manage site creation
- SharePoint site theming overview
- Plan customizations, solutions, and apps for SharePoint

Sample text:
*It's important that your site meets your business needs. If you need to create a custom add-in or deploy a resource-intensive app, work with our internal team. For more information, contact [**insert information on how to contact your IT team**].*

Sharing guidelines

Guidance:

- Provide information on the way your organization has set up sharing. If you have modified the settings from the defaults, you can tell your site owners what the sharing settings are for your organization, including for external sharing.

Resources:

- Plan your permissions strategy

Sample text:
Your site and its contents can be shared internally within our organization or externally with your customers or partners.

As site owner, you receive access requests when someone shares your site. You can approve or decline any requests sent to you.

Capacity guidelines

Guidance:

- Provide information on the site storage guidelines or limits (if you manage them manually). Tell site owners if you have a process and policy for requesting more.

Resources:

- Manage site storage limits

Sample text:

Your site allows for ____ MB/GB of storage. You're encouraged to remove files and content you don't need anymore.

Managing access

Guidance:

- Provide detailed information on site access. What are your processes and policies for managing site access? What level of control do your site owners have? If you manage access on behalf of your site owners, let them know that you're reviewing site permissions regularly to keep them in line with your organization's policies. Explain how you communicate changes to permissions to them.

Resources:

- Secure SharePoint Sites and Files

Sample text:

Plan to review your site's permissions regularly and set the level of access appropriately.

Site lifecycle policy

Guidance:

- Provide your organization's lifecycle policy for sites. Does your organization set site expirations automatically or with a managed process? Do you set Microsoft 365 Group expiration policies that impact SharePoint team sites? Let your site owners know when their site will expire, how they are notified, what will happen and what they need to do to extend their site.
- Setting this policy requires Microsoft 365 Global Administrator permissions.
- Does your organization take extra measures related to site backup and restore? Let your site owners know how long the backup is available and if needed, how to get a site restored.

> **Important**

Microsoft recommends that you use roles with the fewest permissions. Using lower permissioned accounts helps improve security for your organization. Global Administrator is a highly privileged role that should be limited to emergency scenarios.

Resources:

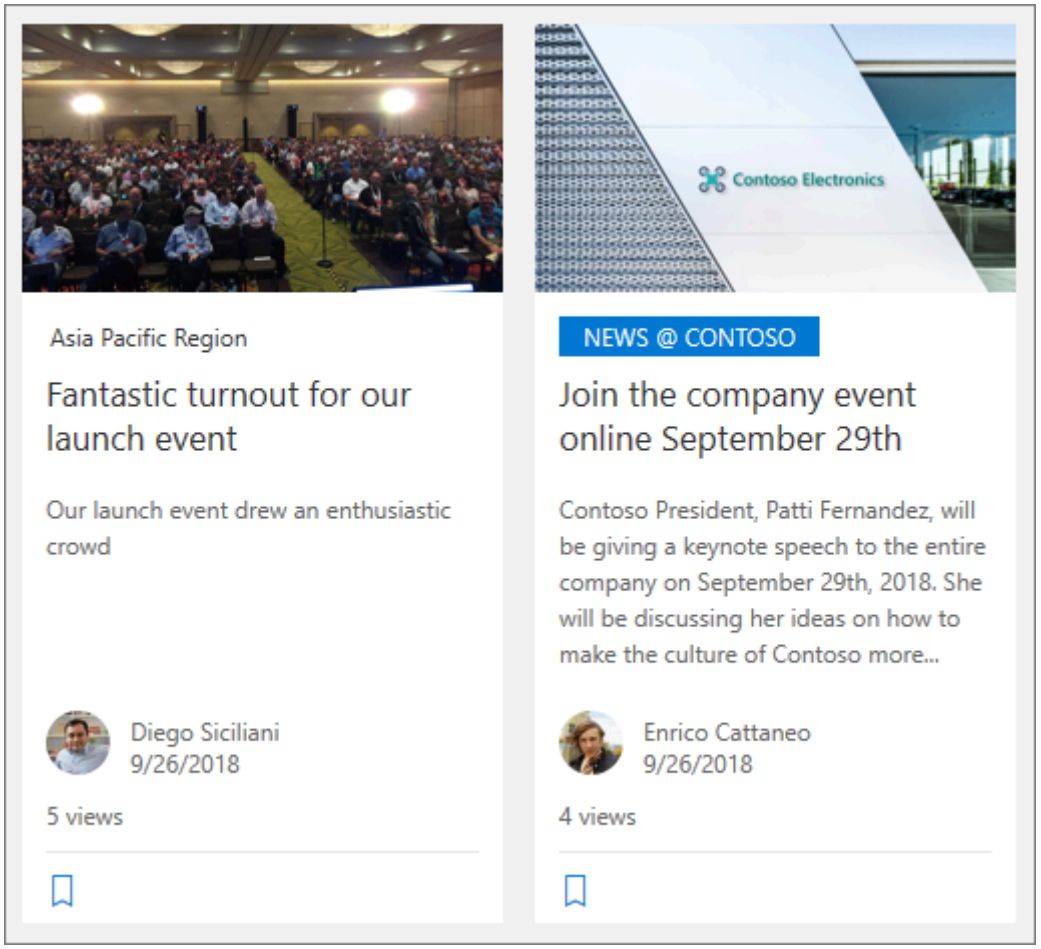
- Microsoft 365 Group Expiration Policy

Last updated on 06/25/2026

Create an organization news site

Article • 02/21/2023

To specify SharePoint sites as "official" or "authoritative" for news in your organization, mark them as organization news sites. These posts get special visual treatment (see the "NEWS @ CONTOSO" color block below), and appear on the SharePoint start page.



SharePoint Administrators can create and specify up to 100 organization news sites. For multi-geo tenants, organization news sites would have to be set up for each geo location. Each geo location could use the same central organization news site, and/or have its own unique site that shows organization news specific to that region.

> **Note**
>
> If you set a communication site as the home site for your organization, it's automatically configured as an organization news site.

For more info about working with news, see Use the News web part on a SharePoint page and Add news posts.

Use Microsoft PowerShell to specify a site as an organization news site

1. Download the latest SharePoint Online Management Shell.

   > **Note**
   >
   > If you installed a previous version of the SharePoint Online Management Shell, go to Add or remove programs and uninstall "SharePoint Online Management Shell."

2. Connect to SharePoint as a Global Administrator or SharePoint Administrator in Microsoft 365. To learn how, see Getting started with SharePoint Online Management Shell.

3. Run the following command to designate the site as an organization news site:

   ```
   PowerShell
   Set-SPOOrgNewsSite -OrgNewsSiteUrl <site URL>
   ```

   Example: `Set-SPOOrgNewsSite -OrgNewsSiteUrl https://contoso.sharepoint.com/sites/Marketing`

Related commands

- View a list of all your organization news sites: Get-SPOOrgNewsSite
- Remove a site from the list of organization news sites: Remove-SPOOrgNewsSite

---

Feedback

Was this page helpful? Yes No

Provide product feedback

Pre-provision OneDrive for users in your organization

Article • 04/10/2025

By default, the first time that a user browses to their OneDrive it's automatically created (provisioned) for them. In some cases, such as the following, you might want your users' OneDrive locations to be ready beforehand, or pre-provisioned:

- Your organization has a custom process for adding new employees, and you want to create a OneDrive when you add a new employee.
- Your organization plans to migrate from SharePoint Server on-premises to Microsoft 365.
- Your organization plans to migrate from another online storage service.

This article describes how to pre-provision OneDrive for your users by using PowerShell.

- For info about setting the default storage size, see Set the default storage space for OneDrive users.
- For info about the storage you get with each plan, see OneDrive Service Description.

> **Important**
>
> The user accounts that you're pre-provisioning must be allowed to sign in and must also have a SharePoint license assigned. To provision OneDrive by using this cmdlet, you must be a SharePoint Administrator and must be assigned a SharePoint license.

> **Note**
>
> If you're pre-provisioning OneDrive for a large number of users, it might take multiple days for the OneDrive locations to be created.

Pre-provision OneDrive for users

1. If you're pre-provisioning OneDrive for many users, create a list of these users and save it as a file. For example, create a text file named Users.txt that contains:

```
user1@contoso.com
user2@contoso.com
user3@contoso.com
```

2. Download the latest SharePoint Online Management Shell.

> **Note**
>
> If you installed a previous version of the SharePoint Online Management Shell, go to Add or remove programs and uninstall "SharePoint Online Management Shell."

3. Connect to SharePoint as a SharePoint Administrator in Microsoft 365. To learn how, see Getting started with SharePoint Online Management Shell.

> **Note**
>
> The PowerShell command Request-SPOPersonalSite works only for users who are allowed to sign in. If you've blocked users from signing in, you can allow them to sign in by running the PowerShell command **Update-MgUser** using the text file you created in Step 1.
>
> PowerShell
>
> ```
> Get-Content -path "C:\Users.txt" | ForEach-Object { Update-MgUser -
> UserPrincipalName $_ -BlockCredential $False }
> ```

4. Run the PowerShell command Request-SPOPersonalSite, consuming the text file you previously created in Step 1.

PowerShell

```
$users = Get-Content -path "C:\Users.txt"
Request-SPOPersonalSite -UserEmails $users
```

To verify that OneDrive has been created for your users, see Get a list of all user OneDrive URLs in your organization.

Pre-provision OneDrive for all licensed users in your organization

The following code snippet pre-provisions OneDrive in batches of 199.

> **Note**
>
> You need to provide your Microsoft 365 Tenant ID. For more information, see Find IDs and domain names.

PowerShell

```
Param(
    [Parameter(Mandatory = $True)]
    [String]
    $SharepointURL,
    [Parameter(Mandatory = $True)]
    [String]
    $tenantID
)

$scope = 'User.Read.All'
Connect-MgGraph -TenantId $tenantId -Scopes $scope
Connect-SPOService -Url $SharepointURL;

$list = @() #list of UPN to pass to the SP command
$Totalusers = 0 #total user provisioned.

#Get licensed users
$users = Get-MgUser -Filter 'assignedLicenses/$count ne 0' -ConsistencyLevel
eventual -CountVariable licensedUserCount -All -Select UserPrincipalName

foreach ($u in $users) {
    $Totalusers++
    Write-Host "$Totalusers/$($users.Count)"
    $list += $u.userprincipalname

    if ($list.Count -eq 199) {
        #We reached the limit
        Write-Host "Batch limit reached, requesting provision for the current
batch"
        Request-SPOPersonalSite -UserEmails $list -NoWait
        Start-Sleep -Milliseconds 655
        $list = @()
    }
}

if ($list.Count -gt 0) {
    Request-SPOPersonalSite -UserEmails $list -NoWait
}
Disconnect-SPOService
Disconnect-MgGraph
Write-Host "Completed OneDrive Provisioning for $Totalusers users"
```

Related topics

Plan hybrid OneDrive

Set the default storage space for OneDrive users

Summarize this article for me

For most subscription plans, the default storage space for each user's OneDrive is 1 TB. Depending on your plan and the number of licensed users, you can increase this storage up to 5 TB. For info, see the OneDrive service description. If you change a user's license, the available storage space is updated automatically within 24 hours after they access OneDrive.

> **Note**
>
> For help with finding out which subscription you have, see What Microsoft 365 Apps for business subscription do I have?.

Set the default OneDrive storage space in the SharePoint admin center

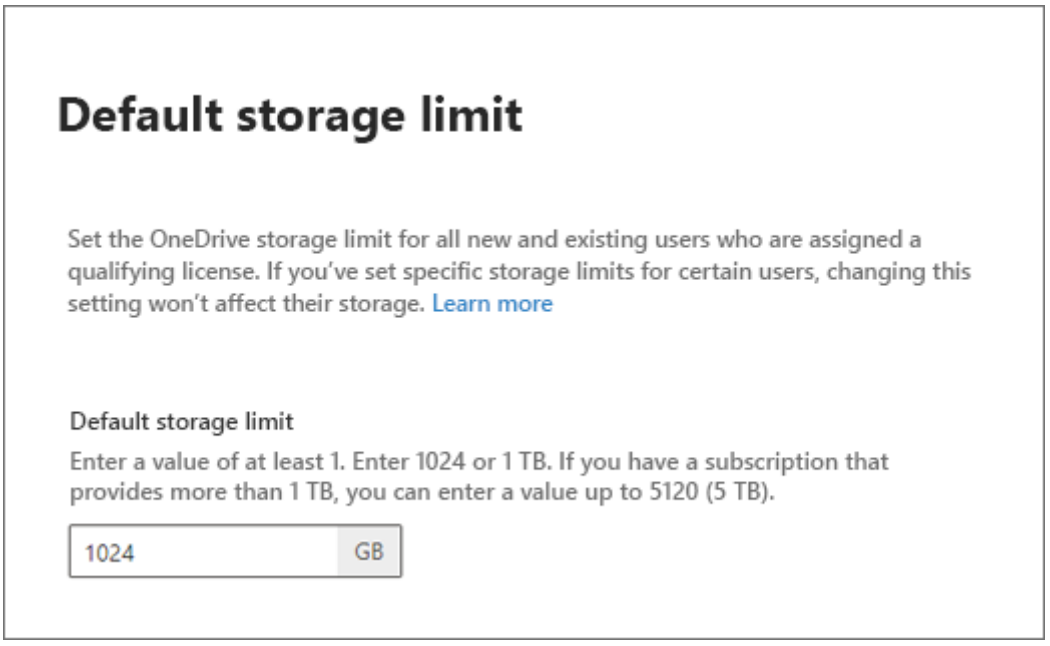
This storage space setting applies to all new and existing users who are licensed for a qualifying plan and for whom you haven't set specific storage limits. (To check if a user has a specific storage limit, see the next section.) To change the storage space for specific users, see Change a specific user's OneDrive storage space.

> **Warning**
>
> If you decrease the storage limit and a user is over the new limit, their OneDrive will become read-only.

1. Go to **Settings** in the new SharePoint admin center, and sign in with an account that has admin permissions for your organization.

   > **Note**
   >
   > If you have Office 365 operated by 21Vianet (China), sign in to the Microsoft 365 admin center, then browse to the SharePoint admin center and open the Settings page.

2. Select the OneDrive **Storage limit** setting.



3. In the **Default storage limit** box, enter the default storage amount (in GB), and then select **Save**.

> ⓘ **Note**
>
> The minimum storage is 1 GB.

Check if a user has the default storage limit or a specific limit

1. Sign in to https://admin.microsoft.com as an IT administrator. (If you see a message that you don't have permission to access the page, you don't have Microsoft 365 admin permissions in your organization.)

> ⓘ **Note**
>
> If you have Office 365 operated by 21Vianet (China), sign in at https://login.partner.microsoftonline.cn/. Then select the Admin tile to open the admin center.

2. In the left pane, select **Users**, and then select **Active users**.

3. Select the user.

4. Select the **OneDrive** tab.

5. Next to "Storage used," look at the max value (for example, 3 GB **of 1024 GB**).

Set the default OneDrive storage space using PowerShell

1. Download the latest SharePoint Online Management Shell.

   > **Note**
   >
   > If you installed a previous version of the SharePoint Online Management Shell, go to **Installed apps** and uninstall "SharePoint Online Management Shell."

2. Connect to SharePoint as a SharePoint Administrator or above in Microsoft 365. To learn how, see Getting started with SharePoint Online Management Shell.

3. Run the following command:

   PowerShell
   ```
   Set-SPOTenant -OneDriveStorageQuota <quota>
   ```

   Where <*quota*> is the value in megabytes for the storage space. For example, 1048576 for 1 TB or 5242880 for 5 TB. You can specify any value that you want, however, if you specify a value greater than that allowed by a given user's license, that user's storage space is rounded down to the maximum value allowed by their license.

   To reset an existing user's OneDrive to the new default storage space, run the following command:

   PowerShell
   ```
   Set-SPOSite -Identity <user's OneDrive URL> -StorageQuotaReset
   ```

   > **Note**
   >
   > When you set site storage limits in PowerShell, you enter them in MB. The values are converted and rounded down to the nearest integer to appear in the admin centers in GB, so a value of 5000 MB becomes 4 GB. If you set a value of less than 1024 MB using PowerShell, it's rounded up to 1 GB.

See also

More info about using Set-SPOTenant

Last updated on 03/10/2026

OneDrive for Business storage quota enforcement: Frequently asked questions

This article answers common questions about recent changes to how OneDrive for Business enforces per-user storage quotas, ensuring they align with each user's license entitlement. These updates address previous inconsistencies and improve quota enforcement reliability.

> **Note**
>
> **This change correctly applies the OneDrive for Business storage your licenses provide.** Every user's maximum OneDrive limit has always been defined by their license. The only users affected are those configured above their licensed entitlement - so no storage that was purchased is removed. This change isn't a change in service or terms.

General

Will the storage quota enforcement changes impact my organization?

Most tenants aren't affected. Only users whose OneDrive storage is set above what their license entitles - typically due to a user-specific limit set higher than the entitlement - are impacted.

To check if your users are affected, run the PnP PowerShell report: Identify OneDrive Users Over License-Based Storage Quota.

If all users are within their licensed quotas, no action is required.

What happens if a user's OneDrive for Business storage allocation is exceeded?

When a user's OneDrive usage exceeds their licensed quota, their OneDrive enters a read-only state. In this state, users can't edit existing files or add new files in their OneDrive, but they can download or delete existing content.

Are extended storage allocations still allowed?

Users keep extended storage only if they continue to hold a license that grants the higher (extended) allocation. Extended storage is tied to qualified Enterprise Plan 2 licenses. If the Enterprise Plan 2 license is present, the extended allocation remains. If a user with extended allocation no longer has a qualifying license, their maximum storage is adjusted to match their current license entitlement.

How can I restore a user's OneDrive for Business from read-only state?

A user's OneDrive becomes read-only when their usage exceeds their licensed quota. To fix this problem, you can:

1. **Upgrade the user's license** to one with a higher entitlement.
2. **Reduce the user's storage usage** to within the licensed limit. Remember that version history, recycle bins, and Preservation Hold libraries are included in storage usage calculations.
3. **Buy extra per-user capacity** by using OneDrive Extra Storage capacity packs, which are available in 100 GB, 500 GB, and 1 TB–6 TB sizes. Each pack is assigned per user and can't be split across users. A single user's total storage can't exceed 25 TB. Add storage space

Note: The pay-as-you-go option, M365 OneDrive Storage, will be available in public preview in July 2026. It's not currently available to education and government customers. Education and Government tenants should use license upgrades, usage reduction, or OneDrive Extra Storage capacity packs.

I'm an Education tenant—are my users impacted?

Generally, only users with a user-specific limit set above their license entitlement are affected.

- **A1:** Entitled to 100 GB per user.
- **A3 / A5:** Licenses that include the “SharePoint (Plan 2) for Education” service plan entitle the user to a 5 TB OneDrive limit, or up to 25 TB if they have extended storage allocation. If you use a less common A3 or A5 SKU, confirm it includes SharePoint (Plan 2) for Education. Admins can set a lower quota, which is honored.
- **Other licenses:** Storage limits of those licenses are enforced. For example, if a user is entitled to 10 GB and is using more, their limit is set to 10 GB and their OneDrive goes read-only.

Student Use Benefit (SUB) licenses: SUB licenses provide a per-user OneDrive entitlement but don't contribute to the tenant’s shared storage pool. These entitlements are separate.

I'm a government tenant—are my users impacted?

Not at this time. Government environments are currently out of scope. Microsoft will communicate separately when this change becomes applicable to those clouds.

Why is Microsoft making this change?

- **To enforce license-based storage:** Each user's OneDrive storage limit is now consistently enforced according to their license. Only users configured above their licensed entitlement are affected.
- **To fix a bug:** Previously, user-specific limits could be incorrectly updated during quota refreshes, causing inaccurate enforcement. This problem included cases where admin-set limits in Education tenants were reset to default. This fix ensures predictable storage behavior.
- **For consistency and reliability:** Admins managing storage at scale can now rely on license storage limits being enforced uniformly.

What is the difference between tenant storage and individual OneDrive storage?

These two types of storage are separate "accounts." This change affects only individual OneDrive storage:

- **Individual OneDrive (per-user) entitlement:** The maximum amount a single user's OneDrive can hold, set by their license. This change enforces this limit.
- **Shared tenant storage pool:** The organization-wide SharePoint pool. This change doesn't affect the pool contribution.

Key point: Storage packs that add to the shared pool don't allow an individual user to exceed their per-user OneDrive entitlement. To increase a specific user's limit, use a OneDrive Extra Storage capacity pack or a higher-tier license. All storage in a user's OneDrive still counts toward the tenant-wide pool.

When will my tenant be impacted?

- **General Availability:** Rollout begins July 1, 2026, and is expected to complete by mid-July 2026. Timing varies by tenant.
- Admins receive advance notice via Message Center post MC1310684.
- **Government clouds:** Not scheduled at this time.

Related content

- Add storage space (Buy more OneDrive/SharePoint storage: capacity packs & pay-as-you-go)
- Troubleshooting: OneDrive site is read-only because storage quota was exceeded
- SharePoint limits (Service description—pooled storage math)
- OneDrive service description - Service Descriptions | Microsoft Learn (Storage limits by service plan)
- Microsoft 365 Education storage options
- PnP script sample: Identify OneDrive Users Over License-Based Storage Quota

---

Last updated on 07/01/2026

Change a specific user's OneDrive storage space

As an IT administrator, you can adjust a user's OneDrive storage space using the SharePoint admin center or PowerShell.

> **Note**
>
> For setting the default storage space for all users, see Set the default storage space for OneDrive users. For details on available storage for your Microsoft 365 subscription, see the OneDrive service description.

> **Important**
>
> If a user has run out of storage, advise them to proactively review and manage their storage. Instructions can be found at Manage your OneDrive for work.
>
> If your tenant has Microsoft 365 OneDrive Storage enabled, you can set a user's OneDrive storage limit higher than the storage included with their license. For more information, see Add Microsoft 365 OneDrive Storage.

Change storage space in the Microsoft 365 admin center

1. Sign in to the Microsoft 365 admin center with your admin credentials.

   > **Note**
   >
   > For Office 365 operated by 21Vianet (China), sign in here.

2. In the left pane, expand **Users** and select **Active users**.

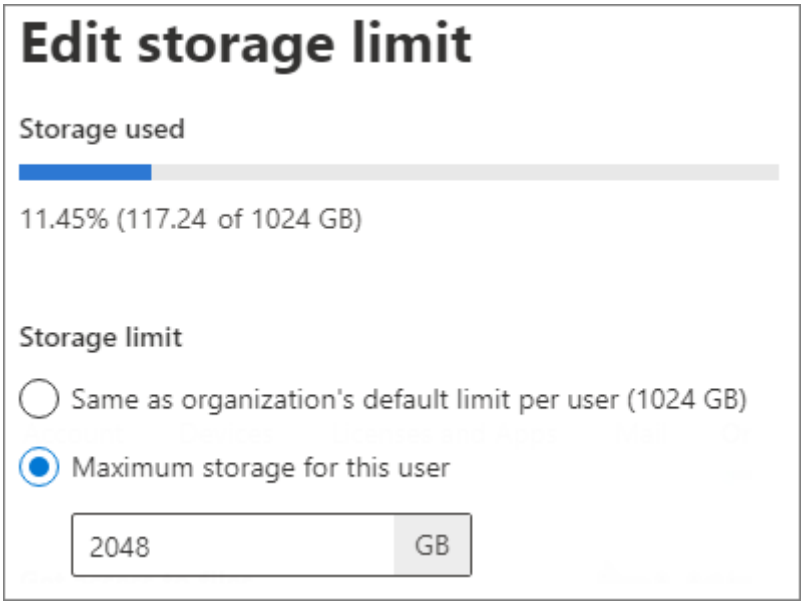
3. Select the user whose storage you want to change.

4. Go to the **OneDrive** tab.

5. Under **Storage used**, select **Edit**.

6. Choose the **Maximum storage for this user** option and set the storage limit.

7. Select **Save**.



> **Note**
>
> For Office 365 A1 users, storage is limited to 100 GB. For more information, see Office 365 Education service descriptions.

Change storage space using PowerShell

1. Download the latest SharePoint Online Management Shell.

> **Note**
>
> Uninstall any previous versions of the SharePoint Online Management Shell before installing the latest version.

2. Save the following PowerShell script to a file (for example, you can save it as *UpdateOneDriveStorage.ps1*):

PowerShell

```
$TenantUrl = Read-Host "Enter the SharePoint admin center URL"
Connect-SPOService -Url $TenantUrl
```

```
$OneDriveSite = Read-Host "Enter the OneDrive Site URL"
$OneDriveStorageQuota = Read-Host "Enter the OneDrive Storage Quota in MB"
$OneDriveStorageQuotaWarningLevel = Read-Host "Enter the OneDrive Storage Quota
Warning Level in MB"
Set-SPOSite -Identity $OneDriveSite -StorageQuota $OneDriveStorageQuota -
StorageQuotaWarningLevel $OneDriveStorageQuotaWarningLevel
Write-Host "Done"
```

3. Open the SharePoint Online Management Shell and run the following script:

PowerShell

```
PS C:\>.\UpdateOneDriveStorage.ps1
```

> **Note**
>
> If you receive an error regarding script execution, you may need to adjust your PowerShell execution policies. For more information, see About execution policies.

4. Enter the required values when prompted, including:

   - The SharePoint admin center URL (for example, `https://contoso-admin.sharepoint.com`)
   - The OneDrive site URL (for example, `https://contoso-my.sharepoint.com/personal/user_contoso_onmicrosoft_com`)
   - Storage Quota in MB
   - Storage Quota Warning Level in MB

Here's a reference table for MB to TB conversions:

Expand table

MB	TB
1,048,576	1
2,097,152	2
3,145,728	3
4,194,304	4
5,242,880	5

> **Note**
>
> To change storage space for multiple users, you can list OneDrive accounts via PowerShell and use the Set-SPOSite command to apply changes.

Troubleshooting OneDrive storage issues

If you encounter issues when adjusting storage or if the storage amount reverts to its original value, a Microsoft 365 administrator can run diagnostics in the Microsoft 365 admin center.

1. Select the following **Run Tests** button, which populates the diagnostic in the Microsoft 365 admin center.

   Run Tests: OneDrive Storage Quota

   > **Note**
   >
   > Diagnostics are unavailable for GCC High, DoD, Microsoft 365 operated by 21Vianet, and Microsoft 365 Education.

2. Follow the recommendations provided by the diagnostic.

   > **Note**
   >
   > For information on disabling OneDrive creation for specific users, see Manage user profiles in the SharePoint admin center.

Last updated on 09/29/2026

Set the OneDrive retention for deleted users

Article • 04/05/2025

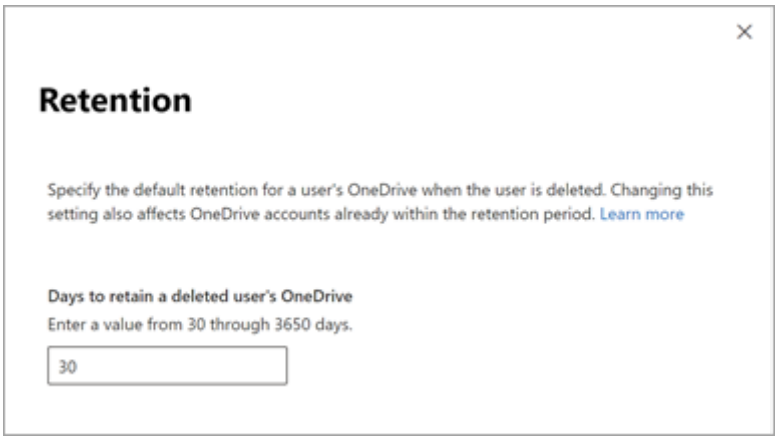
If a user's Microsoft 365 account is deleted, their OneDrive files are preserved for a period of time. You can set this time period.

Set the retention time for OneDrive accounts

1. Go to **Settings** in the new SharePoint admin center, and sign in with an account that has admin permissions for your organization.

   > **Note**
   >
   > If you have Office 365 operated by 21Vianet (China), sign in to the Microsoft 365 admin center, then browse to the SharePoint admin center and open the Sharing page.

2. Select the **Retention** setting.

3. Enter a value from 30 through 3650 in the **Days to retain files a deleted user's OneDrive** box.

   The setting is activated for the next user that is deleted as well as any users that are in the process of being deleted. The count begins as soon as the user account was deleted in the Microsoft 365 admin center, even though the deletion process takes time.

4. Select **Save**.

Related articles

Delete a user from your organization

Set up OneDrive to alert managers and delegate access automatically when users leave your organization

Overview of retention policies

Standard storage for unlicensed OneDrive accounts

Overview

Standard storage gives SharePoint administrators more control over how long unlicensed OneDrive accounts remain active before they are archived. It also lets an administrator reactivate a specific archived account for longer than the ordinary 30-day reactivation period. It builds on the default unlicensed account lifecycle described in Manage unlicensed OneDrive user accounts.

The billing experience has two distinct steps:

- **Connect pay-as-you-go billing.** Before admins can reactivate archived unlicensed OneDrive accounts, set up pay-as-you-go billing in the Microsoft 365 admin center. Follow Set up pay-as-you-go billing to link an Azure subscription, then enable that billing subscription for unlicensed OneDrive account billing. For more information about the unlicensed account lifecycle and billing states, see Manage unlicensed OneDrive user accounts.
- **Enable Standard storage.** Standard storage is a separate opt-in that unlocks the tenant-wide duration control and lets selected reactivated accounts remain active beyond 30 days. When Standard storage is available, enable it from the dedicated unlicensed OneDrive accounts experience in the Microsoft 365 admin center. There is no SharePoint Online PowerShell parameter for enabling the billing policy or Standard storage.

Enabling Standard storage does not reactivate every archived account. Increasing the tenant-wide active-storage period also applies to existing unlicensed accounts: archived accounts that have been unlicensed for less than the newly configured period are reactivated. Accounts already beyond that period remain archived. Administrators can use account-specific reactivation controls for selected accounts. Content is billed according to its current tier: archived content uses the Archive meter, and active content retained through Standard storage uses the Standard meter.

Increasing the tenant-wide period can incur reactivation fees for eligible archived accounts that are reactivated. During calendar year 2026, these reactivation fees are waived when Standard storage is enabled. See Pricing.

> ⓘ **Note**

Standard storage will be generally available for unlicensed OneDrive accounts starting in October 2026. Until then, the Standard storage billing option might not appear in the Microsoft 365 admin center, even after you connect pay-as-you-go billing.

Capabilities

Standard storage billing

Set up pay-as-you-go billing and enable Standard storage in the Microsoft 365 admin center before using the new duration controls. There is no SharePoint Online PowerShell parameter for enabling the billing policy or Standard storage.

Duration and account controls

Expand table

Scenario	Scope	Intended behavior
Set the active-storage period	Tenant (all applicable unlicensed OneDrive accounts)	Changes when accounts become read-only and are archived. Supported values are 93 through 3,650 days.
Check the current period	Tenant	Reads the current active-storage period through Get-SPOTenant.
Reactivate until a specific date	One archived unlicensed OneDrive account	Reactivates the account and keeps it active until the date supplied with -KeepActiveUntil.
Extend an active period	One active or reactivating account	Updates the Standard storage end date by running the same command with a later valid date.
Archive early	One active account	Returns the account to Archive storage before its scheduled date.

The tenant period can't exceed 3,650 days, and an account-specific extension requires a date. Both the tenant period and the per-account `-KeepActiveUntil` flag require a duration or date. There's no way to keep an account active indefinitely. Extend the period or date later if continued access is required.

Manage these duration controls through SharePoint Online PowerShell. Controls for the same scenarios are planned for the SharePoint admin center later.

Pricing

Archive storage, Standard storage, and reactivation are billed through pay-as-you-go. For current prices, see Storage services.

An ordinary reactivation includes the standard 30-day access period. Standard storage charges apply when an account remains active beyond that window. During calendar year 2026, the reactivation fee is waived when Standard storage is enabled.

Reactivation fees also apply when an archived account is reactivated by increasing `UnlicensedOneDriveAccountsActiveStoragePeriod`, not only when an administrator runs a per-account reactivation command. The published reactivation rate is $0.60 per GB reactivated; see Storage services for current pricing. During calendar year 2026, the fee is waived when Standard storage is enabled. Reactivation fees are separate from ongoing storage charges. Accounts that remain archived continue to use the Archive meter, while active content retained through Standard storage uses the Standard meter.

Lifecycle example

The default tenant-wide archive point is 93 days after an account becomes unlicensed. The account becomes read-only 33 days before it is archived. For the complete default timeline, including read-only, eDiscovery, and deletion milestones, see Manage unlicensed OneDrive user accounts.

If an administrator changes the tenant period to 365 days:

- The account remains active through day 331.
- The account becomes read-only on day 332.
- The account is archived on day 365.

After an account is archived, ordinary reactivation provides 30 days of access. Use `-KeepActiveUntil` when the account must remain active beyond that standard window.

Before you begin

Confirm the following prerequisites:

- Pay-as-you-go billing is connected for unlicensed OneDrive accounts. For details about identifying and managing these accounts, see Manage unlicensed OneDrive user accounts.
- Standard storage is enabled in the Microsoft 365 admin center.
- You're using a SharePoint Online Management Shell version that exposes the new parameters.

- You're connected to SharePoint Online as a SharePoint administrator.
- You have the OneDrive personal-site URL for each account you want to manage.

Connect to the SharePoint Online admin endpoint:

PowerShell

```
Connect-SPOService -Url "https://contoso-admin.sharepoint.com"
```

Replace contoso and all sample OneDrive URLs in this article with values for your tenant.

Admin workflow

1. Set the tenant-wide Standard storage period

Use `Set-SPOTenant` to specify how many days an unlicensed OneDrive account remains active before it is archived:

PowerShell

```
Set-SPOTenant `
    -UnlicensedOneDriveAccountsActiveStoragePeriod 365
```

The supported range is 93 through 3,650 days. The command displays a confirmation prompt. The read-only stage begins 33 days before the configured archive date.

Standard storage normally must be enabled to change this setting. If a tenant previously configured a custom value and later disables Standard storage billing, the service defaults to 93 days functionally.

The setting applies retroactively, not only to accounts that become unlicensed after the change. Increasing the period can therefore reactivate existing archived accounts without a separate per-account reactivation command.

For example, increasing the tenant period from 93 to 180 days has these results:

Expand table

Account	Days unlicensed	State before change	Result	Reactivation fee from this change
A	38	Active	Remains active	None; no reactivation occurs

Account	Days unlicensed	State before change	Result	Reactivation fee from this change
B	105	Archived	Reactivated because it is within the new period	Applies, unless the change is made during calendar year 2026 with Standard storage enabled
C	227	Archived	Remains archived because it is beyond the new period	None; no reactivation occurs

Reactivation caused by this tenant-setting change incurs the reactivation fee, except during calendar year 2026 when the fee is waived with Standard storage enabled. The read-only stage still begins 33 days before the configured archive date.

Best practice: Keep the default at 93 days unless your organization has a defined business, legal, or compliance need for a longer lifecycle. Use the shortest period that meets the requirements.

2. Check the current tenant setting

PowerShell

```
Get-SPOTenant | Select-Object UnlicensedOneDriveAccountsActiveStoragePeriod
```

If the property returns 0, the connected SharePoint Online endpoint might not yet expose the property. Update the SharePoint Online Management Shell and verify that the feature is available for the tenant.

3. Reactivate an account for the ordinary 30-day period

Use ordinary reactivation when 30 days of access is sufficient:

PowerShell

```
Set-SPOSiteArchiveState `
    -Identity "https://contoso-my.sharepoint.com/personal/user_contoso_com" `
    -ArchiveState Active
```

The target must be an archived unlicensed OneDrive personal site. Connecting the billing policy permits this ordinary reactivation even when the account-specific Standard storage extension is not used.

4. Reactivate an account until a specific date

Use `-KeepActiveUntil` when access is required beyond the ordinary 30-day period:

PowerShell

```
Set-SPOSiteArchiveState `
    -Identity "https://contoso-my.sharepoint.com/personal/user_contoso_com" `
    -ArchiveState Active `
    -KeepActiveUntil "2027-08-13"
```

The supplied date is interpreted in the administrator's local time and converted to UTC. For a newly reactivated account, the date must extend beyond the ordinary 30-day reactivation window. The server validates billing eligibility, rollout availability, site type, site state, and the date.

5. Extend an account that is active or reactivating

Run the same command with a later valid date:

PowerShell

```
Set-SPOSiteArchiveState `
    -Identity "https://contoso-my.sharepoint.com/personal/user_contoso_com" `
    -ArchiveState Active `
    -KeepActiveUntil "2027-10-31"
```

This command updates the stored Standard storage date. It doesn't change the tenant-wide active-storage period.

6. Return an account to Archive storage early

When active access is no longer needed, archive the account before its scheduled date:

PowerShell

```
Set-SPOSiteArchiveState `
    -Identity "https://contoso-my.sharepoint.com/personal/user_contoso_com" `
    -ArchiveState Archived
```

This command returns the account to Archive storage and stops continued Standard storage use for that account.

Choose the right control

Expand table

Scenario	Recommended action
The default 93-day lifecycle is appropriate for most accounts	Leave the tenant period at 93 days.
All applicable unlicensed accounts need a longer lifecycle	Set UnlicensedOneDriveAccountsActiveStoragePeriod to a justified value from 94 through 3,650.
A single archived account needs access for 30 days or less	Reactivate it with -ArchiveState Active and omit -KeepActiveUntil.
A single archived account needs access beyond 30 days	Reactivate it with -ArchiveState Active and a valid -KeepActiveUntil date.
An active or reactivating account needs more time	Run the command again with a later -KeepActiveUntil date.
Access is no longer needed	Set -ArchiveState Archived to return the account to Archive storage early.

Best practices

- Use a longer tenant-wide period only when the requirement applies broadly. Use account-specific dates for exceptions.
- Return accounts to Archive storage when active access is no longer required.
- Monitor both Archive and Standard storage consumption and charges.

Troubleshooting

The tenant parameter isn't recognized

Update the SharePoint Online Management Shell. Confirm that the installed build includes UnlicensedOneDriveAccountsActiveStoragePeriod.

Get-SPOTenant returns 0 for the property

The connected endpoint might not yet have the server build that exposes the read-back property. Verify rollout eligibility and try again after updating the management shell.

These standard-storage properties require PowerShell version 16.0.27600.12000 or higher.

The tenant setting update is rejected

Verify that:

- The value is from 93 through 3,650.
- Standard storage billing is enabled.

If billing was disabled after a custom value was configured, only a reset to 93 is allowed.

Reactivation or extension is rejected

Verify that:

- The URL identifies a OneDrive personal site, not a SharePoint team or communication site.
- The account is unlicensed and in a supported archive, active, or reactivating state.
- You use `-KeepActiveUntil` only with `-ArchiveState Active`.
- Standard storage is enabled when you request a date beyond the ordinary 30-day period.
- The date is valid and extends beyond the standard reactivation window.

The account should no longer use Standard storage

Run `Set-SPOSiteArchiveState` with `-ArchiveState Archived` to return it to Archive storage.

Related guidance

- Manage unlicensed OneDrive user accounts
- Connect to SharePoint Online PowerShell

Last updated on 10/13/2026

Restore a deleted OneDrive

Article • 02/07/2025

When you delete a user in the Microsoft 365 admin center (or when a user is removed through Active Directory synchronization), the user's OneDrive is retained for the number of days you specify in the SharePoint admin center. (For info, see Set the default file retention for deleted OneDrive users.) The default is 30 days. During this time, other users can still access shared content. At the end of the time period, the OneDrive remains in a deleted state for 93 days and can only be restored by a SharePoint Administrator.

For info about using Files Restore to restore a OneDrive to a previous point in time, see Restore your OneDrive.

For info about restoring items from the recycle bin in OneDrive, see Restore deleted files or folders.

Restore a deleted OneDrive when the deleted user no longer appears in the Microsoft 365 admin center

If the user was deleted within 30 days, you can restore the user and all their data from the Microsoft 365 admin center. To learn how, see Restore a user in Microsoft 365. If you deleted the user more than 30 days ago, the user will no longer appear in the Microsoft 365 admin center, and you need to use PowerShell to restore the OneDrive.

1. Download the latest SharePoint Online Management Shell.

   > **Note**
   >
   > If you installed a previous version of the SharePoint Online Management Shell, go to Add or remove programs and uninstall "SharePoint Online Management Shell."

2. Connect to SharePoint as a SharePoint Administrator in Microsoft 365. To learn how, see Getting started with SharePoint Online Management Shell.

3. Determine if the OneDrive is available for restore.

   - If you know the URL of the OneDrive, run the following command:

     ```
     PowerShell
     ```

```
Get-SPODeletedSite -Identity <URL>
```

A user's OneDrive URL is based on their username. For example, `https://contoso-my.sharepoint.com/personal/user1_contoso_com`. You can find their username on the Active users (or Deleted users) page in the Microsoft 365 admin center.

- If you don't know the URL of the deleted OneDrive, run the following command:

  PowerShell

  ```
  Get-SPODeletedSite -IncludeOnlyPersonalSite | FT url
  ```

- If the OneDrive appears in the results, it can be restored.

4. Restore the OneDrive to an active state:

   PowerShell

   ```
   Restore-SPODeletedSite -Identity <URL>
   ```

5. Assign an administrator to the OneDrive to access the needed data:

   PowerShell

   ```
   Set-SPOUser -Site <URL> -LoginName <UPNofDesiredAdmin> -IsSiteCollectionAdmin
   $True
   ```

For more info about these cmdlets, see Get-SPODeletedSite and Restore-SPODeletedSite.

> **Note**
>
> When a OneDrive is restored, it continues to remain available until it's explicitly deleted.

Permanently delete a OneDrive

After you recover the data you need from the OneDrive, we recommend that you permanently delete the OneDrive by running the following command:

PowerShell

```
Remove-SPOSite -Identity <URL>
```

```
Remove-SPODeletedSite -Identity <URL>
```

> **Caution**
>
> When you permanently delete a OneDrive, you won't be able to restore it.

See also

OneDrive retention and deletion
Manage site redirects

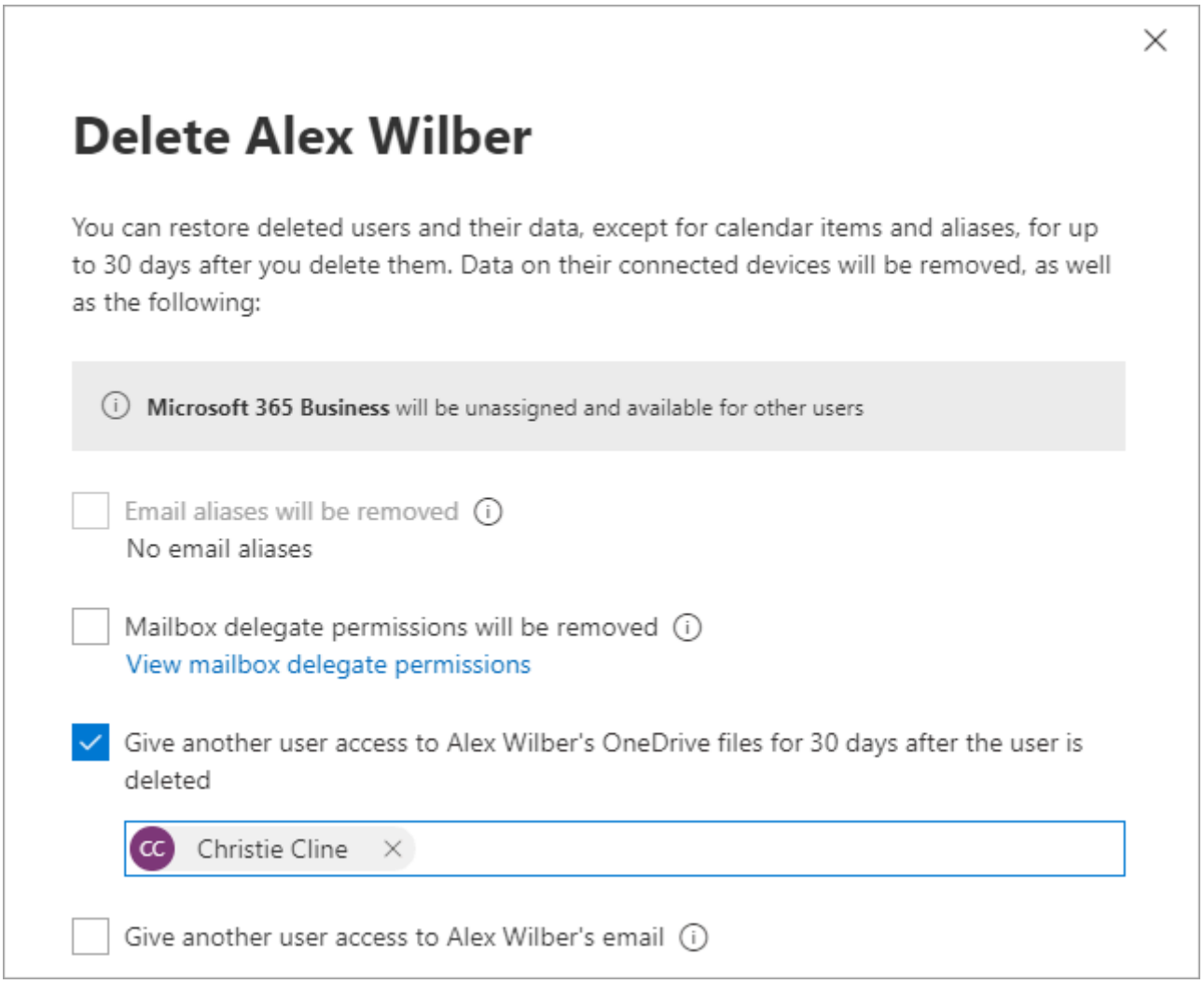
OneDrive retention and deletion

This article describes how you can manage a user's OneDrive when you delete the user's Microsoft 365 account for your organization, and what steps happen automatically.

> **Important**
>
> All OneDrive accounts that don't have a valid OneDrive license are automatically archived on their 93rd unlicensed day. Retention settings, retention policies, eDiscovery, and all holds are still honored while an unlicensed account is in the paid archive state. After 12 month of Unpaid storage/archive the OneDrive Data might be deleted regardless of Retention settings, retention policies, eDiscovery, and all holds. For more info, see Manage unlicensed OneDrive user accounts.

Deleting a user from the Microsoft 365 admin center

When you delete a user from the Active users page in the Microsoft 365 admin center, you can choose what you want to do with the user's product licenses, email, and OneDrive. For more info, see Delete a user from your organization.



If you give another user access to the OneDrive, that user has 30 days by default to access and download the files they want to keep. (To change the retention time, see Set the OneDrive retention for deleted users).

Configure automatic access delegation

By default, when a user is deleted, the user's manager is automatically given access to the user's OneDrive. Follow these steps to confirm that this automatic access delegation is enabled for your organization, and to set a secondary owner in case a user doesn't have a specified manager. If access delegation is disabled or a manager or secondary owner isn't set for a user, no one has automatic access when the user is deleted or be warned that the OneDrive will be deleted. For guidance on transferring files securely when an employee leaves, see Simplified file transfer for departing employees.

1. Go to More features in the new SharePoint admin center, and sign in with an account that has admin permissions for your organization.

> **Note**

> If you have Office 365 operated by 21Vianet (China), sign in to the Microsoft 365 admin center, then browse to the SharePoint admin center and open the More features page.

2. Under **User profiles**, select **Open**.
3. Under **My Site Settings**, select **Setup My Sites**.
4. Next to **My Site Cleanup**, make sure **Enable access delegation** is selected.
5. We recommend that you also specify a secondary owner account in the **My Site Cleanup** section. This account is the appointed owner of the OneDrive if the user's manager isn't set in Microsoft Entra ID. Email notifications will also be sent to the secondary owner account when the value is populated.
6. Select **OK**.

The OneDrive deletion process

The OneDrive retention period for cleanup of OneDrive begins when a user account is deleted from Microsoft Entra ID. No other action causes the cleanup process to occur, including blocking the user from signing in or removing the user's license. For info about removing a user's license, see Remove licenses from users in Microsoft 365 for business.

> **Note**
>
> Unlicensed OneDrive accounts get automatically archived on their 93rd unlicensed day, even if the account is retained for longer than 93 days due to the retention period. When a user account is deleted from Microsoft Entra ID, the OneDrive account is considered unlicensed. To learn more about the unlicensed process, see Manage unlicensed OneDrive user accounts.

The OneDrive deletion process works as follows:

1. A user is deleted from the Microsoft 365 admin center or is removed through Active Directory synchronization.
2. The account deletion is synchronized to SharePoint.

3. The OneDrive Clean Up Job runs, and the OneDrive is marked for deletion. The deleted user appears in the Microsoft 365 admin center for 30 days. The default retention period for OneDrive is also 30 days, but you can change this in the SharePoint admin center. See Set the OneDrive retention for deleted users or by using the PowerShell cmdlet `Set-SPOTenant -OrphanedPersonalSitesRetentionPeriod <int32>`. For more information about using this cmdlet, see Set-SPOTenant.

4. If a manager is specified for the deleted user, the manager receives an email telling them that they have access to the OneDrive, and that the OneDrive will be deleted at the end of the OneDrive retention period. For info about specifying a user's manager in the Microsoft Entra admin center, see Add or update a user's profile information.

   If a manager isn't specified for the user account, but a secondary owner was entered in the SharePoint admin center, the secondary owner receives an email telling them that they have access to the OneDrive, and that the OneDrive will be deleted at the end of the retention period.

5. Seven days before the OneDrive retention period expires, a second email is sent to the manager or secondary owner as a reminder that the OneDrive will be deleted in seven days.

6. After seven days, the OneDrive for the deleted user is moved to the site collection recycle bin, where it's kept for 93 days. During this time, users will no longer be able to access any shared content in the OneDrive. To restore the OneDrive, you need to use PowerShell. For info, see Restore a deleted OneDrive.

   > **Note**
   >
   > The Recycle Bin isn't indexed and therefore searches don't find content there. This means that an eDiscovery hold can't locate any content in the Recycle Bin in order to hold it.

Microsoft 365 retention settings from retention policies and retention labels always take precedence to the standard OneDrive deletion process, so content included for OneDrive retention could be deleted before 30 days or retained for longer than the OneDrive retention period. Likewise, if a OneDrive is put on hold as part of an eDiscovery case, managers and secondary owners are sent email about the pending OneDrive deletion, but the OneDrive won't be deleted until the hold is removed.

Related articles

- Managers or designated secondary users can move files from a departing employee's OneDrive to their own OneDrive or to a SharePoint site. Follow a guided walkthrough to complete the transfer securely, see Simplified file transfer for departing employees .

Last updated on 06/23/2026

View OneDrive URLs for users in your organization

Article • 04/05/2025

As a SharePoint Administrator, you can confirm OneDrive URLs for specific users in your organization. Whether you're troubleshooting, provisioning new accounts, or simply ensuring accurate information, understanding the methods to retrieve OneDrive URLs is essential.

About OneDrive URLs

The URL for a user's OneDrive is usually in the following format: `https://<tenant name>-my.sharepoint.com/personal/<user principal name>`. For the user principal name (UPN), any special characters such as a period, comma, space, and the at sign ("@") are converted to underscores ("_"). See the following table for examples.

Expand table

Domain	UPN	OneDrive URL
`onmicrosoft.com`	`rsimone@contoso.onmicrosoft.com`	`https://contoso-my.sharepoint.com/personal/rsimone_contoso_onmicrosoft_com`
custom	`rsimone@contoso.com`	`https://contoso-my.sharepoint.com/personal/rsimone_contoso_com`

Numbers or GUIDs might be appended to the URL if a conflict is detected. We recommend you confirm a user's OneDrive URL if you need to specify it.

> **Note**
>
> Unless OneDrive accounts are pre-provisioned, the URL isn't created until a user accesses their OneDrive for the first time.
>
> Also, the OneDrive URL will automatically change if the user's UPN changes. For example, if the user changes their name or the domain name changes for a repositioning or business restructuring.

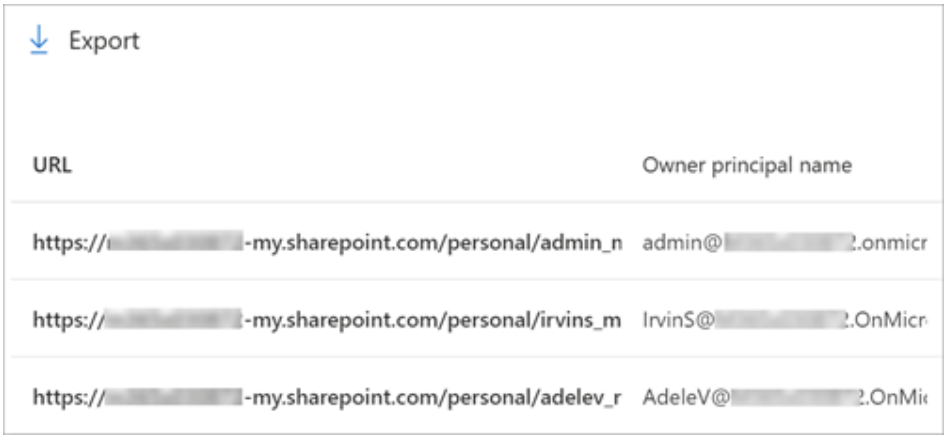
Use the OneDrive usage report to view the list of OneDrive users and URLs

1. Go to the OneDrive usage report in the Microsoft 365 admin center and sign in as a SharePoint Administrator, or reports reader. If you see a message that you don't have

permission to access the page, you don't have one of these roles in your organization. For more roles with access, see Microsoft 365 Reports in the admin center.

> **Note**
>
> If you have Office 365 operated by 21Vianet (China), sign in to the Microsoft 365 admin center, browse to **Reports** > **Usage**. Under **OneDrive files**, select **View more**.

2. Scroll to the table below the charts.



If you see GUIDs in the table instead of URLs and names, go to the Reports setting and clear the box **In all reports, display deidentified names for users, groups, and sites**.

You can copy individual OneDrive URLs from the URL column. For easier searching and copying, export the table as a .csv file. In the upper left of the table, select **Export**.

Learn more about the Microsoft OneDrive usage report

Use PowerShell to create a list of all the OneDrive URLs in your organization

The list you create in these steps are saved to a text file.

1. Download the latest SharePoint Online Management Shell.

> **Note**
>
> If you installed a previous version of the SharePoint Online Management Shell, go to Add or remove programs and uninstall "SharePoint Online Management Shell."

2. Save the following text to a PowerShell file. For example, you could save it to a file named OneDriveSites.ps1.

```
PowerShell
```

```
$TenantUrl = Read-Host "Enter the SharePoint admin center URL"
$LogFile = [Environment]::GetFolderPath("Desktop") + "\OneDriveSites.log"
Connect-SPOService -Url $TenantUrl
Get-SPOSite -IncludePersonalSite $true -Limit all -Filter "Url -like '-
my.sharepoint.com/personal/'" | Select -ExpandProperty Url | Out-File $LogFile -
Force
Write-Host "Done! File saved as $($LogFile)."
```

3. Open the SharePoint Online Management Shell. Navigate to the directory where the script was saved and run:

```
PS C:\>.\OneDriveSites.ps1
```

> **Note**
>
> If an error message about being unable to run scripts appears, you need to change your execution policies. For more information, see About Execution Policies.

4. The script prompts you for the SharePoint admin center URL. For example, `https://contoso-admin.sharepoint.com` is the Contoso SharePoint admin center URL.

5. When prompted, sign in with your SharePoint Administrator account credentials.

After the script successfully completes, a text file is created in the location specified by the **$LogFile** variable in the script. This file contains a list of all OneDrive URLs in your organization. The following text provides an example of how the list of URLs in this file should be formatted.

```
https://contoso-my.sharepoint.com/personal/annb_contoso_onmicrosoft_com/
https://contoso-my.sharepoint.com/personal/carolt_contoso_onmicrosoft_com/
https://contoso-my.sharepoint.com/personal/esterv_contoso_onmicrosoft_com/
https://contoso-my.sharepoint.com/personal/hollyh_contoso_onmicrosoft_com/
```

Once you have the URL for a user's OneDrive, you can get more info about it by using the Get-SPOSite cmdlet, and change settings by using the Set-SPOSite cmdlet.

Other methods to retrieve OneDrive URLs

Method 1: Using the Diagnostic Information section in OneDrive settings

1. As an administrator of the OneDrive site, navigate to the site.
2. In the upper right-hand corner, select the **Settings** icon.

3. Select **OneDrive Settings** and **More Settings**.
4. Under the **Diagnostic Information** section, copy the OneDrive Web URL.

Method 2: Using PnP PowerShell (Get-PnPUserProfileProperty)

PnP PowerShell is a versatile tool for managing SharePoint and OneDrive. To retrieve the PersonalURL (OneDrive URL) for a user, follow these steps:

1. **Install PnP PowerShell** if you haven't already. Run the following command in PowerShell:

   ```PowerShell
   Install-Module PnP.PowerShell -Scope CurrentUser
   ```

   - If you need more details on installation, refer to the official PnP PowerShell installation guide.

2. Run the following command:

   ```PowerShell
   Get-PnPUserProfileProperty -Account "user@example.com" | Select-Object -
   ExpandProperty PersonalUrl
   ```

   - Replace `"user@example.com"` with the actual user's email address.

Method 3: Microsoft Graph API

The Microsoft Graph API provides programmatic access to OneDrive and other Microsoft 365 services. To get the OneDrive URL using Graph API:

1. **Install the Microsoft Graph PowerShell module** if you haven't already. Use this command:

   ```PowerShell
   Install-Module Microsoft.Graph
   ```

   - For step-by-step instructions, check out this tutorial on installing PnP PowerShell for SharePoint Online and Azure Cloud Shell.

2. Authenticate and connect to Microsoft Graph:

   ```PowerShell
   Connect-MgGraph -Scopes "Directory.ReadWrite.All", "Sites.ReadWrite.All",
   "Files.ReadWrite.All"
   ```

3. Retrieve the OneDrive URL for a specific user:

PowerShell

```
$userPrincipalName = "user@example.com"
$userObject = Get-MgUser -Filter "userPrincipalName eq '$userPrincipalName'"
$userOneDrive = Get-MgUserDefaultDrive -UserId $userObject.id
$oneDriveWebUrl = $userOneDrive.webUrl
Write-Host "OneDrive WebURL for $userPrincipalName: $oneDriveWebUrl"
```

How UPN changes affect the OneDrive URL and OneDrive features

Article • 04/04/2025

A User Principal Name (UPN) is made up of two parts, the prefix (user account name) and the suffix Domain Name System (DNS). For example:

user1@contoso.com

In this case, the prefix is "user1" and the suffix is "contoso.com."

You can change a user's UPN in the Microsoft 365 admin center by changing the user's username or by setting a different email alias as primary. You can also change a user's UPN in the Microsoft Entra admin center by changing their username. And you can change a UPN by using Microsoft PowerShell.

> **Note**
>
> A user's UPN (used for signing in) and email address can be different. If you just need to add a new email address for a user, you can add an alias without changing the UPN.

Types of UPN changes

You can change a UPN by changing the prefix, suffix, or both:

- Changing the prefix. For example, if a person's name changed, you might change their account name:

  user1@contoso.com to user2@contoso.com

- Changing the suffix. For example, If a person changed divisions, you might change their domain:

  user1@contoso.com to user1@contososuites.com

> **Important**
>
> UPN changes can take several hours to propagate through your environment.

OneDrive URL

A user's OneDrive URL is based on their UPN:

`https://contoso-my.sharepoint.com/personal/user1_contoso_com`

(where user1_contoso_com corresponds with user1@contoso.com)

> **Note**
>
> If the user's UPN contains an underscore, it's present in the resultant OneDrive URL.

In this case, if you changed the prefix to user2 and the suffix to contososuites.com, the user's OneDrive URL would change to:

`https://contoso-my.sharepoint.com/personal/user2_contososuites_com`

After you change a UPN, any saved links to the user's OneDrive (such as desktop shortcuts or browser favorites) will no longer work and will need to be updated.

Sync

The sync app (on both Windows and Mac) will automatically switch to sync with the new OneDrive location after a UPN change. While the UPN change is propagating through your environment, users might see an error in the OneDrive sync app that "One or more libraries couldn't be synced." If they select for more information, they see "You don't have permission to sync this library." Users who see this error should restart the sync app. The error goes away when the UPN change is fully propagated and the sync app is updated to use the user's new OneDrive URL.

> **Note**
>
> Synced team sites aren't impacted by the OneDrive URL change.

OneNote

After a UPN change, users will need to close and reopen their OneNote notebooks stored in OneDrive.

Close a notebook in OneNote for Windows

Open a notebook in OneNote for Windows

Microsoft Teams

After a UPN change, accessing the OneDrive app in Microsoft Teams can result in an error: 404 Files not found.

Until a fix is released, to resolve the error:

1. Create a 1:1 chat with another user.
2. In the message box, select **Actions and apps** > **Attach file** > **Upload from this device**.
3. Select a file you send to the other user, then select **Open**.
4. Press **Enter** to send the file or select **Send**.

After sending the file, navigate to the OneDrive app in Teams.

Recent files lists

After a UPN change, users will need to browse to reopen active OneDrive files in their new location. Any links to the files (including browser favorites, desktop shortcuts, and "Recent" lists in Office apps and Windows) no longer work.

Shared OneDrive files

If a user shared OneDrive files with others, the links will no longer work after a UPN change. The user needs to reshare the files.

Office Backstage View

After a UPN change, although Office will continue to work as expected, the user's original UPN will continue to be displayed in the Office Backstage View. To update the Office Backstage View to display the changed UPN, the user needs to sign out and then sign in using the Office client.

Search and Delve

After a UPN change, it might take a while for files at the new OneDrive URL to be indexed. During this time, search results in OneDrive and SharePoint will use the old URL. Users can copy the URL, paste it in the address bar, and then update the portion for the new UPN.

Delve will also link to old OneDrive URLs for a period of time after a UPN change. As activity occurs in the new location, the new links start appearing.

SharePoint automated workflows and customizations

Any automated workflows that were created with Power Automate or SharePoint 2013 workflows and refer to a OneDrive URL won't work after a UPN change. Similarly, any SharePoint apps (including Power Apps) that reference a OneDrive URL will need to be updated after a UPN change.

Recommendations

- If you're changing many UPNs within your organization, make the UPN changes in batches to manage the load on the system.
- If possible, apply changes before a weekend or during non-peak hours to allow time for the change to propagate and not interfere with your users' work.

See also

Info about UserPrincipalName attribute population in hybrid identity

Sync in SharePoint and OneDrive

Article • 05/29/2025

When users install the OneDrive sync app for Windows or Mac, and sync the files on a team site, they can work with the files in File Explorer or Finder. They can also easily save files to the team site from the programs they use.

If the user adds, changes, or deletes files and folders on the site, the changes also apply to the files and folders of the user's computer and vice versa.

To upload files to the team site, users can copy or move them to the site in File Explorer or Finder. They can also use File Explorer or Finder to easily organize the document library by creating new folders, and moving and renaming files and folders. All these changes sync automatically.

Windows 10 devices come with the OneDrive sync app installed. Office 2016 and later installations also have the sync app installed.

SharePoint file sync and OneDrive shortcuts

Users have two options when syncing files in SharePoint libraries and Teams. They can

- Add shortcuts to libraries and folders to their OneDrive.
- Use the Sync button in the document library.

Deciding between OneDrive sync options

Both OneDrive shortcuts and OneDrive Sync options allow essentially the same thing—users can access files on their local computer in Explorer or Finder.

However, adding OneDrive shortcuts allows content to be accessed on all devices, whereas sync is related to a specific device. Additionally, OneDrive shortcuts offer improved performance versus using the sync button.

We recommend using OneDrive shortcuts as the more versatile option.

Turn off OneDrive sync for SharePoint libraries

You can turn off OneDrive sync from all the SharePoint libraries in your organization with SharePoint Online Management Shell.

To turn off OneDrive sync from all the SharePoint libraries in your organization:

1. Download the latest SharePoint Online Management Shell.

> **Note**
>
> If you installed a previous version of the SharePoint Online Management Shell, go to Add or remove programs and uninstall "SharePoint Online Management Shell."

2. Connect to SharePoint as a SharePoint Administrator or above in Microsoft 365. To learn how, see Getting started with SharePoint Online Management Shell. by using this Set-SPOTenant PowerShell cmdlet to remove the OneDrive sync button:

3. Run the following cmdlets:

```PowerShell
Set-SPOTenant -HideSyncButtonOnTeamSite $true
```

Removing the sync button blocks new syncs from being started but doesn't affect existing syncs.

Related articles

Read the release notes and install the latest fully released versions.

Read about Invalid file names and file types in OneDrive and SharePoint.

Fix OneDrive sync problems

Network utilization planning for the OneDrive sync app

Article • 09/01/2024

This article is for IT admins planning to deploy the OneDrive sync app and wanting to estimate the network bandwidth users will need for syncing. If you're not an IT admin, follow the steps in this article to limit the network bandwidth used for syncing your files: Change the OneDrive sync app upload or download rate.

Estimate the network bandwidth you need in your organization

Follow these steps to estimate the bandwidth that will be used when you fully deploy the sync app.

1. Assess the number of users and computers per user to which you'll deploy the sync app. Each installation multiplies the bandwidth used, so a user who has three syncing computers uses three times the bandwidth as a user who has a single syncing computer.

2. Assess the available bandwidth and network conditions.

3. Measure the network utilization of the sync app for a pilot group.

When you deploy, Control sync throughput.

Assess the available bandwidth and network conditions

You can use third-party speed test tools, like Wireshark or Fiddler, to understand the actual download and upload throughput that the users experience.

Packet loss, latency, and other factors can also impact OneDrive upload and download experience. For example, a high-latency network or network experiencing loss could result in a degraded OneDrive upload and download experience even on high-bandwidth networks (1,000 Mbps, for example). The loss and latency will likely vary based on the number of users that are on the same network and what those users are doing (like downloading or uploading large files).

The bandwidth used by the sync app is predominantly file upload and download traffic and is closely correlated with file size and the number of files being synced. Therefore,

the bandwidth used depends on the number of files in the user's OneDrive and in SharePoint document libraries they choose to sync, multiplied by the size of files, and then by the rate of change of any file. Other sync app traffic (such as checking for file changes and checking for app updates) is minimal.

Measure the network utilization of the sync app for a pilot group

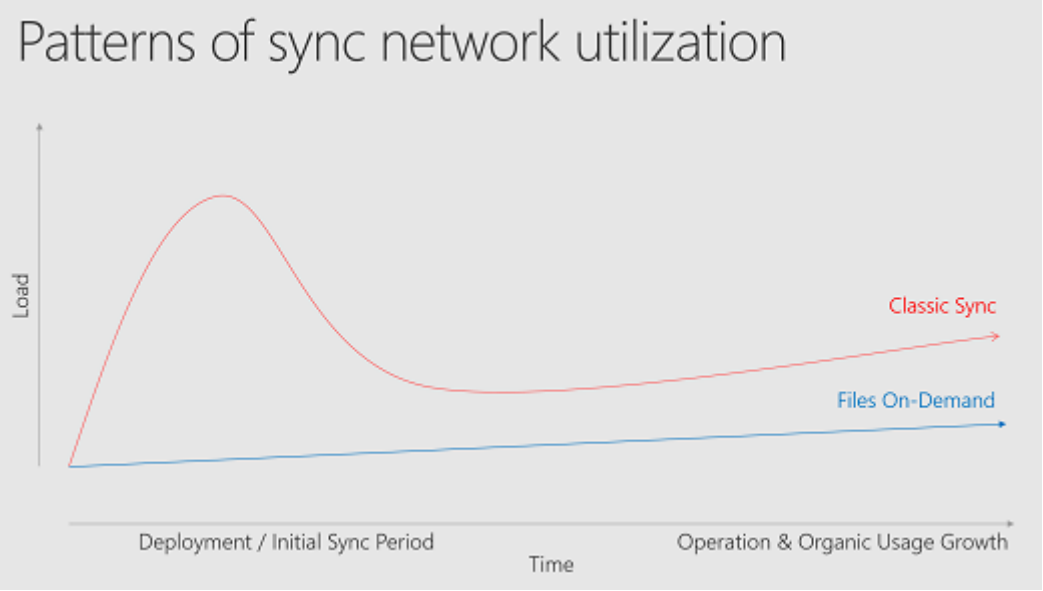
When you create a pilot group, make sure the users are representative of the different profiles of people in your organization and the different geographic locations. To establish a group:

- Estimate the number of files, typical file sizes, file types, total size of each library, how frequently files are modified, and how frequently new files are added.
- Evaluate network utilization during each sync state as described below.
- Use the measurements from the pilot group to extrapolate the entire organization's needs and re-test to validate the estimations. Each organization is different.

Initial deployment and initial sync of team sites

When users download locations for the first time, bandwidth usage will spike. To avoid this spike, enable Learn about OneDrive Files On-Demand. This allows users to browse their files in File Explorer without downloading them.

The following image illustrates the network utilization over time with Files On-Demand enabled and not enabled.



Operational sync

After the initial sync is complete, the network usage will decrease and then level out.

The OneDrive sync app provides differential sync for all file types stored in OneDrive and SharePoint. Differential sync enables the sync app to sync only the parts of large files that have changed, instead of the entire file. During everyday usage, when users change files, only the changes are uploaded or downloaded and not the whole file. This makes the file synchronization process faster for these files. It reduces the time it takes to upload and download the file and the bandwidth sync consumes.

> **Note**
>
> Windows Notification Service or WNS plays an important role in efficient network utilization. Instead of the sync app constantly pulling to check for remote changes, WNS ensures that any changes from the cloud get pushed down to the device as fast as possible. It saves both network bandwidth and device battery life. This benefits both Windows and macOS. Make sure the connection to the service is enabled. Work with your network team to make sure proxies allow network traffic to bypass *.wns.windows.com and avoid HTTPS decryption for *.wns.windows.com.

A spike in upload traffic is expected if you deploy the Known Folder Move setting in your organization. If your organization is large and your users have many files in their known folders, make sure you roll out the policies slowly to minimize the network impact of uploading files. For detailed deployment guidance on Known Folder Move, see Redirect and move Windows known folders to OneDrive.

Control sync throughput

If you need to control sync app traffic, we recommend using network throughput policies provided by the OneDrive sync app. You can also use your network quality of service (QoS) policies or Windows QoS policies, or let users choose their throughput settings. For info about the network settings you can make available to your users, see Change the OneDrive sync app upload or download rate.

Use OneDrive policies

You can use policies included with the OneDrive sync app to control network throughput. These policies are available in the OneDrive installation directory `%localappdata%\Microsoft\OneDrive\BuildNumber\adm\` where `BuildNumber` is the number displayed in sync app settings on the About tab.

For info about these policies, see:

- Enable automatic upload bandwidth management for OneDrive - Recommended for best user experience
- Limit the sync app upload speed to a fixed rate
- Limit the sync app download speed to a fixed rate
- Limit the sync app upload rate to a percentage of throughput

Prioritize traffic by using Windows Quality of Service (QoS) policy

To define the priority of outbound network traffic, you can configure a QoS policy with a specific differentiated services code point (DSCP) value. Network routers use the DSCP value to classify network packets and determine the appropriate queue. A higher value indicates a higher priority for the packet. The number of queues and their prioritization behavior needs to be designed as part of your organization's QoS strategy.

To manage the use of network bandwidth, you can configure a QoS policy with a specific throttle rate for outbound traffic. With throttling, a QoS policy limits the outgoing network traffic to a specified rate.

1. Open the Group Policy Management Console.
2. Browse to the location where you want to create the new policy. For example, if all your client computers are located in an OU (Organizational Unit) named "Clients" then the new policy should be created in the "Clients" OU.
3. Right-click the location, select **Create a GPO in this domain**, and then select **Link it here**.
4. In the **New GPO** dialog, enter a name for the new Group Policy object in the **Name** box (for example, "OneDrive sync app") and then select **OK**.
5. Right-click the policy, and then select **Edit**.
6. In the Group Policy Management Editor, expand **Computer Configuration**, expand **Policies**, expand **Windows Settings**, right-click **Policy-based QoS**, and then select **Create new policy**.
7. In the **Policy-based QoS** dialog, enter a name for the new policy in the **Name** box (for example, "OneDrive sync app").

8. Select **Specify DSCP Value** and set the appropriate value between 0 and 63 based on your organization's QoS strategy.

9. In the **Outbound Throttle Rate** box, enter a rate in KBps, and select **Next**.

10. Select **Only applications with this executable name** and to apply the QoS policy to only the OneDrive sync app process, enter "onedrive.exe". Select **Next**.

11. Make sure that both **Any source IP address** and **Any destination IP address** are selected, and then select **Next**. These two settings ensure that packets will be managed regardless of which computer (IP address) sent those packets and which computer (IP address) will receive those packets.

12. In the **Select the protocol this QoS policy applies to** list, select **TCP**. Leave **from any source port** and **to any destination** selected.

13. Select **Finish**.

See also

Network planning and performance tuning for Microsoft 365

Feedback

Was this page helpful? Yes No

Provide product feedback

Recommended sync app configuration

07/29/2025

For the best performance, reliability, and user experience, follow these "ideal state" recommendations when you configure the OneDrive sync app.

Updates and rings

- **Allow access to oneclient.sfx.ms and g.live.com**. Computers must be able to reach these URLs to apply updates and bug fixes, and enable or disable features. Updates are installed automatically; so, you don't need to package and deploy them. Because OneDrive runs in the background, updates are also installed silently and don't affect users.

- **Use the Insiders and Production rings**. Select several people in your IT department as early adopters to join the Insiders ring and receive features early. Leave everyone else in the organization on the default Production ring to ensure they receive bug fixes and new features in a timely fashion. This recommendation applies even if you are on the Semi-Annual Enterprise Channel for Windows and Office. For more information about the rings, see Sync app update process. To set the update ring on Windows, see Set the sync app update ring. To set it on Mac, see Deploy and configure the new OneDrive sync app for Mac.

Windows Notification Service

- **Make sure connection to the service is enabled**. Work with your network team to ensure proxies:

  - Allow network traffic to bypass *.wns.windows.com

  - Avoid HTTPS decryption for *.wns.windows.com

    This requirement applies to both Windows and Mac. See the complete list of required URL and IP address ranges.

Files On-Demand and Storage Sense

- **Keep Files On-Demand enabled**. OneDrive Files On-Demand helps users access all their files (individual or shared) without having to download them and use storage space. This setting is on by default for Windows 10 and Mac. To check this setting for Windows, see

Use OneDrive Files On-Demand. To check it for Mac, see Deploy and configure the new OneDrive sync app for Mac.

- **Use Storage Sense policies on PCs**. These policies let you automatically clean up "locally available" files users haven't explicitly pinned as "always available." For additional information, see More info about Storage policies.

Silent account configuration

- **Silently configure user accounts on PCs**. When you enable the silent account configuration policy, users are signed in automatically; so, they don't need to open OneDrive or enter their password. For more information, see Use silent account configuration.

Application start-up

- **Always start OneDrive automatically when signing in to Windows**. When you enable the autostart configuration policy, OneDrive will automatically start every time users sign in to Windows. For more information, see Start OneDrive automatically when signing in to Windows.

Known Folder Move

Windows users are familiar and comfortable with saving files to their desktop, documents, and pictures folders from years of developing it as a habit. When you redirect and move these folders to OneDrive, users can continue saving files to these locations, and they're backed up and available from any device. For more information, see Redirect known folders.

- **On new PCs, enable the silent policy**. Silently move Windows known folders to OneDrive
- **On existing PCs, gradually enable the prompt and/or silent policy**. About the Known Folder Move Group Policy objects

Office integration

- **Keep Office file collaboration enabled** Office uses differential sync to sync only changes instead of the entire file each time. This makes sync faster and reduces network bandwidth. For more information, see Coauthor and share in Office desktop apps. For information about this setting for Mac, see Deploy and configure the new OneDrive sync app for Mac.

> **Note**
>
> As of May 2025, the coauthoring and in-app sharing of Office files setting is enabled by default for all tenants. If this setting is disabled, Office file collaboration is turned off, and when file conflicts occur, both versions of the file are kept. If the setting isn't previously disabled by organizations, end users shouldn't experience any changes.

Offline mode

- **Keep offline mode enabled** With offline mode, users can work with OneDrive in the web in low or no internet situations. This setting is on by default on Windows and Mac. For more info, see Prevent users from getting silently signed in to offline experiences on the web, Prevent users at your organization from enabling offline mode in OneDrive on the web, and Prevent users at your organization from enabling offline mode in OneDrive on the web for libraries and folders that are shared from other organizations. For info about this setting for Mac, see DisableOfflineMode and DisableOfflineModeForExternalLibraries.

Shortcuts to shared folders

Users have two options when syncing files in SharePoint libraries and Teams. They can

- Add shortcuts to libraries and folders to their OneDrive.
- Use the Sync button in the document library.

It's recommended to use shortcuts instead of using the Sync button. Shortcuts are more performant because rather than syncing the entire library, only the specific folder is synced. Additionally, because the shortcuts are added to a user's OneDrive rather than to the device, it's easier to access content across all devices.

If you're an admin and want to hide the Sync button in document libraries, use the following PowerShell command:

```
Set-SPOTenant -HideSyncButtonOnTeamSite $true
```

Sync reports

The OneDrive sync reports in the Apps Admin Center provides you with sync health reports for tracking relevant health issues and advisories, checking the sync status and app version of individual devices, and monitoring Known Folder Move roll out. You must enable this setting on the devices from which you want to get reports. For more info, see Enable sync health

reporting for OneDrive. For info about this setting for Mac, see Deploy and configure the new OneDrive sync app for Mac.

Deploy OneDrive apps by using Intune

Article • 06/04/2024

As an Intune Administrator, you can use Intune to deploy OneDrive apps. Before you begin deploying, make sure you review the planning information and deployment options in the Plan file sync for SharePoint and OneDrive in Microsoft 365.

To deploy apps in Intune, you use the Microsoft Intune admin center.

Deploy the OneDrive sync app to Windows devices

OneDrive is preinstalled on Windows 10 and later. You can choose to switch to per-machine installation.

For info about configuring sync app settings using Intune, see Configure settings with Intune.

Deploy the OneDrive app to iOS devices

There are two options for deploying the OneDrive app on iOS:

- **Apple VPP.** Using this option and deploying with device licensing, the app is installed without user interaction. For more information, see How to manage iOS and macOS apps purchased through Apple Business Manager with Microsoft Intune.
- **iOS Store app.** Using this option doesn't require any connection to Apple Business Manager, however users will be prompted to enter their Apple ID password to install the app. For more information, see Add iOS store apps to Microsoft Intune.

Deploy the OneDrive app to Android devices

There are two options for deploying the OneDrive app on Android:

- Add Managed Google Play apps to Android Enterprise devices with Intune
- Add Android store apps to Microsoft Intune.
  - Use **https://play.google.com/store/apps/details?id=com.microsoft.skydrive** as the Appstore URL.

Deploy the OneDrive app to macOS devices

There are two options for deploying the OneDrive app using Intune:

- **Microsoft 365 Apps.** You can deploy Microsoft 365 apps including OneDrive with Intune. For more information, see Assign Microsoft 365 to macOS devices with Microsoft Intune.
- **Deploy a standalone PKG**

    1. Download the app package (.pkg)
    2. Deploy using Add an unmanaged macOS PKG app to Microsoft Intune

For more information about OneDrive on macOS, see Deploy and Configure OneDrive on macOS.

See also

For information about assigning apps to groups, see Assign apps to groups with Microsoft Intune.

Feedback

Was this page helpful? Yes No

Provide product feedback

Deploy OneDrive apps using Microsoft Endpoint Configuration Manager

Article • 04/10/2025

You can use Microsoft Endpoint Configuration Manager to deploy the new OneDrive sync app (OneDrive.exe), and the mobile apps for iOS and Android. Before you begin deploying, make sure you have reviewed the planning information and deployment options in the Plan file sync for SharePoint and OneDrive in Microsoft 365.
https://learn-video.azurefd.net/vod/player?id=502d1d70-de8b-4180-adc6-5786a518e0e7&locale=en-us&embedUrl=%2FSharePoint%2Fdeploy-on-windows

Deploy the OneDrive sync app for Windows

The OneDrive sync app (OneDrive.exe) can be installed on Windows 7 and later. It can also be installed on macOS. For info about deploying the OneDrive sync app on macOS, see Configure the new OneDrive sync app on macOS.

The new OneDrive sync app can be used with SharePoint Server 2019, but not earlier versions of SharePoint Server. For more information about the restrictions and limitations of the OneDrive sync app, see Invalid file names and file types in OneDrive and SharePoint.

OneDrive is installed per user by default. You can also install it per machine. For more information, see Learn about installing OneDrive per machine.

Make sure that WNS is set up correctly

The OneDrive sync app uses Windows Push Notification Services (WNS) for optimum performance and battery life. Make sure you allow access from your network to the endpoints that OneDrive uses. To see all our recommendations for configuring the sync app, see Recommended sync app configuration.

Check if users already have the OneDrive sync app

If the computers in your organization are running Windows 10, they already have the new sync app installed. If the computers have Office 2016 or Office 2013 (Home & Student, Home & Business, Professional, Personal, Home, or University) installed, they might also have the new sync app.

Deploy any administrative settings

To set registry keys on computers in your domain, install OneDrive and copy the OneDrive.admx and OneDrive.adml files from %localappdata%\Microsoft\OneDrive\BuildNumber\adm\ to your Group Policy central store. For more info, see Use OneDrive policies to control OneDrive sync app settings.

Use Microsoft Endpoint Configuration Manager to deploy the OneDrive sync app

1. In Configuration Manager, select **Create Device Collection**, and follow the steps in the Create Device Collection wizard.

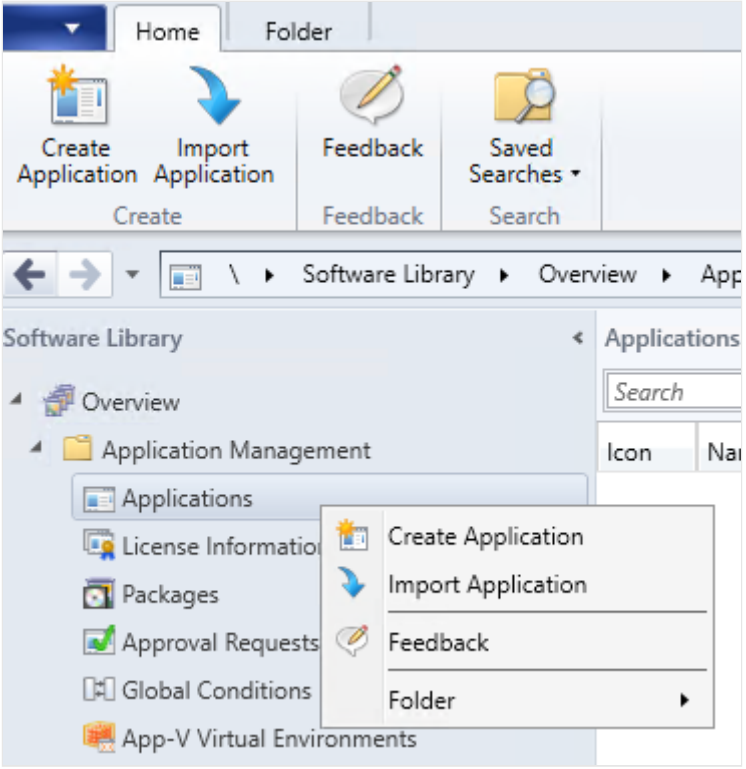
2. Save the OneDriveSetup.exe installer for Windows to your local computer or a network share. Download the Production ring OneDriveSetup.exe installer for Windows or download the Deferred ring OneDriveSetup.exe installer for Windows.

3. Download the sample Configuration Manager package. It's a .zip file that contains the script installer deployment type. For more information about packages and programs in Configuration Manager, see Packages and programs in Configuration Manager.

   > **Note**
   >
   > The script installer deployment type already has a detection method script and will correctly assess the installation. Also, there is an uninstall switch, which means that you can easily remove the OneDrive sync app, if necessary.

4. Copy the installer to a folder in the Configuration Manager source content share.

5. In Configuration Manager, select the **Software Library** workspace. Under **Application Management**, right-click **Applications**, and then select **Import Application**.



6. Select the sample package.

7. On the bottom of Configuration Manager, select the **Deployment Types** tab, right-click the deployment, and to update the **Content location**, edit the properties.

8. Right-click the package, select **Deploy**, and follow the steps in the Deploy Software Wizard.

If you don't use the sample package, run the following command using Microsoft Endpoint Configuration Manager:

```
Execute <pathToExecutable>\OneDriveSetup.exe /silent
```

(where pathToExecutable is a location on the local computer or an accessible network share).

> **Note**
>
> This command must be run at user logon and using Administrator permissions. It must be run for each user on a machine. For an example of how to deploy an .exe on every user account, see How to deploy the OneDrive sync app with Configuration Manager.
>
> If you run the command with no command-line parameter, users will see the installation status. After installation, OneDriveSetup.exe will automatically execute OneDrive.exe and display OneDrive Setup to users. If you run the command with the **/silent** parameter, OneDrive.exe will be installed transparently and OneDrive Setup won't appear. You'll need

to run OneDrive.exe with an additional command. If you want to control the launch of OneDrive across your organization, we recommend using the **/silent** parameter.

Learn more about application management in Configuration Manager. The installer will install the OneDrive executable file under **%localappdata%\Microsoft\OneDrive**.

Help users sign in

To help users sign in, you can use silent account configuration or one of these methods:

- Use the following URL to start OneDrive Setup on users' computers. When users select to begin Setup, a sign-in window appears for users can enter email address.

  `odopen://launch`

- Use the following URL with each user's email address to start Setup and prepopulate user email addresses in the sign-in window.

  `odopen://sync?useremail=youruseremail@organization.com`

- Run the following command using Configuration Manager script:

  `%localappdata%\Microsoft\OneDrive\OneDrive.exe`

  It starts the OneDrive process. If users haven't set up any accounts, it displays OneDrive Setup. To display OneDrive Setup specifically to users who haven't set up an account for your organization, use the command-line parameter:

  `/configure_business:<tenantId>`

> **Note**
>
> When you use Microsoft Endpoint Configuration Manager, make sure you run OneDrive.exe with User permissions (not as an Administrator).
> For help finding your tenant ID, see Find your Microsoft 365 tenant ID.

Autoconfigure SharePoint site synchronization

If you want to autoconfigure a SharePoint site to be synced, you can use the URL below as a guide to build the path to the SharePoint site you want to sync automatically. You can also use a policy to sync sites automatically. For info, see Configure team site libraries to sync automatically.

`odopen://sync/?siteId=<siteId>&webId=<webId>&webUrl=<webURL>&listId=<listId>&userEmail=<userEmail>&webTitle=<webTitle>&listTitle=<listTitle>`

where:

- **<siteId>** is the SharePoint site siteId GUID, enclosed in curly brackets. You can get this GUID visiting https://<TenantName>.sharepoint.com/sites/<SiteName>/_api/site/id.
- **<webId>** is the SharePoint site webId GUID, enclosed in curly brackets. You can get this GUID visiting https://<TenantName>.sharepoint.com/sites/<SiteName>/_api/web/id.
- **<webUrl>** is the SharePoint site URL. You can get this URL visiting https://<TenantName>.sharepoint.com/sites/<SiteName>/_api/web/url.
- **<listId>** is the SharePoint site documents library GUID, enclosed in curly brackets. You can get this GUID visiting the document library in the browser, select in the gear icon and choosing "Library Settings". The URL shows the listId GUID at the end of URL, i.e. https://<tenant>.sharepoint.com/sites/<SiteName>/_layouts/15/listedit.aspx?List=%7B**xxxxxxxx-xxxx-xxxx-xxxx-xxxxxxxxxxxx**%7D (a GUID with escaped curly brackets).
- **<userEmail>** is the OneDrive's user email address used to sign in into OneDrive.
- **<webTitle>** and **<listTitle>** are used to compose the name of the local folder where the OneDrive content is synchronized. By default, when you use the "Sync" button when in the browser to synchronize a document library, OneDrive uses the SharePoint site name and the document library name to compose the local folder name, in the form of %userprofile%\<TenantName>\<SiteName> - <DocumentLibraryName>. You could use any other values if you prefer to. If you don't use these parameters, the local folder is named "<TenantName> - Documents", despite of site and library names.

For example, if you want to synchronize `https://contoso.sharepoint.com/sites/SalesTeam-01/ProjectX`, where "ProjectX" is the documents library to synchronize, to "%userprofile%\Contoso\Sales - Unicorn" folder, you need the following parameters to compose the odopen:// URL:

- siteId: {ssssssss-ssss-ssss-ssss-sssssssssssss}
- webId: {wwwwwwww-wwww-wwww-wwww-wwwwwwwwwwww}
- webUrl: `https://contoso.sharepoint.com/sites/SalesTeam-01`
- listId: {llllllll-llll-llll-llll-lllllllllllll}
- userEmail: user@contoso.com
- webTitle: Sales (you would use *SalesTeam-01* to mimic Sync button behavior instead)
- listTitle: Unicorn (you would use *ProjectX* to mimic Sync button behavior instead)

The resulting odopen:// URL is:

```
odopen://sync/?siteId={ssssssss-ssss-ssss-ssss-sssssssssssss}&webId={wwwwwwwww-wwww-wwww-wwww-wwwwwwwwwwwww}&webUrl=https://contoso.sharepoint.com/sites/SalesTeam-01&listId={llllllll-llll-llll-llll-lllllllllllll}&userEmail=user@contoso.com&webTitle=Sales&listTitle=Unicorn
```

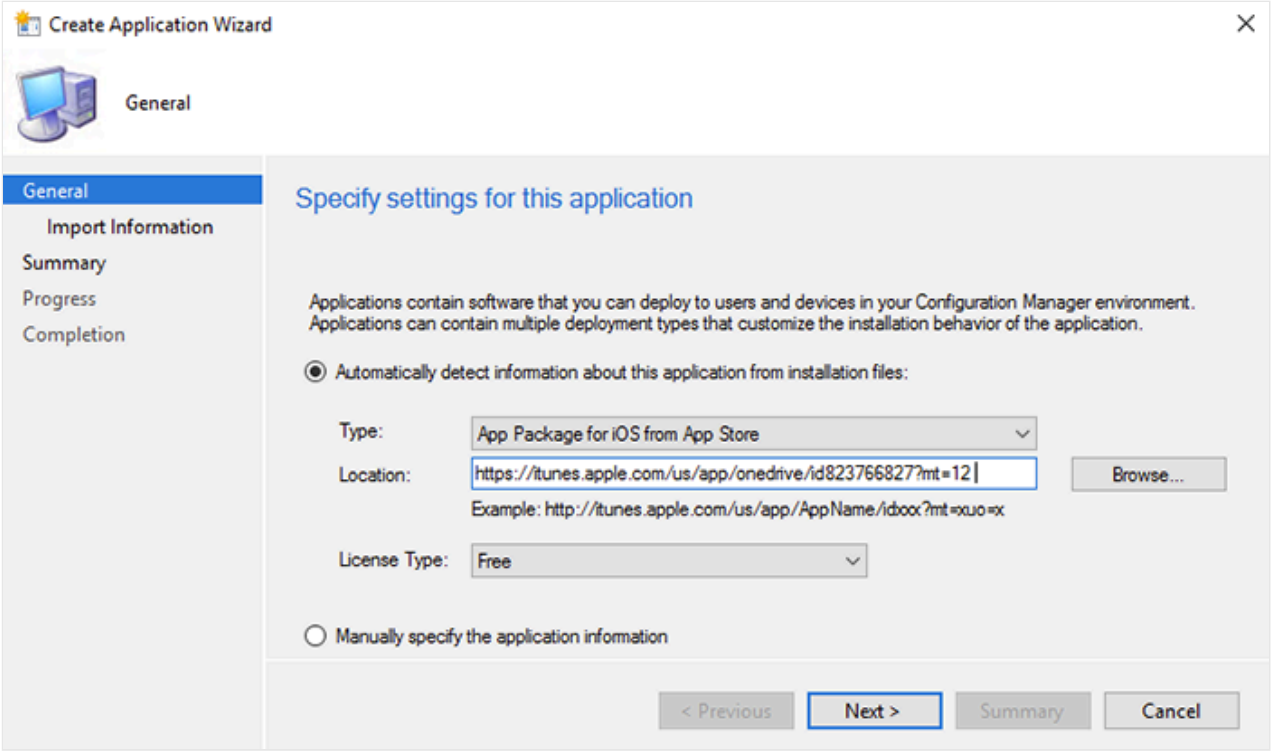
> **Note**
>
> You will need Client Side Object Model (CSOM) knowledge if you want to automate querying the team site to determine the appropriate siteId, webId, and listId to build the appropriate URL.

Deploy the OneDrive app on mobile devices running iOS or Android

You can use Microsoft Endpoint Configuration Manager to deploy apps to mobile devices. Before you do, however, you need to complete a few prerequisite steps because integration with Intune is required to manage mobile devices in Configuration Manager. For information about managing mobile devices with Configuration Manager and Intune, see Manage Mobile Devices with Configuration Manager and Microsoft Intune.

Deploy the OneDrive app for iOS

1. In Configuration Manager, on the Home ribbon, select **Create Application**.
2. In the **Type** box, select **App Package for iOS from App Store**.
3. In the **Location** box, enter the app store URL, https://itunes.apple.com/us/app/onedrive/id823766827?mt=12 .



4. Target the app to users.

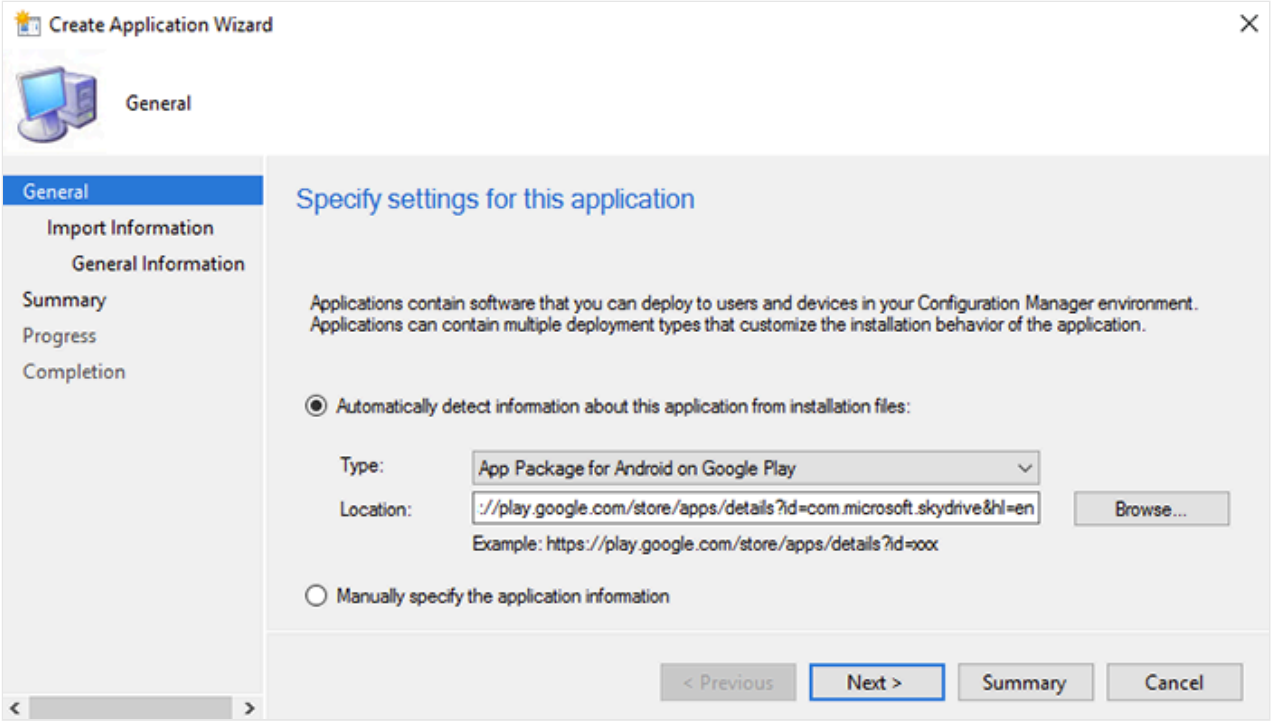
For more info, see Create iOS applications with Configuration Manager, and use as the app location, as shown below.

Deploy the OneDrive app for Android

1. In Configuration Manager, on the Home ribbon, select **Create Application**.

2. In the **Type** box, select **App Package for Android on Google Play**.

3. In the **Location** box, enter the app store URL, https://play.google.com/store/apps/details?id=com.microsoft.skydrive&hl=en .



4. Target the app to users.

For more info, see Create Android applications with Configuration Manager.

See also

Invalid file names and file types in OneDrive and SharePoint

Install the sync app per-machine

Article • 11/05/2024

By default, the OneDrive sync app installs per-user, meaning that you need to install the app for each user on a machine. With the per-machine installation option, you need to install the app once on a PC. This option is especially useful for computers with multiple users and for when you don't want executable files running from a user profile.

Other than where the sync app is installed, the behavior is the same.

Updates

The OneDrive sync app with the installation option of either per-machine or per-user both use the same release notes, support the same update rings, and update in the same time-frame. More info about the sync app update process.

If you're moving from per-user to per-machine, update settings aren't affected.

Requirements

The per-machine installation's system requirements are the same as the per-user installation.

The per-machine installation option supports syncing OneDrive and SharePoint files in Microsoft 365 and in SharePoint Server 2019.

The per-machine installation option provides automatic transitioning from the previous OneDrive sync app (Groove.exe).

Deployment instructions

1. Download OneDriveSetup.exe.
2. Run "OneDriveSetup.exe /allusers" from a command prompt window (which results in a User Account Control prompt) or by using Microsoft Endpoint Configuration Manager.

- The per-user option installs OneDrive for each user account on a PC under the %localappdata% folder.
- The per-machine option installs OneDrive under the "Program Files (x86)" or "Program Files" directory (depending on the OS architecture).

When setup completes, OneDrive starts. If accounts were added on the computer, they're migrated automatically.

Verify per-machine installation

To verify that you have the per-machine installation, you can use the following registry detection rule in Configuration Manager:

Expand table

Field	Value
Hive	HKEY_LOCAL_MACHINE
Key	SOFTWARE\Microsoft\OneDrive
Name	Version
32-bit on 64-bit	TRUE
Type	REG_SZ
Value	19.043.0304.0007

Revert back to the per-user sync app

We don't support automated migration from per-machine to per-user. To revert back after installing per-machine, uninstall the sync app and install the latest released version without the "/allusers" parameter.

Feedback

Was this page helpful? Yes No

Provide product feedback

Use the sync app on virtual desktops

For all supported operating systems, the OneDrive sync app supports:

- Virtual desktops that persist between sessions.
- Non-persistent virtual desktops that use Azure Virtual Desktop.
- Non-persistent virtual desktops that have FSLogix Apps or FSLogix Office Container, and a Microsoft 365 subscription for all of the following operating systems:
  - Windows 10 and 11, 32-bit or 64-bit (supports VMDK/Virtual Machine Disk files)
  - Windows Server 2022 or newer (supports VHDX/Virtual Hard Disk)

> **Note**
>
> Check the latest versions at these links: OneDrive, FSLogix App Using the OneDrive sync app with non-persistent environments requires that you install the sync app per machine. For Windows Server, the SMB network file sharing protocol is also required. The OneDrive sync app is supported in a remote app scenario hosted as a Citrix Virtual App. The OneDrive sync app with FSLogix doesn't support running multiple instances of the same container simultaneously.

Set up OneDrive in Citrix Virtual Apps

This section describes how to enable and use OneDrive in Citrix Virtual Apps.

Prerequisites

To enable OneDrive in Citrix Virtual Apps, you must have the following versions of Windows and Citrix Virtual Apps and Desktops (CVAD):

Windows:

- Windows 11: KB5014019
- Windows Server 2022: KB5014021
- Windows 10: KB5014023
- Windows Server 2019: KB5014022

Citrix:

- CVAD 7 2203 LTSR/Long Term Service Release CU1 or later.
- VDA/Virtual Delivery Agent 2212 enables Shellbridge by default. All earlier versions require Shellbridge to be enabled manually.
- To enable this feature, On 2203 LTSR TS VDA (2019 Server, 2022 Server, Windows 10 RDSH/Remote Desktop Session Host, or Windows 11 RDSH/Remote Desktop Service Host) add the following registry details:
  - `HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\Citrix Virtual Desktop Agent`
  - `Name: Shellbridge`
  - `Type: REG_DWORD`
  - `Value: 1`

To ensure that the feature is correctly enabled, open a command window (cmd.exe) and run `start ms-settings:printers`. If the feature is enabled, the printer setting window is displayed.

We recommend adding OneDrive.exe to `LogoffCheckSysModules`.

- `HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Citrix\wfshell\TWI`
- `Value Name:LogoffCheckSysModules`
- `Type:REG_SZ`
- `String:OneDrive.exe, Microsoft.Sharepoint.exe`

> **Important**
>
> FSLogix must be used in conjunction with Citrix Virtual Apps for OneDrive to be supported.

How to set up OneDrive

1. Install OneDrive Sync app per machine. See Install the sync app per-machine.
2. Install the latest version of FSLogix. See Install FSLogix Applications.

   > **Note**
   >
   > All non-persistent VDI environments require the latest version of FSLogix. Ensure you install the latest version. See OneDrive sync error FSLogix_unsupported_environment on VMs.

3. Add OneDrive to `HKLM\Software\Microsoft\Windows\CurrentVersion\` by using the following command:

```
REG ADD HKLM\Software\Microsoft\Windows\CurrentVersion\Run /v OneDrive /t REG_SZ /d "\"C:\Program Files\Microsoft OneDrive\OneDrive.exe\" /background"
```

4. Silently configure user accounts. See Silently configure user accounts.

> **Note**
>
> Silent sign-in should work if your machine is connected to Microsoft Entra ID. Make sure to turn off this setting if your computer isn't Microsoft Entra joined.

Set up OneDrive in Omnissa Horizon Virtual Apps

This section describes how to enable and use OneDrive in Omnissa Horizon Virtual Apps.

Prerequisites

- Omnissa Horizon
- Windows
  - Windows 10 and Windows 11 Guest Operating Systems for Horizon Agent and Remote Experience, for Omnissa Horizon 8.x (2006 and later) (78714). For more information, see this article.
  - Non-Windows 10 and 11 Guest Operating Systems for Horizon 8 Agent (78715). For more information, see this article.
- FSLogix
- Omnissa Dynamic Environment Manager (DEM) or a product which enables user environment personalization. The system on which you plan to install DEM must meet certain software requirements. For more information, see this article.

Registry Keys

The following registry keys help to roam the user environment on multiple nodes in the virtual application farm. Omnissa Dynamic Environment Manager or a similar user environment management tool can be used to deploy the registry keys to all farm servers.

- [IncludeRegistryTrees]
  - `HKCU\Software\Microsoft\Office`
  - `HKCU\Software\Microsoft\Internet Explorer`
  - `HKCU\Software\Microsoft\Windows\CurrentVersion\Internet Settings`
  - `HKCU\Software\Microsoft\Windows\CurrentVersion\Shell Extensions\Cached`
  - `HKCU\Software\Microsoft\OneDrive`
- [IncludeFolderTrees]
  - `<Appdata>\Microsoft\Windows\Recent`
  - `<Appdata>\Microsoft\crypto`
  - `<Appdata>\SystemCertificates`
  - `<LocalAppdata>\Microsoft\IdentityCache`
  - `<LocalAppdata>\Microsoft\Internet Explorer`
  - `<LocalAppdata>\Microsoft\Windows\INetCache`

Configure Omnissa Dynamic Environment Manager with Horizon Apps

1. Launch the Omnissa Dynamic Environment Manager management console, select **Create Config File**, and select **Use an Application Template**.
2. Select the application template (Microsoft Office 2016 and 2019, or Microsoft 365), select **OneDrive for Business**, and click **Next**.
3. Provide the file name and description and select **Finish**.
4. Add the previously listed **required registry keys** to **Import / Export** settings.

Configure FSLogix with Omnissa Dynamic Environment Manager

Configuring FSLogix in combination with Dynamic Environment Manager will help with store OneDrive cache and the save location for Microsoft and non-Microsoft applications.

For more info on how to configure FSLogix Office Container (ODFC) on all Horizon Virtual App farm servers, refer to this article.

- Install the per-machine version of the OneDrive sync app on all the Horizon Virtual App farm hosts.
- Create the following entries in each Horizon farm servers. You can use DEM or similar user environment management tool to deploy the registry to all virtual app farm servers.
  - Key: `HKLM\Software\Microsoft\Windows\CurrentVersion\Run`
  - Type: `REG_SZ`
  - Name: `OneDrive`
  - Data: `"C:\Program Files\Microsoft OneDrive\OneDrive.exe"/background`
  - Key: `HKLM\Software\Policies\Microsoft\OneDrive`
  - Type: `REG_DWORD`
  - Name: `SilentAccountconfig`
  - Data: `1`

> **Note**
>
> Sometimes the silent login will take several seconds. If the first attempt fails, a second attempt might be required.

See also

Learn more about VHDX/Virtual Hard Disk and VHD/Virtual Hard Disk.

For info about creating virtual hard disks, see Manage virtual hard disks.

Last updated on 10/08/2026

The OneDrive sync app update process

This article is for IT admins who manage the OneDrive sync app (OneDrive.exe) in an enterprise environment. It explains how we release updates to the sync app for Windows and the standalone sync app for Mac through rings of validation, and how the app checks for updates. If you deploy the sync app alongside Office (via the Office Deployment Tool or some other means), it continues to check for updates independent of any Office update restrictions you set.

> **Note**
>
> If you allow your users to sync personal OneDrive accounts, the update process described in this article and any settings you select apply to all instances of the sync app.
>
> The sync app installed from the Mac App Store follows a separate update process. After we finish rolling out updates within the Production ring, we publish them to the Mac App Store, where they're immediately released to everyone.

How we release updates through multiple rings

After we validate updates through rings within Microsoft, we release them to the first public ring, Insiders. To try these latest features, join the Windows Insider program or the Office Insider program. It takes about three days to roll out to this ring. Later, we release to organizations in the default update ring, Production. We roll them out to a small percentage of users in the ring at first, and slowly roll them out to everyone in the ring. This process typically takes one to two weeks. At each increase along the way, we monitor telemetry for quality assurance purposes. In the rare case when we detect an issue, we suspend the release, address the issue, and release a new update to users in the same order. After updates roll out completely within the Production ring, and remain in Production for at least 60 days, we release them to the next ring, Deferred.

Expand table

Insiders	>	Production	>	Deferred
1-2 times per week	>	Every 1-2 weeks	>	Every 2-3 months

> **Important**

We recommend selecting several people in your IT department as early adopters to join the Insiders ring and receive features early. We recommend leaving everyone else in the organization in the default Production ring to ensure they receive bug fixes and new features in a timely fashion. **See all our recommendations for configuring the sync app**

The Deferred ring provides builds that were monitored throughout the Production rollout, so fewer releases are suspended. The Deferred ring also lets you as an admin:

- Control when you deploy updates (within 60 days of their release).
- Deploy new versions from an internal network location to avoid using Internet bandwidth. (If you don't deploy an update after 60 days, it will be automatically downloaded and installed.)

However, as the slowest ring, the Deferred ring receives performance improvements, reliability fixes, and new features last.

> **Note**
>
> Microsoft reserves the right to bypass the 60-day grace period for critical updates.

- To learn how to set the Deferred ring for the Windows sync app using Group Policy, see Set the sync app update ring.
- To learn how to set it for the Mac sync app, see Configure the new OneDrive sync app on macOS.
- For info about the Microsoft 365 update process, see Overview of update channels for Microsoft 365 Apps for enterprise.

How the sync app checks for and applies updates

The OneDrive sync app checks for available updates every 24 hours when it's running. If it stops and doesn't check for updates in more than 24 hours, the sync app checks for updates as soon as it starts. Windows also has a scheduled task that updates the sync app even when it's not running.

To determine if an update is available, the OneDrive sync app checks if:

- The latest version released to the update ring is higher than what is installed on the computer. If the installed version is too old to be updated to the current version, the sync app first updates to the minimum version within the ring.
- The update is available to the computer based on the rollout percentage we set within the ring.

If both of these conditions are true, OneDrive downloads the update to a hidden folder without any user interaction. After the download is complete, OneDrive verifies and installs it. If OneDrive is running, it stops and then restarts. Users don't need to sign in again, and they don't need administrative rights to install the update.

For info about the latest releases, see New OneDrive sync app release notes.

> **Note**
>
> To apply sync app updates, computers in your organization must be able to reach the following: "oneclient.sfx.ms" and "g.live.com." Make sure you don't block these URLs. They're also used to enable and disable features and apply bug fixes. See **More info about the URLs and IP address ranges used in Microsoft 365**.

Deploying updates in the Deferred ring

At any given time, the next planned Deferred ring release publishes on the OneDrive sync app release notes page with a link to the corresponding installer and the version's targeted release date. On the specified date, the "Rolling out" version for the Deferred ring becomes the new minimum. All sync apps below that version automatically download the installer from the Internet and update themselves.

To deploy an updated version of the sync app for Windows, run the following command using Microsoft Endpoint Configuration Manager:

```
Execute <pathToExecutable>\OneDriveSetup.exe /update /restart
```

Where pathToExecutable is a location on the local computer or an accessible network share and OneDriveSetup.exe is the target version downloaded from the release notes page. Running this command restarts OneDrive.exe on all computers. If you don't want to restart the sync app,

remove the /restart parameter. See Deploy using Microsoft Endpoint Configuration Manager for tips on how to set up the Microsoft Endpoint Configuration Manager deployment package.

To deploy an updated version of the sync app for Mac, deploy the OneDrive.pkg with the target version by using your MDM solution.

Last updated on 07/27/2026

Transition from the previous OneDrive for Business sync app

Article • 09/18/2024

> **Important**
>
> Support for the previous OneDrive sync app (Groove.exe) ended on January 11, 2021. As of February 1, 2021, users can no longer sync OneDrive or SharePoint files in Microsoft 365 by using Groove.exe. Groove.exe will continue to work only for files in SharePoint Server.

This article is for global and SharePoint admins who want to transition their users off of the previous OneDrive sync app (Groove.exe) so that they sync with only the new OneDrive sync app (OneDrive.exe).

If you're not an IT admin, to learn how to begin syncing files using the new OneDrive sync app, see Sync files with the new OneDrive sync app in Windows .

> **Note**
>
> If your organization never used the previous OneDrive sync app, or had fewer than 250 licensed Office 365 users in June 2016, your users are already using the new OneDrive sync app to sync files in OneDrive and SharePoint.

Syncing files with OneDrive sync app to OneDrive sync app

When users who are syncing files with the previous OneDrive sync app (Groove.exe) sign in to the new OneDrive sync app (OneDrive.exe), the following things happen:

- If the new OneDrive sync app can take over syncing a library, the previous sync app stops syncing it,, and the new OneDrive sync app takes over syncing it without redownloading the content. If the new OneDrive sync app can't sync the library, the previous sync app continues to sync it. If a library requires checkout or has required columns or metadata, it's synced read-only.
- The previous sync app stops running and removes itself from automatic startup, unless it's still syncing libraries that the new OneDrive sync app can't sync.

When SharePoint libraries begin syncing with the new OneDrive sync app, the folder hierarchy that appears in File Explorer may be simplified.

Limits

The following library types aren't yet supported by the new OneDrive sync app, and won't transition from the previous sync app:

- On-premises locations in SharePoint Server 2016 or earlier. Learn about using the OneDrive sync app with SharePoint Server 2019
- SharePoint libraries that people from other organizations shared that your users are syncing with the previous sync app.

For more info about sync restrictions and limitations, see Invalid file names and file types in OneDrive and SharePoint

Requirements

To transition users off of the previous sync app, first make sure users have:

- Windows 10, Windows 8.1, Windows 8, or Windows 7.
- A current version of the new OneDrive sync app installed. For info about deploying the new OneDrive sync app, see Deploy OneDrive apps using Microsoft Endpoint Configuration Manager. OneDrive.exe must be deployed and configured before you try the takeover command. Download the latest version of the new OneDrive sync app that's fully released to production. To learn about the versions that are rolling out to different rings, see New OneDrive sync app release notes.
- The following versions of Office or higher installed. For info about deploying Office, see Choose how to deploy Microsoft 365 Apps for enterprise. Make sure you don't install the previous OneDrive sync app. For info, see Changes to OneDrive sync app deployment in Office Click-to-Run.

Expand table

Office version	Minimum version
Microsoft 365 Apps for enterprise	16.0.7167.2*
Office 2016 MSI	16.0.4432.1*
Office 2013 MSI/C2R	15.0.4859.1*

> **Note**
>
> If any users have Office 2010 installed, we strongly recommend removing the SharePoint Workspace component. If users previously set up SharePoint Workspace (even if they're no longer using it), it will cause problems syncing team sites. Before starting OneDrive Setup, either Uninstall Office from a PC or modify the installation. To do this by running Setup, first create the following XML file:
>
> XML
>
> ```xml
> <?xml version="1.0" encoding="UTF-8"?>
> <Configuration Product="ProPlus">
>  <Display Level="none" CompletionNotice="no" SuppressModal="yes" NoCancel="yes" AcceptEula="yes" />
>  <Logging Type="standard" Path="C:\Windows\temp\" Template="MicrosoftSharePointWorkspaceSetup(*).txt" />
>  <Setting Id="SETUP_REBOOT" Value="Never" />
>  <OptionState Id="GrooveFiles" State="absent" Children="force" />
> </Configuration>
> ```
>
> Then run Setup:
>
> Console
>
> ```
> Setup.exe /modify ProPlus /config RemoveSharepointDesigner.xml
> ```
>
> For more info, see Setup command-line options for Office 2010 and Config.xml file in Office 2010.

- The latest Rights Management Service (RMS) client if you want users to be able to sync IRM-protected SharePoint document libraries and OneDrive locations.

Configure takeover

When the required software is installed on your users' computers, you can configure automatic takeover of syncing silently (review the prerequisites and steps), and then use this policy.

After you install and configure OneDrive.exe, Groove.exe should no longer be able to sync. If the takeover didn't succeed, or your users are stuck in a hybrid state (some content syncing with OneDrive.exe and some with Groove.exe), try running: `%localappdata%\Microsoft\OneDrive\OneDrive.exe /takeover`.

> **Tip**
>
> Make sure to run the command in a user context, rather than as admin, or the error "OneDrive.exe cannot be run with Admin privileges" appears.
> To affect all users on the computer, configure the command to run on every user account so it will run for any user who signs in.

If the takeover didn't succeed, the previous OneDrive sync app (Groove.exe) may be an older version that can't successfully transition to the new client. To patch the previous sync app, update groove-x in Office 2016 or Office 2013, and then try again.

See also

To help your users get started with the OneDrive sync app, you can refer them to the following articles:

- Sync files with the new OneDrive sync app in Windows
- Get started with the new OneDrive sync app for Mac
- Sync SharePoint files with the new OneDrive sync app

Feedback

Was this page helpful? Yes No

Provide product feedback

Control Groove.exe installation when deploying Office using Click-to-Run

Article • 09/19/2024

> **Important**
>
> Support for the previous OneDrive for Business sync app (Groove.exe) ended on January 11, 2021. As of February 1, 2021, users can longer sync OneDrive or SharePoint files in Microsoft 365 by using Groove.exe. Groove.exe will continue to work only for files in SharePoint Server.

Starting in October 2017, we changed how the previous OneDrive for Business sync app installs for enterprise customers who deploy Office 2013 or 2016 by using Click-to-Run.

- The previous sync app (Groove.exe) is no longer installed by default with Office 2016 Click-to-Run. If your organization provides an Office deployment configuration file to Setup.exe, you need to update your file to exclude Groove.exe from the install.
- When not in use or running, the previous sync app (Groove.exe) is uninstalled, unless: (a) Groove.exe is already configured to sync one or more SharePoint or SharePoint Server libraries or (b) a "PreventUninstall" registry key is present on the computer.

These changes don't affect your organization if you're already using the new OneDrive sync app (OneDrive.exe) to sync OneDrive and SharePoint files. These changes also don't affect your organization if you deploy Office using the traditional Windows Installer-based (MSI) method.

> **Note**
>
> The new OneDrive sync app (OneDrive.exe) is the recommended option for SharePoint Server 2019 customers. However, the previous sync app (Groove.exe) is still used and supported for earlier versions of SharePoint Server. Which version of OneDrive am I using?

Ensure Groove.exe is no longer installed

If your organization provides an Office deployment configuration file to Setup.exe, add this to your config file to exclude Groove in your deployment:

```
<Product ID="O365ProPlusRetail" > <Language ID="en-us" /> <ExcludeApp ID="Groove" /> </Product>
```

For more info about configuration options, see Configuration options for the Office Deployment Tool.

To override the default behavior and make sure the previous OneDrive for Business sync app installs and stays installed, you must provide a config file that doesn't exclude Groove.exe. Also, you must set the "PreventUninstall" registry key on all computers where you need Groove.exe installed, so that the process doesn't uninstall Groove.exe.

Uninstall Groove.exe when not in use

On Office upgrade, the installer runs on each computer to detect whether Groove.exe is currently in use or the "PreventUninstall" registry key is set. If either Groove.exe is in use or the registry key is set, Groove.exe is left in place. Otherwise, if Groove.exe isn't in use and the registry key isn't set, Groove.exe gets uninstalled automatically on that computer.

Prevent uninstallation (registry key)

[HKLM\SOFTWARE\Microsoft\Office\Groove] "PreventUninstall"=dword:00000001

Timeline

The following table shows more detail about which Office installations were affected by these changes and when.

Expand table

Office version	Groove.exe is no longer installed by default	Groove.exe is uninstalled on next update if not in use for 30 days
MSI (all versions)	Not applicable	Not applicable
Office 2013 Click-to-Run	Not applicable	Not applicable
Office 2016 Click-to-Run - Office Insider	Sept. 2017 - Version 1710 (Build 8530.1000)	Sept. 2017 - Version 1710 (Build 8530.1000)

Office version	Groove.exe is no longer installed by default	Groove.exe is uninstalled on next update if not in use for 30 days
Office 2016 Click-to-Run - Monthly Channel	Oct. 2017 - Version 1709 (Build 8528.2139)	Oct. 2017 - Version 1709 (Build 8528.2139)
Office 2016 Click-to-Run - Semi-Annual Enterprise Channel (Preview)	Sept. 2018 - Version 1808 (Build 10730.20102)	Sept. 2018 - Version 1808 (Build 10730.20102)
Office 2016 Click-to-Run - Semi-Annual Enterprise Channel	Jan. 2019 - Version 1808 (Build 10730.20264)	Jan. 2019 - Version 1808 (Build 10730.20264)

For more info about Office channels, see Overview of update channels for Microsoft 365 Apps for enterprise.

Related topics

Learn more about the Sync button update on SharePoint sites

Feedback

Was this page helpful? Yes No

Provide product feedback

Prevent users from installing the OneDrive sync app

Article • 04/05/2025

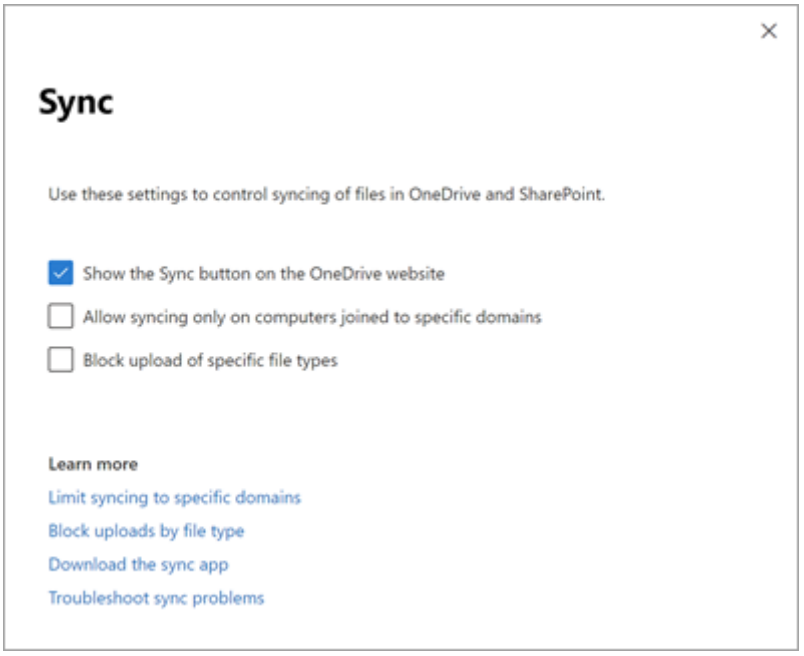
The Sync button helps users install and set up the new OneDrive sync app. If you want to manage the rollout of the sync app to your organization, you can hide the Sync button on the OneDrive website to prevent your users from downloading the sync app themselves.

To prevent users from downloading the OneDrive sync app

1. Go to Settings in the new SharePoint admin center, and sign in with an account that has admin permissions for your organization.

   > **Note**
   >
   > If you have Office 365 operated by 21Vianet (China), sign in to the Microsoft 365 admin center, then browse to the SharePoint admin center and open the Sharing page.

2. Select **Sync**.



3. Clear the **Show the Sync button on the OneDrive website** check box.

4. Select **Save**.

See also

Use OneDrive policies to control sync settings

Silently configure user accounts

Article • 04/05/2025

This article is for IT admins who would like to silently configure user accounts when deploying the new OneDrive sync app (OneDrive.exe) to managed Windows computers in their enterprise. This feature works for computers that are joined to Microsoft Entra ID.

If you enable this feature, OneDrive.exe attempts to silently (without user interaction) sign-in to the work or school user account that was used to sign into Windows (known as the Windows Primary Account). That Windows account must be a Microsoft Entra account or be linked to a Microsoft Entra account through a hybrid authentication configuration (see Prerequisites below).

Before OneDrive.exe begins syncing, it checks the available disk space. If syncing the user's entire OneDrive would cause the available space to drop below 1 GB or if the size exceeds the threshold you set (on devices that don't have Files On-Demand enabled), OneDrive prompts the user to choose folders to sync. For info about setting this threshold using Group Policy, see Set the maximum size of a user's OneDrive that can download automatically.

When the user is configured in the sync app, if the same user account is syncing files with the previous OneDrive sync app (Groove.exe), the new sync app (OneDrive.exe) will attempt to take over syncing those files.

> **Important**
>
> We recommend enabling silent account configuration when you configure the sync app. **See all our recommendations for configuring the sync app**

Prerequisites

Before you can enable silent account configuration, you need to join your devices to Microsoft Entra ID. You can join devices running Windows 10 or newer, and Windows Server 2016 or newer, directly to Microsoft Entra ID. To learn how, see Join your work device to your organization's network.

If you have an on-premises environment that uses Active Directory, you can enable Microsoft Entra hybrid joined devices to join devices on your domain to Microsoft Entra ID. Devices must be running one of the following operating systems:

- Windows 11
- Windows 10

- Windows Server 2019
- Windows Server 2016
- Windows Server 2012 R2

If you federate your on-premises Active Directory with Microsoft Entra ID, you must use AD FS to enable this feature. For info about using Microsoft Entra Connect, see Getting started with Microsoft Entra Connect using express settings.

> **Note**
>
> For more info, see How to configure Microsoft Entra hybrid joined devices. To check the join status and fix problems, see Troubleshoot Microsoft Entra hybrid joined devices.

Enable silent configuration

If the computers on your network are joined to Active Directory on-premises, you can use domain group policy to configure silent account configuration.

Using Group Policy:

1. Enable silent account configuration. For info, see Silently sign in users to the OneDrive sync app with their Windows credentials.
2. Optionally, specify the maximum OneDrive size that downloads automatically in silent configuration. For info, see Set the maximum size of a user's OneDrive that can download automatically. If you enable Files On-Demand, OneDrive ignores the maximum size value.
3. Optionally, set the default location for the OneDrive folder. For info, see Set the default location for the OneDrive folder.

> **Tip**
>
> See the Verify SilentAccountConfig section below to verify and troubleshoot your configuration.

> **Note**
>
> Silent account configuration won't work on devices for users who require multifactor authentication. Select third-party identity providers (IdPs) are supported, but there are caveats. For more information, make sure to check out the Microsoft Entra federation compatibility list.

Configuration with Alternate IDs is only supported within Microsoft 365 Government environments.

If the computers on your network aren't connected to Active Directory on-premises, but only to Microsoft Entra ID, we recommend using Intune and a Microsoft PowerShell script to set the registry keys required to enable silent account configuration. Be sure you have automatic enrollment set up for Windows 10 or newer devices.

Using a script:

PowerShell

```
$HKLMregistryPath = 'HKLM:\SOFTWARE\Policies\Microsoft\OneDrive'##Path to HKLM
keys
$DiskSizeregistryPath =
'HKLM:\SOFTWARE\Policies\Microsoft\OneDrive\DiskSpaceCheckThresholdMB'##Path to
max disk size key
$TenantGUID = 'xxxxxxxx-xxxx-xxxx-xxxx-xxxxxxxxxxxx'

if(!(Test-Path $HKLMregistryPath)){New-Item -Path $HKLMregistryPath -Force}
if(!(Test-Path $DiskSizeregistryPath)){New-Item -Path $DiskSizeregistryPath -
Force}

New-ItemProperty -Path $HKLMregistryPath -Name 'SilentAccountConfig' -Value '1' -
PropertyType DWORD -Force | Out-Null ##Enable silent account configuration
New-ItemProperty -Path $DiskSizeregistryPath -Name $TenantGUID -Value '102400' -
PropertyType DWORD -Force | Out-Null ##Set max OneDrive threshold before prompting
```

Windows Image Prep requirements

SilentAccountConfig creates a SilentBusinessConfigCompleted registry entry once SilentAccountConfig has successfully provisioned the user in OneDrive.exe. This prevents SilentAccountConfig from reprovisioning the user in OneDrive.exe if the user manually stops syncing.

If SilentAccountConfig has successfully completed on a computer you're going to use to build a Windows deployment image (for example, SysPrep), you need to ensure this registry key and also ClientEverSignedIn and PersonalUnlinkedTimeStamp registry keys are removed before you prepare your image. You can do so by running the following commands:

Console

```
reg delete HKCU\Software\Microsoft\OneDrive /v SilentBusinessConfigCompleted /f
reg delete HKCU\Software\Microsoft\OneDrive /v ClientEverSignedIn /f
```

```
reg delete HKCU\Software\Microsoft\OneDrive /v PersonalUnlinkedTimeStamp /f
reg delete HKCU\Software\Microsoft\OneDrive /v OneAuthUnrecoverableTimestamp /f
```

Verify SilentAccountConfig

Instructions for SharePoint in Microsoft 365

1. Unlink all preexisting Business instances in OneDrive.

2. Clear the registry of any previous successful Silent Business Config runs:

Console

```
reg delete HKCU\Software\Microsoft\OneDrive /v SilentBusinessConfigCompleted /f
reg delete HKCU\Software\Microsoft\OneDrive /v ClientEverSignedIn /f
reg delete HKCU\Software\Microsoft\OneDrive /v PersonalUnlinkedTimeStamp /f
reg delete HKCU\Software\Microsoft\OneDrive /v OneAuthUnrecoverableTimestamp /f
```

3. Set the Silent Config policy registry entry (must be run from an administrator CMD window):

   Console

   ```
   reg add HKLM\SOFTWARE\Policies\Microsoft\OneDrive /v SilentAccountConfig /t
   REG_DWORD /d 0x1 /f
   ```

4. Sign out of Windows (Ctrl+Alt+Delete Sign out).

5. Sign in to Windows.

6. Shortly you should see a blue cloud icon in the notification area of the taskbar. Selecting the icon should show the activity center pop-up showing ongoing/recent activity from the first sync. If so, SilentAccountConfig has worked correctly.

7. If instead you see the "Set up OneDrive" screen, SilentAccountConfig couldn't silently sign in or failed for another reason. Verify you completed these steps correctly by repeating them again. Follow the Verify Single Sign On (SSO) steps later in this article to confirm that SSO isn't a problem. Gather sync app logs to send to the engineering team for further help.

Instructions for SharePoint Server 2019 or newer

1. Ensure you can manually get the OneDrive sync app to sync content with your on-premises SharePoint Server, 2019 or newer, before proceeding. See Configure sync app for syncing with SharePoint Server for details.

2. Set the SharePointOnPremPrioritization reg key value to 1 (this ensures that your on premises SharePoint Server takes precedence over Microsoft 365 SharePoint cloud, delete the registry key to revert to SharePoint in Microsoft 365):

   Console

   ```
   reg add HKLM\SOFTWARE\Policies\Microsoft\OneDrive /v
   SharePointOnPremPrioritization /t REG_DWORD /d 0x1 /f
   ```

3. Follow steps 1 through 6 in the previous procedure for SharePoint in Microsoft 365.

4. If instead, you see the "Set up OneDrive" screen, SilentAccountConfig was unable to silently sign in or failed for another reason. Verify you've completed these steps correctly by repeating them again. Gather sync app logs to send to the engineering team for further help.

To prevent Silent Business Config

Console

```
reg delete HKLM\SOFTWARE\Policies\Microsoft\OneDrive /v SilentAccountConfig /f
```

Verify that Single Sign On (SSO) is working

The most common reason for SilentAccountConfig to fail is the credentials aren't available to OneDrive.exe without user interaction. Follow these steps to determine if this is a problem in your case.

If you have a computer you think should work with SilentAccountConfig, you can manually verify that SSO is working correctly to ensure that the environment is configured correctly.

1. Ensure OneAuth is enabled

   Console

   ```
   reg delete HKCU\Software\Microsoft\OneDrive /v OneAuthUnrecoverableTimestamp
   /f
   ```

2. Shut down any running OneDrive.exe processes (verify in the Task Manager Details tab - Ctrl+Shift+Esc).

3. Start menu - OneDrive, you should see the **Set up OneDrive** screen (if not unlink/stop syncing any business accounts and start over).

4. Enter the same email address that the user used to sign into Windows (try alias@domain and domain\alias forms).

5. Select the **Sign in** button.

6. The dialog should switch to a "signing in" page with a spinning icon for a few seconds. It should then continue to the next part of the wizard without asking for a password.

7. If a password prompt doesn't appear, your auth environment is properly configured and SilentAccountConfig should work for your users.

8. If you do see a password prompt, the environment isn't configured properly for silent sign-on. This could be due to a problem with how the computer is domain joined (for example, a trust relationship problem), a problem with ADFS configuration, a Microsoft Entra Conditional Access policy requiring user interaction, you didn't provide the same user email address as the one used to sign into Windows, or some other reason. You need to resolve whatever is blocking silent sign-on before SilentAccountConfig works for you.

9. Remove any OneAuth failure timestamp

Console

```
reg query HKCU\Software\Microsoft\OneDrive /v OneAuthUnrecoverableTimestamp
reg delete HKCU\Software\Microsoft\OneDrive /v OneAuthUnrecoverableTimestamp /f
```

Redirect and move Windows known folders to OneDrive

Article • 03/27/2025

This article is for IT admins managing the OneDrive sync app.

There are two primary advantages of moving or redirecting Windows known folders (Desktop, Documents, Pictures, Screenshots, and Camera Roll) to Microsoft OneDrive for the users in your domain:

- Your users can continue using the folders they're familiar with. They don't have to change their daily work habits to save files to OneDrive.
- Saving files to OneDrive backs up your users' data in the cloud and gives them access to their files from any device.

For these reasons, we recommend moving (redirecting) known folders to OneDrive if you're an enterprise or large organization. See all our recommendations for configuring the sync app. Small or medium businesses might also find this process useful, but keep in mind you need some experience configuring policies. For info about the end-user experience, see Protect your files by saving them to OneDrive.

Prepare to move known folders on existing devices

We recommend that you upgrade to the latest available build before you deploy.

For information on issues that can prevent folders from being moved, see Fix problems with folder protection. Known Folder Move doesn't work for users syncing OneDrive files in SharePoint Server.

> **Important**
>
> If your organization is large and your users have many files in their known folders, make sure you roll out the configuration slowly to minimize the network impact of uploading files. For users who have many files in their known folders, consider using the policy **Limit the sync app upload rate to a percentage of throughput** temporarily to minimize the network impact and then disable the policy once uploads are complete.

Folders redirected to other organizations

If a user's Documents, Pictures, or Desktop folders are currently redirected to OneDrive in a different organization, redirecting to your organization's OneDrive creates new Documents, Pictures, or Desktop folders and the user then sees an empty desktop. The user has to manually migrate files from the other organization's OneDrive to OneDrive in your organization. We recommend that you disable the redirect to the other organization before redirecting to your organization if possible.

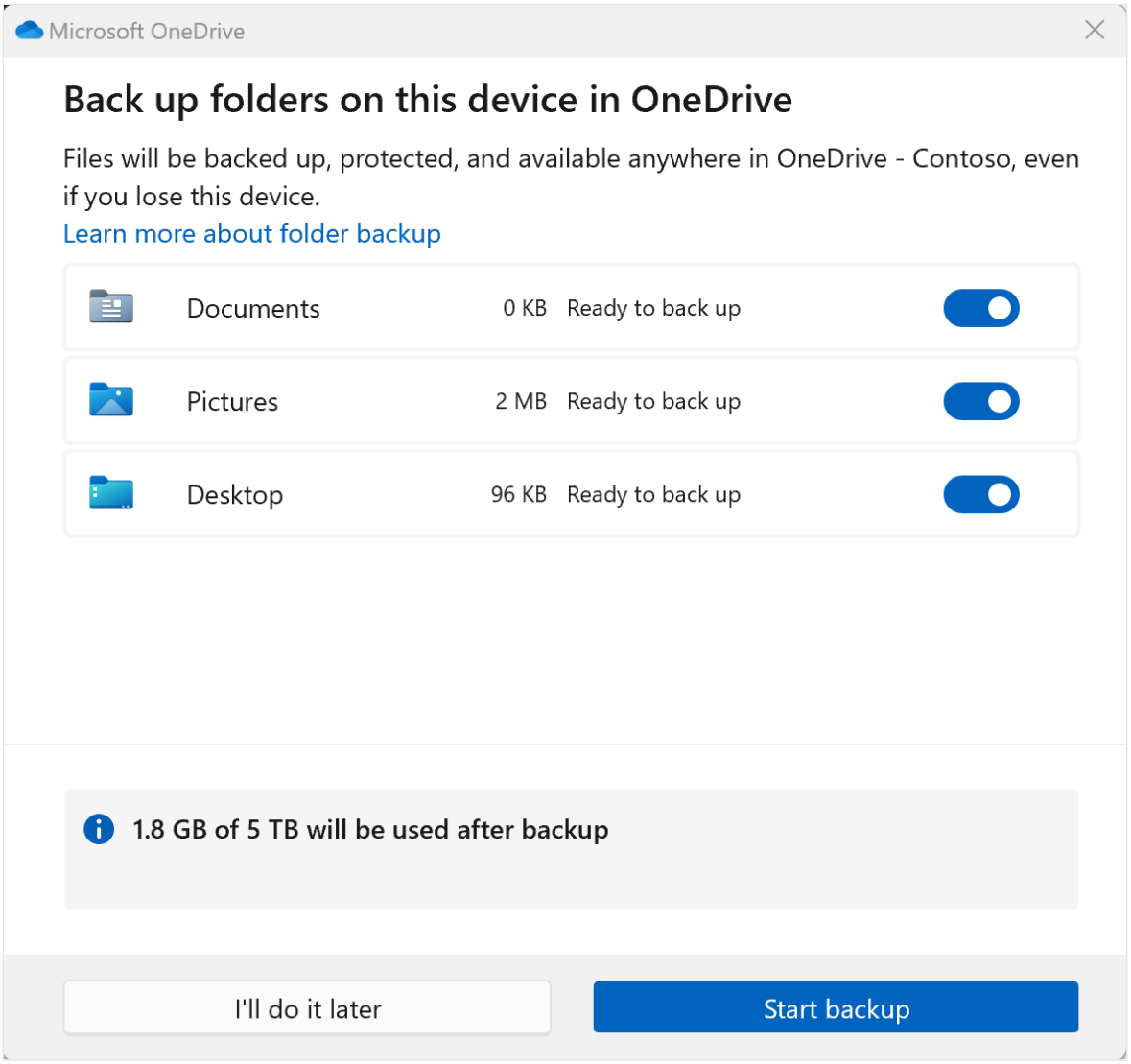
About the Known Folder Move policies

OneDrive policies can be set using Group Policy, Intune Windows 10 Administrative Templates, or by configuring registry settings. For a full reference of available policies and their registry settings, see Use OneDrive policies to control sync settings.

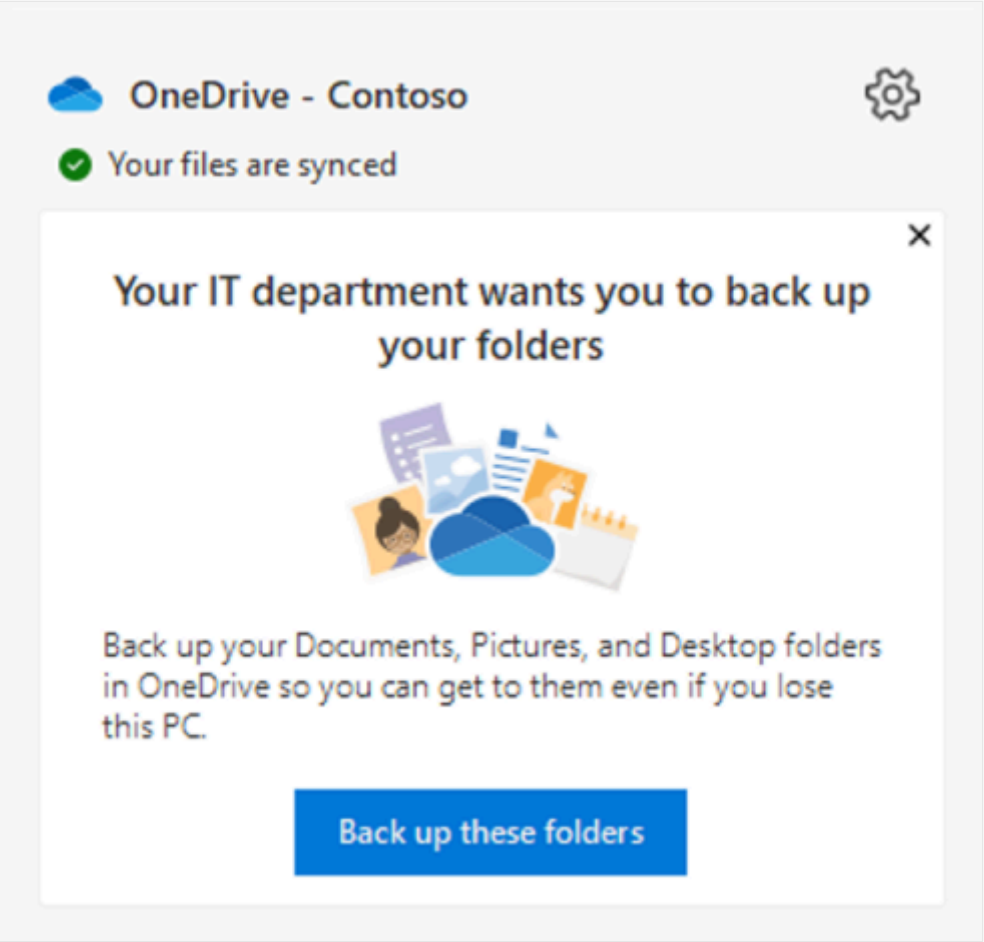
The following policies control the Known Folder Move feature:

- Prompt users to move Windows known folders to OneDrive

  Use this setting to give the users a call to action to move their Windows known folders.



If users dismiss the prompt, a reminder notification appears in the activity center until they move all known folders or an error occurs with the move, in which case the reminder notification can be dismissed.



> **Important**
>
> We recommend deploying the prompt policy for existing devices only, and limiting the deployment to 5,000 devices a day and not exceeding 20,000 devices a week between macOS and Windows.

- Silently move Windows known folders to OneDrive

  Use this setting to redirect and move known folders to OneDrive without any user interaction. Move all the folders or select the desired individual folders. After a folder is moved, the policy won't affect the folder again, even if the selection for the folder changes.

  You can choose to display a notification to users after their folders have been redirected.

  We also recommend using this setting together with Prompt users to move Windows known folders to OneDrive.. If moving the known folders silently doesn't succeed, users are prompted to correct the error and continue.

> **Important**

> We recommend deploying the silent policy for existing devices and new devices while limiting the deployment of existing devices to 1,000 devices a day and not exceeding 4,000 devices a week between macOS and Windows.

- Prevent users from turning off Known Folder Move

  Use this setting to require users to keep their known folders directed to OneDrive.

  > ⓘ **Note**
  >
  > Users can direct their known folders by opening OneDrive sync app settings, clicking the **Backup** tab, and then clicking **Manage backup**.

- Prevent users from moving their Windows known folders to OneDrive

  Use this setting to prevent users from moving their known folders to any OneDrive account.

For info about using the OneDrive policies, see Use Group Policy to control OneDrive sync app settings.

Transition from the Windows Folder Redirection Group Policy objects

The OneDrive Known Folder Move Group Policy objects doesn't work if you previously used Windows Folder Redirection Group Policy objects to redirect the Documents, Pictures, or Desktop folders to a location other than OneDrive. The OneDrive Group Policy objects don't affect the Music and Videos folders, so you can keep them redirected with the Windows Group Policy objects. Follow these steps to switch to using the Known Folder Move Group Policy objects.

> ⓘ **Note**
>
> Extending the scope of folders synced by OneDrive using Windows Folder Redirection Group Policy isn't supported.

- If folders have been redirected to OneDrive using Windows Folder Redirection Group Policy:

  1. Disable the Window Folder Redirection Group Policy and make sure to leave the folder and contents on OneDrive.

2. Enable Known Folder Move Group Policy. Known folders remain in OneDrive.

- If folders have been redirected to a location on a local PC:

  1. Disable the Window Folder Redirection Group Policy and make sure to leave the folder and contents at the redirected location.
  2. Enable Known Folder Move Group Policy. Known folders move to OneDrive.

- If folders have been redirected to a network file share:

  1. Use Migration Manager to copy contents in the network file share location to a user's OneDrive, making sure that all contents go into the existing Documents, Pictures, or Desktop folders.

     > **Note**
     >
     > If Migration Manager creates the Documents, Pictures, or Desktop folders, ensure that **Preserve file share permissions** isn't selected when performing the migration.

  2. Disable the Window Folder Redirection Group Policy and make sure to leave the folder and contents on the network file share.

  3. Enable Known Folder Move Group Policy. Known folders move to OneDrive and will merge with the existing Desktop, Documents, and Pictures folders, which contain all the file share content that you moved in the first step.

Feedback

Was this page helpful? Yes No

Provide product feedback

Deploy Restrict Known Folder Move from Office Group Policy

Article • 04/22/2025

The Restrict Known Folder Move from Office (Restrict KFM from Office) Group Policy allows administrators to control whether Office apps display prompts encouraging users to back up their files to Microsoft OneDrive.

When this policy is enabled and deployed, Office doesn't display the message bar, even if users are eligible for the Known Folder Move (KFM) feature. This policy applies only to Office apps and doesn't affect other OneDrive or KFM configurations. It's available in the Administrative Template files for Microsoft Office (version 5497.1000 or newer).

> **Tip**
>
> - Enable this policy if you don’t want users to see prompts to back up their files.
> - If KFM is blocked in your organization, the message bar doesn't appear, even if users are eligible.
> - Microsoft respects existing policies that block KFM and doesn't display prompts in those environments.

What users see when eligible

When the policy isn't enabled, eligible users might see a message bar in Microsoft Word, Excel, and PowerPoint (Windows desktop versions) prompting them to enroll in OneDrive Known Folder Move (KFM). The message bar allows users to select folders to back up to OneDrive.

> **Important**
>
> If users aren't enrolled in KFM, they might see the message:
> **"BACK UP THIS DOCUMENT: Share and work with others in this and other files using OneDrive."**
>
> Selecting **Open OneDrive** lets users choose which folders to back up.

By enabling and deploying the **Restrict KFM from Office** Group Policy, administrators can prevent these prompts and maintain control over KFM adoption.

When the Message Bar isn't displayed

The message bar doesn't appear under the following conditions:

- The user is already enrolled in KFM.
- OneDrive isn't provisioned, installed, or running.
- The policy Prevent users from moving their Windows known folders to OneDrive is enabled.
- The **Restrict KFM from Office** policy is enabled.

Deployment methods

Option 1: Deploy via Group Policy (Active Directory or hybrid environments)

If you're using Active Directory, Microsoft Entra, or a hybrid environment, you can deploy the policy using Group Policy Objects (GPOs).

1. Download the Administrative Template files (ADMX/ADML) for Microsoft Office.
2. Select **Download**, then choose the 32-bit (x86), 64-bit (x64), or both versions.
3. Select **Next**, then choose a location to save the file.
4. Run the downloaded **admintemplates_XXXXXXX_en-us.exe** and follow the prompts to extract the files.
5. After extracting, you'll see **admin** and **admx** folders.
6. On your Active Directory server:
    - Copy the `.admx` files into **%SYSTEMROOT%\PolicyDefinitions**
    - Copy the corresponding language `.adml` files into **%SYSTEMROOT%\PolicyDefinitions[Language-CountryRegion]**
        - For example, copy U.S. English `.adml` files into the `en-us` folder.
7. Open **Group Policy Management**.
8. Under **Domains**, select the appropriate policy (for example, **Default Domain Policy**) and choose **Edit**.
9. In the Group Policy Management Editor, go to:
   User Configuration > **Policies** > **Administrative Templates: Policy Definitions** > **All Settings**
10. Locate **Restrict KFM from Office**, right-click it, and select **Edit**.
11. Change the setting from **Not Configured** to **Enabled**, then select **Apply** and **OK**.
12. The policy setting should now display as **Enabled**.

Restrict KFM from Office

Restrict KFM from Office

Previous Setting | Next Setting

- ○ Not Configured
- ◉ Enabled
- ○ Disabled

Comment:

Disable KFM pop ups on Office files

Supported on:

At least Windows Server 2008 R2 or Windows 7

Options:

Help:

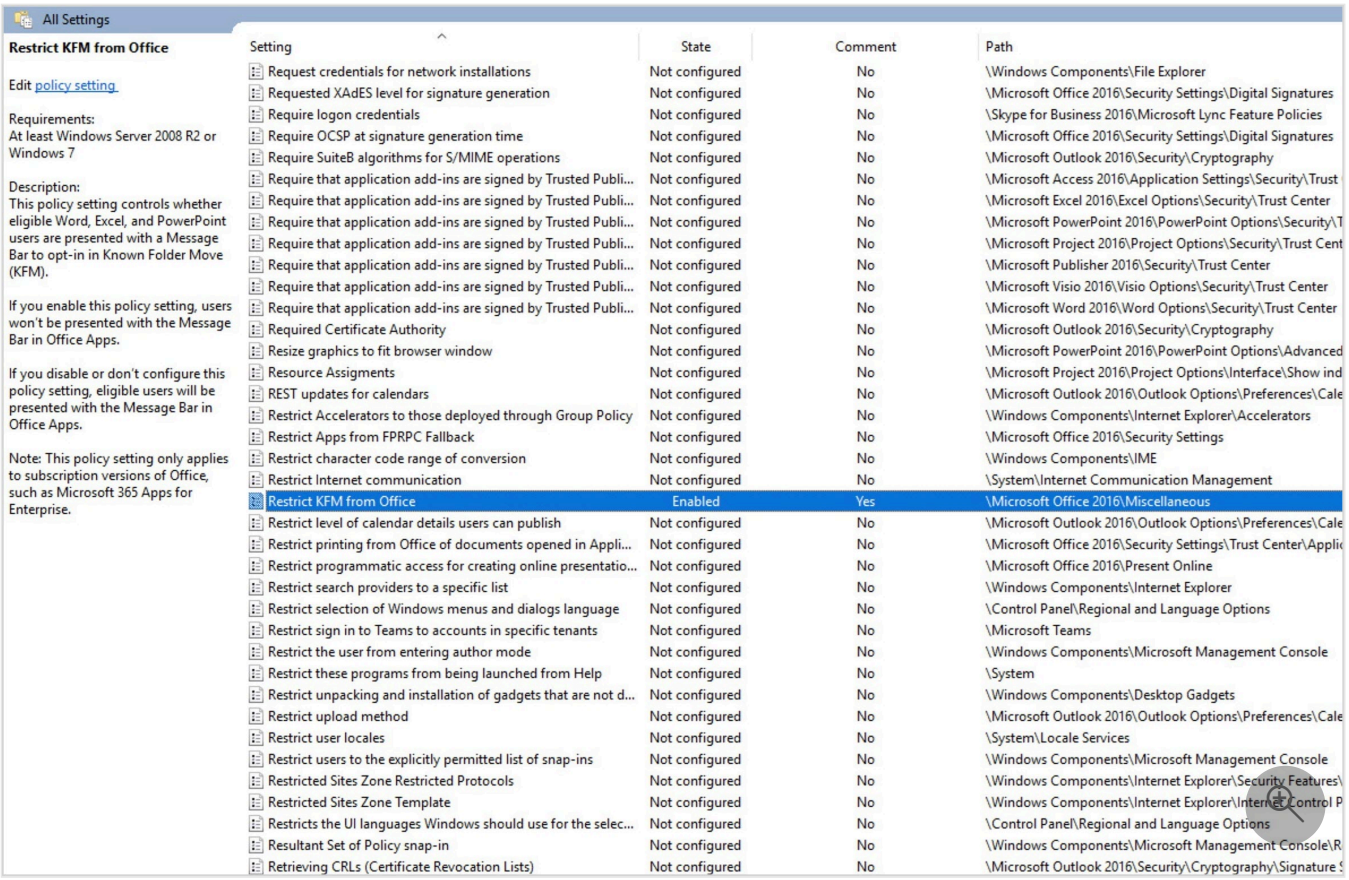
This policy setting controls whether eligible Word, Excel, and PowerPoint users are presented with a Message Bar to opt-in in Known Folder Move (KFM).

If you enable this policy setting, users won't be presented with the Message Bar in Office Apps.

If you disable or don't configure this policy setting, eligible users will be presented with the Message Bar in Office Apps.

Note: This policy setting only applies to subscription versions of Office, such as Microsoft 365 Apps for Enterprise.

OK | Cancel | Apply



All Settings

Restrict KFM from Office

Edit policy setting

Requirements:
At least Windows Server 2008 R2 or Windows 7

Description:
This policy setting controls whether eligible Word, Excel, and PowerPoint users are presented with a Message Bar to opt-in in Known Folder Move (KFM).

If you enable this policy setting, users won't be presented with the Message Bar in Office Apps.

If you disable or don't configure this policy setting, eligible users will be presented with the Message Bar in Office Apps.

Note: This policy setting only applies to subscription versions of Office, such as Microsoft 365 Apps for Enterprise.

Setting	State	Comment	Path
Request credentials for network installations	Not configured	No	\Windows Components\File Explorer
Requested XAdES level for signature generation	Not configured	No	\Microsoft Office 2016\Security Settings\Digital Signatures
Require logon credentials	Not configured	No	\Skype for Business 2016\Microsoft Lync Feature Policies
Require OCSP at signature generation time	Not configured	No	\Microsoft Office 2016\Security Settings\Digital Signatures
Require SuiteB algorithms for S/MIME operations	Not configured	No	\Microsoft Outlook 2016\Security\Cryptography
Require that application add-ins are signed by Trusted Publi...	Not configured	No	\Microsoft Access 2016\Application Settings\Security\Trust
Require that application add-ins are signed by Trusted Publi...	Not configured	No	\Microsoft Excel 2016\Excel Options\Security\Trust Center
Require that application add-ins are signed by Trusted Publi...	Not configured	No	\Microsoft PowerPoint 2016\PowerPoint Options\Security\T
Require that application add-ins are signed by Trusted Publi...	Not configured	No	\Microsoft Project 2016\Project Options\Security\Trust Cent
Require that application add-ins are signed by Trusted Publi...	Not configured	No	\Microsoft Publisher 2016\Security\Trust Center
Require that application add-ins are signed by Trusted Publi...	Not configured	No	\Microsoft Visio 2016\Visio Options\Security\Trust Center
Require that application add-ins are signed by Trusted Publi...	Not configured	No	\Microsoft Word 2016\Word Options\Security\Trust Center
Required Certificate Authority	Not configured	No	\Microsoft Outlook 2016\Security\Cryptography
Resize graphics to fit browser window	Not configured	No	\Microsoft PowerPoint 2016\PowerPoint Options\Advanced
Resource Assigments	Not configured	No	\Microsoft Project 2016\Project Options\Interface\Show ind
REST updates for calendars	Not configured	No	\Microsoft Outlook 2016\Outlook Options\Preferences\Cale
Restrict Accelerators to those deployed through Group Policy	Not configured	No	\Windows Components\Internet Explorer\Accelerators
Restrict Apps from FPRPC Fallback	Not configured	No	\Microsoft Office 2016\Security Settings
Restrict character code range of conversion	Not configured	No	\Windows Components\IME
Restrict Internet communication	Not configured	No	\System\Internet Communication Management
Restrict KFM from Office	Enabled	Yes	\Microsoft Office 2016\Miscellaneous
Restrict level of calendar details users can publish	Not configured	No	\Microsoft Outlook 2016\Outlook Options\Preferences\Cale
Restrict printing from Office of documents opened in Appli...	Not configured	No	\Microsoft Office 2016\Security Settings\Trust Center\Applic
Restrict programmatic access for creating online presentatio...	Not configured	No	\Microsoft Office 2016\Present Online
Restrict search providers to a specific list	Not configured	No	\Windows Components\Internet Explorer
Restrict selection of Windows menus and dialogs language	Not configured	No	\Control Panel\Regional and Language Options
Restrict sign in to Teams to accounts in specific tenants	Not configured	No	\Microsoft Teams
Restrict the user from entering author mode	Not configured	No	\Windows Components\Microsoft Management Console
Restrict these programs from being launched from Help	Not configured	No	\System
Restrict unpacking and installation of gadgets that are not d...	Not configured	No	\Windows Components\Desktop Gadgets
Restrict upload method	Not configured	No	\Microsoft Outlook 2016\Outlook Options\Preferences\Cale
Restrict user locales	Not configured	No	\System\Locale Services
Restrict users to the explicitly permitted list of snap-ins	Not configured	No	\Windows Components\Microsoft Management Console
Restricted Sites Zone Restricted Protocols	Not configured	No	\Windows Components\Internet Explorer\Security Features\
Restricted Sites Zone Template	Not configured	No	\Windows Components\Internet Explorer\Internet Control P
Restricts the UI languages Windows should use for the selec...	Not configured	No	\Control Panel\Regional and Language Options
Resultant Set of Policy snap-in	Not configured	No	\Windows Components\Microsoft Management Console\R
Retrieving CRLs (Certificate Revocation Lists)	Not configured	No	\Microsoft Outlook 2016\Security\Cryptography\Signature S

> **Note**
>
> It might take up to 24 hours for the policy to take effect.

Option 2: Deploy via Cloud Policy service

You can also deploy this policy using the Cloud Policy service for Microsoft 365. This method works even if the device isn't domain-joined. When a user signs into Microsoft 365 Apps for Enterprise on a device, the policy settings roam to that device. See Overview of Cloud Policy to learn more about cloud policies for Microsoft 356 Apps.

To deploy the policy:

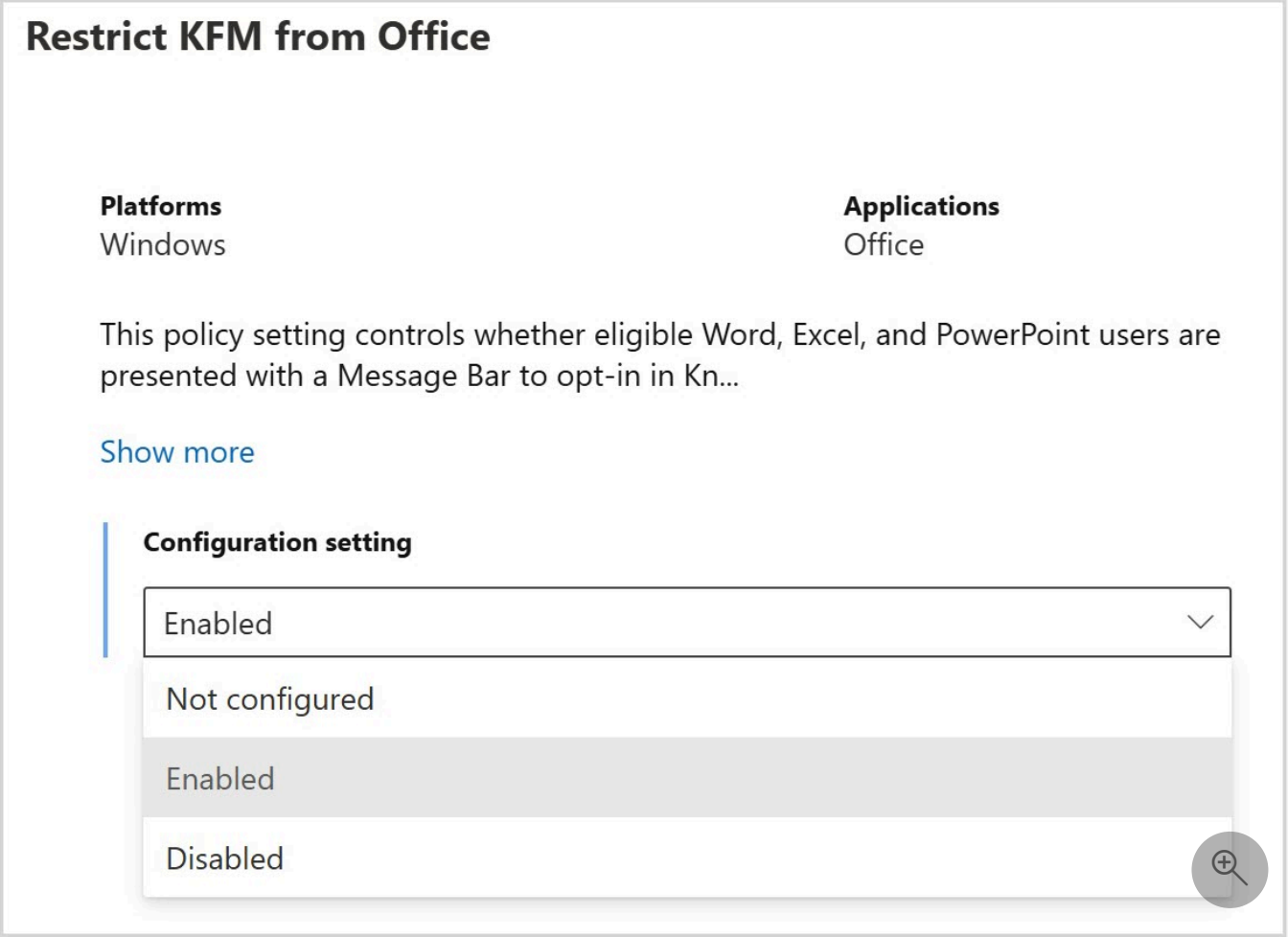
1. Sign in to the Microsoft 365 Apps admin center with administrative credentials.
2. Under **Customization**, select **Policy Management**.
3. On the **Policy configurations** page, select **Create**.
4. On the **Start with the basics** page, enter a **Name** (required) and **Description** (optional), then select **Next**.
5. On the **Choose the scope** page, select whether the policy applies to:

    - All users
    - Specific groups
    - Users accessing Office for the web anonymously

6. If applying to specific groups, select **Add Groups** and choose the relevant groups.

> ⓘ **Note**
>
> Adding multiple groups to a single policy configuration allows for the same group to be included in multiple policy configurations, facilitating a more streamlined and efficient policy management process.

7. Select **Next**.
8. On the **Configure Settings** page:
    - Search for **Restrict KFM from Office** or use a filter.
    - Set the configuration to **Enabled**, then select **Apply**.
9. Review your selections and choose **Create**.
10. Select **Done**.



Once configured, the policy will apply to eligible users the next time they sign in to Microsoft 365 Apps on any device.

Related topics

- Redirect and move Windows known folders to OneDrive
- Use OneDrive policies to control sync settings
- Group Policy Objects

IT Admins - Use OneDrive policies to control sync settings

This article describes the OneDrive Group Policy objects (GPOs) that administrators can configure by using Group Policy or by using administrative templates in Microsoft Intune. You can use the registry key information in this article to confirm that a setting is enabled.

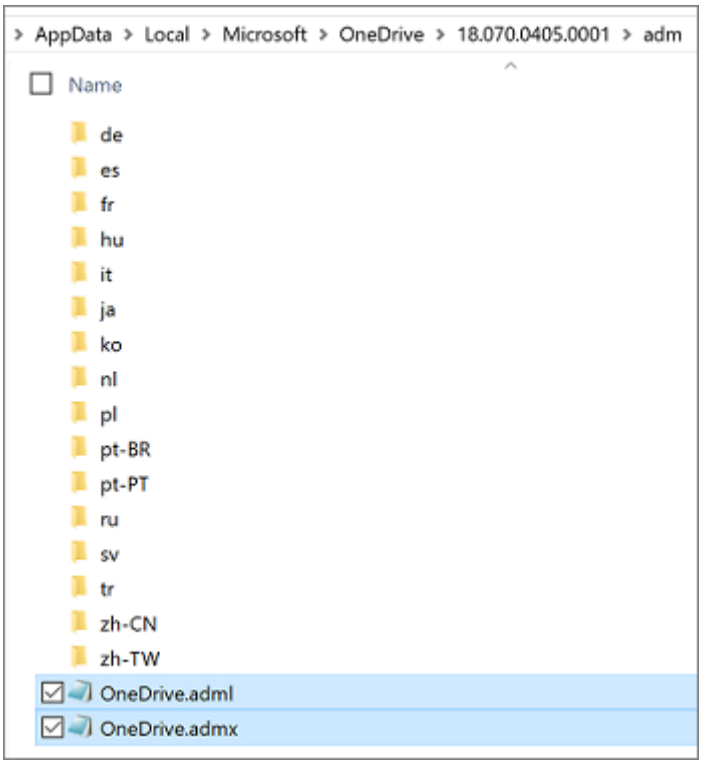
> **Note**
>
> If you're not an IT administrator, see Sync files with the new OneDrive sync app in Windows for information about OneDrive sync settings.

https://learn-video.azurefd.net/vod/player?id=9732f86a-fd9f-48e9-bd2d-216432a36549&locale=en-us&embedUrl=%2FSharePoint%2Fuse-group-policy

Manage OneDrive using Group Policy

1. Install the OneDrive sync app for Windows. (For information on the builds that are being released, and on the download builds, see release notes.) Installing the sync app downloads the .adml and .admx files.

2. Browse to `%localappdata%\Microsoft\OneDrive\\*BuildNumber*\adm\` (for per-machine sync app browse to `%ProgramFiles(x86)%\Microsoft OneDrive\BuildNumber\adm\` or `%ProgramFiles%\Microsoft OneDrive\BuildNumber\adm\` (depending on the OS architecture)) to the subfolder for your language, as necessary (where *BuildNumber* is the number displayed in sync app settings under the **About** tab).



3. Copy the .adml and .admx files.

4. Paste the .admx file in your domain's Central Store, `\\\\*domain*\sysvol\domain\Policies\PolicyDefinitions` (where *domain* is your domain name, such as corp.contoso.com), and the .adml file in the appropriate language subfolder, such as en-us. If the PolicyDefinitions folder doesn't exist, see How to create and manage the Central Store for Group Policy Administrative Templates in Windows, or use your local policy store under `%windir%\policydefinitions`.

5. Configure settings from the domain controller or on a Windows computer by running the Remote Server Administration Tools.

6. Link the GPOs to an Active Directory container (a site, domain, or an organizational unit). For more information, see Link Group Policy objects to Active Directory containers.

7. Use security filtering to narrow the scope of a setting. By default, a setting is applied to all user and computer objects within the container to which it's linked, but you can use security filtering to narrow the scope of the policy's application to a subset of users or computers. For more information, see Filtering the scope of a GPO.

   The OneDrive GPOs work by setting registry keys on the computers in your domain.

   - When you enable or disable a setting, the corresponding registry key is updated on computers in your domain. If you later change the setting back to **Not configured**, the

corresponding registry key isn't modified, and the change doesn't take effect. After you configure a setting, set it to **Enabled** or **Disabled**, going forward.
    - The location where registry keys are written has been updated. When you use the latest files, you might delete registry keys that you set previously.

> **Note**
>
> For information about storage, see OneDrive Files On-Demand and Storage Sense for Windows 10 and Policy CSP - Storage.

List of policies by string ID

- (AddedFolderHardDeleteOnUnmount) Hard-delete the contents of a folder shortcut when unmounted
- (AddedFolderUnmountOnPermissionsLoss) Hard-delete contents of a folder shortcut when user loses permissions to the folder
- (AllowTenantList) Allow syncing OneDrive accounts for only specific organizations
- (AutomaticUploadBandwidthPercentage) Limit the sync app upload rate to a percentage of throughput
- (AutoMountTeamSites) Configure team site libraries to sync automatically
- (BlockExternalListSync) This setting controls Lists sync and is listed here for convenience. For more information, see Prevent users from syncing lists shared from other organizations.
- (BlockExternalSync) Prevent users from syncing libraries and folders shared from other organizations
- (BlockKnownFolderMove) Prevent users from moving their Windows known folders to OneDrive
- (BlockTenantList) Block syncing OneDrive accounts for specific organizations
- (CustomSyncRootFolderName) Set a custom name for the OneDrive folder
- (DefaultRootDir) Set the default location for the OneDrive folder
- (DehydrateSyncedTeamSites) Convert synced team site files to online-only files

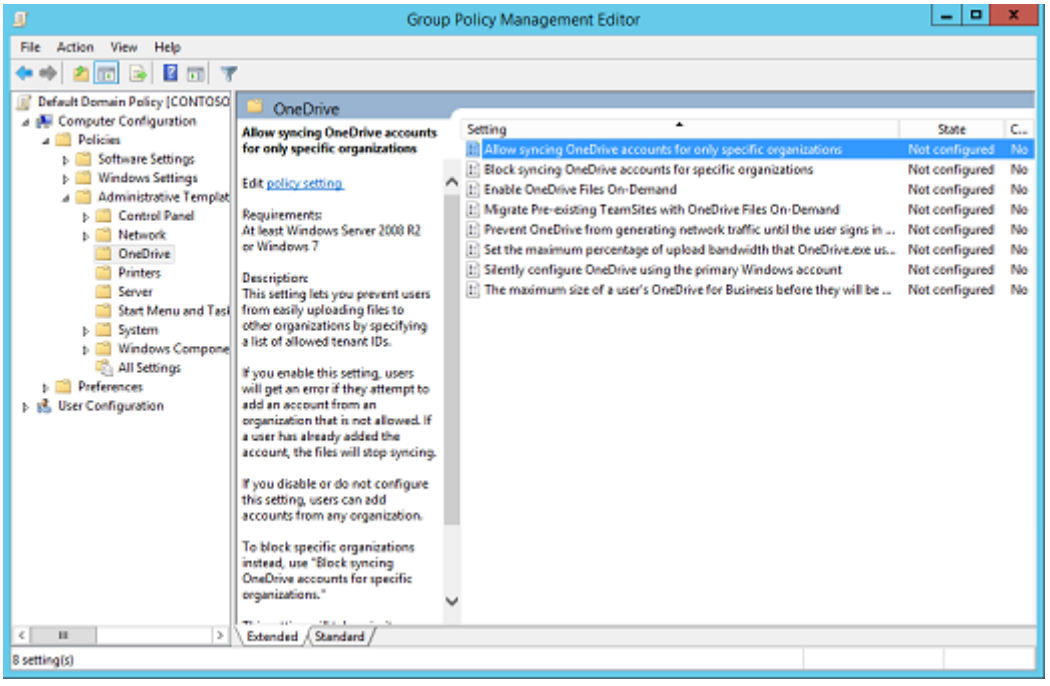
- (DisableAutoConfig) Prevent the sync app from automatically signing in users with existing credentials
- (DisableChangesToODIgnoreList) Prevent users at your organization from changing the default ignored extension and folder lists
- (DisableCustomRoot) Prevent users from changing the location of their OneDrive folder
- (DisableDefaultODIgnoreList) Disable the default ignored extension and folder lists
- (DisableFirstDeleteDialog) Hide the "Deleted files are removed everywhere" reminder
- (DisableFREAnimation) Disable animation that appears during OneDrive Setup
- (DisableFRETutorial) Disable the tutorial that appears at the end of OneDrive Setup
- (DisableListSync) This setting controls Lists sync and is listed here for convenience. For more information, see Prevent Lists sync from running on the device.
- (DisableListSyncSilentConfig) Prevent users from getting silently signed in to offline experiences on the web.
- (DisableNewAccountDetection) Hide toast and activity center notifications that prompt users to sign in to the OneDrive sync app with existing credentials
- (DisableOfflineMode) Prevent users at your organization from enabling offline mode in OneDrive on the web
- (DisableOfflineModeForExternalLibraries) Prevent users at your organization from enabling offline mode in OneDrive on the web for libraries and folders that are shared from other organizations
- (DisablePauseOnBatterySaver) Continue syncing when devices have battery saver mode turned on
- (DisablePauseOnMeteredNetwork) Continue syncing on metered networks
- (DisablePersonalSync) Prevent users from syncing personal OneDrive accounts
- (DiskSpaceCheckThresholdMB) Set the maximum size of a user's OneDrive that can download automatically
- (DownloadBandwidthLimit) Limit the sync app download speed to a fixed rate

- (EnableAutomaticUploadBandwidthManagement) Enable automatic upload bandwidth management for OneDrive
- (EnableAutoStart) Start OneDrive automatically when signing in to Windows
- (EnableFeedbackAndSupport) Allow users to contact Microsoft for feedback and support
- (EnableODIgnoreListFromGPO) Exclude specific kinds of files from being uploaded
- (EnableODIgnoreFolderListFromGPO) Exclude specific kinds of folders from being uploaded
- (EnableSyncAdminReports) Enable sync health reporting for OneDrive
- (FilesOnDemandEnabled) Use OneDrive Files On-Demand
- (ForcedLocalMassDeleteDetection) Require users to confirm large delete operations
- (GPOSetUpdateRing) Set the sync app update ring
- (IgnoreWebProxy) Configure the sync client to bypass web proxy detection
- (KFMBlockOptOut) Prevent users from redirecting their Windows known folders to their PC
- (KFMForceWindowsDisplayLanguage) Always use the user's Windows display language when provisioning known folders in OneDrive
- (KFMOptInNoWizard) Silently move Windows known folders to OneDrive
- (KFMOptInWithWizard) Prompt users to move Windows known folders to OneDrive
- (LocalMassDeleteFileDeleteThreshold) Prompt users when they delete multiple OneDrive files on their local computer
- (MinDiskSpaceLimitInMB) Block file downloads when users are low on disk space
- (PermitDisablePermissionInheritance) Allow OneDrive to disable Windows permission inheritance in folders synced read-only
- (PreventNetworkTrafficPreUserSignIn) Prevent the sync app from generating network traffic until users sign in
- (SharedContentDeleteConfirmation) Prompt users to confirm when they delete shared content

- (SharePointOnPremApplicationIdUri) Specify the Application ID URI for your Entra application for OIDC
- (SharePointOnPremFrontDoorUrl) Specify SharePoint Server URL and organization name. This setting is for customers who have SharePoint Server 2019. For information about using the new OneDrive sync app with SharePoint Server 2019, see Configure syncing with the new OneDrive sync app.
- (SharePointOnPremOIDC) Enable OpenID Connect (OIDC) authentication for syncing content from an on-prem SharePoint Server using the OneDrive sync app
- (SharePointOnPremPrioritization) Specify the OneDrive location in a hybrid environment. This setting is for customers who have SharePoint Server 2019. For information about using the new OneDrive sync app with SharePoint Server 2019, see Configure syncing with the new OneDrive sync app.
- (SilentAccountConfig) Silently sign in users to the OneDrive sync app with their Windows credentials
- (UploadBandwidthLimit) Limit the sync app upload speed to a fixed rate
- (WarningMinDiskSpaceLimitInMB) Warn users who are low on disk space

Computer Configuration policies

Under Computer Configuration\Policies\Administrative Templates\OneDrive, navigate to **Computer Configuration** > **Policies**.



Allow OneDrive to disable Windows permission inheritance in folders synced read-only

Applies to: Group Policy, Intune

This setting lets the OneDrive sync app remove all inherited permissions within read-only folders syncing on a user's PC. This removal of inherited permissions improves the performance of the sync app when syncing folders that the user has read-only permission to.

Enabling this setting for a user doesn't change their permissions to view or edit content in SharePoint.

We don't recommend setting this policy for users not syncing read-only content.

Enabling this policy sets the following registry key value to 1:

```
[HKLM\SOFTWARE\Policies\Microsoft\OneDrive]"PermitDisablePermissionInheritance"=dword:00000001
```

Allow syncing OneDrive accounts for only specific organizations

Applies to: Group Policy, Intune

This setting lets you prevent users from easily uploading files to other organizations by specifying a list of allowed tenant IDs.

If you enable this setting, users get an error if they attempt to add an account from an organization that isn't allowed. If a user has already added the account, the files stop syncing.

To enter a tenant ID, in the **Options** box, select **Show**.

This policy sets the following registry key:

```
[HKLM\SOFTWARE\Policies\Microsoft\OneDrive\AllowTenantList] "1111-2222-3333-4444"
```

where "1111-2222-3333-4444" is the tenant ID.

This setting takes priority over Block syncing OneDrive accounts for specific organizations. Don't enable both settings at the same time.

Allow users to contact Microsoft for feedback and support

Applies to: Group Policy, Intune

This setting specifies whether users can contact Microsoft through user experiences in the app.

If you enable or do not configure this setting, users can use the experiences in the OneDrive app to contact Microsoft directly for feedback and support.

If you disable this setting, users will be unable to contact Microsoft for support, feedback, or suggestions within the app. Users will still have access to help content and self-help tools.

Enabling this policy sets the following registry key values:

`[HKLM\SOFTWARE\Policies\Microsoft\OneDrive]"EnableSendFeedback"=dword:00000001`

`[HKLM\SOFTWARE\Policies\Microsoft\OneDrive]"EnableSurveyCampaigns"=dword:00000001`

`[HKLM\SOFTWARE\Policies\Microsoft\OneDrive]"EnableContactSupport"=dword:00000001`

Set any value to 0 to disable that specific feature.

Always use the user's Windows display language when provisioning known folders in OneDrive

Applies to: Group Policy, Intune

> **Note**
>
> This policy can also be configured under User Configuration.

When you move Windows known folders to OneDrive, they are provisioned in the user's Windows display language by default, unless the user sets a different preferred language. This setting lets you override the user's preferred language setting. It works with both Known Folder Move settings (Silently move Windows known folders to OneDrive and Prompt users to move Windows known folders to OneDrive).

If you enable this setting, known folders are provisioned using the user's Windows display language, even if the user sets a different preferred language.

If you disable or do not configure this setting, and the user set a preferred language, their known folders are provisioned in OneDrive using that language.

This policy can be deployed under Computer Configuration (HKLM) or User Configuration (HKCU). The setting applies from whichever location it is configured. Enabling this policy sets the following registry key values to 1:

```
[HKLM\SOFTWARE\Policies\Microsoft\OneDrive]"KfmForceWindowsDisplayLanguage"=dword:00000001
```

```
[HKCU\SOFTWARE\Policies\Microsoft\OneDrive]"KfmForceWindowsDisplayLanguage"=dword:00000001
```

Block file downloads when users are low on disk space

Applies to: Group Policy, Intune

This setting lets you specify a minimum amount of available disk space and block the OneDrive sync app (OneDrive.exe) from downloading files when users have less than this amount.

Users are prompted with options to help free up space.

Enabling this policy sets the following registry key value to a number from 0 through 10240000:

```
[HKLM\SOFTWARE\Policies\Microsoft\OneDrive] "MinDiskSpaceLimitInMB"=dword:00000000
```

Block syncing OneDrive accounts for specific organizations

Applies to: Group Policy, Intune

This setting lets you prevent users from uploading files to another organization by specifying a list of blocked tenant IDs.

If you enable this setting, users get an error if they attempt to add an account from an organization that's blocked. If a user has already added the account, the files stop syncing.

To enter the tenant ID, in the **Options** box, select **Show**.

This policy sets the following registry key:

```
[HKLM\SOFTWARE\Policies\Microsoft\OneDrive\BlockTenantList] "1111-2222-3333-4444"
```

where "1111-2222-3333-4444" is the tenant ID.

This setting does NOT work if you enable the Allow syncing OneDrive accounts for only specific organizations setting. Don't enable both settings at the same time.

Configure the sync client to bypass web proxy detection

Applies to: Group Policy

This setting controls whether the OneDrive sync client performs web proxy detection.

If you enable this setting, the sync client won't perform web proxy detection and will attempt direct connections to the internet web endpoints it needs to communicate with. This is equivalent to having no web proxy settings configured and no automatic proxy script.

If you disable or don't configure this setting, the sync client will detect if a web proxy is configured on your network and use it if so.

For more information, see Configure proxy server settings in Windows.

Enabling this policy sets the following registry key value to 1:

```
[HKLM\SOFTWARE\Policies\Microsoft\OneDrive]"IgnoreWebProxy"=dword:00000001
```

Convert synced team site files to online-only files

Applies to: Group Policy, Intune

This setting lets you convert synced SharePoint files to online-only files when you enable **OneDrive Files On-Demand**. If you have many PCs syncing the same team site, enabling this setting helps you minimize network traffic and local storage usage.

If you enable this setting, files in currently syncing team sites are changed to online-only files, by default. Files later added or updated in the team site are also downloaded as online-only files. To use this setting, the computer must be running Windows 10 Fall Creators Update (version 1709) or later, and you must enable **OneDrive Files On-Demand**. This feature isn't enabled for on-premises SharePoint sites.

Enabling this policy sets the following registry key value to 1:

```
[HKLM\SOFTWARE\Policies\Microsoft\OneDrive]"DehydrateSyncedTeamSites"=dword:00000001
```

For information about querying and setting file and folder states, see Query and set Files On-Demand states.

Disable the default ignored extension and folder lists

Applies to: Group Policy

Microsoft maintains a default list of file extensions and folder names that the OneDrive sync app doesn't upload to OneDrive or SharePoint. The list currently includes shortcut (.lnk) files. Microsoft might update the list through service updates.

This setting lets you turn off the default list.

If you enable this setting, the sync app doesn't apply the default list. The OneDrive sync app must be restarted after this setting is enabled for the setting to take effect. After the restart, files and folders that were skipped only because of the default list start uploading.

> **Note**
>
> Files and folders that already sync aren't excluded when the default list changes.

The following exclusions still apply when this setting is enabled:

- Exclusions that you configure with Exclude specific kinds of files from being uploaded and Exclude specific kinds of folders from being uploaded.
- Exclusions that users add in OneDrive settings, unless you also enable Prevent users at your organization from changing the default ignored extension and folder lists.

If you disable or don't configure this setting, the sync app applies the default list.

This setting applies only to work or school accounts.

Enabling this policy sets the following registry key value to 1:

```
[HKLM\SOFTWARE\Policies\Microsoft\OneDrive]"DisableDefaultODIgnoreList"=dword:00000001
```

Enable automatic upload bandwidth management for OneDrive

Applies to: Group Policy, Intune

This setting lets the OneDrive sync app (OneDrive.exe) upload data in the background only when unused bandwidth is available. It prevents the sync app from interfering with other apps that are using the network. This setting is powered by the Windows LEDBAT (Low Extra Delay Background Transport) protocol. When LEDBAT detects increased latency that indicates other TCP connections are consuming bandwidth, the sync app reduces its own consumption to prevent interference. When network latency decreases again and bandwidth is freed up, the sync app increases the upload rate and consume the unused bandwidth.

If you enable this setting, the sync app upload rate is set to **Adjust automatically** based on bandwidth availability, and users won't be able to change it.

If you don't configure this setting, users can choose to limit the upload rate to a fixed value (in KB/second), or set it to **Adjust automatically**.

> ⓘ **Important**
>
> If you enable or disable this setting, and then change it back to **Not Configured**, the last configuration will remain in effect. We recommend enabling this setting instead of **Limit the sync app upload speed to a fixed rate**. You shouldn't enable both settings at the same time. This setting will override **Limit the sync app upload rate to a percentage of throughput** if both are enabled on the same device.

Enabling this policy sets the following registry key value to 1:

```
[HKLM\Software\Policies\Microsoft\OneDrive]"EnableAutomaticUploadBandwidthManagement"=dword:00000001
```

Enable OpenID Connect (OIDC) authentication for syncing content from an on-prem SharePoint Server using the OneDrive sync app

Applies to: Group Policy

This setting lets the OneDrive sync app (OneDrive.exe) authenticate requests to an on-premises SharePoint Server using OpenID Connect (OIDC) authentication, if supported by the server. To use this setting, you must also enable Specify SharePoint Server URL and organization name. This setting affects only OneDrive for Business sync functionality. It does not impact syncing team sites in SharePoint Online.

If you enable this setting, you can select one of two options:

- **Disable OIDC Authentication**: The sync app will not attempt to use OIDC authentication, even if the server supports it.
- **Enable OIDC Authentication**: The sync app will attempt to use OIDC authentication if the server supports it.

If you disable or do not configure this setting, the sync app will attempt to use legacy network authentication schemes that the server supports.

Enabling this policy sets the following registry key:

```
[HKLM\SOFTWARE\Policies\Microsoft\OneDrive]"SharePointOnPremOIDC"=dword:00000001
```

Enable sync health reporting for OneDrive

Applies to: Group Policy, Intune

This policy lets the OneDrive sync app report sync device and health data included in administrative sync reports.

If you enable this setting, the OneDrive sync app reports device and health data to include in administrative sync reports. You must enable this setting on the devices you want to get reports from.

If you disable or don't configure this setting, OneDrive sync app device and health data won't appear in the admin reports.

Enabling this policy sets the following registry key value to 1:

```
[HKLM\SOFTWARE\Policies\Microsoft\OneDrive]"EnableSyncAdminReports"=dword:00000001
```

Exclude specific kinds of files from being uploaded

Applies to: Group Policy, Intune

This setting lets you enter keywords to prevent the OneDrive sync app (OneDrive.exe) from uploading certain files to OneDrive or SharePoint. You can enter complete names, such as "setup.exe", or use the asterisk (*) as a wildcard character to represent a series of characters, such as *.pst. Keywords aren't case-sensitive.

> **Note**
>
> The OneDrive sync app doesn't sync .tmp and .ini files.

If you enable this setting, the sync app doesn't upload new files that match the keywords you specified. No errors appear for the skipped files, and the files remain in the local OneDrive folder.

> **Note**

This setting will only block files that match your specification. It won't apply to existing files that are renamed to match the specified keywords. Additionally, new files that are created inside the synced folder and named to match the specified keywords will also not be blocked.

In File Explorer, the files appear with an "Excluded from sync" icon in the **Status** column. The OneDrive sync app must be restarted after this setting is enabled, for the setting to take effect.

Users will also see a message in the OneDrive activity center that explains why the files aren't syncing.

> **Note**
>
> Users can still browse to their OneDrive in a web browser to upload a file that has been excluded from their local OneDrive folder. We recommend that users remove the local file after doing this upload because having a file with the same name in the same folder will result in a sync conflict with the skipped file.

If you disable or don't configure this setting, all supported files in all synced folders will be uploaded.

Enabling this policy creates a list of strings under the following path:

`HKLM\SOFTWARE\Policies\Microsoft\OneDrive\EnableODIgnoreListFromGPO`

> **Note**
>
> This setting gives you more flexibility than the Block syncing of specific file types setting in the admin center. Also, with this setting, users don't see errors for the excluded files. This setting doesn't support upload of Office files that are being excluded. All other file types are supported.

> **Note**

The sync app combines the exclusions from this setting with Microsoft's default list and with exclusions that users add in OneDrive settings. Users can't remove exclusions that you set with this setting. To turn off the default list, see Disable the default ignored extension and folder lists. To prevent users from changing exclusions, see Prevent users at your organization from changing the default ignored extension and folder lists.

Exclude specific kinds of folders from being uploaded

Applies to: Group Policy

This setting lets you enter complete folder names to prevent the OneDrive sync app (OneDrive.exe) from uploading matching folders to OneDrive or SharePoint. Folder-name matching isn't case-sensitive. For example, enter "PowerShell" to exclude folders named "PowerShell". Wildcards aren't supported.

If you enable this setting, the sync app doesn't upload new folders that match the names you specified. New files created in an existing matching folder also aren't uploaded. No errors appear for the skipped folders, and the folders remain in the local OneDrive folder.

> **Important**
>
> This setting doesn't retroactively remove a folder or its existing content from OneDrive or SharePoint. Moving files that are already syncing into an excluded folder isn't supported.

The OneDrive sync app must be restarted after this setting is enabled or changed for the setting to take effect.

If you disable or don't configure this setting, the sync app uploads all supported folders. Removing an exclusion can cause matching local content to begin uploading. Review the local content before removing a rule.

Enabling this policy creates a list of strings under the following path:

`HKLM\SOFTWARE\Policies\Microsoft\OneDrive\EnableODIgnoreFolderListFromGPO`

Hard-delete the contents of a folder shortcut when unmounted

Applies to: Group Policy

This setting determines the behavior of the Sync client when it encounters a request to unmount a folder shortcut (a folder added to OneDrive via "Add shortcut to OneDrive").

If you enable this setting, when an unmount of a folder shortcut is received, the Sync client will hard-delete all the contents of the folder.

If you disable or do not configure this setting, Sync will by default move the contents of the unmounted folder to the recycle bin.

Enabling this policy sets the following registry key value to 1:

`[HKLM\SOFTWARE\Policies\Microsoft\OneDrive]"AddedFolderHardDeleteOnUnmount"=dword:00000001`

Hard-delete the contents of a folder shortcut when user loses permissions to the folder

Applies to: Group Policy

This setting determines the behavior of the Sync client when the user loses permissions to a folder shortcut (a folder added to OneDrive via "Add shortcut to OneDrive").

If you enable this setting, when the Sync client detects that the user lost permissions to a folder shortcut, the Sync client will hard-delete all the contents of the folder and the folder itself.

If you disable or do not configure this setting, Sync will by default mark the folder in error and prompt the user to remove it. When the user confirms the removal, the contents of the folder are moved to the recycle bin.

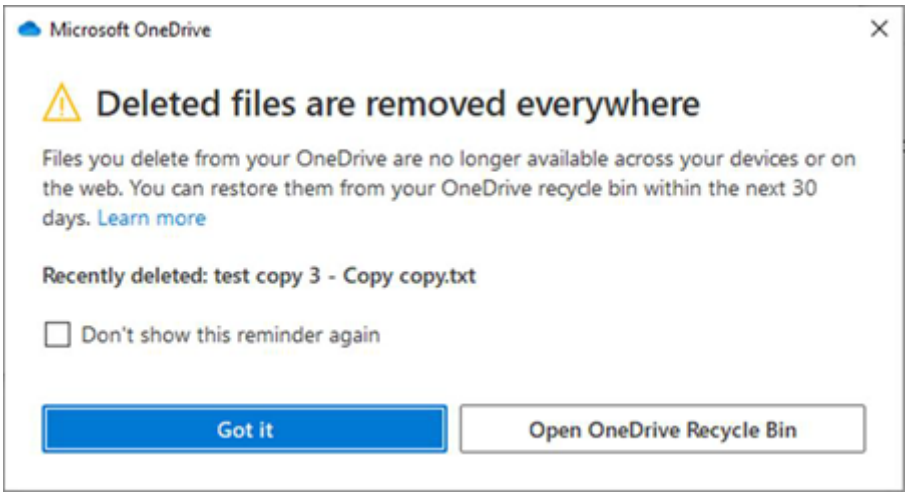
Enabling this policy sets the following registry key value to 1:

`[HKLM\SOFTWARE\Policies\Microsoft\OneDrive]"AddedFolderUnmountOnPermissionsLoss"=dword:00000001`

Hide the "Deleted files are removed everywhere" reminder

Applies to: Group Policy, Intune

When a user deletes local files from a synced location, a warning message appears that the files will no longer be available across all the devices of the user and on the web. This setting lets you hide the warning message.



If you enable this setting, users won't see the **Deleted files are removed everywhere** reminder when they delete files locally. (This reminder is called "Deleted files are removed for everyone" when a user deletes files from a synced team site.)

If you disable or don't configure this setting, the reminder appears until users select **Don't show this reminder again**.

Enabling this policy sets the following registry key value to 1:

`HKLM\SOFTWARE\Policies\Microsoft\OneDrive\DisableFirstDeleteDialog =dword:00000001`

Hide toast and activity center notifications that prompt users to sign in to the OneDrive sync app with existing credentials

Applies to: Group Policy, Intune

This setting determines whether a user will be prompted to sync their Consumer files when a Microsoft Account (MSA) is detected on the device.

If you enable this setting, users will not be prompted to sign in with their MSA and sync their Consumer files. Users can still manually configure their Consumer accounts to sync their OneDrive Consumer files. Enabling this policy sets the following registry key value to 1:

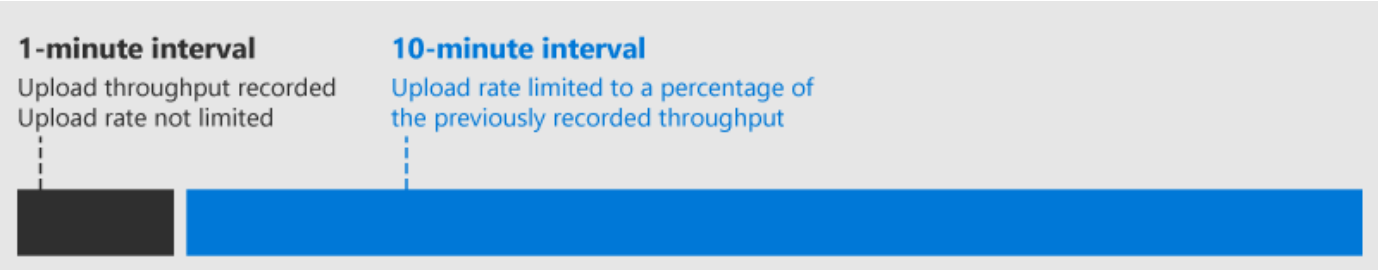
`[HKLM\SOFTWARE\Policies\Microsoft\OneDrive]"DisableNewAccountDetection"=dword:00000001`

If you disable this setting or do not configure it, users will be prompted to sign in with their MSA and sync their Consumer files.

Limit the sync app upload rate to a percentage of throughput

Applies to: Group Policy, Intune

This setting lets you balance the performance of different upload tasks on a computer by specifying the percentage of the computer's upload throughput that the OneDrive sync app (OneDrive.exe) can use to upload files. Setting this throughput as a percentage lets the sync app respond to both increases and decreases in throughput. The lower the percentage you set, the slower the files get uploaded. We recommend a value of 50% or higher. The sync app periodically uploads without restriction for one minute and then slows down to the upload percentage you set. This pattern lets small files upload quickly while preventing large uploads from dominating the computer's upload throughput. We recommend enabling this setting temporarily when you roll out Silently move Windows known folders to OneDrive, or Prompt users to move Windows known folders to OneDrive to control the network impact of uploading known folder contents.



> ⓘ **Note**
>
> The maximum throughput value detected by the sync app can sometimes be higher or lower than expected because of the different traffic-throttling mechanisms that your Internet Service Provider (ISP) might use. For information about estimating the network bandwidth you need for a sync, see Network utilization planning for the OneDrive sync app.

If you enable this setting and enter a percentage (from 10 to 99) in the **Bandwidth** box, computers use the percentage of upload throughput that you specify when uploading files to OneDrive, and users can't change it.

Enabling this policy sets the following registry key to a value described in the following example:

```
[HKLM\SOFTWARE\Policies\Microsoft\OneDrive]"AutomaticUploadBandwidthPercentage"=dword:00000032
```

The previous registry key sets the upload throughput percentage to 50, using the hexadecimal value for 50, which is 00000032.

If you disable or don't configure this setting, users can choose to limit the upload rate to a fixed value (in KB/second), or set it to **Adjust automatically**, which sets the upload rate to 70% of

throughput. For information about the end-user experience, see Change the OneDrive sync app upload or download rate.

> **Important**
>
> If you enable or disable this setting, and then change it back to **Not Configured**, the last configuration remains in effect. We recommend enabling this setting instead of **Limit the sync app upload speed to a fixed rate** to limit the upload rate. You shouldn't enable both settings at the same time.

Prevent the sync app from automatically signing in users with existing credentials

Applies to: Group Policy, Intune

This setting determines whether or not the Sync client can automatically sign in.

If you enable this setting, it prevents Sync from automatically signing in with an existing Microsoft Entra credential that is made available to Microsoft applications.

If you disable or don't configure this setting, Sync will automatically sign in.

Enabling this policy sets the following registry key:

```
[HKLM\SOFTWARE\Policies\Microsoft\OneDrive]"DisableAutoConfig"=dword:value
```

Where the value is a bitmask:

- `1` = Prevent automatic sign-in with Microsoft Entra ID (AAD) credentials
- `2` = Prevent automatic sign-in with Microsoft account (MSA) credentials
- `3` = Prevent automatic sign-in with both AAD and MSA credentials

Prevent the sync app from generating network traffic until users sign in

Applies to: Group Policy, Intune

This setting lets you block the OneDrive sync app (OneDrive.exe) from generating network traffic (checking for updates) until users sign in to OneDrive or start syncing files on their computer.

If you enable this setting, users must sign in to the OneDrive sync app on their computer, or select to sync OneDrive or SharePoint files on the computer, for the sync app to start automatically.

If you disable or don't configure this setting, the OneDrive sync app starts automatically when users sign in to Windows.

> **Important**
>
> If you enable or disable this setting, and then change it back to **Not Configured**, the last configuration remains in effect.

Enabling this policy sets the following registry key value to 1:

`[HKLM\SOFTWARE\Policies\Microsoft\OneDrive]"PreventNetworkTrafficPreUserSignIn"=dword:00000001`

Prevent users at your organization from changing the default ignored extension and folder lists

Applies to: Group Policy

By default, users can add file extensions to exclude from upload in OneDrive settings, and remove entries from Microsoft's default list. This setting keeps exclusions under administrator control.

If you enable this setting:

- Users can't add or remove exclusions in OneDrive settings. The default list and the exclusions that you configure by policy are shown, but users can't change them.
- Exclusions that users added earlier aren't applied.
- Default entries that users removed earlier are applied again.

The OneDrive sync app must be restarted after this setting is enabled for the setting to take effect.

If you disable or don't configure this setting, users can add and remove exclusions in OneDrive settings. Users can't change exclusions that you configure with Exclude specific kinds of files from being uploaded or Exclude specific kinds of folders from being uploaded.

This setting applies only to work or school accounts.

Enabling this policy sets the following registry key value to 1:

```
[HKLM\SOFTWARE\Policies\Microsoft\OneDrive]"DisableChangesToODIgnoreList"=dword:00000001
```

Prevent users at your organization from enabling offline mode in OneDrive on the web

Applies to: Group Policy

By default, offline mode is turned on for users of OneDrive on the web. If you enable this policy, offline mode in OneDrive on the web will be disabled for all the users on the device.

Enabling this policy sets the following registry key value to 1:

```
[HKLM\SOFTWARE\Policies\Microsoft\OneDrive]"DisableOfflineMode"="dword:1"
```

To re-enable offline mode in OneDrive on the web for users at your organization, set the following registry key value to 0:

```
[HKLM\SOFTWARE\Policies\Microsoft\OneDrive]"DisableOfflineMode"="dword:0"
```

Prevent users at your organization from enabling offline mode in OneDrive on the web for libraries and folders that are shared from other organizations

Applies to: Group Policy

Enabling this setting prevents users at your organization from enabling offline mode for libraries and folders that are shared from other organizations. After the setting is enabled (by entering value **1**) on a computer, libraries and folders shared by other organizations won't have the option of enabling offline mode when working with them in OneDrive on the web. Disable the setting (by entering the value **0**) to allow your users to enable or disable offline mode in OneDrive on the web when working with libraries and folders that are shared from other organizations.

Prevent users at your organization from enabling offline mode in OneDrive on the web for libraries and folders that are shared from other organizations with:

```
[HKLM\SOFTWARE\Policies\Microsoft\OneDrive]"DisableOfflineModeForExternalLibraries"="dword:1"
```

Re-enable offline mode in OneDrive on the web for libraries and folders that are shared from other organizations with:

`[HKLM\SOFTWARE\Policies\Microsoft\OneDrive]"DisableOfflineModeForExternalLibraries"="dword:0"`

Prevent users from fetching files remotely

> **Note**
>
> This setting has been removed from the OneDrive administrative template files (ADMX/ADML) because the Fetch files feature was deprecated on July 31, 2020.

Prevent users from moving their Windows known folders to OneDrive

Applies to: Group Policy, Intune

This setting prevents users from moving their Documents, Pictures, and Desktop folders to any OneDrive account.

> **Note**
>
> Moving known folders to personal OneDrive accounts is already blocked on domain-joined PCs.

If you enable this setting, users aren't prompted with a window to protect their important folders, and the *Manage backup* command is disabled. If the users have already moved their known folders, the files in those folders remain in OneDrive. To redirect the known folders back to the user's device, select **No**. This setting doesn't take effect if you've enabled **Prompt users to move Windows known folders to OneDrive** or **Silently move Windows known folders to OneDrive**.

If you disable or don't configure this setting, users can choose to move their known folders.

Enabling this policy sets the following registry key value to 1:

`[HKLM\SOFTWARE\Policies\Microsoft\OneDrive]"KFMBlockOptIn"=dword:00000001`

To redirect the known folders back to the user's device and enable this policy, set the following registry key value to 2:

`[HKLM\SOFTWARE\Policies\Microsoft\OneDrive]"KFMBlockOptIn"=dword:00000002`

> **Note**
>
> This policy's registry value name (KFMBlockOptIn) differs from the policy name (BlockKnownFolderMove). When verifying this policy is applied, look for `KFMBlockOptIn` in the registry.

Prevent users from redirecting their Windows known folders to their PC

Applies to: Group Policy, Intune

This setting forces users to keep their Documents, Pictures, and Desktop folders directed to OneDrive.

If you enable this setting, the **Stop protecting** button in the **Set up protection of important folders** window is disabled, and users receive an error if they try to stop syncing a known folder.

If you disable or don't configure this setting, users can choose to redirect their known folders back to their PC.

Enabling this policy sets the following registry key value to 1:

```
[HKLM\SOFTWARE\Policies\Microsoft\OneDrive]"KFMBlockOptOut"=dword:00000001
```

Prevent users from syncing libraries and folders shared from other organizations

Applies to: Group Policy, Intune

The B2B Sync feature of the OneDrive sync app lets users at an organization to sync OneDrive and SharePoint libraries and folders shared with them from another organization. For more information, see B2B Sync.

Enabling this setting prevents users at your organization from being able to use B2B Sync. After the setting is enabled (by entering value 1) on a computer, the sync app doesn't sync libraries and folders shared from other organizations. Modify the setting to the disabled state (by entering value 0) to restore B2B Sync capability for your users.

Prevent B2B Sync with:

```
[HKLM\SOFTWARE\Policies\Microsoft\OneDrive] "BlockExternalSync"=dword:1
```

Restore B2B Sync with:

```
[HKLM\SOFTWARE\Policies\Microsoft\OneDrive] "BlockExternalSync"=dword:0
```

Prompt users to confirm when they delete shared content

Applies to: Group Policy, Intune

When local synced files, which multiple users have access to, are deleted, a dialog appears informing the user that other users will no longer have access to that content and asking them to confirm the action before OneDrive completes the deletes online. After confirming, deletes of other shared content, for a short period of time, do not trigger additional confirmations. Other content will continue to sync. Enable this setting to prevent users from hiding the confirmation dialog. Each time the user deletes shared content, their confirmation is required before the item is deleted for everyone online. Disable this setting to not show the delete confirmation message. Deletes will immediately be made in the cloud.

Enabling this policy sets the following registry key to the value shown in the following example:

```
[HKLM\SOFTWARE\Policies\Microsoft\OneDrive]"SharedContentDeleteConfirmation"=dword:1
```

Prompt users to move Windows known folders to OneDrive

Applies to: Group Policy, Intune

This setting shows a window that prompts users to move their Documents, Pictures, and Desktop folders to OneDrive.

If you enable this setting and provide your tenant ID, users who are syncing their OneDrive see the previous window when they're signed in. If they close the window, a reminder notification appears in the Activity Center until they move all their known folders. If users have already redirected their known folders to a different OneDrive account, they're prompted to direct the folders to the account for your organization (leaving existing files behind).

If you disable or don't configure this setting, the window that prompts users to protect their important folders doesn't appear.

Enabling this policy sets the following registry key to the value shown in the following example:

```
[HKLM\SOFTWARE\Policies\Microsoft\OneDrive]"KFMOptInWithWizard"="1111-2222-3333-4444"
```

where "1111-2222-3333-4444" is the tenant ID.

For information and recommendations, see Redirect and move Windows known folders to OneDrive.

Prompt users when they delete multiple OneDrive files on their local computer

Applies to: Group Policy, Intune

This policy sets the threshold for how many files a user can delete from a local OneDrive folder before the user is notified that the files will also be deleted from the cloud.

If you enable this policy, users see a notification if they delete more than the specified number of files from OneDrive on their local computer. The user is given the option to continue to remove the cloud files, or restore the local files.

> **Note**
>
> Even if you enable this policy, users won't receive notifications if they've checked the **Always remove files** checkbox on a previous notification, or if they've cleared the **Notify me when many files are deleted in the cloud** checkbox in OneDrive sync app settings.

If you disable this policy, users won't receive a notification when they delete numerous OneDrive files on their local computer.

If you don't configure this policy, users will see a notification when they delete more than 200 files within a short period of time.

Enabling this policy sets the following registry key value to a number from 0 through 100000:

`[HKLM\SOFTWARE\Policies\Microsoft\OneDrive]"LocalMassDeleteFileDeleteThreshold"`

Require users to confirm large delete operations

Applies to: Group Policy, Intune

This setting makes users confirm that they want to delete files in the cloud when they delete a large number of synced files.

If you enable this setting, a warning always appears when users delete a large number of synced files. If a user doesn't confirm a delete operation within seven days, the files aren't deleted.

If you disable or don't configure this setting, users can choose to hide the warning, and always delete files in the cloud.

Enabling this policy sets the following registry key value to 1:

```
[HKLM\SOFTWARE\Policies\Microsoft\OneDrive]"ForcedLocalMassDeleteDetection"=dword:00000001
```

Set a custom name for the OneDrive folder

Applies to: Group Policy

This setting lets you customize the local OneDrive sync root folder name on users' computers. By default, the folder name is *OneDrive - {organization name}*. Shortening this name increases the available path length for nested folders and files.

If you enable this setting and provide a custom folder name, OneDrive will use that name when creating the sync root folder for new users. Users who are already syncing will need to unlink and relink their account for the change to take effect.

If you disable this setting, the folder name will revert to *OneDrive - {organization name}*. Users who were using a custom folder name will need to unlink and relink their account for the change to take effect.

If you do not configure this setting, the default folder name will be used.

To configure the setting, in the **Options** box, select **Show**, enter your tenant ID in the **Value Name** field, and then enter the custom folder name in the **Value** field.

Enabling this policy sets the following registry key to the value shown in the following example:

```
[HKLM\SOFTWARE\Policies\Microsoft\OneDrive\CustomSyncRootFolderName]
"TenantID"="CustomFolderName"
```

Best practices

- For new users, change sync root folder name before setting up OneDrive, so the users don't need to unlink and relink their accounts.
- For existing users, users will need to unlink and relink their account. To avoid file duplications, users should follow the steps below.
  - Go to **OneDrive settings** and click on **Manage backup** button. Click on **Stop backup and choose where to keep files.** Choose **Only in OneDrive** option**.**

- The users must then unlink their OneDrive account before the new local OneDrive sync root folder name is set.
- After the new local OneDrive sync root folder name is set, users must relink their account, and they can start backup when they sign back into their OneDrive account.

- Use as few characters as possible to minimize the likelihood of hitting max path errors.
- To further reduce the local path length, customize the default location for the OneDrive folder: Set the default location for the OneDrive folder.

> **Important**
>
> - You must provide at least one character for the custom folder name.
> - The custom folder name cannot be "OneDrive".
> - The full OneDrive sync root folder path (for example, `C:\Users\{alias}\OneDrive - {organization name}`) cannot exceed 120 characters.
> - Custom folder names cannot contain characters that are invalid for Windows folders. For a list of unsupported characters, see Invalid characters.

Set the maximum size of a user's OneDrive that can download automatically

Applies to: Group Policy, Intune

This setting is used with Silently sign in users to the OneDrive sync app with their Windows credentials on devices that don't have **OneDrive Files On-Demand** enabled. Any user who has a OneDrive that's larger than the specified threshold (in MB) is prompted to choose the folders they want to sync before the OneDrive sync app (OneDrive.exe) downloads the files.

To enter the tenant ID and the maximum size in MB (from 0 to 4294967295), in the **Options** box, select **Show**. The default value is **500**.

Enabling this policy sets the following registry key:

`[HKLM\SOFTWARE\Policies\Microsoft\OneDrive\DiskSpaceCheckThresholdMB]"1111-2222-3333-4444"=dword:0005000`

where "1111-2222-3333-4444" is the tenant ID and "0005000" sets a threshold of "5000 MB".

Set the sync app update ring

Applies to: Group Policy, Intune

We release OneDrive sync app (OneDrive.exe) updates to the public through three rings - first to Insiders, then Production, and finally Deferred. This setting lets you specify the ring for users in your organization. When you enable this setting and select a ring, users can't change it.

"Insiders ring" users receive builds that let them preview new features coming to OneDrive.

"Production ring" users get the latest features as they become available. This ring is the default one.

"Deferred ring" users get new features, then bug fixes, and performance improvements last. This ring lets you deploy updates from an internal network location, and control the timing of the deployment (within a 60-day window).

> **Important**
>
> We recommend selecting several people in your IT department as early adopters to join the "Insiders ring" and receive features early. We recommend leaving everyone else in the organization in the default "Production ring" to ensure they receive bug fixes and new features in a timely fashion. See all our recommendations for configuring the sync app.

If you disable or don't configure this setting, users can join the Windows Insider program or the Office Insider program to get updates on the "Insiders ring".

Enabling this policy sets the following registry key:

```
[HKLM\SOFTWARE\Policies\Microsoft\OneDrive]"GPOSetUpdateRing"=dword:0000000X
```

Set the value **4** for Insider, **5** for Production, or **0** for Deferred. When you configure this setting to **5** for Production, or **0** for Deferred, the **Get OneDrive Insider preview updates before release** checkbox in the sync app doesn't appear on the **Settings** > **About** tab.

For more information on the builds currently available in each ring, see the release notes. For more information about the update rings and how the sync app checks for updates, see The OneDrive sync app update process.

Silently move Windows known folders to OneDrive

Applies to: Group Policy, Intune

Use this setting to redirect and move your users' Documents, Pictures, and/or Desktop folders to OneDrive without any user interaction.

> **Note**
>
> We recommend deploying the silent policy for existing devices and new devices while limiting the deployment of existing devices to 1,000 devices a day and not exceeding 4,000 devices a week. We also recommend using this setting together with Prompt users to move Windows known folders to OneDrive. If moving the known folders silently doesn't succeed, users will be prompted to correct the error and continue. See all our recommendations for configuring the sync app.

You can move all folders at once or select the folders you want to move. After a folder is moved, this policy won't affect that folder again, even if you clear the checkbox for the folder.

If you enable this setting and provide your tenant ID, you can choose whether to display a notification to users after their folders have been redirected. If you disable or don't configure this setting, your users' known folders aren't silently redirected to OneDrive.

Enabling this policy sets the following registry keys:

`[HKLM\SOFTWARE\Policies\Microsoft\OneDrive]"KFMSilentOptIn"="1111-2222-3333-4444"`

where "1111-2222-3333-4444" is a string value representing the tenant ID.

`[HKLM\SOFTWARE\Policies\Microsoft\OneDrive]"KFMSilentOptInWithNotification"=dword:00000001`

Setting this value to **1** shows a notification after a successful redirection.

If you don't set any of the following policies, then the default policy will move all the folders (Desktop, Documents, and Pictures) into OneDrive. If you want to specify the folders to move, then you can set any combination of the following policies:

`[HKLM\SOFTWARE\Policies\Microsoft\OneDrive]"KFMSilentOptInDesktop"=dword:00000001`: Setting this value to **1** will move the Desktop folder.

`[HKLM\SOFTWARE\Policies\Microsoft\OneDrive]"KFMSilentOptInDocuments"=dword:00000001`: Setting this value to **1** will move the Documents folder.

`[HKLM\SOFTWARE\Policies\Microsoft\OneDrive]"KFMSilentOptInPictures"=dword:00000001`: Setting this value to **1** will move the Pictures folder.

> **Important**
>
> The Group Policy object **User Configuration** > **Administrative Templates** > **Desktop** > **Prohibit User from manually redirecting Profile Folders** must be set to **Disabled** or **Not configured**. Folders will not move to OneDrive if set to **Enabled**.

For more information, see Redirect and move Windows known folders to OneDrive.

Silently sign in users to the OneDrive sync app with their Windows credentials

Applies to: Group Policy, Intune

> **Important**
>
> Microsoft Authentication Library (MSAL) is enabled automatically when the sync user is provisioned via `SilentAccountConfig`; so you don't have to enable it separately.
>
> The *Silently sign in users to the OneDrive sync app with their Windows credentials* feature works for computers that are joined to Microsoft Entra ID.

If you enable this setting, users who are signed in on a PC that's joined to Microsoft Entra ID can set up the sync app without entering their account credentials. Users will still be shown OneDrive Setup so that they can select folders to sync and change the location of their OneDrive folder. If a user is using the previous OneDrive for Business sync app (Groove.exe), the new sync app attempts to take over syncing the user's OneDrive from the previous app, and preserves the user's sync settings. This setting is frequently used together with Set the maximum size of a user's OneDrive that can download automatically on PCs that don't have **OneDrive Files On-Demand** but have Set the default location for the OneDrive folder.

> **Important**
>
> We recommend enabling silent account configuration when you configure the sync app. See all our recommendations for configuring the sync app.

Enabling this policy sets the following registry key value to 1:

```
[HKLM\SOFTWARE\Policies\Microsoft\OneDrive]"SilentAccountConfig"=dword:00000001
```

For more information about this feature, including troubleshooting steps, see Silently configure user accounts. Let us know if you have feedback on this feature or encounter any issues. Right-click the OneDrive icon in the notification area and select **Report a problem**. Tag any feedback with "SilentConfig" so that your feedback is sent directly to engineers working on this feature.

Specify SharePoint Server URL and organization name

Applies to: Group Policy, Intune

This setting is for customers who have SharePoint Server 2019. For information about using the new OneDrive sync app with SharePoint Server 2019, see Configure syncing with the new OneDrive sync app.

Enabling this policy sets the following registry key:

```
[HKLM\SOFTWARE\Policies\Microsoft\OneDrive]"SharePointOnPremFrontDoorUrl"="https://sharepoint.contoso.local/"
```

> **Important**
>
> Enter the URL with a trailing slash (/). If the trailing slash is missing, sync setup can fail even when the URL is otherwise correct. For example, use `https://sharepoint.contoso.local/`, not `https://sharepoint.contoso.local`.

Specify the Application ID URI for your Entra application for OIDC

Applies to: Group Policy

This setting allows you to specify an Application ID URI for your Entra application for OIDC if it is different from your SharePoint Server URL. To use this setting, you must also enable Enable OpenID Connect (OIDC) authentication for syncing content from an on-prem SharePoint Server using the OneDrive sync app. This setting affects only OneDrive for Business sync functionality. It does not impact syncing team sites in SharePoint Online.

If you enable this setting and provide the Application ID URI, this value will be used for requests to the SharePoint Server.

If you disable or do not configure this setting, the SharePoint Server URL will be used as the Application ID URI instead.

Enabling this policy sets the following registry key:

`[HKLM\SOFTWARE\Policies\Microsoft\OneDrive]"SharePointOnPremApplicationIdUri"="your-application-id-uri"`

Specify the OneDrive location in a hybrid environment

Applies to: Group Policy, Intune

This setting is for customers who have SharePoint Server 2019. For information about using the new OneDrive sync app with SharePoint Server 2019, see Configure syncing with the new OneDrive sync app.

Use OneDrive Files On-Demand

Applies to: Group Policy, Intune

This setting lets you control whether **OneDrive Files On-Demand** is enabled for your organization. **OneDrive Files On-Demand** helps you save storage space on your users' computers, and minimize the network impact of a sync. The feature is available to users running Windows 10 Fall Creators update (version 1709 or later). For more information, see Save disk space with OneDrive Files On-Demand for Windows 10.

> **Important**
>
> We recommend keeping **OneDrive Files On-Demand** enabled. **See all our recommendations for configuring the sync app.**

If you enable this setting, new users who set up the sync app see online-only files in File Explorer, by default. File contents don't download until a file is opened. If you disable this setting, Windows 10 users have the same sync behavior as users of previous versions of Windows, and aren't able to turn on **OneDrive Files On-Demand**. If you don't configure this setting, users can turn on or off the **OneDrive Files On-Demand** option.

Enabling this policy sets the following registry key value to 1:

```
[HKLM\SOFTWARE\Policies\Microsoft\OneDrive]"FilesOnDemandEnabled"=dword:00000001
```

Meet Windows and OneDrive sync app requirements and still can't see **OneDrive Files On-Demand** option available at "Settings"? Ensure the service "Windows Cloud Files Filter Driver" start type is set to **2** (AUTO_START). Enabling this feature sets the following registry key value to 2:

```
[HKLM\SYSTEM\CurrentControlSet\Services\CldFlt]"Start"=dword:00000002
```

Warn users who are low on disk space

Applies to: Group Policy, Intune

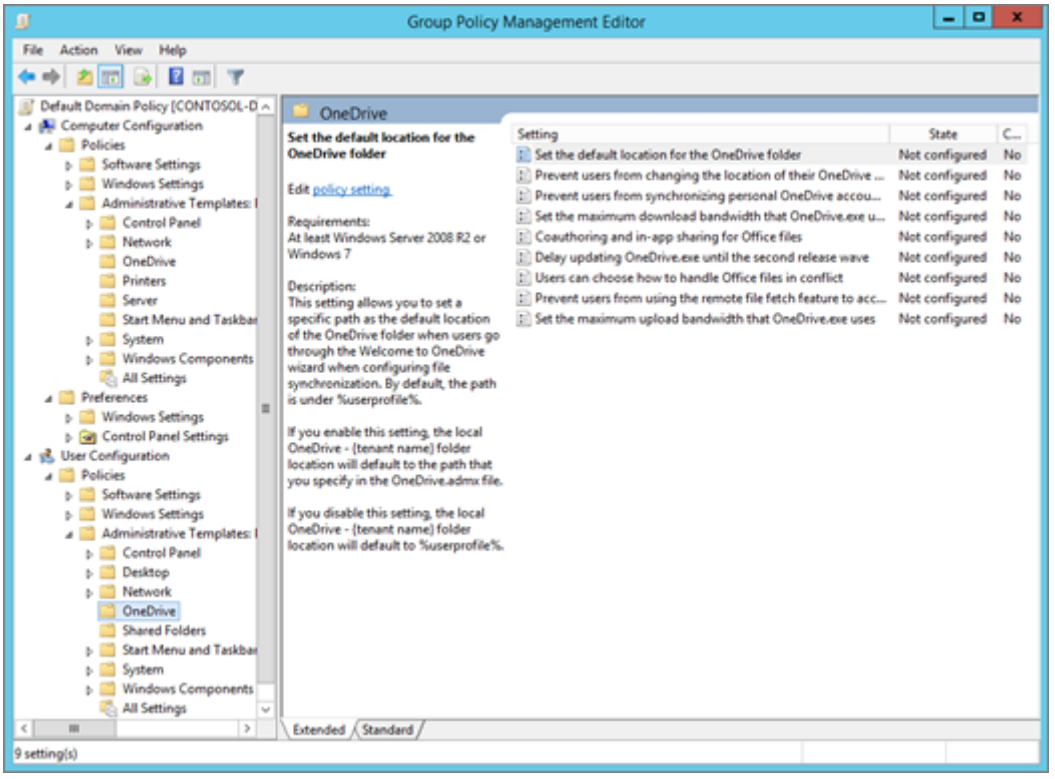
This setting lets you specify a minimum amount of available disk space, and warn users when the OneDrive sync app (OneDrive.exe) downloads a file that causes them to have less than this amount. Users are prompted with options to help free up space.

Enabling this policy sets the following registry key value to a number from 0 through 10240000:

```
[HKLM\SOFTWARE\Policies\Microsoft\OneDrive] "WarningMinDiskSpaceLimitInMB"=dword:00000000
```

User Configuration policies

Find *User Configuration policies* under User Configuration\Policies\Administrative Templates\OneDrive.



Configure team site libraries to sync automatically

Applies to: Group Policy, Intune

> **Note**
>
> This policy can also be configured under Computer Configuration.

This setting lets you specify SharePoint team site libraries to sync automatically the next time users sign in to the OneDrive sync app (OneDrive.exe), within an eight-hour window, to help distribute network load. To use this setting, the computer must be running Windows 10 Fall Creators Update (version 1709) or later, and you must enable **OneDrive Files On-Demand**. This feature isn't enabled for on-premises SharePoint sites.

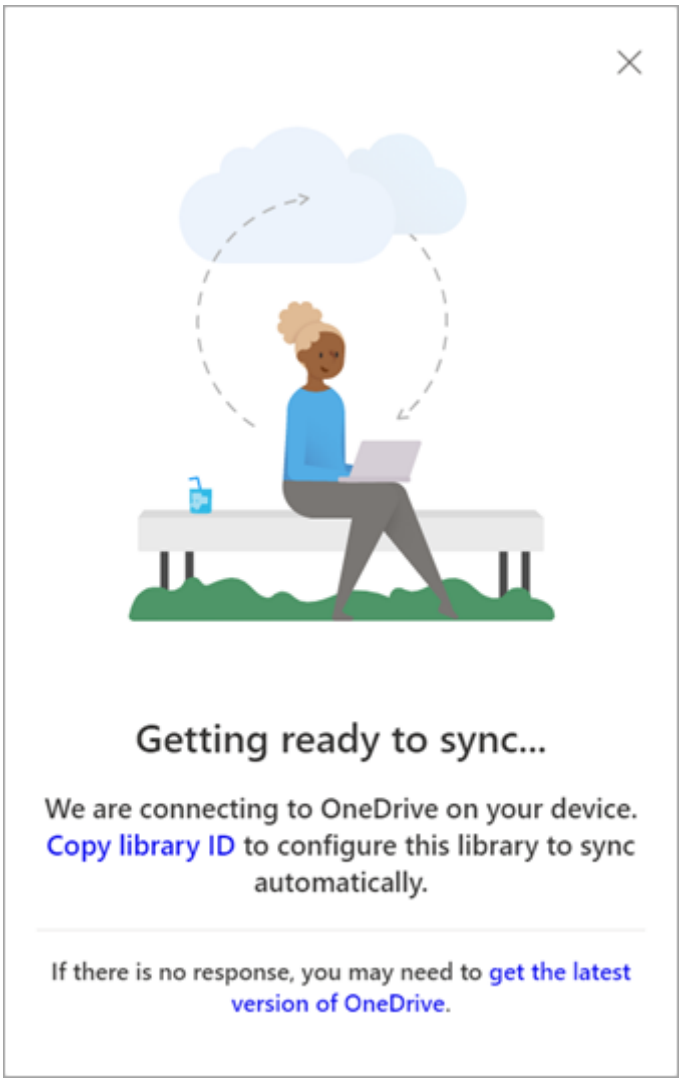
> **Important**
>
> For performance reasons, we recommend not enabling this setting to libraries with more than 5,000 files or folders. Don't enable this setting to the same library with more than 1,000 devices.

If you enable this setting, the OneDrive sync app automatically syncs the contents of the libraries you specified as online-only files the next time the user signs in. The user isn't able to stop syncing the libraries.

If you disable this setting, team site libraries that you've specified aren't automatically synced for new users. Existing users can choose to stop syncing the libraries, but the libraries won't stop syncing automatically.

To configure the setting, in the **Options** box, select **Show**, enter a friendly name to identify the library in the **Value Name** field, and then enter the entire library ID (tenantId=xxx&siteId=xxx&webId=xxx&listId=xxx&webUrl=httpsxxx&version=1) in the **Value** field.

To find the library ID, sign in as a global or SharePoint administrator in Microsoft 365, browse to the library, and select **Sync**. In the **Starting sync** dialog, select the **Copy library ID** link.



The special characters in this copied string are in Unicode and must be converted to ASCII according to the following table.

Expand table

Find	Replace
%2D	-
%7B	{
%7D	}
%3A	:
%2F	/
%2E	.

Alternatively, you can run the following command in PowerShell, replacing "Copied String" with the library ID:

PowerShell

```
[uri]::UnescapeDataString("Copied String")
```

Enabling this policy sets the following registry key, using the entire URL from the library ID you copied:

`[HKCU\Software\Policies\Microsoft\OneDrive\TenantAutoMount]"LibraryName"="LibraryID"`

Continue syncing on metered networks

Applies to: Group Policy, Intune

This setting lets you turn off the auto-pause feature when devices connect to metered networks.

If you enable this setting, syncing continues when devices are on a metered network. OneDrive doesn't automatically pause syncing.

If you disable or don't configure this setting, syncing pauses automatically when a metered network is detected, and a notification appears. To not pause, in the notification, select **Sync Anyway**. When syncing is paused, to resume syncing, in the notification area of the taskbar, select the OneDrive cloud icon, and at the top of the Activity Center, select the alert.

Enabling this policy sets the following registry key value to 1:

`[HKCU\SOFTWARE\Policies\Microsoft\OneDrive] "DisablePauseOnMeteredNetwork"=dword:00000001`

Continue syncing when devices have battery saver mode turned on

Applies to: Group Policy, Intune

This setting lets you turn off the auto-pause feature for devices that have battery saver mode turned on.

If you enable this setting, syncing continues when users turn on battery saver mode. OneDrive doesn't automatically pause syncing.

If you disable or don't configure this setting, syncing pauses automatically when battery saver mode is detected, and a notification appears. To not pause, in the notification, select **Sync Anyway**. When syncing is paused, to resume syncing, in the notification area of the taskbar, select the OneDrive cloud icon, and at the top of the Activity Center, select the alert.

Enabling this policy sets the following registry key value to 1:

```
[HKCU\SOFTWARE\Policies\Microsoft\OneDrive] "DisablePauseOnBatterySaver"=dword:00000001
```

Deploy Restrict Known Folder Move from Office Group Policy

Applies to: Group Policy, Intune

The Restrict Known Folder Move from Office (Restrict KFM from Office) Group Policy allows administrators to control whether Office apps display prompts encouraging users to back up their files to Microsoft OneDrive.

When this policy is enabled and deployed, Office apps won't display the message bar, even if users are eligible for the Known Folder Move (KFM) feature. This policy applies only to Office apps and does not affect other OneDrive or KFM configurations. It is available in the Administrative Template files for Microsoft Office (version 5497.1000 or newer).

See Deploy Restrict Known Folder Move from Office Group Policy for more information on how to enable and deploy this policy.

Disable animation that appears during OneDrive Setup

Applies to: Group Policy, Intune

This setting lets you prevent the animation from showing during OneDrive Setup.

Enabling this policy sets the following registry key value to 1:

```
HKCU\SOFTWARE\Policies\Microsoft\OneDrive\DisableFREAnimation =dword:00000001
```

Disable the tutorial that appears at the end of OneDrive Setup

Applies to: Group Policy, Intune

This setting lets you prevent the tutorial from showing at the end of OneDrive Setup.

If you enable this setting, users don't see the tutorial after they complete OneDrive Setup.

If you disable or do not configure this setting, the tutorial will appear at the end of OneDrive Setup.

Limit the sync app download speed to a fixed rate

Applies to: Group Policy, Intune

This setting lets you configure the maximum speed at which the OneDrive sync app (OneDrive.exe) can download files. This rate is a fixed value in kilobytes per second, and applies only to syncing, not to downloading updates. The lower the rate, the slower the files download.

We recommend that you use this setting in cases where **OneDrive Files On-Demand** is NOT enabled, and where strict traffic restrictions are required, such as when you initially deploy the sync app in your organization or enable syncing of team sites. We don't recommend that you use this setting on an ongoing basis because it decreases sync app performance and negatively impacts the user experience. After the initial sync, users typically sync only a few files at a time, and it doesn't have a significant effect on network performance. If you enable this setting, computers use the maximum download rate that you specify, and users can't change it.

If you enable this setting, enter the rate (from 1 to 100000) in the **Bandwidth** box. The maximum rate is 100000 KB/s. Any input lower than 50 KB/s sets the limit to 50 KB/s, even if the UI shows a lower value.

If you disable or don't configure this setting, the download rate is unlimited, and users can choose to limit it in OneDrive sync app settings. For information about the end-user experience, see Change the OneDrive sync app upload or download rate.

Enabling this policy sets the following registry key value to a number from 50 through 100,000:

```
[HKCU\SOFTWARE\Policies\Microsoft\OneDrive] "DownloadBandwidthLimit"=dword:00000032
```

The previous registry key sets the download throughput rate limit to 50 KB, using the hexadecimal value for 50, which is 00000032.

> **Note**
>
> OneDrive.exe must be restarted on users' computers to apply this setting.

For information about estimating the network bandwidth you need for a sync, see Network utilization planning for the OneDrive sync app.

Limit the sync app upload speed to a fixed rate

Applies to: Group Policy, Intune

This setting lets you configure the maximum speed at which the OneDrive sync app (OneDrive.exe) can upload files. This rate is a fixed value in kilobytes per second. The lower the rate, the slower the computer uploads files.

If you enable this setting and enter the rate (from 1 to 100000) in the **Bandwidth** box, computers use the maximum upload rate that you specify, and users can't change it in OneDrive settings. The maximum rate is 100000 KB/s. Any input lower than 50 KB/s sets the limit to 50 KB/s, even if the UI shows a lower value.

If you disable or don't configure this setting, users can choose to limit the upload rate to a fixed value (in KB/second), or set it to **Adjust automatically** which sets the upload rate to 70% of throughput. For information about the end-user experience, see Change the OneDrive sync app upload or download rate.

We recommend that you use this setting only in cases where strict traffic restrictions are required. In scenarios where you need to limit the upload rate (such as when you roll out Known Folder Move), we recommend enabling Limit the sync app upload rate to a percentage of throughput to set a limit that adjusts to changing conditions. You shouldn't enable both settings at the same time.

Enabling this policy sets the following registry key value to a number from 50 through 100,000:

```
[HKCU\SOFTWARE\Policies\Microsoft\OneDrive]"UploadBandwidthLimit"=dword:00000032
```

The previous registry key sets the upload throughput rate limit to 50 KB, using the hexadecimal value for 50, which is 00000032.

> **Note**
>
> OneDrive.exe must be restarted on users' computers to apply this setting.

For information about estimating the network bandwidth you need for a sync, see Network utilization planning for the OneDrive sync app.

Prevent users from changing the location of their OneDrive folder

Applies to: Group Policy, Intune

This setting lets you block users from changing the location of the OneDrive folder on their computer.

To use this setting, in the **Options** box, select **Show**, and enter your tenant ID. To enable the setting, enter **1**; to disable it, enter **0**.

If you enable this setting, the **Change location** link is hidden in OneDrive Setup. The OneDrive folder is created in the default location, or in the custom location you specified if you enabled Set the default location for the OneDrive folder.

Enabling this policy sets the following registry key value to 1:

```
[HKCU\Software\Policies\Microsoft\OneDrive\DisableCustomRoot] "1111-2222-3333-4444"=dword:00000001
```

where "1111-2222-3333-4444" is the tenant ID.

If you disable this setting, users can change the location of their sync folder in OneDrive Setup.

Prevent users from syncing personal OneDrive accounts

Applies to: Group Policy, Intune

This setting lets you block users from signing in with a Microsoft account to sync their personal OneDrive files. By default, users are allowed to sync personal OneDrive accounts.

If you enable this setting, users are prevented from setting up a sync relationship for their personal OneDrive account. Users who are already syncing their personal OneDrive when you enable this setting can't continue syncing (they receive a message that syncing has stopped), but any files synced to the computer remain on the computer.

Enabling this policy sets the following registry key value to 1:

```
[HKCU\SOFTWARE\Policies\Microsoft\OneDrive]"DisablePersonalSync"=dword:00000001
```

> **Note**
>
> Mac operating system (MacOS) clients should either sign out and restart OneDrive or restart the client machine to apply this setting.

Set the default location for the OneDrive folder

Applies to: Group Policy, Intune

This setting lets you set a specific path as the default location of the OneDrive folder on users' computers. By default, the path is under %userprofile%.

If you enable this setting, the default location of the *OneDrive - {organization name}* folder is the path that you specify. To specify your tenant ID and the path, in the **Options** box, select **Show**.

This policy sets the following registry key to a string that specifies the file path:

`[HKCU\SOFTWARE\Policies\Microsoft\OneDrive\DefaultRootDir] "1111-2222-3333-4444"="{User path}"`

where "1111-2222-3333-4444" is the tenant ID.

If you disable this setting, the local *OneDrive - {organization name}* folder location defaults to %userprofile%.

> **Note**
>
> The %logonuser% environment variable won't work through Group Policy. We recommend you use %username% instead.

Start OneDrive automatically when signing in to Windows

Applies to: Group Policy, Intune

This policy overrides the user's choice, ensuring OneDrive will automatically start every time they sign in to Windows.

Enabling this policy sets the following registry key value to 1:

`[HKCU\Software\Policies\Microsoft\OneDrive]"EnableAutoStart"=dword:00000001`

See also

Deploy the new OneDrive sync app in an enterprise environment

Prevent users from installing the sync app

Allow syncing only on computers joined to specific domains

Block syncing of specific file types

Deploy and configure the new OneDrive sync app for Mac

Lists sync policies

ⓘ**Note:** The author created this article with assistance from AI. Learn more

---

Last updated on 09/29/2026

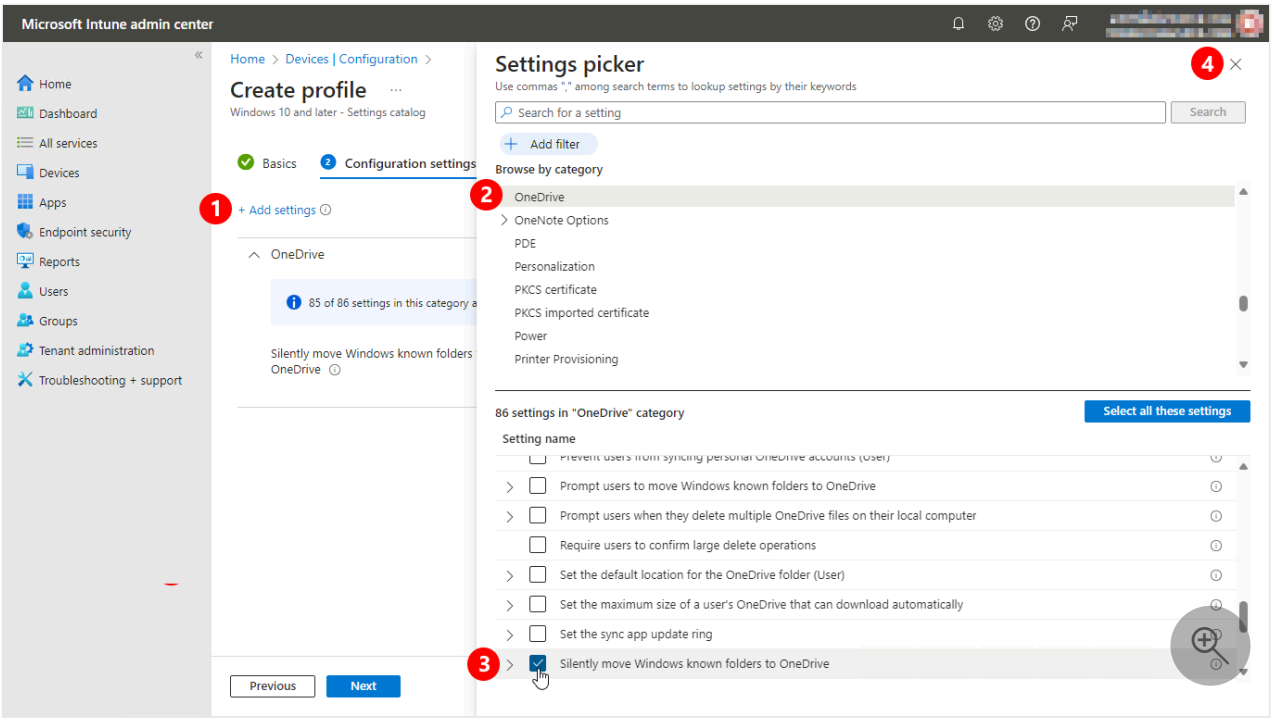
Configure settings with Intune

Article • 04/10/2025

Profiles in Microsoft Intune let you configure settings and push them to devices in your organization. The settings catalog built into Microsoft Intune make configuring the Microsoft OneDrive sync app easier than ever.

Create a profile

1. Sign in to the Microsoft Intune admin center.
2. Select **Devices** > **Configuration** > **Create**.
3. Enter the following properties:
   - **Platform**: Select **Windows 10 and later**.
   - **Profile type**: Select **Settings catalog**.
4. Select **Create**.
5. In **Basics**, enter the following properties:
   - **Name**: Enter a descriptive name for the profile. Name your profiles so you can easily identify them later. For example, a good profile name is **Windows: OneDrive**.
   - **Description**: Enter a description for the profile. This setting is optional, but recommended.
6. Select **Next**.
7. In **Configuration settings**, select **Add settings**.
8. In the settings picker, select **OneDrive** to see all the available settings.
9. Select any setting you want to configure. Or, choose **Select all these settings**. After you add your settings, close the settings picker. For info about these settings, see Use OneDrive policies. For info about the recommended settings, see Recommended sync app configuration.



10. Configure the settings the way you want, and then select **OK**.

> ⓘ **Note**
>
> Some settings require entering your tenant ID. Learn how to find it. When you're done, select **Next**.

11. Select scope tags, and then select **Next**. For information about scope tags, see Use role based access controls (RBAC) and scope tags for distributed IT.

12. In **Assignments**, include or exclude the profile from selected groups. For info about assigning profiles, see Assign user and device profiles.

> ⓘ **Note**
>
> If the profile is assigned to user groups, then configured Administrative Template Files (ADMX) settings apply to any device that the user enrolls, and signs in to. If the profile is assigned to device groups, then configured ADMX settings apply to any user that signs into that device. This assignment happens if the ADMX setting is a computer configuration (`HKEY_LOCAL_MACHINE`), or a user configuration (`HKEY_CURRENT_USER`). With some settings, a computer setting assigned to a user can also affect the experience of other users on that device.
>
> For more info, see User groups vs. device groups.

When you're done, select **Next**.

13. In **Review + create**, review your settings. When you select **Create**, your changes are saved, and the profile is assigned. The policy is also shown in the profiles list.

See also

- Use the settings catalog to configure settings on Windows
- Understanding ADMX-backed policies
- Monitor device profiles in Microsoft Intune

Query and set Files On-Demand states in Windows

Article • 09/01/2024

With OneDrive Files On-Demand, files can be in one of three states. Each of these states corresponds to a file attribute state. To query the current state of a file or folder, use the following command:

- attrib <Path to file or folder>

Scriptable commands

Use the following commands to set file and folder states.

Expand table

Files On-Demand state	File attribute state	Command
Always available	Pinned	attrib +p <path>
Locally available	Clearpin	attrib -p <path>
Online-only	Unpinned	attrib +u <path>

Note

Pinning an online-only file makes the sync app download the file contents, and unpinning a downloaded file frees up space on the device by not storing the file contents locally.
To set an online-only file or folder to "locally available," you must first set it to "always available."
If you meet the Sync app requirements and still can't see the Files On-Demand option under "Settings", make sure the service "Windows Cloud Files Filter Driver" start type is set to 2 (AUTO_START). Enabling this feature sets the following registry key value to 2.
`[HKLM\SYSTEM\CurrentControlSet\Services\CldFlt]"Start"="dword:00000002"`

Feedback

Was this page helpful? Yes No

Provide product feedback

Deploy and configure the OneDrive sync app for Mac

> **Important**
>
> The standalone OneDrive sync app is necessary for deploying and configuring Folder Backup settings. The Mac App Store OneDrive sync app is not currently supported with regards to Folder Backup.

There are two basic ways that you, as an administrator, can deploy the OneDrive sync app to Mac users in your organization:

- Install and set up the OneDrive sync app by following the instructions in Sync files with OneDrive on macOS. To install the OneDrive sync app for Mac, the user has to be an administrator on the Mac.
- Download the installer package file to your local network, and then use your software distribution tools to deploy the app to your users. By using a software distribution tool, you have more control over the deployment, including which users get the sync app and when. The OneDrive sync app for Mac uses the Apple Installer technology for installation allowing you to use the software distribution tools that you normally use to deploy software to Mac users. You can use Microsoft Intune. Other common tools are Jamf Pro, Munki, and AutoPkg. You can also use Apple Remote Desktop and AppleScript.

Manage OneDrive settings on macOS using property list (.plist) files

After the OneDrive sync app for Mac is installed, users can configure settings for the app. These settings are called preferences. As an administrator, you might want to provide users in your organization with a standard set of preferences. Preferences for the OneDrive sync app for Mac are stored in property list (.plist) files.

Expand table

	Standalone	Mac App Store
.plist location	`/Library/Preferences/com.microsoft.OneDrive.plist`	`/Library/Containers/com.microsoft.OneDrive-mac/Data/Library/Preferences/com.microsoft.OneDrive-mac.plist`
Domain	`com.microsoft.OneDrive`	`com.microsoft.OneDrive-mac`

Configure sync app settings

Configure the settings on macOS as follows:

1. Define the settings you want to change by creating a .plist file with the values needed. You can use a script to set the values.
2. Quit the OneDrive app.
3. Deploy the settings onto the local computer.
4. Refresh the preferences cache.

On the next start of OneDrive, the new settings are picked up.

Background services

> **Important**
>
> macOS 13 (Ventura) contains new privacy enhancements. Beginning with this version, by default, applications cannot run in background without explicit consent. OneDrive must run its daemon process in background. This configuration profile grants Background Service permissions to OneDrive. If you previously configured OneDrive through Microsoft Intune, we recommend you update the deployment with this configuration profile.

You need to create system configuration profiles that OneDrive needs to open at sign-in and run reliably in the background. Here's an example:

XML

```xml
<?xml version="1.0" encoding="UTF-8"?>
<!DOCTYPE plist PUBLIC "-//Apple//DTD PLIST 1.0//EN"
"http://www.apple.com/DTDs/PropertyList-1.0.dtd">
<plist version="1">
<dict>
<key>PayloadUUID</key>
<string>9FE052B5-E7B6-4BF9-94EB-DB611E0E323E</string>
<key>PayloadType</key>
<string>Configuration</string>
<key>PayloadOrganization</key>
<string>Microsoft Corporation</string>
<key>PayloadIdentifier</key>
<string>9FE052B5-E7B6-4BF9-94EB-DB611E0E323E</string>
<key>PayloadDisplayName</key>
<string>OneDrive - Background Services</string>
<key>PayloadDescription</key>
<string/>
<key>PayloadVersion</key>
<integer>1</integer>
<key>PayloadEnabled</key>
<true/>
<key>PayloadRemovalDisallowed</key>
<true/>
<key>PayloadScope</key>
<string>System</string>
<key>PayloadContent</key>
<array>
<dict>
<key>PayloadDescription</key>
<string>Background Service Management for OneDrive</string>
<key>PayloadIdentifier</key>
<string>4C3F2438-464E-43F5-8961-D4672D4A9F5D.privacy.C7B71805-73F2-43F6-A5AA-
29C9CAD728B4</string>
<key>PayloadUUID</key>
<string>F9EE3920-EAD8-4472-AF2F-52D2B57FDB31</string>
<key>Rules</key>
<array>
<dict>
<key>RuleType</key>
<string>LabelPrefix</string>
<key>RuleValue</key>
<string>com.microsoft.OneDrive</string><!--This would be com.microsoft.OneDrive-mac
for the Store app-->
</dict>
<dict>
<key>RuleType</key>
<string>BundleIdentifierPrefix</string>
<key>RuleValue</key>
<string>com.microsoft.OneDriveLauncher</string>
</dict>
</array>
<key>PayloadType</key>
<string>com.apple.servicemanagement</string>
<key>PayloadDisplayName</key>
<string>Background Service Management for OneDrive</string>
</dict>
</array>
</dict>
</plist>
```

Manage login item registration via command line

> **Important**
>
> OneDrive 26.027 and macOS 13 (Ventura) or later is required. The OneDrive app must be present at the path where the command is being executed.

OneDrive for Mac supports two command-line arguments that let administrators programmatically register or unregister the OneDrive login item. These are fire-and-exit commands: OneDrive performs the requested operation and immediately terminates without launching the full sync client.

Syntax

Bash

```bash
# Register OneDrive as a login item
open -a OneDrive --args /createloginitem

# Unregister OneDrive as a login item
open -a OneDrive --args /removeloginitem
```

Overview of settings

Use the following keys to preconfigure or change settings for your users. The keys are the same whether you run the standalone or Mac App Store edition of the sync app. However, the .plist file name and domain name are different. When you apply the settings, ensure that you target the appropriate domain depending on the edition of the sync app.

List of settings

- AddedFolderHardDeleteOnUnmount
- AddedFolderUnmountOnPermissionsLoss
- AllowTenantList
- AutomaticUploadBandwidthPercentage
- BlockExternalSync
- BlockTenantList
- DefaultFolderLocation
- DisableAutoConfig
- DisableChangesToODIgnoreList
- DisableDefaultODIgnoreList
- DisableFirstDeleteDialog
- DisableFREAnimation
- DisableOfflineMode
- DisableOfflineModeForExternalLibraries
- DisablePersonalSync
- DisableTutorial
- DownloadBandwidthLimited
- EnableODIgnore
- EnableODIgnoreFolders
- EnableSyncAdminReports
- HideDockIcon
- HydrationDisallowedApps
- KFMBlockOptIn
- KFMBlockOptOut
- KFMOptInWithWizard

- KFMSilentOptIn
- LocalMassDeleteFileDeleteThreshold
- MinDiskSpaceLimitInMB
- OpenAtLogin
- SharePointOnPremFrontDoorUrl
- SharePointOnPremPrioritizationPolicy
- SharePointOnPremTenantName
- Tier
- UploadBandwidthLimited
- WarningMinDiskSpaceLimitInMB

AddedFolderHardDeleteOnUnmount

This setting will control the contents of the folder when an unmount of an Added Folder is detected.

Set the setting's value to **True**, to hard-delete all the contents of the folder when an unmount of an Added Folder is received. Set the value to **False** or don't enable the setting to move the contents of the unmounted folder to the recycle-bin by default.

The example for this setting in the .plist file is:

XML

```xml
<key>AddedFolderHardDeleteOnUnmount</key>
<(Bool)/>
```

AddedFolderUnmountOnPermissionsLoss

This setting will control the contents of the folder and the folder itself when the Sync client detects that the user lost permissions to an Added Folder.

Set the setting's value to **True**, to hard-delete all the contents of the folder and the folder itself when the Sync client detects that the user lost permissions to an Added Folder. Set the value to **False** or don't enable the setting to default mark the folder in error and prompt the user to remove it. When the user confirms the removals, the contents of the folder are moved to the recycle-bin.

The example for this setting in the .plist file is:

XML

```xml
<key>AddedFolderUnmountOnPermissionsLoss</key>
<(Bool)/>
```

AllowTenantList

This setting prevents the users from uploading files to other organizations by specifying a list of allowed tenant IDs. If you enable this setting, the user gets an error if they attempt to add an account from an organization that isn't in the allowed tenants list. If the user is already added the account, the files stop syncing. This setting takes priority over the **BlockTenantList** setting. Do **NOT** enable both settings at the same time.

The parameter for the **AllowTenantList** key is **TenantID** and its value is a string, which determines the tenants for whom the **Allow Tenant** setting is applicable. For the setting to be complete, this parameter also requires a boolean value to be set to it. If the boolean value is set to **True**, the tenant is allowed to sync.

The example for this setting in the .plist file is:

XML

```
<key>AllowTenantList</key>
<dict>
<key>TenantId1</key>
<true/>
<key>TenantId2</key>
<true/>
</dict>
```

AutomaticUploadBandwidthPercentage

This setting enables the sync app to automatically set the amount of bandwidth that can be used for uploading files, based on available bandwidth.

To enable this setting, you must define a number between 1 and 99 that determines the percentage of bandwidth the sync app can use out of the total available bandwidth.

The example for this setting in the .plist file is:

XML

```
<key>AutomaticUploadBandwidthPercentage</key>
<integer>(Bandwidth)</integer>
```

BlockExternalSync

This setting prevents the sync app from syncing libraries and folders shared from other organizations.

Set the setting's value to **True**, to prevent the users from syncing OneDrive, SharePoint libraries, and folders with organizations other than the user's own organization. Set the value to **False** or don't enable the setting to allow the OneDrive, and SharePoint files to be synced with other organizations also.

The example for this setting in the .plist file is:

XML

```
<key>BlockExternalSync</key>
<(Bool)/>
```

BlockTenantList

This setting prevents the users from uploading files to organizations that are included in the **blocked tenant IDs** list.

If you enable this setting, the users get an error if they attempt to add an account from an organization that is blocked. If a user is already added an account for a blocked organization, the files stop syncing. This setting does **NOT** work if you have the **AllowTenantList** setting enabled. Do **NOT** enable both settings at the same time.

Enable this setting by defining IDs for the **TenantID** parameter, which determines the tenants to whom the **block tenant** setting is applicable. Also set the boolean value to **True** for the ID of every tenant you want to prevent from syncing with the OneDrive and SharePoint files and folders.

> ⓘ **Note**
>
> In the list, inclusion of the tenant ID alone doesn't suffice. It's mandatory to set the boolean value to **True** for the ID of each tenant who is to be blocked.

The example for this setting in the .plist file is:

```XML
<key>BlockTenantList</key>
<dict>
<key>TenantId1</key>
<true/>
<key>TenantId2</key>
<true/>
</dict>
```

DefaultFolderLocation

This setting specifies the default location of the OneDrive folder for each organization.

The parameters are **TenantID** and **DefaultFolderPath**. The **TenantID** value is a string that determines the tenants to whom the **default folder location** setting is applicable. The **DefaultFolderPath** value is a string that specifies the default location of the folder. If you want to enforce the location to be the home directory of the user (that is, the default location), you can specify the path as ~/. The string would look like this:

`<string>~/</string>`

The following are the conditions governing the default folder location: -**Mac App Store**: The path must already exist when the user is setting up the sync app. -**Standalone**: The path will be created (if it doesn't already exist) after the user sets up the sync app. Only with the Standalone sync app you can prevent users from changing the location.

The example for this setting in the .plist file is:

```XML
<key>DefaultFolder</key>
<dict>
<key>Path</key>
<string>(DefaultFolderPath)</string>
<key>TenantId</key>
<string>(TenantID)</string>
</dict>
```

DisableAutoConfig

This setting determines whether or not the sync app can automatically sign in.

If you set this setting's value to 1, the sync app is prevented from automatically signing with an existing Microsoft Entra credential that is made available to Microsoft applications.

The example for this setting in the .plist file is:

```XML
<key>DisableAutoConfig</key>
<integer>1</integer>
```

DisableChangesToODIgnoreList

This setting prevents users from changing which files and folders are excluded from upload.

If you set this setting's value to True, users can't add or remove exclusions in OneDrive settings. Exclusions that users added earlier aren't applied, and default entries that users removed earlier are applied again. The OneDrive sync app must be restarted after this setting is changed for the setting to take effect.

This setting applies only to work or school accounts.

The example for this setting in the .plist file is:

```XML
<key>DisableChangesToODIgnoreList</key>
<true/>
```

DisableDefaultODIgnoreList

Microsoft maintains a default list of file extensions and folder names that the OneDrive sync app doesn't upload to OneDrive or SharePoint. The list currently includes shortcut (.lnk) files. Microsoft might update the list through service updates. This setting lets you turn off the default list.

If you set this setting's value to True, the sync app doesn't apply the default list. Exclusions that you configure with EnableODIgnore and EnableODIgnoreFolders still apply. Exclusions that users add in OneDrive settings also still apply, unless you set DisableChangesToODIgnoreList to True. The OneDrive sync app must be restarted after this setting is changed for the setting to take effect. After the restart, files and folders that were skipped only because of the default list start uploading.

> **Note**
>
> Files and folders that already sync aren't excluded when the default list changes.

If you set this setting's value to False or don't configure it, the sync app applies the default list.

This setting applies only to work or school accounts.

The example for this setting in the .plist file is:

```XML
<key>DisableDefaultODIgnoreList</key>
<true/>
```

DisableFirstDeleteDialog

When a user deletes local files from a synced location, a warning message appears that the files are no longer available across all the devices of the user and on the web. This setting lets you hide the warning message.

If you set the setting's value to 1, users don't see the Deleted files are removed everywhere reminder when they delete files locally. (This reminder is called "Deleted files are removed for everyone" when a user deletes files from a synced team site.)

The example for this setting in the .plist file is:

```XML
<key>DisableFirstDeleteDialog</key>
<integer>1</integer>
```

DisableFREAnimation

If you set the setting's value to 1, users don't see the Deleted files are removed everywhere reminder when they delete files locally. (This reminder is called "Deleted files are removed for everyone" when a user deletes files from a synced team site.) This setting lets you prevent the animation from showing during OneDrive Setup.

If you set the setting's value to 1, animations will not be shown during OneDrive Setup.

The example for this setting in the .plist file is:

```XML
<key>DisableFREAnimation</key>
<integer>1</integer>
```

DisableOfflineMode

This setting prevents users from enabling offline mode in OneDrive on the web.

The preferences for this setting are stored in the following .plist files.

Expand table

	Offline mode preferences location	OneDrive group preferences
.plist location	~/Library/Preferences/com.microsoft.SharePoint-mac.plist	~/Library/Group Containers/UBF8T346G9.OneDriveStandaloneSuite/Library/Preferences/UBF8T3

By default, offline mode is turned on for users of OneDrive on the web.

To prevent users at your organization from enabling offline mode in OneDrive on the web, use the following example:

```XML
<key>DisableOfflineMode</key>
<integer>1</integer>
```

To re-enable offline mode in OneDrive on the web for users, use the following example:

```XML
<key>DisableOfflineMode</key>
<integer>0</integer>
```

DisableOfflineModeForExternalLibraries

This setting prevents users from enabling offline mode in OneDrive on the web for libraries and folders that are shared from other organizations.

The preferences for this setting are stored in the following .plist files:

Expand table

	Offline mode preferences location	OneDrive group preferences
.plist location	`~/Library/Preferences/com.microsoft.SharePoint-mac.plist`	~/Library/Group Containers/UBF8T346G9.OneDriveStandaloneSuite/Library/Preferences/UBF8T

To prevent users at your organization from enabling offline mode in OneDrive on the web for libraries and folders that are shared from other organizations, use the following example:

```XML
<key>DisableOfflineModeForExternalLibraries</key>
<integer>1</integer>
```

To re-enable offline mode in OneDrive on the web for libraries and folders that are shared from other organizations, use the following example:

```XML
<key>DisableOfflineModeForExternalLibraries</key>
<integer>0</integer>
```

DisablePersonalSync

This setting blocks users from signing in and syncing files in personal OneDrive accounts. If this setting is configured after a user sets up sync with a personal account, the user gets signed out.

If you set the setting's value to **True**, users are prevented from adding or syncing personal accounts.

The example for this setting in the .plist file is:

```xml
<key>DisablePersonalSync</key>
<(Bool)/>
```

DisableTutorial

This setting prevents the tutorial from being shown to the users after they set up OneDrive.

If you set this setting's value to **True**, the tutorial is blocked from being shown to the users after they set up the OneDrive sync app.

The example for this setting in the .plist file is:

```xml
<key>DisableTutorial</key>
<(Bool)/>
```

DownloadBandwidthLimited

This setting sets the maximum download throughput rate in kilobytes (KB)/sec for computers running the OneDrive sync app.

Set this setting's value to an integer between 50 and 100000 to specify the download throughput in KB/sec that the sync app can use.

The example for this setting in the .plist file is:

```xml
<key>DownloadBandwidthLimited</key>
<integer>(Download Throughput Rate in KB/sec)</integer>
```

EnableODIgnore

This setting lets you enter keywords to prevent the OneDrive sync app from uploading certain files to OneDrive or SharePoint. You can enter complete names, such as "setup.exe" or use the asterisk `*` as a wildcard character to represent a series of characters, such as `*.pst`. Keywords aren't case-sensitive.

If you enable this setting, the sync app doesn't upload new files that match the keywords you specified. No errors appear for the skipped files, and the files remain in the local OneDrive folder. In Finder, the files appear with an "Excluded from sync" icon.

Users see a message in the OneDrive activity center that explains why the files aren't syncing.

The example for this setting in the .plist file is:

```xml
<key>EnableODIgnore</key>
<array>
```

```
<string>(Keyword such as *.PST)</string>
</array>
```

EnableODIgnoreFolders

This setting lets you enter complete folder names to prevent the OneDrive sync app from uploading matching folders to OneDrive or SharePoint. Folder-name matching isn't case-sensitive. For example, enter `PowerShell` to exclude folders named "PowerShell". Wildcards aren't supported.

If you enable this setting, the sync app doesn't upload new folders that match the names you specified. New files created in an existing matching folder also aren't uploaded. No errors appear for the skipped folders, and the folders remain in the local OneDrive folder.

> **Important**
>
> This setting doesn't retroactively remove a folder or its existing content from OneDrive or SharePoint. Moving files that are already syncing into an excluded folder isn't supported.

The OneDrive sync app must be restarted after this setting is enabled or changed for the setting to take effect.

If you don't configure this setting, the sync app uploads all supported folders. Removing an exclusion can cause matching local content to begin uploading. Review the local content before removing a rule.

The example for this setting in the .plist file is:

XML

```
<key>EnableODIgnoreFolders</key>
<array>
<string>(Folder name such as PowerShell)</string>
</array>
```

EnableSyncAdminReports

This setting lets the OneDrive sync app report device and health data that's to be included in sync admin reports. You must enable this setting on the devices you want to get reports from. For more information about these reports, see OneDrive sync reports in the Apps Admin Center.

If you disable or don't configure this setting, OneDrive sync app device and health data don't appear in the sync admin reports.

The following example shows how this setting looks like in the .plist file:

XML

```
<key>EnableSyncAdminReports</key>
<integer>1</integer>
```

> **Note**
>
> We recommend keeping Files On-Demand enabled. See all our recommendations for configuring the sync app

HideDockIcon

This setting specifies whether a dock icon for OneDrive is shown.

If you set this setting's value to **True**, the OneDrive dock icon is hidden even if the app is running.

The example for this setting in the .plist file is:

```XML
<key>HideDockIcon</key>
<(Bool)/>
```

HydrationDisallowedApps

This setting prevents apps from automatically downloading online-only files. You can use this setting to lock down apps that don't work correctly with your deployment of Files On-Demand.

To enable this setting, you must define a string in JSON format:

`[{"ApplicationId":"appId","MaxBundleVersion":"1.1","MaxBuildVersion":"1.0"}]`

"appID" can be either the BSD process name or the bundle display name. "MaxBuildVersion" denotes the maximum build version of the app that can be blocked. "MaxBundleVersion" denotes the maximum bundle version of the app that can be blocked.

The example for this setting in the .plist file is:

```XML
<key>HydrationDisallowedApps</key>
<string>[{"ApplicationId":"appId","MaxBundleVersion":"1.1","MaxBuildVersion":"1.0"},
{"ApplicationId":"appId2","MaxBundleVersion":"3.2","MaxBuildVersion":"2.0"}]</string>
<(Bool)/>
```

KFMBlockOptIn

This setting prevents users from moving their Documents and Desktop folders to any OneDrive account.

If you enable `KFMBlockOptIn`, users aren't prompted to protect their Desktop and Documents folders, and the *Manage backup* command is disabled. If the user previously moved their Desktop and Documents folders, the files in those folders remain in OneDrive. This setting doesn't take effect if you enabled `KFMOptInWithWizard` or `KFMSilentOptIn`.

If you set this setting's value to 1, it prevents Folder Backup. If you set the value to 2, it redirects any folders previously used for Folder Backup back to the user's device and stops the setting from running further.

The example for this setting in the .plist file is:

```XML
<key>KFMBlockOptIn</key>
<integer>(1 or 2)</integer>
```

KFMBlockOptOut

This setting forces users to keep their Documents and Desktop folders directed to OneDrive.

If you enable this setting, the **Stop Backup** button in the **Manage Folder Backup** window is disabled, and users receive an error if they try to stop syncing their Desktop or Documents folder.

The example for this setting in the .plist file is:

```XML
<key>KFMBlockOptOut</key>
<(Bool)/>
```

KFMOptInWithWizard

This setting displays a wizard that prompts users to move their Documents and Desktop folders to OneDrive.

If you enable this setting and provide your tenant ID, users who are syncing their OneDrive sees the Folder Backup wizard window when they're signed in. If they close the window, a reminder notification appears in the Sync Activity Center until they move their Desktop and Documents folders.

The example for this setting in the .plist file is:

XML

```xml
<key>KFMOptInWithWizard</key>
<string>(TenantID)</string>
```

KFMSilentOptIn

Use this setting to redirect and move your users' Documents and/or Desktop folders to OneDrive without any user interaction.

You can move both folders at once or select which folder you want to move. After a folder is moved, this setting won't affect that folder again.

The example for this setting in the .plist file is:

XML

```xml
<key>KFMSilentOptIn</key>
<string>(TenantID)</string>
```

If you enable this setting and provide your tenant ID, you can choose whether to display a notification to users after their folders are redirected:

XML

```xml
<key>KFMSilentOptInWithNotification</key>
<(Bool)/>
```

If you don't set any of the following settings, then the default setting moves both folders into OneDrive. If you want to specify which folder to move, you should set any combination of the following settings:

XML

```xml
<key>KFMSilentOptInDesktop</key>
<(Bool)/>
<key>KFMSilentOptInDocuments</key>
<(Bool)/>
```

LocalMassDeleteFileDeleteThreshold

This setting specifies the threshold for how many files a user can delete from a local OneDrive folder before the user is notified that the files will also be deleted from the cloud.

> **Note**
>
> This policy sets the threshold for how many files a user can delete from a local OneDrive folder before the user is notified that the files will also be deleted from the cloud. If you enable this policy, users see a notification if they delete more than the specified number of

files from OneDrive on their local computer. The user is given the option to continue to remove the cloud files, or restore the local files.

To enable this setting, set a value between 0 and 100000, users will see a notification if they delete more than the specified number of files from OneDrive on their local computer. The user is given the option to continue to remove the cloud files, or restore the local files.

If you don't set this setting, users will see a notification when they delete more than 200 files within a short period of time.

The example for this setting in the .plist file is:

XML

```xml
<key>LocalMassDeleteFileDeleteThreshold</key>
<integer>(Number of items deleted)</integer>
```

MinDiskSpaceLimitInMB

This setting lets you specify a minimum amount of available disk space and block the OneDrive sync app from downloading files when users have less than this amount. Users are prompted with options to help free up space.

To enable this setting, set a value between 0 and 10240000.

The example for this setting in the .plist file is:

XML

```xml
<key>MinDiskSpaceLimitInMB</key>
<integer>(Available disk space)</integer>
```

OpenAtLogin

> ⓘ **Important**
>
> The OpenAtLogin setting will be deprecated with Sync app 24.113. Please refer to Background services to configure the appropriate profile for enabling OneDrive to start automatically when the user logs in.

This setting specifies whether OneDrive starts automatically when the user logs in.

If you set this setting's value to **True**, OneDrive starts automatically when the user logs in to their Mac.

The example for this setting in the .plist file is:

XML

```xml
<key>OpenAtLogin</key>
<(Bool)/>
```

SharePointOnPremFrontDoorUrl

This setting specifies the SharePoint Server 2019 on-premises URL that the OneDrive sync app must try to authenticate and sync against.

To enable this setting, you must define a string containing the URL of the on-premises SharePoint Server.

The example for this setting in the .plist file is:

```XML
<key>SharePointOnPremFrontDoorUrl</key>
<string>https://Contoso.SharePoint.com</string>
```

More info about configuring the OneDrive sync app for SharePoint Server 2019

SharePointOnPremPrioritizationPolicy

This setting determines whether or not the sync app should set up sync for SharePoint Server on-premises or SharePoint in Microsoft 365 first during the first-run scenario when the account is the same for both SharePoint Server and SharePoint in Microsoft 365 in a hybrid scenario.

If you set this setting's value to **1**, the OneDrive sync app sets up SharePoint Server first, followed by SharePoint in Microsoft 365.

The example for this setting in the .plist file is:

```XML
<key>SharePointOnPremPrioritizationPolicy</key>
<integer>(0 or 1)</integer>
```

SharePointOnPremTenantName

This setting enables you to specify the name of the folder created for syncing the SharePoint Server 2019 files specified in the Front Door URL.

If this setting is enabled, you can specify a TenantName that is the name the folder uses in the following convention: OneDrive – TenantName (specified by you)

If you don't specify any TenantName, the folder uses the first segment of the FrontDoorURL as its name. For example, https://Contoso.SharePoint.com uses Contoso as the Tenant Name in the following convention: OneDrive – Contoso

The example for this setting in the .plist file is:

```XML
<key>SharePointOnPremTenantName</key>
<string>Contoso</string>
```

More info about configuring the OneDrive sync app for SharePoint Server 2019

Tier

This setting lets you specify the sync app update ring for users in your organization. The OneDrive sync app updates to the public through three rings; first to Insiders, then to Production, and finally to Deferred. When you enable this setting and select a ring, users aren't able to change it.

We recommend selecting several people in your IT department as early adopters to join the Insiders ring and receive features early. We also recommend leaving everyone else in the organization in the default Production ring to ensure they receive bug fixes and new features in a timely fashion. See all our recommendations for configuring the sync app.

Insiders: The Insiders ring users receive builds that let them preview new features coming to OneDrive.

Production: The Production ring users get the latest features as they become available. This ring is the default.

Enterprise (also known as "Deferred"): The Enterprise ring users get new features, bug fixes, and performance improvements last. This ring lets you deploy updates from an internal network

location, and control the timing of the deployment (within a 60-day window).

For more information on the builds currently available in each ring, see the OneDrive release notes. For more information about the update rings and how the sync app checks for updates, see the OneDrive sync app update process.

Expand table

.plist Location	Domain
~/Library/Preferences/com.microsoft.OneDriveUpdater.plist	com.microsoft.OneDriveUpdater

The example for this setting in the .plist file is:

XML

```
<key>Tier</key>
<string>(UpdateRing)</string>
```

> **Note**
>
> If you want to hide the option "Get pre-release Microsoft internal updates to display", you will need to opt into the Deferred update ring. For example, `defaults write com.microsoft.OneDrive Tier -string "Deferred"`.

UploadBandwidthLimited

This setting defines the maximum upload throughput rate for computers running the OneDrive sync app.

To enable this setting, set a value between 50 and 100000 that is the upload throughput rate in KB/sec the sync app can use.

The example for this setting in the .plist file is:

XML

```
<key>UploadBandwidthLimited</key>
<integer>(Upload Throughput Rate in KB/sec)</integer>
```

WarningMinDiskSpaceLimitInMB

This setting lets you specify a minimum amount of available disk space, and warn users when the OneDrive sync app downloads a file that causes them to have less than this amount. Users are prompted with options to help free up space.

To enable this setting, set a value between 0 and 10240000.

The example for this setting in the .plist file is:

XML

```
<key>WarningMinDiskSpaceLimitInMB</key>
<integer>(available disk space)</integer>
```

Related articles

Find your Microsoft 365 tenant ID

OneDrive sync reports in the Apps Admin Center (EnableSyncAdminReports)

Note: The author created this article with assistance from AI. Learn more

Last updated on 09/29/2026

Redirect and move macOS Desktop and Documents folders to OneDrive

Article • 09/16/2024

This article is for IT admins managing the OneDrive sync app for macOS.

There are two primary advantages of moving or redirecting macOS Desktop and Documents folders to Microsoft OneDrive for the users in your organization:

- Your users can continue using the folders they're familiar with. They don't have to change their daily work habits to save files to OneDrive.
- Saving files to OneDrive backs up your users' data in the cloud and gives them access to their files from any device.

For these reasons, we recommend moving (redirecting) Desktop and Documents folders to OneDrive with Folder Backup if you're an enterprise or large organization. See all our recommendations for configuring the sync app. Small or medium businesses may also find this useful, but keep in mind you'll need some experience configuring settings. For info about the end-user experience, see Protect your files by saving them to OneDrive.

> **Note**
>
> OneDrive sync for macOS runs natively on Apple silicon. This support is generally available starting with build 22.022.

Prepare to move Desktop and Documents folders on existing devices

The standalone OneDrive sync app (not from the Mac App Store) is required for Folder Backup. This app requires Full Disk Access, which can be granted and deployed by IT admins. For more information, see Configure device restriction settings in Microsoft Intune.

We recommend that you upgrade to the latest available build before you deploy.

> **Important**

If your organization is large and your users have a lot of files in their Desktop and Documents folders, make sure you roll out the configuration slowly to minimize the network impact of uploading files. For users who have a lot of files in their folders, consider using the setting **AutomaticUploadBandwidthPercentage** temporarily to minimize the network impact and then disable the setting once uploads are complete.

Folders redirected to other organizations

If a user's Desktop and Documents folders are currently redirected to OneDrive in a different organization, redirecting to your organization's OneDrive will create new Desktop and Documents folders and the user will see an empty desktop. The user will have to manually migrate files from the other organization's OneDrive to OneDrive in your organization. We recommend that you disable the redirect to the other organization before redirecting to your organization if possible.

About the Folder Backup settings

You can set OneDrive settings using software distribution tools such as Microsoft Intune and Jamf Pro, Munki, AutoPkg, Apple Remote Desktop, and AppleScript. You can also configure settings in a .plist file. For a full reference of available preferences and their settings, see Deploy and configure the OneDrive sync app for macOS.

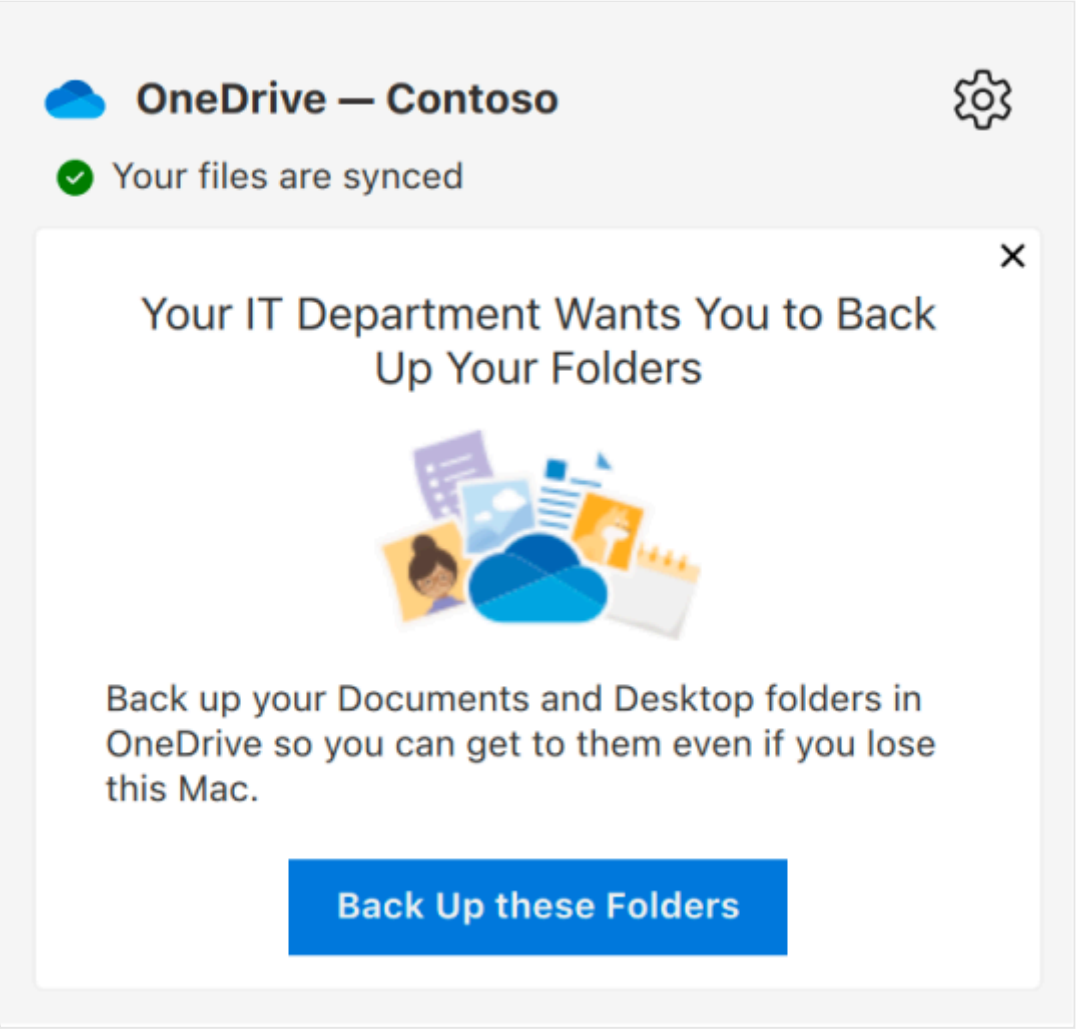
For new machines, Folder Backup can be configured from the start, so all new files are uploaded to the cloud. This is great for organizations as it increases user engagement with OneDrive, and admins can easily protect files with enterprise-level security and compliance that comes built in.

The following settings control the Folder Backup feature:

- Prompt users to move Desktop and Documents folders to OneDrive (KFMOptInWithWizard)

  Use **KFMOptInWithWizard** to give the users a call to action to move their Desktop and Documents macOS folders.

If users dismiss the prompt, a reminder notification appears in the Sync Activity Center until they move all available folders.



> **Important**
>
> We recommend deploying the prompt setting for existing devices only, and limiting the deployment to 5,000 devices a day and not exceeding 20,000 devices a week between macOS and Windows.

- Silently move macOS Desktop and Documents folders to OneDrive (KFMSilentOptIn)

  Use **KFMSilentOptIn** to redirect and move folders to OneDrive without any user interaction. Move all the folders or select the desired individual folders. By default, the Desktop and Documents folders are moved. After a folder is moved, the setting won't affect the folder again, even if the selection for the folder changes.

  You can choose to display a notification to users after their folders have been redirected.

  We also recommend using this setting together with **KFMOptInWithWizard**. If moving the Desktop and Documents folders silently doesn't succeed, users are prompted to correct the error and continue.

> **Important**
>
> We recommend deploying the silent setting for existing devices and new devices while limiting the deployment of existing devices to 1,000 devices a day and not exceeding 4,000 devices a week between macOS and Windows.

- Prevent users from turning off Folder Backup (KFMBlockOptOut)

  Use **KFMBlockOptOut** to force users to keep their Desktop and Documents folders directed to OneDrive.

  > **Note**
  >
  > Users can direct their Desktop and Documents folders by opening OneDrive sync app preferences, clicking the **Backup tab**, and then clicking **Manage Backup**.

- Prevent users from moving their macOS Desktop and Documents folders to OneDrive (KFMBlockOptIn)

  Use **KFMBlockOptIn** to prevent users from moving their Desktop and Documents folders to any OneDrive account.

For info about using the OneDrive sync settings, see Deploy and configure the OneDrive sync app for macOS.

Feedback

Was this page helpful? Yes No

Provide product feedback

Query and set Files On-Demand states on Mac

Article • 09/18/2024

With OneDrive Files On-Demand, files can be in one of three states. Each of these states corresponds to a file attribute state.

To query the current state of a file or folder, use the following command:

- /Applications/OneDrive.App/Contents/MacOS/OneDrive /getpin <Path to file or folder>

Scriptable commands

Use the following commands to set file and folder states. Quit the OneDrive sync app before running these commands.

Expand table

Files On-Demand state	File attribute state	Command
Always available	Pinned	/Applications/OneDrive.App/Contents/MacOS/OneDrive /pin <path>
Locally available	Clearpin	/Applications/OneDrive.App/Contents/MacOS/OneDrive /clearpin <path>
Online-only	Unpinned	/Applications/OneDrive.App/Contents/MacOS/OneDrive /unpin <path>

Note

To set the file attribute state for all items within a folder, add the /r parameter.
Pinning an online-only file makes the sync app download the file contents, and unpinning a downloaded file frees up space on the device by not storing the file contents locally.
To set an online-only file or folder to "locally available," you must first set it to "always available."

Feedback

Was this page helpful? Yes No

Provide product feedback

Allow syncing only on computers joined to specific domains

To ensure users sync OneDrive files only on managed computers, you can configure OneDrive to sync only on PCs joined to specific domains.

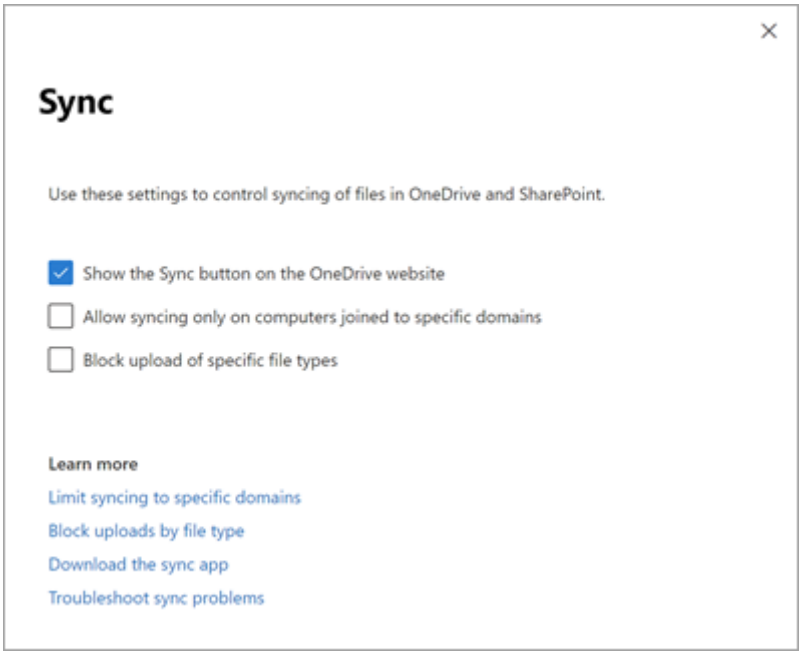
How do I allow syncing only on PCs joined to specific domains?

> **Note**
>
> These settings apply to SharePoint sites and OneDrive. In a multi-geo environment, this setting can be configured separately for each geo location to apply to users with that preferred data location.

1. Go to Settings in the SharePoint admin center {:target="_blank"}, and sign in with an account that has admin permissions for your organization.

   > **Note**
   >
   > If you have Office 365 operated by 21Vianet (China), sign in to the Microsoft 365 admin center, then browse to the SharePoint admin center and open the Sharing page.

2. Select **Sync**.



3. Select the **Allow syncing only on computers joined to specific domains** check box.

4. Enter the GUID of each domain for the member computers that you want to be able to sync.

> **Note**
>
> Make sure to add the domain GUID of the computer domain membership. If users are in a separate domain, the only requirement is adding the domain GUID the computer account is joined to.

> **Important**
>
> This setting is only applicable to Active Directory domains. It doesn't apply to Microsoft Entra domains. If you have devices that are only Microsoft Entra joined, consider using a **Conditional Access Policy** instead. For details, see **Enable conditional access support in the OneDrive sync app**.

5. Select **Save**.

For info about setting this sync app restriction by using PowerShell, see Set-SPOTenantSyncClientRestriction.

For information about blocking or limiting access to SharePoint and OneDrive content from unmanaged devices, see SharePoint and OneDrive unmanaged device access controls for administrators.

Last updated on 12/22/2025

Work with OneDrive web app when offline

We know how important it is for you to access and work with your files on the web quickly and smoothly. That's why we built the next generation of OneDrive web app with performance as one of our main goals. We made sure that OneDrive delivers the best possible web experience for every user, regardless of the internet connection quality. In addition to that, you can now keep working with your files on OneDrive web app even when you're offline and have no internet access.

On Windows 10 or later and macOS 12 Monterey or later devices running the OneDrive sync app, you can now continue working with the OneDrive web app in your browser, OneDrive Progressive Web App (PWA), or Microsoft Teams even when you're offline or lose internet connection with the help of OneDrive Offline mode. You can view, rename, move, copy all of your files, and create new folders. When your files are available for offline access, you can open them on your device in a native app directly from inside OneDrive web app. All the metadata changes you make offline to your files in the browser are automatically synced back to OneDrive when your internet connection is restored.

To accomplish this, a copy of your file metadata that powers OneDrive web app is securely stored locally on your device. This data on your device is only available to you. If someone else was to sign in to your device, the local data on the device wouldn't be available to them. We adhere to privacy guidelines outlined in the Microsoft Privacy Statement.

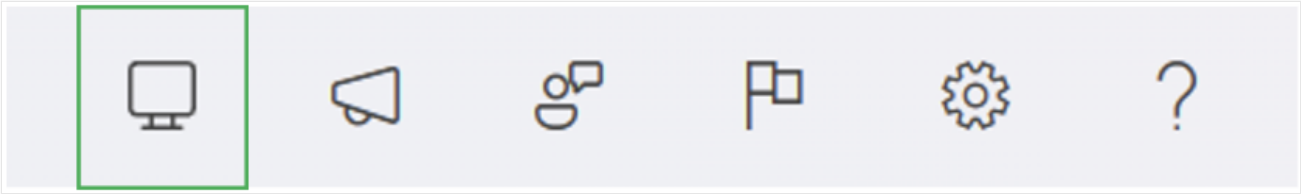
A secure local web server on your device handles the operations that you perform on your files, such as viewing, sorting, renaming, moving, and copying. Traditionally, these operations would need to be handled by the OneDrive cloud service. This results in fast and smooth interactions with your files like loading your files and folders, sorting, renaming, moving, and more. And all these operations continue to work even when you're offline, lose your internet connection, or run into a service disruption in the app.

Verify that OneDrive Offline mode is ready for use

> **Note**
>
> Offline mode is per-device setting and needs to be configured on every device that you use to access OneDrive web app.

1. Open **OneDrive** for web.

2. In the upper right of the page, locate the icon that informs you that Offline mode is ready for you to use.



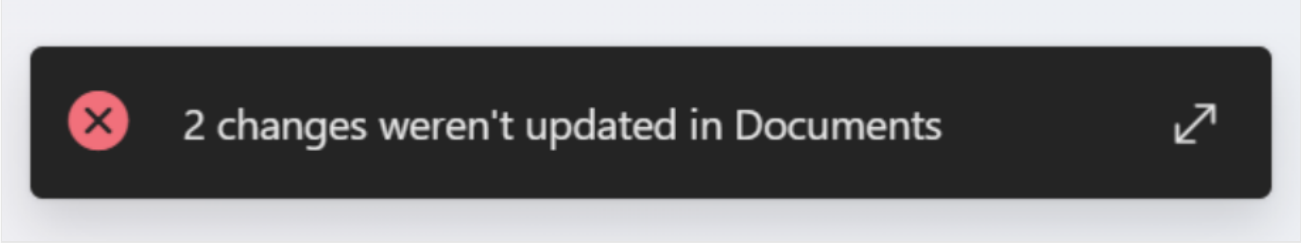
When Offline mode is turned on, the changes you make are synced back to the cloud—either immediately (if you're online) or later when internet connection is restored (if you're offline at the time you make the changes).

Resolve conflicting offline changes

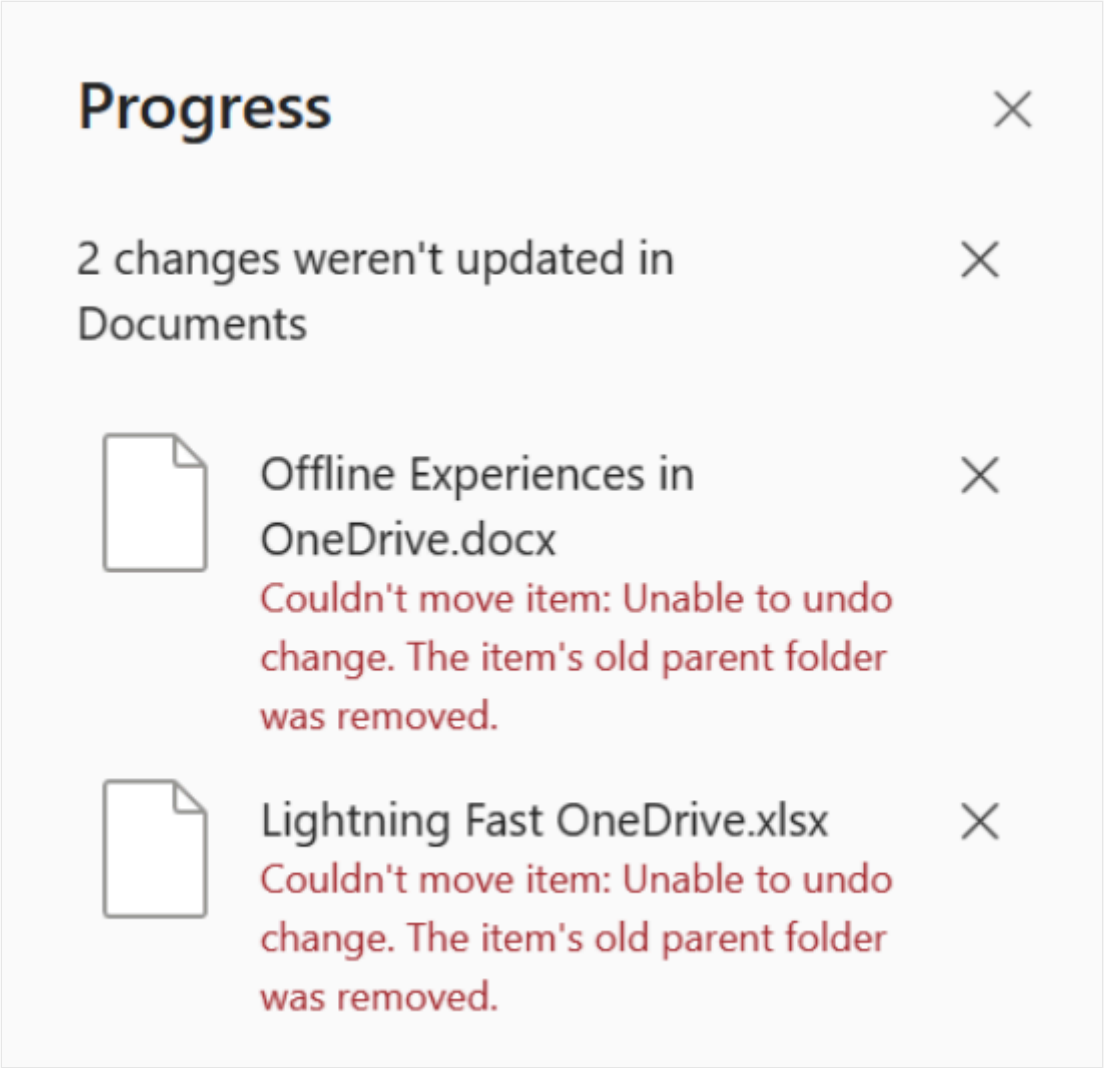
When working offline, it's possible for a conflict to occur if two people change the same item at the same time in different ways. OneDrive tries to resolve the conflict automatically. But if it can't do that, it notifies you about the conflict so that you can resolve it in an appropriate way.

To resolve a conflict:

1. If a conflict exists, you see a toast notification in OneDrive for web.



2. Select the icon on the toast to learn more about the reason for a conflict.



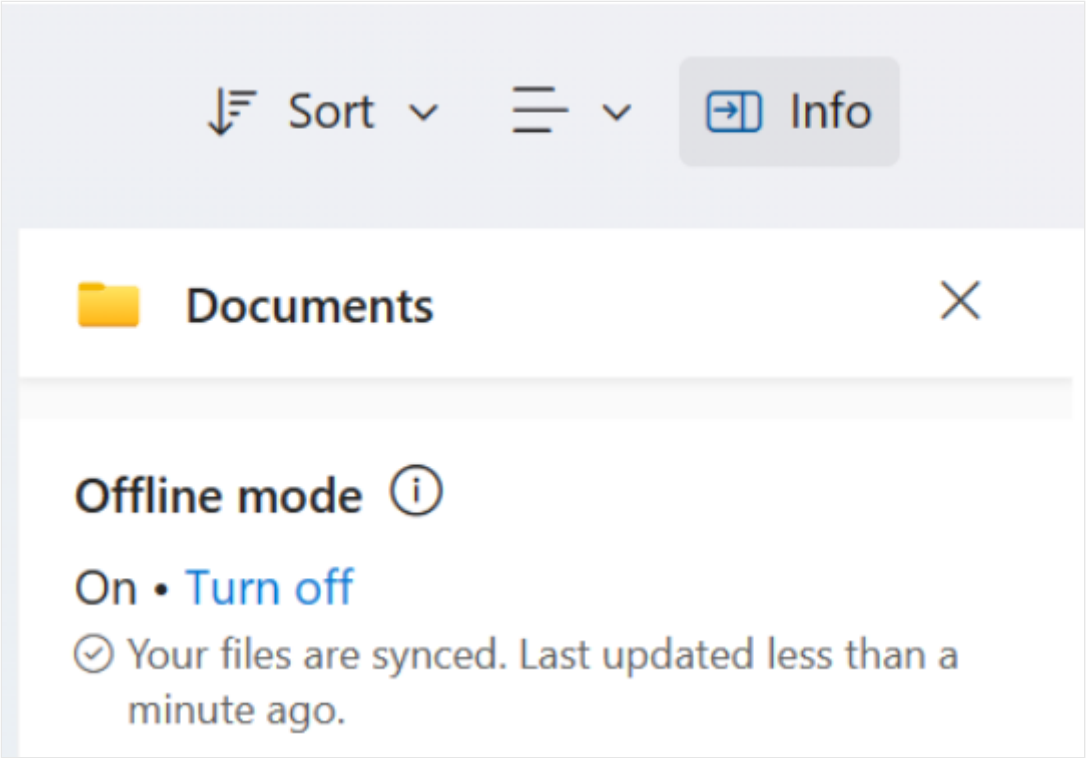
3. You resolve conflicts by dismissing them or by manually correcting them.

Turn off Offline mode

> ⓘ **Note**
>
> Offline mode is per-device setting and needs to be configured on every device that you use to access OneDrive web app.

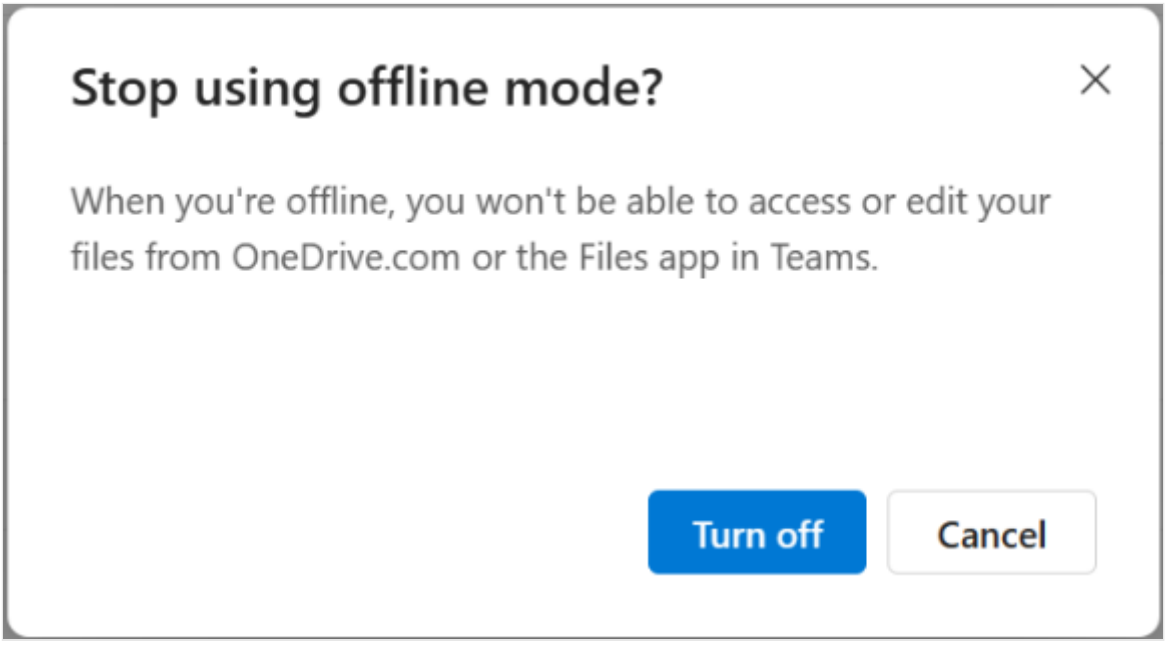
1. To turn off Offline mode, navigate to **My files** view.

2. Expand the info pane by clicking the **Info** button.



3. Select **Turn off** to turn off Offline mode.

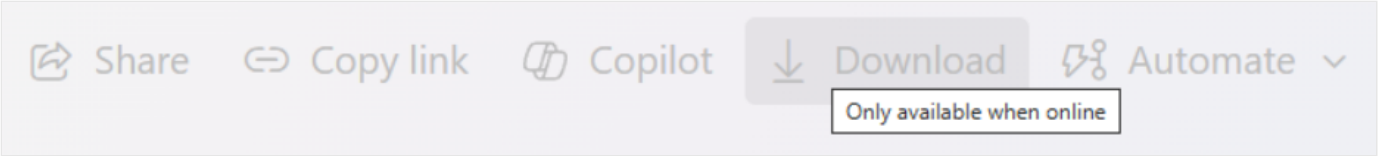
4. In the confirmation dialog that appears, you can proceed with turning off Offline mode or canceling.



After you turn off Offline mode, next time you open OneDrive for web, you'll no longer see the Offline mode icon in the upper right of the page and when you're offline, you won't be able to access or edit your files from OneDrive.com or the Files app in Teams.

Work with OneDrive web app while offline

When you're working offline, you can still open and work with OneDrive for web. Features that aren't available while you're offline are grayed out to indicate that you can't use them at the moment, as illustrated below. When offline, you'll still be able to see, rename, move, copy your files, and create new folders.



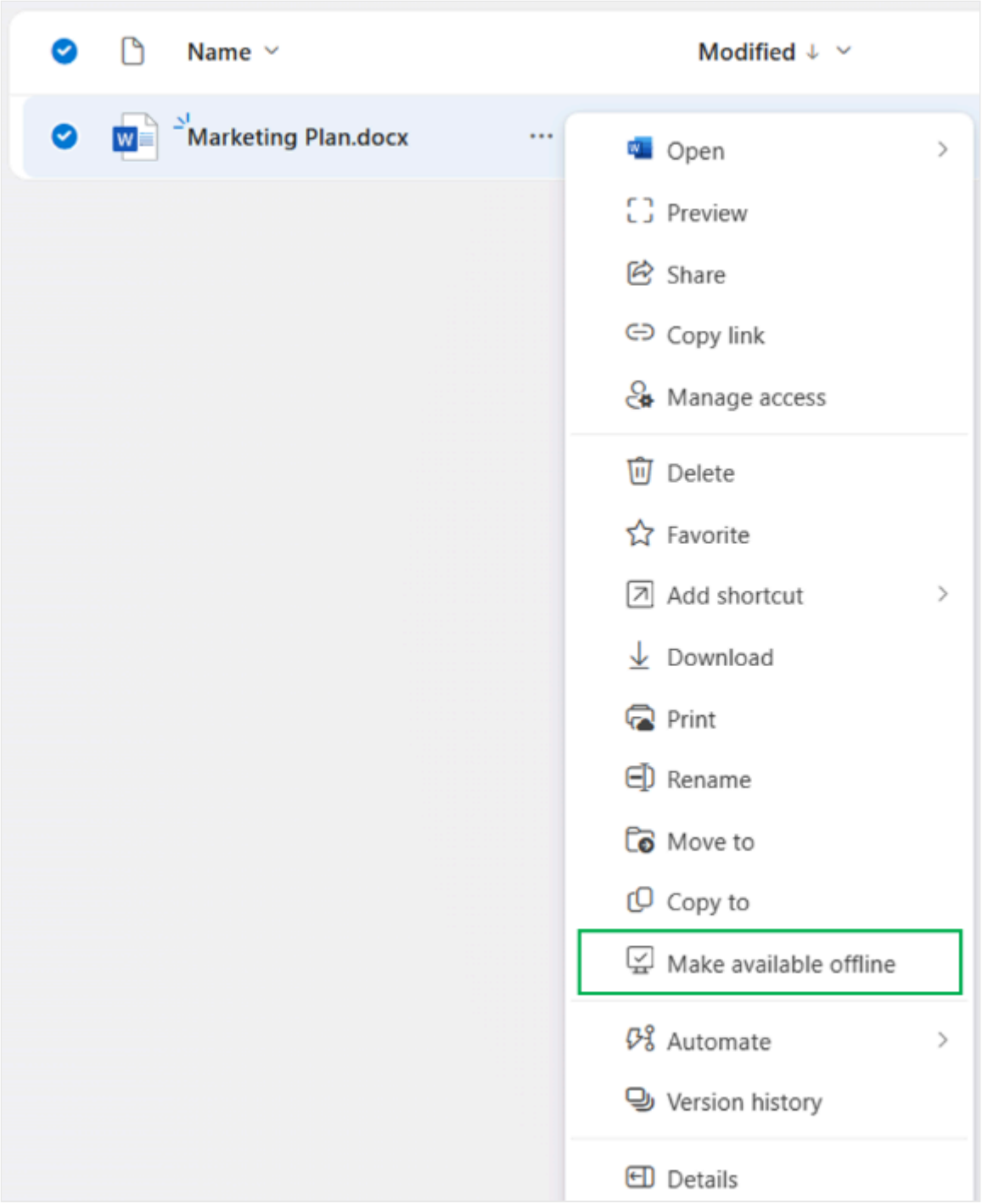
Make files available offline

Offline file access and sync are fundamental to OneDrive and now you can use the power of OneDrive files on-demand in OneDrive web app. When you want files and folders available for offline access on your device, you can select them to be always available locally directly from OneDrive web app. You can make files available offline on your device or even free up space by making offline files online-only. And you can do it directly from the OneDrive web app without having to navigate away to File Explorer or Finder to accomplish these tasks.

To make file or folder available offline:

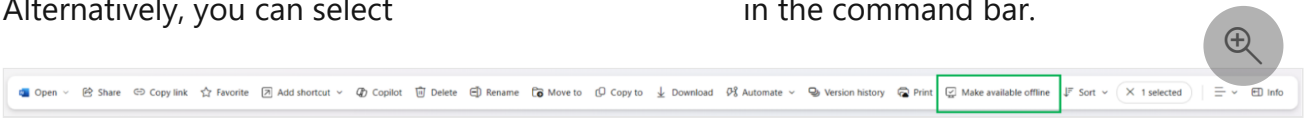
1. Make sure you're syncing your OneDrive with OneDrive sync app.
2. Select the file or folder (you can select multiple) that you want to make available offline on your device.
3. Select "..." (select more actions for this item) and in the context menu that opens select

   Make available offline

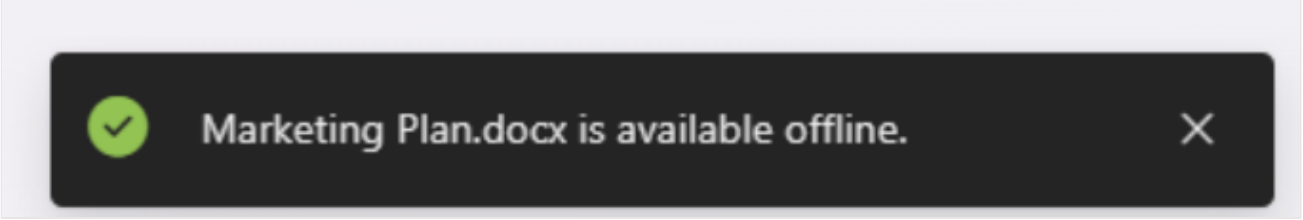


Alternatively, you can select

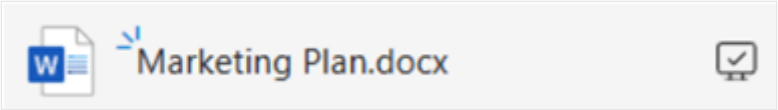
in the command bar.



4. The file or folder is then downloaded to your computer. Once completed, you're notified with a toast that the file is available to you when you're offline.



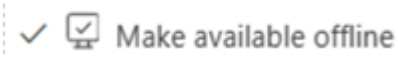
5. You see an "available offline" icon next to the files and folder that you marked to be available offline.



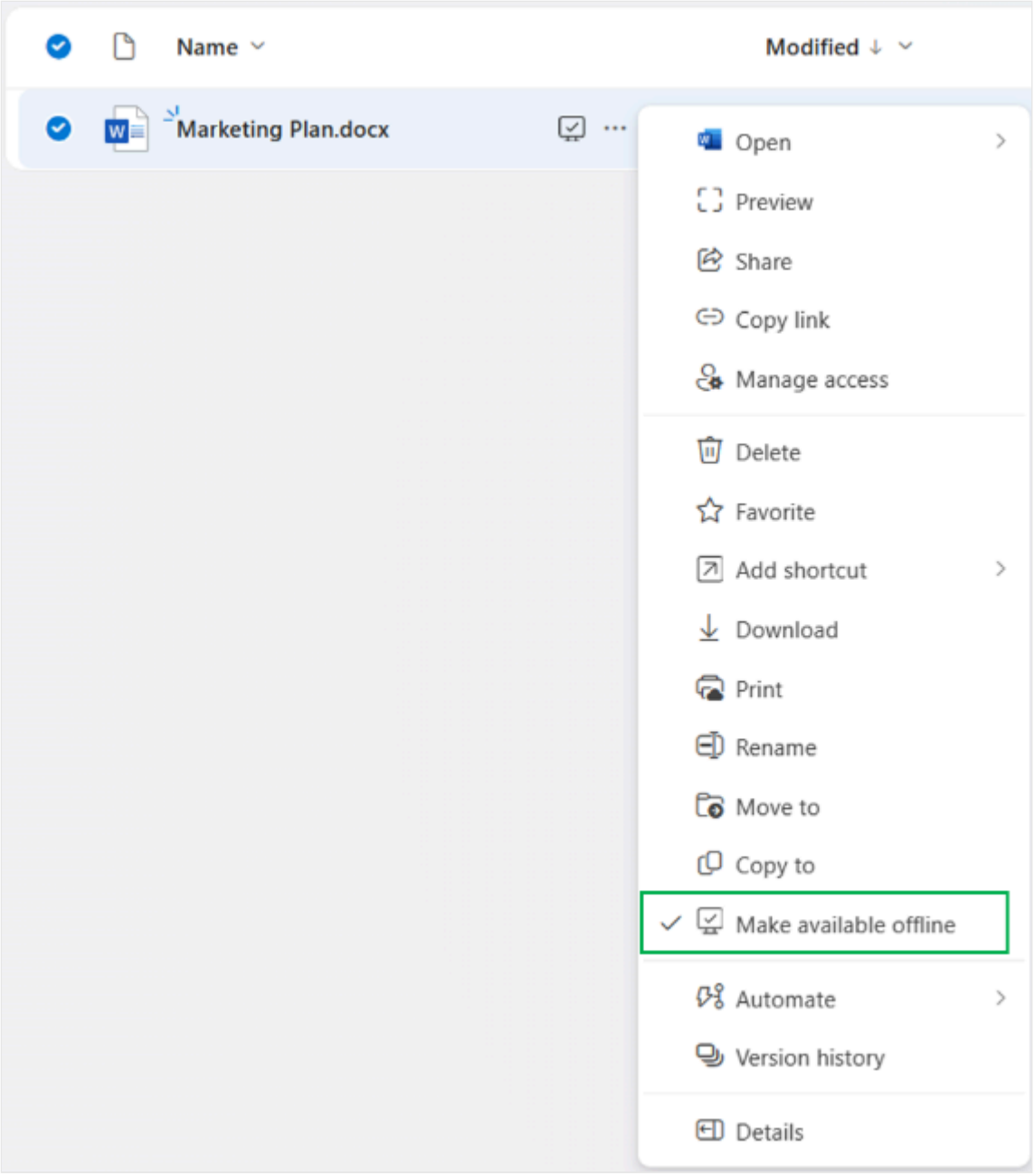
Free up space on your device

You can also free up space on your computer by making offline files online-only. You'll only be able to open these files when you're online, but you'll still be able to rename, move, or copy these files when you're offline.

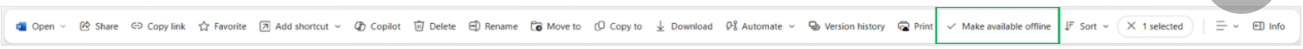
1. Select a file or folder (you can select multiple) that are marked as "available offline" that you no longer want to be available offline.

2. Select "..." (select more actions for this item) and in the context menu that opens select 

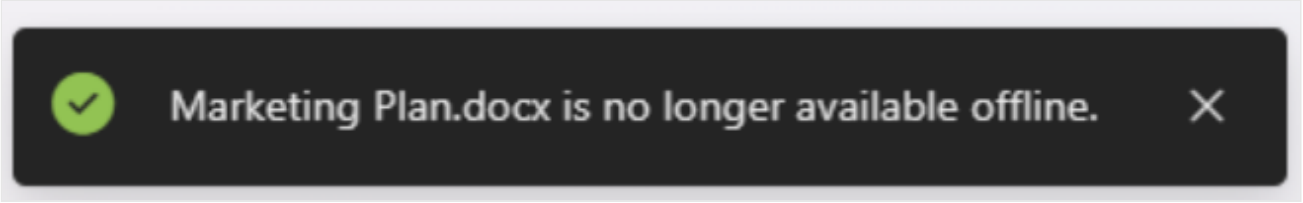
option.



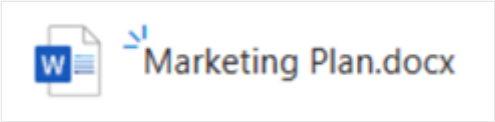
Alternatively, you can select ✓ Make available offline in the command bar.



3. The file or folder is marked as online-only. Once completed, you're notified with a toast that the file is no longer available to you when you're offline.



4. You'll no longer see "available offline" icon next to the file or folder that you chose not to be available offline on your computer.



> **Note**
>
> - "Make available offline" action works across OneDrive for Web and OneDrive sync app on Windows and macOS.
> - You can make the file available offline in Windows File Explorer or macOS Finder and the file's offline availability state will be updated in OneDrive for Web as well.

Current limitations of Offline mode

1. Offline mode is currently supported only on Windows (Windows 10 and later), macOS devices (macOS 12 Monterey or later), and Chromium-based browsers (Microsoft Edge, Google Chrome)
2. Currently, Offline mode isn't supported in the following situations:

    - If you added a shortcut to shared folders in OneDrive

3. A *full* offline experience in OneDrive for web—where you can perform all the operations that are available online isn't yet supported. The following features aren't available when you're offline.

    - Sharing, copying links, adding new files, downloading your files
    - Managing access to your files
    - Previewing your file in online previewer
    - Using **Search**
    - Creating and managing Power Automate flows
    - Copilot
    - Deleting files
    - Viewing file version history
    - Navigating to **Recycle bin**

Bandwidth involved in using Offline mode

When compared to OneDrive sync app, bandwidth consumed by Offline mode is minimal, and largely depends on the size of your OneDrive and how frequently your OneDrive files are modified. When setting up Offline mode for the first time, a local copy of your file metadata is

downloaded and securely stored on your computer. The actual contents of your files won't be downloaded. After Offline mode is set up, only changes to your file metadata will result in upload or download activity over the network.

Last updated on 11/01/2024

How sync works

Article • 09/14/2024

This article gives you an overview of how sync works in Microsoft OneDrive. It helps you understand the logic behind how information flows between applications, how the technologies work together, and how data is secured.

Download the PDF

Microsoft

OneDrive Sync

How does OneDrive sync files?

The business of sync with OneDrive.exe

The new OneDrive sync client (OneDrive.exe) uses the Windows Notification Service (WNS) to check for changes that are made to items that are stored in the cloud.

WNS tells the sync client when a change actually happens, which initiates a query for changes. The user interface communicates with storage through a REST API.

Technologies used in sync

Microsoft-my.sharepoint.com/personal/<your library id>/_api/SPFileSync.svc
Used for tasks such as finding changes, uploading, and querying for available storage space.

Microsoft-my.sharepoint.com/personal/<useraccount_company_com>/_layouts/15/download.aspx
Used for downloading items.

odc.officeapps.live.com
Used to discover what sites and organizations a user has permission to access.

How information flows

When changes are made to files in the cloud

1 When changes are made to files in the cloud

The Windows Notification Service (WNS) informs the OneDrive sync client when changes are made to items in the cloud.

Changes in the cloud are added to OneDrive's Internal Server Changes Queue.

- Metadata (move, rename, delete) changes happen immediately.
- Content downloads start a download session with the service.

How information flows

When changes are made on the local device

2 The Windows Notification Service (WNS) informs the OneDrive sync client when changes are made to items on the local device.

A Your cloud database has metadata pointers to Microsoft Azure.

B Each file chunk is encrypted with a unique key. File chunks are stored across multiple containers in Azure. All keys are required to reassemble the file.

C Each unique key used to encrypt a file chunk is also encrypted by a master key before the data is stored. This is to ensure protection at rest.

Syncing of Office files

D For all items except Office 2019 or Office 2016 files

Local changes are placed in a Changes to Send queue and are sent in the following ways:

- New or changed files up to a size defined by server settings (for example, 8 MB) are sent inline in a single HTTPS request.
- New or changed files over the defined size are divided in "chunks" and are sent one at a time through a Background Intelligent Transfer Service (BITS) session.
- Other changes are batched together with other related changes of the same type into HTTPS requests to the server.

For Office 2019 and Office 2016 files:

- OneDrive communicates with individual Office apps to trade metadata about changes so that syncing is done correctly.
- Collaborative syncing is handled by the Office desktop

How information flows

The OneDrive sync app uses Windows Push Notification Services (WNS) to sync files in real time. WNS informs the sync app whenever a change actually happens, eliminating redundant polling and saving on unnecessary computing power.

Here's how it works:

- A change occurs in Microsoft 365.
- WNS alerts the sync app of the change.
- OneDrive adds it to the Internal Server Changes Queue.
  - Any metadata changes happen immediately, like renaming or deleting files.
  - Downloading content also starts a specific session with the client.
- Microsoft 365 has metadata pointers directing it through Microsoft Azure.
- The changes are processed in the order they're received.

The previous OneDrive sync app (Groove.exe) used a polling service to check for changes on a predetermined schedule. Polling can lead to system lag and slowness because it requires a significant amount of computing power. Using WNS is a significant enhancement.

Authentication protocols

The authentication protocols depend on which version of SharePoint you're using.

- SharePoint Server 2019 uses NTLM.
- SharePoint in Microsoft 365 uses FedAuth.

Syncing different file types

OneDrive handles sync differently depending on the type of file.

For Office 2016 and Office 2019 files, OneDrive collaborates directly with the specific apps to ensure data are transferred correctly. If the Office desktop app is running, it handles the syncing. If it isn't running, OneDrive will.

For other types of files and folders, items smaller than 8 MB are sent inline in a single HTTPS request. Anything 8 MB or larger is divided into file chunks and sent separately one at a time through a Background Intelligent Transfer Service (BITS) session. Other changes are batched together into HTTPS requests to the server.

The underlying technologies

The OneDrive sync app uses the following to sync files:

- To find new changes and upload information: `https://<tenant_name, i.e. contoso>-my.sharepoint.com/personal/<user_contoso_onmicrosoft_com>/_api/SPFileSync/sync/<default document library ID GUID>/`
- To download items: `https://<tenant_name, i.e. contoso>-my.sharepoint.com/personal/<user_contoso_onmicrosoft_com>/_layouts/15/download.aspx`
- To discover the sites and organizations a user can access: `https://odc.officeapps.live.com/odc/servicemanager/userconnected`

Security and encryption

File chunks are stored in multiple containers in Azure, each of which is given a unique key. Each key is required to reassemble the complete file. There's also a separate master key encrypting each file chunk key, ensuring the data remain secure even when not moving.

Related topic

- SharePoint Authentication in Microsoft 365

Feedback

Was this page helpful? Yes No

Provide product feedback

B2B Sync for SharePoint and OneDrive

B2B Sync in the OneDrive sync app allows users to sync libraries or folders in Microsoft SharePoint or Microsoft OneDrive that are shared from other organizations. This scenario is often referred to as Business-to-Business (B2B) Collaboration.

Microsoft Entra guest accounts are essential for B2B Collaboration. A guest account at one organization links to a member account at another organization. Once created, a guest account allows Microsoft 365 services like OneDrive and SharePoint to grant a guest permission to sites and folders, just like a member within the organization. Because the accounts at two organizations are linked, users only need to remember the username and password for their own organization's account. A single sign-in enables access to content from their own organization and from any other organizations that created guest accounts for them.

> **Important**
>
> We recommend that you enable SharePoint and OneDrive integration with Microsoft Entra B2B to help ensure that the required Microsoft Entra guest account for the share recipient is created in your organization's directory.

What are the requirements for B2B Sync?

For people outside your organization to sync shared libraries and folders:

- You must enable external sharing for your organization.
- You must enable external sharing for the site or OneDrive.
- You must share the content with people outside the organization at the site or folder level. If a folder is shared, it must be through a link that requires sign-in.
- Sharing recipients must have a Microsoft 365 work or school account (in Microsoft Entra ID) in the same cloud as the content tenant - Microsoft Azure Commercial, Microsoft Azure Government, or Microsoft Azure China 21Vianet. (Microsoft Azure Commercial contains the Microsoft 365 commercial and GCC cloud environments, and Microsoft Azure Government contains the GCC High and DoD cloud environments.)
- Any Microsoft Entra Conditional Access policies must be compatible with guests. See Conditional Access policies for more information on external access and compatibility.
- Microsoft Authentication Library must not be enabled if using builds before 19.086.

This article gives an overview of the B2B Sync experience and describes these requirements in more detail.

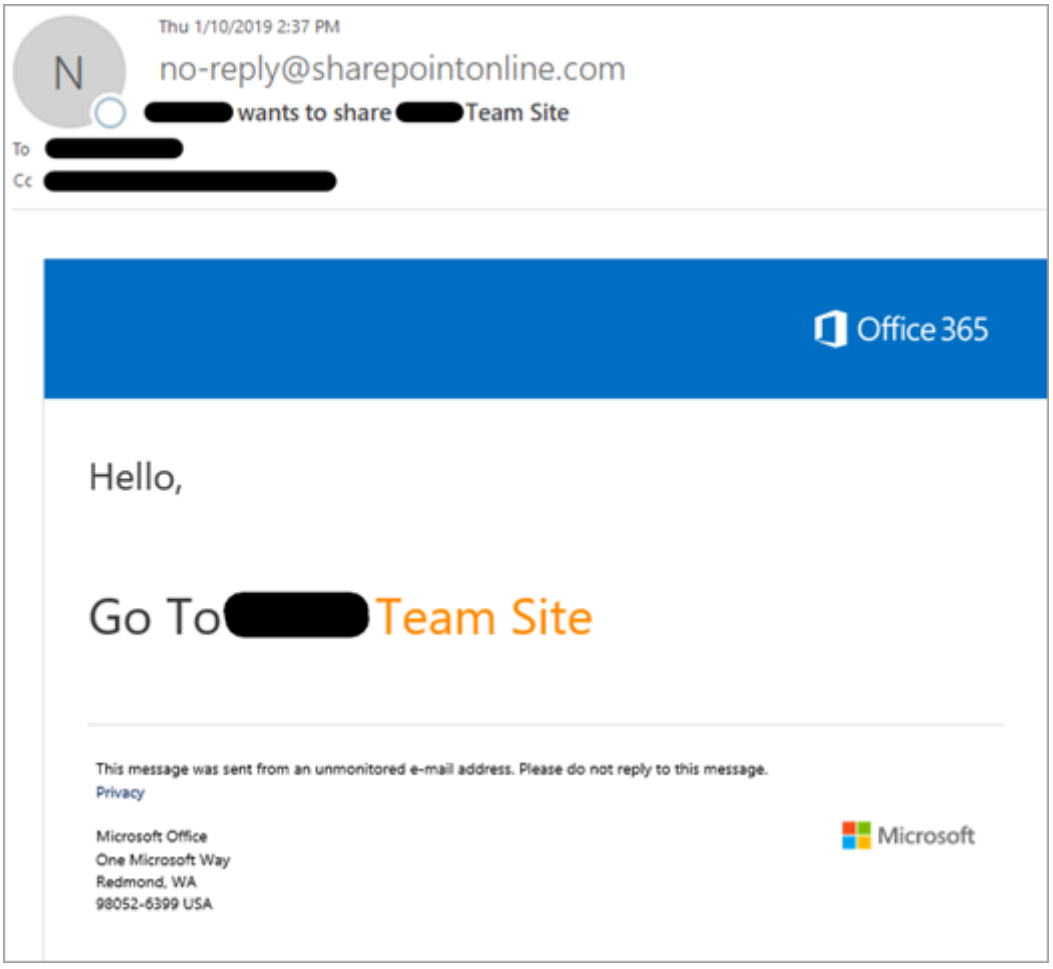
What are the known issues?

- Sync between users in different clouds isn't supported For example, content shared from a tenant in Microsoft Azure China 21Vianet isn't synched for a user with a Microsoft Azure Commercial cloud.
- On the Mac, Files On-Demand thumbnails won't display from external organization's sites. Thumbnails display correctly for files from the user's own organization.
- On the Mac, if the guest account was created with a different email address format than the form they're using with the sync app, the external site's content can't be synced. For example, first.last@fabrikam.com vs alias@fabrikam.com.
- On Mac, the external content can be placed on the local computer in the user's own organization's folder instead of one with the external organization's name.
- Interactive authentication UI for guest accounts from an external organization isn't supported by the sync client.

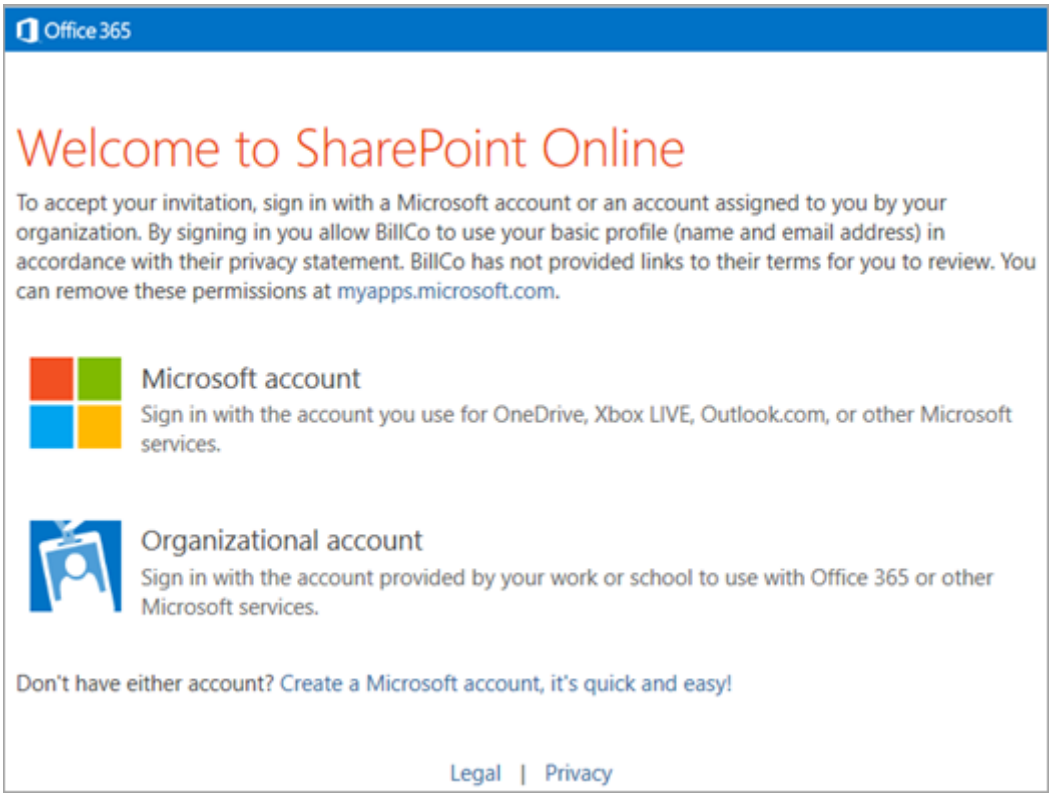
How does the B2B Sync experience work?

Here's an example of what happens after someone at "Contoso" shares a site or folder with someone at "Fabrikam":

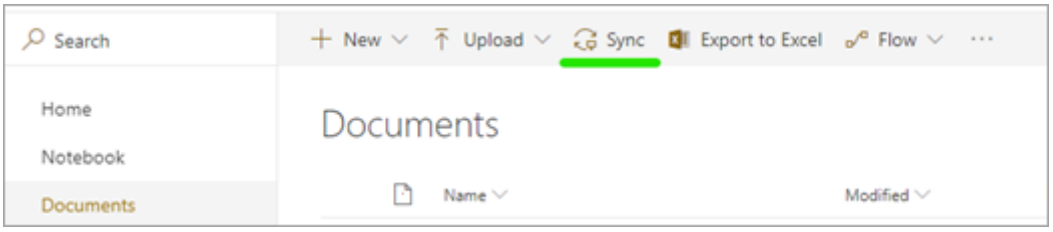
1. The Fabrikam recipient receives an email like the following.



2. When the recipient selects the link in the email to go to the shared item, they need to select "Organizational account" to sign in with their Fabrikam account. Behind the scenes, this creates the Contoso guest account in Microsoft Entra ID.



3. The recipient may need to enter their Fabrikam username or password, and then they can view the shared item. If they don't want to sync everything that was shared, they can browse to the library or folder they want to sync. To set up syncing, they need to select the Sync button.



4. The guest's browser displays up a message asking if they want to open "Microsoft OneDrive," and they'll need to allow this.

5. If this is the first time the guest has used the sync app with their Fabrikam account, they need to sign in. The email address is automatically set to the Fabrikam account used in the previous steps. The guest needs to select "Sign in."

6. The guest might be able to sign in to the sync app without entering their Fabrikam password if they're signed in to Windows with the same account. Otherwise they need to enter their password.

7. The guest confirms where they want to sync the shared item on their computer.

> **Note**
>
> The content is placed in a folder whose name includes the name of the organization ("SharePoint - Contoso" in this example). If the user is syncing SharePoint content from Fabrikam as well, they'll also have a "SharePoint - Fabrikam" folder.

8. The guest continues through OneDrive sync app setup.

9. After the guest completes setup, the site will begin syncing. The user can select the blue cloud icon in the notification area to open the OneDrive sync activity center and see the files syncing, open the local folder with the files, or open the SharePoint site in a web browser.

How do I enable external sharing for my organization?

To allow users at your organization to share with their partners at other organizations, you must enable external sharing at the organization level. You must be a Global Administrator or SharePoint Administrator in Microsoft 365 to do this. After you enable external sharing at the organization level, you can restrict it site by site. A site's settings can be the same as the organization setting, or more restrictive, but not more permissive.

You can change your organization-level sharing settings in two different places (both control the same thing):

- On the Sharing page in the new SharePoint admin center. For more info, see Change the organization-level external sharing setting
- In the Microsoft 365 admin center, on the Org settings page > SharePoint.

> **Important**
>
> If you allow Anyone links (sometimes referred to as "anonymous access" links), these links don't create guest accounts and therefore the external share recipient won't be able to use B2B Sync when receiving that link type.

For more info, see External sharing overview.

Control external sharing

When you allow users to share content from your organization externally, you can use several features in Microsoft 365 to manage who has access to the content. Admins and site owners can review permissions and audit access to sites. For info, see Searching for site content shared with people outside your organization and Turn on external sharing notifications. You can enable external sharing with only specific internet domains, or you can block specific domains. For info, see Restricted domains sharing. You can also allow only members of specific security groups to share externally. For info, see Turn external sharing on or off.

We recommend creating separate sites (site collections, not subsites) for each unit of work that you want to share externally. This way, you can clearly annotate the sites to indicate that people outside the organization have access, and avoid unintentional disclosure of information. For individual users sharing content from their OneDrive, we recommend creating separate folders for different projects or collaboration groups.

You can remove a guest's permission to a site or folder, or you can delete the guest account to remove their permission from all of your organization's content.

> **Important**
>
> Any synced content will remain on the user's computer after permissions have been removed.

How do I enable external sharing for a site?

To view or change the sharing setting for any site, use the new SharePoint admin center.

1. Go to **Active sites** in the SharePoint admin center, and sign in with an account that has admin permissions for your organization.

   > **Note**
   >
   > If you have Office 365 operated by 21Vianet (China), sign in to the Microsoft 365 admin center, then browse to the SharePoint admin center and open the Active sites page.

2. Customize the view as necessary to see the External sharing column.

3. If you need to, change the external sharing setting for a site.

How do I ensure Conditional Access policies are compatible?

As an admin, you can enable several kinds of conditional access policies at your tenant. When a guest accesses a tenant's content, you might need to adjust those policies for the guests to ensure they can gain access.

- Currently the sync client doesn't support interactive authentication UI when syncing external content. Any policy that would require a sign-in UI such as MFA (multifactor authentication) or TOU (terms of use) prompt, will prevent the syncing of the external content from that tenant. If a tenant admin deploys such a policy before a guest starts syncing from that tenant, the user is unable to establish the sync relationship. If the policy is deployed after a guest is syncing content from the tenant, that guest will receive an error and be unable to continue to sync from the tenant.

- Tenants may update their Terms of Use (TOU) from time to time. A policy can trigger the user to view and accept the updated TOU via an interactive authentication prompt. Since sync doesn't support external tenant sign-in UI, sync indicates it's unable to sync the external site's content.

- Device Compliance requires user machines to be managed by the tenant and then to be up to date with requirements. For guests, their machines are likely to be managed by their own organization and thus are incompatible with requiring their machines to be managed by the content sharing tenant.

- Location-based conditional access policies are typically used to enforce more requirements like MFA when the user isn't connecting from a trusted location (such as the tenant's office network). Typically in a guest scenario the client machine won't be located at the trusted locations, and since sync doesn't support MFA, you likely don't want this policy to apply to your guests.

For more information, see Authentication and Conditional Access for External Identities.

What are the methods of sharing?

Sites and folders can be shared in different ways in SharePoint and OneDrive:

- If users are syncing a folder, they can right-click it in File Explorer to share it.
- Users can go to the SharePoint site or folder on the web and select the Share button to share it.
- Users can share sites and folders in the SharePoint and OneDrive mobile apps.

- Admins can create guest accounts and use the admin center or PowerShell to add them to sites.

> **Note**
>
> For more info about these methods, see Learn how to share a site and Learn how to share a folder.

B2B Sync works with all these methods of sharing. It has only the following requirements:

- For guests to sync shared content, the content must be shared at the site or folder level. Guests can't sync files that are shared individually (for example, from the Office apps).
- B2B sync works only when guest accounts are created in the organization, and when the recipient has a Microsoft Entra account. It doesn't work when users share by creating an Anyone link (also known as "anonymous access" link), or when they share with people who have a Microsoft account or other personal account.

How do I add guests to SharePoint sites?

As an admin in Microsoft 365, you can share with people outside the organization by creating guests individually in the Microsoft Entra admin center, and then adding them to a SharePoint team site individually or by adding them to a security group that already has permissions to the site you want to share. If you grant permissions by using the advanced permissions page (instead of by using the Share site button), you need to inform the guest that you've given them permission to the site. They won't receive an invitation email.

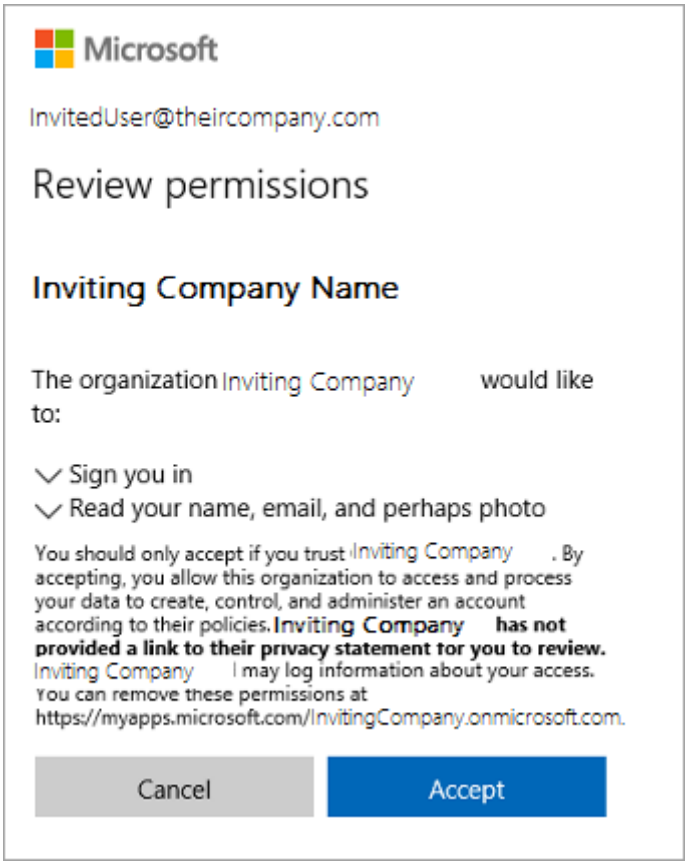
> **Important**
>
> If you use the advanced permissions page, we recommend granting permissions at the site level, not at the document library or folder level.

How do I use PowerShell to bulk create guest accounts?

If you need to create and grant permissions to many guest accounts, you can use the following PowerShell script, which creates guest accounts and grants them permissions to a site. The script takes a CSV (comma-separated value) file as input, which contains a list of user display names and email addresses. For each name and email address, a guest account is created and that account is added to a security group to grant it permission. The script is designed so that you can feed the resulting output CSV as input to the script on a subsequent run. This lets you add more users to your CSV file or retry creating any failed account.

> **Note**
>
> Azure AD and MSOnline PowerShell modules are deprecated as of March 30, 2024. To learn more, read the deprecation update. After this date, support for these modules are limited to migration assistance to Microsoft Graph PowerShell SDK and security fixes. The deprecated modules will continue to function through March, 30 2025.
>
> We recommend migrating to Microsoft Graph PowerShell to interact with Microsoft Entra ID (formerly Azure AD). For common migration questions, refer to the Migration FAQ.
>
> Be aware that versions 1.0.*x* of MSOnline may experience disruption after June 30, 2024.

As users are added to the Microsoft Entra group, they should receive an email welcoming them to the group. After running the script, you'll need to email the users with a direct link to the SharePoint site you gave them permissions to. When they select the link, they're presented with the below UI to accept the terms of the invitation. Once they accept, they're taken to the site you shared with them. At that point they can select the Sync button to begin syncing the sites files to their PC or Mac.



PowerShell

```
# first line of InviteGuests.ps1 PowerShell script
# requires latest AzureADPreview
# Get-Module -ListAvailable AzureAD*
# Uninstall-Module AzureAD
```

```
# Uninstall-Module AzureADPreview
# Install-Module AzureADPreview


# customizable properties for this script

$csvDir = ''
$csvInput = $csvDir + 'BulkInvite.csv'
$csvOutput = $csvDir + 'BulkInviteResults.csv'

$domain = 'YourTenantOrganization.onmicrosoft.com'
$admin = "admin@$domain"
$redirectUrl = 'https://YourTenantOrganization.sharepoint.com/sites/SiteName/'
$groupName = 'SiteName'


# CSV file expected format (with the header row):
# Name,Email
# Jane Doe,jane@contoso.com

$csv = import-csv $csvInput

# will prompt for credentials for the tenantorganization admin account
# (who has permissions to send invites and add to groups)
Connect-AzureAD -TenantDomain $domain -AccountId $admin

$group = (Get-AzureADGroup -SearchString $groupName)

foreach ($row in $csv)
{
    Try
    {
        if ((Get-Member -inputobject $row -name 'error') -and `
            ($row.error -eq 'success'))
        {
            $out = $row  #nothing to do, user already invited and added to group
        }
        else
        {
            echo ("name='$($row.Name)' email='$($row.Email)'")

            $inv = (New-AzureADMSInvitation -InvitedUserEmailAddress $row.Email -
InvitedUserDisplayName $row.Name `
                        -InviteRedirectUrl $redirectUrl -SendInvitationMessage
$false)

            $out = $row
            $out|Add-Member -MemberType ScriptProperty -force -name 'time' -Value
{$(Get-Date -Format u)}
            $out|Add-Member -MemberType ScriptProperty -force -name 'status' -Value
{$inv.Status}
            $out|Add-Member -MemberType ScriptProperty -force -name 'userId' -Value
{$inv.InvitedUser.Id}
            $out|Add-Member -MemberType ScriptProperty -force -name 'redeemUrl' -
Value {$inv.inviteRedeemUrl}
```

```
            $out|Add-Member -MemberType ScriptProperty -force -name 'inviteId' -
Value {$inv.Id}

            # this will send a welcome to the group email
            Add-AzureADGroupMember -ObjectId $group.ObjectId -RefObjectId
$inv.InvitedUser.Id

            $out|Add-Member -MemberType ScriptProperty -force -name 'error' -Value
{'success'}
        }
    }
    Catch
    {
        $err = $PSItem.Exception.Message
        $out|Add-Member -MemberType ScriptProperty -force -name 'error' -Value
{$err}
    }
    Finally
    {
        $out | export-csv -Path $csvOutput -Append
    }
}

# for more information please see
# https://learn.microsoft.com/azure/active-directory/b2b/b2b-tutorial-bulk-invite
# end of InviteGuests.ps1 powershell script
```

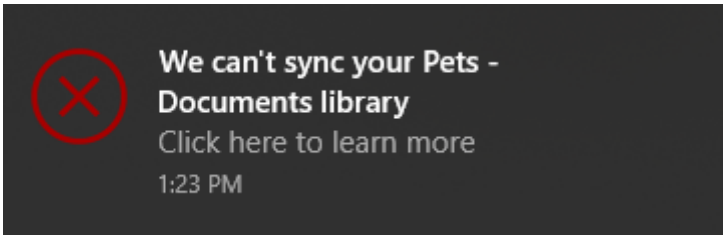
For more info, see:

- Redemption experience
- Add user without invite

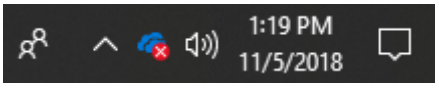
What happens when a guest loses access?

If a person's guest account is deleted or their permission to shared content is removed, the sync app displays an error.

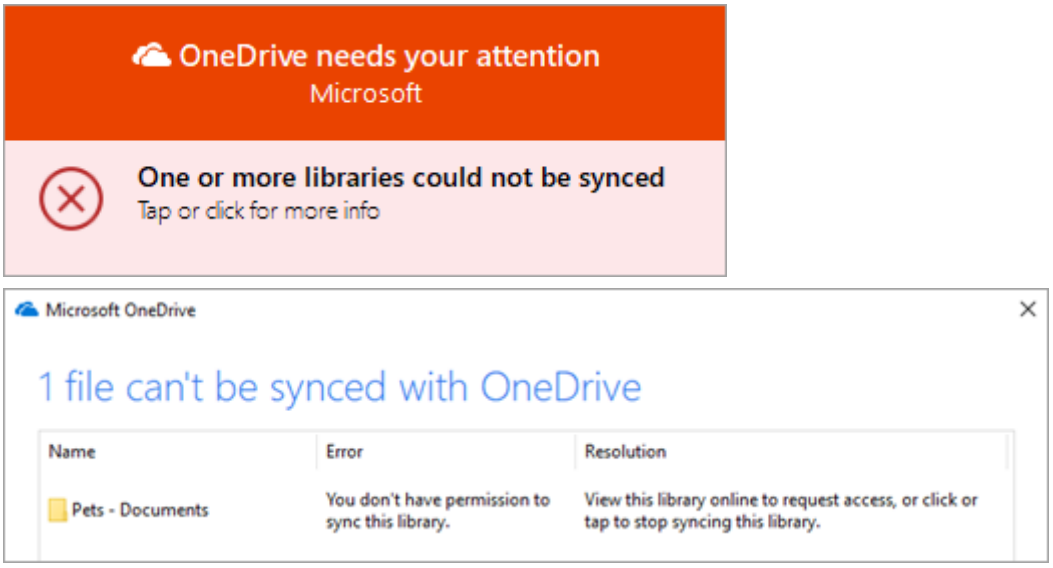
- A notification appears indicating that the library can't be synced.



- The OneDrive icon in the notification area shows an error.



When the guest selects the icon, they see an error banner in the activity center.



How do I prevent B2B Sync?

You can prevent users at your organization from using B2B Sync by setting a policy value on your users' Windows PC or Mac to block external sync.

The new BlockExternalSync setting is described in the adm\OneDrive.admx and OneDrive.adml files installed as part of the OneDrive sync product build 19.086.* or higher. If you use ADM to manage your sync app policies, import the new files as you normally would in order to see the new setting.

If you're using other management systems to deploy policies to your users' Windows PCs, use the equivalent of the following command to prevent B2B Sync:

Windows Command Prompt

```
reg add "HKLM\SOFTWARE\Policies\Microsoft\OneDrive" /v BlockExternalSync /t
REG_DWORD /d 1
```

On a Mac with the Apple Store version of OneDrive, use the equivalent of the following command to prevent B2B Sync:

Windows Command Prompt

```
defaults write com.microsoft.OneDrive-mac BlockExternalSync -bool YES
```

On a Mac with the Standalone version of OneDrive, use the equivalent of the following command to prevent B2B Sync:

Windows Command Prompt

```
defaults write com.microsoft.OneDrive BlockExternalSync -bool YES
```

Last updated on 12/19/2025

Block syncing of specific file types

Article • 04/10/2025

You can prevent users from uploading specific file types when they sync their OneDrive files.

This setting prevents file types from being uploaded but not downloaded. If users already blocked file types in their OneDrive, the files sync to their computer, but any changes they make on their computer aren't uploaded.

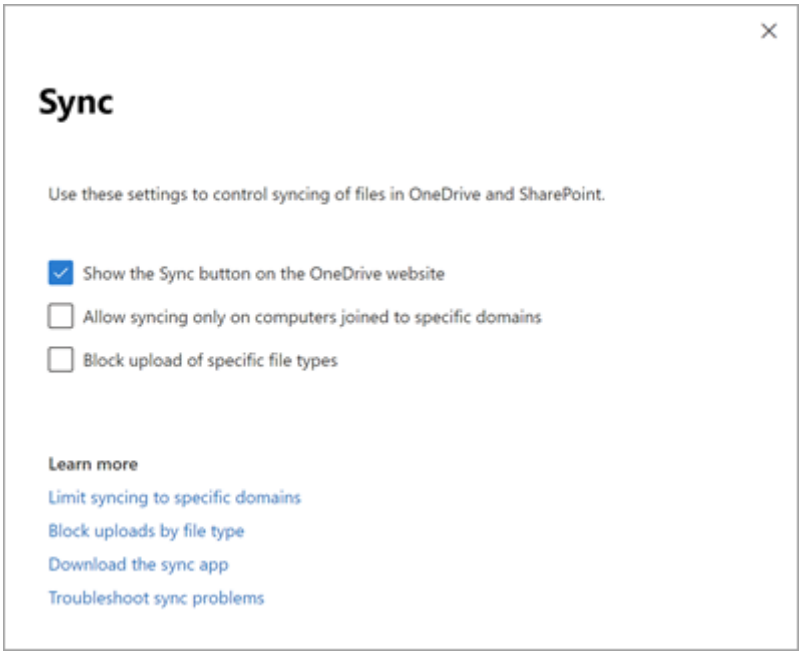
> **Note**
>
> The OneDrive sync app doesn't sync .tmp and .ini files.

To block uploading of specific file types

1. Go to Settings in the SharePoint admin center, and sign in with an account that has admin permissions for your organization.

   > **Note**
   >
   > If you have Office 365 operated by 21Vianet (China), sign in to the Microsoft 365 admin center, then browse to the SharePoint admin center and open the Sharing page.

2. Select **Sync**.



3. Select the **Block upload of specific file types** check box.

4. Enter the file name extensions you want to block, for example: **exe** or **mp3**.

> **Important**
>
> Don't include the periods with the extensions, or any other punctuation, spaces, or special characters.

5. Select **Save**.

> **Note**
>
> When you configure this setting, it takes approximately 8 hours for the OneDrive sync app to detect it and apply the change.

For info about setting this sync app restriction by using PowerShell, see Set-SPOTenantSyncClientRestriction. For info about using a policy to block upload of specific files, see Exclude specific kinds of files from being uploaded.

OneDrive sync reports in the Apps Admin Center

Use the OneDrive sync health dashboard in the Microsoft 365 Apps Admin Center to get an executive summary of everything happening with OneDrive so that you can resolve common issues quickly and focus on other strategic tasks as an administrator.

Proactively keeping OneDrive healthy helps ensure that your organization's information is protected. The dashboard provides you with sync health reports for tracking relevant health issues and advisories, checking the sync status and app version of individual devices, and monitoring Known Folder Move roll out.

In this article, you learn how to set up and navigate the sync health dashboard to better manage your OneDrive users and increase OneDrive adoption.

Requirements

Before getting started, be sure that you're familiar with the requirements needed to access the dashboard:

- OneDrive sync app version 22.232 or later for Windows and macOS.
- OneDrive sync apps on the Insiders, Production, or Deferred ring. Set the sync app update ring.
- Office Apps Administrator or Microsoft 365 Administrator role access is required to enable and set up the dashboard for your organization. After the feature is enabled by one of these roles, one can also view the dashboard using Global Reader, Security Administrator, Office Apps Administrator, or Reports Reader access. To learn more about administrator roles and permissions in Microsoft 365, visit About Admin Roles.
- Devices in your organization should allow connections to `https://clients.config.office.net`.

> **Note**
>
> This feature isn’t available to customers who have Office 365 operated by 21Vianet.

Set up the OneDrive sync health dashboard

In this section, you learn how to set up sync reports on Windows and macOS devices.

Windows

This tab provides how-to steps for enabling sync reports on Windows devices.

> **Note**
>
> The previous Group Policy HKLM\SOFTWARE\Policies\Microsoft\OneDrive\SyncAdminReports is no longer supported, and machines using that key will no longer appear in the sync health dashboard. Admins need to switch to the currently supported key (additional information below): HKLM\SOFTWARE\Policies\Microsoft\OneDrive\EnableSyncAdminReports.

1. Ensure you have the required role and app versions listed in the previous section.
2. Go to Microsoft 365 Apps admin center and sign in as an Office App Administrator.
3. From the left navigation menu, select **Health** > **OneDrive Sync**.
4. In the left navigation menu, select **Setup**.
5. Verify that a **Tenant Association Key** is present in the text field. If the field is empty, select **Generate new key**. When you generate a new key for the first time, it can take up to 30 seconds for it to appear.

   > **Note**
   >
   > Customers who have Office 365 GCC or Office 365 GCC High and DoD do not need a **Tenant Association Key**.

6. Enable the OneDrive EnableSyncAdminReports Group Policy Object (GPO).

   > **Important**
   >
   > **You must enable this setting on the devices from which you want to get reports.** This setting doesn't affect users. We recommend a gradual rollout starting with a

few test devices per day, then up to 100 devices per day, then gradually up to 10,000 devices per day until you finish.

You can enable this setting in multiple ways:

- Edit the registry

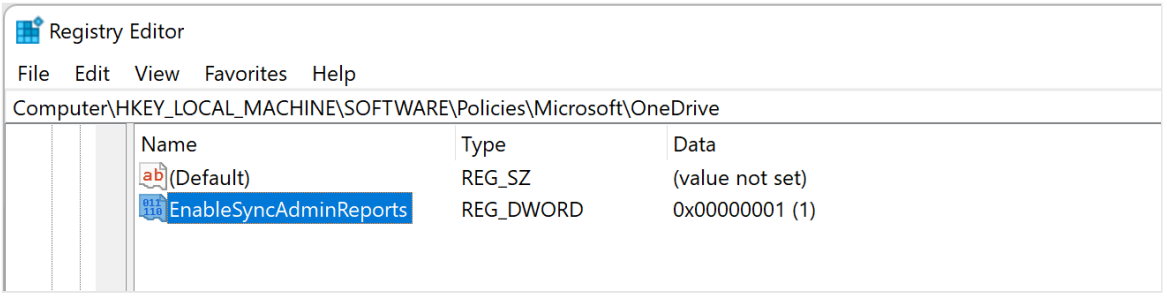
  a. Go to HKLM\SOFTWARE\Policies\Microsoft\OneDrive

  b. Right-click > **New** > **DWORD (32-bit) Value**

  c. Name: EnableSyncAdminReports

  d. Type: REG_DWORD

  e. Data: 1



- Run Command Prompt as an administrator, and then run the following command:

  PowerShell

  ```
  reg.exe add HKLM\Software\Policies\Microsoft\OneDrive /v EnableSyncAdminReports /t REG_DWORD /d 1
  ```

- Use Group Policy.

To apply the setting on a single PC, follow these steps:

- Open Group Policy Editor (gpedit.msc).
- Go to Computer Configuration\Administrative Templates\OneDrive.
- Choose **Enable sync health reporting for OneDrive**.
- Select **Enabled** and then press **OK**.

ⓘ Important

When you enable the EnableSyncAdminReports setting on devices, it can take up to three days for reports to be available. Devices will appear in the report after this time. Forcing a specific device to report data is unsupported.

> **Note**
>
> OneDrive sync health reports can also be enabled using administrative templates in Intune. For more information, see Use administrative templates in Intune.

Navigate the OneDrive Sync health dashboard

In this section, you'll learn how to successfully navigate the OneDrive Sync health dashboard. Learn about the reporting insights available to you and how they can help you proactively manage OneDrive for your organization.

Jump to:

- Overview
- Devices
- Issues
- Export data for custom reporting

> **Note**
>
> After you set up the dashboard as described in the previous section, the Global Reader admin role is sufficient to access and view reports.

Overview

The **Overview** tab (the default view) shows a summary of devices that have at least one sync issue, a percentage of the devices in your organization using Known folder move, and the number of devices running on the current version of OneDrive.

Expand table

Card name	Description
Sync errors	*Shows how many devices have sync errors or not.* Sorting through errors can help you proactively reach out to educate people while resolving common issues and improving user experience. Users may not report OneDrive issues to you immediately. Unreported issues could lead to unwanted problems while they're working on important tasks. With the **Sync errors** card, you won't have to wait to be notified by users to take action.
Known folders	*Shows a snapshot of the number of known folders currently in use.* **Known Folder Move** allows people to keep their Desktop, Documents, and Pictures folders protected by syncing them to the cloud with OneDrive. If you're rolling out Known Folder Move for your organization, the **Known folders** card is a great way for you to monitor progress.
Sync app version	*Shows the number of devices running on the current version of OneDrive.* Running the current version of OneDrive helps users stay up to date with all the latest and greatest fixes and features from Microsoft. Hover over the **Sync app version** card for a filtered view of operating systems on the current version. Note: Mac App store devices are excluded from this section and will appear in the count as "devices excluded".

Devices

The **Devices** tab shows all users, their current health state, their known folders currently moved in OneDrive, their current app version and operating system version, a timestamp of the last time the app was fully up to date, and a timestamp of the last time the sync app reported health data to the dashboard. The last status reported timestamp (UTC) is updated every ~36 hours, or ~1 hour after the client starts up. An icon and status in the **Errors** column indicate the state of each device.

This table provides a summary of the information found in each column of the **Devices** tab:

Expand table

Column name	Description
User	The name of the user
User email	The user's email address
Device name	The device name
Errors	The health status of a device

Column name	Description
Known folders	The name of folders moved to OneDrive
App version	The current version of OneDrive running on the device
Operating system	The current version of the OS running on the device
Last synced timestamp (UTC)	The last time that the sync app was fully up to date with the cloud
Last status reported timestamp (UTC)	The last time that the sync app reported health data to the dashboard

Customize your view of which devices show up on the dashboard by using the filter option in the command bar. Standard filters include "all devices" where you can see every device and "devices with errors" where you'll only see devices with errors.

You can easily create a custom filter with your own conditions. From the command bar, select **Filter** > **New filter** to open the **Custom filter** panel. Name your filter and select your desired conditions. If you'd like to filter by app version, be sure that you enter the complete sync app version number including periods. Afterwards, select **Create** to use your new filter.

When someone in your organization reports a problem with syncing files to OneDrive, you can investigate quickly without having to ask for extra details of the error message via Microsoft Teams chat or Outlook email. Select a user to see more information on their device and sync status. This detailed view lets you see a user's essential OneDrive information including any errors they might be experiencing.

Issues

The **Issues** tab shows you a list of OneDrive error messages found in the health report and the number of devices affected by them in your organization. Use this view to see if there are any common patterns between users and the errors present across your organization.

You can learn more about the error and devices affected by selecting an error message from the list. The **Issues** panel appears with a summary of the devices affected, along with a list of users and their current app version and operating system. Partner with your users to fix common OneDrive sync issues.

To learn more about OneDrive error messages, see What do the OneDrive error codes mean?.

Export sync health data for custom reporting

Use the dashboard for day-to-day monitoring and troubleshooting. If you need to retain data, build custom reports, or combine sync health data with other organizational data, use Microsoft Graph Data Connect to copy the data to a supported destination that you manage.

Microsoft Graph Data Connect provides the following OneDrive datasets:

- `BasicDataSet_v0.OneDriveSyncHealth_v1` contains information about report-enabled devices, including the user, device, operating system, sync app version, update ring, Known Folder Move status, error count, and last-synced and last-status-reported timestamps.
- `BasicDataSet_v0.OneDriveSyncErrors_v1` contains details about sync errors. Join this dataset with the sync health dataset by using the `OneDriveDeviceId` property.

For the complete schemas, see Microsoft Graph Data Connect datasets.

> **Important**
>
> Sync health data can include user and device information. Before you export data, plan how you'll restrict access, apply your organization's retention requirements, and monitor the Azure resources that store and process the data. Microsoft Graph Data Connect and the Azure services used by your pipeline can incur charges.

Before you begin

Make sure that:

- You've set up the OneDrive sync health dashboard. Only devices that have sync health reporting enabled are included in the dataset.
- Your Microsoft 365 tenant and Azure subscription are in the same Microsoft Entra tenant.
- You have a Global Administrator to enable Microsoft Graph Data Connect and approve the application.
- A different user has the Application Administrator or Application Developer role to register the application. The user who registers the application can't also approve it.
- The user who creates the Azure resources has sufficient permissions in the Azure subscription to create the selected compute and destination resources and assign the required roles.
- Your Azure storage and compute resources are in a region supported for your Microsoft 365 data location.
- If your organization uses Microsoft 365 Multi-Geo, you plan a separate pipeline for each region that you need to extract. A single pipeline can't extract data from multiple Microsoft

365 regions.

Configure Microsoft Graph Data Connect

1. Follow Build your first Microsoft Graph Data Connect application to:

    - Enable Microsoft Graph Data Connect in the Microsoft 365 admin center.
    - Register a single-tenant Microsoft Entra application.
    - Create the compute and destination resources for your pipeline.
    - Assign the application the permissions required for the selected destination. For Azure Blob Storage or Azure Data Lake Storage Gen2, assign the **Storage Blob Data Contributor** role.

2. In the Microsoft Graph Data Connect registration wizard in the Azure portal, select the compute type, activity type, and destination that you intend to use. Make sure that the destination URI and the pipeline linked service match. For example, use an Azure Data Lake Storage Gen2 linked service for a DFS URI and an Azure Blob Storage linked service for a blob URI.

    Add `BasicDataSet_v0.OneDriveSyncHealth_v1`. Add `BasicDataSet_v0.OneDriveSyncErrors_v1` if you need detailed error information. Select only the columns required for your reporting scenario.

3. Ask the Global Administrator to approve the application:
    a. In the Microsoft 365 admin center, go to **Settings** > **Org settings**.
    b. On the **Security & privacy** tab, select **Microsoft Graph Data Connect applications**.
    c. Select the application, review its datasets, columns, and destination, and then select **Approve**.

4. Create a pipeline by using Microsoft Fabric, Azure Synapse, or Azure Data Factory. Select a compute, activity, and destination combination supported by Microsoft Graph Data Connect, and make sure that the choices match the application registration. Configure:

    - **Source:** Microsoft 365 (Office 365).
    - **Dataset:** `BasicDataSet_v0.OneDriveSyncHealth_v1` and, if needed, `BasicDataSet_v0.OneDriveSyncErrors_v1`.
    - **Sink:** A supported Azure storage destination.
    - **Authentication:** The service principal for the approved Microsoft Entra application.

    For detailed pipeline instructions, see Set up your pipeline resource.

5. Validate and publish the pipeline, and then run it. Monitor the pipeline until its status is **Succeeded**, and verify that the output is available in your storage destination.

For copy activities, Microsoft Graph Data Connect writes JSON output. The sync health dataset captures daily records and doesn't support delta extraction. The sync errors dataset covers the preceding 30 days and also doesn't support delta extraction. For recurring runs, write each extraction to a run-specific path and account for overlapping records when you build historical reports.

Analyze the exported data

You can use Power BI or another analytics tool that can read the destination used by your pipeline. To analyze the data in Power BI:

1. In Power BI Desktop, select **Get data** and connect to the destination used by your pipeline.
2. Select or transform the output from the pipeline. For JSON output from a copy activity, exclude pipeline metadata files before combining the data files, if applicable.
3. Use fields such as `SyncAppVersion`, `OSName`, `LastSyncedTimestampUTC`, and `KFMEnabledFolders` to create the views required by your organization.
4. If you exported both datasets for a single reporting period, relate the sync health and sync errors data by using `OneDriveDeviceId`. If you retain multiple extractions, add the extraction date or run identifier to your model and deduplicate or filter records to the reporting period you want to analyze.

For an example of connecting Power BI to Azure Data Lake Storage Gen2, see Analyze data in Azure Data Lake Storage Gen2 by using Power BI.

Data for the OneDrive sync health dashboard

The sync reports use health data that your OneDrive sync apps send to Microsoft. You have choices when it comes to the technology you use and the data you share. Use the EnableSyncAdminReports setting to manage which devices send data.

To learn more about the controls available to you, see Overview of privacy controls for Microsoft 365 Apps. To learn more about required service data, see Required service data for Office.

Known limitations and considerations

This section describes known limitations and considerations in sync reporting.

Limitations

Device Records: By default, device records are kept in inventory for 30 days, after which they expire from the report.

Folders in OneDrive: Devices with folders in OneDrive appear in reports as a device with 0-3 known folders. If a device hasn't enabled folders in OneDrive, it appears in reports as a device that is **Not eligible** in the **Known Folders** section of the **Overview** tab. In the **Devices** tab, a hyphen ("-") will appear in the cell value of the **Known folders** table for devices that aren't applicable devices. This behavior is expected.

Sync app version: Mac App Store edition: For devices using the Mac App Store edition of the sync app, the version installed on each device is displayed in the **Devices** tab. The dashboard doesn't currently track whether or not the Mac App Store edition is the latest version of the sync app available in the Mac App Store. If any devices use this edition, they are excluded from the **Sync app version** section of the **Overview** tab and the number of excluded devices is displayed. This is the expected result.

Minimum time device is on for eligibility: Devices need to be turned on for a minimum of five hours to be eligible for the report. Devices that are turned off frequently and not on for that amount of time might be missing from the dashboard, even if the group policy is set.

User sign-in: Clients won't report status to the report if the user is signed out.

Considerations

- There's negligible impact to a network after enabling the sync reports setting on devices.
- Microsoft continues its commitment to meet and exceed the requirements of EU data protection laws. All data storage is EU Data Boundary compliant.
- There are no Power BI templates available for sync reports.
- Admins see errors based on the user's client language, not in the admin's configured language.

Troubleshooting

Use this section to troubleshoot if the OneDrive sync reports don't appear after three days.

> **Important**

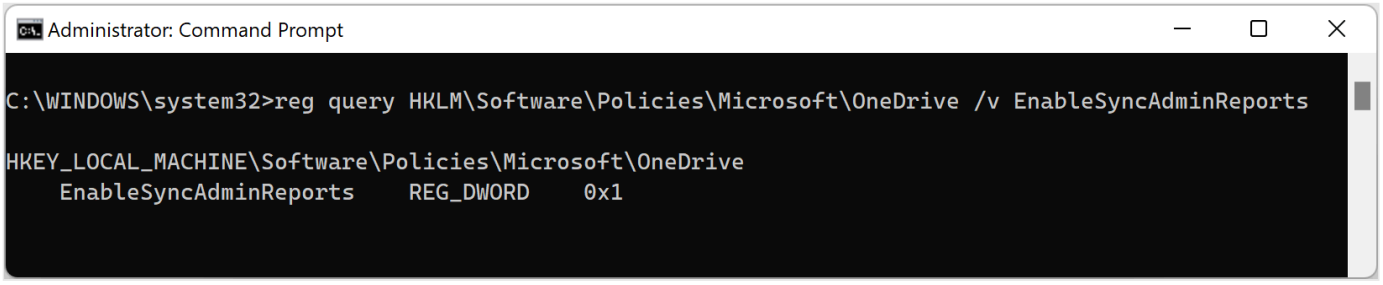
> If you enable the EnableSyncAdminReports setting on devices that don't meet the requirements, it has no effect. The app won't send reports.

Confirm that the EnableSyncAdminReports setting is applied to the device. Run Command Prompt as an administrator, and then run the following command:

PowerShell

```
reg.exe query HKLM\Software\Policies\Microsoft\OneDrive /v EnableSyncAdminReports
```

The output should look like this:



If the EnableSyncAdminReports setting wasn't applied, go back and follow the steps under Set up the OneDrive sync health dashboard.

If the setting was applied correctly, wait for 36 hours with the device turned on and signed in to OneDrive. If the device still doesn't appear on the dashboard, open a support ticket with Microsoft. For more information, see the next section, Report a problem.

Report a problem

If you encounter a problem with viewing the report dashboard, first verify that you've completed the steps in the troubleshooting section.

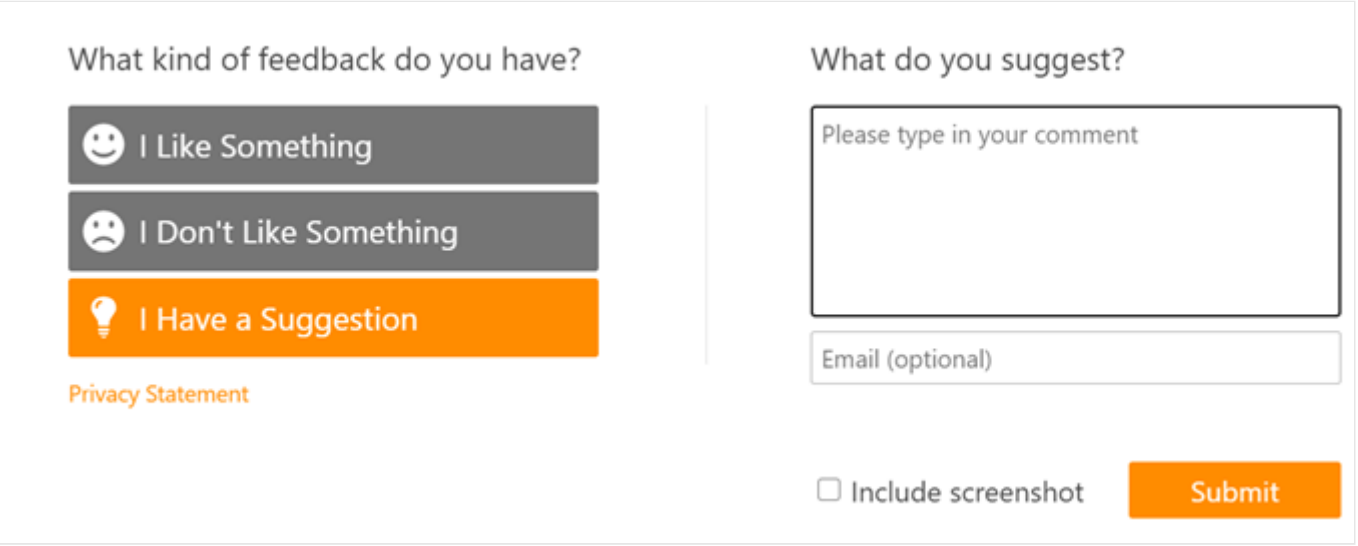
If problems persist after troubleshooting, open a support ticket with Microsoft. Make sure that the device isn't powered off during this period so that the sync app can still run and send a health report.

For quick investigations, be sure to have the date and time when the EnableSyncAdminReports setting was enabled and either the user's email or the OneDrive device ID available in your issue report.

To get the OneDrive device ID, select the OneDrive sync app in the notification area > **Help & Settings** > **Settings** > **About**.

Send feedback

We value your feedback. To submit feature suggestions and report issues, you can use the Feedback button in the top-right corner of the dashboard page.



Last updated on 10/14/2026

OneDrive Sync Release Notes

> **Note**
>
> New versions roll out gradually, so if your version number is higher than the versions listed here, your device is running a newer build that this page doesn't yet reflect.

> **Important**
>
> If you're not getting the latest updates automatically, check that you don't have any Family Safety settings, browser extensions, or firewall rules that are blocking access to OneDrive's "oneclient.sfx.ms" and "g.live.com" domains.

> **Important**
>
> The OneDrive sync app requires Windows 10 22H2 or Windows 11 to receive updates. After August 15, 2026, devices running earlier versions of Windows 10 will remain on their currently installed version and will not receive new releases listed on this page. For details, see OneDrive system requirements.

Windows

Current Version

Expand table

Ring	Released	Rolling Out
Production	26.173.0906.0008 (amd64 | arm64)	26.178.0913.0006 (amd64 | arm64)
Deferred	26.123.0628.0001 (amd64 | arm64)	

What's New

- We resolved product issues to improve the reliability and performance of the OneDrive sync app.
- **Copy links from Activity Center:** Users can now copy a link to a file directly from the per-item menu for recently synced files in the OneDrive Activity Center. (Version 26.150.0804.0010)
- **Browse your photos in OneDrive:** OneDrive now brings the photos experience from OneDrive on the web and mobile to your desktop, so you can browse, search, and organize photos from your OneDrive and your PC in one place. Available for personal Microsoft accounts. Select **View photos** in the OneDrive activity center to open it. Learn more (Version 26.123.0628.0001)
- **Improved max path handling for OneDrive shortcuts:** OneDrive now uses the correct root path when checking Folder Shortcuts against the maximum path length, so fewer files are incorrectly flagged as exceeding the limit. (Version 26.119.0622.0003)
- **Clearer sync status messages:** OneDrive sync status messages in File Explorer, the Windows notification area, and the OneDrive Activity Center are now clearer and more consistent. We removed outdated status strings and refreshed key states, so "Your files are synced" and "Up to date" now read "Backed up and synced." (Version 26.074.0420.0001)
- **Move folders to OneDrive from File Explorer:** Right-click any folder in File Explorer to move it directly to OneDrive, making it easier to back up and sync local folders. (Version 26.045.0308.0003)

Windows Production Ring

26.178.0913.0006 (October 2, 2026)

- We resolved product issues to improve the reliability and performance of the OneDrive sync app.

26.173.0906.0008 (September 25, 2026)

- We resolved product issues to improve the reliability and performance of the OneDrive sync app.

26.168.0830.0006 (September 18, 2026)

- We resolved product issues to improve the reliability and performance of the OneDrive sync app.

26.163.0823.0004 (September 11, 2026)

- We resolved product issues to improve the reliability and performance of the OneDrive sync app.

26.158.0816.0002 (September 4, 2026)

- We resolved product issues to improve the reliability and performance of the OneDrive sync app.

26.153.0809.0004 (August 28, 2026)

- We resolved product issues to improve the reliability and performance of the OneDrive sync app.

26.150.0804.0011 (August 21, 2026)

- We resolved product issues to improve the reliability and performance of the OneDrive sync app.
- New features gradually rolling out:
  - **Copy links from Activity Center:** Users can now copy a link to a file directly from the per-item menu for recently synced files in the OneDrive Activity Center.
  - **Check in and check out synced files:** Users with work or school accounts can now check files in and out of SharePoint document libraries that require check-out. When you check out a file, its synced copy becomes editable locally instead of read-only, and Check In and Check Out commands are available from the right-click menu in File Explorer. Checking a file back in restores the read-only state.

26.145.0728.0011 (August 14, 2026)

- We resolved product issues to improve the reliability and performance of the OneDrive sync app.

26.139.0720.0007 (August 7, 2026)

- We resolved product issues to improve the reliability and performance of the OneDrive sync app.
- New features gradually rolling out:
  - **Self-service file exclusions:** Users with work or school accounts can now exclude specific files from syncing to OneDrive or SharePoint. Administrators can hide these

controls with the DisableChangesToODIgnoreList policy to keep exclusions organization-managed.
    - **Control the default exclusion list:** The new DisableDefaultODIgnoreList policy lets administrators opt out of Microsoft's built-in default exclusion list, which is expanding to include more file types over time.

26.134.0713.0007 (July 31, 2026)

- We resolved product issues to improve the reliability and performance of the OneDrive sync app.
- New features gradually rolling out:
    - **Exclude specific folders from syncing:** Administrators can use a new Group Policy setting to keep folders with specific names on the device rather than uploading them to OneDrive or SharePoint. Existing synced content is not affected.

26.129.0706.0004 (July 24, 2026)

- We resolved product issues to improve the reliability and performance of the OneDrive sync app.

26.123.0628.0001 (July 17, 2026)

- We resolved product issues to improve the reliability and performance of the OneDrive sync app.
- New features gradually rolling out:
    - **Browse your photos in OneDrive:** OneDrive now brings the photos experience from OneDrive on the web and mobile to your desktop, so you can browse, search, and organize photos from your OneDrive and your PC in one place. Available for personal Microsoft accounts. Select **View photos** in the OneDrive activity center to open it. Learn more

26.119.0622.0003 (July 10, 2026)

- We resolved product issues to improve the reliability and performance of the OneDrive sync app.
- New features gradually rolling out:
    - **Improved max path handling for OneDrive shortcuts:** OneDrive now uses the correct root path when checking Folder Shortcuts against the maximum path length, so fewer files are incorrectly flagged as exceeding the limit.

26.113.0614.0004 (July 3, 2026)

- We resolved product issues to improve the reliability and performance of the OneDrive sync app.

26.108.0607.0002 (June 26, 2026)

- We resolved product issues to improve the reliability and performance of the OneDrive sync app.

26.106.0603.0003 (June 19, 2026)

- We resolved product issues to improve the reliability and performance of the OneDrive sync app.

26.098.0524.0004 (June 12, 2026)

- We resolved product issues to improve the reliability and performance of the OneDrive sync app.

26.095.0519.0003 (June 5, 2026)

- We resolved product issues to improve the reliability and performance of the OneDrive sync app.

26.088.0510.0004 (May 29, 2026)

- We resolved product issues to improve the reliability and performance of the OneDrive sync app.

26.084.0504.0007 (May 26, 2026)

- We resolved product issues to improve the reliability and performance of the OneDrive sync app.

26.078.0426.0002 (May 15, 2026)

- We resolved product issues to improve the reliability and performance of the OneDrive sync app.
- New features gradually rolling out:
  - **Clearer sync status messages:** OneDrive sync status messages in File Explorer, the Windows notification area, and the OneDrive Activity Center are now clearer and

more consistent. We removed outdated status strings and refreshed key states, so "Your files are synced" and "Up to date" now read "Backed up and synced."

26.070.0414.0001 (May 1, 2026)

- We resolved product issues to improve the reliability and performance of the OneDrive sync app.

26.063.0405.0002 (April 24, 2026)

- We resolved product issues to improve the reliability and performance of the OneDrive sync app.

26.062.0402.0002 (April 17, 2026)

- We resolved product issues to improve the reliability and performance of the OneDrive sync app.

26.055.0323.0004 (April 10, 2026)

- We resolved product issues to improve the reliability and performance of the OneDrive sync app.

26.051.0316.0004 (April 4, 2026)

- We resolved product issues to improve the reliability and performance of the OneDrive sync app.

26.045.0308.0003 (March 27, 2026)

- We resolved product issues to improve the reliability and performance of the OneDrive sync app.
- New features gradually rolling out:
  - **Move folders to OneDrive from File Explorer:** Right-click any folder in File Explorer to move it directly to OneDrive, making it easier to back up and sync local folders.

26.040.0301.0001 (March 20, 2026)

- We resolved product issues to improve the reliability and performance of the OneDrive sync app.

26.035.0222.0002 (March 13, 2026)

- We resolved product issues to improve the reliability and performance of the OneDrive sync app.

26.032.0217.0003 (March 6, 2026)

- We resolved product issues to improve the reliability and performance of the OneDrive sync app.
- New features gradually rolling out:
  - **Improved First Run Experience:** The OneDrive first-run setup experience has been rebuilt with a modern, streamlined interface for faster and simpler account configuration.
  - **Custom OneDrive folder name:** Administrators can now set a custom name for the local OneDrive sync folder on users' computers, replacing the default "OneDrive - {organization name}" convention. Shortening the folder name increases available path length for nested files and folders. Learn more

26.026.0209.0004 (February 27, 2026)

- We resolved product issues to improve the reliability and performance of the OneDrive sync app.

26.022.0203.0006 (February 20, 2026)

- We resolved product issues to improve the reliability and performance of the OneDrive sync app.
- Folders that contain only content excluded from sync now remain on disk as local-only when deleted from the cloud.

26.017.0126.0002 (February 13, 2026)

- We resolved product issues to improve the reliability and performance of the OneDrive sync app.

26.012.0119.0002 (February 6, 2026)

- We resolved product issues to improve the reliability and performance of the OneDrive sync app.

26.007.0112.0002 (January 30, 2026)

- We resolved product issues to improve the reliability and performance of the OneDrive sync app.

26.002.0105.0001 (January 23, 2026)

- We resolved product issues to improve the reliability and performance of the OneDrive sync app.
- New features gradually rolling out:
  - **Mark of the Web for Outlook attachments:** Email attachments saved to OneDrive from Outlook now include the Mark of the Web (MOTW) security tag, ensuring Windows security features like Protected View apply when these files are opened.

25.243.1211.0001 (January 19, 2026)

- We resolved product issues to improve the reliability and performance of the OneDrive sync app.

25.238.1204.0001 (January 12, 2026)

- We resolved product issues to improve the reliability and performance of the OneDrive sync app.

25.224.1116.0003 (January 5, 2026)

- We resolved product issues to improve the reliability and performance of the OneDrive sync app.

▼ 2025 releases

25.222.1112.0002 (December 9, 2025)

- We resolved product issues to improve the reliability and performance of the OneDrive sync app.

25.216.1104.0002 (December 3, 2025)

- We resolved product issues to improve the reliability and performance of the OneDrive sync app.

25.209.1026.0002 (November 17, 2025)

- We resolved product issues to improve the reliability and performance of the OneDrive sync app.

25.206.1021.0003 (November 10, 2025)

- We resolved product issues to improve the reliability and performance of the OneDrive sync app.

25.199.1012.0002 (November 3, 2025)

- We resolved product issues to improve the reliability and performance of the OneDrive sync app.
- New features gradually rolling out:
  - **OneDrive Sync Health Dashboard for Government Clouds:** The OneDrive Sync health dashboard now supports GCC, GCC High, and DoD environments, enabling administrators to proactively monitor sync health, identify issues, and streamline support operations.

25.194.1005.0003 (October 27, 2025)

- We resolved product issues to improve the reliability and performance of the OneDrive sync app.
- New features gradually rolling out:
  - **Copilot Actions in File Explorer and OneDrive Activity Center:** Users with a work or school account and a Microsoft 365 Copilot license can now use Copilot in File Explorer and OneDrive Activity Center to summarize documents, generate FAQs, compare files, or get answers about their files saved in OneDrive.

25.189.0928.0002 (October 20, 2025)

- We resolved product issues to improve the reliability and performance of the OneDrive sync app.
- New features gradually rolling out:
  - **SharePoint Server Subscription Edition Version 23H2 Support with OIDC Authentication:** OneDrive Sync now supports SharePoint Server Subscription Edition Version 23H2 with OIDC authentication using Entra ID, enabling modern authentication for on-premises SharePoint environments.

25.184.0921.0004 (October 13, 2025)

- We resolved product issues to improve the reliability and performance of the OneDrive sync app.

25.179.0914.0003 (October 6, 2025)

- We resolved product issues to improve the reliability and performance of the OneDrive sync app.

25.174.0907.0003 (September 29, 2025)

- We resolved product issues to improve the reliability and performance of the OneDrive sync app.
- **Refreshed OneDrive Icon**: The updated OneDrive icon introduces a cleaner, more modern look across all devices and apps.

25.170.0901.0003 (September 19, 2025)

- We resolved product issues to improve the reliability and performance of the OneDrive sync app.
- New features gradually rolling out:
  - **Improved Folder Backup Opt-Out Experience:** The PC Folder Backup (Known Folder Move) opt-out process is now more intuitive, letting users choose whether to keep files in OneDrive or move them back to their PC for greater clarity and control.

25.164.0824.0003 (September 12, 2025)

- We resolved product issues to improve the reliability and performance of the OneDrive sync app.
- New features gradually rolling out:
  - **LocalNetworkAccess Support:** Chromium v142+ requires browsers to prompt users or admins for access to OneDrive and SharePoint URLs to enable offline mode. For per-machine installations, OneDrive Sync automatically applies the required permissions and policies for existing users in Chrome and Edge. For per-user installations, OneDrive Sync prompts users via a notification to enable these permissions. Available for work or school accounts.

25.159.0817.0003 (September 5, 2025)

- We resolved product issues to improve the reliability and performance of the OneDrive sync app.

25.155.0811.0002 (August 29, 2025)

- We resolved product issues to improve the reliability and performance of the OneDrive sync app.

25.149.0803.0003 (August 22, 2025)

- We resolved product issues to improve the reliability and performance of the OneDrive sync app.
- **OneDrive offline mode process update:** On Windows, the process for offline mode is now called Microsoft OneDrive Sync Service (OneDrive.Sync.Service.exe), replacing Microsoft SharePoint (Microsoft.SharePoint.exe). The icon changed from SharePoint to OneDrive for improved clarity.

25.140.0720.0001 (August 8, 2025)

- We resolved product issues to improve the reliability and performance of the OneDrive sync app.

25.137.0715.0001 (July 31, 2025)

- We resolved product issues to improve the reliability and performance of the OneDrive sync app.

25.130.0706.0004 (July 25, 2025)

- We resolved product issues to improve the reliability and performance of the OneDrive sync app.
- New features gradually rolling out:
  - **Copilot Actions in File Explorer:** Users with Microsoft 365 Personal, Family, or Premium accounts can now use Copilot in File Explorer to summarize documents, generate FAQs, compare files, or get answers about their files saved in OneDrive.

25.127.0701.0005 (July 18, 2025)

- We resolved product issues to improve the reliability and performance of the OneDrive sync app.

25.122.0624.0003 (July 11, 2025)

- We resolved product issues to improve the reliability and performance of the OneDrive sync app.

25.115.0615.0002 (July 7, 2025)

- We resolved product issues to improve the reliability and performance of the OneDrive sync app.

25.110.0608.0001 (June 30, 2025)

- We resolved product issues to improve the reliability and performance of the OneDrive sync app.

25.105.0601.0002 (June 23, 2025)

- We resolved product issues to improve the reliability and performance of the OneDrive sync app.

25.095.0518.0002 (June 9, 2025)

- We resolved product issues to improve the reliability and performance of the OneDrive sync app.

25.091.0512.0001 (June 3, 2025)

- We resolved product issues to improve the reliability and performance of the OneDrive sync app.

25.085.0504.0002 (May 26, 2025)

- We resolved product issues to improve the reliability and performance of the OneDrive sync app.

25.080.0427.0003 (May 19, 2025)

- We resolved product issues to improve the reliability and performance of the OneDrive sync app.

25.075.0420.0002 (May 12, 2025)

- We resolved product issues to improve the reliability and performance of the OneDrive sync app.

25.070.0413.0001 (May 5, 2025)

- We resolved product issues to improve the reliability and performance of the OneDrive sync app.

25.065.0406.0002 (April 25, 2025)

- We resolved product issues to improve the reliability and performance of the OneDrive sync app.

25.060.0330.0003 (April 18, 2025)

- We resolved product issues to improve the reliability and performance of the OneDrive sync app.

25.056.0324.0003 (April 14, 2025)

- We resolved product issues to improve the reliability and performance of the OneDrive sync app.

25.051.0317.0003 (March 29, 2025)

- We resolved product issues to improve the reliability and performance of the OneDrive sync app.

25.046.0310.0005 (March 21, 2025)

- We resolved product issues to improve the reliability and performance of the OneDrive sync app.

25.041.0303.0002 (March 17, 2025)

- We resolved product issues to improve the reliability and performance of the OneDrive sync app.

25.035.0223.0003 (March 7, 2025)

- We resolved product issues to improve the reliability and performance of the OneDrive sync app.

25.031.0217.0003 (February 28, 2025)

- We resolved product issues to improve the reliability and performance of the OneDrive sync app.

25.025.0209.0001 (February 20, 2025)

- We resolved product issues to improve the reliability and performance of the OneDrive sync app.

25.020.0202.0001 (February 14, 2025)

- We resolved product issues to improve the reliability and performance of the OneDrive sync app.
- New features gradually rolling out:
  - **Unlicensed OneDrive accounts:** OneDrive Sync now shows a warning when a user does not have a license assigned. Accounts start in read-only mode and then they will be archived. Learn more

Windows Deferred Ring

26.123.0628.0001 (October 6, 2026)

- We resolved product issues to improve the reliability and performance of the OneDrive sync app.
- New features gradually rolling out:
  - **Improved max path handling for OneDrive shortcuts:** OneDrive now uses the correct root path when checking Folder Shortcuts against the maximum path length, so fewer files are incorrectly flagged as exceeding the limit.

26.078.0426.0002 (August 5, 2026)

- We resolved product issues to improve the reliability and performance of the OneDrive sync app.
- **Clearer sync status messages:** OneDrive sync status messages in File Explorer, the Windows notification area, and the OneDrive Activity Center are now clearer and more consistent. We removed outdated status strings and refreshed key states, so "Your files are synced" and "Up to date" now read "Backed up and synced."
- **Move folders to OneDrive from File Explorer:** Right-click any folder in File Explorer to move it directly to OneDrive, making it easier to back up and sync local folders.

26.040.0301.0001 (June 1, 2026)

- We resolved product issues to improve the reliability and performance of the OneDrive sync app.
- **Improved First Run Experience:** The OneDrive first-run setup experience has been rebuilt with a modern, streamlined interface for faster and simpler account configuration.
- **Custom OneDrive folder name:** Administrators can now set a custom name for the local OneDrive sync folder on users' computers, replacing the default "OneDrive - {organization name}" convention. Shortening the folder name increases available path length for nested files and folders. Learn more
- **Mark of the Web for Outlook attachments:** Email attachments saved to OneDrive from Outlook now include the Mark of the Web (MOTW) security tag, ensuring Windows security features like Protected View apply when these files are opened.

25.224.1116.0003 (March 24, 2026)

- We resolved product issues to improve the reliability and performance of the OneDrive sync app.
- **OneDrive Sync Health Dashboard for Government Clouds:** The OneDrive Sync health dashboard now supports GCC, GCC High, and DoD environments, enabling administrators to proactively monitor sync health, identify issues, and streamline support operations.
- **Copilot Actions in File Explorer and OneDrive Activity Center:** Users with a work or school account and a Microsoft 365 Copilot license can now use Copilot in File Explorer and OneDrive Activity Center to summarize documents, generate FAQs, compare files, or get answers about their files saved in OneDrive.
- **SharePoint Server Subscription Edition Version 23H2 Support with OIDC Authentication:** OneDrive Sync now supports SharePoint Server Subscription Edition Version 23H2 with OIDC authentication using Entra ID, enabling modern authentication for on-premises SharePoint environments.

25.179.0914.0003 (January 20, 2026)

- We resolved product issues to improve the reliability and performance of the OneDrive sync app.
- **Refreshed OneDrive Icon**: The updated OneDrive icon introduces a cleaner, more modern look across all devices and apps.
- **Improved Folder Backup Opt-Out Experience:** The PC Folder Backup (Known Folder Move) opt-out process is now more intuitive, letting users choose whether to keep files

in OneDrive or move them back to their PC for greater clarity and control.

- **LocalNetworkAccess Support:** Chromium v142+ requires browsers to prompt users or admins for access to OneDrive and SharePoint URLs to enable offline mode. For per-machine installations, OneDrive Sync automatically applies the required permissions and policies for existing users in Chrome and Edge. For per-user installations, OneDrive Sync prompts users via a notification to enable these permissions. Available for work or school accounts.
- **OneDrive offline mode process update:** On Windows, the process for offline mode is now called Microsoft OneDrive Sync Service (OneDrive.Sync.Service.exe), replacing Microsoft SharePoint (Microsoft.SharePoint.exe). The icon changed from SharePoint to OneDrive for improved clarity.

25.137.0715.0004 (October 13, 2025)

- We resolved product issues to improve the reliability and performance of the OneDrive sync app.
- **Copilot Actions in File Explorer:** Users with Microsoft 365 Personal, Family, or Premium accounts can now use Copilot in File Explorer to summarize documents, generate FAQs, compare files, or get answers about their files saved in OneDrive.

25.095.0518.0002 (August 18, 2025)

- We resolved product issues to improve the reliability and performance of the OneDrive sync app.

25.056.0324.0003 (June 9, 2025)

- We resolved product issues to improve the reliability and performance of the OneDrive sync app.
- New features gradually rolling out:
  - **Unlicensed OneDrive accounts:** OneDrive Sync now shows a warning when a user does not have a license assigned. Accounts start in read-only mode and then they will be archived. Learn more

25.005.0112.0003 (April 10, 2025)

- We resolved product issues to improve the reliability and performance of the OneDrive sync app.
- New features gradually rolling out:

- **Improved experience when adding a Folder Shortcut to an already syncing folder:** Users will be able to directly replace their existing syncing locations with the new Folder Shortcut.

Last updated on 10/07/2026

Overview of external sharing in SharePoint and OneDrive in Microsoft 365

> **Note**
>
> As of June 2024, invitations sent through the legacy SharePoint Invitation Manager no longer grant access. Users must reshare documents to generate valid invitations.

External sharing in SharePoint and OneDrive allows users to share content with people outside your organization, such as partners, vendors, clients, or customers. You can also use external sharing to share between licensed users on multiple Microsoft 365 subscriptions. External sharing in SharePoint is part of secure collaboration with Microsoft 365. Also see Overview of external collaboration options in Microsoft 365.

> **Important**
>
> Trial tenants can use SharePoint's robust collaboration features, but the scope of external sharing is restricted compared to licensed tenants. This restriction helps prevent potential abuse and ensures a safe experience for all users.

Include external sharing as part of your overall permissions planning for SharePoint and OneDrive. This article describes what happens when users share, depending on what they're sharing and with whom.

If you want to get straight to setting up sharing, choose the scenario you want to enable:

- Collaborate with guests on a document
- Collaborate with guests in a site
- Collaborate with guests in a team

(If you're trying to share a file or folder, see Share OneDrive files and folders or Share SharePoint files or folders in Microsoft 365.)

> **Note**

External sharing is turned on by default for your entire SharePoint and OneDrive environment. You might want to turn it off globally before people start using sites or until you know exactly how you want to use the feature.

How do SharePoint and OneDrive integrate with Microsoft Entra B2B?

SharePoint and OneDrive use two external sharing models:

- SharePoint external authentication
- SharePoint and OneDrive integration with Microsoft Entra B2B

When you use Microsoft Entra B2B integration, Microsoft Entra external collaboration settings, such as guest invite settings and collaboration restrictions, apply.

The following table shows the differences between the two sharing models.

Expand table

Sharing method	What happens when sharing files and folders?	What happens when sharing sites?
SharePoint external authentication (Microsoft Entra B2B integration not enabled)	No guest account created* Microsoft Entra settings don't apply	N/A (Microsoft Entra B2B always used)
Microsoft Entra B2B integration enabled	Guest account always created Microsoft Entra settings apply	Guest account always created Microsoft Entra settings apply

*A guest account might already exist from another sharing workflow, such as sharing a team, in which case it's used for sharing.

For information on how to enable or disable Microsoft Entra B2B integration, see SharePoint and OneDrive integration with Microsoft Entra B2B.

How do external sharing settings work?

SharePoint has external sharing settings at both the organization level and the site level (previously called the "site collection" level). To allow external sharing on any site, you must allow it at the organization level. You can then restrict external sharing for other sites. If a site's external

sharing option and the organization-level sharing option don't match, the most restrictive value always applies. OneDrive sharing settings can be the same as or more restrictive than the SharePoint settings.

Whichever option you choose at the organization or site level, the more restrictive functionality is still available. For example, if you choose to allow unauthenticated sharing by using "Anyone" links, users can still share with guests, who sign in, and with internal users.

> **Note**
>
> Even if your organization-level setting allows external sharing, not all new sites allow it by default. See Default site sharing settings for more information.

What are the security and privacy considerations?

If you have confidential information that you shouldn't share externally, store it in a site that has external sharing turned off. Create extra sites as needed for external sharing. This approach helps you manage security risk by preventing external access to sensitive information.

> **Note**
>
> To limit *internal* sharing of contents on a site, you can prevent site members from sharing, and enable access requests. For info, see Set up and manage access requests .
>
> When users share a folder with multiple guests, the guests can see each other's names in the Manage Access panel for the folder (and any items within it).

How do I share Microsoft 365 group-connected team sites?

When you or your users create Microsoft 365 groups (for example in Outlook, or by creating a team in Microsoft Teams), you also create a SharePoint team site. Admins and users can also create team sites in SharePoint, which creates a Microsoft 365 group. For group-connected team sites, the group owners are site owners, and the group members are site members. In most cases, you want to share these sites by adding people to the Microsoft 365 group. However, you can share only the site.

> **Important**
>
> It's important that all group members have permission to access the team site. If you remove the group's permission, many collaboration tasks (such as sharing files in Teams chats) won't work. Only add guests to the group if you want them to access the site. For info about guest access to Microsoft 365 groups, see Manage guest access in Groups.

What happens when users share content?

When users share with people outside the organization, an invitation is sent to the person in email, which contains a link to the shared item.

Because these guests don't have a license in your organization, they're limited to basic collaboration tasks:

- They can use Office.com for viewing and editing documents. If your plan includes Office Professional Plus, they can't install the desktop version of Office on their own computers unless you assign them a license.
- They can perform tasks on a site based on the permission level that you give them. For example, if you add a guest as a site member, they have Edit permissions and they can add, edit, and delete lists. They can also view, add, update, and delete list items and files.
- They can see other types of content on sites, depending on the permissions you give them. For example, they can navigate to different subsites within a shared site. They can also do things like view site feeds.

If your authenticated guests need greater capability such as OneDrive storage or creating a Power Automate flow, you must assign them an appropriate license.

How do I stop sharing?

To stop sharing with guests, remove their permissions from the shared item or remove them as a guest in your directory.

To stop sharing with people who have an *Anyone* link, go to the file or folder that you shared and delete the link or turn off *Anyone* links for the site.

Learn how to stop sharing an item

Need more help?

If you have technical questions about this topic, you might find it helpful to post them on the SharePoint discussion forum. It's a great resource for finding others who have worked with similar issues or who have encountered the same situation.

See also

Searching for site content shared externally

Configure Teams with three tiers of protection

Create a secure guest sharing environment

Settings interactions between Microsoft 365 Groups, Teams and SharePoint

Pricing - Active Directory External Identities

Last updated on 05/07/2026

Manage sharing settings for SharePoint and OneDrive in Microsoft 365

As a SharePoint Administrator in Microsoft 365, you can change the organization-level sharing settings for SharePoint and OneDrive. These settings control sharing at the organization level. You can configure more restrictive settings for specific sites if needed.

For end-to-end guidance on how to configure guest sharing in Microsoft 365, see:

- Set up secure collaboration with Microsoft 365
- Collaborate with guests on a document
- Collaborate with guests in a site
- Collaborate with guests in a team

To change the sharing settings for a site after you set the organization-level sharing settings, see Change sharing settings for a site. To learn how to change the external sharing setting for a specific user's OneDrive, see Change the external sharing setting for a user's OneDrive.

> **Tip**
>
> As a companion to this article, see our **Microsoft Sharepoint setup guide** to review best practices and understand the deployment process from site creation to data migration. Features include protection labels, data loss prevention policies, and file activity auditing. For a customized experience based on your environment, you can access the **Set up SharePoint in Microsoft 365 guide** in the Microsoft 365 admin center.

How do SharePoint and OneDrive integrate with Microsoft Entra B2B?

SharePoint and OneDrive use two external sharing models:

- SharePoint external authentication
- SharePoint and OneDrive integration with Microsoft Entra B2B

When you use Microsoft Entra B2B integration, Microsoft Entra external collaboration settings, such as guest invite settings and collaboration restrictions, apply.

The following table shows the differences between the two sharing models.

Expand table

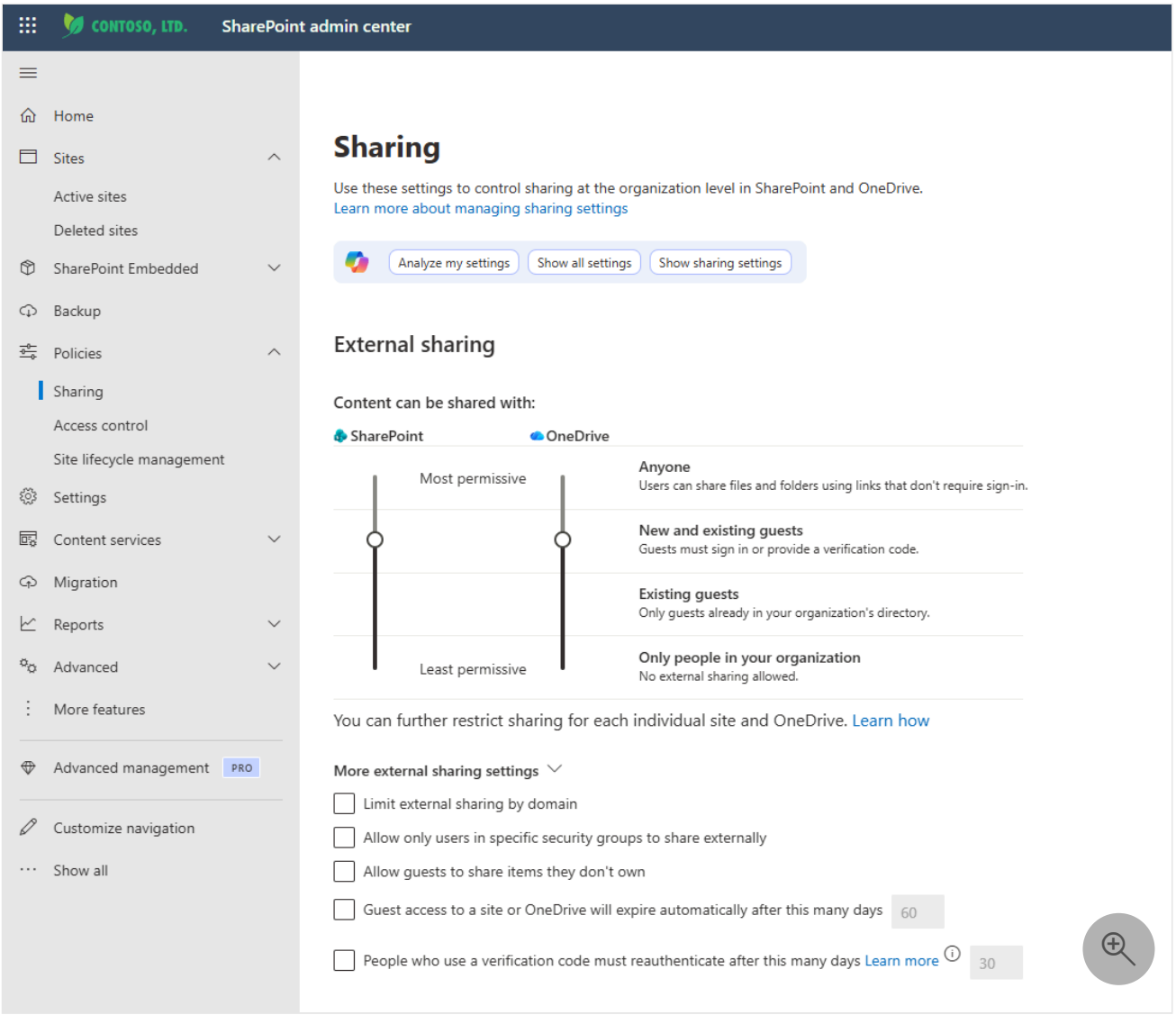
Sharing method	Files and folders	Sites
SharePoint external authentication (Microsoft Entra B2B integration not enabled)	No guest account created (see the note following this table) Microsoft Entra settings don't apply	N/A (Microsoft Entra B2B always used)
Microsoft Entra B2B integration enabled	Guest account always created Microsoft Entra settings apply	Guest account always created Microsoft Entra settings apply

> **Note**
>
> A guest account might already exist from another sharing workflow, such as sharing a team, in which case it's used for sharing.

For information on how to enable or disable Microsoft Entra B2B integration, see SharePoint and OneDrive integration with Microsoft Entra B2B.

Change organization-level external sharing setting

1. In the SharePoint admin center, expand **Policies**, and then select **Sharing**.



2. Under **External sharing**, set your sharing level for SharePoint and OneDrive. Keep these points in mind:

    - The SharePoint setting applies to all site types, including sites connected to Microsoft 365 groups and teams. Groups and Teams guest sharing settings also affect connected SharePoint sites.
    - The OneDrive setting can be more restrictive than the SharePoint setting, but not more permissive.
    - External sharing settings are for your organization overall. Each site has its own sharing setting that you can set independently, though it must be at the same or more restrictive setting as the organization. See Change the external sharing setting for a site for more information.

3. Expand **More external sharing settings** and then select the options you want to use.

    See More external sharing settings (in this article).

4. Select **Save**.

> **Important**
>
> Microsoft Entra external collaboration settings determine who can invite guests in your organization for site sharing (always) and file and folder sharing (if Azure B2B collaboration is enabled). Be sure to review Microsoft Entra guest access settings as part of your SharePoint and OneDrive sharing setup.

External sharing options

The following table describes sharing options for SharePoint and OneDrive.

Expand table

Option	Description
Anyone	Allow users to share files and folders by using links that anyone who has the link can access the files or folders without authenticating. This setting also allows users to share sites with new and existing guests who authenticate. If you select this setting, you can restrict the Anyone links so that they must expire within a specific number of days, or so that they can give only View permission. File requests requires that OneDrive be set to **Anyone** and edit permissions for **Anyone** links be enabled. OneDrive settings other than **Anyone** disable file requests. See Best practices for sharing files and folders with unauthenticated users for more information.
New and existing guests	Require people who receive invitations to sign in with their work or school account (if their organization uses Microsoft 365) or a Microsoft account, or to provide a code to verify their identity. Users can share with guests already in your organization's directory, and they can send invitations to people who are added to the directory if they sign in. For more info about verification codes, see Secure external sharing in SharePoint
Existing guests	Allow sharing only with guests who are already in your directory. These guests might exist in your directory because they previously accepted sharing invitations or because they were manually added, such as through Azure B2B collaboration. (To see the guests in your organization, go to the Guests page in the Microsoft 365 admin center).
Only people in your organization	Turn off external sharing.

> **Note**

If you turn off external sharing for your organization and later turn it back on, guests regain access. If you know that external sharing was previously turned on and in use for specific sites and you don't want guests to regain access, first turn off external sharing for those specific sites.

If you restrict or turn off external sharing, guests typically lose access within one hour of the change.

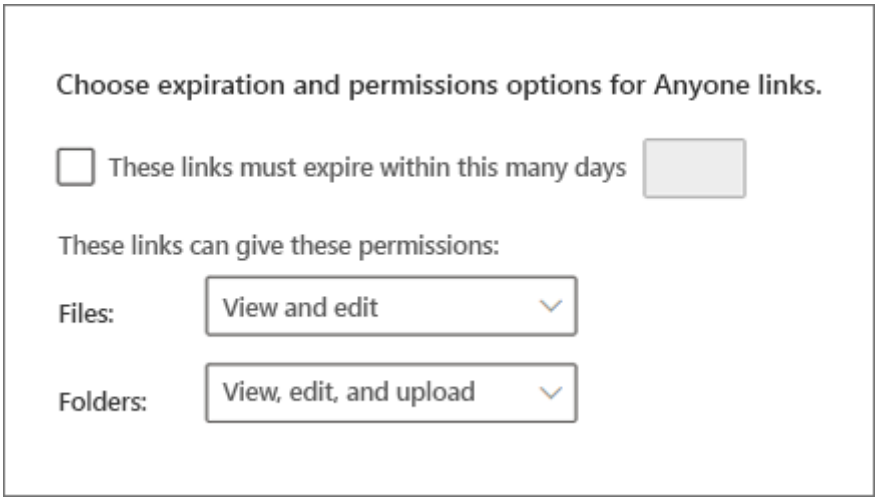
More external sharing settings

Expand table

Setting	Description
Limit external sharing by domain	This setting is useful if you want to limit sharing with particular partners, or help prevent sharing with people at certain organizations. The organization-level setting on this page affects all SharePoint sites and each user's OneDrive. To use this setting, list the domains (maximum of 5,000) in the box, using the format *domain.com*. To list multiple domains, press Enter after adding each domain. You can also limit external sharing by domain by using the Set-SPOTenant Microsoft PowerShell cmdlet with `-SharingDomainRestrictionMode` and either `-SharingAllowedDomainList` or `-SharingBlockedDomainList`. For information about limiting external sharing by domain at the site level, see Restricted domains sharing. Allowed or blocked domains in Microsoft Entra ID also affect SharePoint and OneDrive site sharing (always) and file and folder sharing (if Azure B2B collaboration is enabled). Be sure to review Microsoft Entra collaboration restrictions as part of your SharePoint and OneDrive sharing setup.
Allow only users in specific security groups to share externally	See Manage security groups.
Allow guests to share items they don't own	By default, guests must have full control permission to share items externally.
Guest access to a site or OneDrive will expire automatically after this many days	Administrators can set an expiration time for guest access. Each guest who's invited to the site or with whom individual files and folders are shared has access for some days. For more information visit, Manage guest expiration for a site

Setting	Description
People who use a verification code must reauthenticate after this many days	If people who use a verification code select to "stay signed in" in the browser, they must prove they can still access the account they used to redeem the sharing invitation by entering a code sent to that account. See Secure external sharing recipient experience. If Azure B2B collaboration is enabled, the Microsoft Entra setting is used instead of this setting.
File and folder links	Specifies options to show by default when a user creates a sharing link.
Specific people	This option is most restrictive and impedes broad internal sharing. If you allow external sharing, this option lets users share with specific people outside the organization.
Only people in your organization	If links are forwarded, they work for anyone in the organization. This option is best if your organization shares broadly internally and rarely shares externally.
Anyone with the link	This option is available only if your external sharing setting is set to **Anyone**. Forwarded links work internally or externally, but you can't track who has access to shared items or who has accessed shared items. This option is best for friction-free sharing if most files and folders in SharePoint and OneDrive aren't sensitive. If you select **Anyone with the link**, but the site or OneDrive is set to allow sharing only with guests who sign in or provide a verification code, the default link is **Only people in your organization**. Users need to change the link type to **Specific people** to share files and folders in the site or OneDrive externally.

Advanced settings for "Anyone" links



Link expiration - You can require all **Anyone** links to expire, and specify the maximum number of days allowed. If you change the expiration time, existing links keep their current expiration time if the new setting is longer, or update to the new setting if the new setting is shorter.

Link permissions - You can restrict **Anyone** links so that they can only provide view permission for files or folders.

To use the *Request Files* feature, set the link permissions to **View, edit, and upload** or **View and Upload** for folders.

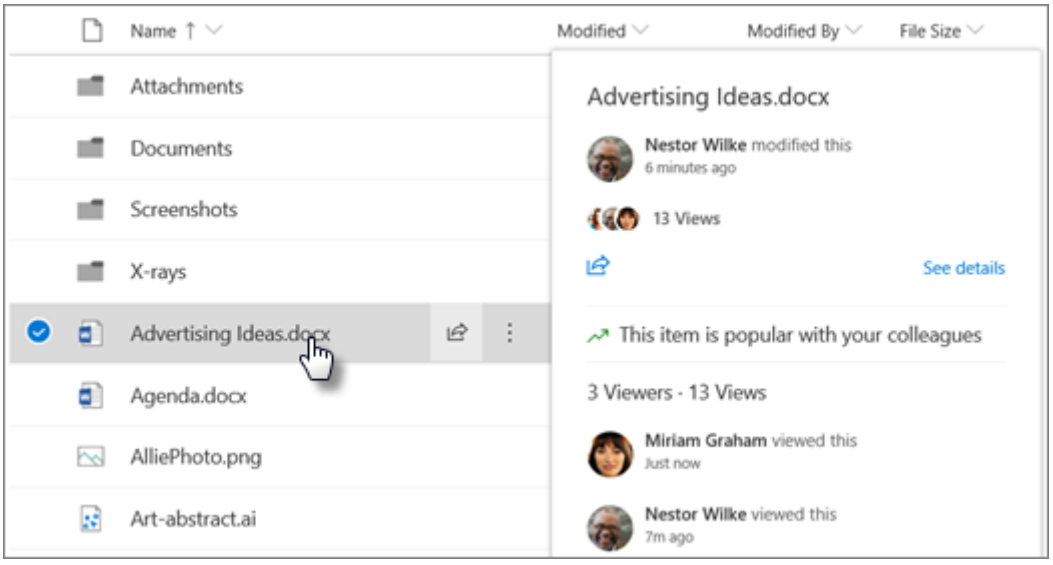
Show owners the names of people who viewed their files in OneDrive

This setting controls whether the owner of a shared file can see on the file card the people who only view (and don't edit) the file in OneDrive. The file card appears when users hover over a file name or thumbnail in OneDrive. The info includes the number of views on the file, the number of people who viewed it, and the list of people who viewed it. To learn more about the file card, see See files you shared in OneDrive .

> **Note**
>
> This setting is selected by default. If you clear it, file viewer info is still recorded and available to you to audit as an admin. OneDrive owners can also still see people who viewed their shared Office files by opening the files from Office.com or from the Office desktop apps.

Let site owners choose to display the names of people who viewed files or pages in SharePoint

This setting specifies whether site owners can allow users who have access to a file, page, or news post to see on the file card who viewed the item.



This setting is turned on by default at the organization level and off at the site level for existing sites. Viewer information shows only when the setting is on at both the organization and site level. Turn on this feature only on team sites that don't have sensitive information. Learn how site owners can turn on this feature.

> **Note**
>
> Historical data is included when this setting is enabled. Likewise, if the setting is turned off and back on at the organization level or site level, the views during the off period are included in the history.

Use short links for sharing files and folders

Use a shorter link format for sharing files and folders. This format is useful if you have integrations that require a shorter URL.

Need more help?

If you have technical questions about this topic, you might find it helpful to post them on the SharePoint discussion forum. It's a great resource for finding others who have worked with similar issues or who have encountered the same situation.

For help on security and permissions, see these YouTube videos from SharePoint community experts.

See also

Limit accidental exposure to files when sharing with guests

Create a secure guest sharing environment

Stop sharing files or folders or change permissions

Last updated on 06/30/2026

Change the sharing settings for a site

You must be at least a SharePoint Administrator in Microsoft 365 to change the sharing settings for a site. Site owners can't change these settings.

The steps in this article apply to team sites, communication sites, and classic sites. To learn how to change the external sharing setting for a user's OneDrive, see Change the external sharing setting for a user's OneDrive. For info about changing your organization-level settings, see Manage sharing settings. Guest sharing settings for Microsoft 365 Groups and Teams affect connected SharePoint sites.

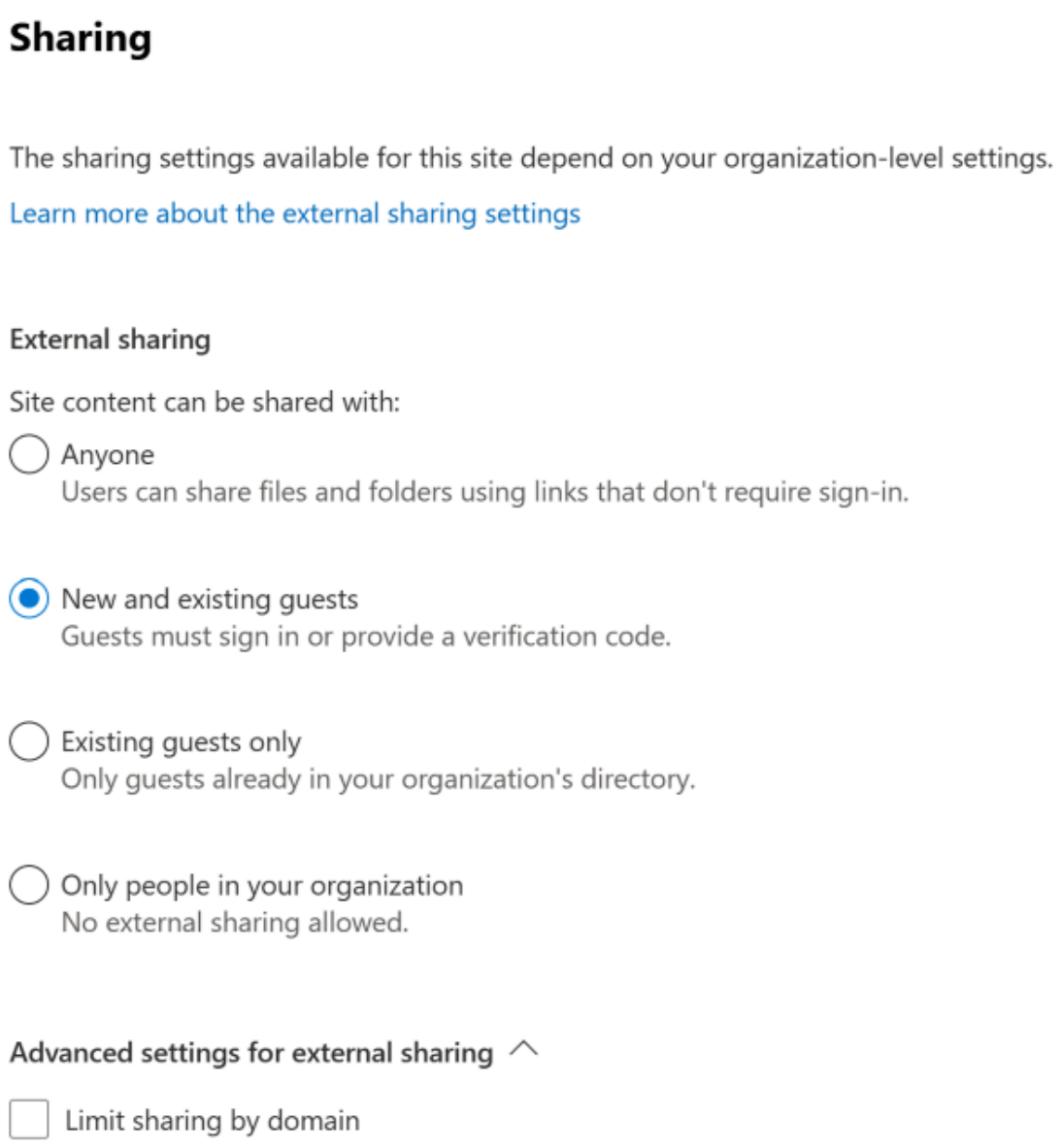
For detailed information about how to set up guest access for a site, see Collaborate with guests in a site.

> **Important**
>
> Microsoft Entra external collaboration settings determine who can invite guests in your organization for site sharing (always) and file and folder sharing (if Azure B2B collaboration is enabled). Be sure to review Microsoft Entra guest access settings as part of your SharePoint and OneDrive sharing setup.

How do I change the external sharing setting for a site?

To change the external sharing setting:

1. Go to **Active sites** in the new SharePoint admin center, and sign in with an account that has admin permissions for your organization.
2. In the left column, select a site. (For a channel site, select the link in the **Channel sites** column and then select the site.)
3. On the **Settings** tab, select **More sharing settings**.
4. Select an external sharing option (see the table in the next section).

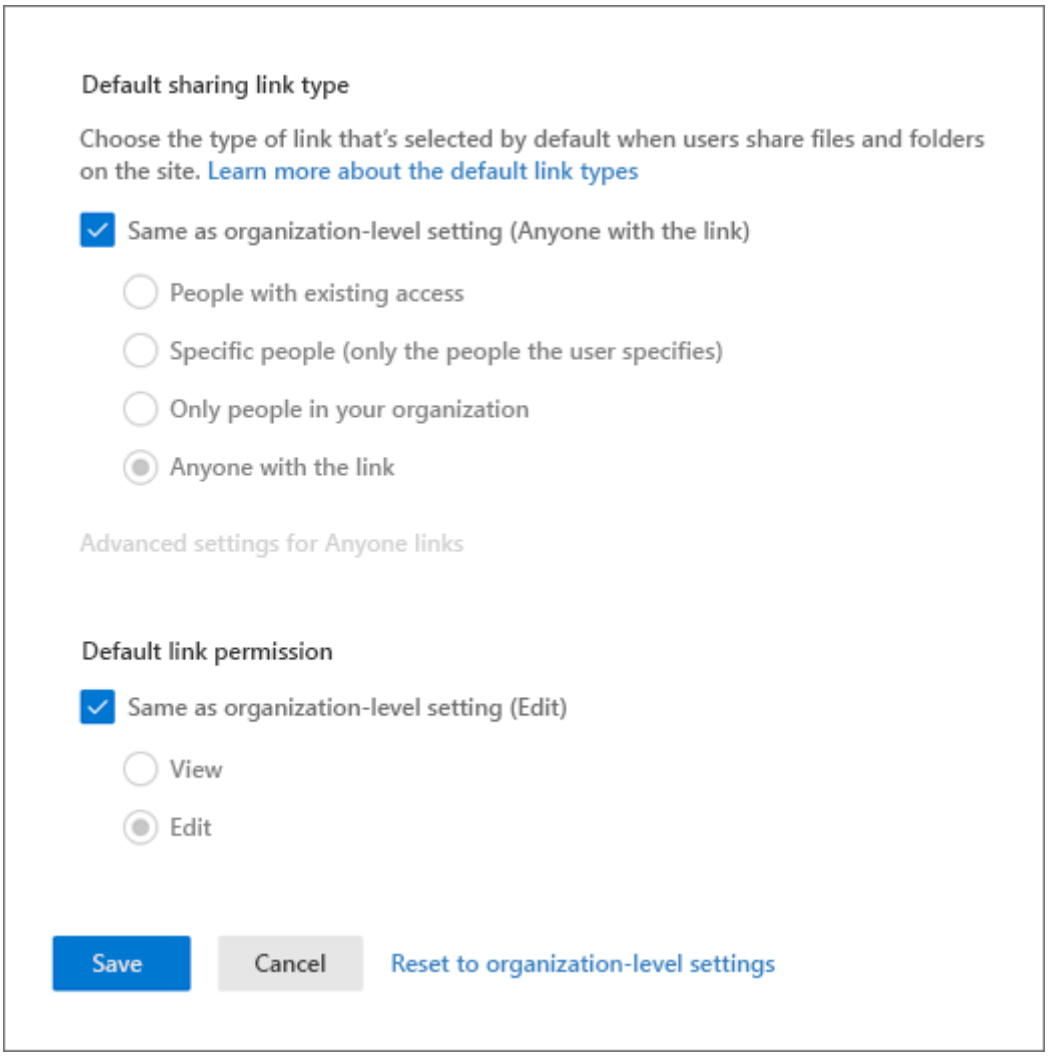


5. If you want to limit the sharing of this site by domain, select the **Limit sharing by domain** check box by expanding **Advanced settings for external sharing**, and add the domains that you want to allow or block.

> **Important**
>
> Allowed or blocked domains in Microsoft Entra ID also affect SharePoint and OneDrive site sharing (always) and file and folder sharing (if Azure B2B collaboration is enabled). Be sure to review Microsoft Entra collaboration restrictions as part of your SharePoint and OneDrive sharing setup.

6. If you want to change the guest access expiration setting for this site, clear the **Same as organization-level setting** check boxes and set the values that you want to use for this site.

7. If you want to change the default sharing link type or permissions for this site, clear the **Same as organization-level setting** check boxes and set the values that you want to use for this site. For more info, see Change the default sharing link for a site.



8. Select **Save**.

Which sharing option should I select?

Expand table

Select this option:	If you want to:
Anyone	Allow site owners and others with full control permission to share the site with people who authenticate. Allow site users to decide when sharing files and folders to require authentication or allow unauthenticated people to access the item. Anyone links to files and folders can be freely forwarded.
New and existing guests	Allow site owners and others with full control permission to share the site with people outside the organization. These people need to sign in and are added to the directory.

Select this option:	If you want to:
	Allow site users to share files and folders with people who aren't in the organization's directory.
Existing guests	Allow sharing with only people already in your directory. These users exist in your directory because they previously accepted sharing invitations or because they were manually added. (These users have **#EXT#** in their user principal name.)
Only people in your organization	Prevent all site users from sharing any site content externally.

The available settings depend on your organization-level setting. If you enable external sharing for a site and later turn it off for your organization, external sharing becomes unavailable at the site level and any shared links stop working. If you turn it back on for the organization, the site sharing setting returns to what it was before and the shared links resume working.

> **Note**
>
> You might have site content shared with a Microsoft 365 group that has guest members, and the group settings prevent guest members from accessing group resources. In this case, even if you turn on external sharing for the site, guests of the group might not be able to access site content. To enable or disable Microsoft 365 Group guest member access, see Manage guest access in Microsoft 365 Groups.

What are the default site sharing settings?

The following table shows the default sharing setting for each site type.

Expand table

Site type	Default sharing setting
Classic	**Only people in your organization**
OneDrive	**Anyone**
Group-connected sites (including Teams)	**New and existing guests** if the Microsoft 365 Groups setting **Let group owners add people outside the organization to groups** is **On**; otherwise **Existing guests only**
Communication	**Only people in your organization**

Site type	Default sharing setting
Modern sites with no group (#STS3 TeamSite)	**Only people in your organization**

> **Note**
>
> The root communication site (tenant-name.sharepoint.com) has a default sharing setting of **Anyone**.

Related articles

Best practices for sharing files and folders with unauthenticated users

Create a more secure guest sharing environment

File collaboration in SharePoint with Microsoft 365

Stop sharing files or folders or change permissions

Last updated on 05/07/2026

Change the external sharing setting for a user's OneDrive

After you set the organization-wide sharing settings for Microsoft SharePoint and Microsoft OneDrive, you can further restrict the external sharing for a specific OneDrive user.

> **Tip**
>
> Instead of changing the external sharing setting for an individual user's OneDrive, consider blocking external sharing of sensitive information by using Microsoft Purview data loss prevention.

How do I change the external sharing setting?

1. Sign in to https://admin.microsoft.com.
2. In the left pane, select **Users** > **Active users**.
3. Select the user.
4. Select the **OneDrive** tab. Under **Sharing**, select **Manage external sharing**.
5. Select a new external sharing level, and then select **Save**.

How do I change the external sharing setting by using PowerShell?

You can also change the external sharing setting for a specific OneDrive user by using PowerShell. Use the Set-SPOSite cmdlet with the `-SharingCapability` parameter.

Last updated on 05/07/2026

How shareable links work in OneDrive and SharePoint in Microsoft 365

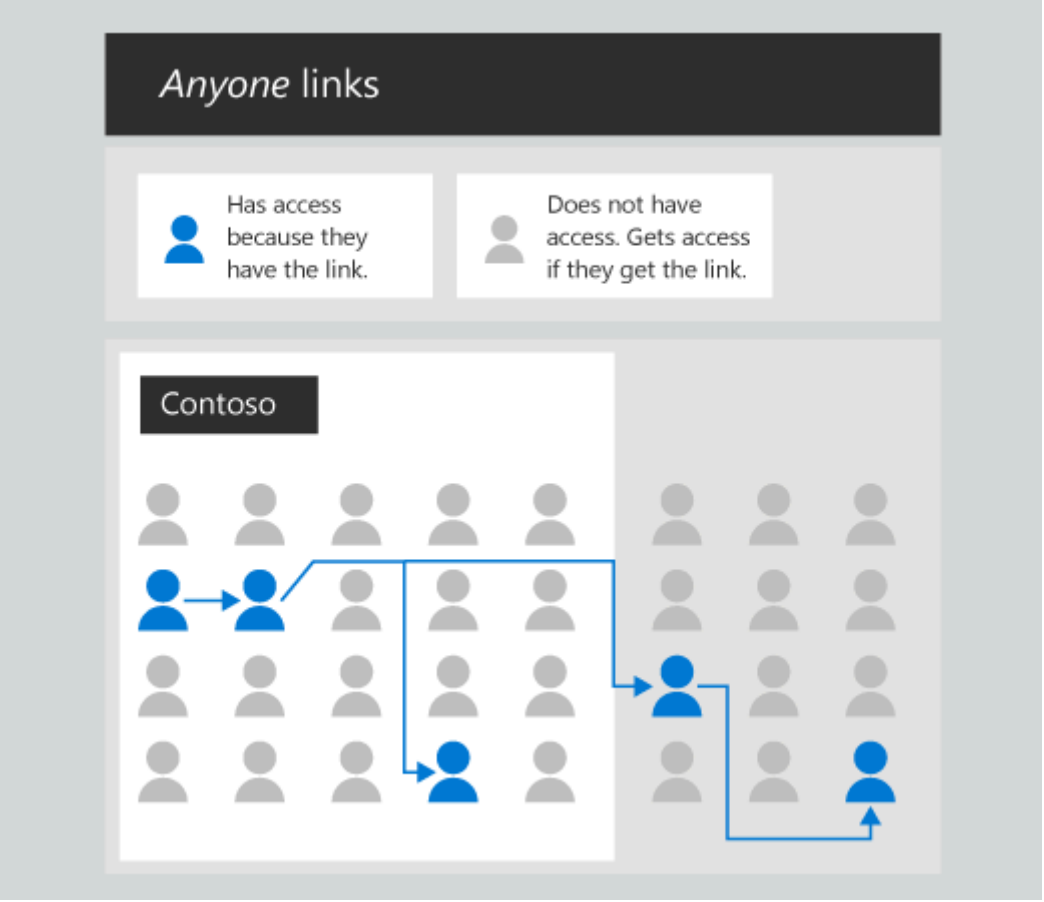
When a user shares a file or folder in Microsoft 365, they create a shareable link with permissions to the item. There are three primary link types:

- "Anyone" links
- "People in your organization" links
- "Specific people" links

It's important for everyone to understand how sharing links work and which ones to use to maintain data security. This article describes different types of sharing links and includes links to more resources.

"Anyone" links

Anyone links give access to the item to anyone who has the link. People using an *Anyone* link don't have to authenticate, and their access can't be audited.



An *Anyone* link is a transferable, revocable secret key.

- It's transferable because it can be forwarded to others.
- It's revocable because you can revoke access for everyone who used the link by deleting it.
- It's secret because it can't be guessed or derived.

The only way to get access is to get the link, and the only way to get the link is for somebody to give it to you. *Anyone* links can't be used with files in a Microsoft Teams shared channel site.

Creating an *Anyone* link doesn't make the associated content appear in search results or make it accessible through Copilot. It also doesn't immediately grant access to the content to everyone. An *Anyone* link must be activated by clicking the link (redemption) before the shared content becomes searchable by the person who has the link.

"People in your organization" links

People in your organization links work only for people inside your Microsoft 365 organization. They don't work for guests in the directory, only members.

Like an *anyone* link, a *People in my organization* link is a transferable, revocable secret key. These links only work for people who are inside your Microsoft 365 organization. When somebody

opens a *People in my organization* link, they need to be authenticated as a member in your directory. If they're not currently signed in, they're prompted to sign in.

Creating a *People in your organization* link doesn't make the associated file or folder appear in search results or make it accessible through Copilot. It also doesn't grant access to everyone within the organization. Creating this link doesn't provide organizational-wide access to the content. For individuals to access the file or folder, they must possess the link, and it needs to be activated through redemption (clicking it). A user redeems the link by selecting it.

If you send the link from the SharePoint or OneDrive Web UI, or by using email in Outlook or a chat message in Microsoft Teams, you automatically redeem it for individual recipients, up to a limit of 100. This feature isn't supported for group recipients, or for messages posted in Microsoft Teams channels. The link doesn't work for guests or other people outside your organization.

Expiration of "People in your organization" links

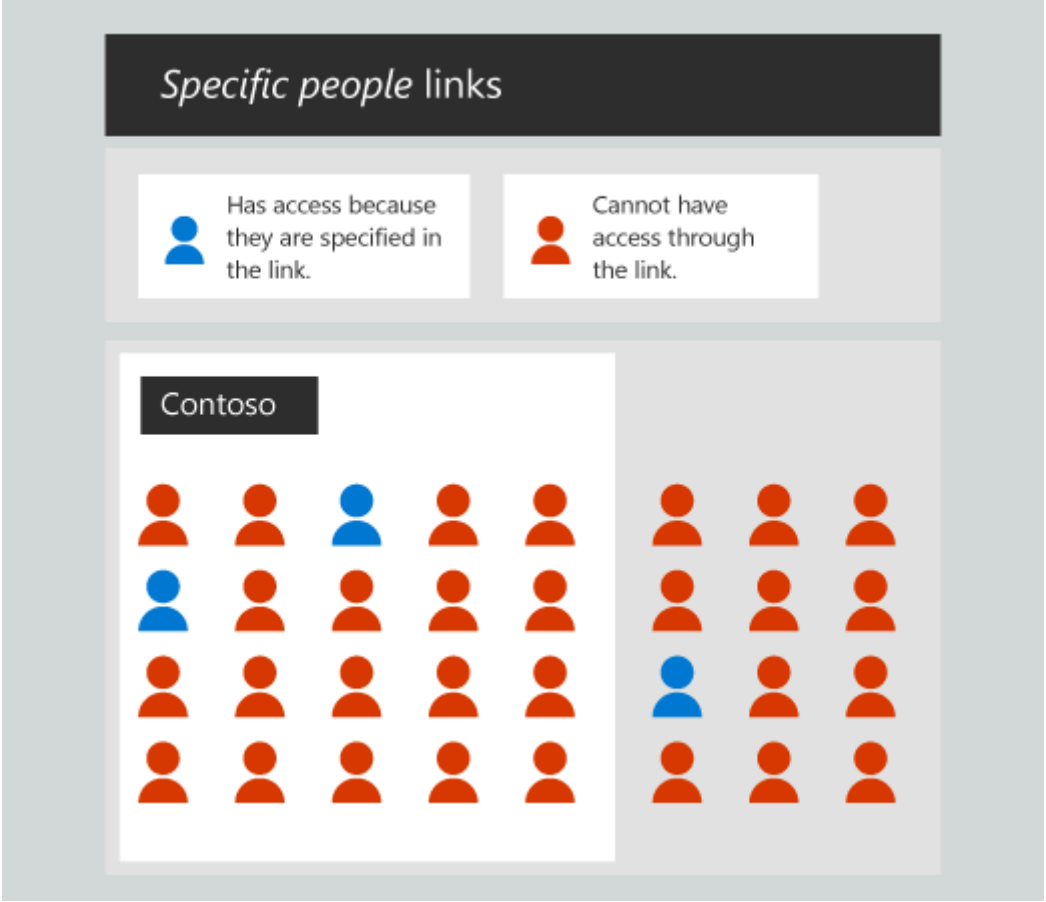
Administrators can configure expiration policies for *People in your organization* sharing links in SharePoint and OneDrive. When an expiration policy is enabled, newly created links get an expiration date and stop working after that date.

Existing *People in your organization* links aren't automatically modified when an expiration policy is enabled. However, when an existing link is accessed after the policy is in effect, the link is evaluated against the configured expiration limit using its original creation date. If the link exceeds the allowed age, it's treated as expired and can no longer be used to access the content.

When a sharing link expires, only the link is affected. The file or folder isn't deleted, and users who have access through other permissions can continue to access the content.

"Specific people" links

Specific people links only work for the people that users specify when they share the item.



A *Specific people* link is a nontransferable, revocable secret key. *Specific people* links don't work if they're opened by anybody other than the persons who are specified by the sender. Moreover, *Specific people* links make the associated file or folder appear in search results and make it accessible through Copilot for all user and security group members who are added to the sharing link.

Specific people links can be used to share with users in the organization and people outside the organization. In both cases, the recipient needs to authenticate as the user specified in the link. For files in a Microsoft Teams shared channel site, *Specific people* links can only be sent to others in the channel.

Next steps

To manage or change sharing options, see the following articles:

- Manage sharing settings for SharePoint and OneDrive in Microsoft 365
- Change the default sharing link type for a site

To help end users understand sharing options, send these articles to them:

- Share OneDrive files and folders
  - Share SharePoint files or folders

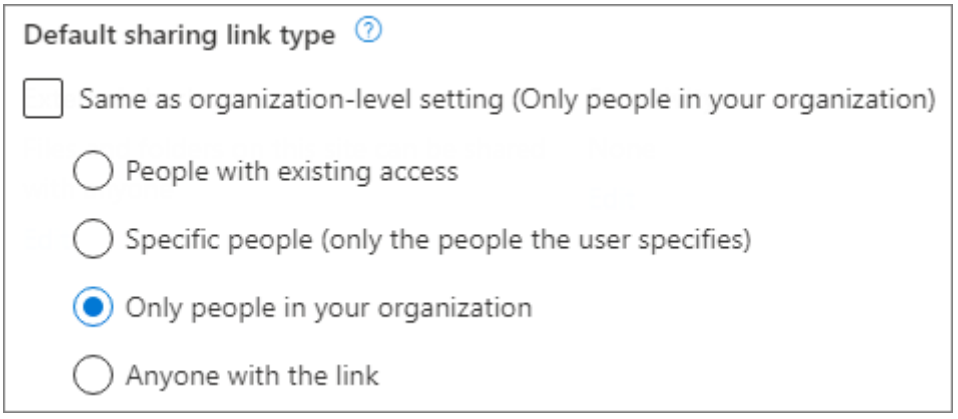
Ensure you include information about your organization's policies for sharing information.

Last updated on 08/13/2026

Change the default sharing link type for a site

In Microsoft SharePoint, users can share files and folders by sending a link. They should select a link type based on the people to whom they want to give permission. The following link types are available:

- Anyone with the link (previously called "anonymous access" or "shareable")
- People in your organization with the link
- People with existing access
- Specific people



As a SharePoint Administrator, you might want to enable users to send "Anyone" links, but you might not want this type of link to be the default when users select to share files and folders. Set the default type of link to something more restrictive, while still allowing users to select other types of links as needed. Change this setting at the organization level and at the site (previously called "site collection") level.

> **Note**
>
> The default sharing link setting applies only to libraries that use the new experience.
> This setting doesn't affect Outlook Web App, Outlook 2016, or Office clients prior to Office 2016.

For info about changing this setting at the organization level, see External sharing settings .

How do I change the default link type for a site?

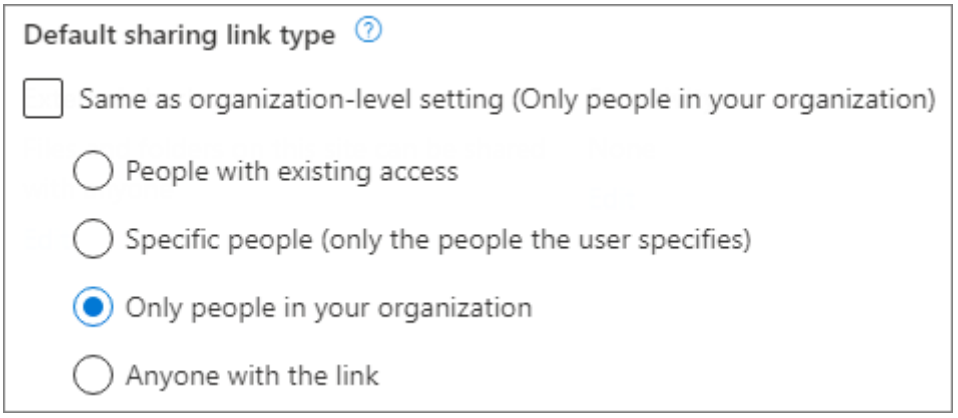
1. Go to **Active sites** in the SharePoint admin center, and sign in with an account that has admin permissions for your organization.

   > **Note**
   >
   > If you have Office 365 operated by 21Vianet (China), sign in to the Microsoft 365 admin center, then browse to the SharePoint admin center and open the Active sites page.

2. In the left column, select a site.

3. Select **Sharing** on the command bar.

4. Under **Default sharing link type**, clear the **Same as organization-level setting** checkbox.



5. Choose the default sharing link setting that you want to use for this site, and then select **Save**.

   > **Note**
   >
   > To change the default link type for a Teams private or shared channel site, you must use the Set-SPOSite PowerShell cmdlet.

How do I change the default sharing link permission for a site?

1. Following the steps 1-3 in the preceding section, under **Default link permission**, clear the **Same as organization-level setting** checkbox.

2. Choose the default sharing link permission that you want to use for this site, and then select **Save**.

Can I use a sensitivity label to configure the default sharing link settings?

If you use sensitivity labels to classify and protect your SharePoint sites, you can also configure the default sharing link type and sharing link permissions for a site and individual documents by using a sensitivity label.

For more information about this scenario, see Use sensitivity labels to configure the default sharing link type for sites and documents in SharePoint and OneDrive.

Related topics

Turn external sharing on or off for a site

Last updated on 06/30/2026

Turn on OneDrive file activity notifications

By default, users receive notifications about file activity in OneDrive and SharePoint. These notifications appear across apps and devices. For example, the service sends notifications through the Firebase Cloud Messaging service to the Office mobile app for Android or the Apple Push Notification service to the Office mobile app for iOS. It also sends notifications to the OneDrive sync app for Windows or Mac. As a global or SharePoint admin in Microsoft 365, you can turn off these notifications for all users for compliance purposes. If you allow these notifications, users can select to turn them off app by app where they don't want them.

> **Note**
>
> Currently, the service sends notifications to users when files are shared with them. Later, it sends notifications when people @mention the user in a comment. Other notifications might be added in the future.

Allow or block notifications

1. Go to **Settings** in the new SharePoint admin center, and sign in with an account that has admin permissions for your organization.
2. Select the **Notifications** setting for OneDrive.
3. Select or clear **Allow notifications**.

You can also control this setting in PowerShell by using Set-SPOTenant -NotificationsInOneDriveForBusinessEnabled.

The **Notifications** page of the OneDrive admin center includes three other settings under **Email OneDrive owners when**:

- Other users invite more external users to shared files. You can control this setting by using Set-SPOTenant -NotifyOwnersWhenItemsReshared.
- External users accept invitations to access files. (This setting no longer works for the new sharing experience that appears in most places.)
- An anonymous access link is created or changed. You can control this setting by using Set-SPOTenant -OwnerAnonymousNotification.

Related topics

To learn more about controlling SharePoint notifications, see Control notifications. To control whether sharing emails include "At a glance" content, see Set-SPOTenant -IncludeAtAGlanceInShareEmails.

Last updated on 04/07/2026

Enable file requests in SharePoint or OneDrive

By using the file request feature in OneDrive or SharePoint, users can request files by sending a link where others can upload files. When users upload files, they can't view, edit, delete, or download files in the folder or see who else uploaded.

Admins can manage the **Request files** feature through the SharePoint Online Management Shell.

> **Important**
>
> File request is only available if:
>
> - You're using OneDrive for work or school.
> - The admin enabled Anyone links.
> - Folder permissions are set to **View, edit, and upload** for **Anyone** links.
> - **Allow only specific security groups** isn't enabled.
> - Not available for Office 365 operated by 21Vianet, OneDrive for home, or Office 365 Germany.

> **Note**
>
> Disabling **Anyone** links also disables **Request files** on SharePoint and OneDrive.

Enable or disable request files for SharePoint

To manage **Request files** for SharePoint:

1. Ensure **Anyone** links are enabled at the organization level.
2. Set folder permissions to **View, edit, and upload** or **View and upload**.
3. Verify `CoreRequestFilesLinkEnabled` is **True** through the SharePoint Online Management Shell:
   - Run `Get-SPOTenant`.
   - If not set to **True**, use `Set-SPOTenant -CoreRequestFilesLinkEnabled $True`.

4. (Optional) Set link expiration by using `Set-SPOTenant -CoreRequestFilesLinkExpirationInDays`.

Enable or disable request files for OneDrive

To manage **Request files** for OneDrive:

1. Enable **Anyone** links.
2. Set folder permissions to **View, edit, and upload** or **View and upload**.
3. Configure **Anyone** links for OneDrive at the tenant level.
4. Verify `OneDriveRequestFilesLinkEnabled` is **True** via the SharePoint Online Management Shell:
   - Run `Get-SPOTenant`.
   - If not set to **True**, use `Set-SPOTenant -OneDriveRequestFilesLinkEnabled $True`.
5. (Optional) Set link expiration using `Set-SPOTenant -OneDriveRequestFilesLinkExpirationInDays`.

Enable or disable request files per site

To manage **Request files** for a specific site:

1. Ensure **Anyone** links are enabled.
2. Set folder permissions to **View, edit, and upload** or **View and upload**.
3. Verify `RequestFilesLinkEnabled` is **True** via the SharePoint Online Management Shell:
   - Run `$r=Get-SPOSite -Identity <SiteURL> -Detailed`.
   - If not set to **True**, use `Set-SPOSite -RequestFilesLinkEnabled $True`.
4. (Optional) Set link expiration using `Set-SPOSite -RequestFilesLinkExpirationInDays`.

For more information on file requests, see Create a file request.

Last updated on 05/07/2026

Plan and deploy a file collaboration environment - SharePoint

By using Microsoft 365 services, you can create a secure and productive file collaboration environment for your users. SharePoint powers much of this environment, but the capabilities of file collaboration in Microsoft 365 go beyond the traditional SharePoint site. Teams, OneDrive, and various governance and security options all play a role in creating a rich environment where users can collaborate easily and where your organization's sensitive content remains secure.

In the following sections, you find the options and decisions that you as an administrator should consider when setting up a collaboration environment:

- How SharePoint relates to other collaboration services in Microsoft 365, including OneDrive, Microsoft 365 Groups, and Teams.
- How you can create an intuitive and productive collaboration environment for your users.
- How you can protect your organization's data by managing access through permissions, data classifications, governance rules, and monitoring.

This article is part of the broader Microsoft 365 collaboration story:

- Secure collaboration with Microsoft 365
- Collaboration governance
- Meetings, webinars, and live events

Download the Microsoft Teams and related productivity services in Microsoft 365 for IT architects poster and refer to it while you read this article. This poster provides detailed illustrations of how the collaboration services in Microsoft 365 relate to each other and interact.

Creating a successful collaboration experience

Choose technical implementation options for file collaboration in Microsoft 365 that balance what can seem to be contradictory requirements:

- Protecting your intellectual property
- Enabling self-service
- Creating a smooth user experience

Protecting your intellectual property

Several options discussed later in this article can help you protect your intellectual property. These options include limiting who can share files, applying governance policies by using sensitivity labels, and managing the devices that users use to access content.

Consider a balanced approach when choosing options:

A configuration that allows users to share content freely can lead to accidental sharing of confidential data. However, a user experience that's difficult to use or too restrictive can lead to users finding alternative collaboration options that circumvent your governance policies, ultimately leading to even greater risk.

By using a combination of features – depending on the sensitivity of your data – you can create a collaboration environment that's easy to use and provides the security and auditing controls that you need.

Enabling self-service

In Microsoft 365, allow users to create Teams, Microsoft 365 Groups, and SharePoint sites as needed. Use sensitivity labels to enforce permissions governance, take advantage of compliance features that protect your content, and use expiration and renewal policies to make sure unused sites don't accumulate.

By choosing options that favor user self-service, you can minimize the impact on your IT staff while creating an easier experience for your users.

Creating a smooth user experience

The key to creating a smooth user experience is to avoid creating barriers for your users that they don't understand or that they must escalate to your help desk. For example, turning external sharing off for a site might cause user confusion or frustration. Labeling the site and its contents as confidential and using data loss prevention policy tips and emails to educate your users in your governance policies can lead to a smoother experience for them.

SharePoint, Microsoft 365 Groups, and Teams

In SharePoint in Microsoft 365, each SharePoint team site is part of a Microsoft 365 group. A Microsoft 365 group is a single permissions group that's associated with various Microsoft 365 services, including a SharePoint site, an instance of Planner, a mailbox, a shared calendar, and others. When you add owners or members to the Microsoft 365 group, they get access to the SharePoint site along with the other connected services.

While you can continue to manage SharePoint site permissions separately by using SharePoint groups, manage permissions for SharePoint by adding people to or removing them from the associated Microsoft 365 group. This approach provides easier administration and gives users access to a host of related services that they can use for better collaboration.

Microsoft Teams provides a hub for collaboration by bringing together all the Microsoft 365 group-related services, plus various Teams-specific services, in a single user experience with persistent chat. Teams uses the associated Microsoft 365 group to manage its permissions. Within the Teams experience, users can directly access SharePoint along with the other services without having to switch applications. This approach provides a centralized collaboration space with a single place to manage permissions. Teams uses the SharePoint site that is connected to the Microsoft 365 group for files in standard channels and creates separate SharePoint sites for each private or shared channel. For collaboration scenarios in your organization, use Teams rather than using services such as SharePoint independently.

For details about how SharePoint and Teams interact, see Overview of Teams and SharePoint integration and Manage settings and permissions when SharePoint and Teams are integrated.

Collaboration in client applications

Office applications such as Word, Excel, and PowerPoint provide a wide variety of collaboration features, including coauthoring and @mentions. These applications also integrate with sensitivity labels and data loss prevention (discussed later).

Deploy Microsoft 365 Apps for enterprise. Microsoft 365 Apps for enterprise provides an always up-to-date experience for your users, with the latest features and updates delivered on a schedule that you can control.

For details about deploying Microsoft 365 Apps for enterprise, see Deployment guide for Microsoft 365 Apps.

OneDrive libraries

While SharePoint provides shared libraries for shared files that teams can collaborate on, users also have an individual library in OneDrive where they can store files that they own.

When a user adds a file to OneDrive, that file isn't shared with anyone else. OneDrive provides the same sharing capabilities as SharePoint, so users can share files in OneDrive as needed.

A user's individual library can be accessed from Teams, and from the OneDrive web interface and mobile application.

On devices running Windows or macOS, users can install the OneDrive sync app to sync files from both OneDrive and SharePoint to their local disk. This sync app allows them to work on files offline and also provides the convenience of opening files in their native application (such as Word or Excel) without the need of going to the web interface.

The two main decisions to consider for using OneDrive in collaboration scenarios are:

- Do you want to allow Microsoft 365 users to share files in OneDrive with people outside your organization?
- Do you want to restrict file sync in any way – such as only to managed devices?

You can configure these settings in the SharePoint admin center.

Securing your data

A significant part of a successful collaboration solution is making sure your organization's data remains secure. Microsoft 365 provides various features to help you keep your data secure while enabling a seamless collaboration experience for your users.

To help protect your organization's information, you can:

- **Control sharing** by configuring sharing settings for each site that are appropriate to the type of information in the site, you can create a collaboration space for users while securing your intellectual property.
- **Classify and protect information** by classifying the types of information in your organization, you can create governance policies that provide higher levels of security to information that is confidential compared to information that is meant to be shared freely.
- **Manage devices** with device management, you can control access to information based on device, location, and other parameters.
- **Monitor activity** by monitoring the collaboration activity happening in Teams and SharePoint, you can gain insights into how your organization's information is being used. You can also set alerts to flag suspicious activity.
- **Protect against threats** by using policies to detect malicious files in SharePoint, OneDrive, and Teams, you can help ensure the safety of your organization's data and network.

These options are discussed in more detail in the following sections. Depending on the needs of your organization, choose the options that give you the best balance of security and usability. If you're in a highly regulated industry or work with highly confidential data, you might want to put more of these controls in place. If your organization's information isn't sensitive, you might want to rely on basic sharing settings and malicious file alerts.

Control sharing

The sharing settings that you configure for SharePoint and OneDrive determine who your users can collaborate with, both inside and outside your organization. Depending on your business needs and the sensitivity of your data, you can:

- Disallow sharing with people outside your organization.
- Require people outside your organization to authenticate.
- Restrict sharing to specified domains.

You can configure these settings for the entire organization, or for each site independently (except private or shared channel sites). For detailed information, see Turn sharing on or off and Turn sharing on or off for a site.

For more guidance about sharing with people outside your organization, see Limit accidental exposure to files when sharing with guests.

When users share files and folders, they create a shareable link that has permissions to the item. There are three primary link types:

- *Anyone* links that work for anyone and don't require sign-in
- *People in your organization* links that work for users in your organization
- *Specific people* links that work for the people specified when the link is created

For more information about these link types, see How shareable links work in OneDrive and SharePoint in Microsoft 365.

Unauthenticated access with *Anyone* links

Anyone links are a great way to easily share files and folders with people outside your organization. However, if you're sharing sensitive information, this option might not be the best choice.

If you require people outside your organization to authenticate, users can't use *Anyone* links and you can audit guest activity on shared files and folders.

Though *Anyone* links don't require people outside your organization to authenticate, you can track the usage of *Anyone* links and revoke access if needed.

If you want to allow *Anyone* links, several options provide a more secure sharing experience.

You can restrict *Anyone* links to read-only. You can also set an expiration time limit, after which the link stops working.

Another option is to configure a different link type to be displayed to the user by default. This option can help minimize the chances of inappropriate sharing. For example, if you want to allow *Anyone* links but are concerned that they only be used for specific purposes, you can set the default link type to *Specific people* links or *People in your organization* links instead of *Anyone* links. Users must then explicitly select *Anyone* links when they share a file or folder.

You can also use data loss prevention to restrict *Anyone* link access to files that contain sensitive information.

People in your organization links

People in your organization links are a great way to share information within your organization. *People in your organization* links work for anyone in your organization, so users can share files and folders with people who aren't part of a team or members of a site. When redeemed, the link gives access to the particular file or folder and can be passed around inside the organization. This access allows for easy collaboration with stakeholders from groups that might have separate teams or sites – such as design, marketing, and support groups.

Creating a *People in your organization* link doesn't make the associated file or folder appear in search results, be accessible via Copilot, or grant access to everyone within the organization. Simply creating this link doesn't provide organizational-wide access to the content. For individuals to access the file or folder, they must possess the link and activate it through redemption. A user redeems the link by clicking on it, or in some instances, the link might be automatically redeemed when sent to someone via email, chat, or other communication methods. The link doesn't work for guests or other people outside your organization.

Specific people links

Specific people links are best for circumstances where users want to limit access to a file or folder. The link only works for the person specified and they must authenticate in order to use it. These links can be internal or external (if you enable guest sharing).

Classify and protect information

Microsoft Purview Data Loss Prevention provides a way to classify your teams, groups, sites, and documents, and to create a series of conditions, actions, and exceptions to govern how they're used and shared.

By classifying your information and creating governance rules around them, you can create a collaboration environment where users can easily work with each other without accidentally or intentionally sharing sensitive information inappropriately.

With data loss prevention policies in place, you can be relatively liberal with your sharing settings for a given site and rely on data loss prevention to enforce your governance requirements. This approach provides a friendlier user experience and avoids unnecessary restrictions that users might try to work around.

For detailed information about data loss prevention, see Learn about data loss prevention.

Sensitivity labels

Sensitivity labels provide a way to classify teams, groups, sites, and documents with descriptive labels that you can use to enforce a governance workflow.

Using sensitivity labels helps your users share information safely and maintain your governance policies without needing to become experts in those policies.

For example, you could configure a policy that requires Microsoft 365 groups classified as confidential to be private rather than public. In such a case, a user creating a group, team, or SharePoint site would only see the **private** option when they choose a classification of confidential. For information about using sensitivity labels with teams, groups, and sites, see Use sensitivity labels to protect content in Microsoft Teams, Microsoft 365 groups, and SharePoint sites.

Conditions and actions

By using data loss protection conditions and actions, you can enforce a governance workflow when a given condition is met.

Examples include:

- If customer information is detected in a document, users can't share that document with guests.
- If a document contains the name of a confidential project, guests can't open the document even if it is shared with them.

For more information, see Learn about data loss prevention.

Conditional access

Microsoft Entra Conditional Access provides extra controls to prevent users from accessing your organization's resources in risky situations, such as untrusted locations or devices that aren't up to date.

Examples include:

- Block guests from signing in from risky locations.
- Require multifactor authentication for mobile devices.

Create access policies specifically for guests to mitigate risk for people who most likely have unmanaged devices.

For detailed information, see What is Conditional Access?.

Monitoring with reports

Microsoft 365 offers a variety of reports to help you monitor site usage, document sharing, governance compliance, and a host of other events.

For information about how to view reports on SharePoint site usage, see Microsoft 365 Reports in the Admin Center - SharePoint site usage.

For information about how to view data loss prevention reports, see View the reports for data loss prevention.

For information on reports that can help you monitor content sharing, see Data access governance reports for SharePoint sites.

Related articles

Create a secure guest sharing environment

Best practices for sharing files and folders with unauthenticated users

Microsoft SharePoint - SharePoint Advanced Management overview

---

Last updated on 05/07/2026

SharePoint and OneDrive integration with Microsoft Entra B2B

> **Important**
>
> Between May and July 2026, Microsoft enabled SharePoint and OneDrive integration with Microsoft Entra B2B for new external sharing in commercial tenants. The `EnableAzureADB2BIntegration` setting no longer controls sharing behavior for these tenants, and the integration can't be disabled.
>
> Starting in October 2026, Microsoft will retire SharePoint Online one-time passcode (OTP) authentication for commercial tenants. Microsoft Entra B2B email one-time passcode authentication remains supported.
>
> When SharePoint OTP retirement reaches your tenant, external users need a matching Microsoft Entra B2B guest account in your directory to access previously shared **Specific people** links. Users with a matching guest account retain access. If a guest account is missing, an administrator can create one, or a user with sharing permissions can share or reshare at least one file, folder, or site to create it and restore access to previously shared content.
>
> For more information, see FAQ on improvements to external sharing in OneDrive and SharePoint.

This article describes how to enable Microsoft SharePoint and Microsoft OneDrive integration with Microsoft Entra B2B.

Microsoft Entra B2B provides authentication and management of guests. When enabled, email one-time passcode is a fallback for guests who can't sign in through another supported authentication method.

When you integrate SharePoint and OneDrive with Microsoft Entra B2B Invitation Manager, you can share files, folders, list items, document libraries, and sites with external people. This feature provides an upgraded experience from the existing secure external sharing recipient experience. Additionally, Microsoft Entra B2B Invitation Manager offers a one-time passcode feature. This feature allows users without work, school, or Microsoft accounts to authenticate by using a code, instead of creating a new account.

Enabling this integration doesn't change your sharing settings. For example, if you have site collections where external sharing is turned off, it remains off.

SharePoint and OneDrive integration with the Microsoft Entra B2B one-time passcode feature is enabled by default for new tenants.

Advantages of Microsoft Entra B2B include:

- Invited people outside your organization each get an account in the directory and are subject to Microsoft Entra ID access policies such as multifactor authentication.
- Invitations to a SharePoint site use Microsoft Entra B2B and no longer require users to have or create a Microsoft account.
- If you have Google federation in Microsoft Entra ID, federated users can now access SharePoint and OneDrive resources that you shared with them.
- SharePoint and OneDrive sharing is subject to the Microsoft Entra organizational relationships settings, such as **Members can invite** and **Guests can invite**. As with Microsoft 365 Groups and Teams, if a Microsoft Entra organizational relationship setting is more restrictive than a SharePoint or OneDrive setting, the Microsoft Entra setting prevails.

> **Note**
>
> Microsoft Entra B2B doesn't support Microsoft accounts in Microsoft 365 operated by 21Vianet.

Enabling the integration

For commercial tenants, Microsoft Entra B2B integration is already enabled for new external sharing. You don't need to run the command below. The following procedure applies only to tenants where the `EnableAzureADB2BIntegration` setting still controls the integration.

> **Note**
>
> When you enable the integration, people outside the organization are invited through the Azure B2B platform when sharing from SharePoint. They sign in based on the Microsoft Entra B2B redemption policy. When you don't enable the integration, people outside the organization continue to use their existing accounts created when previously invited to the tenant. Any sharing to new people outside the organization may result in either Microsoft

Entra ID-backed accounts or SharePoint-only email auth guests that use a SharePoint One Time Passcode experience to sign in.

To enable SharePoint and OneDrive integration with Microsoft Entra B2B

1. Download the latest SharePoint Online Management Shell.
2. Connect to SharePoint with permissions of a SharePoint Administrator or more in Microsoft 365. To learn how, see Getting started with SharePoint Online Management Shell.
3. Run the following cmdlets:

```
PowerShell
Set-SPOTenant -EnableAzureADB2BIntegration $true
```

> **Note**
>
> Review any custom domain sharing restrictions in SharePoint and OneDrive and decide if they should be moved to the Microsoft Entra B2B Allow/Deny list. The Microsoft Entra ID Allow/Deny list also affects other Microsoft 365 services like Teams and Microsoft 365 Groups.

Disabling the integration

Microsoft Entra B2B integration can't be disabled in commercial tenants. The following procedure applies only to tenants where the `EnableAzureADB2BIntegration` setting still controls the integration.

You can disable the integration by running Set-SPOTenant `-EnableAzureADB2BIntegration $false`.

> **Important**
>
> When you disable the integration, previously shared users remain Microsoft Entra Guest Users for future shares. To convert a user from a Microsoft Entra Guest User back to a SharePoint OTP user, you need to delete the guest in Microsoft Entra ID and remove all SPUser objects in your organization that reference that guest user.

Frequently asked questions

The following questions address SharePoint OTP retirement and access to content shared with external users.

1. How can I check if my tenant has enabled SharePoint and OneDrive integration with Entra B2B?

Answer: In commercial tenants, integration is already enabled for new external sharing, regardless of the `EnableAzureADB2BIntegration` value. For tenants where the setting still controls the integration, run `Get-SPOTenant` in the SharePoint Online Management Shell and check the `EnableAzureADB2BIntegration` property. A value of `True` means the integration is enabled; `False` means it isn't enabled.

2. Which tenants are affected by the October 2026 SharePoint OTP retirement?

Answer: The October 2026 retirement applies to commercial tenants. It affects external users who access previously shared **Specific people** links through SharePoint OTP and don't have a matching Microsoft Entra B2B guest account in your directory.

3. What happens to previously shared links when SharePoint OTP is retired?

Answer: External users with a matching Microsoft Entra B2B guest account retain access to previously shared links. Once retirement reaches your commercial tenant during October 2026, users without a matching guest account receive access denied on previously shared **Specific people** links. To restore access, create a guest account matching the email address used for the original sharing link, or share or reshare at least one file, folder, or site with that user. You don't need to reshare each item individually.

4. Is there a way to report which previously shared links and external users are affected?

Answer: Yes. You can use audit logs to assess the impact. For more information, see Use sharing auditing in the audit log. Additionally, site sharing reports available through Microsoft Graph Data Connect can help identify affected content and users. Details are provided in the Microsoft Graph Data Connect for SharePoint Blog. You can also report on file and folder sharing in a SharePoint site using this sharing report.

5. Can I proactively invite existing users to join via Entra B2B before this change takes effect?

Answer: Yes. You can create a Microsoft Entra B2B guest account in advance using the email address associated with the original sharing link. A matching guest account lets the user retain access to previously shared content without resharing. For more information, see Add and manage B2B collaboration users.

6. Can exceptions be made to this change?

Answer: No. This update is part of Microsoft's ongoing efforts to enhance security.

7. Can this change be applied at the site level?

Answer: No. The change applies at the tenant level and can't be scoped to individual sites.

See also

Set-SPOTenant

External sharing overview

ⓘ**Note:** The author created this article with assistance from AI. Learn more

---

Last updated on 10/07/2026

Frequently Asked Questions: Improvements to external sharing in OneDrive & SharePoint - Retiring SPO OTP & Transition to Microsoft Entra B2B

1. **Is OTP being retired as a supported authentication method for guests?**

   SharePoint Online (SPO) one-time passcode (OTP) authentication will be retired for commercial tenants during October 2026. Microsoft Entra B2B email one-time passcode (OTP) authentication isn't being retired.

   When enabled, Microsoft Entra B2B email OTP is a fallback for guests who can't sign in through another supported authentication method. For more information, see Email one-time passcode authentication.

2. **Can I opt out of this change?**

   No. Commercial tenants can't opt out of SharePoint OTP retirement or disable Microsoft Entra B2B integration for new external sharing.

3. **Can I choose when SharePoint OTP is retired for my tenant?**

   No. Retirement rolls out to commercial tenants during October 2026. Tenants are selected automatically, and you can't choose a specific date.

4. **Do all previously shared links need to be reshared?**

   No. External users with a matching Microsoft Entra B2B guest account in your directory retain access to previously shared links. If a guest account is missing, you can create one in Microsoft Entra B2B, or share or reshare at least one file, folder, or site to create the guest account automatically. You don't need to reshare each item individually.

5. **How can I identify guests who don't have a guest account yet?**

   At site level, use the external sharing report to get a list of guests invited via SPO OTP who do not yet have a Microsoft Entra B2B guest account. Refer to the "User E-mail" column. Learn more. For guests without a Microsoft Entra B2B guest account, you can proactively create the account in your directory to retain access to all previously shared files.

6. **Do I need to enable Microsoft Entra B2B integration for my commercial tenant?**

   No. Integration is already enabled for new external sharing in commercial tenants. The `EnableAzureADB2BIntegration` setting no longer controls sharing behavior for these tenants, and the integration can't be disabled.

7. **Are duplicate guest accounts created?**

   No. If a Microsoft Entra B2B guest account already exists for a collaborator outside your organization, a duplicate is not created.

8. **Do my guest users retain access to files shared before the integration?**

   External users with a matching Microsoft Entra B2B guest account in your directory retain access. Once SharePoint OTP retirement reaches your commercial tenant during October 2026, users without a matching guest account receive access denied on previously shared **Specific people** links. See FAQ #9 for how to restore access.

9. **How is a guest account created in my directory?**

   An administrator can create a Microsoft Entra B2B guest account using the email address associated with the original sharing link. Alternatively, a user with sharing permissions can share or reshare at least one file, folder, or site with the external user. This automatically creates the guest account in Microsoft Entra B2B.

   Once a matching guest account exists, the external user can access previously shared links without each item being reshared.

10. **Is there any impact on Anyone/Anonymous links?**

    No, SPO OTP retirement and use of Entra B2B for external sharing does not impact Anyone/Anonymous links.

ⓘ**Note:** The author created this article with assistance from AI. Learn more

---

Last updated on 10/07/2026

Restrict sharing of SharePoint and OneDrive content by domain

To restrict sharing with other organizations, either at the organization level or site level, limit sharing by domain.

> **Note**
>
> If you enroll in the SharePoint and OneDrive integration with Microsoft Entra B2B, SharePoint invitations also follow any domain restrictions configured in Microsoft Entra ID.

Limiting domains

You can limit domains by allowing only the domains you specify or by allowing all domains except those you block.

Limit domains at the organization level

1. Go to **Sharing** in the SharePoint admin center, and sign in with an account that has admin permissions for your organization.

   If you have Office 365 operated by 21Vianet (China), sign in to the Microsoft 365 admin center, then browse to the SharePoint admin center and open the Sharing page.

2. Under **More external sharing settings**, select the **Limit external sharing by domain** check box, and then select **Add domains**.

3. To create an allow list (most restrictive), select **Allow only specific domains**; to block only the domains you specify, select **Block specific domains**.

4. List the domains (maximum of 5,000) in the box provided, using the format *domain.com*. If you list more than one domain, enter each domain on a new line.

   Wildcards aren't supported for domain entries.

5. Select **Save**.

You can also configure the organization-wide setting by using the Set-SPOTenant PowerShell cmdlet.

Limit domains at the site level

You can also limit domains at the site level. Keep the following considerations in mind:

- In there are conflicts, the organization-wide configuration takes precedence over the site configuration.
- If you set up an organization-wide allow list and you want to set up a site-level allow list, the site-level allow list must be a subset of the organization's allow list.
- If you set up an organization-wide block list, you can set up either an allow list or a block list at the site collection level.
- For individual OneDrive site collections, you can only set up limit domains by using the Set-SPOSite Windows PowerShell cmdlet.

Limit the domains for a site

1. Go to **Active sites** in the SharePoint admin center, and sign in with an account that has admin permissions for your organization.

   If you have Office 365 operated by 21Vianet (China), sign in to the Microsoft 365 admin center, then browse to the SharePoint admin center and open the More features page.

2. Select the site name that you want to restrict domains to open the details panel.

3. On the panel, select the **Settings** tab and select **More sharing settings** under **External sharing**.

4. Under **Advanced settings for external sharing**, select the **Limit external sharing by domain** check box, and then select **Add domains**.

5. Select **Allow only specific domains** to create an allow list (must be a subset of the organization's allow list), or to block only the domains you specify, select **Block specific domains**. You can't use the **Block specific domains** feature if your organization already set up an allow list.

6. List the domains (maximum of 500) in the box provided, using the format *domain.com*. If listing more than one domain, enter each domain on a new line.

   Wildcards aren't supported for domain entries.

7. Select **Save**, and then select **Save** again.

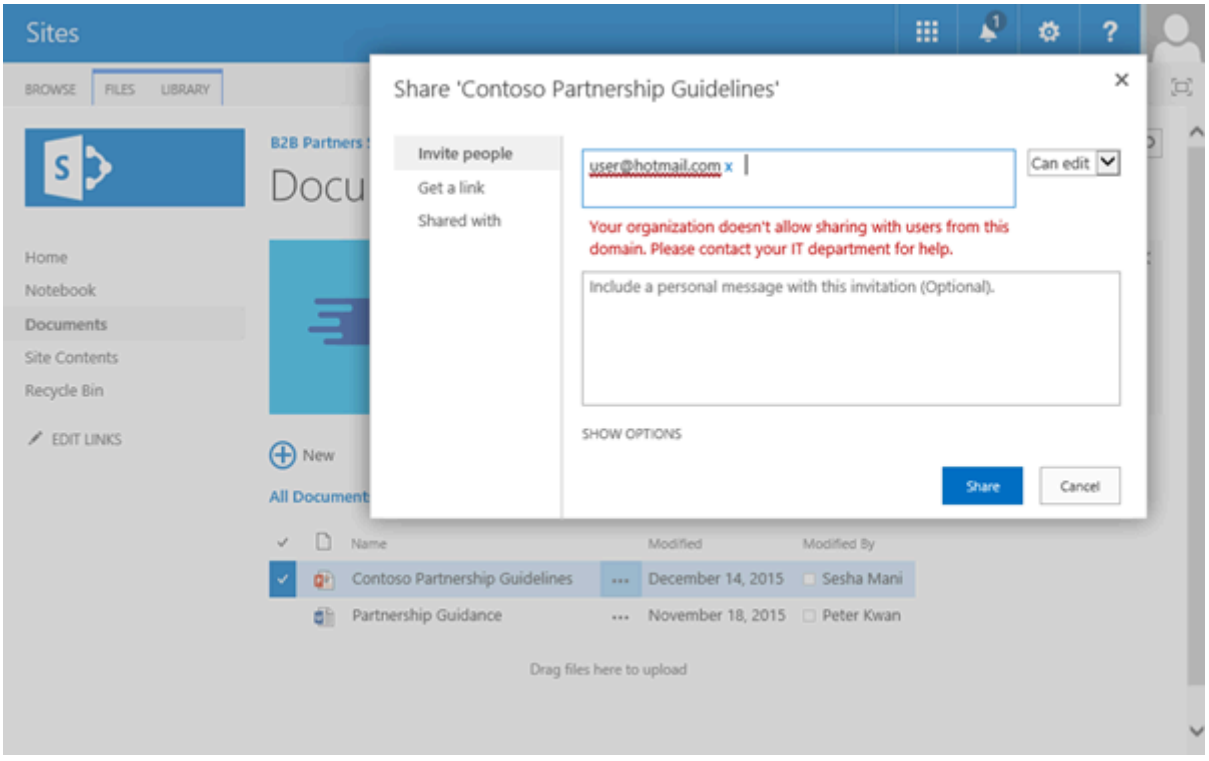
> ⓘ **Note**
>
> To configure the site collection setting for site collections that don't appear in this list (such as Group-connected sites or individual OneDrive site collections), you must use the Set-SPOSite PowerShell cmdlet.

Sharing experience

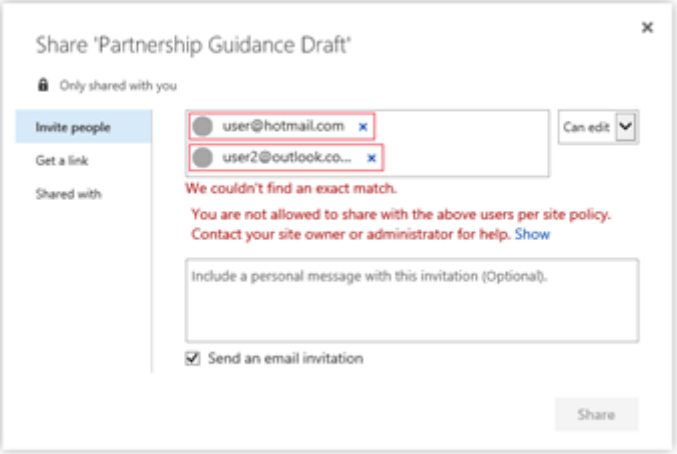
After you limit sharing by domain, here's what you see when you share a document:

- **Sharing content with email domains that aren't allowed.** If you attempt to share content with a guest whose email address domain isn't allowed, an error message displays, and sharing isn't allowed.

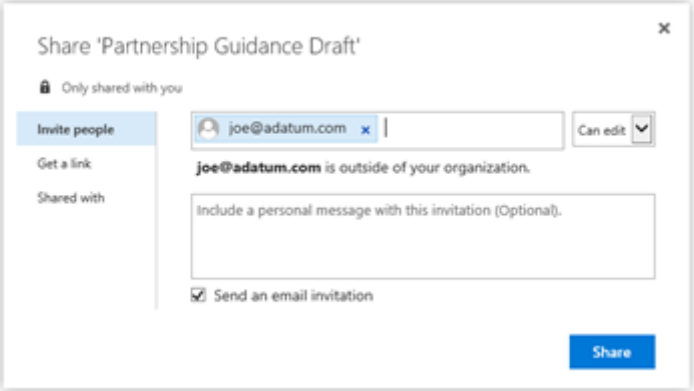
  (If the user is already in your directory, you don't see the error, but they're blocked if they attempt to access the site.)



- **Sharing OneDrive files with guests on domains that aren't allowed.** If a user tries to share a OneDrive file with a guest whose email domain isn't allowed, an error message displays, and sharing isn't allowed.



- **Sharing content with email domains that are allowed.** Users can successfully share the content with the guest. A tooltip appears to let them know that the guest is outside of their organization.



User auditing and lifecycle management

As with any extranet sharing scenario, it's important to consider the lifecycle of your guests, how to audit their activity, and eventually how to archive the site. As a site owner or admistrator, you can create a CSV file of every unique file, user, permission, and link on a given SharePoint site or OneDrive. As a SharePoint admin or other administrator, with SharePoint advanced management, you can run Data access governance reports to audit shared links. See Planning SharePoint business-to-business (B2B) extranet sites for more information.

See also

External sharing overview

Extranet for Partners with Microsoft 365

Set-SPOTenant

Last updated on 05/07/2026

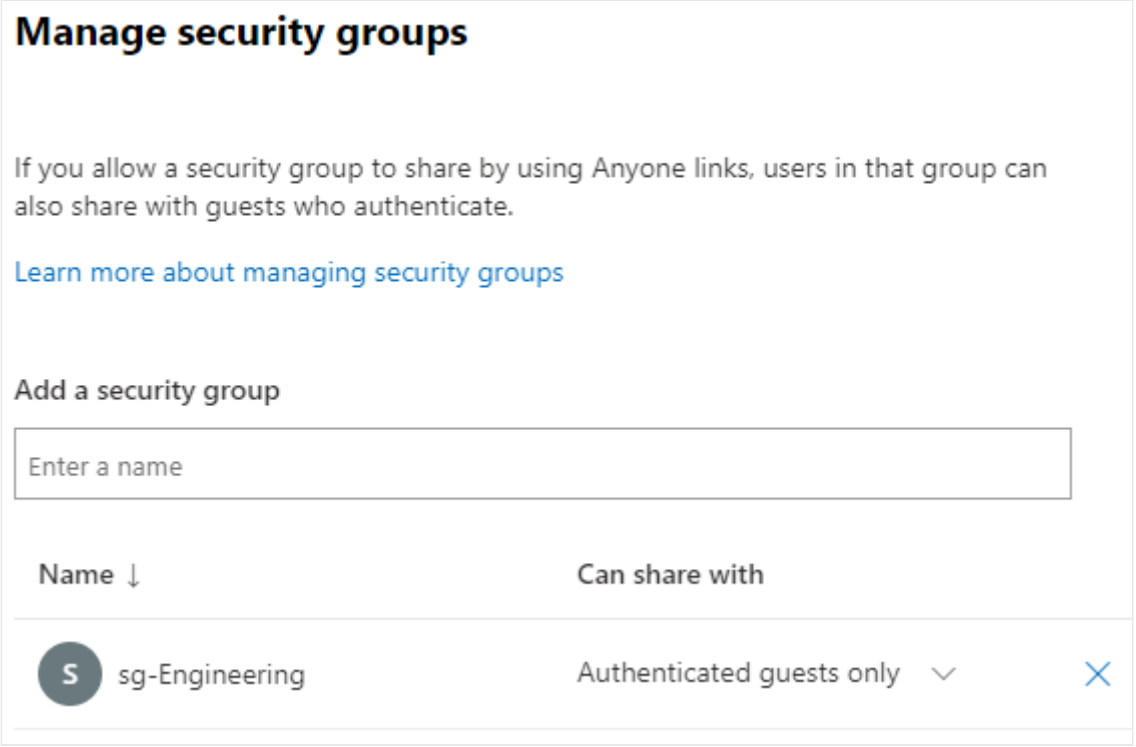
Allow only members of specific security groups to share SharePoint and OneDrive files and folders externally

As a SharePoint Administrator or other administrator in Microsoft 365, you can restrict external sharing of SharePoint and OneDrive content so that only users in specific security groups can share externally. The users in these security groups must be allowed to invite guests in the Microsoft Entra guest invite settings.

1. Go to **Sharing** in the SharePoint admin center, and sign in with an account that has admin permissions for your organization.

2. Under **External sharing**, expand **More external sharing settings**.

3. Select **Allow only users in specific security groups to share externally**, and then select **Manage security groups**.



4. In the **Add a security group** box, search for and select the security groups you want to use (up to 12).

5. Next to the security group name, from the **Can share with** dropdown, select either:

   - **Authenticated guests only** (default)

- **Anyone**

6. Select **Save**.

By selecting **Anyone**, users in that security group can share links to files and folders externally that don't require users to authenticate by using the **Anyone link** in the **Share** dialog box. Forwarded **Anyone links** work internally or externally, but you can't track who has access to shared items or who has accessed shared items. Users in this group can also share to authenticated guests. This option is best for friction-free sharing, provided files and folders in SharePoint and OneDrive aren't considered sensitive.

By selecting **Authenticated guests only**, sharing externally is limited to those guests who authenticate. This option is best for sharing sensitive or proprietary information because it requires guests to verify their identity before they can access the file or folder.

Last updated on 05/07/2026

Report on file and folder sharing in a SharePoint site

You can create a CSV file of every unique file, user, permission, and link on a given SharePoint site or OneDrive. This report helps you understand how sharing is used and if any files or folders are shared with guests. You must be a site admin to run the report. For more reporting options, see Microsoft Graph Data Connect.

When you run the report, you save the CSV file to a location you choose on the site. If you don't want site members to see the report, consider creating a folder with different permissions where only site owners can access the report.

The report might take some time to run depending on the size of the site. When the report finishes running, you receive an email with a link to the report.

Run the report for a SharePoint site

1. Open the site where you want to run the report.
2. On the **Settings** menu, select **Site usage**.
3. In the **Shared with external users** section, select **Run report**.
4. Choose a location to save the report, and then select **Save**.

Run the report for OneDrive

1. From the Microsoft 365 app launcher, select the OneDrive tile.
2. On the **Settings** menu, select **OneDrive settings**.
3. Select **More settings**, and then select **Run sharing report**.
4. Choose a location to save the report, and then select **Save**.

CSV format

For items shared with direct access, the report contains one row for each user and item combination. The report shows SharePoint groups, but not individual users inside them.

For items shared with a link, the report contains a row for each signed-in user who uses the link or receives the link through the sharing dialog. The report doesn't include links that are emailed directly but aren't clicked, or *Anyone* links.

The report contains the following columns:

Expand table

Column	Description
Resource Path	The relative URL of the item
Item Type	The type of item (web, folder, file, and so on)
Permission	The permission level the user has on this item
User Name	Friendly name of the user or group that has access to this item. If this is a sharing link, the user name is *SharingLink*
User E-mail	The email address of the user who has access to this item. This is blank for SharePoint groups.
User or Group Type	The type of user or group: Member (internal), Guest (external), SharePoint group, Security group, or Microsoft 365 group. (*Member* refers to a member in the directory, not a member of the site.)
Link ID	The GUID of the sharing link if user name is *Sharing Link*
Link Type	The type of link (Anonymous, Organization, Specific People) if user name is *Sharing Link*
AccessViaLinkID	The **Link ID** used to access the item if a user's permission to an item is via a link.

Related articles

Overview of Microsoft Graph Data Connect

Last updated on 05/07/2026

Use SharePoint as a business-to-business (B2B) extranet solution

An extranet site in Microsoft SharePoint is a site that you create to let external partners access specific content and collaborate with them. Extranet sites are a way for partners to securely do business with your organization. You keep the content for your partner in one place, and they have only the content and access they need. They don't need to email the documents back and forth or use tools that aren't sanctioned by your IT department.

Traditionally, deploying a SharePoint *on-premises* extranet site involves complex configuration to establish security measures and governance, including granting access inside the corporate firewall, and expensive initial and ongoing costs.

But with Microsoft 365, partners connect directly to a members-only site in SharePoint, a team in Microsoft Teams, or a Teams shared channel without access to your on-premises environment or any other teams or sites. You can access Microsoft 365 extranet sites anywhere there's an Internet connection.

Depending on your collaboration needs, you can include Microsoft 365 groups or Microsoft Teams as part of your extranet.

Why use Microsoft 365 for a B2B extranet?

Time-to-value and cost savings: A Microsoft 365 B2B extranet eliminates the need for creating a costly on-premises extranet site. No other hardware is required. Using Microsoft 365 greatly reduces the resource and labor costs. Your IT department can focus on more important tasks than creating and maintaining extranet infrastructure.

Secure sharing: Microsoft 365 B2B extranet provides a highly secure sharing experience with the IT governance and policies that you require, including:

- The ability to protect yourself against accidental sharing by using owner-approved sharing through Microsoft 365 Groups or Teams, which prevents users from inviting new users without approval.
- The ability to restrict partner users to a single site or team. They can't search for or view any content on sites or teams to which they aren't invited.

Seamless collaboration: Collaborate with your partner users as if they're part of your organization, including allowing them to chat and confer through Teams.

Auditing and reporting. Microsoft 365 B2B extranet offers visibility into the access of your content by external partner users. One of the key IT benefits is to be able to audit usage, including being able to see who is inviting whom and when a guest logs in to access the content. See Search the audit log in the Microsoft Purview portal for more information.

Security and governance. Microsoft 365 features such as Microsoft Purview Data Loss Prevention and Microsoft Defender for Cloud Apps provide a robust feature set to help you create a secure guest sharing environment.

Compare Microsoft 365 extranet with a traditional SharePoint on-premises extranet

Expand table

Condition	Microsoft 365 extranet	SharePoint "on-premises" extranet
Firewall access required for guests	No	Yes
Complex network and infrastructure configuration required	No	Yes
Security hardening	Managed through Microsoft 365 configurations	Manually configured by IT staff
IT labor intensive	No	Yes
Ongoing maintenance needed	Minimal	Considerable
Other hardware needed	No	Often
Controlling sharing experience for the extranet	Part of Microsoft 365 sites functionality	Often requires custom solutions/apps

Get started

To get started setting up a SharePoint extranet site, see the following articles:

- Collaborate with guests in a site if you want to limit your extranet to a site with a Microsoft 365 Group, or Collaborate with guests in a team if you want to include a team.

- Create a B2B extranet with managed guests if you want to delegate guest access management to specific approvers in either your organization or the partner organization.
- Collaborate with external participants in a channel if you want to use a shared channel in Teams where partners can use their existing work or school account for a single sign-on experience.
- Limit accidental exposure to files when sharing with guests and Create a secure guest sharing environment to learn about options for securing your guest sharing environment.

See also

Microsoft 365 guest sharing settings reference

Last updated on 05/07/2026

SharePoint site permissions

This article covers advanced scenarios for customizing site permissions. Most organizations don't need these options. If you just want to share files or folders, see Share SharePoint files or folders. If you want to share a site, see Share a site.

While SharePoint offers extensive customization for site permissions, use the built-in SharePoint groups for communication site permissions and manage team site permissions through the associated Microsoft 365 group. For more information about managing permissions in the SharePoint modern experience, see Sharing and permissions in the SharePoint modern experience.

If you need to customize SharePoint groups, this article describes how.

Customize site permissions

A SharePoint group is a collection of users who all have the same set of permissions to sites and content. Instead of assigning permissions one person at a time, use groups to conveniently assign the same permission level to many people at once.

> **Note**
>
> To complete the following steps, you need a permission level that includes permissions to *Create Groups* and *Manage Permissions*. The **Full Control** level has both. For more information, see Understanding permission levels in SharePoint.

Create a group

1. On your website or team site, select **Settings**, and select **Site permissions**.
2. On the **Permissions** page, select **Advanced Permissions Settings**.
3. On the **Permissions** tab, select **Create Group**.
4. On the **Create Group** page, in the **Name** and **About me** boxes, type a name and description for this SharePoint group.
5. In the **Owner** box, specify a single owner of this security group.

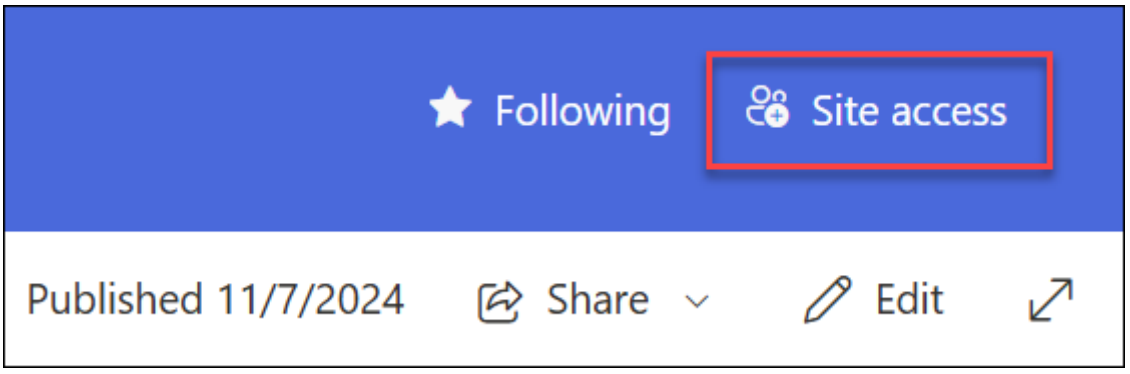
6. In the **Group Settings** section, specify who can view and edit the membership of this group.
7. In the **Membership Requests** section, select the settings that you want for requests to join or leave the group. You can specify the email address to which requests should be sent.
8. In the **Give Group Permissions to this Site** section, choose a permission level for this group.
9. Select **Create**.

Add users to a group

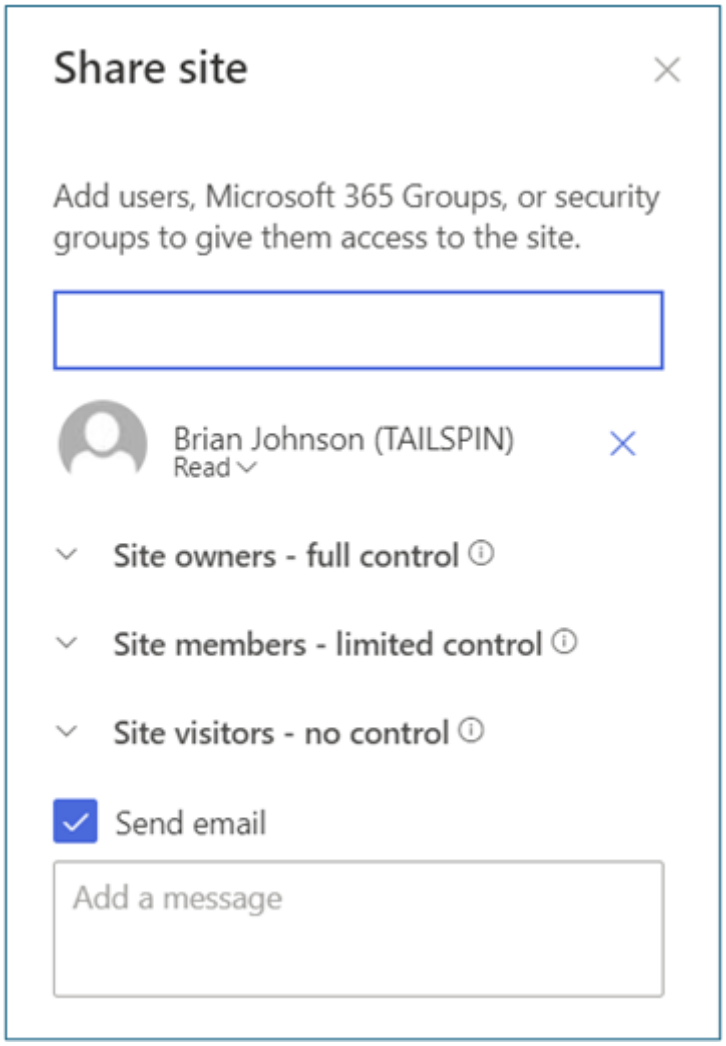
You can add users to a group at any time.

If you're on a communication site, follow these steps:

1. Select **Site access**.



2. In the **Site access** dialog, enter the name or email address of the user or group that you want to add. When the name appears, choose the permission level from the dropdown.



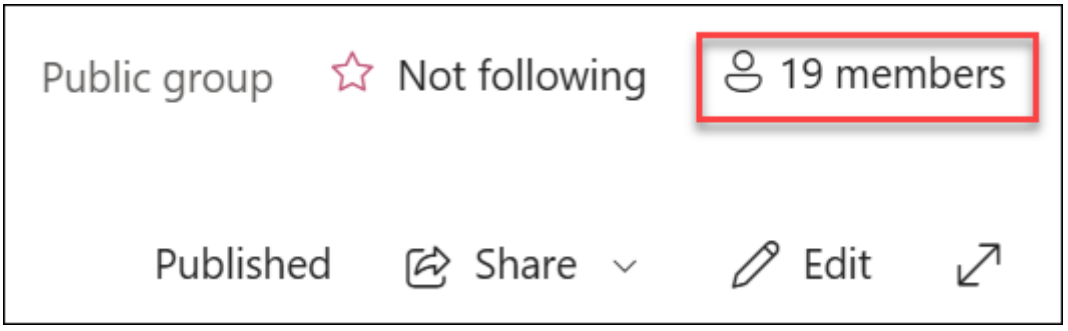
3. If you want to add more names, repeat these steps.

4. Enter a message to send to the new users in the **Add a message** box.

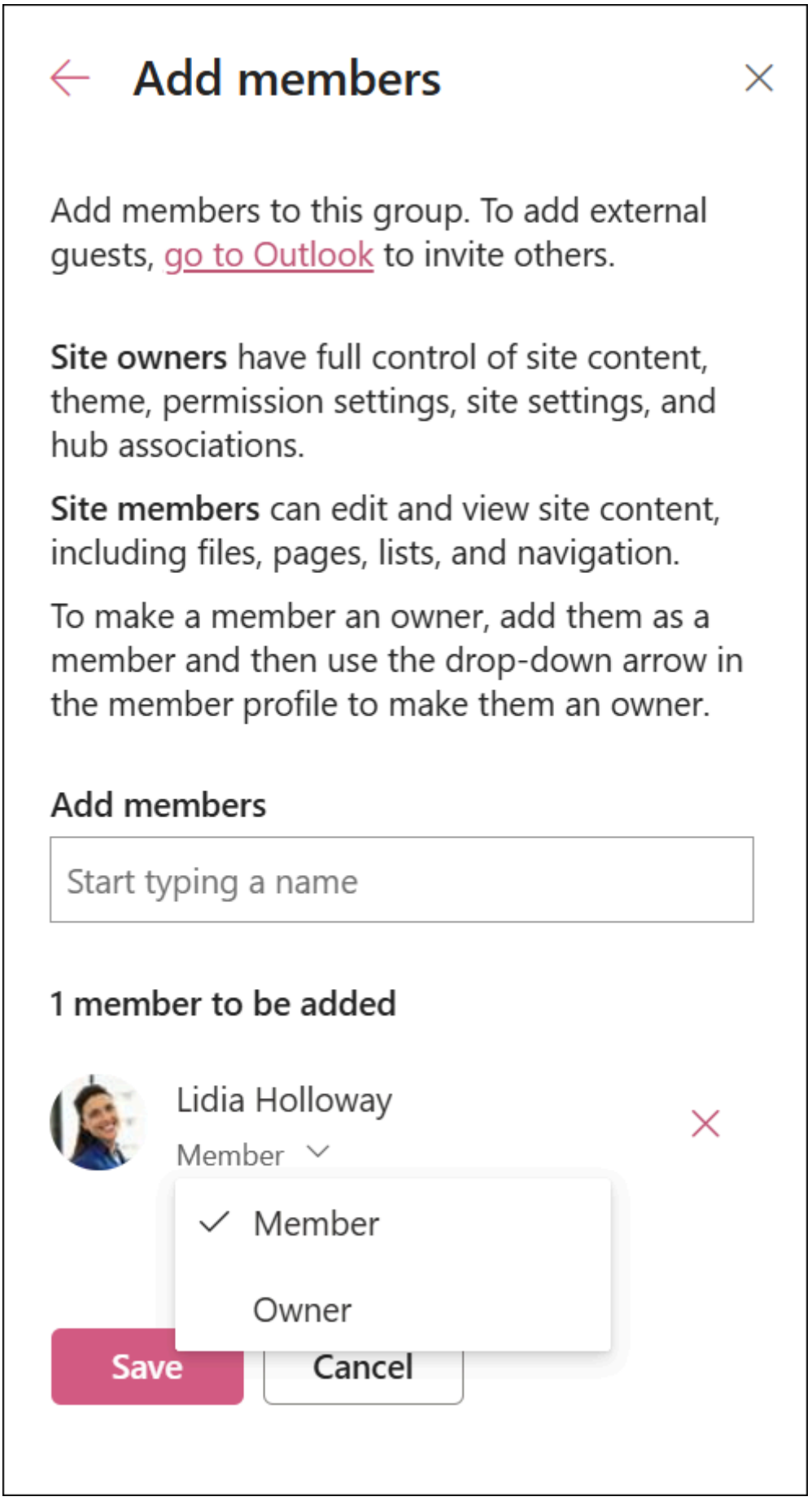
5. Select **Share**.

If you're on a team site, follow these steps:

1. Select **members**.



2. In the **Group membership** dialog, select **Add members**. Start typing the name of the user that you want to add. When the name appears, select it. You can add multiple users at once.



To make a member an owner, add them as a member and then use the drop-down arrow in the member profile to make them an owner.

Remove users from a group

1. On your website or team site, select **Settings**, and select **Site settings**. If you don't see **Site settings**, select **Site information**, and then select **View all site settings**. On some pages, you might need to select **Site contents**, and then select **Site settings**.

2. Under **Users and Permissions**, select **People and Groups**.

3. Under **Groups**, select the name of the group that you want to remove users from.

4. Select the check boxes next to the users you want to remove, select **Actions**, and then select **Remove Users from Group**.

5. In the confirmation window, select **OK**.

Grant site access to a group

1. On your website or team site, select **Settings**, and select **Site permissions**.

2. On the **Permissions** page, select **Advanced Permissions Settings**.

3. On the **Permissions** tab, select **Grant Permissions**.

4. In the **Share** dialog, type the name of the SharePoint group that you want to give access to.

5. By default, the **Share** dialog displays the message **Invite people to Edit** or **Invite people** with **Can edit** permissions. This message grants permissions in the SharePoint Members group. To choose a different permission level, select **Show options** and then choose a different SharePoint group or permission level under **Select a permission level** or **Select a group or permission level**. The drop-down box shows both groups and individual permission levels, like **Edit** or **View Only**.

6. Select **Share.**

Delete a group

> ⊗ **Caution**
>
> Don't delete any of the default SharePoint groups. Deleting default SharePoint groups can make the system unstable. Only delete groups that you created and no longer want to use.

1. On your website or team site, select **Settings**, and select **Site settings**. If you don't see **Site settings**, select **Site information**, and then select **View all site settings**. On some pages,

you might need to select **Site contents**, and then select **Site settings**.

2. Under **Users and Permissions**, select **People and Groups**.

3. On the **People and Groups** page, select the name of the SharePoint group that you want to delete.

4. Select **Settings**, and then select **Group Settings**.

5. At the bottom of the **Change Group Settings** page, select **Delete**.

6. In the confirmation window, select **OK**.

Assign a new permission level to a group

If you customize a permission level or create a new permission level, you can assign it to groups or users.

1. On your website or team site, select **Settings**, and select **Site settings**. If you don't see **Site settings**, select **Site information**, and then select **View all site settings**. On some pages, you might need to select **Site contents**, and then select **Site settings**.

2. On the **Site Settings** page, under **Users and Permissions**, select **Site Permissions**.

3. Select the check box next to the user or group to which you want to assign the new permission level.

4. On the **Permissions** tab, select **Edit User Permissions**.

5. On the **Edit Permissions** page, select the check box next to the name of the new permission level. If you select multiple permission levels, the permission level assigned to the group is the union of the individual permissions in the different levels. That is, if one level includes permissions (A, B, C), and the other level includes permissions (C, D), the new level for the group includes permissions (A, B, C, D).

6. Select **OK**.

> **Note**
>
> You can't modify permissions for the default SharePoint groups (Owners, Members, and Visitors) for Team sites that are connected to a Microsoft 365 group.

Add, change, or remove a site admin

1. On the site, select **Settings** , and select **Site settings**. If you don't see **Site settings**, select **Site information**, and then select **View all site settings**. On some pages, you might need to select **Site contents**, and then select **Site settings**.

2. Under **Users and Permissions**, select **Site Collection Administrators**.

3. In the **Site Collection Administrators** box, do one of the following:

   - To add a site collection administrator, enter the name or user alias of the person you want to add.
   - To change a site admin, select the **X** next to the name of the person, and then enter a new name.
   - To remove a site admin, select the **X** next to the name of the person.

4. Select **OK**.

> **Note**
>
> To see the **Site Collection Administrators** link, you must be at least a SharePoint Administrator. This link isn't displayed to site owners.

Last updated on 05/07/2026

Permissions inheritance in SharePoint

While SharePoint offers extensive customization options for site permissions, including changing inheritance, don't break inheritance. Use the built-in SharePoint groups for communication sites, and manage team site permissions through the associated Microsoft 365 group. Use sharing links to share individual files and folders with people outside the site. This approach makes administration much easier. For more information about managing permissions in the SharePoint modern experience, see Sharing and permissions in the SharePoint modern experience.

What is permissions inheritance?

Permissions inheritance means that the permission settings of an element in a site collection are passed on to the children of that element. In this way, sites inherit permissions from the top-level ("root") site of the site collection, libraries inherit from the site that contains the library, and so on. Permission inheritance enables you to make a permission assignment once, and have that permission apply to all sites, lists, libraries, folders, and items that inherit permissions. This behavior can reduce complexity and the amount of time site collection administrators and site owners spend on security management.

By default, SharePoint sites inherit permissions from a parent site. When you assign a user to the Members group, the user's permissions automatically cascade through all the sites, lists, libraries, folders, and items that inherit the permission level.

What is a parent in SharePoint permissions?

The term parent, when used in SharePoint permissions, emphasizes inheritance. The parent passes down its permission settings to all its children. By default, the root site of a site collection is the first parent for all the sites and other objects that are below it in the site hierarchy.

The root site of a site collection isn't the only parent. Every securable object (sites, libraries, lists, and so on) in a site collection can be a parent. That is, the root site is the parent of its subsites, each site is the parent of its libraries and lists, and each list is the parent of the list items in it. In this terminology, an object with a parent is known as a child. So, a subsite is the child of its parent site, a list item is the child of its list parent, and so on.

> **Important**

Create a site collection for each unit of work instead of using subsites to create a hierarchical structure. [Learn about using hub sites to organize your intranet](#).

By default, permissions are inherited from parent to child. That is, if you don't change the permission structure, a list item inherits permissions (through its parent list) from the root site in the collection. However, even if you break inheritance for a list, that list is still a parent for its own list items. The list items for the list inherit the permissions that the list has, and if you change the permissions for the list, the list items inherit the changes.

When you break the chain of inheritance from parent to child, the child starts with a copy of the parent's permissions. Then, you edit these permissions to make them the way that you want. You can add permissions, remove permissions, create special groups, and so on. None of the changes affect the original parent. If you decide that breaking inheritance was the wrong decision, you can resume inheriting permissions at any time.

When a user shares or stops sharing an item that contains other items with broken inheritance, a one-time push down of that permission addition or removal is sent to all child items, even those with broken inheritance. This rule applies to both direct permissions and sharing links. When managing permissions for an item with broken inheritance, users can remove any direct permissions on it. If an item with broken inheritance is accessible by a sharing link that was created on one of its parent folders and a user doesn't want that link to grant access to the item, users can either remove the link entirely or move the file outside of the folder for which sharing link has permissions.

More about permissions inheritance

Permission inheritance enables an administrator to assign permission levels at one time, and have the permissions apply throughout the site collection. Permissions pass from parent to child throughout the SharePoint hierarchy, from the top level of a site to the bottom. Permission inheritance can save time for site administrators, especially on large or complex site collections.

However, some scenarios have different requirements. In one scenario, you might have to restrict access to a site because it contains sensitive information that you must protect. In a different scenario, you might want to expand access and invite others to share information. If you want, you can break the inheritance behavior (stop inheriting permissions) at any level in the hierarchy.

Let's look at examples of these different scenarios.

Suppose that you have a company called Northwind Traders. You create a communication site called "Benefits" with the URL northwindtraders.sharepoint.com/sites/benefits. At the site collection root, you set up SharePoint groups, assign permission levels, and add users to the groups.

Suppose then that you create subsites for the "Benefits" site, such as "Health care" (northwindtraders.sharepoint.com/sites/benefits/healthcare) and "Retirement" (northwindtraders.sharepoint.com/sites/benefits/retirement). These subsites could even contain more subsites. For example, the "Health care" subsite could have a "Dental" subsite (northwindtraders.sharepoint.com/sites/benefits/healthcare/dental).

A scenario that uses default behavior

By default, permissions pass directly to subsites. That is, the groups and permission levels that you assigned at the site collection root pass down automatically to the subsite for reuse.

A scenario that restricts access to a site and its children

Suppose that your company offers special benefits only for executives. In this case, the administrators decide to separate the "Executive" subsite and break inheritance from the parent site, "Benefits."

The site owners for the "Executive" site change the permissions for the site, removing some groups and creating others. The subsites of the "Executive" site, "Bonuses" and "Company transportation," now inherit permissions only from the "Executive" subsite. Only the groups and users for "Executive" can access the lists and libraries that contain sensitive information.

For ease of maintenance, use a similar method to restrict access. Organize your site so that sensitive material is in the same place. If you organize the site this way, you only have to break inheritance one time, for that specific site or library. This approach is much less overhead. It requires much less work than creating separate permission structures in many locations for individual subsites and libraries.

A scenario that shares access to a folder and its children

Suppose that an employee at Northwind Traders hires consultants and wants to collaborate with them on documents in SharePoint. The employee doesn't want to give the consultants access to anything else on the SharePoint site.

When the employee shares the folder with the consultants, SharePoint automatically handles all the details of permissions and access by breaking inheritance on the folder itself. The consultants can access all the documents in the folder but can't view or access any other information on the site. Even though inheritance is technically broken, if you later add people to the parent site collection, you automatically give them permission to the shared folder.

Last updated on 05/07/2026

Permission levels in SharePoint

While SharePoint offers various permission levels for sites, use the built-in SharePoint groups for communication sites and manage team site permissions through the associated Microsoft 365 group. This approach makes administration easier. For information about managing permissions in the SharePoint modern experience, see Sharing and permissions in the SharePoint modern experience.

Understanding permission levels

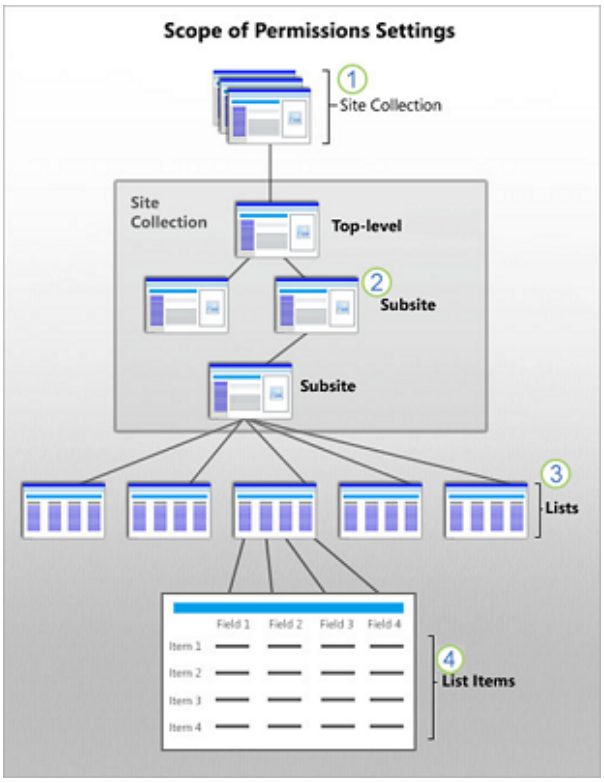
The easiest way to work with permissions is to use the default groups and permission levels, which cover most common scenarios. But, if you need to, you can set more fine-grained permissions beyond the default levels. This article describes the different permissions and permission levels, how SharePoint groups and permissions work together, and how permissions cascade through a site collection.

> **Note**
>
> Want to go straight to the steps for changing or setting permission levels? See **How to create and edit Permission Levels**.

Overview and permissions inheritance

If you work on a site, you're working inside a site collection. Every site exists in a site collection, which is a group of sites under a single top-level site. The top-level site is the root site of the site collection.

The following illustration of a site collection shows a simple hierarchy of sites, lists, and list items. The permissions scopes are numbered, starting at the broadest level at which you can set permissions, and ending at the narrowest level (a single item in a list).



Inheritance

An important concept to understand is permissions inheritance. By design, all the sites and site content in a collection inherit the permissions settings of the root or top-level site. When you assign unique permissions to sites, libraries, and items, those items no longer inherit permissions from their parent site. Here's more information on how permissions work within the hierarchy:

- A site collection administrator configures permissions for the top level site or root site for the whole collection.
- If you're a site owner, you can change permission settings for the site, which stops permission inheritance for the site.
- Lists and libraries inherit permissions from the site to which they belong. If you're a site owner, you can stop permissions inheritance and change the permission settings for the list or library.
- List items and library files inherit permissions from their parent list or library. If you have control of a list or library, you can stop permissions inheritance and change permissions settings directly on a specific item.

  It's important to know that a user can interrupt the default permission inheritance for a list or library item by sharing a document or item with someone who doesn't have access. In that case, SharePoint automatically stops inheritance on the document.

Default permission levels

Default permission levels make it easy to give common levels of permissions to one user or groups of users.

You can change any of the default permission levels, except **Full Control** and **Limited Access**. The following table describes these two permission levels.

Expand table

Permission Level	Description
Full Control	Contains all available SharePoint permissions. By default, the Owners group has this permission level. You can't customize or delete it.
Design	Create lists and document libraries, edit pages, and apply themes, borders, and style sheets on the site. No SharePoint group is automatically assigned this permission level.
Edit	Add, edit, and delete lists; view, add, update, and delete list items and documents. By default, the Members group has this permission level.
Contribute	View, add, update, and delete list items and documents.
Read	View pages and items in existing lists and document libraries and download documents.
Limited Access	Enables a user or group to browse to a site page or library to access a specific content item when they don't have permissions to open or edit any other items in the site or library. SharePoint automatically assigns this permission level when you provide access to one specific item. You can't assign Limited Access permissions directly to a user or group. Instead, when you assign edit or open permissions to the single item, SharePoint automatically assigns Limited Access to other required locations, such as the site or library in which the single item is located. This permission level allows SharePoint to render the user interface correctly and show the user some context around their location in the site. Limited Access doesn't grant any additional permissions to the user, so they can't see or access any other content.
Web-Only Limited Access	Web-Only Limited Access is a variant of the Limited Access permission level that enables users' access to the web object only.
Approve	Edit and approve pages, list items, and documents. By default, the *Approvers* group has this permission.
Manage Hierarchy	Create sites and edit pages, list items, and documents. By default, this permission level is assigned to the *Hierarchy Managers* group.
Restricted Read	View pages and documents, but not historical versions or user permissions.
View Only	View pages, items, and documents. Any document that has a server-side file handler can be viewed in the browser but not downloaded. File types that don't have a server-side file

Permission Level	Description
	handler (can't be opened in the browser), such as video files and .png files, can still be downloaded.

> **Note**
>
> Microsoft 365 subscriptions create a security group called "Everyone except external users" that contains every person you add into the Microsoft 365 directory (except people who you add explicitly as External Users). This security group is added to the Members group automatically on Modern Team sites with *Public* privacy settings, so that users in Microsoft 365 can access and edit the SharePoint site. Also, for Modern Team sites created as *Private*, "Everyone except external users" can't be granted any permissions and people must be explicitly granted permissions. In addition, Microsoft 365 subscriptions create a security group called "Company Administrators", which contains Microsoft 365 Admins (such as Global and Billing Admins). This security group is added to the Site Collection Administrators group. For more info, see **Default SharePoint groups**.

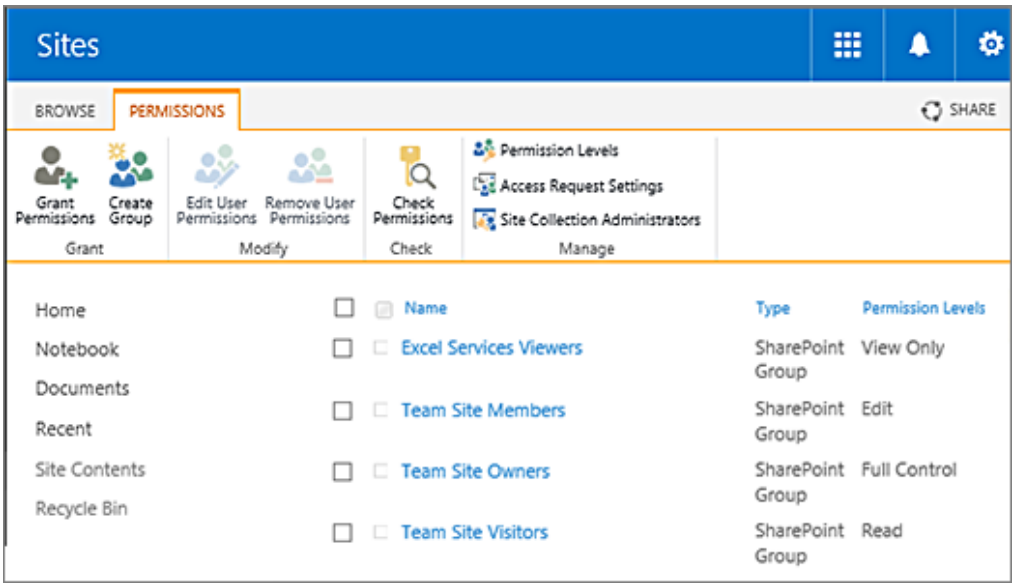
By default, site owners and members can add new users to the site.

To learn more about "Everyone except external users" permission, see Special SharePoint Groups.

Permission levels and SharePoint groups

Permission levels work together with SharePoint groups. A SharePoint group is a set of users who all have the same permission level.

The way this works is that you put related permissions together into a permission level. Then you assign that permission level to a SharePoint group.



By default, each kind of SharePoint site includes certain SharePoint groups. For example, a Team Site automatically includes the Owners, Members, and Visitors group. A Publishing Portal site includes those groups and several more, such as Approvers, Designers, Hierarchy Managers, and so on. When you create a site, SharePoint automatically creates a pre-defined set of SharePoint groups for that site. In addition, a SharePoint admin can define custom groups and permission levels.

To learn more about SharePoint groups, see Understanding SharePoint groups.

The SharePoint groups and permission levels that are included by default in your site might differ, depending on:

- The template that you choose for the site
- Whether a SharePoint admin created a unique permissions set on the site that has a specific purpose, such as Search

The following table describes the default permission levels and associated permissions for three standard groups: Visitors, Members, and Owners.

Expand table

Group	Permission level
Visitors	**Read** This level includes these permissions: Open View Items, Versions, pages, and Application pages Browse User Information Create Alerts Use Self-Service Site Creation Use Remote Interfaces Use Client Integration Features

Group	Permission level
Members	**Edit** This level includes all permissions in Read, plus: View, add, update, and delete Items Add, Edit, and Delete Lists Delete Versions Browse Directories Edit Personal User Information Manage Personal Views Add, Update, or Remove Personal Web Parts
Owners	**Full Control** This level includes all available SharePoint permissions.

Site permissions and permission levels

Site permissions apply generally across a SharePoint site. The following table describes the permissions that apply to sites, and shows the permission levels that use them.

Expand table

Permission	Full Control	Design	Edit	Contribute	Read	Limited Access	Approve	Manage Hierarchy	Restricted Read	View Only
Manage Permissions	X							X		
View Web Analytics Data	X							X		
Create Subsites	X							X		
Manage Web Site	X							X		
Add and Customize Pages	X	X						X		
Apply Themes and Borders	X	X								
Apply Style Sheets	X	X								
Create Groups	X									

Permission	Full Control	Design	Edit	Contribute	Read	Limited Access	Approve	Manage Hierarchy	Restricted Read	View Only
Browse Directories	X	X	X	X			X	X		
Use Self-Service Site Creation	X	X	X	X	X		X	X		X
View Pages	X	X	X	X	X		X	X	X	X
Enumerate Permissions	X							X		
Browse User Information	X	X	X	X	X	X	X	X		X
Manage Alerts	X							X		
Use Remote Interfaces	X	X	X	X	X		X	X		X
Use Client Integration Features	X	X	X	X	X	X	X	X		X
Open	X	X	X	X	X	X	X	X	X	X
Edit Personal User Information	X	X	X	X			X	X		

List permissions and permission levels

List permissions apply to content in lists and libraries. The following table describes the permissions that apply to lists and libraries, and shows the permission levels that use them.

Expand table

Permission	Full Control	Design	Edit	Contribute	Read	Limited Access	Approve	Manage Hierarchy	Restricted Read	View Only
Manage Lists	X	X	X					X		

Permission	Full Control	Design	Edit	Contribute	Read	Limited Access	Approve	Manage Hierarchy	Restricted Read	View Only
Override Check-Out	X	X					X	X		
Add Items	X	X	X	X			X	X		
Edit Items	X	X	X	X			X	X		
Delete Items	X	X	X	X			X	X		
View Items	X	X	X	X	X		X	X	X	X
Approve Items	X	X					X			
Open Items	X	X	X	X	X		X	X	X	
View Versions	X	X	X	X	X		X	X		X
Delete Versions	X	X	X	X			X	X		
Create Alerts	X	X	X	X	X		X	X		X
View Application Pages	X	X	X	X	X		X	X		X

Personal permissions and permission levels

Personal permissions apply to content that belongs to a single user. The following table describes the permissions that apply to personal views and web parts, and shows the permission levels that use them.

Expand table

Permission	Full Control	Design	Edit	Contribute	Read	Limited Access	Approve	Manage Hierarchy	Restricted Read	View Only
Manage Personal Views	X	X	X	X			X	X		
Add/Remove Private Web	X	X	X	X			X	X		

Permission	Full Control	Design	Edit	Contribute	Read	Limited Access	Approve	Manage Hierarchy	Restricted Read	View Only
Parts										
Update Personal Web Parts	X	X	X	X			X	X		

Permissions and dependent permissions

SharePoint permissions can depend on other SharePoint permissions. For example, you must be able to open an item to view it. In this way, View Items permission depends on Open permission.

When you select a SharePoint permission that depends on another, SharePoint automatically selects the associated permission. Similarly, when you clear SharePoint permission, SharePoint automatically clears any SharePoint permission that depends on it. For example, when you clear View Items, SharePoint automatically clears Manage Lists (you can't manage a list if you can't view an item).

> **Tip**
>
> The only SharePoint permission without a dependency is Open. All other SharePoint permissions depend on it. To test a custom permission level, you can just clear "Open". This action automatically clears all other permissions.

The following sections contain tables that describe SharePoint permissions for each permission category. For each permission, the table shows the dependent permissions.

- Site permissions and dependent permissions
- List permissions and dependent permissions
- Personal permissions and dependent permissions

Site permissions and dependent permissions

The following table describes the permissions that apply to sites, and shows the permissions that depend on them.

Expand table

Permission	Description	Dependent permissions
Manage Permissions	Create and change permission levels on the website and assign permissions to users and groups.	View Items, Open Items, View Versions, View Pages, Browse Directories, Enumerate Permissions, Browse User Information, Open
View Web Analytics Data	View reports on website usage.	View Pages, Open
Create Subsites	Create subsites such as team sites, Meeting Workspace sites, and Document Workspace sites.	View Pages, Browse User Information, Open
Manage website	Perform all administration tasks for the website, which includes managing content.	View Pages, Add and Customize Pages, Browse Directories, Enumerate Permissions, Browse User Information, Open
Add and Customize Pages	Add, change, or delete HTML pages or Web Part pages, and edit the website by using a Windows SharePoint Services-compatible editor.	View Items, Browse Directories, View Pages, Open
Apply Themes and Borders	Apply a theme or borders to the whole website.	View Pages, Open
Apply Style Sheets	Apply a style sheet (.css file) to the website.	View Pages, Open
Create Groups	Create a group of users who can be used anywhere within the site collection.	View Pages, Browse User Information, Open
Browse Directories	Enumerate files and folders in a website, by using an interface such as SharePoint Designer or web-based Distributed Authoring and Versioning (Web DAV).	View Pages, Open
Use Self-Service Site Creation	Create a website by using Self-Service Site Creation.	View Pages, Browse User Information, Open
View Pages	View pages in a website.	Open
Enumerate Permissions	Enumerate permissions on the website, list, folder, document, or list item.	View Items, Open Items, View Versions, Browse Directories, View Pages, Browse User Information, Open
Browse User Information	View information about users of the website.	Open
Manage Alerts	Manage alerts for all users of the website	View Items, Create Alerts, View Pages, Open

Permission	Description	Dependent permissions
Use Remote Interfaces	Use Simple Object Access Protocol (SOAP), Web DAV, or SharePoint Designer interfaces to access the website.	Open
Use Client Integration Features	Use features that launch client applications.	Use Remote Interfaces, Open
Open*	Open a website, list, or folder to access items inside that container.	No dependent permissions
Edit Personal User Information	Allow a user to change personal information, such as adding a picture.	Browse User Information, Open

List permissions and dependent permissions

The following table describes the permissions that apply to lists and libraries, and shows the permissions that depend on them.

Expand table

Permission	Description	Dependent permissions
Manage Lists	Create and delete lists, add or remove columns in a list, and add or remove public views of a list.	View Items, View Pages, Open, Manage Personal Views
Override Check-Out	Discard or check in a document that is checked out to another user.	View Items, View Pages, Open
Add Items	Add items to lists, add documents to document libraries, and add web discussion comments.	View Items, View Pages, Open
Edit Items	Edit items in lists, edit documents in document libraries, edit web discussion comments in documents, and customize Web Part Pages in document libraries.	View Items, View Pages, Open
Delete Items	Delete items from a list, documents from a document library, and web discussion comments in documents.	View Items, View Pages, Open
View Items	View items in lists, documents in document libraries, and web discussion comments.	View Pages, Open
Approve Items	Approve a minor version of a list item or document.	Edit Items, View Items, View Pages, Open
Open Items	View the source of documents that use server-side file handlers.	View Items, View Pages, Open

Permission	Description	Dependent permissions
View Versions	View past versions of a list item or document.	View Items, View Pages, Open
Delete Versions	Delete past versions of a list item or document.	View Items, View Versions, View Pages, Open
Create Alerts	Create e-mail alerts.	View Items, View Pages, Open
View Application Pages	View documents and views in a list or document library.	Open

Personal permissions and dependent permissions

The following table describes the permissions that apply to personal views and web parts, and shows the permissions that depend on them.

Expand table

Permission	Description	Dependent permissions
Manage Personal Views	Create, change, and delete personal views of lists.	View Items, View Pages, Open
Add/Remove Private Web Parts	Add or remove private Web Parts on a Web Part Page.	View Items, View Pages, Open, Update Personal Web Parts
Update Personal Web Parts	Update Web Parts to display personalized information.	View Items, View Pages, Open

Lockdown mode

Limited-access user permission lockdown mode is a site collection feature that you can use to secure published sites. When you turn on lockdown mode, it reduces fine-grain permissions for the limited access permission level. The following table details the default permissions of the limited access permission level and the reduced permissions when the lockdown mode feature is turned on.

Expand table

Permission	Limited access - default	Limited access - lockdown mode
List permissions: View Application Pages	X	

Permission	Limited access - default	Limited access - lockdown mode
Site permissions: Browse User Information	X	X
Site permissions: Use Remote Interfaces	X	
Site permissions: Use Client Integration Features	X	X
Site permissions: Open	X	X

Lockdown mode is on by default for all publishing sites, including if a legacy publishing site template is applied to the site collection. Lockdown mode is the recommended configuration if greater security on your sites is a requirement.

If you disable the limited-access user permission lockdown mode site collection feature, users in the "limited access" permissions level (such as Anonymous Users) can gain access to certain areas of your site.

Plan your permission strategy

Now that you understand permissions, inheritance, and permission levels, plan your strategy. Set guidelines for your users, minimize maintenance, and ensure compliance with your organization's data governance policies. For tips on planning your strategy, see Plan your permissions strategy.

Last updated on 04/30/2025

Permission levels

While SharePoint offers extensive customization options for site permissions, including custom permission levels, use the built-in SharePoint groups for communication site permissions. Manage team site permissions through the associated Microsoft 365 group. This approach simplifies administration. For more information about managing permissions in the SharePoint modern experience, see Sharing and permissions in the SharePoint modern experience.

If you need to create custom permission levels, this article describes how.

Create and edit permission levels

Permissions grant SharePoint users the ability to perform specific actions, such as editing items in a list or creating a site. However, you can't assign individual permissions to individual users in SharePoint. Instead, group related permissions together into a permission level. Then, assign that permission level to a SharePoint group that includes the people you're assigning permissions to.

SharePoint includes default permission levels that you can use, such as **Contribute** and **View Only**. If one of those default permission levels doesn't meet your needs, create a new permission level. It's easier to keep track of permission levels if you don't change the default permission levels.

Create a permission level

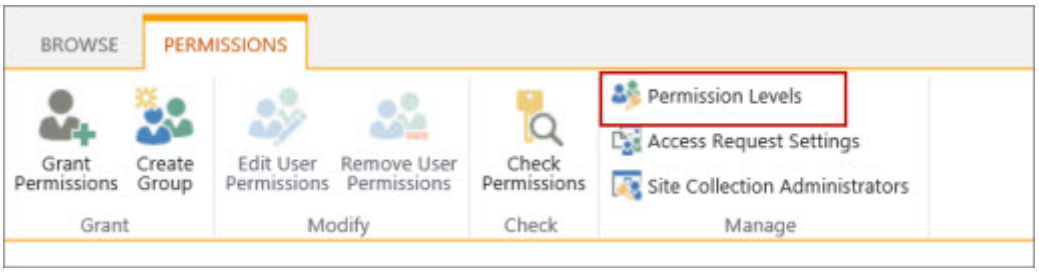
Create and change permission levels on the **Permissions Levels** page.

To create or change permission levels, you must belong to a SharePoint group that includes the permission to Manage Permissions. By default, you have this permission if you belong to the Owners group or if you're a Site Collection Administrator.

1. On the top-level site of the site collection, select **Settings** ⚙.

- For a classic site, select **Site settings**. On the **Site Settings** page, in the **Users and Permissions** section, select **Site permissions**.
- For a modern site, select **Site permissions**, and then **Advanced permissions settings**.

1. On the **Permissions** tab, in the Manage group, choose **Permission Levels**.



2. On the **Permission Levels** page, choose **Add a Permission Level**.

3. On the **Add a Permission Level** page, enter the name and the description.

4. In the **Permissions** area, select the check boxes next to the list, site, and personal permissions that you want this permission level to include.

5. Select **Create**.

You can change any of the listed permission levels, except **Full Control** and **Limited Access**.

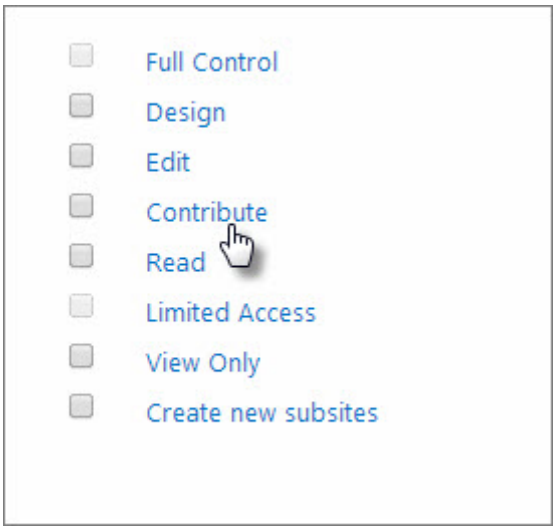
After you create the permission level, assign it to a SharePoint group.

Create a permission level by copying an existing permission level

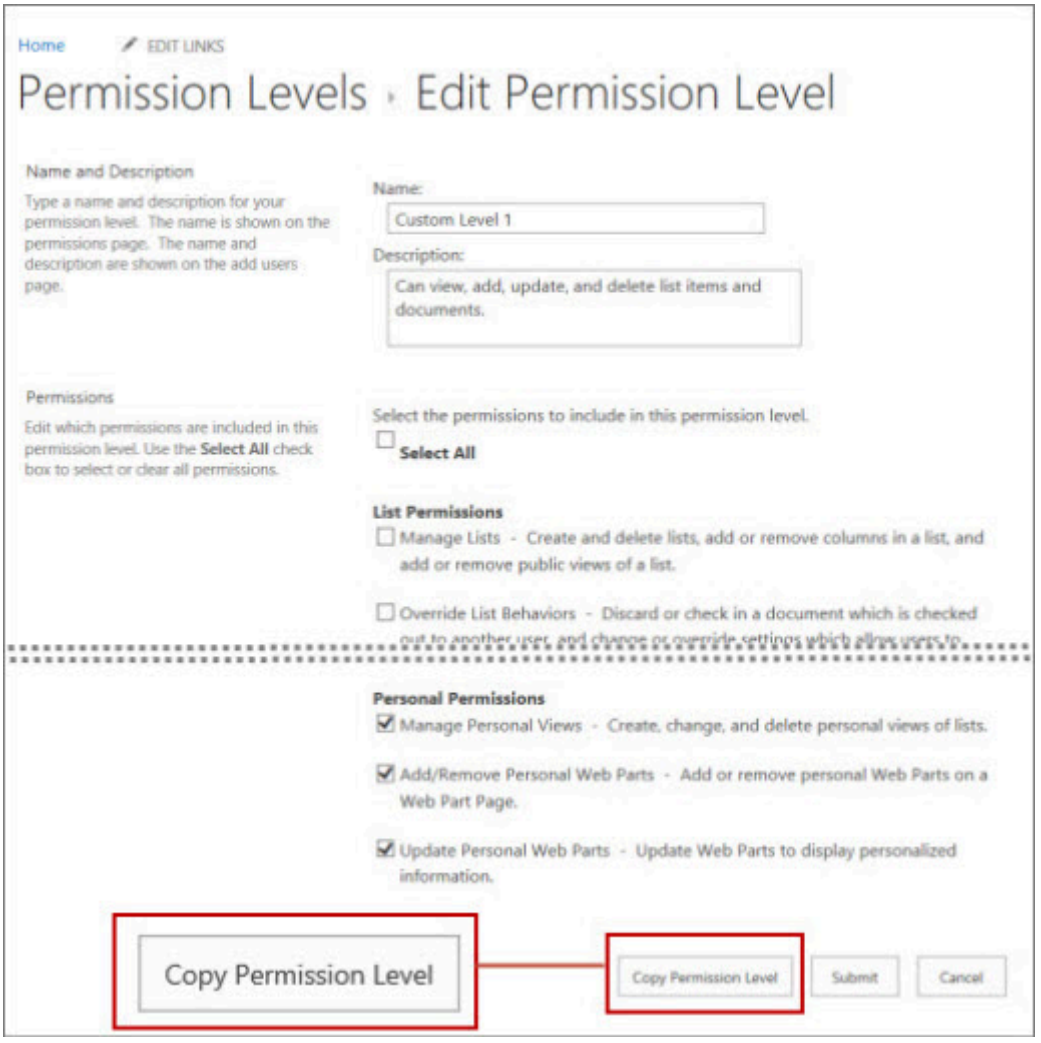
A quick way to create a new permission level is to copy an existing permission level. You might want to copy an existing permission level when it has permissions similar to what the new permission level needs. After you make the copy, you can add or remove the permissions you need for the new permission level.

Copy a permission level

1. On the **Permission Levels** page, select the name of the permission level that you want to copy. Be sure to select the link; don't select the checkbox next to the name. For example, **Contribute**, as shown in the following figure.



2. On the **Edit Permission Level** page, select **Copy Permission Level**. This option is at the bottom of the page after the **Personal Permissions** section.



3. On the **Copy Permission Level** page, type a name and description for the new permission level.

4. Choose which permissions you want to add or remove, and then select **Create**.

After you create the permission level, assign it to a SharePoint group.

Make changes to a permission level

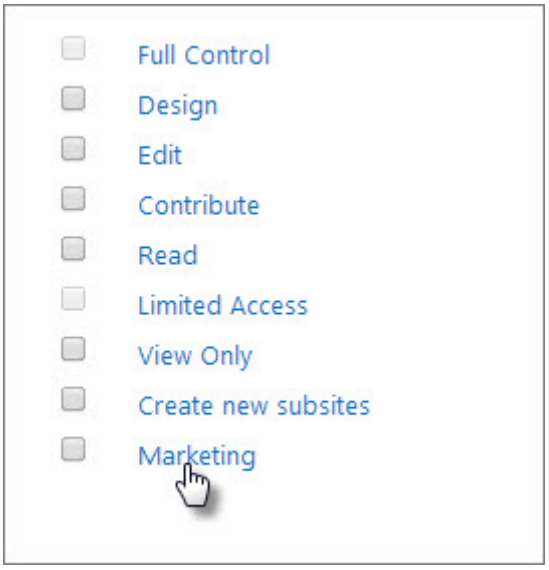
You can make the following changes to a permission level:

- Update the name or description
- Add or remove permissions

Don't change the default permission levels that come with SharePoint. You can't change the **Full Control** and **Limited Access** default permission levels.

Change a permission level

1. On the **Permission Levels** page, select the name of the permission level you want to edit. Be sure to select the link; don't select the checkbox next to the name. For example, **Marketing**, as shown in the following figure.



2. On **Edit Permission Level**, you can:

- Change the description.
- Add or remove permissions to the level.

1. After you make your changes, select **Submit**.

You can delete any permission level, except for **Full Control** and **Limited Access**. Don't delete a default permission level.

To delete a permission level, on the **Permission Levels** page, select the check box next to the permission level that you want to delete, and then choose **Delete Selected Permission Levels**.

> **Important**
>
> You can create permission levels that don't grant the minimum required permissions. The modern user experience uses client-side rendering, which requires that all users have the "Use Remote Interfaces" permission. Removing "Use Remote Interfaces" from a permissions level results in Access Denied errors that either prevent features on a modern page from loading or prevent the entire modern page from loading, resulting in an Access Denied error for the user.

Best practices for permission levels

Permission levels apply to a specific site collection. This condition means that any changes you make to a permission level affect the entire site collection. Therefore, follow these recommendations:

- **Don't edit default permission levels** If you change a default permission level, your changes affect all the built-in SharePoint groups within the site collection. It can also cause confusion if you have two site collections that have permission levels with the same name, but each contains a different set of permissions.
- **Don't delete default permission levels** If you delete a default permission level, you remove it from all built-in SharePoint groups that contain it within the site collection. This action can cause users assigned to those groups to lose critical permissions.
- **Assign permission levels to SharePoint groups** You can assign a permission level to a single SharePoint user, but it's easier to keep track of who has permissions to which sites if you assign permission levels to a SharePoint group, and add that individual to the group. This practice can also help site performance.

Last updated on 05/07/2026

Default SharePoint groups

When you create a site (previously called a "site collection"), SharePoint automatically creates the default SharePoint groups. These default groups use SharePoint's default permission levels, which are sometimes called SharePoint roles, to grant users rights and access. The permission levels that these groups have represent common levels of access that users need. They're a good starting point when you add users to a SharePoint site.

Administrators can create extra groups to better align with specific business needs. How you design and populate your SharePoint groups affects security for your site and site content.

For more information about permissions, see the following articles:

- Understanding permission levels in SharePoint
- Edit and manage permissions for a SharePoint list or library

Permission levels for default SharePoint groups

Use SharePoint groups to control access for sets of users instead of individual users. SharePoint groups usually consist of many individual users. They can also hold Microsoft Entra security groups (created in Microsoft 365 or Microsoft Entra ID), or they can be a combination of individual users and security groups.

Each SharePoint group has a permission level. A permission level is simply a collection of individual permissions, such as Open, View, Edit, or Delete. All the users in a group automatically have the permission level of the group. You can organize users into any number of groups, depending on the complexity of your organization or your needs.

Each site template has a set of SharePoint groups associated with it. When you create a site, you use a site template, and SharePoint automatically creates the correct set of SharePoint groups for the site. The specific collection of groups depends on the type of template that you choose.

For example, the following table shows the groups and permission levels that are created for team sites:

Expand table

SharePoint groups	Default permission level	Applies to team sites
Approvers	Approve	No
Designers	Design, Limited Access	No
Hierarchy Managers	Manage Hierarchy	No
<site name> Members	Edit	Yes
<site name> Owners	Full Control	Yes
<site name> Visitors	Read	Yes
Restricted Readers	Restricted Read	No
Style Resource Readers	Limited Access	No
Quick Deploy Users	Contribute	No
Translation Managers	Limited Access	No

Suggested uses for SharePoint groups

The following table describes the SharePoint groups that are created when you use a standard site template to create a site. The table also provides suggested uses for each group.

Expand table

Group Name	Permission level	Use this group for
Approvers	Approve	Members of this group can edit and approve pages, list items, and documents.
Designers	Design	Members of this group can edit lists, document libraries, and pages in the site. Designers can create Master Pages and Page Layouts in the Master Page Gallery and can change the behavior and appearance of each subsite by using master pages and CSS files.
Hierarchy Managers	Manage Hierarchy	Members of this group can create sites, lists, list items, and documents.
Owners	Full Control	People who must be able to manage site permissions, settings, and appearance.
Members	Edit or Contribute	People who must be able to edit site content. Permission level depends on the site template that was used to create the site
Visitors	Read	People who must be able to see site content, but not edit it.

Group Name	Permission level	Use this group for
Restricted Readers	Restricted Read	People who should be able to view pages and documents but not view versions or permissions.
Style Resource Readers	Restricted Read	People in this group have Limited Access to the Style Library and Master Page Gallery.
Quick Deploy Users	Contribute	These users can schedule Quick Deploy jobs (Content Deployment).
Viewers	View Only	These users see content, but can't edit or download it.

Special SharePoint Groups

"Everyone except external users" is a special group that doesn't appear in the Microsoft 365 admin center, and "Company Administrator" acts like a group but is a role in Microsoft Entra ID.

Everyone except external users All users added to your organization automatically become members of "Everyone except external users." You can't change default permissions granted to "Everyone except external users" on Microsoft 365 group-connected team sites. If a group-connected team site is set to "Public," then "Everyone except external users" has a default permission level of "Edit."

When a group-connected team site is set to "Private," then "Everyone except external users" can be manually added to the site through "Site permissions." To change the privacy setting for a group-connected team site, select the Settings icon, and then select **Site information**.

Company Administrator This group contains all users who are assigned the global admin role. For more info about this role and its permissions in Microsoft Entra ID, see Company administrator. The root site for your organization is created with "Company Administrator" as the primary admin.

Site administrators

Expand table

Description	SharePoint in Microsoft 365	SharePoint Server
Who can use this group?	Yes	Yes

A site can have several site admins, but it must have one primary administrator. Any site admin can add or remove other admins. Site admins have full control of the site root and any subsites in the site, and can audit all site content.

In SharePoint Server, you designate a site collection administrator when you create a site.

SharePoint admins

Expand table

Description	SharePoint in Microsoft 365	SharePoint Server
Who can use this group?	Yes	No, by default. Requires special installation.

In SharePoint in Microsoft 365, there's also a SharePoint admin. A SharePoint admin can use the SharePoint admin center or PowerShell to manage settings for all sites. Any global admin in Microsoft 365 also has the permissions of a SharePoint admin. For more info about the SharePoint admin role, see About the SharePoint admin role in Microsoft 365.

If you're using SharePoint Server, you don't have a SharePoint admin or SharePoint admin center.

Last updated on 05/07/2026

Sharing errors in SharePoint and OneDrive

This article covers the different errors that you might encounter when sharing files or folders from SharePoint or OneDrive in Microsoft 365. To fix these errors, you need to be a SharePoint Administrator or other administrator in your organization. If you're not an administrator, contact your help desk and give them your error code.

Changing these settings changes the types of external sharing that are allowed in your organization. In some cases, someone in your organization sets these settings for business reasons.

OSE201

Error OSE201 indicates that external sharing is turned off for all of your SharePoint and OneDrive sites.

First, change the external sharing setting for your organization:

1. Go to **Sharing** in the SharePoint admin center, and sign in.

   If you have Office 365 operated by 21Vianet (China), sign in to the Microsoft 365 admin center, and then browse to the SharePoint admin center and open the Sharing page.

2. Under **External sharing**, for both SharePoint and OneDrive, select **Anyone** or **New and existing guests**.

3. Select **Save**.

Next, check the external sharing settings for the site that you want to share from.

If you're sharing from a SharePoint site

1. In the new SharePoint admin center, select **Sites** > **Active sites**.

2. Select the site that you want to share from, and then select **Sharing**.

3. Make sure that either **New and existing guests** or **Anyone** is selected. If you made changes, select **Save**.

Try sharing again.

If you're sharing from OneDrive

1. In the Microsoft 365 admin center, in the left pane, under **Users**, select **Active users**.
2. Select the user, and then select the **OneDrive** tab.
3. Select **Manage external sharing**.
4. Make sure **Let people outside your organization access your site** is turned on, and **Allow sharing with anonymous guest links and authenticated users** or **Allow sharing to authenticated guest users with invitations** is selected.

Try sharing again.

OSE202

Error OSE202 indicates you can share with only those guests who are already in your directory. You can add guests directly through Microsoft Entra ID, or change the setting by following these steps:

First, change the external sharing setting for your organization.

1. Go to **Sharing** in the SharePoint admin center, and sign in.

   If you have Office 365 operated by 21Vianet (China), sign in to the Microsoft 365 admin center, and then browse to the SharePoint admin center and open the Sharing page.

2. Under **External sharing**, select **Anyone** or **New and existing guests** for both SharePoint and OneDrive.
3. Select **Save**.

Next, check the external sharing settings for the site that you want to share from.

If you're sharing from a SharePoint site

1. In the navigation pane of the new SharePoint admin center, select **Sites** > **Active sites**.
2. Select the site that you want to share from, and then select **Sharing**.
3. Make sure that either **New and existing guests** or **Anyone** is selected. If you made changes, select **Save**.

Try sharing again.

If you're sharing from OneDrive

1. In the Microsoft 365 admin center, in the left pane, under **Users**, select **Active users**.
2. Select the user, and then select the **OneDrive** tab.
3. Select **Manage external sharing**.
4. Make sure **Let people outside your organization access your site** is turned on, and **Allow sharing with anonymous guest links and authenticated users** or **Allow sharing to authenticated guest users with invitations** is selected.

Try sharing again.

OSE204

Error OSE204 indicates sharing is turned off for the site that you're trying to share from. In this scenario, change the setting as follows:

1. Go to **Active sites** in the SharePoint admin center, and sign in.

   If you have Office 365 operated by 21Vianet (China), sign in to the Microsoft 365 admin center, then browse to the SharePoint admin center and open the Active sites page.

2. Select the site that you want to share from, and then select **Sharing**.
3. Make sure that either **New and existing guests** or **Anyone** is selected, and then select **Save**.

Try sharing again.

OSE205

Error OSE205 indicates you can share the site with only those guests who are already in your directory. You can add guests directly through Microsoft Entra ID, or change the setting by doing the following steps:

1. Go to **Active sites** in the SharePoint admin center, and sign in.

   If you have Office 365 operated by 21Vianet (China), sign in to the Microsoft 365 admin center, then browse to the SharePoint admin center and open the Active sites page.

2. Select the site that you want to share from, and then select **Sharing**.

3. Make sure that either **New and existing guests** or **Anyone** is selected, and then select **Save**.

OSE207

Error OSE207 indicates external sharing is turned off for OneDrive. In this scenario, change this setting as follows:

1. Go to **Sharing** in the SharePoint admin center, and sign in.

   If you have Office 365 operated by 21Vianet (China), sign in to the Microsoft 365 admin center, and then browse to the SharePoint admin center and open the Sharing page.

2. Under **External sharing**, select **Anyone** or **New and existing guests** for OneDrive.

3. Select **Save**.

Try sharing again.

OSE208

Error OSE208 indicates you can share OneDrive files and folders with only those guests who are already in your directory. You can add guests directly through Microsoft Entra ID, or change the setting by doing the following steps:

1. Go to **Sharing** in the SharePoint admin center, and sign in.

   If you have Office 365 operated by 21Vianet (China), sign in to the Microsoft 365 admin center, and then browse to the SharePoint admin center and open the Sharing page.

2. Under **External sharing**, change the OneDrive setting to either **Anyone** or **New and existing external users**.

3. Select **Save**.

Try sharing again.

OSE303

Error OSE303 indicates the person sharing the file or folder isn't a member of the security groups that are allowed to share with guests and by using "Anyone" links. To change this setting:

1. Go to **Sharing** in the SharePoint admin center, and sign in.

If you have Office 365 operated by 21Vianet (China), sign in to the Microsoft 365 admin center, and then browse to the SharePoint admin center and open the Sharing page.

2. Select **Limit external sharing to specific security groups**.

3. Under **Who can share outside your organization**, note the security groups listed for **Let only users in selected security groups share with authenticated external users and using anonymous links**. You need to add the user to one of the listed security groups. (Instead, you can clear the check box and remove the sharing restriction.)

Add a user to a security group

1. On the Groups page of the Microsoft 365 admin center, find the group you want to edit.

2. Select the group. On the **Members** tab, select **View all and manage members**.

3. Select **Add members**.

4. Enter the user's name in the search box, select the check box in the results list, and then select **Save**.

5. Select **Close** three times.

Try sharing again.

OSE304

Error OSE304 indicates the person sharing the file or folder isn't a member of the security groups that are allowed to share with guests. To change this setting:

1. Go to **Sharing** in the SharePoint admin center, and sign in.

   If you have Office 365 operated by 21Vianet (China), sign in to the Microsoft 365 admin center, and then browse to the SharePoint admin center and open the Sharing page.

2. Select **Limit external sharing to specific security groups**.

3. Under **Who can share outside your organization**, note the security groups listed for **Let only users in selected security groups share with authenticated external users**. You need to add the user to one of the listed security groups. (Instead, you can clear the check box and remove the sharing restriction.)

Add a user to a security group

1. On the Groups page of the Microsoft 365 admin center, find the group you want to edit.
2. Select the group. On the **Members** tab, select **View all and manage members**.
3. Select **Add members**.
4. Enter the user's name in the search box, select the check box in the results list, and then select **Save**.
5. Select **Close** three times.

Try sharing again.

OSE401

Error OSE401 indicates your organization-level setting lets you share with only people on specific domains. The person you're trying to share with isn't on one of the listed domains. To change this setting:

1. Go to **Sharing** in the SharePoint admin center, and sign in.

   If you have Office 365 operated by 21Vianet (China), sign in to the Microsoft 365 admin center, and then browse to the SharePoint admin center and open the Sharing page.

2. Under **Advanced settings for external sharing**, select **Add domains**, add the domain that you want to share with to the list of allowed domains, and select **OK**. Instead, you can turn off domain filtering by clearing the **Limit external sharing by domain** check box.
3. Select **Save**.

Try sharing again.

OSE402

Error OSE402 indicates your organization-level setting blocks sharing with people on specific domains. The person you're trying to share with is on one of the listed domains. To change this setting:

1. Go to **Sharing** in the SharePoint admin center, and sign in.

   If you have Office 365 operated by 21Vianet (China), sign in to the Microsoft 365 admin center, and then browse to the SharePoint admin center and open the Sharing page.

2. Under **Advanced settings for external sharing**, select **Add domains**, remove the domain from the list of blocked domains, and select **OK**. Instead, you can turn off domain filtering by clearing the **Limit external sharing by domain** check box.

3. Select **Save**.

Try sharing again.

OSE403

Error OSE403 indicates the site from which you're sharing lets you share with only people on specific domains. The person you're trying to share with isn't on one of the listed domains. To change this setting:

1. Go to **More features** in the SharePoint admin center, and sign in.

   If you have Office 365 operated by 21Vianet (China), sign in to the Microsoft 365 admin center, then browse to the SharePoint admin center and open the More features page.

2. Under **Classic site collections page**, select **Open**.

3. Select the site that you're sharing from, and in the ribbon, select **Sharing**.

4. Under **Site collection additional settings**, add the domain that you want to share with to the list of allowed domains. Instead, you can turn off domain filtering by clearing the **Limit external sharing using domains** check box.

5. Select **Save**.

Try sharing again.

OSE404

Error OSE404 indicates the site from which you're sharing blocks sharing with people on specific domains. The person you're trying to share with is on one of the listed domains. To change this setting:

1. Go to **More features** in the SharePoint admin center, and sign in.

   If you have Office 365 operated by 21Vianet (China), sign in to the Microsoft 365 admin center, then browse to the SharePoint admin center and open the More features page.

2. Under **Classic site collections page**, select **Open**.

3. Select the site that you're sharing from, and in the ribbon, select **Sharing**.
4. Under **Site collection additional settings**, remove the domain that you want to share with from the list of blocked domains. Instead, you can turn off domain filtering by clearing the **Limit external sharing using domains** check box.
5. Select **Save**.

Try sharing again.

See also

External sharing overview

Manage sharing settings

Stop sharing files or folders or change permissions

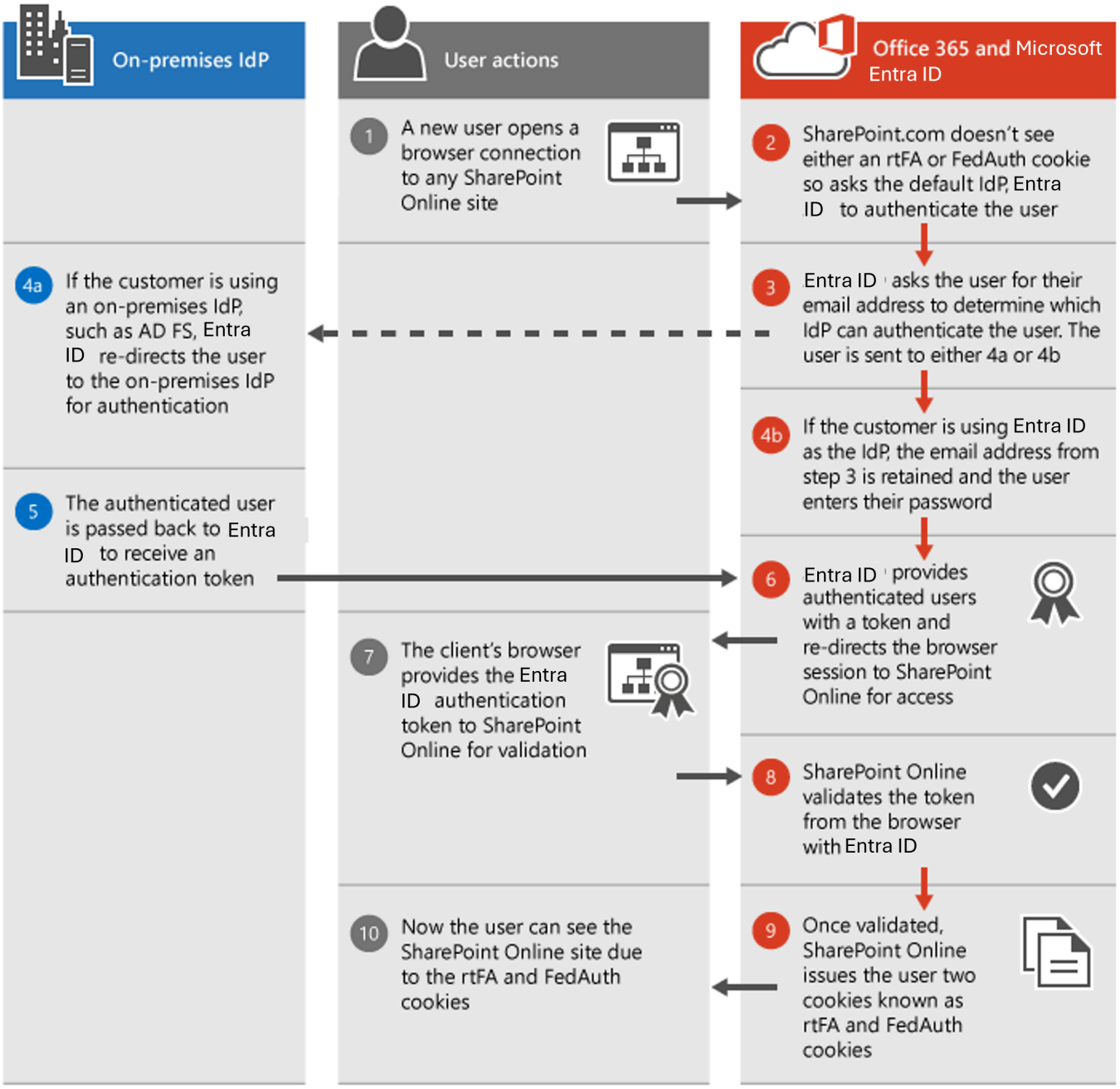
Last updated on 05/07/2026

SharePoint authentication

SharePoint in Microsoft 365 serves a wide range of customers with a variety of usability and security needs. Some customers don't mind asking users to reauthenticate if it means their data will be more secure. Other customers want to minimize the number of sign-in screens that users see, especially in situations where it seems as though SharePoint should already know who the user is. Luckily, customers don't have to choose usability or security because they work together in a lot of great ways.

The following diagram outlines the SharePoint authentication process. It walks through how the scenario works using either your own Identity Provider (IdP) or the default Microsoft Entra IdP.

The Federation Authentication (FedAuth) cookie is for each top-level site in SharePoint such as the root site, OneDrive, and the admin center site. The root Federation Authentication (rtFA) cookie is used across all of SharePoint. When a user visits a new top-level site or another company's page, the rtFA cookie is used to authenticate them silently without a prompt. When a user signs out of SharePoint, the rtFA cookie is deleted.



> **Note**
>
> For information about SharePoint authentication in hybrid scenarios, see The building blocks of Microsoft 365 hybrid.

Session and persistent cookies

By default, all SharePoint cookies are **session** cookies. These cookies are not saved to the browser's cookie cache and instead are deleted whenever the browser is closed. Microsoft Entra ID provides a **Keep Me Signed In** button during login that passes a signal to Microsoft 365 to enable **persistent** cookies. These cookies are saved to the browser's cache and will persist even if the browser is closed or the computer is restarted.

Persistent cookies have a huge impact on the sign-in experience by reducing the number of authentication prompts users see. Persistent cookies are also required for some SharePoint features, such as **Open with Explorer** and **Mapped Drives**.

For more info about session timeouts, see Session timeouts for Microsoft 365.

Last updated on 01/26/2026

How SharePoint and OneDrive safeguard your data in the cloud

Article • 01/13/2025

You control your data. When you put your data in SharePoint and OneDrive for Microsoft 365, you remain the owner of the data. For more info about the ownership of your data, see Microsoft 365 Privacy by Design.

How we treat your data

Microsoft engineers administer SharePoint and OneDrive using a PowerShell console that requires two-factor authentication. We perform day-to-day tasks by running workflows so we can rapidly respond to new situations. Check-ins to the service require code review and management approval.

No engineer has standing access to the service. When engineers need access, they must request it. Eligibility is checked, and if engineer access is approved, it's only for a limited time. In rare cases where Microsoft engineers need access to content (for example, if you submit a support ticket because a user can't access an important file that we believe is damaged), the engineers must check in a specific workflow that requires business justification and manager approval. An audit event is generated that you can view in the Microsoft 365 admin center. You can also turn on a feature called Customer Lockbox, so you need to approve the request. The engineer gets access only to the file in question. To learn how to turn on or off Customer Lockbox and approve and deny requests, see Microsoft Purview Customer Lockbox Requests.

How you can safeguard your data

One of the most important things you can do to safeguard your data is to require two-factor authentication for your identities in Microsoft 365. This prevents credentials from being used without a second factor and mitigates the impact of compromised passwords. The second factor can be made through a phone call, text message, or app. When you roll out two-factor authentication, start with your Global Administrators, and then other admins and site collection admins. For info about how to do this, see Set up multi-factor authentication for Microsoft 365 users.

Other things we recommend to increase security:

- Use Microsoft Entra device-based conditional access to block or limit access on unmanaged devices like airport or hotel kiosks. See Control access from unmanaged devices.
- Create policies to sign users out of Microsoft 365 web sessions after a period of inactivity. For information, see Sign out inactive users.
- Evaluate the need for IP-based sessions. These simulate the access model of an on-premises deployment. Read more at Control access based on network location or app.
- Empower workers to share broadly but safely. You can require sign-in or use links that expire or grant limited privileges. See Manage external sharing for your SharePoint environment.
- Prevent accidental exposure of sensitive content. Create DLP policies to identify documents and prevent them from being shared. See Learn about data loss prevention.

Protected in transit and at rest

Protected in transit

When data transits into the service from clients, and between datacenters, it's protected using best-in-class encryption. For info, see Data Encryption in OneDrive and SharePoint. We only permit secure access. We won't make authenticated connections over HTTP but, instead, redirect to HTTPS.

Protected at rest

Physical protection: Only a limited number of essential personnel can gain access to datacenters. Their identities are verified with multiple factors of authentication, including smart cards and biometrics. There are on-premises security officers, motion sensors, and video surveillance. Intrusion detection alerts monitor anomalous activity.

Network protection: The networks and identities are isolated from the Microsoft corporate network. We administer the service with dedicated Active Directory domains, we have separate domains for test and production, and the production domain is divided into multiple isolated domains for reliability and security. For more information about the built-in physical and logical security from Microsoft 365, see Built-in security from Microsoft 365.

Application security: Engineers who build features follow the security development lifecycle. Automated and manual analyses help identify possible vulnerabilities. The Microsoft security response center (Microsoft Security Response Center) helps triage incoming vulnerability reports and evaluate mitigations. Through the Microsoft Cloud Bug Bounty, people across the world can earn money by reporting vulnerabilities. Read more about this at Microsoft Cloud Bug Bounty Terms.

Content protection: Your data is encrypted at the disk level using BitLocker encryption and at the file level using keys. For info, see Data Encryption in OneDrive and SharePoint. For information about using Customer Key to provide and control the keys that are used to encrypt your data at rest in Microsoft 365, see Service encryption with Microsoft Purview Customer Key FAQ.

The Microsoft 365 anti-malware engine scans documents at upload time for content matching an AV signature (updated hourly). For info, see Virus detection in SharePoint. For more advanced protection, use Microsoft 365 Advanced Threat Protection (ATP). ATP analyzes content that's shared and applies threat intelligence and analysis to identify sophisticated threats. For info, see Microsoft 365 Advanced Threat Protection.

To limit the risk of content being downloaded to untrusted devices:

- Limit sync to devices on the domains you specify: Allow syncing only on computers joined to specific domains.
- Use Intune to limit access to content in the OneDrive and SharePoint mobile apps: Control access to features in the OneDrive and SharePoint mobile apps.

To manage content at rest:

- Configure IRM policies on SharePoint document libraries to limit download of content. See Set up Information Rights Management (IRM) in SharePoint admin center.
- Evaluate the use of Azure Information Protection (AIP). Classification and labeling let you track and control how data is used. Visit Azure Information Protection.

Highly available, always recoverable

Our datacenters are geo-distributed within the region and fault tolerant. Data is mirrored in at least two datacenters to mitigate the impact of a natural disaster or service-impacting outage. For more information, see Where your Microsoft 365 customer data is stored.

Metadata backups are kept for 14 days and can be restored to any point in time within a five-minute window.

In the case of a ransomware attack, you can use Version history (Enable and configure versioning for a list or library) to roll back, and the recycle bin or site collection recycle bin to restore (Restore deleted items from the site collection recycle bin). If an item is removed from the site collection recycle bin, you can call support within 14 days to access a backup. For information about the new Files Restore feature that lets users restore an entire OneDrive to any point within the past 30 days, see Restore your OneDrive.

Continuously validated

We continuously monitor our datacenters to keep them healthy and secure. This starts with inventory. An inventory agent scans each subnet looking for neighbors. For each machine, we perform a state capture.

After we have an inventory, we can monitor and remediate the health of machines. The security patch train applies patches, updates anti-virus signatures, and makes sure we have a known good configuration saved. We have role-specific logic that ensures we only patch or rotate out a certain percentage of machines at a time.

We have an automated workflow to identify machines that don't meet policies and queue them for replacement.

The Microsoft 365 "Red Team" within Microsoft is made up of intrusion specialists. They look for any opportunity to gain unauthorized access. The "Blue Team" is made up of defense engineers who focus on prevention, detection, and recovery. They build intrusion detection and response technologies. To keep up with the learnings of the security teams at Microsoft, see Security, Compliance, and Identity Blog.

To monitor and observe activity in your Microsoft 365 subscription:

- If you have an on-premises security operations center or SIEM, you can monitor activity with the Management Activity API. For information, see Microsoft 365 Management APIs overview. This will show you activity from across SharePoint, Exchange, Microsoft Entra ID, DLP, and more. If you don't have an on-premises security operations center or SIEM, you can use Cloud App Security. Cloud App Security uses the Management Activity API. For info, see Overview of Microsoft 365 Cloud App Security. Through Cloud App Security, you can report, search, and alert on activity.

- Use Microsoft Entra ID Protection. This applies machine learning to detect suspicious account behavior, for example, simultaneous sign-ins from the same user in different parts of the world. You can configure identity protection to take action to block these sign-ins. For more info, see Microsoft Entra ID Protection.
- Use Secure Score to evaluate the security profile of your subscription against a known good baseline, and identify opportunities to increase protection. For more info, see Microsoft Secure Score.

Audited and compliant

Regulatory compliance is fundamental to Microsoft 365. We make sure the service complies with regulatory and compliance standards. We also help you meet your audit and compliance obligations. The Service Trust Portal is a one-stop-shop for compliance and trust information for Microsoft enterprise services. The portal contains reports, whitepapers, vulnerability assessments, and compliance guides. For more info about the Service Trust Portal, see Get started with the Microsoft Service Trust Portal.

To meet your regulatory requirements:

- Audit Microsoft 365 activity in the Security & Compliance Center: Search the audit log in the Microsoft 365 Security & Compliance Center.
- Create eDiscovery cases: Manage eDiscovery cases in the Microsoft 365 Security & Compliance Center.
- Apply retention policies: Create and apply information management policies.

Feedback

Was this page helpful? Yes No

Provide product feedback

IT Admins - SharePoint and OneDrive unmanaged device access controls

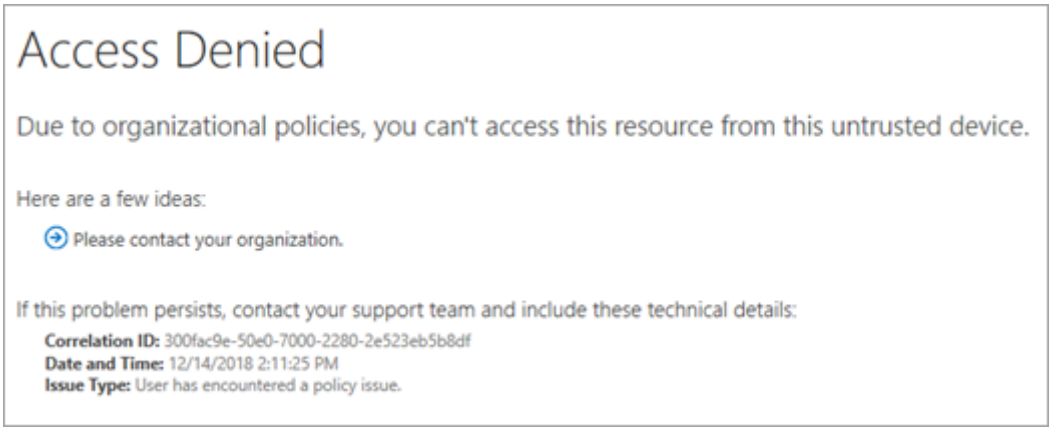
With at least the permissions of a SharePoint Administrator in Microsoft 365, you can block or limit access to SharePoint and OneDrive content from unmanaged devices (those not hybrid AD joined or compliant in Intune). You can block or limit access for:

- All users in the organization or only some users or security groups.
- All sites in the organization or only some sites.

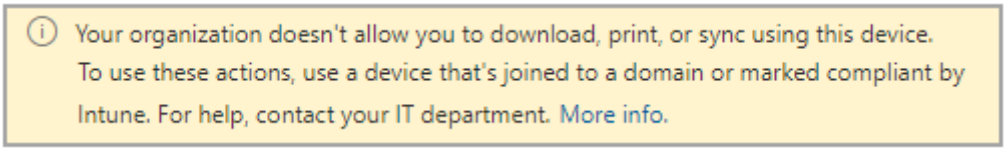
What happens when access is blocked or limited?

Blocking access helps provide security but comes at the cost of usability and productivity. When access is blocked, users see the following error:

> Access Denied. Due to organization policy, you can't access this resource from this untrusted device.



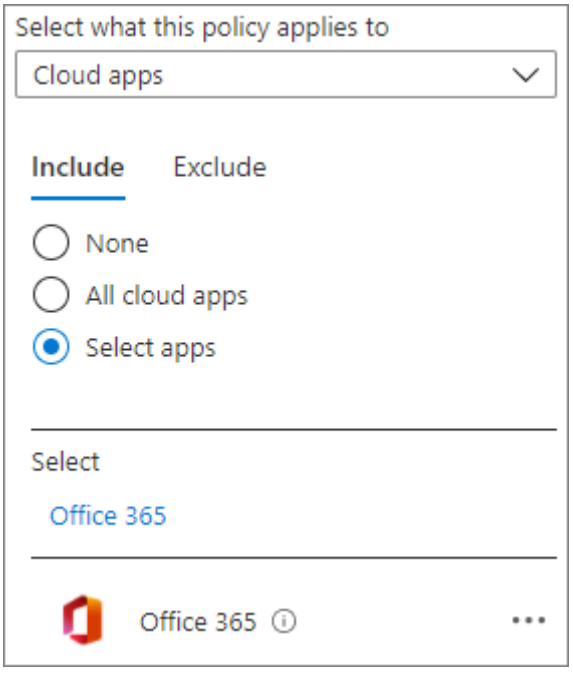
Limiting access allows users to remain productive while addressing the risk of accidental data loss on unmanaged devices. When you limit access, users on managed devices have full access (unless they use one of the browser and operating system combinations listed in Supported browsers). Users on unmanaged devices have browser-only access with no ability to download, print, or sync files. They also won't be able to access content through apps, including the Microsoft Office desktop apps. When you limit access, you can choose to allow or block editing files in the browser. When web access is limited, users see the following message at the top of sites.



> **Note**
>
> - Blocking or limiting access on unmanaged devices relies on Microsoft Entra Conditional Access policies. Learn about Microsoft Entra ID licensing. For an overview of conditional access in Microsoft Entra ID, see Conditional access in Microsoft Entra ID.
> - For info about recommended SharePoint access policies, see Policy recommendations for securing SharePoint sites and files.
> - If you limit access on unmanaged devices, users on managed devices must use one of the supported OS and browser combinations, or they will also have limited access.
> - Because Microsoft Entra ID doesn't offer Multi-Geo Capabilities, blocking or limiting unmanaged devices impact all Geos within the Microsoft 365 tenant.

How do I control device access across Microsoft 365?

The procedures in this article only affect SharePoint access by unmanaged devices. If you want to expand control of unmanaged devices beyond SharePoint, you can Create a Microsoft Entra Conditional Access policy for all apps and services in your organization instead. To configure this policy specifically for Microsoft 365 services, select the **Office 365** cloud app under **Cloud apps or actions**.



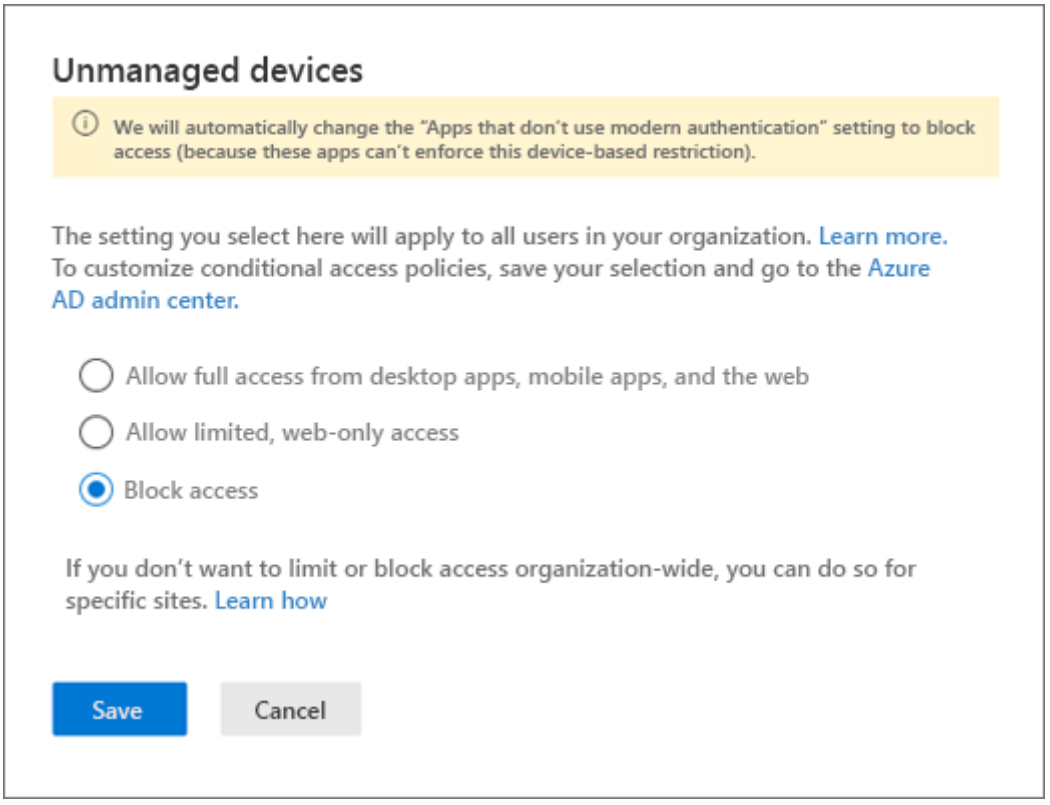
Using a policy that affects all Microsoft 365 services can lead to better security and a better experience for your users. For example, when you block access to unmanaged devices in SharePoint only, users can access the chat in a team with an unmanaged device, but will lose access when they try to access the **Files** tab. Using the Office 365 cloud app helps avoid issues with service dependencies.

How do I block access?

1. Go to **Access control** in the new SharePoint admin center, and sign in with an account that has admin permissions for your organization.

   > **Note**
   >
   > If you have Office 365 operated by 21Vianet (China), sign in to the Microsoft 365 admin center, then browse to the SharePoint admin center and open the Access control page.

2. Select **Unmanaged devices**.



3. Select **Block access**, and then select **Save**.

   > **Important**

- Selecting this option disables any previous conditional access policies you created from this page, and creates a new conditional access policy that applies to all users. Any customizations you made to previous policies won't be carried over.
- It can take up to 24 hours for the policy to take effect. It won't take effect for users who are already signed in from unmanaged devices.
- If you block access from unmanaged devices, we recommend also blocking access from apps that don't use modern authentication. Some third-party apps and versions of Office prior to Office 2013 don't use modern authentication and can't enforce device-based restrictions. This means they allow users to bypass conditional access policies that you configure in Azure. In Access control in the new SharePoint admin center, select **Apps that don't use modern authentication**, select **Block access**, and then select **Save**.

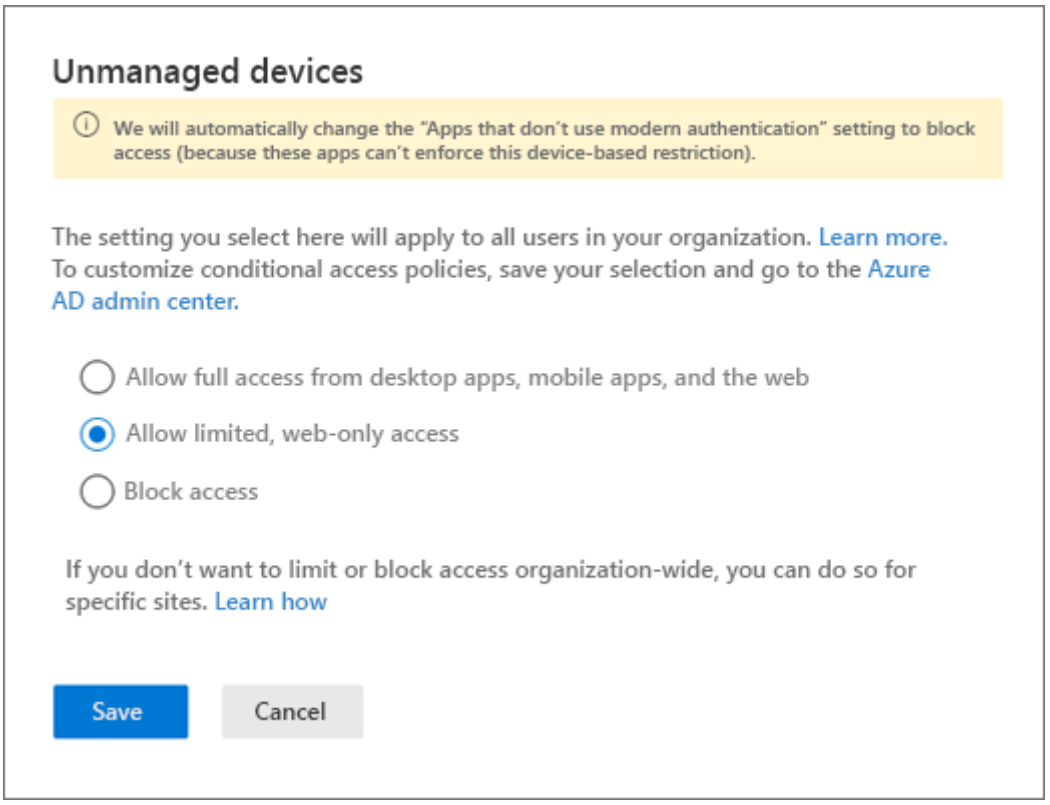
How do I limit access?

1. Go to **Access control** in the new SharePoint admin center, and sign in with an account that has admin permissions for your organization.

   > **Note**
   >
   > If you have Office 365 operated by 21Vianet (China), sign in to the Microsoft 365 admin center, then browse to the SharePoint admin center and select **Policies** to expand, then select **Access Control**.

2. Select **Unmanaged devices**.

3. Select **Allow limited, web-only access**, and then select **Save**. (Note that selecting this option disables any previous conditional access policies you created from this page and create a new conditional access policy that applies to all users. Any customizations you made to previous policies won't be carried over.)



If you revert back to **Allow Full Access**, it could take up to 24 hours for the changes to take effect.

> **Important**
>
> - If you limit access from unmanaged devices, we recommend also blocking access from apps that don't use modern authentication. Some third-party apps and versions of Office prior to Office 2013 don't use modern authentication and can't enforce device-based restrictions. This means they allow users to bypass conditional access policies that you configure in Azure. In Access control in the new SharePoint admin center, select **Apps that don't use modern authentication**, select **Block access**, and then select **Save**.
> - If you limit access and edit a site from an unmanaged device, image web parts won't display images that you upload to the site assets library or directly to the web part. To work around this issue, you can use this SPList API to exempt the block download policy on the site assets library. This allows the web part to download images from the site assets library.
> - When Access Control for Unmanaged Devices in SharePoint is set to **Allow limited, web-only access**, SharePoint files can't be downloaded but they can be previewed. The previews of Office files work in SharePoint but the previews don't work in Microsoft Viva Engage.

How do I limit access using PowerShell?

1. Download the latest SharePoint Online Management Shell.

   > **Note**
   >
   > If you installed a previous version of the SharePoint Online Management Shell, go to **Add or remove programs**, and uninstall **SharePoint Online Management Shell**.

2. Connect to SharePoint with at least the permissions of a SharePoint Administrator in Microsoft 365. To learn how, see Getting started with SharePoint Online Management Shell.

3. Run the following command:

   PowerShell

   ```
   Set-SPOTenant -ConditionalAccessPolicy AllowLimitedAccess
   ```

   > **Note**
   >
   > By default, this policy allows users to view and edit files in their web browser. To change this, see Advanced configurations.

How do I block or limit access to a specific SharePoint site or OneDrive?

To block or limit access to specific sites, follow these steps. If you have configured the organization-wide policy, the site-level setting you specify must be at least as restrictive as the organization-level setting.

1. Manually create a policy in the Microsoft Entra admin center by following the steps in Use app-enforced restrictions.

2. Set the site-level setting by using PowerShell, or a sensitivity label:

   - To use PowerShell, continue to the next step.

   - To use a sensitivity label, see the following instructions and specify the label setting for **Access from unmanaged devices**: Use sensitivity labels to protect content in Microsoft Teams, Microsoft 365 groups, and SharePoint sites.

3. To use PowerShell: Download the latest SharePoint Online Management Shell.

> **Note**
>
> If you installed a previous version of the SharePoint Online Management Shell, go to **Add or remove programs** and uninstall **SharePoint Online Management Shell**.

4. Connect to SharePoint with at least the permissions of a SharePoint Administrator in Microsoft 365. To learn how, see Getting started with SharePoint Online Management Shell.

5. Run one of the following commands.

   To block access to a single site:

   PowerShell
   ```
   Set-SPOSite -Identity https://<SharePoint online URL>/sites/<name of site or OneDrive account> -ConditionalAccessPolicy BlockAccess
   ```

   To limit access to a single site:

   PowerShell
   ```
   Set-SPOSite -Identity https://<SharePoint online URL>/sites/<name of site or OneDrive account> -ConditionalAccessPolicy AllowLimitedAccess
   ```

   To update multiple sites at once, use the following command as an example:

   PowerShell
   ```
   Get-SPOSite -IncludePersonalSite $true -Limit all -Filter "Url -like '-my.sharepoint.com/personal/'" | Set-SPOSite -ConditionalAccessPolicy AllowLimitedAccess
   ```

   This example gets the OneDrive for every user and passes it as an array to Set-SPOSite to limit access.

> **Note**
>
> By default, a setting that includes web access allows users to view and edit files in their web browser. To change this, see Advanced configurations.

What are the advanced configurations for limiting access?

You can use the following parameters with `-ConditionalAccessPolicy AllowLimitedAccess` for both the organization-wide setting and the site-level setting:

`-AllowEditing $false` Prevents users from editing Office files in the browser.

`-ReadOnlyForUnmanagedDevices $true` Makes the entire site read-only for impacted users.

`-LimitedAccessFileType OfficeOnlineFilesOnly` Allows users to preview only Office files in the browser. This option increases security but may be a barrier to user productivity.

`-LimitedAccessFileType WebPreviewableFiles` (default) Allows users to preview Office files in the browser. This option optimizes for user productivity but offers less security for files that aren't Office files. **Warning:** This option is known to cause problems with PDF and image file types because they can be required to be downloaded to the end user's machine to render in the browser. Plan the use of this control carefully. Otherwise, your users could be faced with unexpected "Access Denied" errors.

`-LimitedAccessFileType OtherFiles` Allows users to download files that can't be previewed, such as .zip and .exe. This option offers less security. If this mode is enabled, then for downloading files like .zip or .exe, you can copy the url of the file and paste in browser (example: `https://contoso.sharepoint.com/:u:/r/sites/test/Shared%20Documents/test1.zip`).

The `AllowDownlownloadingNonWebViewableFiles` parameter is no longer supported. Use `LimitedAccessFileType` instead.

People outside the organization will be affected when you use conditional access policies to block or limit access from unmanaged devices. If users have shared items with specific people (who must enter a verification code sent to their email address), you can exempt them from this policy by running the following command.

PowerShell

```
Set-SPOTenant -ApplyAppEnforcedRestrictionsToAdHocRecipients $false
```

> **Note**
>
> "Anyone" links (shareable links that don't require sign-in) aren't affected by these policies. People who have an "Anyone" link to a file or folder will be able to download the item. For all sites where you enable conditional access policies, you should disable "Anyone" links.

How does this affect apps?

Blocking access and blocking download may impact the user experience in some apps, including some Office apps. We recommend that you turn on the policy for some users and test the experience with the apps used in your organization. In Office, make sure to check the behavior in Power Apps and Power Automate when your policy is on.

> **Note**
>
> Apps that run in "app-only" mode in the service, like antivirus apps and search crawlers, are exempted from the policy.
>
> If you're using classic SharePoint site templates, site images may not render correctly. This is because the policy prevents the original image files from being downloaded to the browser.
>
> For new tenants, apps using an ACS app-only access token is disabled by default. We recommend using the Microsoft Entra ID app-only model which is modern and more secure. But you can change the behavior by running `set-spotenant -DisableCustomAppAuthentication $false` (needs the latest SharePoint admin PowerShell).

Need more help?

SharePoint Q&A

See also

Policy recommendations for securing SharePoint sites and files

Control access to SharePoint and OneDrive data based on defined network locations

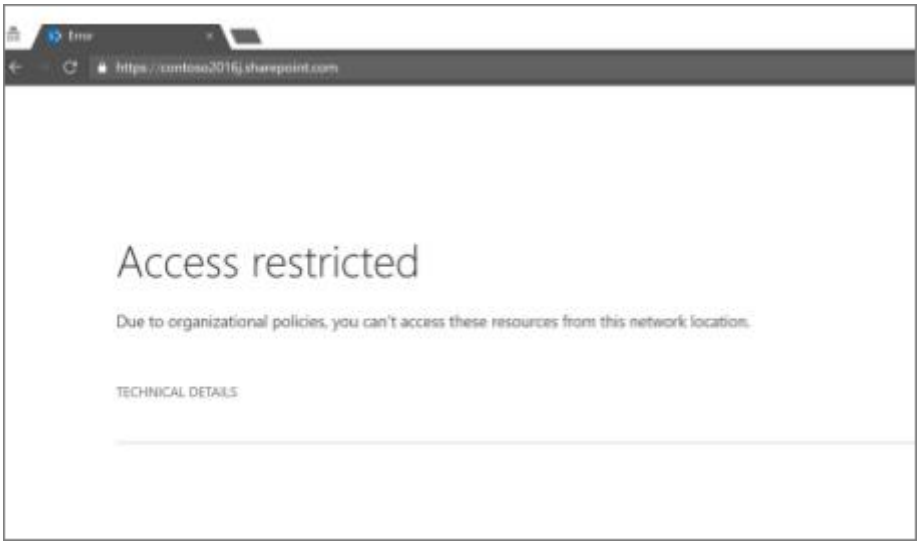
---

Last updated on 01/26/2026

Control access to SharePoint and OneDrive data based on network location

As an IT admin, you can control access to SharePoint and OneDrive resources in Microsoft 365 based on defined network locations that you trust. This is also known as a location-based policy.

To do this, you define a trusted network boundary by specifying one or more authorized IP address ranges. Any user who attempts to access SharePoint and OneDrive from outside this network boundary (using a web browser, desktop app, or mobile app on any device) is blocked.



What should I consider before setting a location-based policy?

Here are some important considerations for setting a location-based policy:

- **External sharing**: If you share files and folders with guests who authenticate, they can't access the resources outside of the defined IP address range.
- **Access from first and third-party apps**: Normally, you can access a SharePoint document from apps like Exchange, Viva Engage, Skype, Teams, Planner, Power Automate, PowerBI, Power Apps, OneNote, and so on. When you enable a location-based policy, apps that don't support location-based policies are blocked. The only apps that currently support location-based policies are Teams, Viva Engage, and Exchange. This means that all other apps are blocked, even when these apps are hosted within the trusted network boundary. This is because SharePoint can't determine whether a user of these apps is within the trusted boundary.

> **Note**
>
> We recommend that when you enable a location-based policy for SharePoint, you configure the same policy and IP address ranges for Exchange and Viva Engage. SharePoint relies on these services to enforce that the users of these apps are within the trusted IP range. For protecting access to SharePoint via the Office.com portal, we recommend using the Microsoft Entra Conditional Access policy for "Office 365" and configuring the trusted IP range there.

- **Access from dynamic IP ranges**: Several services and providers host apps which have dynamic originating IP addresses. For example, a service that accesses SharePoint while running from one Azure data center might start running from a different data center due to a failover condition or other reason, thus dynamically changing its IP address. The location-based conditional access policy relies on fixed, trusted IP address ranges. If you can't determine the IP address range up front, location-based policy might not be an option for your environment.

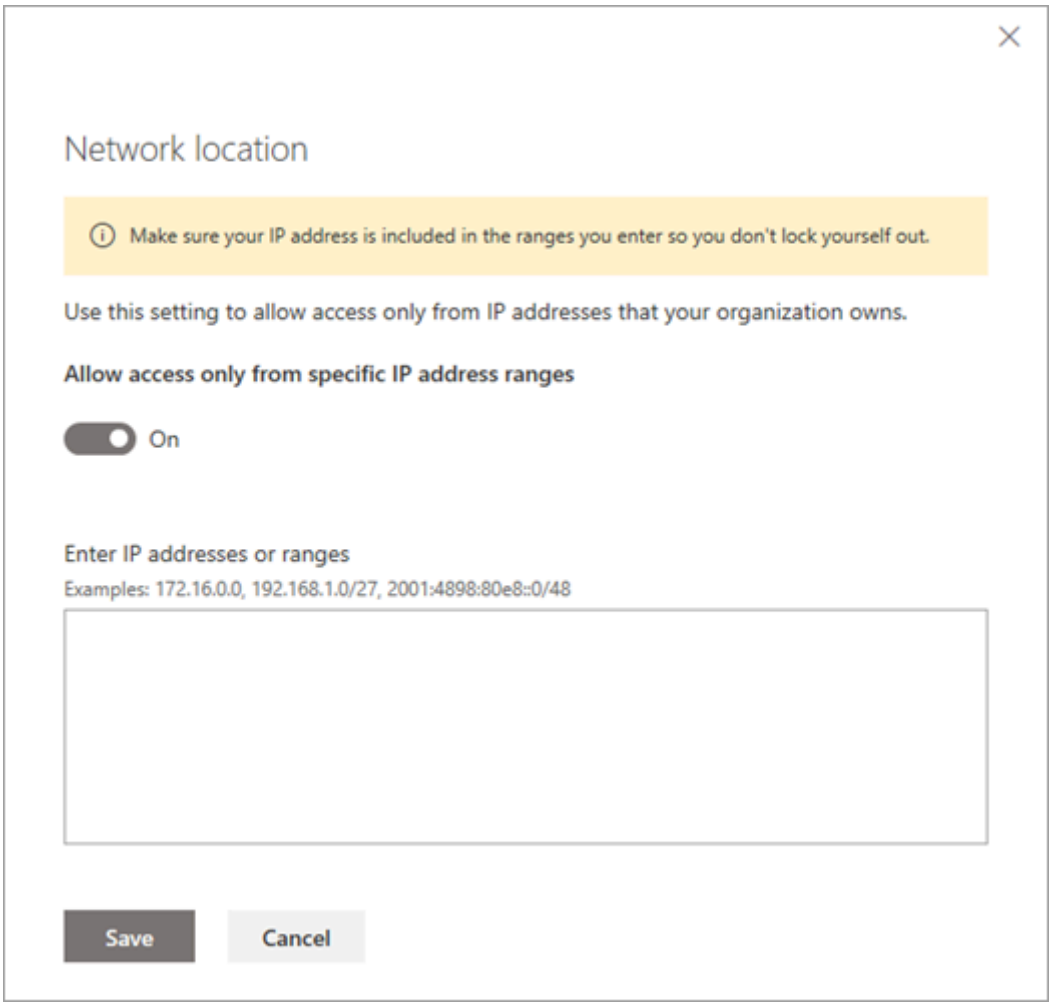
How do I set a location-based policy in the SharePoint admin center?

> **Note**
>
> It can take up to 15 minutes for these settings to take effect.

1. Go to **Access control** in the new SharePoint admin center, and sign in with an account that has admin permissions for your organization.

> **Note**
>
> If you have Office 365 operated by 21Vianet (China), sign in to the Microsoft 365 admin center, then browse to the SharePoint admin center and open the Access control page.

2. Select **Network location**, and turn on **Allow access only from specific IP address ranges**.



3. Enter IP addresses and address ranges separated by commas.

> **Important**
>
> Make sure you include your own IP address so you don't lock yourself out. This setting not only restricts access to OneDrive and SharePoint sites, but also to the OneDrive and SharePoint admin centers, and to running PowerShell cmdlets. If you lock yourself out and can't connect from an IP address within a range you specified, you will need to contact Support for help.
> If you save overlapping IP addresses, your users will see a generic error message with a correlation ID that points to "The input IP allow list has overlaps."

> **Note**
>
> To set a location-based policy by using PowerShell, run Set-SPOTenant with the -IPAddressAllowList parameter. For more info, see Set-SPOTenant.

Last updated on 12/22/2025

Enable conditional access support in the OneDrive sync app

Conditional access control capabilities in Microsoft Entra ID offer simple ways for you to secure resources in the cloud. The new OneDrive sync app works with the conditional access control policies to ensure syncing is only done with compliant devices. For example, you might require sync to be available only on domain-joined devices or devices that meet compliance as defined by the Mobile Device Management system (like Intune).

For information about how conditional access works, see:

- Microsoft Entra Conditional Access
- Require managed devices for cloud app access with conditional access
- Configure Microsoft Entra hybrid join for managed domains
- Control access from unmanaged devices

Recommendations for Windows

We recommend using this feature on Windows together with silent account configuration for the best experience. The OneDrive sync app supports both device-based and location-based conditional access policies.

Known issues

The following are known issues with this release:

- If you create a new access policy after the device has authenticated, it may take up to 24 hours for the policy to take effect.
- In some cases, the user may be prompted for credentials twice. We're working on a fix for this issue.
- Certain AD FS configurations may require additional setup to work with this release. Run the following command on your AD FS server to ensure FormsAuthentication is added to the list of PrimaryIntranetAuthenticationProvider:

  ```
  Set-AdfsGlobalAuthenticationPolicy -PrimaryIntranetAuthenticationProvider
  @('WindowsAuthentication', 'FormsAuthentication')
  ```

- If you enable location-based conditional access, users get a prompt about every 90 to 120 minutes by default when they leave the set of approved IP address ranges. The exact timing depends on the access token expiry duration (60 minutes by default), when their computer last obtained a new access token, and any specific conditional access timeouts put in place.

Last updated on 01/26/2026

Block the download of Teams meeting recording files from SharePoint or OneDrive

Article • 09/18/2024

Some features in this article require Microsoft Syntex - SharePoint Advanced Management

As an admin, you can block the download of Teams meeting recording and transcript files from SharePoint or OneDrive. Blocking the download of Teams meeting recording and transcript files allows users to remain productive while addressing the risk of accidental data loss. Users have browser-only access to play the meeting recordings or view transcripts with no ability to download or sync files or access them through apps.

This org-wide policy applies to new meeting recordings and transcripts across your entire organization. When the policy is on, any new Teams meeting recording and transcript files saved in SharePoint and OneDrive are blocked from download. You can exempt people who are members of specified security groups from the policy. Exempting specific security group members allows you to specify governance or compliance specialists who should have download access to meeting recordings and transcripts.

Because this policy affects meeting recordings stored in OneDrive and SharePoint, you must be a SharePoint Administrator to configure it. To learn more about meeting recording in OneDrive and SharePoint, see Teams meeting recording storage and permissions in OneDrive and SharePoint. To learn more about how your users use transcripts, see View live transcription in Microsoft Teams meetings.

This policy doesn't apply to manually uploaded meeting recording and transcript files.

> **Important**
>
> This feature doesn't prevent the download of files that were uploaded by Teams prior to turning the policy on. If you would like to prevent download of these files, you can open a support ticket.

Prerequisites

- You must have a Microsoft Syntex - SharePoint Advanced Management license.

Turn on the policy for your organization

Open the SharePoint Online Management Shell and connect to SharePoint as a SharePoint Administrator. To learn how, see Get started with SharePoint Online Management Shell.

Run the following command:

```
PowerShell

Set-SPOTenant -BlockDownloadFileTypePolicy <$true/$false(default)>  -
BlockDownloadFileTypeIds  TeamsMeetingRecording
```

To block the download of Teams meeting recording files from SharePoint or OneDrive, run this script:

```
PowerShell

Set-SPOTenant -BlockDownloadFileTypePolicy $true  -BlockDownloadFileTypeIds
TeamsMeetingRecording
```

Exempt users in specified security groups from the policy

The `-ExcludedBlockDownloadGroupIds` parameter exempts users in the specified security groups from this policy so that they can download meeting recording and transcript files.

To allow users in specified security groups to download meeting and recording files, use the following script:

```
-ExcludedBlockDownloadGroupIds <comma separated security group IDs>
```

App effect

Blocking the download of Teams meeting recording and transcript files might affect the user experience in some apps, including some Office apps. We recommend that you enable the policy for some users and test the experience with the apps used in your organization.

> ⓘ **Note**

Apps that run in "app-only" mode, like antivirus apps and search crawlers, are exempted from the policy.

Need more help?

- SharePoint Q&A

Related topics

- Block download policy for SharePoint sites and OneDrive
- Policy recommendations for securing SharePoint sites and files
- Admins- Manage transcription and captions for Teams meetings
- Use OneDrive and SharePoint for meeting recordings
- Teams meeting recording

Feedback

Was this page helpful? Yes No

Provide product feedback

Sign out inactive users

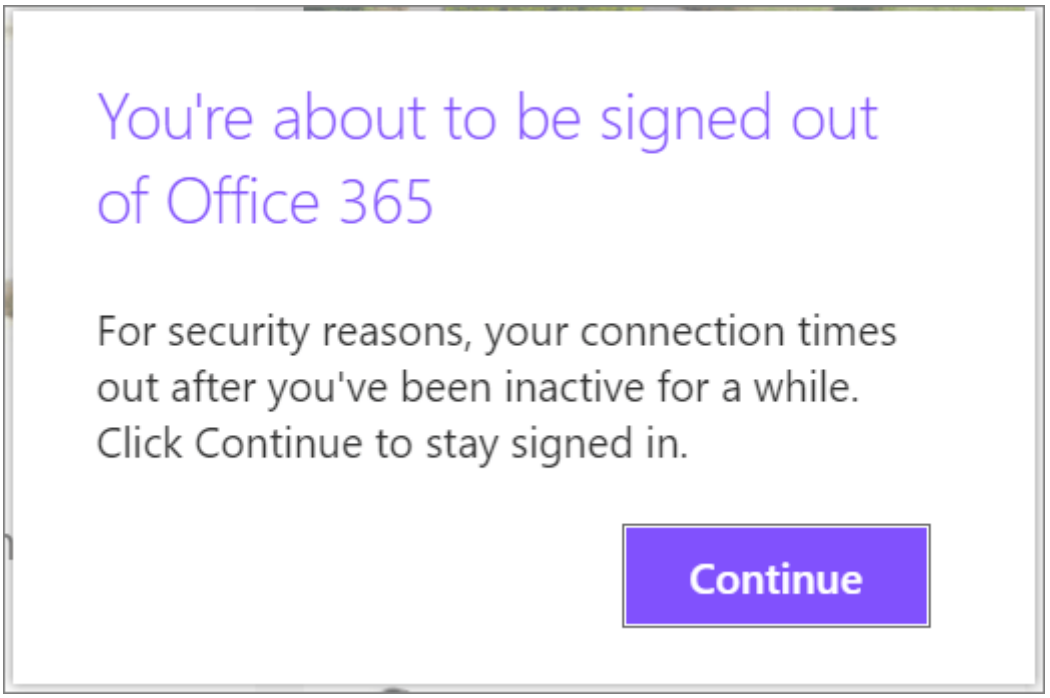
This article is for SharePoint Administrators or above in Microsoft 365 who want to control user access to SharePoint and OneDrive data on unmanaged devices. Idle session sign-out lets you specify a time at which users are warned and are later signed out of Microsoft 365 after a period of browser inactivity in SharePoint and OneDrive.

> **Note**
>
> - Idle session sign-out applies to the entire organization and can't be set for specific sites or users. To target different settings for different users, use Microsoft Entra Conditional Access policies instead (and see the next important note about the Microsoft Entra ID P1 or P2 requirement).
> - This feature relies on Microsoft Entra Conditional Access policies being available. You need a Microsoft Entra ID P1 or P2 subscription for this to work. For more info about this, refer to the Microsoft Entra licensing.

Idle session sign-out is one of many policies you can use with SharePoint and OneDrive to balance security and user productivity and help keep your data safe irrespective of where users access the data from, what device they're working on, and how secure their network connection is. For more ways to control access in SharePoint and OneDrive, see How SharePoint and OneDrive safeguard your data in the cloud.

The idle session sign-out experience

When a user is inactive in SharePoint and OneDrive for the time period you specify, the following message appears:



> **Note**
>
> Activity is counted as requests sent to SharePoint, such as mouse clicks on a UI element like a button, list entry, or a link. Moving the mouse and scrolling aren't counted as activity.

If users don't select **Continue**, they're automatically signed out, and the following message appears.

> **Note**
>
> If a user is active in another Microsoft 365 service (such as Outlook), but inactive in SharePoint and OneDrive, they're signed out across Microsoft 365. If a user has multiple tabs to OneDrive and SharePoint sites open at the same time, they won't be signed out unless they're inactive on all the sites. Users won't be signed out if they selected to stay signed in when they signed in. For info about hiding this option, see Add company branding to your sign-in page in Microsoft Entra ID. Users won't be signed out on a managed device (one that is compliant or joined to a domain), unless they're using

inPrivate mode or a browser other than Microsoft Edge or Internet Explorer. If they use Google Chrome, you need to use an extension to pass the device state claim. For more info about device state claims, see Microsoft Entra Conditional Access settings.

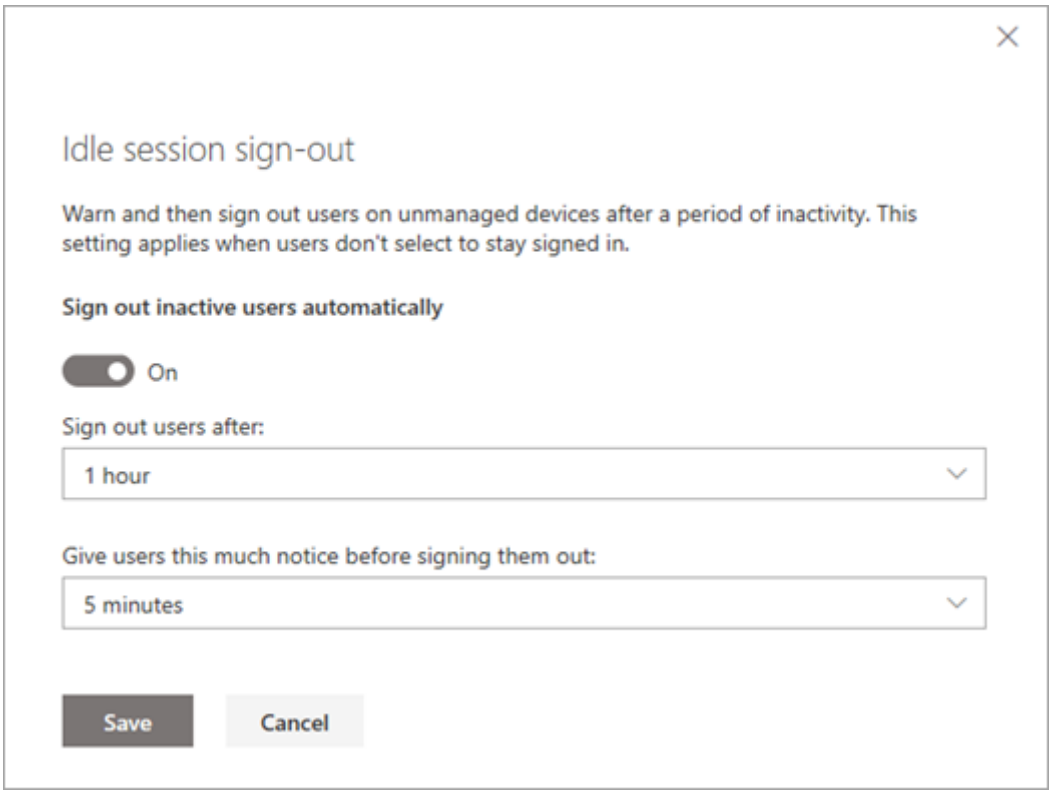
> **Important**
>
> Microsoft 365 apps and services won't support Internet Explorer 11 starting August 17, 2021 (Microsoft Teams won't support Internet Explorer 11 earlier, starting November 30, 2020). Learn more. Please note that Internet Explorer 11 will remain a supported browser. Internet Explorer 11 is a component of the Windows operating system and follows the Lifecycle Policy for the product on which it's installed.

Specify idle session sign-out settings in the new SharePoint admin center

1. Go to **Access control** in the SharePoint admin center, and sign in with an account that has admin permissions for your organization.

   > **Note**
   >
   > If you have Office 365 operated by 21Vianet (China), sign in to the Microsoft 365 admin center, then browse to the SharePoint admin center and open the Access control page.

2. Select **Idle session sign-out**.



3. Turn on **Sign out inactive users automatically**, and then select when you want to sign out users and how much notice you want to give them before signing them out.

4. Select **Save**.

Specify idle session sign-out settings by using PowerShell

1. Download the latest SharePoint Online Management Shell.

> **Note**
>
> If you installed a previous version of the SharePoint Online Management Shell, go to Add or remove programs and uninstall "SharePoint Online Management Shell."
> On the Download Center page, select your language and then select the Download button. You'll be asked to choose between downloading a x64 and x86 .msi file. Download the x64 file if you're running the 64-bit version of Windows or the x86 file if you're running the 32-bit version. If you don't know, see Which version of Windows operating system am I running? After the file downloads, run it and follow the steps in the Setup Wizard.

2. Connect to SharePoint as a SharePoint Administrator or above in Microsoft 365. To learn how, see Getting started with SharePoint Online Management Shell.

3. Run the following command:

```
PowerShell
Set-SPOBrowserIdleSignOut -Enabled $true -WarnAfter (New-TimeSpan -Seconds
2700) -SignOutAfter (New-TimeSpan -Seconds 3600)
```

Where:

- **-Enabled** specifies whether idle session sign-out is enabled or disabled by using **$true** or **$false**.
- **-WarnAfter** specifies the amount of after which a user is notified that they'll be signed out after a period of inactivity as a **New-TimeSpan** which can be configured in seconds, minutes, or hours.
- **-SignOutAfter** specifies the amount of time after which is a user is signed out of Microsoft 365 if they don't respond to the **-WarnAfter** prompt.

> **Note**
>
> You must specify values for both **WarnAfter** and **SignOutAfter**. The **SignOutAfter** must be greater than the **WarnAfter** value.
>
> It takes about 15 minutes for the policy to take effect across your organization. The policy doesn't affect existing sessions. To view the idle session sign-out values you've set, use **Get-SPOBrowserIdleSignOut**.
>
> For info about Microsoft 365 session lengths (regardless of activity), see Session timeouts for Microsoft 365.

Last updated on 01/26/2026

Version history overview

The Version History feature is an integral part of Microsoft's 365 built-in data protection in SharePoint and OneDrive. An item or file's version history lets a user see or restore to a previous version, helpful for undoing unintended changes, whether accidental or due to malicious activities like ransomware. It also ensures auditability to meet an organization's legal and audit requirements.

Users can use version history to:

- **View a previous version**: Users can view a previous version without overwriting their current version. During a review of the version history within a Microsoft Office document, such as a Word or Excel file, versions can be compared to determine what the differences are.
- **Restore to a previous version**: If a user makes a mistake in a current version, the current version gets corrupted, or if they simply like a previous version better, they can replace the current version with a previous one. The restored version becomes the new current version. Learn more Restore a previous version of an item or file in SharePoint.
- **Track history of a file or item**: Users can use version history to see when a file or an item was changed and identify who made the changes.

Last updated on 06/25/2026

Overview of version history limits for document libraries and OneDrive

Article • 04/10/2025

Version history limits control how versions are stored in a SharePoint document library or OneDrive account. Limits can be set at organization, site, library or OneDrive user account level allowing admins and site owners the ability to better manage content recovery and auditing requirements. Global and SharePoint admins in Microsoft 365 can set version history limits at the organization level. These settings apply universally to all new libraries, whether on existing or new SharePoint sites, and on default libraries on new OneDrive sites. Site owners can overwrite organization-level version settings by configuring version settings for sites they own. Site owners can overwrite organization or site settings by configuring version settings for libraries and lists they own.

The following table summarizes the various ways of managing version history limits on your document libraries:

Expand table

Area	How does it work?
Set default organization version history limits	Default organization version history limits are set on all new document libraries created across existing and new SPO sites.
Set site or library level version history limits	If needed, site admins can break inheritance from the default organization limits for an individual site or library.
Report on version storage on a site	Run a report to analyze version storage use of existing versions, understand how a version limit works before configuring limits, or analyze the impact of trimming existing versions before scheduling trim job.
Trim existing versions	Site admins can choose to trim existing versions by queuing a timer job to execute the trimming.

How Version history limits are applied

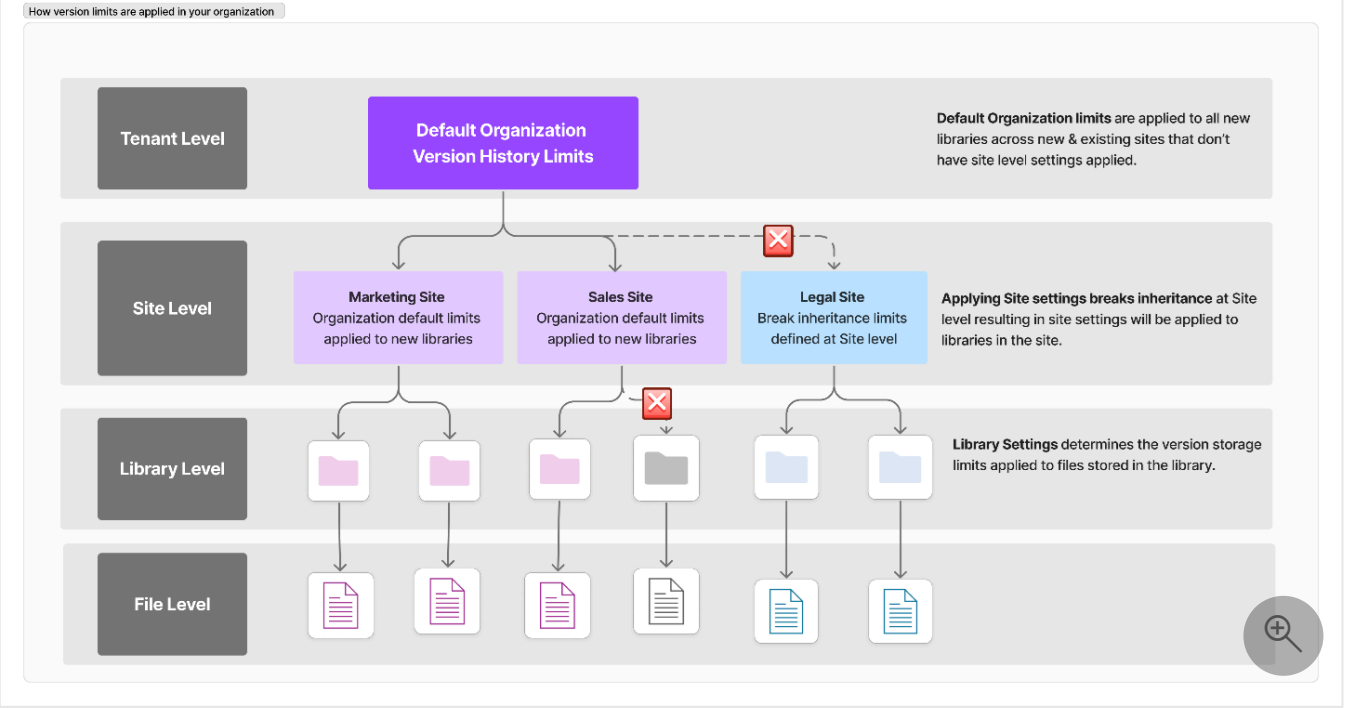
Version history limits are applied in the following ways:

- **Default organization limits:** Organization default settings are applied to all new libraries created on sites that don't have site level settings configured.
- **Site limits:** It is possible to break inheritance for a site by configuring version history limits for the site. When version limits are configured on a site, the settings are applied to all

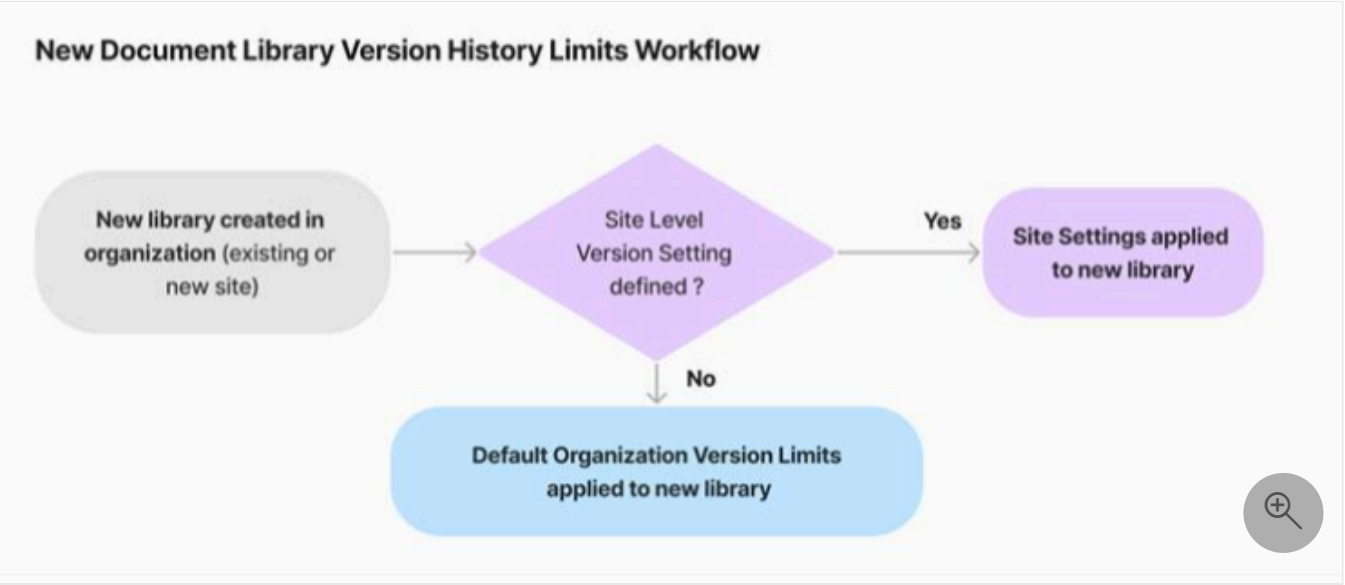
new libraries created on the site.

- **Library limits:** It is possible to break inheritance at library level to define version limits for files stored in the library.

In the following example, default organization limits are applied to new libraries created on marketing and sales sites as these sites do not have site level limits applied. Legal site has site level limits applied and broken inheritance from the organization defaults. Libraries created in the legal site follow the limits applied at the legal site level.



The following figure shows the workflow of applying a version limit on new document libraries. When a new library is created, site level setting check is performed. If no site setting is defined, the organization default setting is applied to new libraries.



Types of version limits

There are two version history settings that admins can use to configure version limits for all new libraries created in their organization:

Automatic setting

Automatic setting is recommended for optimized version storage. It combines the data recovery benefits that version history offers while optimizing for its storage. For admins, this setting offers the most optimal storage option without having to estimate the version count or age limits needed to meet the diversified need of their end users.
For more information, see version storage under automatic limits.

Manual setting

The manual setting allows admins to set count limits on the number of major versions or to set expiration and count limits. When this option is selected, the admins can configure it in the following ways.

- **Major version limit with expiration period**: Versions are deleted after exceeding either the set number of major versions or after the set period of time. For example, if you configure a library to store 500 major versions with a 365-day expiration, the system stores no more than 500 versions, and automatically deletes any version older than 365 days.

- **Major version limits with no expiration period**: Versions are deleted after they exceed the set number of major versions. For example, if a library is configured to store 500 major versions, no more than 500 versions is stored for each file or item.

  For more information, see determining the right count or expiration version limits.

> **Note**
>
> - The UI doesn't allow a value less than 100 major versions or less than 30 days expiration time limits to be set, but it's possible to set the system to store fewer versions using public APIs. For reliability, any value less than 100 versions or less than 30 days expiration time limit isn't recommended and can result in the user activity causing an inadvertent data loss.
>
> - If time version history limits are configured on a library, the file version expiration date is stamped on a version at creation time. The expiration date set on a file version is determined from the SnapshotDate of the version which is the date a

version became a historical version. The SnapshotDate might be estimated if the version was snapshotted before January 1, 2023.

Version storage behavior

Version storage in SharePoint is determined by several factors including limits configured on a library, user deletion activity, or retention policies. The following table enumerates the various scenarios and expected version storage behavior:

The following table enumerates the scenarios and the expected version storage behavior:

Expand table

Scenario	Version Trimming Behavior
User deletes versions from the version history of a file.	When a user deletes a version from the version history of a file, the deleted version is moved to the site's recycle bin and can be recovered for a period. For more information, see Restore items in the recycle bin that were deleted from SharePoint or Teams.
Versions exceed settings applied on the document library.	When versions exceed the limits set at the library, versions matching the criteria are marked for permanent deletion. This version deletion workflow bypasses the normal recycle bin and the deleted versions can't be recovered from recycle bin.
Timer job scheduled to trim existing versions on a library or site.	Versions deleted using scheduled jobs are permanently deleted. This version deletion workflow bypasses the normal recycle bin and deleted versions can't be recovered from recycle bin.
Version storage on items that are subject to retention policy or on an eDiscovery hold.	For items that are subject to a retention policy (or an eDiscovery hold), the versioning limits for the document library are ignored. This exemption continues until the retention period of the document is reached (or the eDiscovery hold is released). For more information, see How retention works with document versions.
Timer job scheduled to trim existing versions on a library or site encounters versions that are subject to retention policy or on an eDiscovery hold.	When a trim job encounters a version under a retention policy or an eDiscovery hold, it will stamp an expiration date on the version instead of deleting it. Once the expiration date is reached: 1) if the retention policy or eDiscovery hold is still in effect for the version, the expiration date is extended; or 2) if the retention policy or eDiscovery hold has been lifted for the version, the version is deleted.
Trimming existing versions on sites that are Read Only (locked sites).	Trimming of expired versions on sites that are under retention or are on hold is suspended until the site is unlocked.

Scenario	Version Trimming Behavior
Versions deletion on items with retention labels applied.	Versioning limits are honored on items with retention labels when the content isn't subject to a retention policy (or an eDiscovery hold). Versions matching the limit criteria are automatically deleted to accommodate new versions, but users are still prevented from deleting versions.
Version deletion on items marked as records.	Version deletion on documents marked as records is blocked. For more information, see Use record versioning in SharePoint or OneDrive.

Auditing versioning events

Audit events are available on the Microsoft Purview portal to help you monitor version history activities. Audit events are logged for the following activities:

- Changes made to organization version history limits.
- Changes made to site version history limits.
- Changes made to library version history limits.
- User queues a job to generate a version storage usage report.
- User queues a job to update the version history limits on all libraries of a site.
- User queues a job to bulk delete version history of files on a library or site.
- User deletes versions from the version history of a file.
- Versions deleted when expired or bulk deleted.

Plan version storage on document libraries

Article • 05/29/2025

The Version history limits you configure need to meet your organization's recovery objectives. In the following sections, we call out the options and decisions that you as an administrator should consider when setting up version limits for your organization.

As you plan your version storage strategy, consider these key decision areas:

- Determine the default new document library version history limit for your organization.
- Identify any exceptions needed from the organization default limits.
- Determine if current content should be updated to align with the default organization version history limits.

Determine default version limits for new document libraries in your organization

To set appropriate default limits for your organization, assess the restore options and storage consumption associated with the three version storage modes offered by SharePoint. This helps you to evaluate how the default limits could affect your users' access to their document versions and the overall storage space utilized by those versions.

Expand table

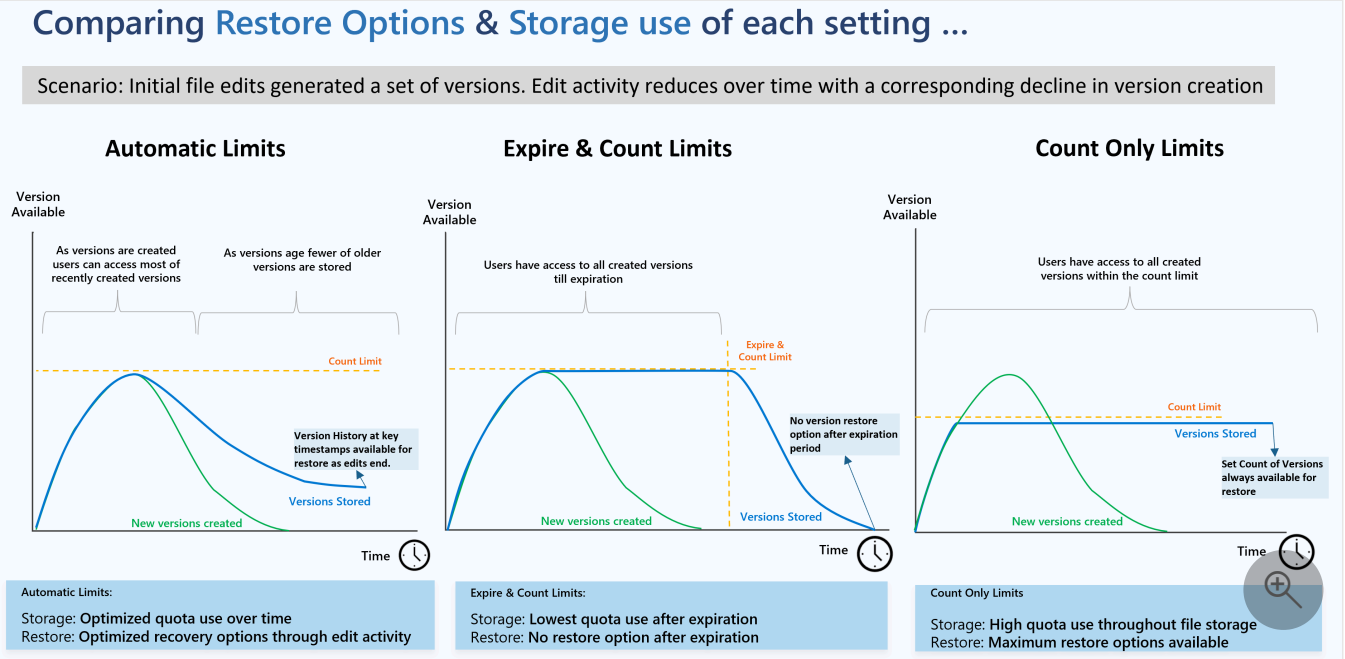
Select this option:	If you want to:	Benefits
Automatic (Recommended)	Automatically optimize storage by storing versions based on their creation date. With this setting, users have access to most of the recently created versions. As versions age, fewer older versions are stored. No other input is required from admins.	**Storage use:** Automatic setting is the recommended setting that offers your users access to high value versions while optimizing version storage use. **Restore options:** This setting ensures version history at key timestamps is always available for restore even on file with no new file edits.
Manual with Major Version Limit and Expiration Period set	Store versions only until the configured expiration period and within the configured major versions count limits. With this setting, users have access to all versions within	**Storage use:** This setting is the best option for ensuring the lowest quota impact from version storage as it trims versions that are older than the configured expiration. **Restore options:** When an expiration limit is set, it's possible for files with no recent edits to have all

Select this option:	If you want to:	Benefits
	the count and expiration period.	their versions trimmed if the updated version policy dictates that. For example, if a file doesn't get edited in six months and a six-month version expiration policy is in place, then all that file's versions are deleted.
Manual with **Major Version Limits and No Time** set	Always store the configured count of versions regardless of version age. Users have access to all the versions within the count limit.	**Storage use:** This setting can lead to high quota consumption from versions if you have a high ratio of heavily edited files or if you set the limits too high. **Restore options:** This setting is the best option for storing a set number of versions offering you predictable version storage behavior.

Tip

- Before updating your default limits, consider running a 'What-if' analysis report on a site or library to understand the impact on version storage of either automatic or manual limits.
- Provide information about default organization version history limits to your users. Tell site owners if you have a process and policy for requesting more.

The following image depicts the restore options and the storage use for each setting:

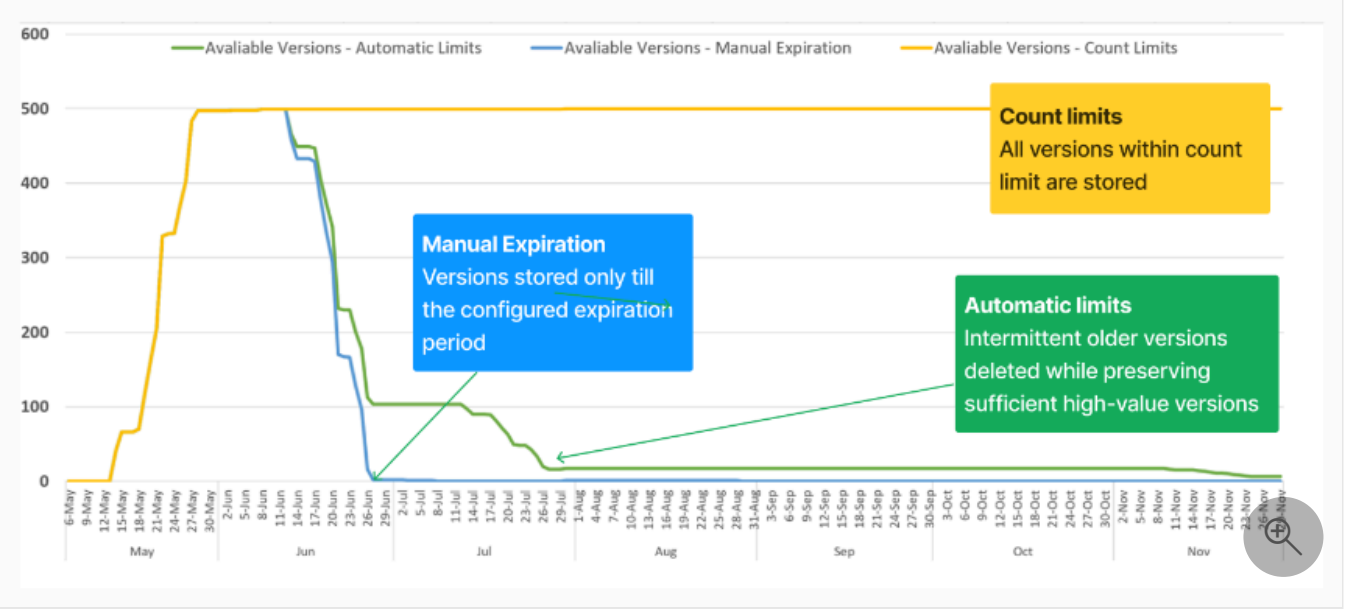


Example Scenario

Take an example of a file where 500 versions were created in May, June, and July. Let's compare the versions available under each version limits:

- **Manual limits: 500 major versions with expiration of 60 days:** No more than 500 versions are stored and any version older than 60 days are also deleted. On this file, all versions are eventually deleted as the versions age.
- **Manual limits: 500 major versions with no limits:** All versions within the count limit of 500 continue to be stored.
- **Automatic limits: Under automatic settings** intermittent older versions are trimmed over time, resulting in 96% version storage reduction in six months period compared to count limits. Users always have access to a set of versions even when there's no new file edit activity.

Version Creation		Versions Available		
Date	Versions Created	Manual Expiration limit	Count Limit	Automatic Limits
May	497	497	497	497
Jun	499	499	499	499
Jul	500	2	500	103
Aug		1	500	17
Sep		0	500	17
Oct		0	500	17
Nov		0	500	17



Understand Version storage under Automatic limits

The algorithm behind automatic version history limits is based on the design principle that restores value of a version degrades as the version ages. When Automatic limit is selected, SharePoint deletes (thins out) intermittent older versions that are least likely to be used, while

preserving sufficient high-value versions. In case restores are required, it ensures that users have access to more versions in the recent past and fewer farther back in time.

Version storage under Automatic setting is determined by the following algorithm:

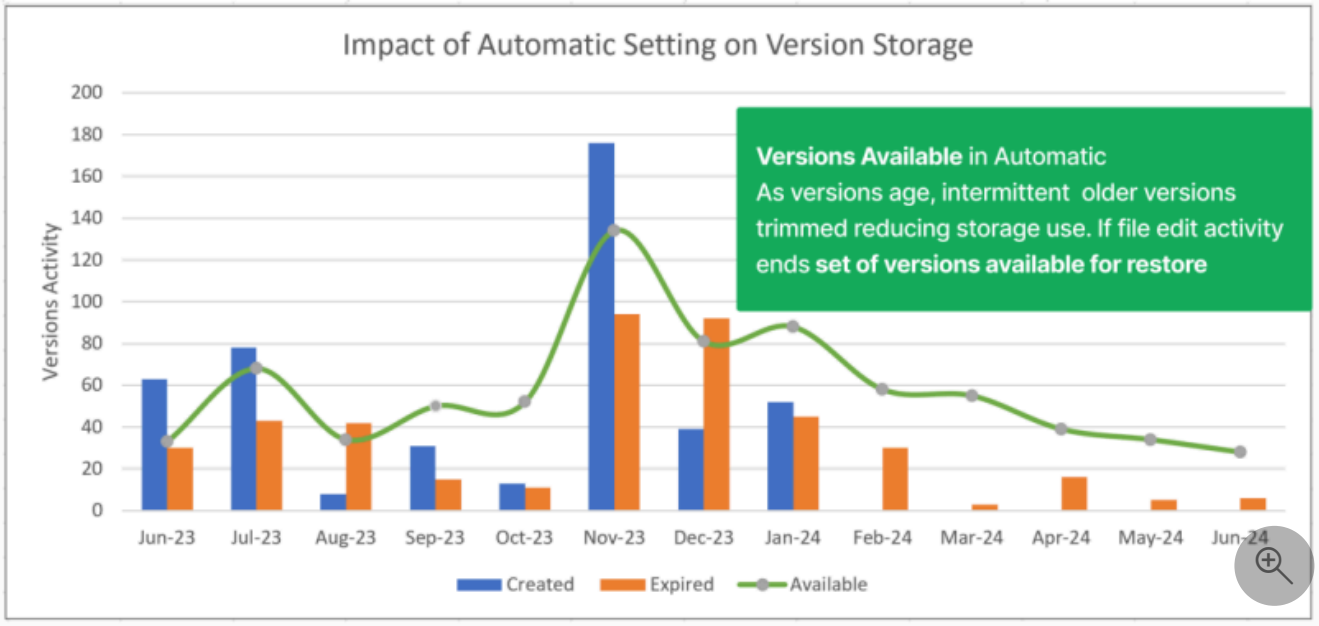
As versions are created, users have access to the following versions:

- All versions created within 500 count limit in first 30 days.
- Hourly versions (versions created at the top of the hour) between 30 to 60 day period.
- Daily versions (versions created at the beginning of each day) between 60 to 180 day period.
- Weekly versions (versions created at the beginning of the week) beyond 180 days or more are available indefinitely until the maximum 500 count limit has reached.

The service trims the intermediate versions as the above milestones are reached.

Take an example of file with a consistent version creation pattern between the months of June until January. Under Automatic setting, intermittent versions are purged as the versions age resulting in ~94% reduction in version storage used compared to applying count limits only.

	Version Activity		
Date	Created	Expired	Available
Jun-23	63	30	33
Jul-23	78	43	68
Aug-23	8	42	34
Sep-23	31	15	50
Oct-23	13	11	52
Nov-23	176	94	134
Dec-23	39	92	81
Jan-24	52	45	88
Feb-24		30	58
Mar-24		3	55
Apr-24		16	39
May-24		5	34
Jun-24		6	28
Totals	**460**	**432**	**28**



Determine right Count or Expiration version limits

In considering which limits to set, we recommend a balanced approach:

- Setting count limits too high or setting expiration limits for longer duration or never expiring, stores most versions created, offering users most of versions to restore from. However, a high proportion of actively edited files can result in versions using a high storage.
- Setting count or expiration limits that are too low can result in data loss due to unrecoverable changes impacting your user's ability to undo unwanted changes, and other recovery scenarios.

Identify any exceptions needed from organization defaults

Since default organization settings are applied to all new document libraries created in your organization, you may need to set distinct version history limits on individual SharePoint Sites, OneDrive user accounts, or individual document libraries to meet business requirements.

When diverging from the default limits, we recommend limiting the exceptions to maintain consistency with your organization's version storage practices and to keep your version storage policies in sync. For instance, evaluate if your business requirements can be met by breaking inheritance on a few document libraries instead of applying changes broadly across the entire site.

Decide if updates to organization version history limits will be applied to existing content

When updating your organization's version limits, consider how existing library settings and file versions should be updated. Avoid impacting existing content by applying the organization limits to new libraries only or align your existing content to organization version limits by updating current library settings and trimming file versions.

Expand table

If you want to	Steps to follow
Apply organization defaults to new libraries only:	Update default organization version limit new libraries to apply the new limits to all new libraries created in your organization without impacting existing content, including current limits set on existing libraries or existing file versions.
Apply organization defaults to new libraries, update settings on existing libraries but do not trim existing versions:	Follow these steps to manage new file versions created on new and existing libraries without impacting any existing file versions: 1. Update default organization version limit to apply the new limits to all new libraries created in your organization. 2. Update the limits on existing document libraries on each site without breaking inheritance to allow new document libraries created in the site to inherit the organization level version history limits.
Apply organization defaults to new libraries, update the settings on existing libraries, and trim existing file versions:	Follow these steps to fully align new and existing libraries and file versions to organization limits: 1. Update default organization version limit to apply the new limits to all new libraries created in your organization. 2. Update the limits on existing document libraries on each site

If you want to	Steps to follow
	without breaking inheritance to allow new document libraries created in the site to inherit the organization level version history limits. 3. Trim existing versions on each site by queuing a job to permanently delete existing versions.

File Type Version Limits

SharePoint supports file-type–specific version history limits. It gives organizations finer control over how versions are retained by allowing certain file types to use different version limits than the default library settings.

The extension of a file determines its file type. Today, the following file-type categories are supported:

Expand table

Name (case-insensitive)	Description	Extensions
audio	Audio files	au, flac, m4a, mp3, ogg, wav, wma, aac, m4b, m4p
video	Video files	mts, m2ts, ts, 3g2, 3gp, 3gp2, 3gpp, asf, wmv, avi, m4v, mov, mp4, mp4v, webm, movie, mkv, mpg, flv, mpeg
outlookpst	Outlook Data File	pst

When you configure a file-type–specific version history limit on a document library, that limit replaces the library's default version history settings for that file type. Versions of the specified file type follow only the file-type version history limit.

Example

Suppose your document library uses an automatic version history limit that applies to all files. You notice that audio files are consuming more storage than expected. To address the storage issue, you want a stricter version limits for audio files and keep the existing automatic limit for all other files.

To implement the version limits, you configure a file-type override that sets a 30-day manual expiration period and a maximum of 100 major versions for audio files. After this change:

- New versions of **audio** files follow the file-type–specific manual limits.
- New versions of **other** file types continue using the library's automatic limit unchanged.

> **Note**
>
> Today, OutlookPST files use a manual limit that keeps 30 major versions and no expiration by default.

Learn More

For more information, check out the following resources:

- Modify and view organization-level version limits
- Modify and view site-level version limits
- Modify and view library-level version limits
- Trimming existing versions

Last updated on 01/08/2026

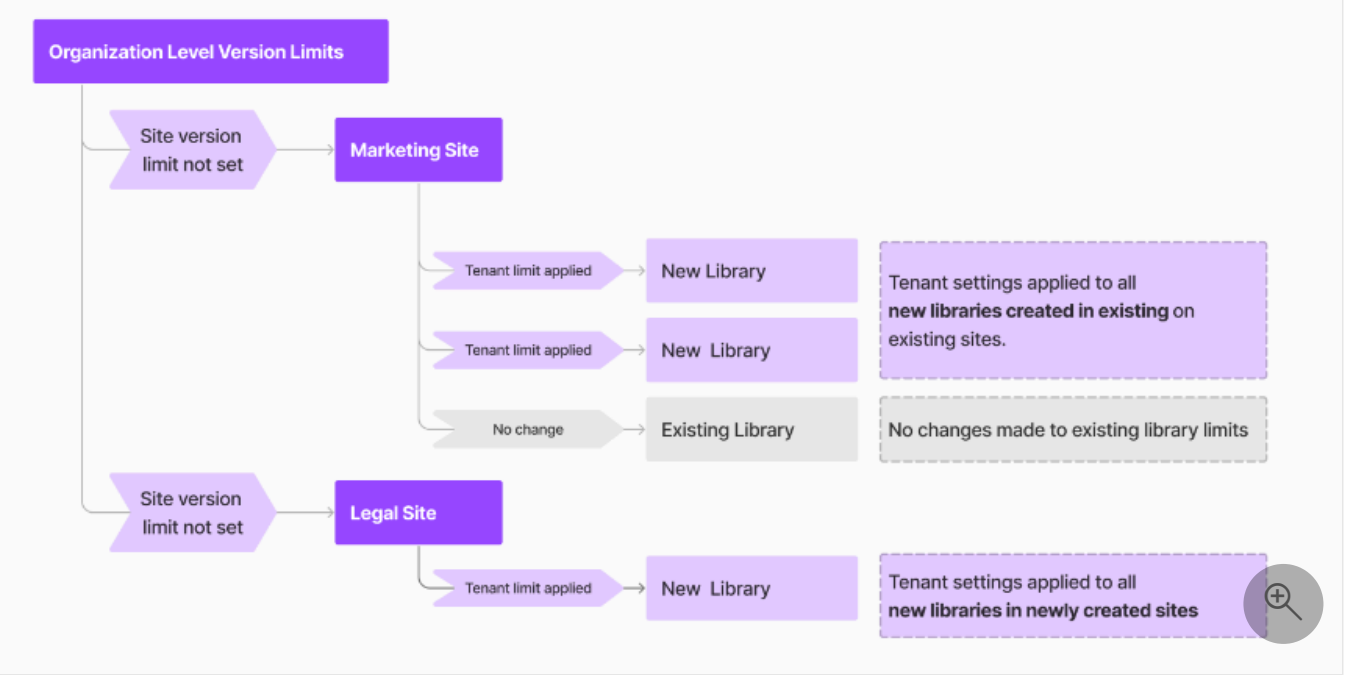
Set default organization version limits for new document libraries and OneDrive accounts

Organization-level version settings define the default version storage limits that apply on all new document libraries created across all existing or newly created SharePoint sites and new OneDrive Accounts. This setting allows admins to define the global default version history limits that apply across the organization to ensure consistent version storage use and restore options.

Example Scenario

Take an example of Contoso with an existing marketing site with a set of libraries set to 500 major version limits. When the admin updates the organization version limits to 'Automatic' library, version limits for document libraries are set in the following ways:

- **Library version limits on existing marketing site**: Version limits on all new libraries created in the marketing site are set to the organization limits of Automatic. Version limits on existing libraries remain unchanged that is, limits aren't updated to Automatic.
- **Library version limits on new legal site**: When a new legal site is created, version limits on all libraries created on the legal site are set to the organization version limits.



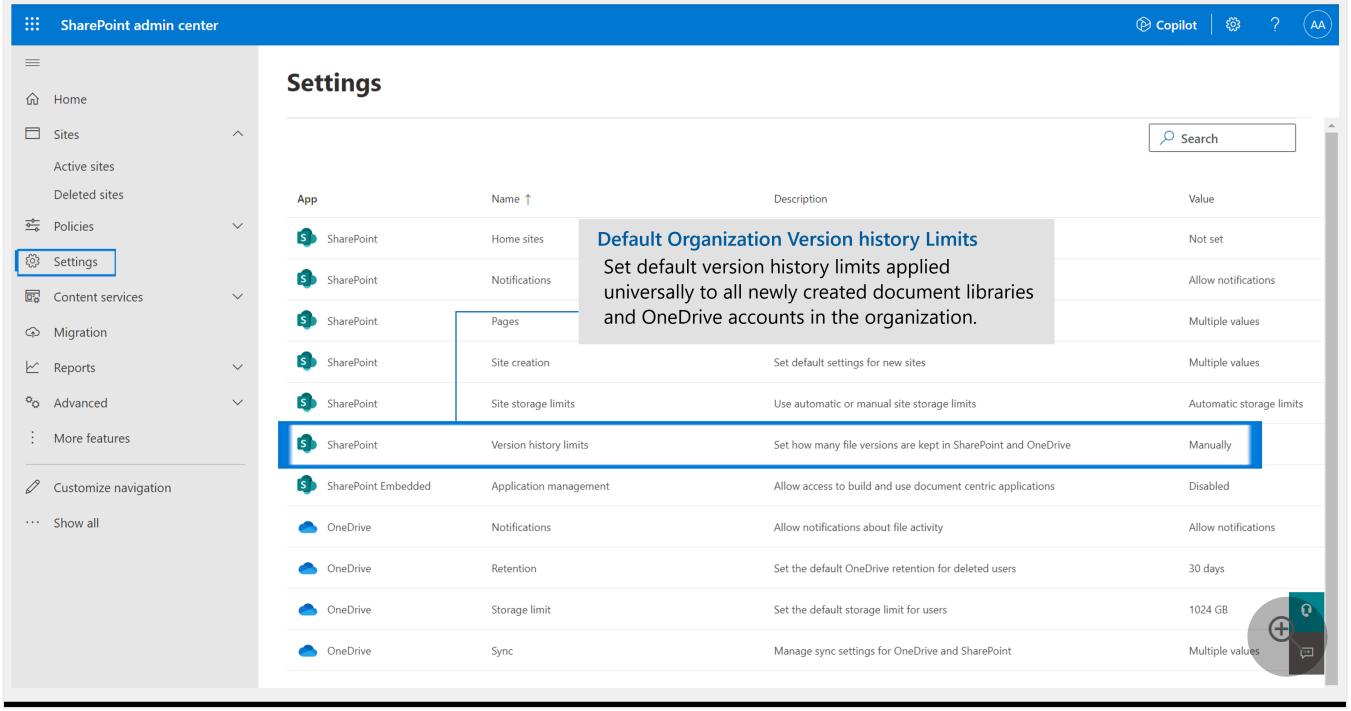
> ⓘ **Important**

- Changes made to organization-level version history limits apply to new SharePoint libraries and OneDrive user accounts created since the change was made. The changes can take upto 24 hours to be reflected on new libraries created.
- Changes made to organization-level version history limits will not update the limits applied to existing document libraries. To update the existing library settings, you can set version limits for existing libraries on a site or set version limits on a library. The ability to apply version history limits to existing document libraries at the organization level is not supported.
- Changes made to the organization-level version history limits will not trim existing version history to the new limits. To delete existing versions, you can trim existing versions from a site, library or OneDrive. The ability to trim existing versions at the organization level is not supported.
- Default Version History limits for your organization is set to Manual version history limits with 500 major version count limit and no expiration.
- Organization-level Document Library version limit settings can be used to configure version settings on libraries only (List template Base Type = 1). List version settings, creation of major and minor versions, or content approval workflows need to be configured at individual library or list level.
- If your organization is configured for multi-geo, the Organization level version history levels can be set for each geo.

Manage version history limits for your organization

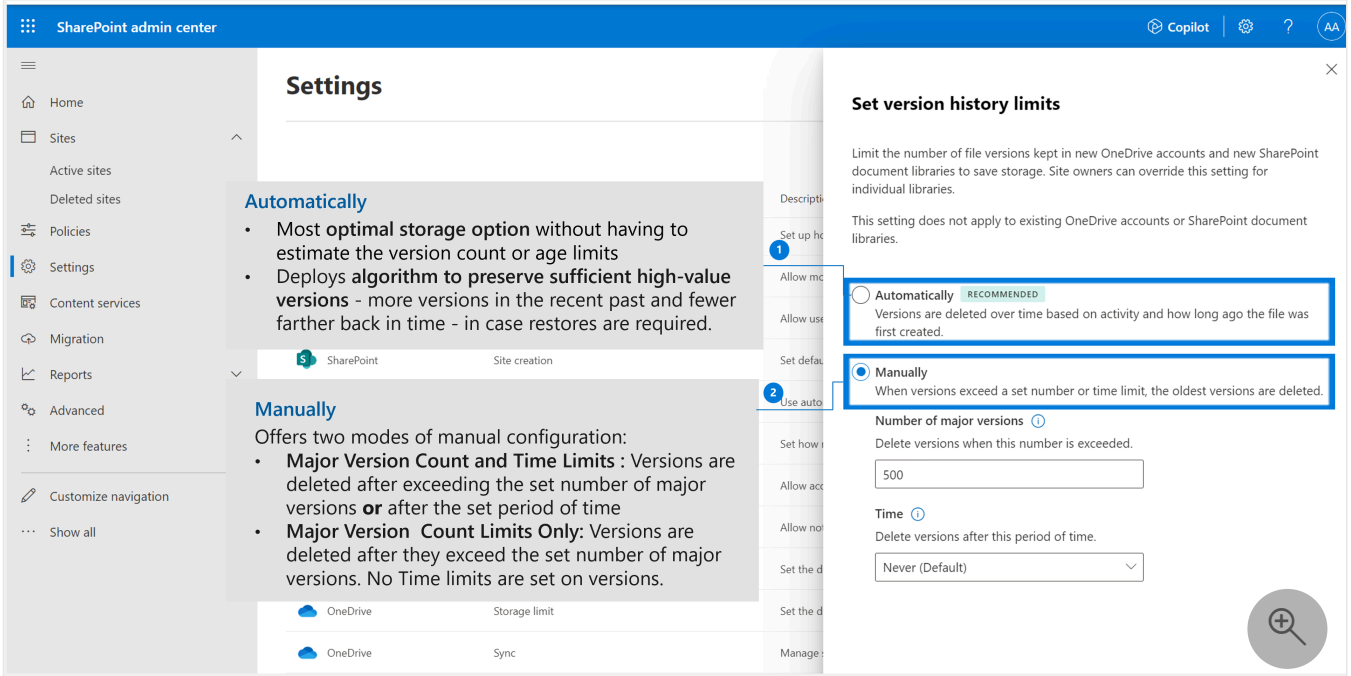
This article describes how global and SharePoint admins in Microsoft 365 can change the default version history limits for all new SharePoint document libraries and OneDrive accounts created in the organization.

Version History Limits – SharePoint Admin Settings



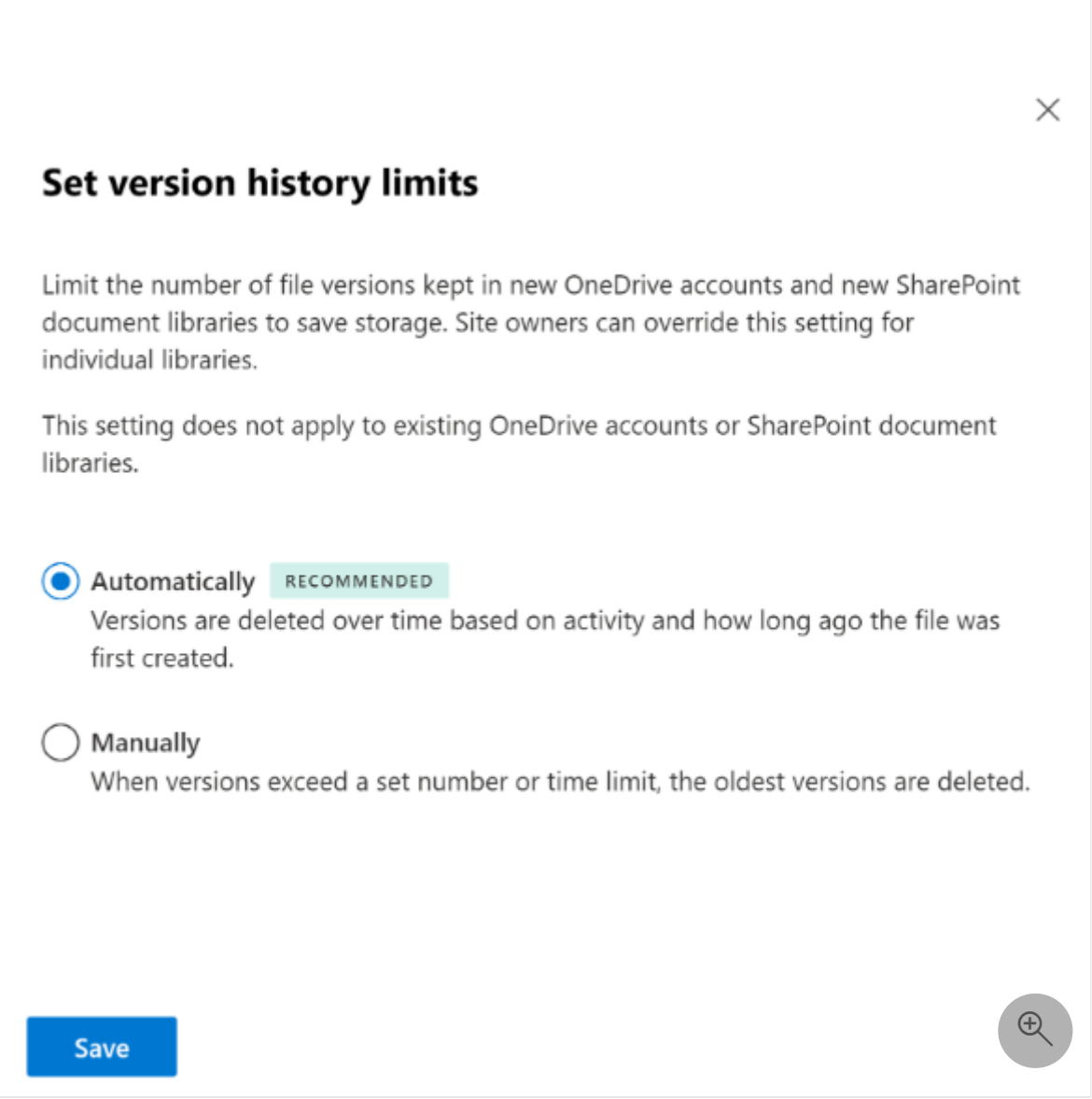
On the version history limits, SharePoint Admin Setting page uses the Organization Level Version History Limits to set global default version history limits that are universally applied to all newly created document libraries in the organization.

Version History Limits – Setting Version history limits from SharePoint Admin Center



Set automatic version history limits for the organization

1. Go to **Settings** in the SharePoint admin center, and sign in with an account that has administrator permissions for your organization.
2. Select **Version History limits**.
3. Select **Automatically**.
4. Select **Save** and **Confirm** to apply the changes to all new libraries created.



To set Automatic version history limits for all new document libraries created in your organization using PowerShell, run the following command:

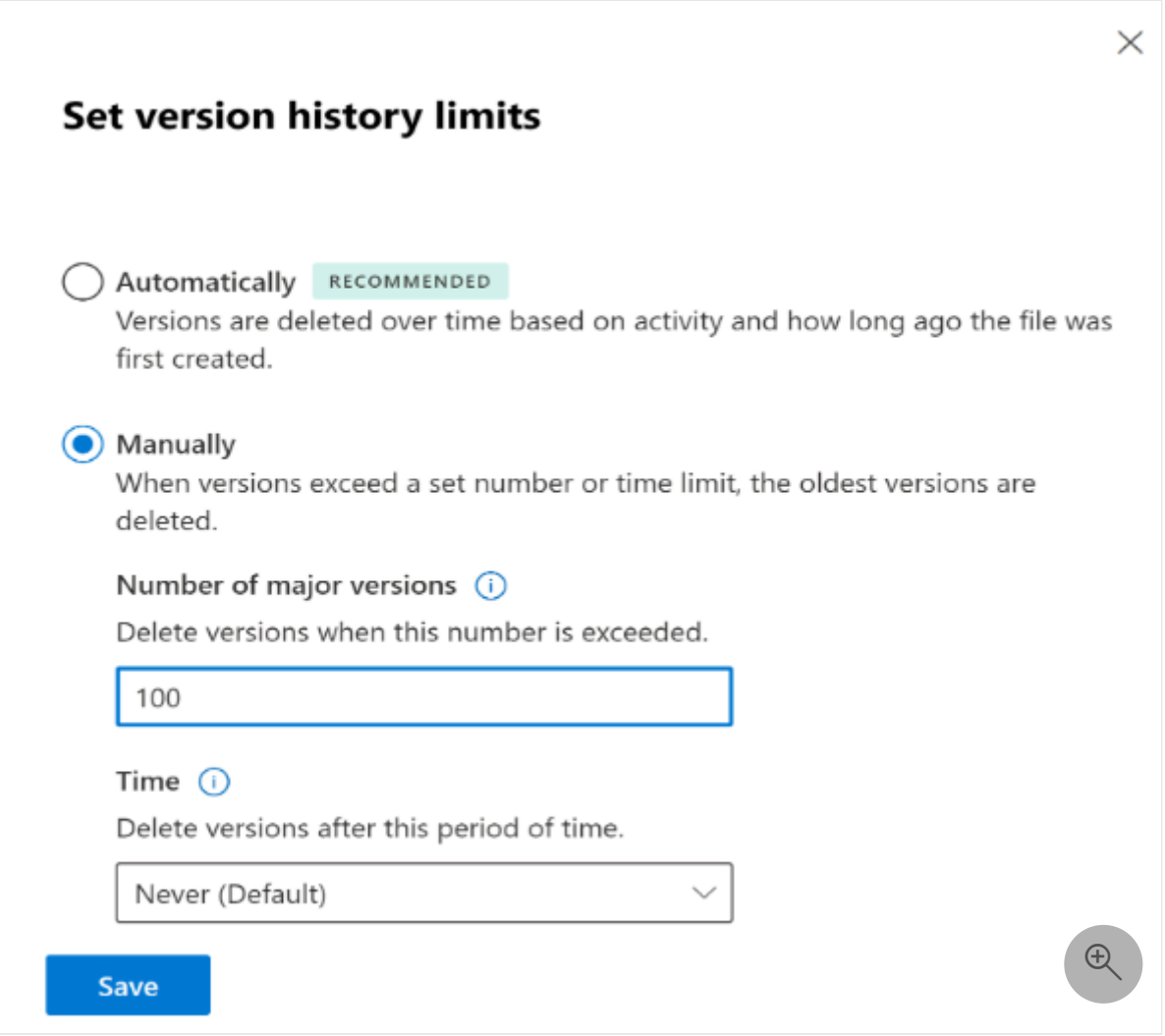
PowerShell

```
Set-SPOTenant -EnableAutoExpirationVersionTrim $true
```

Set manual version count limits with no expiration

1. Go to **Settings** in the SharePoint admin center, and sign in with an account that has administrator permissions for your organization.

2. Select **Version history limits**.
3. Select **Manually**.
4. Enter a value between 100 and 50,000 in the **Number of major versions** box.
5. Set the **Delete versions after this period of time** drop-down option to '**Never**.' This setting ensures that no expiration is stamped on versions.
6. Select **Save** and **Confirm** to apply the changes to all new libraries created.



Set manual version count and expiration storage limits

To set count and expiration limits for all new document libraries created in your organization using SharePoint admin center:

1. Go to **Settings** in the SharePoint admin center, and sign in with an account that has administrator permissions for your organization.
2. Select **Version history limits**.
3. Select **Manually**.
4. Enter a value between 100 and 50,000 in the **Number of major versions** box.

5. Select one of the preset values for **Delete versions after this period of time** drop-down option. or
6. To enter a custom value for **Delete versions after**, select the custom value from the dropbox and enter value greater than 30 days in the **Days** box and **Save**.
7. Select **Save** and **Confirm** to apply the changes to all new libraries created.

To set count and expiration limits for all new document libraries created in your organization using PowerShell, run the following command:

PowerShell

```
Set-SPOTenant `
    -EnableAutoExpirationVersionTrim $false `
    -MajorVersionLimit <int> `
    -ExpireVersionsAfterDays <int, 0 for no expiration>
```

Set file type version limit

Currently only PowerShell is supported. You can run Set-SPOTenant with the FileTypesForVersionExpiration argument to change the limit for a specific file type.

For example, to set the version limit for audio and video files to a manual limit of 100 major versions and 30-day time limit, run the following command:

PowerShell

```
Set-SPOTenant `
    -MajorVersionLimit 100 `
    -ExpireVersionsAfterDays 30 `
    -EnableAutoExpirationVersionTrim $false `
    -FileTypesForVersionExpiration @("audio", "video")
```

Or you can remove a file type version limit override by using the RemoveVersionExpirationFileTypeOverride argument.

For example, to remove the audio file type override, run the following command:

PowerShell

```
Set-SPOTenant -RemoveVersionExpirationFileTypeOverride @("audio")
```

Review organization version storage limits

To review the default version history limits for all new document libraries using SharePoint admin center:

1. Go to **Settings** in the SharePoint admin center, and sign in with an account that has administrator permissions for your organization.
2. Select **Version history limits**.

To review the default version history limits for all new document libraries using PowerShell, run the following command:

PowerShell

```
Get-SPOTenant | select EnableAutoExpirationVersionTrim, ExpireVersionsAfterDays,
MajorVersionLimit
```

To review a file type version limit, select VersionPolicyFileTypeOverride property from the result of Get-SPOTenant. For example, to review the audio file type version limits, run the following command:

PowerShell

```
(Get-SPOTenant).VersionPolicyFileTypeOverride["audio"]
```

Learn More

For more information, check out the following resources:

- Manage Version History Limits for your Organization using Set-SPOTenant
- File Type Version Limits

Last updated on 01/08/2026

Set version limits for a site

By default, organization level settings define the version history limits that are applied to all new document libraries created in a site. However, to meet specific content needs, admins can choose to set distinct version history limits on individual sites. This way, users can break the inheritance from organization limits on an individual site.

Version history limits for an individual site can be managed in the following ways:

Expand table

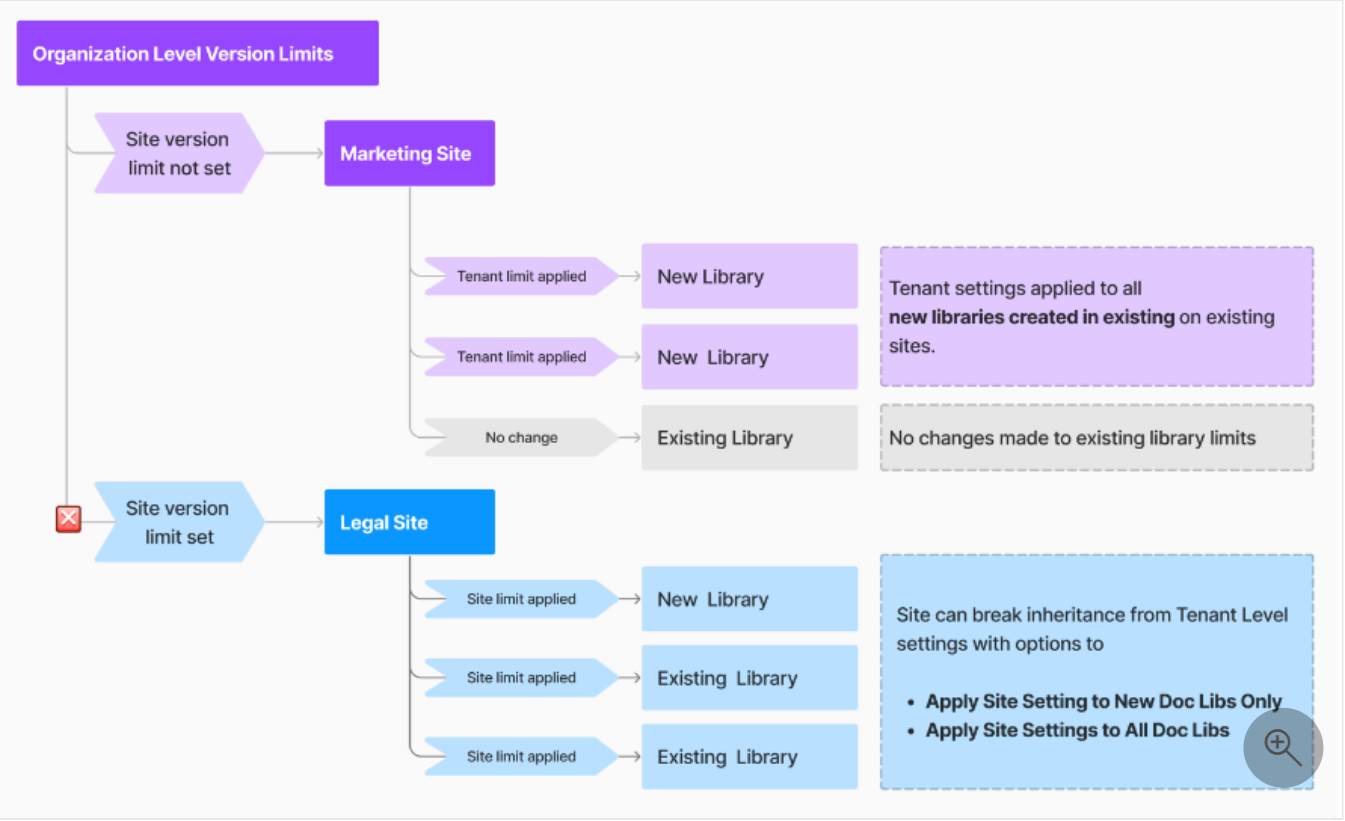
Version history limits option	Description
Apply to all new and existing document libraries in a site:	To achieve a consistent version storage policy for a site, you can choose to **set a limit to universally apply to all libraries** in the site. Using this option, the Version history limit set on site-level is applied to all the new document libraries created in the site and creates a background request to asynchronously process the update on existing document libraries.
Apply to only new document libraries created in a site:	To avoid impacting the settings on existing libraries, you can **set a version history limit only for new libraries**. Using this option, the Version history limits set on site-level are only applied to new document libraries created in the site. There are no changes made to the limits on the existing document libraries or on libraries that aren't enabled for versioning in the site.
Apply to existing document libraries only in a site:	You can update the limits **only on existing document libraries** on a site without setting a site level version history setting for new document libraries. Using this option creates a background request to asynchronously process the update on existing document libraries while allowing the new document libraries created in the site to inherit the organization level version history limits.
Clear existing limits set on a site:	You can **clear the existing limits on a site** to allow new document libraries created in the site to follow organization level limits. **Note:** Clearing a setting on a Site applies only to new document libraries created on the site and doesn't impact the settings on existing doc libraries or trim existing versions.

Example scenario

Take an example of Contoso, where the default organization Version history limits are configured to Automatic setting and no version limits are initially applied on marketing and legal sites. To meet business needs, the admin can decide to apply 'Manual' setting on legal site, thus breaking inheritance of legal site with the organization default version setting.

The following is the version storage for Contoso:

- **Version storage behavior on marketing site**: Since no limits are configured for marketing site, all new document libraries created within marketing site collection inherit the organization default setting of automatic.
- **Version storage on legal site**: Since the legal site has manual settings configured, all new libraries created within the legal site have the manual settings applied.



> **Important**
>
> - Site level Version history limits can be set using PowerShell cmdlets only.
> - Setting site level Version history limits doesn't trim existing versions to meet the new limits. Additional steps are needed to trim existing versions on a site or library.
> - Requests to update the limits on existing libraries are processed asynchronously by a background job, which can take up to 24 hours to process. You can use PowerShell to check the progress of the job.
> - Cancelling an in-progress job stops the update on libraries that were not processed. This action doesn't revert the change for document libraries where the settings update was already processed.

Manage Version history limits for a site using PowerShell

Follow these steps to manage Version history limits for a site by using PowerShell.

1. Download the latest SharePoint Online Management Shell.

> **Note**
>
> If you installed a previous version of the SharePoint Online Management Shell, go to Add or remove programs and uninstall **SharePoint Online Management Shell**.

2. Connect to SharePoint as a SharePoint Administrator in Microsoft 365. To learn how, see Getting started with SharePoint Online Management Shell.

3. Run one of the following commands to manage version history limits on your site:

Expand table

Action	PowerShell Command
View the version history limits set on a site	Get-SPOSite -Identity $siteUrl | fl Url, EnableAutoExpirationVersionTrim, ExpireVersionsAfterDays, MajorVersionLimit

Set Automatic version history limits on a site.	To set Automatic Version History Limits for all libraries on a site:
	
	`Set-SPOSite -Identity $siteUrl`
	`-EnableAutoExpirationVersionTrim $true`
	
	Append `-ApplyToNewDocumentLibraries` parameter to apply only to new document libraries on the site:
	
	`Set-SPOSite -Identity $siteUrl`
	`-EnableAutoExpirationVersionTrim $true`
	`-ApplyToNewDocumentLibraries`
	
	Supply `-FileTypesForVersionExpiration` parameter with an array of file types and append `-ApplyToNewDocumentLibraries` parameter to apply automatic version history limit on those file types in new document libraries on the site:
	
	`Set-SPOSite -Identity $siteUrl`
	`-EnableAutoExpirationVersionTrim $true`
	`-ApplyToNewDocumentLibraries`
	`-FileTypesForVersionExpiration @("<file type 1>", "<file type 2>")`
	
	Append `-ApplyToExistingDocumentLibraries` to apply only to existing document libraries on a site:
	
	`Set-SPOSite -Identity $siteUrl`

Action	PowerShell Command
	`-EnableAutoExpirationVersionTrim $true` `-ApplyToExistingDocumentLibraries`

Set Manual limits with Count and time parameters on a site.	To set Manual limits with Count and time parameters for all libraries on a site:
	
	`Set-SPOSite -Identity $siteUrl`
	`-EnableAutoExpirationVersionTrim $false`
	`-MajorVersionLimit <delete major versions exceeding limit>`
	`-MajorWithMinorVersionsLimit <number of major versions for which all minor versions will be kept>`
	`-ExpireVersionsAfterDays <delete versions exceeding time limit set in days>`
	
	Append `-ApplyToNewDocumentLibraries` parameter to apply only to new document libraries on the site:
	
	`Set-SPOSite -Identity $siteUrl`
	`-EnableAutoExpirationVersionTrim $false`
	`-MajorVersionLimit <delete major versions exceeding limit>`
	`-MajorWithMinorVersionsLimit <number of major versions for which all minor versions will be kept>`
	`-ExpireVersionsAfterDays <delete versions exceeding time limit set in days>`
	`-ApplyToNewDocumentLibraries`
	
	Supply `-FileTypesForVersionExpiration` parameter with an array of file types and append `-ApplyToNewDocumentLibraries` parameter to apply automatic version history limit on those file types in new document libraries on the site:
	
	`Set-SPOSite -Identity $siteUrl`
	`-EnableAutoExpirationVersionTrim $false`
	`-MajorVersionLimit <delete major versions exceeding limit>`
	`-MajorWithMinorVersionsLimit <number of major versions for which all minor versions will be kept>`
	`-ExpireVersionsAfterDays <delete versions exceeding time limit set in days>`
	`-ApplyToNewDocumentLibraries`
	`-FileTypesForVersionExpiration @("<file type 1>", "<file type 2>")`
	
	Append `-ApplyToExistingDocumentLibraries` to apply only to existing document libraries on a site:
	
	`Set-SPOSite -Identity $siteUrl`
	`-EnableAutoExpirationVersionTrim $false`
	`-MajorVersionLimit <delete major versions exceeding limit>`

Action	PowerShell Command

	`-MajorWithMinorVersionsLimit <number of major versions for which all minor versions will be kept>`
	`-ExpireVersionsAfterDays <delete versions exceeding time limit set in days>`
	`-ApplyToExistingDocumentLibraries`

Set Manual count with no expiration limit on a site.	To set Manual limits with Count limits set the `-ExpireVersionsAfterDays` parameter to `0:`
	
	`Set-SPOSite -Identity $siteUrl`
	`-EnableAutoExpirationVersionTrim $false`
	`-MajorVersionLimit <delete major versions exceeding limit>`
	`-MajorWithMinorVersionsLimit <number of major versions for which all minor versions will be kept>`
	`-ExpireVersionsAfterDays 0`
	
	Append `-ApplyToNewDocumentLibraries` parameter to apply only to new document libraries on the site:
	
	`Set-SPOSite -Identity $siteUrl`
	`-EnableAutoExpirationVersionTrim $false`
	`-MajorVersionLimit <delete major versions exceeding limit>`
	`-MajorWithMinorVersionsLimit <number of major versions for which all minor versions will be kept>`
	`-ExpireVersionsAfterDays 0`
	`-ApplyToNewDocumentLibraries`
	
	Supply `-FileTypesForVersionExpiration` parameter with an array of file types and append `-ApplyToNewDocumentLibraries` parameter to apply automatic version history limit on those file types in new document libraries on the site:
	
	`Set-SPOSite -Identity $siteUrl`
	`-EnableAutoExpirationVersionTrim $false`
	`-MajorVersionLimit <delete major versions exceeding limit>`
	`-MajorWithMinorVersionsLimit <number of major versions for which all minor versions will be kept>`
	`-ExpireVersionsAfterDays 0`
	`-ApplyToNewDocumentLibraries`
	`-FileTypesForVersionExpiration @("<file type 1>", "<file type 2>")`
	
	Append `-ApplyToExistingDocumentLibraries` to apply only to existing document libraries on a site:
	
	`Set-SPOSite -Identity $siteUrl`
	`-EnableAutoExpirationVersionTrim $false`

Action	PowerShell Command

	`-MajorVersionLimit <delete major versions exceeding limit>`
	`-MajorWithMinorVersionsLimit <number of major versions for which all minor versions will be kept>`
	`-ExpireVersionsAfterDays 0`
	`-ApplyToExistingDocumentLibraries`

Clear the file type version history limits set on a site for new document libraries created on the site.	`Set-SPOSite -Identity $siteUrl`
	`-RemoveVersionExpirationFileTypeOverride @("<file type 1>", "<file type 2>")`
	`-ApplyToNewDocumentLibraries`

Clear the existing version history limits set on a site and inherit Organization version limits on new document libraries created on the site.	`Set-SPOSite -Identity $siteUrl -InheritVersionPolicyFromTenant`
Cancel in progress update job	`Remove-SPOSiteVersionPolicyJob -Identity $siteUrl`

Start a sync job that updates all document libraries' version history limits to the same as the site	To sync all parts of the version history limit:
	
	`New-SPOSiteManageVersionPolicyJob -Identity $siteUrl -SyncListPolicy`
	
	Append `-ExcludeDefaultPolicy` to not sync the default version history limits:
	
	`New-SPOSiteManageVersionPolicyJob -Identity $siteUrl -SyncListPolicy -ExcludeDefaultPolicy`
	
	Supply `-FileTypes` with an array of file types to only sync the selection of file type version history limits:
	
	`New-SPOSiteManageVersionPolicyJob -Identity $siteUrl -SyncListPolicy -FileTypes @('<file type 1>', '<file type 2>')`
	
	Supply `-FileTypes` with an empty array to only sync the default version history limits:
	
	`New-SPOSiteManageVersionPolicyJob -Identity $siteUrl -SyncListPolicy -FileTypes @()`

Cancel in progress sync job	`Remove-SPOSiteManageVersionPolicyJobProgress $siteUrl`

Track progress of settings update on existing libraries on a site

Version limits on all new libraries created in the site are immediately applied. Settings on existing libraries are asynchronously updated using a background job. Run the following command **to track progress of settings update job**.

If it is an update job was started by `Set-SPOSite`:

PowerShell

```
Get-SPOSiteVersionPolicyJobProgress -Identity $siteUrl
```

If it is a sync job started by `New-SPOSiteManageVersionPolicyJob`:

PowerShell

```
Get-SPOSiteManageVersionPolicyJobProgress -Identity $siteUrl
```

The following table enumerates the various progress status that can be reported when attempting to update the version settings for existing libraries in a site collection:

Expand table

Status	Description
NoRequestFound	There are no requests on the site to set or update version settings on existing document libraries.
New	The update request is New and is not processed yet.
InProgress	The update request is processed and the settings update request is in progress.
CompleteSuccess	The update request is completed successfully.
CompleteWithFailure	The update request is completed, but setting update on some document libraries has failed.

Learn More:

- Tutorial: Manage Version history limits for a Site, Library, or OneDrive account
- Manage Version history limits for a Site using Set-SPOSite
- File Type Version Limits

- Track progress of version settings update request for existing document libraries on a site using Get-SPOSiteVersionPolicyJobProgress
- Cancel further processing of version settings update on existing document libraries on the site collection using Remove-SPOSiteVersionPolicyJob
- Start a version settings sync request for existing document libraries on a site using New-SPOSiteManageVersionPolicyJob
- Track progress of version settings sync request for existing document libraries on a site using Get-SPOSiteManageVersionPolicyJobProgress
- Cancel further processing of version settings sync on existing document libraries on the site using Remove-SPOSiteManageVersionPolicyJob

---

Last updated on 01/08/2026

Generate version storage usage report for a SharePoint site

Article • 10/03/2024

As a SharePoint admin in Microsoft 365, you can request an inventory of the versions on a site, library, or file, which can be used for various scenarios:

- Review current version storage used by existing versions.
- Understand how a version limit impacts new versions by applying the desired limits on existing versions before configuring limits.
- Analyze the impact of trimming existing versions before scheduling a trim job.

> **Note**
>
> Additional reporting options are available with Microsoft Graph Data Connect.

When you run the report, a background timer job is queued to generate a CSV file of every file version on a given SharePoint site. The CSV file is saved to the location of your choice on the site. If you don't want site members to see the report, consider creating a folder with different permissions where only site owners can access the report.

> **Important**
>
> The file version report generation job completes asynchronously over the next few days. The time it takes for the report to complete depends on the size of your library or site. For smaller sites or libraries, it takes over 24 hours to complete. For larger ones, it takes a few days to complete.
>
> While the job is being processed, you can see the report file being gradually populated. Do not update the file during this time. It will cause the job to fail. Check the progress of the report generation to confirm that the report is fully populated and ready to process.
>
> If you wish to cancel an in-progress report generation, you may simply delete the report file.

Report format

The file version expiration report is in Comma-Separated Values (CSV) format. Each row corresponds to a file version and it contains the following columns:

Expand table

File Version Identifiers:	**Description**
`WebId`	The unique identifier of the web and is a compact column [1].
`DocId`	The unique identifier of the document and is a compact column.
`MajorVersion`	The major version number of the file version.
`MinorVersion`	The minor version number of the file version.

Expand table

File Version Information:	**Description**
`WebUrl`	The SharePoint Url to the web and is a compact column.
`FileUrl`	The web relative Url to the file and is a compact column.
`Size`	The size of the version in bytes.
`ModifiedBy_UserId`	The identifier of the user who created this version and is a compact column.
`ModifiedBy_UserDisplayName`	The display name of the user who created this version and is a compact column.
`LastModifiedDate`	The time when the version was last modified.
`SnapshotDate`	The time when the version became a historical version.
`IsSnapshotDateEstimated`	If this identifier is set to true, then the `SnapshotDate` is a best-effort estimation. The `SnapshotDate` might be estimated if the version was snapshot before January 1, 2023.

Expand table

Expiration Schedule information:	**Description**
`CurrentExpirationDate`	Time when the version will expire as it currently stands.
`AutomaticPolicyExpirationDate`	Time when the version would be expiring if an automatic expiration policy were to be retroactively applied, estimated on a best-effort basis.

Expiration Schedule information:	Description
`TargetExpirationDate`	Is populated to the same value as `CurrentExpirationDate`. This column is useful for any What-If analysis and batch-updating the expiration dates.

[1] Compact columns are columns that won't repeat values if two consecutive rows have the same value. It puts empty string for the repeated records. The header for these columns have "Compact" postfix.

How to generate site version storage usage report for site, OneDrive or library

Follow these steps to manage version history limits for a site by using PowerShell.

1. Download the latest SharePoint Online Management Shell.

   > **Note**
   >
   > If you installed a previous version of the SharePoint Online Management Shell, go to Add or remove programs and uninstall **SharePoint Online Management Shell**.

2. Connect to SharePoint as a SharePoint Administrator in Microsoft 365. To learn how, see Getting started with SharePoint Online Management Shell.

3. Run one of the following commands to generate a version storage usage report:

Expand table

Action	PowerShell Command
Generate a version storage usage report for a site or OneDrive account	`New-SPOSiteFileVersionExpirationReportJob -Identity $siteUrl -ReportUrl $reportUrl`
Track progress of the job to generate report for a site or OneDrive account	`Get-SPOSiteFileVersionExpirationReportJobProgress -Identity $siteUrl -ReportUrl $reportUrl`
Generate a version storage usage report for a library	`New-SPOListFileVersionExpirationReportJob -Site $siteUrl -List $libName -ReportUrl $reportUrl`

Action	PowerShell Command
Track progress of the job to generate report for a library	`Get-SPOListFileVersionExpirationReportJobProgress -Site $siteUrl -List $libName -ReportUrl $reportUrl`

Learn More

1. Tutorial: Generate Version Usage Report
2. Tutorial: Run 'What-If' Analysis

Feedback

Was this page helpful? Yes No

Provide product feedback

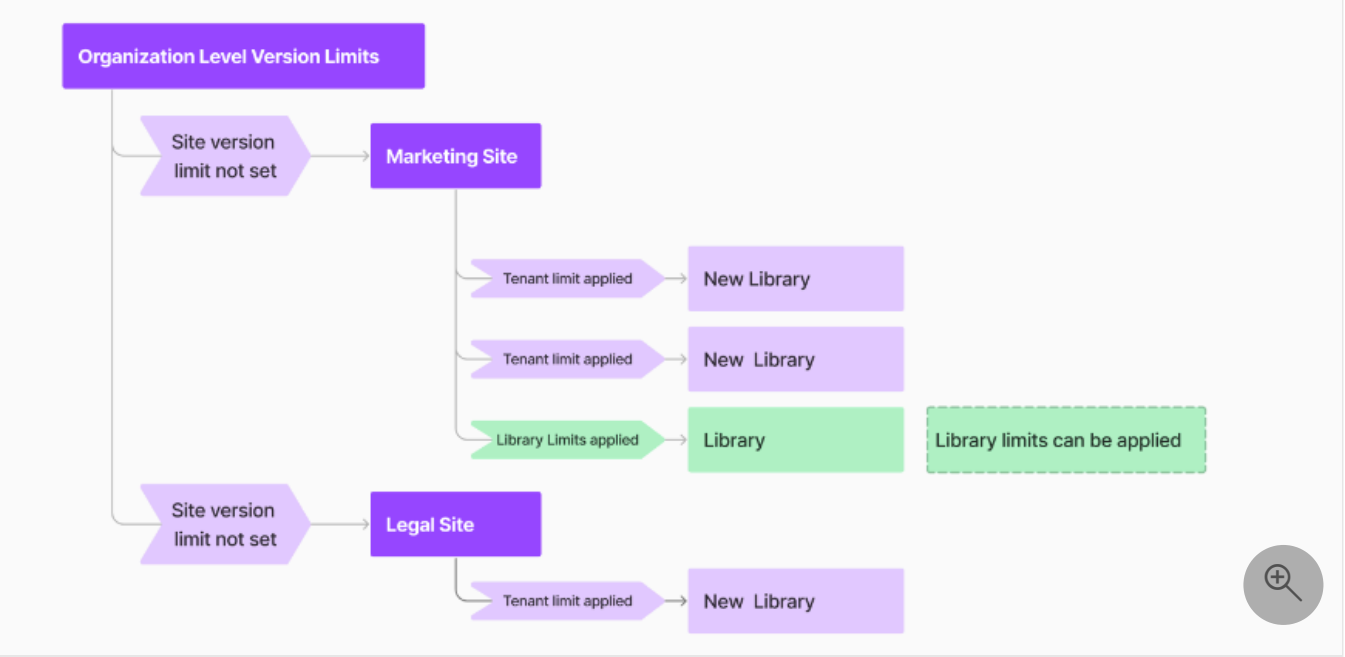
Set version limits for individual document library

The default version history limits for new document libraries are set by either the organization-level limits or the site-level limits. If the site has its own version history limit, it means the site breaks inheritance from the organization. However, to meet specific content requirements, site admins can decide to configure versioning for a library.

Here's a summary of the expected behavior when document libraries version expiration or count limits are updated:

- **When library level version expiration setting is updated**, the new expiration limit is applied to newly created versions only. Take an example of a library with version expiration settings updated from **Never Expire** to **Expire after six months**. New version created is set to expire after six months with no impact on versions that is already created.

- **When library level count limits are updated**, if existing versions exceed the new count limit, then those versions are gradually trimmed when the file is updated. Consider a library where the version count limit is initially set to 500 versions but is later reduced to 300 versions. In this scenario, if there's a file with 500 versions, each time a user updates the file, the system gradually purges the oldest 20 versions with each new version creation until the total number of versions aligns with the updated limit of 300. It's crucial to note that when count limits are lowered, the process of version deletion occurs gradually, with up to 20 versions being removed for every new version created.



Manage version history limits for a library using PowerShell

Follow these steps to manage version history limits for a site by using PowerShell.

1. Download the latest SharePoint Online Management Shell.

   > **Note**
   >
   > If you installed a previous version of the SharePoint Online Management Shell, go to Add or remove programs and uninstall **SharePoint Online Management Shell**.

2. Connect to SharePoint as a SharePoint Administrator in Microsoft 365. To learn how, see Getting started with SharePoint Online Management Shell.

3. Run one of the following commands to manage version history limits on a library:

Expand table

Action	PowerShell Command
View version history limits set on a library	`Get-SPOListVersionPolicy -Site $siteUrl -List $libName`

Set Automatic version history limits on a library	To set the default version history limit to automatic:
	
	`Set-SPOListVersionPolicy -Site $siteUrl -List $libName -EnableAutoExpirationVersionTrim $true`
	
	Supply `-FileTypes` parameter with an array of file types to set their version history limit to automatic:
	
	`Set-SPOListVersionPolicy -Site $siteUrl -List $libName -EnableAutoExpirationVersionTrim $true -FileTypes @("file type 1", "file type 2")`

Set Manual limits with count and time parameters on a library	To set Manual limits for default version history limit with count and time parameters: `Set-SPOListVersionPolicy -Site $siteUrl -List $libName -EnableAutoExpirationVersionTrim $false -MajorVersionLimit <delete major versions exceeding limit> -MajorWithMinorVersionsLimit <number of major versions for which all minor versions will be kept> -ExpireVersionsAfterDays <delete versions exceeding time limit set in days>`

Action	PowerShell Command
	Supply `-FileTypes` parameter with an array of file types to set their version history limit to Manual limits with count and time parameters: `Set-SPOListVersionPolicy -Site $siteUrl -List $libName -EnableAutoExpirationVersionTrim $false -MajorVersionLimit <delete major versions exceeding limit> -ExpireVersionsAfterDays <delete versions exceeding time limit set in days> -FileTypes @("file type 1", "file type 2")`

Set Manual limits with count with no expiration limit on a library	To set Manual limits for default version history limit with count parameter only:
	
	`Set-SPOListVersionPolicy -Site $siteUrl -List $libName -EnableAutoExpirationVersionTrim $false -MajorVersionLimit <delete major versions exceeding limit> -MajorWithMinorVersionsLimit <number of major versions for which all minor versions will be kept> -ExpireVersionsAfterDays 0`
	
	Supply `-FileTypes` parameter with an array of file types to set their version history limit to Manual limits with count parameter only:
	
	`Set-SPOListVersionPolicy -Site $siteUrl -List $libName -EnableAutoExpirationVersionTrim $false -MajorVersionLimit <delete major versions exceeding limit> -ExpireVersionsAfterDays 0 -FileTypes @("file type 1", "file type 2")`

Sync the library version history limits to its parent site	To fully sync the version history limits:
	
	`Set-SPOListVersionPolicy -Site $siteUrl -List $libName -Sync`
	
	Append `-ExcludeDefaultPolicy` to sync only the file type version history limits and exclude the default:
	
	`Set-SPOListVersionPolicy -Site $siteUrl -List $libName -Sync -ExcludeDefaultPolicy`
	
	Supply an array to the `-FileTypes` parameter to sync the select file type version history limits:
	
	`Set-SPOListVersionPolicy -Site $siteUrl -List $libName -Sync -FileTypes @("<file type 1>", "<file type 2>")`

Action	PowerShell Command
	Supply an empty array to the `-FileTypes` parameter to sync only the default version history limits: `Set-SPOListVersionPolicy -Site $siteUrl -List $libName -Sync -FileTypes @()`

Learn More

For more information, check out the following resources:

- File Type Version Limits
- View version history limits for a library using Set-SPOListVersionPolicy
- Manage version history limits for a library using Set-SPOListVersionPolicy

---

Last updated on 01/08/2026

Change version limits on OneDrive using PowerShell

Article • 10/03/2024

By default, organization version history settings are applied to all new OneDrive accounts. As a SharePoint admin in Microsoft 365, you can set the version limits on OneDrive storage for a specific user.

Follow these steps to manage Version history limits for a site by using PowerShell.

1. Download the latest SharePoint Online Management Shell.

   > **Note**
   >
   > If you installed a previous version of the SharePoint Online Management Shell, go to Add or remove programs and uninstall **SharePoint Online Management Shell**.

2. Connect to SharePoint as a SharePoint Administrator in Microsoft 365. To learn how, see Getting started with SharePoint Online Management Shell.

3. Run one of the following commands to manage Version history limits for a specific user:

Expand table

Action	PowerShell Command
View the version history limits set for a user	Get-SPOSite -Identity $siteUrl | fl Url, EnableAutoExpirationVersionTrim, ExpireVersionsAfterDays, MajorVersionLimit
Set automatic Version history limits for a user	`Set-SPOSite -Identity $siteUrl -EnableAutoExpirationVersionTrim $true`
Set manual limits with count and time parameters for a user	`Set-SPOSite -Identity $siteUrl -EnableAutoExpirationVersionTrim $false -MajorVersionLimit <delete major versions exceeding limit> -MajorWithMinorVersionsLimit <number of major versions for which all minor versions will be kept>`

Action	PowerShell Command
	`-ExpireVersionsAfterDays <delete versions exceeding time limit set in days>`
Set manual limits with count with no expiration limit for a user	To set manual limits with count limits set the `-ExpireVersionsAfterDays parameter` to 0: `Set-SPOSite -Identity $siteUrl -EnableAutoExpirationVersionTrim $false -MajorVersionLimit <delete major versions exceeding limit> -MajorWithMinorVersionsLimit <number of major versions for which all minor versions will be kept> -ExpireVersionsAfterDays 0`
Clear the existing Version history limits for a user **Note:** Clearing a setting for a user applies to new versions created on files stored on the user's OneDrive account and doesn't trim existing versions.	`Remove-SPOSiteVersionPolicyJob -Identity $siteUrl`

Learn More

Change a specific user's OneDrive storage space

Feedback

Was this page helpful? Yes No

Provide product feedback

Trim existing versions

Learn how to reduce version storage consumption by analyzing, managing, and trimming file versions at the library, site, or tenant level.

> **Caution**
>
> Versions deleted using trimming jobs are permanently deleted. This deletion workflow bypasses the normal recycle bin retention and deleted versions cannot be recovered, unless the data was previously backed up using Microsoft 365 Backup or a similar backup solution. To prevent unwanted data loss, we highly recommend to run a What-If analysis before trimming activity.

As a Global Administrator or SharePoint Administrator in Microsoft 365, you can queue a job to trim existing versions to reduce the version storage footprint across your organization. Trimming can be applied at different scopes:

- **Site, library, or OneDrive level** — Target specific sites, document libraries, or OneDrive user accounts.
- **Tenant level** — Apply your tenant-level version policy across all sites in one operation.

Version availability is critical for recovery scenarios like undoing unwanted changes. Before trimming at any scope, carefully evaluate your recovery objectives and review the projected impact.

Trim existing versions from site, library, or OneDrive

You can queue a job to trim existing versions on a site, library, or OneDrive user account to reduce the version storage footprint of your site. You can also align existing version storage with updated version history limits by scheduling a job to trim existing versions.

Expand table

Phase	Recommended Actions
Prepare	**Evaluate your recovery objectives and target version storage use:** Determine the right trim mode and trim scope that you need to meet your organization's recovery objectives. **Review**

Phase	Recommended Actions
	Impact: Before committing to trim existing versions, you have the option to review the impact of the purge action by running a 'What-if' analysis operation of the selected trim mode on the specified scope.
Queue Job	Once you're ready to commit to a trim job, you can queue a version trimming job to asynchronously delete versions matching the criteria specified in the trim mode within a site, library, or OneDrive user account.
Track Progress	You can track the progress of all queued jobs to review the progress made in trimming versions.

> **Note**
>
> Trim jobs are background jobs that are influenced by factors such as the volume of file versions to be evaluated, service health, and other jobs being processed on the farm. They are also subject to off-peak hour processing logic. The progress of a trim job can always be tracked.

Review impact by running 'What-if' analysis

Before committing to trim existing versions, you can review the impact of the purge action by running a 'What-if' analysis operation. Running a 'What-if' operation follows these steps:

- **Generate a version storage usage report for a site or library**: This report supports multiple uses, including version storage analytics and gaining key insights on the impact of applying different trimming settings.
- **Run 'What-If' analysis** by setting different trimming modes to preview the changes and analyze the storage savings impact of applying one of the trimming modes to the version storage report CSV file.

> **Important**
>
> Depending on the size of the site or library, the job can take a few days to complete. Check the progress of the job until the status returns as "completed".

Version trim modes

Version trimming workflows allow you to select and apply one of the trimming modes for queuing a trim job on a site, document library, or OneDrive account.

Automatic trim mode (recommended)

The automatic trim mode applies the Automatic algorithm to delete existing versions. Depending on the version age, the job will permanently delete versions or set expiration time according to the automatic version storage algorithm.

To learn more about automatic trim mode, see Understand version storage under Automatic limits.

Manual expiration trim mode

The manual expiration trim mode evaluates the age of versions and deletes versions matching the expiration criteria.

Example: In the following example, a trim job is queued to trim versions older than 60 days. On August 31, the job is picked up and it starts permanently deleting versions older than 60 days as of August 31.

> **Important**
>
> **Known limitations of manual expiration trim mode:**
>
> 1. The manual expiration trim mode doesn't delete versions created in the last 30 days. This means your input can't be less than 30 days.
> 2. The manual expiration trim mode always deletes all versions that were created before January 1, 2023. If you want to trim versions, you can't keep any older versions created before January 1, 2023. This means the value you use for the `DeleteBeforeDays` parameter should result in a date after January 1, 2023.

Manual count limit trim mode

The manual count limit trim mode deletes the oldest versions exceeding the specified count limit.

Example: In the following example, a trim job is queued to delete versions that exceed 50 major version counts. On August 31, the job starts permanently deleting older versions that exceed the 50 major version count limit as of August 31.

> **Tip**

You can run the impact analysis of either applying the Manual Count, Expire, or Automatic trim mode to understand the version delete impact under each mode.

Queue trim job and track progress

The version trimming workflow uses a job to asynchronously delete versions matching the criteria specified in the trim mode.

To queue the trim job, you need to determine the scope for version deletion and the trim mode to set the criteria for existing version deletion. You can delete old file versions based on version age, count limits, or automatic algorithm for all document libraries in a site or for a specific document library.

Once you're ready to commit to the trim, you can queue the job to asynchronously delete versions matching the trim mode criteria. You'll be able to monitor the progress of committed trim jobs to keep track of the deletion progress.

> **Note**
>
> To learn more about how version trimming works on versions that are subject to a retention policy or an eDiscovery hold, see FAQs.

Trim existing versions using PowerShell

Follow these steps to trim existing versions using PowerShell.

1. Download the latest SharePoint Online Management Shell.

   > **Note**
   >
   > If you installed a previous version of the SharePoint Online Management Shell, go to Add or Remove programs and uninstall **SharePoint Online Management Shell**.

2. Connect to SharePoint as a Global Administrator or SharePoint Administrator in Microsoft 365. To learn how, see Getting started with SharePoint Online Management Shell.

3. Run one of the following commands to trim the existing versions:

Expand table

Action	PowerShell Command
Queue a trim job to expire versions	**Expire versions on a site:** `New-SPOSiteFileVersionBatchDeleteJob -Identity $siteUrl -DeleteBeforeDays <days>` **Expire versions on a library:** `New-SPOListFileVersionBatchDeleteJob -Site $siteUrl -list $libName -DeleteBeforeDays <days>`
Queue a trim job to delete versions exceeding the specified count limit	**Delete versions exceeding count limits from a site:** `New-SPOSiteFileVersionBatchDeleteJob -Identity $siteUrl -MajorVersionLimit <delete major versions exceeding limit> -MajorWithMinorVersionsLimit <number of major versions for which all minor versions will be kept>` **Delete versions exceeding count limits from a library:** `New-SPOListFileVersionBatchDeleteJob -Site $siteUrl -list $libName -MajorVersionLimit <delete major versions exceeding limit> -MajorWithMinorVersionsLimit <number of major versions for which all minor versions will be kept>`
Queue trim job to delete versions using the estimated automatic trimming algorithm	**Apply automatic logic to trim existing versions from a Site:** `New-SPOSiteFileVersionBatchDeleteJob -Identity $siteUrl -Automatic` **Apply automatic logic to trim existing versions from a library:** `New-SPOListFileVersionBatchDeleteJob -Site $siteUrl -List $libName -Automatic`
Queue site-level trim job to delete versions using the version history limit of individual document libraries	**Sync all document libraries' version history limit to the same as the site and trim existing versions from the site:** `New-SPOSiteManageVersionPolicyJob -Identity $siteUrl -SyncListPolicy -TrimUseListPolicy`
Queue library-level trim job to delete versions using its version history limits	**Trim existing versions from the library using its version history limits:** `New-SPOListFileVersionBatchDeleteJob -Site $siteUrl -List $libName -TrimUseListPolicy`
Stop further processing of an in-progress trim job	**To stop processing an in-progress site level trim job:** `Remove-SPOSiteFileVersionBatchDeleteJob -Identity $siteUrl` or `Remove-SPOSiteManageVersionPolicyJob -Identity $siteUrl` **To stop processing an in-progress library level trim job:** `Remove-SPOListFileVersionBatchDeleteJob -Site $siteUrl -List $libName`

Action	PowerShell Command
Get the status for a file version trimming job	**To get status of a site level trimming job:** `Get-SPOSiteFileVersionBatchDeleteJobProgress -Identity $siteUrl` or `Get-SPOSiteManageVersionPolicyJobProgress -Identity $siteUrl` **To get status of a library level trimming job:** `Get-SPOListFileVersionBatchDeleteJobProgress -Site $siteUrl -List $libName`

Trim existing versions at the tenant level

> **Note**
>
> Tenant-level version trimming is currently in private preview. This feature may change based on feedback, including the addition of throttling limits on the number of jobs you can run within a specific time period.

Tenant admins can use tenant-level operations to start a file version trimming job across all sites in a tenant, update document library version policies to match the tenant policy, and estimate the storage impact of trimming by using what-if analysis.

Tenant-level file version trimming cmdlets let you:

- Update all document library version policies to match the tenant policy.
- Trim existing versions based on that policy.
- Track progress and delete the tenant-level job.

To help you understand trimming impact, additional cmdlets let you run fast, synchronous what-if analysis queries after an initial asynchronous data collection job.

> **Caution**
>
> Versions deleted using trimming jobs are permanently deleted. This deletion workflow bypasses the normal recycle bin retention and deleted versions cannot be recovered, unless the data was previously backed up using Microsoft 365 Backup or a similar backup solution.

Prerequisites and limitations

- Requires a **SharePoint Advanced Management license** or **Copilot license**.

- Only **one job is allowed per tenant** at a time.
- The following site types are excluded from processing:
  - Read-only sites
  - Locked sites
  - Archived sites
  - Sites with version policy broken inheritance
- If the tenant-level version policy changes while the job is in progress, the job applies the updated policy to remaining unprocessed sites. Sites already processed are not re-evaluated.
- The tenant-level trim uses the version policy configured at the tenant level (Automatic, Manual Expiration, or Manual Count Limit). To understand these trim modes, see Version trim modes above.
- The what-if analysis returns impact data for both **SharePoint sites** and **OneDrive accounts**.
- If your tenant is **Multi-Geo**, the what-if analysis and version trimming must be run separately for each geo location.

Recommended workflow

1. Prerequisites

1. Download the latest SharePoint Online Management Shell.

2. Connect to SharePoint as a Global Administrator or SharePoint Administrator in Microsoft 365. To learn how, see Getting started with SharePoint Online Management Shell.

3. Confirm your tenant-level version policy by running:

   PowerShell
   ```
   Get-SPOTenantVersionPolicy
   ```

   You can also use `Get-SPOTenant` and check the `EnableAutoExpirationVersionTrim`, `MajorVersionLimit`, `ExpireVersionsAfterDays`, and `VersionPolicyFileTypeOverride` properties.

2. (Optional but strongly recommended) What-If Analysis

Before committing to a trim, you can estimate the impact of your tenant version policy without deleting any versions:

1. **Run a data collection job** to gather version data across all sites:

PowerShell

```
New-SPOTenantApplyFileVersionPolicyJob -CollectVersionData
```

2. **Monitor the data collection job** until it completes:

PowerShell

```
Get-SPOTenantApplyFileVersionPolicyJobProgress
```

3. **Run what-if queries** to estimate the impact of applying your policy:

PowerShell

```
Get-SPOTenantApplyFileVersionPolicyJobImpact
```

You can run multiple what-if queries with different policy options using `Get-SPOVersionPolicyWithChanges` to create modified policy objects for comparison.

4. Review the projected impact and choose a desired version policy.

3. Trim existing versions and update document library policies

Once you've confirmed your tenant version policy and reviewed the projected impact:

1. **Run the trim job** with desired options:

PowerShell

```
# Trim existing versions AND set version policy on all libraries
New-SPOTenantApplyFileVersionPolicyJob -TrimVersions -SetVersionPolicy

# Or trim only (without updating library policies)
New-SPOTenantApplyFileVersionPolicyJob -TrimVersions

# Or set policy only (without trimming existing versions)
New-SPOTenantApplyFileVersionPolicyJob -SetVersionPolicy

# Or specify a custom version policy object
$policy = Get-SPOVersionPolicyWithChanges -VersionPolicy (Get-
SPOTenantVersionPolicy) -EnableAutoExpirationVersionTrim $true
New-SPOTenantApplyFileVersionPolicyJob -VersionPolicy $policy -TrimVersions
```

2. **Monitor and validate the trim job:**

PowerShell

```
Get-SPOTenantApplyFileVersionPolicyJobProgress
```

3. **Cancel an in-progress job** (if needed):

PowerShell

```
Remove-SPOTenantApplyFileVersionPolicyJob
```

> **Note**
>
> Once the cmdlet executes successfully, all new asynchronous version deletion is stopped. Canceling a trim job does not impact versions that were permanently deleted while the job was in progress.

Tenant-level PowerShell cmdlet reference

Expand table

Action	PowerShell Cmdlet	Reference
Collect version data (prerequisite for what-if)	`New-SPOTenantApplyFileVersionPolicyJob -CollectVersionData`	New-SPOTenantApplyFileVersionPolicyJob
Estimate impact (what-if query)	`Get-SPOTenantApplyFileVersionPolicyJobImpact`	Get-SPOTenantApplyFileVersionPolicyJobImpact
Trim existing versions using current tenant policy	`New-SPOTenantApplyFileVersionPolicyJob -TrimVersions`	New-SPOTenantApplyFileVersionPolicyJob
Set version policy on all document libraries	`New-SPOTenantApplyFileVersionPolicyJob -SetVersionPolicy`	New-SPOTenantApplyFileVersionPolicyJob
Trim + set policy	`New-SPOTenantApplyFileVersionPolicyJob -TrimVersions -SetVersionPolicy`	New-SPOTenantApplyFileVersionPolicyJob

Action	PowerShell Cmdlet	Reference
Trim with a specific policy object	`New-SPOTenantApplyFileVersionPolicyJob -VersionPolicy $policy -TrimVersions`	New-SPOTenantApplyFileVersionPolicyJob
Track job progress	`Get-SPOTenantApplyFileVersionPolicyJobProgress`	Get-SPOTenantApplyFileVersionPolicyJobProgress
Cancel an in-progress job	`Remove-SPOTenantApplyFileVersionPolicyJob`	Remove-SPOTenantApplyFileVersionPolicyJob
Get current tenant version policy	`Get-SPOTenantVersionPolicy`	Get-SPOTenantVersionPolicy
Create a modified policy object locally	`Get-SPOVersionPolicyWithChanges`	Get-SPOVersionPolicyWithChanges

---

Learn more

For more information, check out the following resources:

- Tutorial: Generate Version Usage Report
- Tutorial: Run 'What-If' analysis
- Tutorial: Queue Trim Job
- File Type Version Limits
- Start a version settings sync and trim request for existing document libraries on a site using New-SPOSiteManageVersionPolicyJob
- Track progress of version settings sync and trim request for existing document libraries on a site using Get-SPOSiteManageVersionPolicyJobProgress
- Cancel further processing of version settings sync and trim on existing document libraries on the site using Remove-SPOSiteManageVersionPolicyJob
- Start a version trim request for a document library using New-SPOListFileVersionBatchDeleteJob
- Track progress of a version trim request for a document library using Get-SPOListFileVersionBatchDeleteJobProgress

- Cancel further processing of a version trim for a document library using Remove-SPOListFileVersionBatchDeleteJob

ⓘ**Note:** The author created this article with assistance from AI. Learn more

---

Last updated on 08/19/2026

Tutorial: Generate and analyze version usage report for SharePoint site

Article • 10/25/2024

By understanding version storage on a site, you can better optimize the Version history settings to meet your organization's recovery objectives and manage storage costs.

This tutorial shows how you can generate a version storage usage report and analyze it to better understand the version storage footprint of the site. The report can also be used to run 'what-if' analysis of applying different version limits or trimming existing versions.

In this tutorial we cover how to:

- Generate version storage usage report file for site or library.
- Check progress of report generation.
- Understand the report file.
- Analyze version storage use using Excel or PowerShell.

In later tutorials, review how you can run impact analysis on the generated CSV report.

Before you begin

1. Identify the SharePoint site, OneDrive account, or document library whose version storage usage you want to understand.
2. Choose a location within the SharePoint document library that you want to save the report to.
3. Download the latest SharePoint Online Management Shell.

> **Note**
>
> 1. The report file is generated within the report location specified.
> 2. The report location must be within a SharePoint document library itself.
> 3. There cannot be a file with the same name as the report in the document library.

Generate version usage report for sites or library

You can generate a report on the current version storage use on a site by running the `New-SPOSiteFileVersionExpirationReportJob` command or on a library by running the `New-SPOListFileVersionBatchDeleteJob` command.

In the following example, a job is queued to generate a site-scoped report at the report location, `https://contoso.sharepoint.com/sites/sites1/reports/MyReports/VersionReport.csv`.

PowerShell

```
New-SPOSiteFileVersionExpirationReportJob -Identity
https://contoso.sharepoint.com/sites/site1 -ReportUrl
"https://contoso.sharepoint.com/sites/sites1/reports/MyReports/VersionReport
.csv"
```

In the following example, a job is queued to generate a library-scoped report at the report location, `https://contoso.sharepoint.com/sites/sites1/reports/MyReports/VersionReport.csv`.

PowerShell

```
New-SPOListFileVersionExpirationReportJob -Site
https://contoso.sharepoint.com/sites/site1 -List "Documents" -ReportUrl
"https://contoso.sharepoint.com/sites/sites1/reports/MyReports/VersionReport
.csv"
```

Check progress on the report generation

Use the `Get-SPOListFileVersionExpirationReportJobProgress` command to track the progress of report generation request.

The example below shows how you can check if your **site scoped report** is fully populated and ready to be analyzed.

PowerShell

```
Get-SPOSiteFileVersionExpirationReportJobProgress -Identity
https://contoso.sharepoint.com/sites/site1 -ReportUrl
"https://contoso.sharepoint.com/sites/sites1/reports/MyReports/VersionReport
.csv"
```

The example below shows how you can check if your **library scoped report** is fully populated and ready to be analyzed.

PowerShell

```
Get-SPOListFileVersionExpirationReportJobProgress -Site
https://contoso.sharepoint.com/sites/site1 -List "Documents" -ReportUrl
"https://contoso.sharepoint.com/sites/sites1/reports/MyReports/VersionReport
.csv"
```

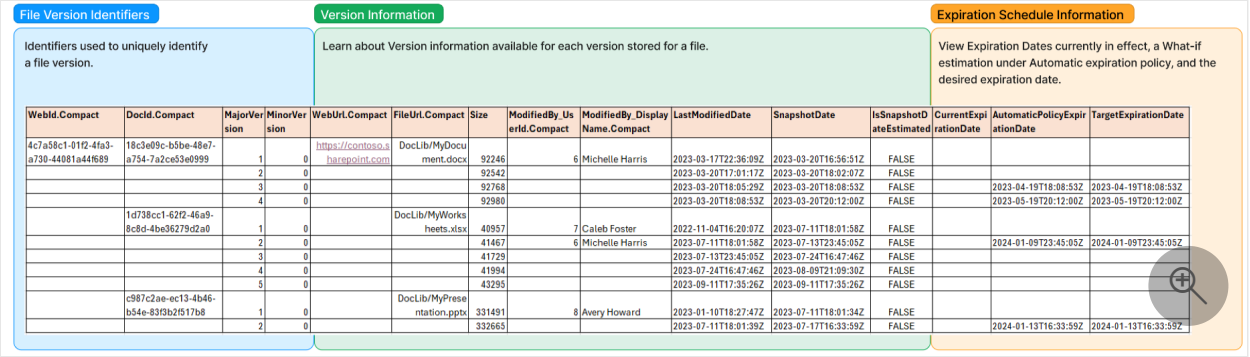
The cmdlet will return a response in JSON format. The returned json response has a key named status. Refer to the table below for one of the following expected values:

Expand table

JSON Status Response	Explanation
“completed”	The job has successfully completed and the report is fully populated.
“in_progress”	There is an active job. The report is partially populated.
“no_report_found”	There are no active jobs populating the specified file.
“failed”	The job to generate the report has failed due to the error message. Check “error_message” for the error message from the failure.

Understand version report file

The generated report is in CSV format with each row corresponds to a file version. Here’s an example of file version expiration report and its column breakdown.



WebId.Compact	DocId.Compact	MajorVersion	MinorVersion	WebUrl.Compact	FileUrl.Compact	Size	ModifiedBy_UserId.Compact	ModifiedBy_DisplayName.Compact	LastModifiedDate	SnapshotDate	IsSnapshotDateEstimated	CurrentExpirationDate	AutomaticPolicyExpirationDate	TargetExpirationDate
4c7a58c1-01f2-4fa3-a730-44081a44f689	18c3e09c-b5be-48e7-a754-7a2ce53e0999	1	0	https://contoso.sharepoint.com	DocLib/MyDocument.docx	92246	6	Michelle Harris	2023-03-17T22:36:09Z	2023-03-20T16:56:51Z	FALSE			
		2	0			92542			2023-03-20T17:01:17Z	2023-03-20T18:02:07Z	FALSE			
		3	0			92768			2023-03-20T18:05:29Z	2023-03-20T18:08:53Z	FALSE		2023-04-19T18:08:53Z	2023-04-19T18:08:53Z
		4	0			92980			2023-03-20T18:08:53Z	2023-03-20T20:12:00Z	FALSE		2023-05-19T20:12:00Z	2023-05-19T20:12:00Z
	1d738cc1-62f2-46a9-8c8d-4be36279d2a0	1	0		DocLib/MyWorksheets.xlsx	40957	7	Caleb Foster	2022-11-04T16:20:07Z	2023-07-11T18:01:58Z	FALSE			
		2	0			41467	6	Michelle Harris	2023-07-11T18:01:58Z	2023-07-13T23:45:05Z	FALSE		2024-01-09T23:45:05Z	2024-01-09T23:45:05Z
		3	0			41729			2023-07-13T23:45:05Z	2023-07-24T16:47:46Z	FALSE			
		4	0			41994			2023-07-24T16:47:46Z	2023-08-09T21:09:30Z	FALSE			
		5	0			43295			2023-09-11T17:35:26Z	2023-09-11T17:35:26Z	FALSE			
	c987c2ae-ec13-4b46-b54e-83f3b2f517b8	1	0		DocLib/MyPresentation.pptx	331491	8	Avery Howard	2023-01-10T18:27:47Z	2023-07-11T18:01:34Z	FALSE			
		2	0			332665			2023-07-11T18:01:39Z	2023-07-17T16:33:59Z	FALSE		2024-01-13T16:33:59Z	2024-01-13T16:33:59Z

The first row is the header with the column identifiers containing File Version Identifiers, Version Metadata information, and expiration timestamp. Compact columns are denoted with `.Compact` post-fix that won’t repeat values if two consecutive rows have the same value. The other rows represent file versions, where each row represents a single version.

Let’s go through the first file version displayed in this report.

- File version identifiers: `WebId`, `DocId`, `MajorVersion`, and `MinorVersion` uniquely identify each version in your SharePoint site.
- Version metadata identifiers: `WebUrl` indicates the version in `https://contoso.sharepoint.com`, and `FileUrl` indicates that the file for this version is located at DocLib/MyDocument.docx. In other words, it is in a Document Library called `DocLib`, while the file is in the root folder of `DocLib` and is named MyDocument.docx.
- `Size` indicates that the version takes 92,246 bytes of storage.
- The next two columns, `ModifiedBy_UserId` and `ModifiedBy_DisplayName` indicate that the user Michelle Harris (with user ID 6) has created this version.
- `LastModifiedDate` indicates that the version's content was last modified on March 13, 2023, at 22:36:09 UTC. `SnapshotDate` displays that the version became a historical version on March 20, 2023, at 16:56:51 UTC. `IsSnapshotDateEstimated` shows that `SnapshotDate` is the actual snapshot date.
- Expiration schedule identifiers: `CurrentExpirationDate` indicates that this version is currently set to never expire. `AutomaticPolicyExpirationDate` shows that under the automatically expire policy, this version is also set to never expire. `TargetExpirationDate` indicates that if we follow this schedule for trimming, we would set this version to never expire.

> **Note**
>
> File versions stored in the preservation hold library will be included in this report as well.

Let's look at the third version.

The `WebId` and `DocId` values are empty because these columns are compact columns, denoted by .*Compact* post-fix, it means they should have values. If we look for the last nonempty above that row, we find `WebId` as `4c7a58c1-01f2-4fa3-a730-44081a44f689`, and `DocId` as `18c3e09c-b5be-48e7-a754-7a2ce53e0999`.

We can also see that the `TargetExpirationDate` is set for April 19, 2023, at 18:08:53 UTC. It means if we trim based on this schedule, we would be setting the expiration date for this version to that time.

> **Note**
>
> All date times are represented in the round-trip format. For more information, see Standard date and time format strings - .NET | Microsoft Learn

Analyze version storage for sites

Before you start your analysis, you should update the `TargetExpirationDate` column in your report file to the dates that you want, like the versions to be expired. Again, if you choose a date that is in the past for a version, then that version will be treated as "version that had already expired" and will be deleted right away after you start the trim.

You can manually update the dates in `TargetExpirationDate` by editing the csv file. However, you may have too many rows to update by hand. To bulk update the column, you can use Excel formulas, or you can also use one of the PowerShell scripts we have provided in Tutorial: Run 'What-If' analysis. Specifically, you may choose a trimming mode, run the corresponding script to get an updated csv file with `TargetExpirationDate` filled out based on that trimming mode, and continue from there.

Option one: Analyze the report using Excel

Open the shared Excel workbook AnalyzeReportFile_Template.xlsx. You can find the following worksheets in it.

- **Configuration**: Use this worksheet to set the date range for generating the different report views.
- **Dataset**: This worksheet is the raw dataset imported from the report file. Various reporting summary views are constructed from this dataset.
- **Preset Reports**: Here's a list of preset views that can be used to understand the impact of applying the selected setting on versions stored in the site:
  - **Summary**: Analyze the current state of version storage for this site and deleted version distribution under the new settings.
  - **Impacted Users**: Review the users whose versions would be impacted under the new settings.
  - **Version Count**: A table and graph showing the numbers of versions that will be available over time under the current schedule and the number of versions that will be available under the new schedule.
  - **Version Size Analysis**: Compare the size of versions that will be deleted over time under the current schedule and the number of versions that will be available under the new schedule.

- **File Level Analysis**: Review file level version deletions under the new settings.

Populate the workbook by following these steps:

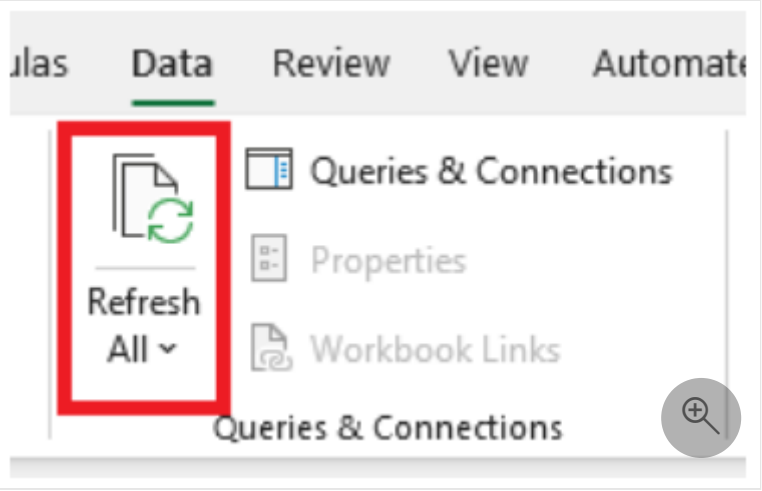
1. On the **Configuration** worksheet, enter the full path to the What-If report file in **Cell B3**.

	A	B
1	Configuration Name	Value
2	General	
3	Data Source	<replace this with the path to your report csv file, please click on **Data > Refresh All** after you update this cell>
4		
5	Number of Versions Avaliable	
6	Date Span Start	10/5/2023
7	Date Span End	10/4/2024
8		
9	Size of Versions Avaliable	
10	Date Span Start	10/5/2023
11	Date Span End	10/4/2024
12		
13	Summary	
14	Number of Files Have Fewer Than or Equal To X Versions	1

2. If you want to change the date range of graphs in **Number of Versions Available** worksheet, or **Size of Versions Expired** worksheet, change the corresponding values in Cells B6, B7, B10, and/or B11. It's optional.

	A	B
1	Configuration Name	Value
2	General	
3	Data Source	C:\Users\blarrywang\OneDrive - Microsoft\Desktop\Version Management\Documentation\Private Preview Documentation\Scripts\Iteration 2\Supporting Files\Report_WhatIf_Auto.csv
4		
5	Number of Versions Avaliable	
6	Date Span Start	10/5/2023
7	Date Span End	10/4/2024
8		
9	Size of Versions Avaliable	
10	Date Span Start	10/5/2023
11	Date Span End	10/4/2024
12		
13	Summary	
14	Number of Files Have Fewer Than or Equal To X Versions	1

3. At the top of Excel, select the **Data** tab, and in the Ribbon, select the **Refresh All** button.



4. On the **File Level Analysis** worksheet, autofill the **Number of Versions** and **Number of Versions Remaining After Deletion** columns.

	A	B	C
1		Number of Versions Per File	
2	DocId	Number of Versions	Number of Versions Remaining After Deletion
3	18c3e09c-b5be-48e7-a754-7a2ce53e0999	148	73
4	1d738cc1-62f2-46a9-8c8d-4be36279d2a0		
5	c987c2ae-ec13-4b46-b54e-83f3b2f517b8		
6	69d0e95e-35d7-452a-82d0-8e35e3cdc8c0		
7	47250f45-822c-4f3c-b9aa-33435875b953		
8	24e5a5d5-5cce-448a-950d-834cdfc40000		
9	763eabd3-fb41-4c3f-a43f-d7cc870711a3		
10	7bd67375-b328-4eca-b82f-f9b478ff8649		
11	e3bf9798-865c-4e93-8a82-e7cba670d374		
12	ada99bc2-4d15-4a6c-9075-b48d088a88eb		
13	15280ba3-efe6-4b91-ac87-17e691ab97b6		
14	3f8a7348-3c0a-43a1-86c8-1ef4850dd5c7		

	A	B	C
1		Number of Versions Per File	
2	DocId	Number of Versions	Number of Versions Remaining After Deletion
3	18c3e09c-b5be-48e7-a754-7a2ce53e0999	148	73
4	1d738cc1-62f2-46a9-8c8d-4be36279d2a0	5	5
5	c987c2ae-ec13-4b46-b54e-83f3b2f517b8	3	3
6	69d0e95e-35d7-452a-82d0-8e35e3cdc8c0	3	3
7	47250f45-822c-4f3c-b9aa-33435875b953	10	9
8	24e5a5d5-5cce-448a-950d-834cdfc40000	3	3
9	763eabd3-fb41-4c3f-a43f-d7cc870711a3	2	2
10	7bd67375-b328-4eca-b82f-f9b478ff8649	3	2
11	e3bf9798-865c-4e93-8a82-e7cba670d374	3	2
12	ada99bc2-4d15-4a6c-9075-b48d088a88eb	1	1
13	15280ba3-efe6-4b91-ac87-17e691ab97b6	1	1
14	3f8a7348-3c0a-43a1-86c8-1ef4850dd5c7	7	3

Tip

You can select the cell with data and double click on the fill handle to complete autofill.

5. On the **Impacted Users** worksheet, autofill the **Number of Versions Will be Deleted** column.

	A	B	C
1	User Id	Display Name	Number of Versions Will Be Deleted
2	6	Alice	250
3	15	Bob	
4	25	Carol	
5	23	Dan	

	A	B	C
1	User Id	Display Name	Number of Versions Will Be Deleted
2	6	Alice	250
3	15	Bob	0
4	25	Carol	3
5	23	Dan	5

All worksheets should now be up to date. You can check the information you're interested in.

Option two: Analyze the report using PowerShell

1. Save the script as a file named **AnalyzeReportFile.ps1**.

PowerShell

```
# save this file as AnalyzeReportFile.ps1

Param(
  [Parameter(Mandatory=$true)][string] $ReportLocalFilePath,
  [Parameter(Mandatory=$false)][int]$ShowFilesWithFewerThanNVersions=10,
  [Parameter(Mandatory=$false)][DateTime]$TimelineStartDate=[DateTime]::Now,
  [Parameter(Mandatory=$false)][int]$TimelineStepDays=10,
  [Parameter(Mandatory=$false)][int]$TimelineNumSteps=10
)
function Import-Dataset($DatasetFilePath)
{
  $Dataset = Import-CSV $DatasetFilePath
  $Columns = $Dataset `
    | Get-Member -MemberType 'NoteProperty' `
    | Select-Object -ExpandProperty Name
  $CompactColumns = $Columns | Where-Object { $_ -Match ".Compact" }

  $Timer = [Diagnostics.Stopwatch]::StartNew()
  for ($RowIndex = 0; $RowIndex -lt $Dataset.Count; $RowIndex++)
  {
    if ($RowIndex -gt 0)
    {
```

```
      $PrevRow = $Dataset[$RowIndex-1]
    }
    $Row = $Dataset[$RowIndex]

    foreach ($ColName in $Columns)
    {
      if ([string]::IsNullOrEmpty($Row.$ColName))
      {
        if (($ColName -in $CompactColumns) -and ($RowIndex -gt 0))
        {
          $Row.$ColName = $PrevRow.$ColName
        }
        else
        {
          $Row.$ColName = $null
        }
      }
    }

    $Row."WebId.Compact" = [Guid]$Row."WebId.Compact"
    $Row."DocId.Compact" = [Guid]$Row."DocId.Compact"
    $Row."MajorVersion" = [Int32]$Row."MajorVersion"
    $Row."MinorVersion" = [Int32]$Row."MinorVersion"
    $Row."WebUrl.Compact" = [String]$Row."WebUrl.Compact"
    $Row."FileUrl.Compact" = [String]$Row."FileUrl.Compact"
    $Row."Size" = [Int64]$Row."Size"
    $Row."ModifiedBy_UserId.Compact" =
[String]$Row."ModifiedBy_UserId.Compact"
    $Row."ModifiedBy_DisplayName.Compact" =
[String]$Row."ModifiedBy_DisplayName.Compact"
    $Row."LastModifiedDate" = [DateTime]$Row."LastModifiedDate"
    $Row."SnapshotDate" = [DateTime]$Row."SnapshotDate"
    $Row."IsSnapshotDateEstimated" = [bool]$Row."IsSnapshotDateEstimated"
    $Row."CurrentExpirationDate" =
[System.Nullable[DateTime]]$Row."CurrentExpirationDate"
    $Row."AutomaticPolicyExpirationDate" =
[System.Nullable[DateTime]]$Row."AutomaticPolicyExpirationDate"
    $Row."TargetExpirationDate" =
[System.Nullable[DateTime]]$Row."TargetExpirationDate"
    $Percent = [Math]::Ceiling(100 * $RowIndex / $Dataset.Count)
    Write-Progress `
      -Activity "Reading dataset" `
      -Status "$Percent% Complete ($($RowIndex + 1) / $($Dataset.Count)
rows):" `
      -PercentComplete $Percent `
      -SecondsRemaining $(($Dataset.Count - ($RowIndex + 1)) / (($RowIndex +
1) / $Timer.Elapsed.Totalseconds))
  }
  $Timer.Stop()
  return $Dataset
}
function Get-NumVersionExpiresByDate($Dataset, $ColName, $DateCutoff)
{
  $VersionsExpired = $Dataset | Where-Object { ($null -ne $_.$ColName) -and
($_.$ColName -le $DateCutoff) }
```

```
  $IsTodayStr = ""
  If ((Get-Date).Date -eq ($DateCutoff).Date)
  {
    $IsTodayStr = "*"
  }
  return [PSCustomObject]@{
    Today              = $IsTodayStr
    Date              = $DateCutoff
    NumberOfVersionsAvailable    = $Dataset.Count - $VersionsExpired.Count
    NumberOfVersionsExpired     = $VersionsExpired.Count
    SizeOfVersionsExpiredInBytes  = ($VersionsExpired | Measure-Object Size
-Sum).Sum
  }
}
function Get-FilesWithFewerThanNVersions($Dataset, $NumVersions)
{
  $AvailableVersionsByFile = $Dataset `
    | Where-Object { ($null -eq $_.TargetExpirationDate) -or
($_.TargetExpirationDate -gt [DateTime]::Now) } `
    | Group-Object -Property WebId.Compact, DocId.Compact
  $AvailableFilesWithNotEnoughVersions = @{}
  # Files with some versions left but not enough
  $AvailableVersionsByFile `
    | Where-Object Count -lt $NumVersions `
    | ForEach-Object { $AvailableFilesWithNotEnoughVersions[$_.Name] =
$_.Count }
  # Files with 0 versions left
  $Dataset `
    | Group-Object -Property WebId.Compact, DocId.Compact `
    | Where-Object { $AvailableVersionsByFile.Name -notcontains $_.Name } `
    | ForEach-Object { $AvailableFilesWithNotEnoughVersions[$_.Name] = 0 }
  # Stitch all of the data together
  return $Dataset `
    | Group-Object -Property WebId.Compact, DocId.Compact `
    | Where-Object Count -ge $NumVersions `
    | Where-Object { $AvailableFilesWithNotEnoughVersions.Contains($_.Name)
} `
    | ForEach-Object `
      {
        $fileUrl = $_.Group[0]."WebUrl.Compact" + "/" +
$_.Group[0]."FileUrl.Compact"
        $numberOfVersionsAvailableBeforeTrim = $_.Count
        $numberOfVersionsAvailableAfterTrim =
$AvailableFilesWithNotEnoughVersions[$_.Name]
        $numberOfVersionsTrimmed = $numberOfVersionsAvailableBeforeTrim -
$numberOfVersionsAvailableAfterTrim
        [PSObject]::new() |
          Add-Member -PassThru -NotePropertyMembers ([Ordered]@{
            FileUrl = $fileUrl
            NumberOfVersionsAvailableBeforeTrim =
$numberOfVersionsAvailableBeforeTrim
            NumberOfVersionsAvailableAfterTrim =
$numberOfVersionsAvailableAfterTrim
            NumberOfVersionsTrimmed = $numberOfVersionsTrimmed
          })
```

```
      } `
    | Sort-Object -Property NumberOfVersionsAvailableAfterTrim
}
function Get-MostImpactedUsers($Dataset)
{
  $VersionsExpired = $Dataset | Where-Object { ($null -ne
$_.TargetExpirationDate) -and ($_.TargetExpirationDate -le [DateTime]::Now)
}
  return $VersionsExpired `
    | Group-Object -Property ModifiedBy_UserId.Compact `
    | Select-Object `
      @{ L = "UserId"; E = { $_.Group[0]."ModifiedBy_UserId.Compact" } }, `
      @{ L = "UserDisplayName"; E = {
$_.Group[0]."ModifiedBy_DisplayName.Compact" } },
      @{ L = "NumberOfVersionsTrimmed"; E = { $_.Count } } `
    | Sort-Object -Property NumberOfVersionsTrimmed -Descending
}
$Dataset = Import-Dataset -DatasetFilePath $ReportLocalFilePath
$CurrentExpirationSummaryTable = @()
$TargetExpirationSummaryTable = @()
$Timer = [Diagnostics.Stopwatch]::StartNew()
for ($Step = 0; $Step -lt $TimelineNumSteps; $Step++)
{
  $DateCutOff = $TimelineStartDate.AddDays($TimelineStepDays * $Step)
  $CurrentExpirationSummaryTable += `
    Get-NumVersionExpiresByDate -Dataset $Dataset -ColName
CurrentExpirationDate -DateCutoff $DateCutOff
  $TargetExpirationSummaryTable += `
    Get-NumVersionExpiresByDate -Dataset $Dataset -ColName
TargetExpirationDate -DateCutoff $DateCutOff
}
$Timer.Stop()
Write-Host "==========================" -ForegroundColor Yellow
Write-Host "Current Expiration Schedule" -ForegroundColor Yellow
Write-Host "==========================" -ForegroundColor Yellow
$CurrentExpirationSummaryTable | Format-Table -Autosize | Out-String |
Write-Host
Write-Host "Total elapsed seconds: $($Timer.Elapsed.TotalSeconds / 2)" -
ForegroundColor Green
Write-Host
Write-Host "=========================" -ForegroundColor Yellow
Write-Host "Target Expiration Schedule" -ForegroundColor Yellow
Write-Host "=========================" -ForegroundColor Yellow
$TargetExpirationSummaryTable | Format-Table -Autosize | Out-String | Write-
Host
Write-Host "Total elapsed seconds: $($Timer.Elapsed.TotalSeconds / 2)" -
ForegroundColor Green
Write-Host
Write-Host "================================" -ForegroundColor Yellow
Write-Host "Files with Fewer Than $ShowFilesWithFewerThanNVersions Versions"
-ForegroundColor Yellow
Write-Host "================================" -ForegroundColor Yellow
$Timer = [Diagnostics.Stopwatch]::StartNew()
Get-FilesWithFewerThanNVersions -Dataset $Dataset -NumVersions
$ShowFilesWithFewerThanNVersions | Format-Table -Autosize | Out-String |
```

```
Write-Host
$Timer.Stop()
Write-Host "Total elapsed seconds: $($Timer.Elapsed.TotalSeconds)" -
ForegroundColor Green
Write-Host
Write-Host "==============" -ForegroundColor Yellow
Write-Host "Users Impacted" -ForegroundColor Yellow
Write-Host "==============" -ForegroundColor Yellow
$Timer = [Diagnostics.Stopwatch]::StartNew()
Get-MostImpactedUsers -Dataset $Dataset | Format-Table -Autosize | Out-
String | Write-Host
$Timer.Stop()
Write-Host "Total elapsed seconds: $($Timer.Elapsed.TotalSeconds)" -
ForegroundColor Green
Write-Host
```

2. Open PowerShell and run the following command, replacing the placeholder values with the appropriate values.

> **Note**
>
> Use PowerShell 7 to run the commands. You can install PowerShell 7 by following these instructions: [Installing PowerShell on Windows - PowerShell | Microsoft Learn](#).

PowerShell

```
. “<path to AnalyzeReportFile.ps1>” –ReportLocalFilePath “<path to the file
version expiration What-If report .csv file>”
```

```
PS > . ".\AnalyzeReportFile.ps1" -ReportLocalFilePath “.\Report_WhatIf_Auto.csv”
Read 0 / 455 rows (0.0001718 sec elapsed, ETA: 0.0779972 sec).
Dataset imported!
```

3. The output displays four tables:

- **Current Expiration Schedule:** this table contains a time-series summary for your versions as they are. It has the following columns:

    1. **Date**: the first column represents the date.
    2. **NumberOfVersionsAvailable**: the number of versions available on that date under the current schedule.
    3. **NumberOfVersionsExpired**: the number of versions expired on that date under the current schedule.
    4. **SizeOfVersionsExpiredMB**: the size of versions expired on that date under the current schedule.

```
==========================
Current Expiration Schedule
==========================

Today Date                  NumberOfVersionsAvailable NumberOfVersionsExpired SizeOfVersionsExpiredMB
----- ----                  ------------------------- ----------------------- -----------------------
*     10/5/2023 2:20:38 PM                        455                       0                       0
      10/15/2023 2:20:38 PM                       455                       0                       0
      10/25/2023 2:20:38 PM                       455                       0                       0
      11/4/2023 2:20:38 PM                        455                       0                       0
      11/14/2023 2:20:38 PM                       455                       0                       0
      11/24/2023 2:20:38 PM                       455                       0                       0
      12/4/2023 2:20:38 PM                        455                       0                       0
      12/14/2023 2:20:38 PM                       455                       0                       0
      12/24/2023 2:20:38 PM                       455                       0                       0
      1/3/2024 2:20:38 PM                         455                       0                       0

Total elapsed seconds: 0.0300437
```

- **Target Expiration Schedule:** this table is the same as Current Expiration Schedule but reflects the updated schedule instead. This table is only helpful if you want to test out different expiration scenarios by changing the **TargetExpirationDate** column in the file version expiration report.

```
==========================
Target Expiration Schedule
==========================

Today Date                  NumberOfVersionsAvailable NumberOfVersionsExpired SizeOfVersionsExpiredMB
----- ----                  ------------------------- ----------------------- -----------------------
*     10/5/2023 2:20:38 PM                        199                     256                   21.94
      10/15/2023 2:20:38 PM                       191                     264                   22.34
      10/25/2023 2:20:38 PM                       183                     272                   22.93
      11/4/2023 2:20:38 PM                        176                     279                   23.60
      11/14/2023 2:20:38 PM                       165                     290                   24.30
      11/24/2023 2:20:38 PM                       162                     293                   24.52
      12/4/2023 2:20:38 PM                        162                     293                   24.52
      12/14/2023 2:20:38 PM                       162                     293                   24.52
      12/24/2023 2:20:38 PM                       162                     293                   24.52
      1/3/2024 2:20:38 PM                         156                     299                   25.73
```

- **Files with Fewer Than 10 Versions:** a list of the URLs, and the number of versions before and after the deletion for those files whose number of versions is fewer than 10 after immediate deletion (but was more than 10 before the immediate deletion).

```
==============================
Files with Fewer Than 10 Versions
==============================

FileUrl                                                      NumberOfVersionsAvailableBeforeTrim NumberOfVersionsAvailableAfterTrim NumberOfVersionsTrimmed
-------                                                      ----------------------------------- ---------------------------------- ----------------------
https://contoso.sharepoint.com/sites/SampleSite/SampleLibrary/26.txt                          12                                  1                     11
https://contoso.sharepoint.com/sites/SampleSite/SampleLibrary/28.txt                          23                                  1                     22
https://contoso.sharepoint.com/sites/SampleSite/SampleLibrary/36.txt                          10                                  1                      9
https://contoso.sharepoint.com/sites/SampleSite/SampleLibrary/33.txt                          24                                  2                     22
https://contoso.sharepoint.com/sites/SampleSite/SampleLibrary/18.txt                          18                                  4                     14
https://contoso.sharepoint.com/sites/SampleSite/SampleLibrary/30.txt                          25                                  4                     21
https://contoso.sharepoint.com/sites/SampleSite/SampleLibrary/22.txt                          19                                  5                     14
https://contoso.sharepoint.com/sites/SampleSite/SampleLibrary/5.txt                           10                                  9                      1

Total elapsed seconds: 0.0154765
```

- **Users Impacted:** the users whose versions would be immediately deleted.

```
==============
Users Impacted
==============

UserId UserDisplayName NumberOfVersionsTrimmed
------ --------------- -----------------------
     6 Alice                               250
    23 Dan                                   3
    25 Carol                                 3


Total elapsed seconds: 0.0065594
```

Optionally, you can adjust the parameters:

- `TimelineStartDate`: the starting date for Table 1 and 2 above.
- `TimelineStepDays`: the number of days in between rows for Table 1 and 2 above.
- `TimelineNumSteps`: the number of rows to calculate for Table 1 and 2 above.
- `ShowFilesWithFewerThanNVersions`: the threshold for the number of versions in Table 3 above.

Feedback

Was this page helpful? Yes No

Provide product feedback

Tutorial: Run 'What-If' analysis on version storage report file

Article • 10/03/2024

In this tutorial, we discuss how to leverage provided scripts and excel examples to understand the impact of applying either automatic or manual limits on version storage or impacted users. You will learn how to:

- Run impact analysis of setting Automatic limits.
- Run impact analysis of expiring versions older than specified days.
- Run impact analysis of storing version within specified count limits.

Before you begin

In the previous tutorial, you had generated a version storage usage report. This tutorial assumes that the report generation job has successfully completed and the report is fully populated.
Start by downloading the report file to your local computer. Use the scripts provided below to apply the desired setting on the file and analyze the impact.

Run impact analysis of setting automatic version history limits

Here's an example of PowerShell script you could apply to generate a What-If Report file that applies the **Automatic Expiration** policy on the report file `C:\Report.csv`.

PowerShell

```
# save this file as ScheduleUpdate_Auto.ps1

param (
  [Parameter(Mandatory=$true)][string]$ImportPath,
  [Parameter(Mandatory=$true)][string]$ExportPath
)

$Schedule = Import-Csv -Path $ImportPath
$Schedule |
  ForEach-Object {
    $_.TargetExpirationDate = $_.AutomaticPolicyExpirationDate
  }
```

```
$Schedule |
  Export-Csv -Path $ExportPath -UseQuotes AsNeeded -NoTypeInformation
```

> ⓘ **Note**
>
> Use PowerShell 7 to run the commands. You can install PowerShell 7 by following these instructions: [Installing PowerShell on Windows - PowerShell | Microsoft Learn](#).

```
. “<path to ScheduleUpdate_Auto.ps1>” -ImportPath “C:\Report.csv” -ExportPath
“C:\Report_WhatIf_Auto.csv”
```

```
PS > . ".\ScheduleUpdate_Auto.ps1" -ImportPath “.\Report.csv” -ExportPath “.\Report_WhatIf_Auto.csv”
```

Run impact analysis of setting manual expiration limits

Here's an example of PowerShell script to generate a What-If Report file. It applies **Manual Expiration** with expire-after days set to **30** on the report file `C:\Report.csv`.

PowerShell

```
# save this file as ScheduleUpdate_ExpireAfter.ps1

param (
  [Parameter(Mandatory=$false)][string]$ImportPath,
  [Parameter(Mandatory=$false)][string]$ExportPath,
  [Parameter(Mandatory=$false)][double]$ExpireAfter
)

function StringToDateTime($Value) { return [string]::IsNullOrEmpty($Value) ?
$null : [DateTime]::ParseExact($Value, "yyyy-MM-ddTHH:mm:ssK", $null) }
function DateTimeToString($Value) { return $null -eq $Value ? "" :
$Value.ToString("yyyy-MM-ddTHH:mm:ssK") }

$Schedule = Import-Csv -Path $ImportPath
$Schedule |
  ForEach-Object {
    $SnapshotDate = StringToDateTime -Value $_.SnapshotDate
    $TargetExpirationDate = $SnapshotDate.AddDays($ExpireAfter)
    $_.TargetExpirationDate = DateTimeToString -Value $TargetExpirationDate
  }
$Schedule |
  Export-Csv -Path $ExportPath -UseQuotes AsNeeded -NoTypeInformation
```

> **Note**
>
> Use PowerShell 7 to run the commands. You can install PowerShell 7 by following these instructions: [Installing PowerShell on Windows - PowerShell | Microsoft Learn.]

```
. “<path to ScheduleUpdate_ExpireAfter.ps1>” -ImportPath “C:\Report.csv” -
ExportPath “C:\Report_WhatIf_ExpireAfter.csv” -ExpireAfter 30
```

```
PS > . ".\ScheduleUpdate_ExpireAfter.ps1" -ImportPath “.\Report.csv” -ExportPath “.\Report_WhatIf_Expi
reAfter.csv” -ExpireAfter 30
```

Run impact analysis of setting manual count limits

Here's an example of PowerShell script to generate a What-If report file. It applies a **Manual with Count Limits** policy with major version limit set to **50** on the report file `C:\Report.csv`.

PowerShell

```
# save this file as ScheduleUpdate_Count.ps1

param (
  [Parameter(Mandatory=$true)][string]$ImportPath,
  [Parameter(Mandatory=$true)][string]$ExportPath,
  [Parameter(Mandatory=$true)][int]$MajorVersionLimit
)

$Report = Import-Csv -Path $ImportPath

$PreviousWebId = [Guid]::Empty
$PreviousDocId = [Guid]::Empty
$PreviousWebUrl = [string]::Empty
$PreviousFileUrl = [string]::Empty
$PreviousModifiedByUserId = [string]::Empty
$PreviousModifiedByDisplayName = [string]::Empty

$FileToVersions = @{}

foreach ($Version in $Report)
{
  $WebId = [string]::IsNullOrEmpty($Version."WebId.Compact") ?
$PreviousWebId : [Guid]::Parse($Version."WebId.Compact")
  $DocId = [string]::IsNullOrEmpty($Version."DocId.Compact") ?
$PreviousDocId : [Guid]::Parse($Version."DocId.Compact")
  $WebUrl = [string]::IsNullOrEmpty($Version."WebUrl.Compact") ?
```

```
$PreviousWebUrl : $Version."WebUrl.Compact"
  $FileUrl = [string]::IsNullOrEmpty($Version."FileUrl.Compact") ?
$PreviousFileUrl : $Version."FileUrl.Compact"
  $ModifiedByUserId =
[string]::IsNullOrEmpty($Version."ModifiedBy_UserId.Compact") ?
$PreviousModifiedByUserId : $Version."ModifiedBy_UserId.Compact"
  $ModifiedByDisplayName =
[string]::IsNullOrEmpty($Version."ModifiedBy_DisplayName.Compact") ?
$PreviousModifiedByDisplayName : $Version."ModifiedBy_DisplayName.Compact"

  $PreviousWebId = $WebId
  $PreviousDocId = $DocId
  $PreviousWebUrl = $WebUrl
  $PreviousFileUrl = $FileUrl
  $PreviousModifiedByUserId = $ModifiedByUserId
  $PreviousModifiedByDisplayName = $ModifiedByDisplayName

  if (($PreviousWebId -eq [Guid]::Empty) -or ($WebId -eq [Guid]::Empty) -or
    ($PreviousDocId -eq [Guid]::Empty) -or ($DocId -eq [Guid]::Empty))
  {
    throw "Compact column error."
  }

  $Version."WebId.Compact" = $WebId
  $Version."DocId.Compact" = $DocId
  $Version."WebUrl.Compact" = $WebUrl
  $Version."FileUrl.Compact" = $FileUrl
  $Version."ModifiedBy_UserId.Compact" = $ModifiedByUserId
  $Version."ModifiedBy_DisplayName.Compact" = $ModifiedByDisplayName

  if ($null -eq $FileToVersions[$DocId])
  {
    $FileToVersions[$DocId] =
[System.Collections.Generic.PriorityQueue[Object, Int32]]::new()
  }

  $VersionsQueue = $FileToVersions[$DocId]

  $VersionNumber = [Int32]::Parse($Version.MajorVersion) * 512 +
[Int32]::Parse($Version.MinorVersion)
  $VersionsQueue.Enqueue($Version, -$VersionNumber)
}

$Schedule = [System.Collections.Generic.List[Object]]::new()

foreach ($FilesAndVersions in $FileToVersions.GetEnumerator())
{
  $VersionsQueue = $FilesAndVersions.Value
  $NumMajorVersionsSeen = 0
  while ($VersionsQueue.Count -gt 0)
  {
    $Version = $VersionsQueue.Dequeue()
    if ($NumMajorVersionsSeen -ge $MajorVersionLimit) {
      $Version.TargetExpirationDate = [DateTime]::new(2000, 1,
1).ToString("yyyy-MM-ddTHH:mm:ssK")
```

```
    }

    if ([int]::Parse($Version.MinorVersion) -eq 0) { $NumMajorVersionsSeen++
}

    $Schedule.Add($Version)
  }
}

$Schedule |
  Export-Csv -Path $ExportPath -UseQuotes AsNeeded -NoTypeInformation
```

> **Note**
>
> Use PowerShell 7 to run the commands. You can install PowerShell 7 by following these instructions: [Installing PowerShell on Windows - PowerShell | Microsoft Learn](#).

```
. "<path to ScheduleUpdate_Count.ps1>" -ImportPath "C:\Report.csv" -
ExportPath "C:\Report_WhatIf_Count.csv" -MajorVersionLimit 50
```

```
PS > . ".\ScheduleUpdate_Count.ps1" -ImportPath ".\Report.csv" -ExportPath ".\Report_WhatIf_Count.csv"
 -MajorVersionLimit 50
```

```
> . ".\OptimizeScheduleFile.ps1" -ImportPath ".\Schedule.csv" -ExportPath ".\Schedule_Optimized.csv"
```

Feedback

Was this page helpful? Yes No

Provide product feedback

Tutorial: Manage version history limits for a site, library, or OneDrive account

Article • 10/03/2024

In this tutorial, you will learn how to manage the version history limits for a site, document library, or OneDrive account. You will learn how to:

- Set Version history limits settings on the site.
- Stop an in-progress settings update job.

Before you begin

- Review your **organization's recovery objectives** and **version storage use quota targets** along with the **site-specific version storage needs** to evaluate if a break of inheritance of version settings at site, library, or OneDrive account level is needed.

- If needed **run an impact analysis** with the desired setting, to understand the impact the new setting would have using current version storage usage patterns.

- For setting site level version limits, evaluate the scope of document libraries that should be updated. Depending on business need, you can choose one of the following:
  - Update new libraries only without impacting existing library settings.
  - Update existing libraries only and inherit organization default settings for new libraries.
  - Update both existing and all new libraries for consistent version storage at the site level.

Set version limits for a site

You can set version limits on a site by running the Set-SPOSite command to break inheritance from the organization version history limits.

- Use the `-ApplyToNewDocumentLibraries` parameter to apply the changes only to new libraries created in the site.

- Use the `-ApplyToExistingDocumentLibraries` to only update the Version history limits on existing libraries on a site. Any new library created inherits the default organization limits.

Example: Apply automatic version history limits to all document libraries on a site

Run the following commands to **apply Automatic setting** to all document libraries on a site.

PowerShell

```
Set-SPOSite -Identity https://contoso.sharepoint.com/sites/site1 -
EnableAutoExpirationVersionTrim $true
```

Example: Apply automatic version history limits to new document libraries on a site

In the following example, Automatic Version history limits are applied to all new document libraries created on the site. The settings on existing libraries will not be impacted.

PowerShell

```
 Set-SPOSite -Identity https://contoso.sharepoint.com/sites/site1 -
EnableAutoExpirationVersionTrim $true -ApplyToNewDocumentLibraries
```

Example: Apply manual setting with count and time version history limits to existing libraries only on a site

In the following example, Version history limits of all existing libraries on a site are updated to Manual Version history limits.

PowerShell

```
Set-SPOSite -Identity https://contoso.sharepoint.com/sites/site1 -
EnableAutoExpirationVersionTrim $false -MajorVersionLimit 500 -
ExpireVersionsAfterDays 30 -ApplyToExistingDocumentLibraries
```

Cancel an in-progress request to update version history limits on existing libraries

If required, you can cancel the update job that is currently `<InProgress>` using the `Remove-SPOSiteVersionPolicyJob`.

> **Note**
>
> Cancelling the job doesn't revert the change for document libraries where the update is already processed.

In the example below, the in-progress job to update settings on site will be stopped.

PowerShell

```
Remove-SPOSiteVersionPolicyJob -Identity
https://contoso.sharepoint.com/sites/site1
```

Learn More

- Track progress of version settings update request for existing document libraries on a site using Get-SPOSiteVersionPolicyJobProgress.
- Cancel further processing of version settings update on existing document libraries on the site collection using Remove-SPOSiteVersionPolicyJob.

Feedback

Was this page helpful? Yes No

Provide product feedback

Tutorial: Queue a trim job for a site or document library

Article • 10/03/2024

In this tutorial, you'll learn how to trim existing versions from a site or library by queuing a trim job using PowerShell. You'll learn how to:

- Queue a job to trim versions from a site.
- Queue a job to trim versions from a library.
- Check progress of your trim job.
- Stop an in-progress trim job.

Before you begin

Versions deleted by a trim job are permanently deleted and can't be recovered from the recycle bin. We recommend you prepare by performing the following actions:

- Review your **organization's recovery objectives** and **version storage usage quota targets** to help determine the trim action and scope needed to meet your requirements.

- If needed, run an impact analysis to understand the trimming impact.

- Determine the **scope of** version deletion. You can create jobs to delete old file versions for all document libraries in a site or for a specific document library.

- Determine the **trim mode** you want to apply on existing versions. You can choose to delete based on version age, count limit, or based on the automatic algorithm.

Queue a job to trim versions on site

You can queue a job to trim versions for all document libraries in the site collection using the `New-SPOSiteFileVersionBatchDeleteJob` PowerShell command.

- Use the `<DeleteBeforeDays>` parameter to specify the age criteria you wish to apply for deleting versions. Versions older than the specified days are deleted asynchronously in batches in the upcoming days.
- Use the `<MajorVersionLimit>` to specify the count limit of major versions to store. Oldest versions exceeding the specified count are deleted asynchronously in batches in the upcoming days.

- Use the `<Automatic>` parameter to apply Automatic setting trimming logic on existing file versions.

Example: Queue a job to trim versions based on age for all libraries on a site

In the following example, the job is queued to trim versions that are older than 180 days for all document libraries in the site collection `https://contoso.sharepoint.com/sites/site1`.

PowerShell

```
New-SPOSiteFileVersionBatchDeleteJob -Identity
https://contoso.sharepoint.com/sites/site1 -DeleteBeforeDays 180
```

Example: Queue a job to trim oldest versions exceeding the specified count limit on a site

In the example below, the job is queued to trim oldest versions that exceed 100 major version count limit for all document libraries in the site collection `https://contoso.sharepoint.com/sites/site1`.

PowerShell

```
New-SPOSiteFileVersionBatchDeleteJob -Identity
https://contoso.sharepoint.com/sites/site1 -MajorVersionLimit 100 -
MajorWithMinorVersionsLimit 0
```

Example: Queue a job to trim versions based on the automatic logic on a site

In the example below, the job is queued to trim versions based on the Automatic algorithm for all document libraries in the site collection `https://contoso.sharepoint.com/sites/site1`.

PowerShell

```
New-SPOSiteFileVersionBatchDeleteJob -Identity
https://contoso.sharepoint.com/sites/site1 -Automatic
```

Queue a job to trim versions on a document library

You can queue a job to trim versions from a particular document library in the site collection using the `New-SPOListFileVersionBatchDeleteJob` PowerShell command.

- Use the `<DeleteBeforeDays>` parameter to specify the age criteria you wish to apply for deleting versions. Versions older than the specified days are asynchronously in batches in the upcoming days.
- Use the `<MajorVersionLimit>` to specify the count limit of major versions to store. Oldest versions exceeding the specified count are deleted asynchronously in batches in the upcoming days.
- Use the `<Automatic>` parameter to apply Automatic setting trimming logic on existing file versions.

Example: Queue a job to trim versions based on age on a single library on a site

To delete versions that are older than 360 days in document library 'Documents' in the site collection `https://contoso.sharepoint.com`.

PowerShell

```
New-SPOListFileVersionBatchDeleteJob -Site https://contoso.sharepoint.com -
List "Documents" -DeleteBeforeDays 360
```

Track progress of a trim job

You can track progress of the trim job using the `Get-SPOSiteFileVersionBatchDeleteJobProgress` cmdlet.

In the following example, the cmdlet reports the progress of the trim job for `https://contoso.sharepoint.com/sites/site1`

PowerShell

```
Get-SPOSiteFileVersionBatchDeleteJobProgress -Identity
https://contoso.sharepoint.com/sites/site1
```

Stop an in-progress trim job

If needed, you can cancel an in-progress trim job. Once the cmdlet executes successfully, the in-progress job is stopped and no further deletions happen.

> **Note**
>
> Stopping a trim job doesn't revert versions that have already been deleted.

Example: Stop a site trim job

To stop an in-progress trim job from additional version trimming on the site collection `https://contoso.sharepoint.com/sites/site1`:

PowerShell

```
Remove-SPOSiteFileVersionBatchDeleteJob -Identity
https://contoso.sharepoint.com/sites/site1
```

Example: Stop a library trim job

To stop an in-progress trim job from additional version trimming in document library 'Documents' in site collection `https://contoso.sharepoint.com/sites/site1`:

PowerShell

```
Remove-SPOListFileVersionBatchDeleteJob -Site
https://contoso.sharepoint.com/sites/site1 -List "Documents"
```

Feedback

Was this page helpful? Yes No

Provide product feedback

FAQs

Article • 02/26/2025

What happens to versions that are deleted, have expired, or exceeded the count limits?

When a user deletes a previous version of an item or a file in SharePoint (microsoft.com), SharePoint moves versions into the recycle bin. Users are able to restore deleted versions from the site collection recycle bin (microsoft.com).

Versions trimmed by the Automatic setting or when a version's age exceeds the manual time limits, are tagged for permanent deletion. They aren't available for restoration from the recycle bin once purged.

> **Note**
>
> Background timer jobs permanently purge expired versions and this process may take a couple of days from the actual expiration date.

Versions that exceed count limits are gradually trimmed when the file is updated. Each file update triggers approximately 20 version deletions until the count limits are met.

How do legal holds or retention policies impact version deletions or expirations?

When a site is on hold or a document with versions is subject to retention settings, the configured retention setting determines the retention of versions. In other words, the retention setting always wins, whether it's a deletion or hold policy. Learn about retention for SharePoint and OneDrive.

When a trim job encounters a version under a retention policy or an eDiscovery hold, it will stamp an expiration date on the version instead of deleting it. Once the expiration date is reached:

- if the retention policy or eDiscovery hold is still in effect for the version, the expiration date is extended;
- if the retention policy or eDiscovery hold has been lifted for the version, the version is deleted.

What happens when organization level or library level version settings are updated?

When **organization-level version settings are updated**, the new settings are applied to all new libraries created since the change was made. The new settings don't apply to existing libraries or versions already created.

When **library-level version expiration setting is updated**, the new expiration limit is applied to newly created versions only. Take an example of a library with version expiration settings updated from **Never Expire** to **Expire after six months**. The newly created versions are set to expire after six months with no impact on previously created versions.

When **library-level count limits are updated**, if existing versions exceed the new count limit, then those versions are gradually trimmed when the file is updated. Take an example of a library with count limits set to 500 versions, was reduced to 300 versions. If you had a file with 500 versions, every time a user updates the file, the oldest 20 versions are purged until you are at the right number of versions.

How will automatic setting impact ability to restore a library or OneDrive?

When **Automatic setting** is selected, users have access to a maximum of 500 versions created within the last 30 days enabling the user to Restore a shared library or Restore your OneDrive.

Feedback

Was this page helpful? Yes No

Provide product feedback

Version history overview

The Version History feature is an integral part of Microsoft's 365 built-in data protection in SharePoint and OneDrive. An item or file's version history lets a user see or restore to a previous version, helpful for undoing unintended changes, whether accidental or due to malicious activities like ransomware. It also ensures auditability to meet an organization's legal and audit requirements.

Users can use version history to:

- **View a previous version**: Users can view a previous version without overwriting their current version. During a review of the version history within a Microsoft Office document, such as a Word or Excel file, versions can be compared to determine what the differences are.
- **Restore to a previous version**: If a user makes a mistake in a current version, the current version gets corrupted, or if they simply like a previous version better, they can replace the current version with a previous one. The restored version becomes the new current version. Learn more Restore a previous version of an item or file in SharePoint.
- **Track history of a file or item**: Users can use version history to see when a file or an item was changed and identify who made the changes.

Last updated on 06/25/2026

Prevent guest access to files while DLP rules are applied

Article • 02/24/2025

> **Note**
>
> Any user whose usertype is member are considered internal and users with member type Guest are only considered external.

When new files are added to SharePoint or OneDrive in Microsoft 365, it takes a while for Microsoft Purview Data Loss Prevention (DLP) policy to scan the content and apply rules to help protect sensitive content. If external sharing is turned on, sensitive content could be shared and accessed by guests before the DLP rule finishes processing.

Instead of turning off external sharing entirely, you can mark the files in your organization as sensitive by default. This blocks guest access to new content until it's scanned for sensitive content and DLP policies that include content-based conditions are applied. Guests are notified that the file is being scanned if they attempt to access it during this time.

Once a file is crawled and no content that would block sharing per DLP rules is detected, guests can access the file. If the policy identifies sensitive content in the document that matches DLP rules, the normal behavior defined by those DLP rules is applied.

This feature doesn't block access to a file if:

- the content has already been crawled and no sensitive content was found that matches the conditions in any DLP rules,
- or if the file has properties that match exemptions in DLP rules that allow it to be shared.

This feature applies to newly added files in SharePoint and OneDrive. It doesn't block sharing if an existing file is changed.

DLP rules are required for content to be shared with guests

When this feature is enabled, any content that isn't explicitly checked in a DLP policy is blocked from being externally accessed. In other words, for content to be shareable

externally, it must be in a location that's covered by a DLP policy and the policies for that location must determine, after content has been crawled and identified, that the file doesn't match any rules that would prevent it from being shared. This helps prevent users from leaking sensitive files by placing them in a location not covered by DLP policies.

If you want to operate under the principle that only locations explicitly checked by DLP can be shared externally, no further action is necessary.

If you want to enable external sharing in locations not currently covered by DLP policies, you can create a DLP rule that includes all SharePoint and OneDrive locations that contain at least one rule with the "content contains" condition (for any content), and that doesn't perform any action (such as limiting or blocking the content), trigger any alerts, or generates any notifications or reports. This policy must be moved to the top of the list and not have the *stop processing more rules* option set, so it's only effective for content that doesn't match any other DLP rule. As a result of such a rule, any file in any location that doesn't match other DLP rules will be allowed for external sharing.

For information about how to create a DLP rule, see Learn how to create and turn on a DLP policy.

Mark files as sensitive by default

This feature is configured using PowerShell.

1. Download the latest SharePoint Online Management Shell.

   > **Note**
   >
   > If you installed a previous version of the SharePoint Online Management Shell, go to **Add or remove programs** and uninstall "SharePoint Online Management Shell."

2. Connect to SharePoint as a SharePoint Administrator or above in Microsoft 365. To learn how, see Getting started with SharePoint Online Management Shell.

3. Run the following command:

   PowerShell

   ```
   Set-SPOTenant -MarkNewFilesSensitiveByDefault BlockExternalSharing
   ```

To disable this feature, run the following command:

```
PowerShell
Set-SPOTenant -MarkNewFilesSensitiveByDefault AllowExternalSharing
```

> **Note**
>
> It might take up to 60 minutes for this new setting to take effect.

Feedback

Was this page helpful? Yes No

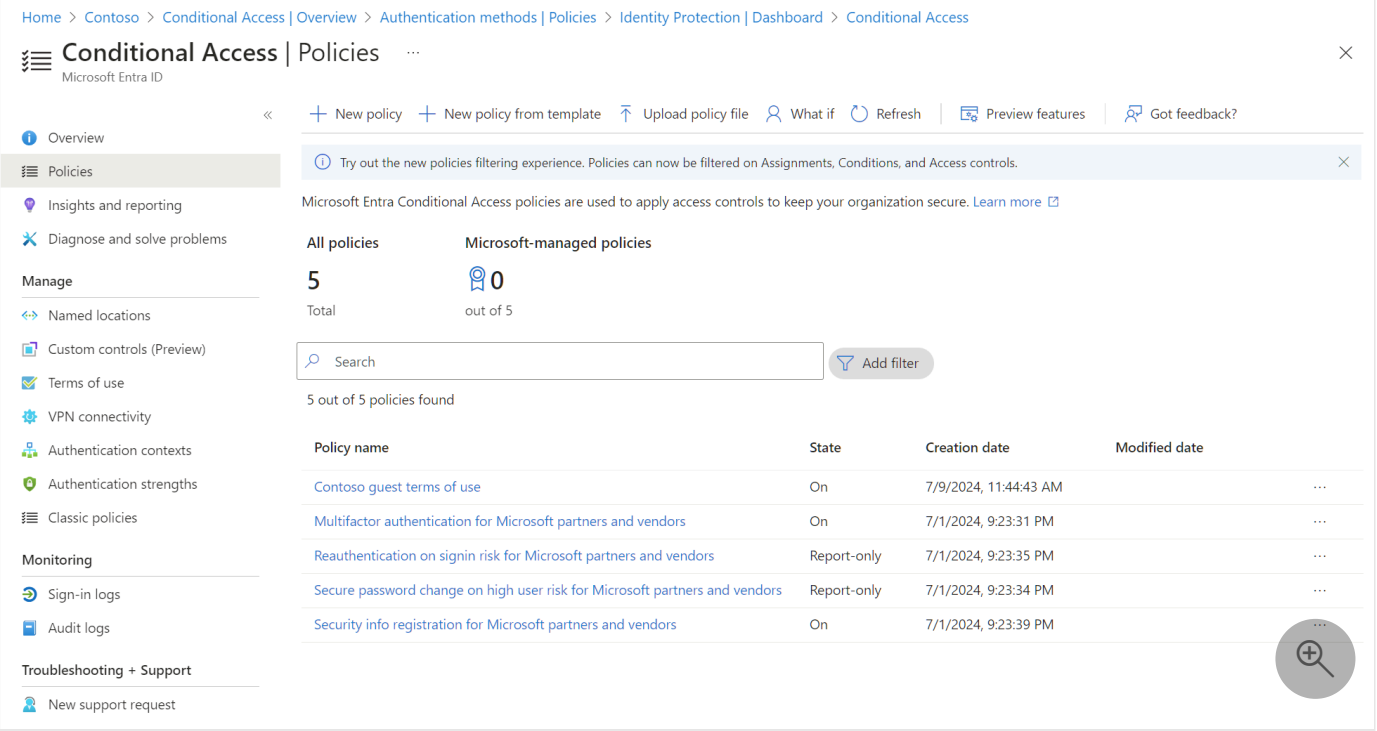
Provide product feedback

Conditional Access policies and SharePoint

By using Microsoft Entra authentication context, you can enforce more stringent access conditions when users access SharePoint sites.

Use authentication contexts to connect an Microsoft Entra Conditional Access policy to a SharePoint site. You can apply policies directly to the site or apply them through a sensitivity label.

You can't apply this capability to the root site in SharePoint (for example, https://contoso.sharepoint.com).



Before you begin

Review the SharePoint Advanced Management prerequisites.

In addition, you need one of the following licenses:

- Microsoft 365 E5/A5 Compliance
- Microsoft 365 E5 Information Protection and Governance

Limitations

Some apps don't work with authentication contexts. Test apps on a site with authentication context enabled before broadly deploying this feature.

The following apps and scenarios don't work with authentication contexts:

- Older versions of Office apps (see the list of supported versions)
- SharePoint mobile apps (iOS and Android)
- Viva Engage
- You can't add the OneNote app to a channel if the associated SharePoint site has an authentication context.
- Teams channel meeting recording upload fails on sites with an authentication context.
- SharePoint folder renaming in Teams fails if the site has an authentication context.
- Teams webinar scheduling fails if OneDrive has an authentication context.
- The OneDrive sync app won't sync sites with an authentication context.
- Associating an authentication context to the enterprise application catalog site collection isn't supported.
- The "Visualize SharePoint List in Power BI" feature doesn't currently support authentication context.
- Outlook on Windows, Mac, Android, and iOS don't support communication with SharePoint sites protected by an Authentication Context.
- The multiple-file download feature currently doesn't function when both the authentication context and 'Use Conditional Access App Control' in session control are enabled in the conditional access policy.
- The multiple-file download feature won't work if an authentication context is set directly on a SharePoint site without an active Conditional Access policy using that context, or if the policy exists but is disabled.
- The file copy and move feature between different regions (cross-geo) currently doesn't function when an authentication context is applied to the destination site.
- Exporting to Excel as an Excel Web Query (IQY) doesn't currently support authentication context.
- Recording or running a script using Office Scripts in Excel for the Web fails if OneDrive has an authentication context.

Set up an authentication context

To set up an authentication context for labeled sites, complete these basic steps:

1. Add an authentication context in Microsoft Entra ID.

2. Create a Conditional Access policy that applies to that authentication context and has the conditions and access controls that you want to use.

3. Do one of the following steps:

   a. Set a sensitivity label to apply the authentication context to labeled sites.

   b. Apply the authentication context directly to a site.

In this article, you see the example of requiring guests to agree to a terms of use before gaining access to a sensitive SharePoint site. You can also use any of the other conditional access conditions and access controls that you might need for your organization.

Add an authentication context

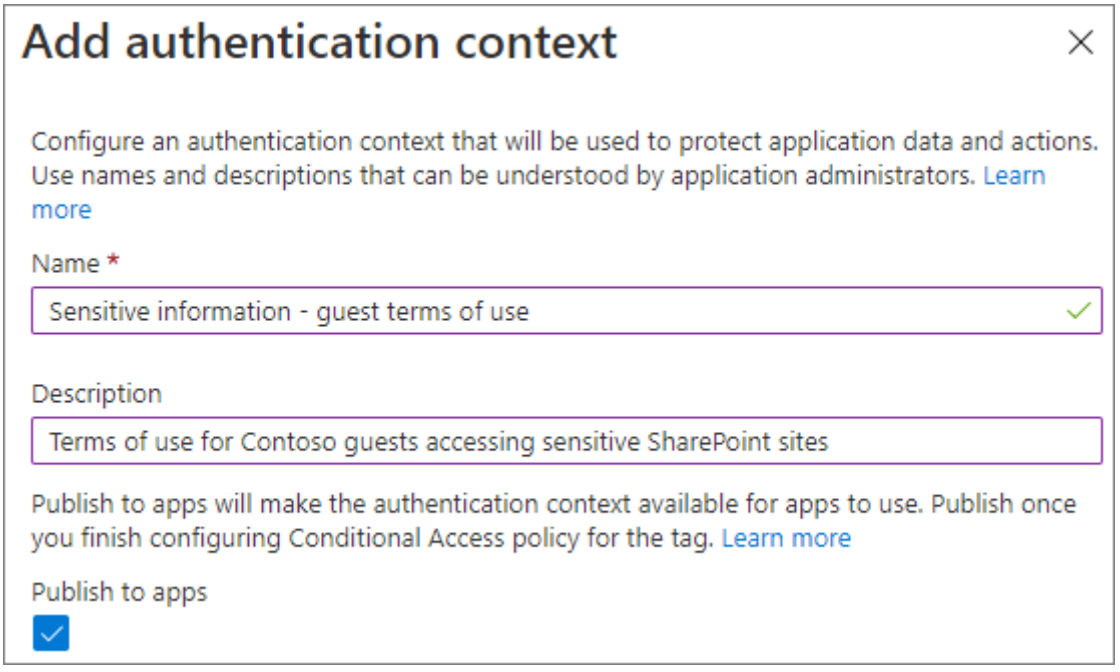
First, add an authentication context in Microsoft Entra ID.

To add an authentication context:

1. In Microsoft Entra Conditional Access, under **Manage**, select **Authentication context**.

2. Select **New authentication context**.

3. Type a name and description, and select the **Publish to apps** check box.



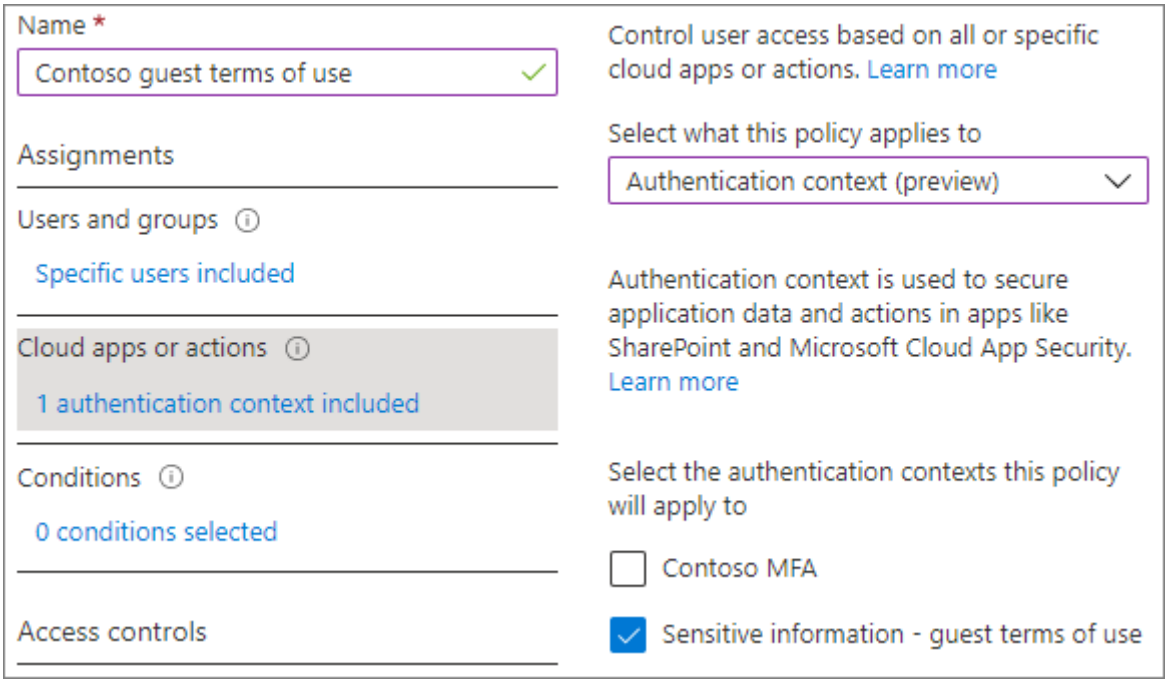
4. Select **Save**.

Create a Conditional Access policy

Next, create a Conditional Access policy that applies to that authentication context and requires guests to agree to terms of use as a condition of access.

To create a Conditional Access policy:

1. In Microsoft Entra Conditional Access, select **New policy**.
2. Enter a name for the policy.
3. On the **Users and groups** tab, choose the **Select users and groups** option, and then select the **Guest or external users** check box.
4. Choose **B2B collaboration guest users** from the dropdown.
5. On the **Cloud apps or actions** tab, under **Select what this policy applies to**, choose **Authentication context**, and select the check box for the authentication context that you created.



6. On the **Grant** tab, select the check box for the terms of use that you want to use, and then select **Select**.
7. Choose if you want to enable the policy, and then select **Create**.

Apply the authentication context directly to a site

You can directly apply an authentication context to a SharePoint site by using the Set-SPOSite PowerShell cmdlet.

> **Note**
>
> This capability requires a Microsoft 365 E5 or Microsoft SharePoint Advanced Management license.

In the following example, you apply the authentication context you created earlier to a site called "research."

PowerShell

```
Set-SPOSite -Identity https://contoso.sharepoint.com/sites/research -
ConditionalAccessPolicy AuthenticationContext -AuthenticationContextName "Sensitive
information - guest terms of use"
```

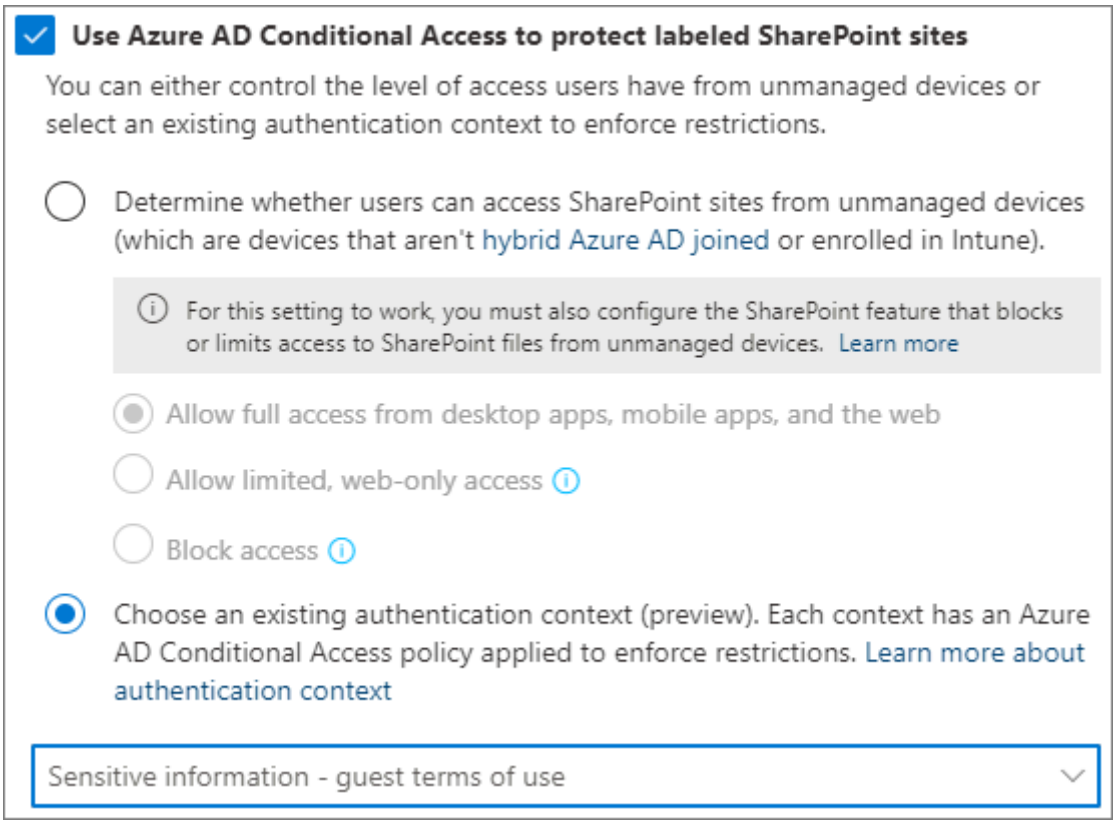
Set a sensitivity label to apply the authentication context to labeled sites

If you want to use a sensitivity label to apply the authentication context, update a sensitivity label (or create a new one) to use the authentication context.

> **Note**
>
> Sensitivity labels require Microsoft 365 E5 or Microsoft 365 E3 plus the Advanced Compliance license.

To update a sensitivity label

1. In the Microsoft Purview portal, on the **Information protection** tab, select the label that you want to update and then select **Edit label**.
2. Select **Next** until you are on the **Define protection settings for groups and sites** page.
3. Ensure that the **External sharing and Conditional Access settings** check box is selected, and then select **Next**.
4. On the **Define external sharing and device access settings page**, select the **Use Microsoft Entra Conditional Access to protect labeled SharePoint sites** check box.
5. Select the **Choose an existing authentication context** option.
6. In the dropdown list, choose the authentication context that you want to use.



7. Select **Next** until you are on the **Review your settings and finish** page, and then select **Save label**.

After you update the label, guests accessing a SharePoint site (or the **Files** tab in a team) with that label must agree to the terms of use before gaining access to that site.

Block background apps

If you set authentication context on a site, admins can choose to prevent background apps from accessing that site for the apps assigned with that authentication context in a Conditional Access policy. You can configure a Conditional Access policy such that a specific authentication context can be assigned to chosen application principals (non-Microsoft applications). You need to explicitly turn on this feature by using the following cmdlet. You should have at least one Conditional Access policy with an application principal configured.

PowerShell

```
Set-SPOTenant -BlockAppAccessWithAuthenticationContext $false/$true (default false)
```

Third-party app integration

Third-party apps that use sites with authentication context attached need to be able to handle claims challenge. See Developer guide to Conditional Access authentication context.

See also

Use sensitivity labels to protect content in Microsoft Teams, Microsoft 365 groups, and SharePoint sites

Conditional Access: Cloud apps, actions, and authentication context

Microsoft 365 licensing guidance for security & compliance

Last updated on 07/28/2026

Privacy, security, and compliance in Microsoft OneDrive

Microsoft is transparent about the specific policies, operational practices, and technologies that help you ensure the privacy, security, and compliance of your data across Microsoft OneDrive.

- Microsoft respects the privacy and ownership of data you use to train and process models in Microsoft OneDrive.
- None of your organization's data is used or transferred by Microsoft to train AI models, large-language models, or any other models.
- Your data remains securely within your organization's tenant.

Privacy

Privacy is built into all Microsoft OneDrive experiences. Microsoft OneDrive services adhere to the Microsoft Privacy Statement and follow Microsoft's compliance with General Data Protection Regulation and the Microsoft EU Data Boundary.

Microsoft OneDrive inherits privacy features and settings from Microsoft 365 and SharePoint, where applicable.

GDPR compliance

Microsoft OneDrive supports compliance with General Data Protection Regulation (GDPR) requirements.

Data residency

Data residency refers to the geographic location where data is stored at rest. The way that data is transferred and stored in Microsoft OneDrive is defined in the Microsoft Products and Services Data Protection Addendum (DPA).

All data within Microsoft OneDrive is stored within the customer tenant for any given service and follows the standard Microsoft 365 data storage guidelines by available geography.

Security

Microsoft OneDrive works with and integrates into Microsoft 365. This means that the Microsoft 365 security capabilities—such role-based access, identity and app management, and others—apply to Microsoft OneDrive.

Compliance

Microsoft offers a comprehensive set of compliance offerings to help your organization comply with national, regional, and industry-specific requirements governing the collection and use and data.

Microsoft OneDrive is also covered under the Microsoft Product Terms and Data Protection Agreement (DPA). Learn more on the Microsoft Trust Center.

For more detailed information, see the following resources:

- **Microsoft 365** – Microsoft Purview risk and compliance solutions
- **Microsoft SharePoint** – Plan compliance requirements for SharePoint and OneDrive
- **Microsoft Graph** – Use the Microsoft Graph compliance and privacy APIs
- **Microsoft Entra ID** – Microsoft Entra security baseline for Microsoft Entra ID
- **Azure** – Azure, Dynamics 365, Microsoft 365, and Power Platform compliance offerings

---

Last updated on 05/18/2026

Manage unlicensed OneDrive user accounts

As an IT administrator, you might encounter situations where some of your users have unmanaged and unlicensed OneDrive accounts within your organization. Unlicensed OneDrive accounts can pose security and compliance risks, as well as create confusion and duplication of files.

In this article, you learn how to identify, monitor, and manage unlicensed OneDrive accounts in your organization. To change how long these accounts stay active before they are archived, or to keep a reactivated account active beyond the ordinary 30-day window, see Standard storage for unlicensed OneDrive accounts.

Enforcement of policy changes for unlicensed OneDrive accounts

Unlicensed OneDrive accounts are automatically put into read-only mode after 60 unlicensed days and archived after 93 unlicensed days. While read-only and archived accounts remain visible to admins through administrative tools, neither admins nor end users have access to their content unless an admin takes a supported action such as assigning a license, enabling applicable billing, reactivating archived content, or moving content that must be retained.

As of July 1, 2026, unlicensed OneDrive accounts that remain unpaid are subject to a cumulative 365-day nonpayment clock. Accounts that were already unlicensed before July 1, 2026 are in scope, and accounts that become unlicensed on or after July 1, 2026 are also in scope. For accounts already unlicensed and unpaid on July 1, 2026, deletion risk begins no earlier than July 1, 2027. For accounts that become unlicensed after July 1, 2026, deletion risk begins when the account reaches 365 cumulative unpaid days.

An unpaid account is an unlicensed OneDrive account that isn't covered by an applicable paid license or billing/storage option.

> **Note**
>
> These changes don't apply to EDU, GCC, or DoD customers.

Unlicensed OneDrive accounts linked to a user account deleted in Entra ID. These accounts are removed following the standard OneDrive deletion process. This process honors retention

mechanisms in the following order when billing is enabled for unlicensed OneDrive accounts:

1. OneDrive retention period
2. Retention policies
3. Legal holds

After all applicable retention mechanisms are honored, the account is recycled and then permanently deleted.

Unlicensed OneDrive accounts linked to a user account that has not been deleted in Entra ID. These accounts are archived on their 93rd unlicensed day. If the account remains unlicensed and unlicensed account billing isn't enabled, it's subject to the cumulative 365-day nonpayment clock for deletion.

Timeline for unlicensed accounts

Expand table

Milestone	Expected state
Day 1	For accounts already unlicensed and unpaid on July 1, 2026, the cumulative nonpayment clock begins on July 1, 2026. For accounts that become unlicensed after July 1, 2026, the clock begins on the date the license is removed or the user is deleted in Entra ID.
Day 60	The account is placed in read-only mode.
Day 93	The account is archived or moved to the recycle bin depending on account and retention state.
Day 275	The account is no longer available in eDiscovery.
Day 365	The account is subject to deletion after 365 cumulative unpaid days.

The following examples show the earliest deletion-risk date for accounts that remain unpaid:

Expand table

Account unlicensed date	Earliest deletion-risk date
January 1, 2026	July 1, 2027
July 1, 2026	July 1, 2027
August 1, 2026	August 1, 2027

Admins are encouraged to monitor account statuses based on these timelines to ensure compliance and take any necessary actions.

These timelines reflect the default tenant settings. If your organization needs a longer active period before archiving, you can change the tenant-wide active-storage period. For more information, see Standard storage for unlicensed OneDrive accounts.

Unlicensed OneDrive account management options

After you identify the unlicensed OneDrive account, you can choose to license or delete the account.

Assign license to unlicensed OneDrive account

Before the unlicensed OneDrive account is archived - To assign a license to an unlicensed OneDrive account, assign a Microsoft 365 or Office 365 subscription to the user that includes OneDrive. When you assign a license, the user can access their OneDrive files with their work or school account, and you can manage their settings and policies.

You can also bulk assign licenses by using either of the following methods:

- Assign licenses to user accounts in the Microsoft 365 admin center
- Assign licenses to user accounts with PowerShell

After the unlicensed OneDrive account is archived - If the archived account has an associated user as the owner (also known as the *primary site collection administrator*), the IT admin can give the user a valid license and the account is automatically reactivated within 24 to 48 hours. Adding a license, such as through the Microsoft 365 admin center, doesn't incur a reactivation fee and doesn't require billing to be enabled for the account to be automatically reactivated for the user that has a license. If the archived account doesn't have an associated user (for example, if the identity was deleted), then we recommend admins move any actively needed content to a SharePoint site or an active and licensed OneDrive account. If the account is already archived and doesn't have an associated user, then the account needs to be reactivated before that data can be moved. For more information about licensing and active users in Microsoft 365, see Assign or unassign licenses for users in the Microsoft 365 admin center.

Delete unlicensed OneDrive account

Before the unlicensed OneDrive account is archived - To delete an unlicensed OneDrive account, remove the user from your organization and delete their data. You can use the Microsoft 365

admin center, PowerShell, or the Microsoft Graph API to permanently delete the user.

When you delete the unlicensed account, both the OneDrive account and its files move to the recycle bin. After 93 days in the recycle bin, the account is permanently deleted, and the user can no longer sign in to their work or school account.

After the unlicensed OneDrive account is archived - You can delete an account from the archived state without reactivation. However, if the account is subject to a retention policy, you can't delete the unlicensed account, and the administrator receives an error message.

Archive unlicensed OneDrive account

If you don't take action, the account remains archived through Microsoft 365 Archive. When you archive the account, you keep the OneDrive account and its data for long periods in case you need to retrieve it later.

For newly unlicensed OneDrive accounts, archiving occurs after 93 days of the license removal or user deletion. For example, a OneDrive account that became unlicensed on August 1, 2025, is inaccessible to users as of November 2, 2025.

To archive accounts later than the default 93 days, use the tenant-wide active-storage period described in Standard storage for unlicensed OneDrive accounts.

Access unlicensed OneDrive account

Accessing an Archived OneDrive Account:

- To access data from an archived OneDrive account, reactivation is required. Follow these prerequisites to set up Microsoft 365 Archive:

    1. Set up and link an Azure subscription in pay-as-you-go.
    2. Ensure you have Global admin or SharePoint admin permissions.
    3. Enable Microsoft 365 Archive Unlicensed Account billing (available starting December 2024).

    After completing the setup and triggering reactivation, it may take up to 24 hours for the account to become accessible. Once reactivated, the account remains active for 30 days before being automatically archived again. To keep a reactivated account active beyond 30 days, see Standard storage for unlicensed OneDrive accounts.

Accessing a Read-Only OneDrive Account:

- If the OneDrive account has been set to read-only, administrators have multiple options to access the content:
  - Add a license
  - Use PowerShell to unlock the site

> ⓘ **Note**
>
> These changes don't apply to EDU, GCC, or DoD customers.

Reporting

Unlicensed OneDrive accounts aren't associated with a Microsoft 365 or Office 365 subscription in your organization. A OneDrive account can become unlicensed when the licensing isn't activated or is expired.

You can also encounter unlicensed OneDrive accounts when accounts are created, but aren't assigned a license. Monitoring unlicensed accounts can help you determine the risk of these accounts, and plan for migration or deletion of user accounts.

Get unlicensed OneDrive users report

You can identify unlicensed OneDrive accounts using the SharePoint admin center. The following steps show how to use the SharePoint admin center to generate a report of unlicensed OneDrive accounts:

1. Sign in to the SharePoint admin center with your work or school account.
2. Go to **Reports** and select **OneDrive Accounts**.
3. You can download the report as a CSV file.
4. Starting January 2025, an interactive UI is available. You can select a username to view the details.

   The report shows the username, email address, account type, and last activity date of each unlicensed OneDrive account.

The following table provides more information on data shown in the unlicensed OneDrive accounts report:

Expand table

Column	Description
Unlicensed accounts	Total number of OneDrive accounts that aren't licensed as of the date the report is generated.
Storage used	Total storage consumed by these unlicensed OneDrive accounts as of the report's date.
Retention period	Unlicensed accounts with a set-retention.md during the process of license removal or user account deletion. The retention period is no longer valid if storage is in a unpaid state.
Retention policy	Unlicensed accounts subject to a /purview/retention set up in Microsoft Purview. The retention policy is no longer valid if storage is in a unpaid state.
Active user with no license	Accounts where the user's license was removed, but the account wasn't deleted as part of the /microsoft-365/admin/add-users/delete-a-user. Starting in January 2025, users who aren't assigned a license, but are still considered active in the system, are archived on the 93rd unlicensed day.
Duplicate account	Unlicensed accounts created when an employee transfers to a different country/region, or firm within the organization. If these duplicate accounts are unnecessary, we recommend using the downloadable CSV from the SharePoint admin center to identify and delete them. If no action is taken, the accounts are automatically archived starting in January 2025 and incurs archive charges.
Unlicensed reason	'*No owner*' – There's no owner assigned to the OneDrive account, meaning that no license can be associated with this account.
	'*Owner deleted from Entra ID*' – The assigned owner was deleted, thus there's no license associated with this account.
	'*License removed by admin*' – The owner is present in Entra ID, but the owner's license has been removed from the account.
	'*Duplicate account*' – The owner has multiple OneDrive accounts associated with their identity. The duplicate account isn't the primary OneDrive account associated with the owner's identity. All nonprimary accounts associated with the owner are considered unlicensed.
Deletion blocked by	'*Retention period*' – The OneDrive account has been marked for deletion but is within the global OneDrive account retention period, as defined by the set-retention.md. Shortening the retention period helps reduce unlicensed OneDrive accounts being retained for this reason.

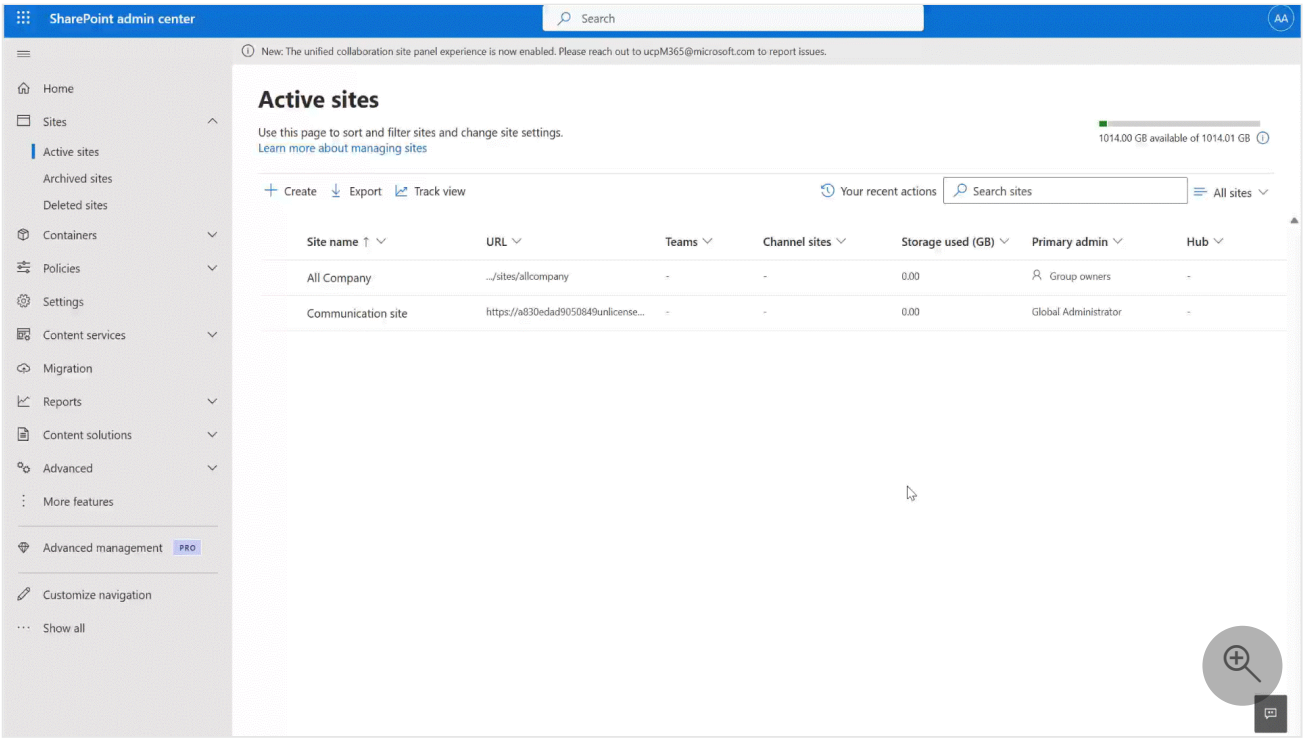
Column	Description
	'*Retention policy*' – A retention policy, a legal hold, or a compliance hold defined in Purview is stopping this account's contents from being deleted. The retention policy might be applied to only a subset of the account's contents, which would prevent the entire OneDrive account from being deleted. Modify your Purview retention or hold requirements to reduce OneDrive accounts held for this reason.
	'*Owner active in Entra ID*' – The OneDrive account's owner is still active in Entra ID, causing the account to not be deleted.
	'*Restored from recycle bin*' – This account was restored from the site recycle bin by an IT administrator. Since the account was intentionally restored, it will no longer be deleted automatically.
	'*Active lock on account*' – This account has an active read-only or no-access lock applied by an IT administrator, which blocks the account from being automatically deleted. IT administrators can use PowerShell to remove the lock state from the account or can delete this account directly.
	'*Previous lock or other state change*' – This account had a previous lock or other admin activity caused a state change which prevents the account from being automatically deleted. IT administrators can directly delete this account via PowerShell or from the SharePoint admin center's detailed OneDrive accounts report page .

View more details on unlicensed OneDrive accounts

You can view details on all unlicensed OneDrive accounts, even ones that aren't past their 93rd unlicensed day yet, in the SharePoint admin center.

1. In the SharePoint admin center, select **Reports**.

2. Select **OneDrive accounts** and then select **View more details**.



From this page, you can do the following actions:

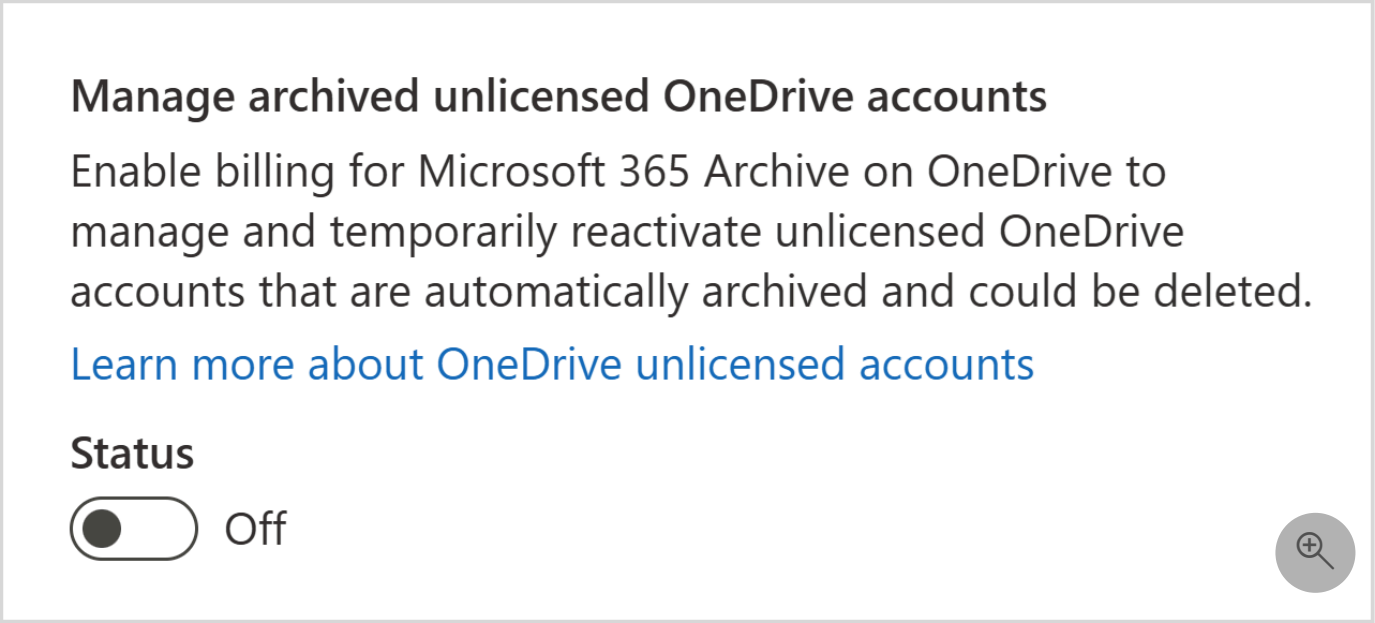
- Enumerate individual unlicensed accounts.
- See account details such as URL, Title, Storage used, Unlicensed date, unlicensed reason, and Archive status. *Note: accounts which are recently archived may have "archiving" as the status.*
- Delete accounts (some caveats exist such as delete failing because the account is on hold).
- Reactivate accounts.

> **Note**
>
> Admins can reactivate accounts from the detailed report. Accounts selected in the detailed report displays a 'Reactivate' button if the account is archived and billing for Unlicensed OneDrive accounts has been enabled. Alternatively, admins can use PowerShell to reactivate accounts with the *Set-SPOSiteArchiveState* cmdlet.

Charges from archived accounts

Once billing for unlicensed OneDrive accounts has been enabled, archived unlicensed OneDrive accounts which aren't deleted will begin to incur charges for both monthly storage and ad-hoc account reactivation.

> **Note**
>
> Billing enablement refers to turning on the Unlicensed OneDrive accounts billing toggle, which can only be enabled once a general pay-as-you-go billing method has been set up. Billing starts when the billing enablement for unlicensed OneDrive accounts is activated, not when an account is reactivated. Reactivation requires billing enablement, and once it's activated, storage charges begin.



If the billing is enabled to reactivate one particular unlicensed account, the reactivation fee is applied for $0.60/GB for that account, and from that month onward, the storage fee of $0.05/GB/Month is applicable for all unlicensed accounts within the organization for longer than 93 days.

For example, if an organization has 100 unlicensed OneDrive accounts, each consuming 1 TB for a total of 100 TB, and enforcement occurs between January and October 2025, the 100 unlicensed accounts are automatically archived. If the organization needs to reactivate a specific account in December 2025 and set up billing, they incur the following costs:

- A one-time reactivation fee of $0.60/GB for 1TB, totaling $614.40.
- A monthly storage fee of $0.05/GB for 100TB, amounting to $5,120/month starting from December 2025.

> **Note**
>
> Unlicensed OneDrive accounts can't utilize unused SharePoint storage quota, even if Microsoft 365 Archive is configured within the tenant. Archived unlicensed OneDrive

accounts are billed for the full amount of consumed storage.

Use Microsoft Purview in Archived State

Microsoft Purview eDiscovery and Content Search are still discoverable in archived content. Exporting the content that's supporting the search results doesn't require manual reactivation of the archived account, and it takes up to 24 hours to complete. However, if billing is not enabled and the account remains unpaid, customers should not rely on retention or legal hold settings alone to preserve content indefinitely in an unpaid, unlicensed OneDrive account.

Changes made to retention policies apply to archived accounts. For example, if the company reduces the retention policy from five years to three years, this update syncs with all archived accounts, for any accounts that fulfill the updated retention period, those accounts are moved to recycle bin, and the recycle bin process begins.

If deletion occurs, eDiscovery hold records remain, but held OneDrive content becomes unrecoverable. Data lifecycle management retention policy or label assignments can still appear healthy, but the target site no longer exists. Existing case exports are unaffected. New searches return no content from the deleted location.

Unlicensed OneDrive accounts and education tenants

An education tenant is any tenant with more than 50% education licenses. Any tenant with fewer than 50% education licenses is considered commercial. However, for any education tenant, unlicensed OneDrive accounts consume pooled storage and can pose security and compliance risks. IT admins can view the unlicensed accounts on the OneDrive accounts page to identify unlicensed accounts and take action.

Frequently Asked Questions

1. What is an unlicensed OneDrive account?

Answer: When an employee leaves an organization or a license is removed, their OneDrive account becomes unlicensed after the admin takes one of two steps:

License Removal:

- Go to the Microsoft 365 admin center.
- Expand Billing and select **Your Products**.

- Select the subscription and select **Remove licenses**.

User Deletion:

- In the Microsoft 365 admin center, expand **Users** and select **Active users**.
- Delete the user.

For more information on deleting users, see Delete a user from your organization.

2. Are all OneDrive account types affected (shared mailboxes, service accounts, room/resource, bots), or only named users?

Answer: The policy applies to all unlicensed OneDrives that remain unpaid in full.

3. What does 12 cumulative months of non-payment mean?

Answer: The policy establishes deletion risk for unlicensed OneDrive accounts at 365 cumulative days of nonpayment. Existing milestones remain: read-only at Day 60 and archive at Day 93.

4. Does the clock reset if a license is temporarily reassigned or billing is temporarily enabled?

Answer: While billing settings can be turned on or off, they should not be used to bypass retention enforcement, and doing so is not supported under the service terms. Billing and licensing should remain aligned with the customer's actual service usage and retention needs.

The 365 days of nonpayment is cumulative.

Expand table

Scenario	Cumulative nonpayment count
Account is unlicensed and unpaid for 90 days	90 days
Billing is enabled for 60 days	Count pauses while the account is paid
Billing is disabled again and the account remains unpaid for another 275 days	Count resumes and reaches 365 cumulative unpaid days
Total unpaid time reaches 365 days	Account is at risk of deletion

5. Can unlicensed ODB leverage unused SPO storage quota?

Answer: No. They're independent. Unlicensed OneDrive accounts can't use unused SharePoint storage quota, even though Microsoft 365 Archive is set up in the SharePoint tenant.

6. What is the outcome if an unlicensed OneDrive account is restored from the recycle bin 93 days after its license removal? Does the account get automatically archived?

Answer: Yes. If 93 days have passed since the license removal, bringing back an unlicensed OneDrive account from the recycle bin leads to automatic archival.

7. How does it impact retention policy, retention setting, or litigation hold?

Answer: Archived OneDrive accounts honor retention policies, settings, and litigation holds when billing is enabled for unlicensed OneDrive accounts. If billing is not enabled for unlicensed OneDrive accounts, and accounts are still retained 365 days after becoming unlicensed, then the unlicensed accounts will be subject to deletion 365 days after being unlicensed even if retention policies, settings, or holds exist on the OneDrive account.

> ⓘ **Note**
>
> If a OneDrive account is retained due to a retention policy, retention setting, or litigation hold and has been archived due to being unlicensed for 93 days or longer, then you still pay for the monthly archive storage costs when billing is enabled.

8. When will I get charged?

Answer: Once a payment method is provided, billing follows the routine cycle for archived content. If there's no retention policy and billing stops, your content is deleted within a 93-day period. The retention period is no longer valid if storage is in a unpaid state. If the account has no retention and billing, the 93-day content deletion lifecycle begins.

As an example, if the billing is put down to reactivate one particular unlicensed account, the reactivation fee is applied for $0.60/GB for that account, and from that month onward, the storing fee of $0.05/GB/Month is applied for all unlicensed accounts within the organization that's longer than 90 days.

9. What's the guidance on 'duplicate accounts'?

Answer: A duplicate account is created when an employee switches to a different country/region or a different firm within the organization. If the duplicate accounts aren't desired, we recommend using the downloadable CSV in the SharePoint Admin Center to identify the accounts and delete them. For already-archived unlicensed OneDrive accounts, it can be deleted from the archived state without the need of reactivation.

10. Once I initiate the reactivation of an account from Microsoft 365 Archive, how long do I have to wait until the data is available?

Answer: It takes up to 24 hours for the account to be accessible. Once the account is reactivated, it remains active for a total of 30 days before it gets automatically archived again.

11. What's the process to relicense an account once it's archived?

Answer: If the archived account has an associated user, the IT admin can give the user a valid license and the account automatically reactivates within 48 hours. If the archived account doesn't have an associated user (for example, if the identity was deleted), then it cannot be relicensed directly. Instead, we recommend:

1. Enabling the Unlicensed OneDrive Active storage meter
2. Moving any actively needed content to a SharePoint site or an active and licensed OneDrive account. The reactivation of the archived account happens automatically and without any reactivation fee once the account is relicensed, even if unlicensed OneDrive account billing isn't enabled.
3. Re-licensing by following the instructions on this page: Fix site user ID mismatch in SharePoint or OneDrive - SharePoint.

12. What happens to external sharing links and Teams file references once an unlicensed OneDrive is deleted?

Answer: Once a OneDrive is deleted, content associated with that OneDrive can no longer be accessed.

13. What happens to version history and Recycle Bin contents?

Answer: Content becomes inaccessible until the data is rehydrated into an active tier or the unlicensed OneDrive is licensed.

14. If a change is made to retention policies, will that change sync down to the archived sites?

Answer: Yes. As an example, if the company retention policy is shortened from five years to three years, this change is synced with all archived accounts, and the recycle bin process begins for accounts that completed the retention policy.

15. Why are there two different report pages with different numbers about unlicensed accounts?

Answer: The top-level report page shows you insights and lets you download the list of accounts which are at least 93 days unlicensed. This page directly indicates the amount of storage that will be billed if you have enabled billing. The detailed report page is linked from the top-level report page, and indicates all accounts that are currently unlicensed, even if they have been unlicensed for fewer than 93 days.

16. Why is the "*deletion scheduled on*" column empty in my CSV export of unlicensed accounts?

Answer: "*Deletion scheduled on*" refers to when the system tries to delete the account next. It takes into account the retention period of the unlicensed OneDrive account. This property may be empty if there's a hold or retention policy applied to the account. Additionally, the column is empty for users who are still active in Entra ID until the deletion part of the enforcement rollout is complete. If you delete the active user from Entra ID, and there's no retention policy or hold applied, then the "*Deletion scheduled on*" column will be populated within 7 days.

17. Will the unlicensed account enforcement override existing read-only or NoAccess settings which are already applied to my OneDrive accounts?

Answer: No. When enforcing unlicensed OneDrive accounts, the system won't override existing read-only or NoAccess modes. When the system tries to put an account into read-only mode, it skips the account if the account is already in read-only or NoAccess mode. When the account gets Archived, it will retain any read-only and NoAccess settings which the admin applied, which will take effect if the account is reactivated.

18. Will an account get enforced if the site 'owner' property (also known as the primary site collection admin) has been modified from the original user?

Answer: No. Modifying the 'owner' property of a OneDrive account to any user or group other than the user who the account was provisioned for results in an unsupported state of the OneDrive account. This can cause many issues for the account. However, the unlicensed enforcement effort doesn't utilize the 'owner' property to validate licensing. Therefore, modifying the 'owner' property, while generally not a supported change, won't directly cause an account to be considered unlicensed.

19. I have chosen not to enable Microsoft 365 Archive, what will happen to my unlicensed OneDrive accounts?

Answer: Enabling Microsoft 365 Archive has no impact on the enforcement of unlicensed OneDrive accounts. Unlicensed OneDrive accounts will get enforced no matter what, including

being put into read-only mode and eventually Archive. You can decide whether you want to enable billing for unlicensed OneDrive accounts, but you cannot prevent their archival. Microsoft 365 Archive and unlicensed OneDrive billing are two independent enablement toggles in the Microsoft 365 admin center and have no effect on each other. The enforcement flow for unlicensed accounts when Microsoft 365 Archive is enabled or disabled is identical and outlined fully in this article.

Related topics

- Standard storage for unlicensed OneDrive accounts
- OneDrive retention and deletion
- Pricing model for Microsoft 365 Archive
- Learn about retention for SharePoint and OneDrive
- Set the OneDrive retention for deleted users
- Create retention labels for exceptions
- Delete a user from your organization
- Assign or unassign licenses for users in the Microsoft 365 admin center

---

Last updated on 08/26/2026

Configure a default sensitivity label for a SharePoint document library

> *Microsoft Purview service description*

When SharePoint is enabled for sensitivity labels, you can configure a default label for document libraries. Then, any new files uploaded to that library, or existing files edited in the library will have that label applied if they don't already have a sensitivity label, or they have a sensitivity label but with lower priority.

For example, you configure the **Confidential** label as the default sensitivity label for a document library. A user who has **General** as their policy default label saves a new file in that library. SharePoint will label this file as **Confidential** because of that label's higher priority. For a quick summary of the possible outcomes, see Will an existing label be overridden on this page.

A default label offers a baseline level of protection and a form of automatic labeling without content inspection. To help you distinguish between this feature's default label with the default label in label policies:

- **Default sensitivity label for a document library**: Location-based labeling, applicable only for SharePoint. Overrides a lower-priority label unless manually applied.
- **Default sensitivity label from a policy**: Always applicable for all locations. Never overrides an existing label.

When you use Office for the web to create or edit a file, the default sensitivity label for a document library can be applied without delays. However, labeling is not immediate if you upload a file or create it using Microsoft 365 Apps on Windows, macOS, iOS or Android, and then save to SharePoint:

- File upload: it can take a few minutes for the label to be applied.
- Microsoft 365 Apps: the label is applied after the app is closed.

To read the preview announcement for this feature, see the blog post.

Will an existing label be overridden?

Summary of outcomes:

Expand table

Existing label	Override with library default label
Manually applied, any priority	No
Automatically applied, lower priority	Yes
Automatically applied, higher priority	No
Default label from policy, lower priority	Yes
Default label from policy, higher priority	No

Requirements

- You've created and published sensitivity labels that include the label scope of **Files & other data assets** and these labels are published to the users who will select a default sensitivity label for a SharePoint document library.
- You've enabled sensitivity labels for Office files in SharePoint and OneDrive. To check this status, you can run `(Get-SPOTenant).EnableAIPIntegration` from the SharePoint Online Management Shell to confirm the value is set to **True**.
- To support sensitivity labels for PDFs, you've added support for PDFs in SharePoint. To check this status, you can run `(Get-SPOTenant).EnableSensitivityLabelforPDF` from the SharePoint Online Management Shell to confirm the value is set to **True**.
- SharePoint Information Rights Management (IRM) is not enabled for the library. This older technology isn't compatible with using a default sensitivity label for a SharePoint document library. If a library is enabled for IRM, you won't be able to select a default sensitivity label.
- Site admin permissions are needed to apply and change the sensitivity label in SharePoint.
- Files must contain content to be labeled. Empty files are labeled when they are updated with content.

If you need to review a list of file types that are supported by sensitivity labels in SharePoint, see Supported file types.

Limitations

- Doesn't apply to existing files at rest in SharePoint.

- Unless you've enabled co-authoring for files encrypted with sensitivity labels, you'll see a delay in applying the default sensitivity label for a document library when users select the **File** > **Save as** option.

- As with sensitivity labels for Office for the web, some label configurations that apply encryption aren't suitable for SharePoint, and so don't support a default sensitivity label for a SharePoint document library:
  - **Let users assign permissions when they apply the label** and the checkbox **In Word, PowerPoint, and Excel, prompt users to specify permissions** is selected. This setting is sometimes referred to as "user-defined permissions".
  - **User access to content expires** is set to a value other than **Never**.
  - **Double Key Encryption** is selected.

How to configure a default sensitivity label for a SharePoint document library

This configuration is done by a SharePoint site admin: Add a sensitivity label to SharePoint document library.

> **Important**
>
> From the **Library settings** pane, select a sensitivity label and don't select the checkbox **Extend protection on download, copy, or move**. This setting is currently in preview and supports a different labeling scenario. For more information, see **Configure SharePoint with a sensitivity label to extend permissions to downloaded documents**.

Monitoring application of library default sensitivity labels

Use the SharePoint **Sensitivity** column to see the names of sensitivity labels applied to files. When the label has been applied by this features, the tooltip for the label name displays **This file has been automatically labeled**. However, this tooltip isn't exclusive to the default sensitivity label for a document library. It also displays when sensitivity labels are applied by using auto-labeling policies or as a result of a user's default label from sensitivity label policies.

To specifically identify when the label was applied because of the library's default sensitivity label, use the audit log search tool and the **Applied sensitivity label file** auditing event from the **Sensitivity label activities** group. Then:

1. Select an entry to view the details in a flyout pane.

2. From the details pane, scroll to the **SensitivityLabelEventData section**, and identify the value for **ActionScourceDetails**.

3. A value of **6** is used for when the label was applied because of the default sensitivity label for the document library.

To audit the configuration setting for this feature, use the **Updated list** auditing event from the **SharePoint list activities** group. In the details flyout pane for the document library, scroll to the **SensitivityLabelEventData** section where **OldSensitivityLabeld** and **SensitivityLabelId** can reflect three changes of states:

- Sensitivity label applied
- Sensitivity label changed from one label to another
- Sensitivity label removed

To map sensitivity label GUIDs to label names, use the Get-Label cmdlet:

1. First, connect to Security & Compliance PowerShell.

2. Then run the following command, where you specify the GUID:

PowerShell

```
Get-Label -Identity "<GUID>" | Name
```

How to turn off this feature

If you need to, you can turn off this feature that supports a default sensitivity label for SharePoint document libraries. This is a tenant-level setting that requires you to use the Set-SPOTenant cmdlet with the *DisableDocumentLibraryDefaultLabeling* parameter set to **True** by using the current SharePoint Online Management Shell:

PowerShell

```
Set-SpoTenant -DisableDocumentLibraryDefaultLabeling $true
```

After you run this command, you won't see the option to configure **Default sensitivity labels** for a document library. You won't be able to select a default sensitivity label for new or existing libraries.

For document libraries that were previously configured for a default sensitivity label:

- The label selection for the document library remains but is deactivated so new files won't have the selected sensitivity label applied.
- Sensitivity labels that were applied as a default label aren't removed.

As with all tenant-level configuration changes for SharePoint, it takes about 15 minutes for the change to take effect.

Next steps

Default labeling ensures a minimum level of protection but doesn't take into account the file contents that might require a higher level of protection. Consider supplementing this labeling method with automatic labeling that uses content inspection, and encourage manual labeling for users to replace the default label when needed.

- Learn about Double Key Encryption

Last updated on 06/10/2025

Use Information Barriers with SharePoint

Microsoft Purview Information Barriers (IB) are policies that prevent users from communicating and collaborating with each other. This article covers IB behavior in SharePoint.

For SharePoint, Information Barriers can determine and prevent the following kinds of unauthorized collaborations:

- Adding a user to a site
- User access to a site or site content
- Sharing a site or site content with other users

Information Barriers modes and SharePoint sites

Information Barriers modes help strengthen access, sharing, and membership of a site based on its IB mode and segments associated with the site.

> **Important**
>
> Microsoft recommends that you use roles with the fewest permissions. Minimizing the number of users with the Global Administrator role helps improve security for your organization. Learn more about Microsoft Purview roles and permissions.

When you use Information Barriers with SharePoint, the following IB modes apply:

- **Open**: The site has no segments. Anyone can be invited to be a member. This mode is the default when a SharePoint site doesn't have segments.
- **Owner Moderated**: The site owner moderates collaboration between incompatible segments. Only the resource owner can add new members per their IB policy.
- **Implicit**: Microsoft Teams sets the site's IB mode when it provisions the site. A SharePoint Administrator or Global Administrator can't manage segments with the *Implicit* mode configuration.
- **Explicit**: Segments are associated with the site, either through user site creation or by a SharePoint Administrator. Only users matching the site's segments can access and share content.

Open mode

Open mode sharing behavior

When a site has no segments and you set the site's IB mode to *Open*:

- Users can share the site and its contents based on the IB policy applied to them. For example, if a user in HR is allowed to communicate with users in Research, the user can share the site with those users.

> **Tip**
>
> If you want to allow sharing of *Open* mode sites with mail-enabled security groups, see the **Allow sharing of Open mode sites with mail-enabled security groups** section in this article.

Open mode access behavior

For a user to access a SharePoint site that has no segment and the site's Information Barriers mode is set to *Open*:

- The user has site access permissions.

Owner Moderated mode

Owner Moderated sharing behavior

When you set a site's Information Barriers mode to *Owner Moderated*:

- The option to share with *Anyone with the link* is disabled.
- The option to share with *Company-wide link* is disabled.
- (For group connected sites) The site and its content can be shared with existing members.
- (For non-group connected sites) Only the site owner can share the site and its content, according to their IB policy.

Owner moderated access behavior

For a user to access a SharePoint site with the site's Information Barriers mode set to *Owner Moderated*:

- (For non-group connected sites) The user has site access permissions.
- (For group connected sites) The user must be a member of the Microsoft 365 group connected to the site.

Implicit mode

Implicit mode sharing behavior

When you set a site's Information Barriers mode to *Implicit*:

- The option to share with *Anyone with the link* is disabled.
- The option to share with *Company-wide link* is disabled.
- The site and its content can be shared with existing members via a sharing link.
- You can't add new users to the site directly. The Team owner should add users to the Team's group by using Microsoft Teams.

> **Note**
>
> If you enabled Information Barriers for SharePoint in your organization before March 15, 2022, see the **Enable SharePoint and OneDrive Information Barriers** section in this article.

Implicit mode access behavior

To access SharePoint sites that use Information Barriers mode set to *Implicit*:

- You're a member of the Microsoft 365 group connected to the site.
- If you're not a member of the Microsoft 365 group connected to the site, you can't access the site.
- The Information Barriers compliance assistant ensures the group membership is IB compliant.

> **Note**
>
> If you enabled Information Barriers for SharePoint in your organization before March 15, 2022, see the **Enable SharePoint and OneDrive Information Barriers** section in this article.

Explicit mode

Explicit mode sharing behavior

When you associate a site with segments and set the site's Information Barriers mode to *Explicit*:

- The option to share with *Anyone with the link* is disabled.

- The option to share with *Company-wide link* is disabled.
- You can share the site and its content only with users whose segment matches that of the site. For example, if you associate a site with the HR segment, you can share the site with just HR users (even though HR is compatible with both Sales and Research segments).
- You can add new users as site members only if their segment matches the segment of the site.

Explicit mode access behavior

To access SharePoint sites that use segments and site's Information Barriers mode is *Explicit*:

- Your segment matches a segment that's associated with the site.

  AND

- You have access permission to the site.

Non-segment users can't access a site associated with segments. They see an error message.

Allow apps running in app-only mode to access IB sites

Many organizations use applications running in an app-only context in their organization. To allow these apps running in app-only mode to access IB protected sites, SharePoint admins can enable the opt-in capability.

> **Important**
>
> Information Barriers policies might impact the applications accessing sites in app-only mode. Enable the policy and then test the experience for the apps used in your organization.

To enable applications running in app-only mode to access IB sites, run the following command:

PowerShell

```
Set-SPOTenant -AppBypassInformationBarriers $true
```

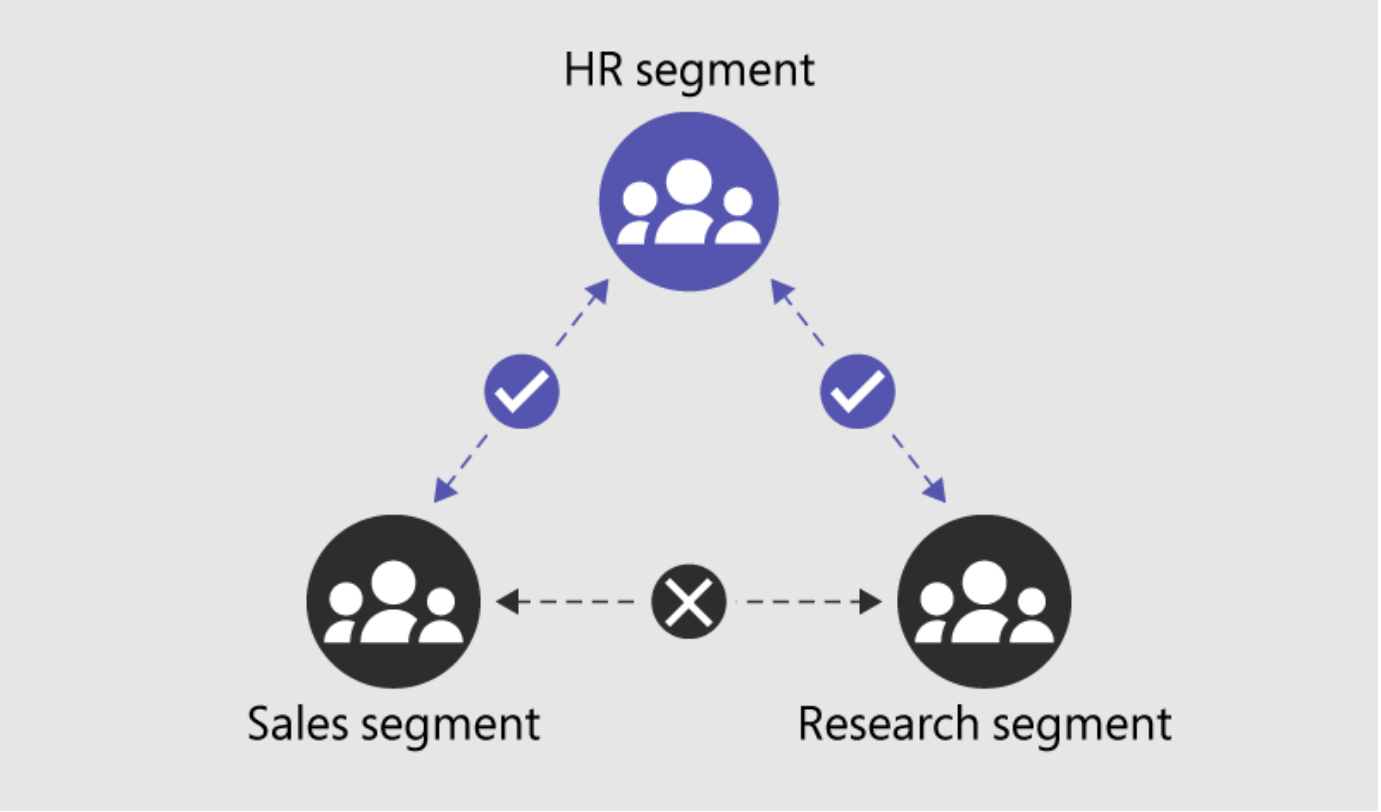
If you enable Teams Meeting Recording or EDU Assignment application in your organization, run the following command to allow these applications to interact with IB protected sites:

PowerShell

```
Set-SPOTenant -AppOnlyBypassPeoplePickerPolicies $true
```

Example scenario

The following example illustrates three segments in an organization: HR, Sales, and Research. An IB policy blocks communication and collaboration between the Sales and Research segments. These segments are incompatible.



By using SharePoint Information Barriers, a SharePoint Administrator or Global Administrator can associate segments to a site to prevent the site from being shared with or accessed by users outside the segments. You can associate up to 100 compatible segments with a site. You associate the segments at the site level (previously called site collection level). The Microsoft 365 group connected to the site is also associated with the site's segment.

> **Important**
>
> Microsoft recommends that you use roles with the fewest permissions. Minimizing the number of users with the Global Administrator role helps improve security for your organization. Learn more about Microsoft Purview roles and permissions.

In the previous example, the HR segment is compatible with both Sales and Research. However, because the Sales and Research segments are incompatible, you can't associate them with the

same site.

Prerequisites

1. Make sure you meet the licensing requirements for Information Barriers.
2. Create IB policies that allow or block communication between the segments, and then set them to active. Create segments and define the users in each segment.
3. Wait 24 hours after configuring and activating your IB policies for the changes to propagate through your organization.
4. Complete the steps in the following sections to enable and manage SharePoint and OneDrive Information Barriers in your organization.

Enable SharePoint and OneDrive Information Barriers in your organization

> **Important**
>
> Microsoft recommends that you use roles with the fewest permissions. Minimizing the number of users with the Global Administrator role helps improve security for your organization. Learn more about Microsoft Purview **roles and permissions**.

SharePoint Administrators or Global Administrators can enable Information Barriers in SharePoint and OneDrive in your organization. Complete the following steps to enable Information Barriers for your organization:

1. You must use the latest version of the SharePoint Online Management Shell. If you installed a previous version of the SharePoint Online Management Shell, go to **Add or remove programs** and uninstall *SharePoint Online Management Shell*. Then, install the latest version. To learn more, see Get started with SharePoint Online Management Shell.

2. Connect to SharePoint Online as a Global Administrator or SharePoint Administrator in Microsoft 365. For more information, see Getting started with SharePoint Online Management Shell.

3. Run the following command to enable Information Barriers in SharePoint and OneDrive:

   PowerShell

   ```
   Set-SPOTenant -InformationBarriersSuspension $false
   ```

4. Wait for approximately 1 hour for the changes to take effect after you enable Information Barriers for SharePoint and OneDrive in your organization.

> **Note**
>
> If you enabled Information Barriers for SharePoint in your organization before March 15, 2022, the default access and sharing control for Implicit mode for Microsoft Teams-connected sites are based on the segments associated with the site.

To enable Microsoft 365 group-membership based access and sharing control for all Implicit mode Teams-connected sites in your tenant, run the following command:

PowerShell

```
Set-SPOTenant -IBImplicitGroupBased $true
```

> **Note**
>
> If you have Microsoft 365 Multi-Geo, run this command for each of your geolocations.

View and manage segments as an administrator

> **Important**
>
> Microsoft recommends that you use roles with the fewest permissions. Minimizing the number of users with the Global Administrator role helps improve security for your organization. Learn more about Microsoft Purview roles and permissions.

SharePoint Administrators or Global Administrators can view and manage segments on a SharePoint site. Your organization can have up to 5,000 segments, and users can be assigned to multiple segments.

> **Important**
>
> Support for 5,000 segments and assigning users to multiple segments is only available when your organization isn't in *Legacy* mode. Assigning users to multiple segments requires extra

steps to change the Information Barriers mode for your organization. For more information, see [Use multi-segment support in Information Barriers](#).

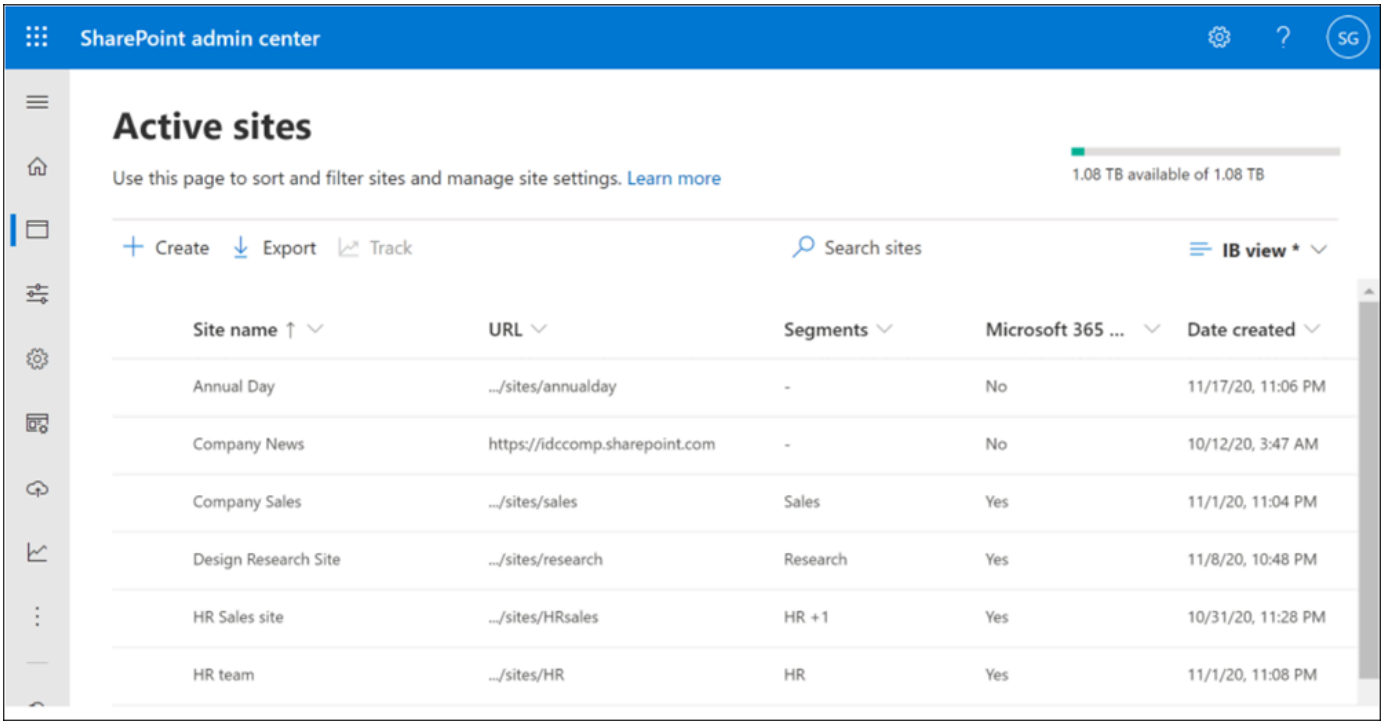
For organizations in *Legacy* mode, the maximum number of segments supported is 250, and users are restricted to being assigned to only one segment. Organizations in *Legacy* mode are eligible to upgrade to the newest version of Information Barriers in the future. For more information, see the [Information Barriers roadmap](#).

View and manage Information Barriers segments as follows:

1. Use the SharePoint admin center to view and manage information segments

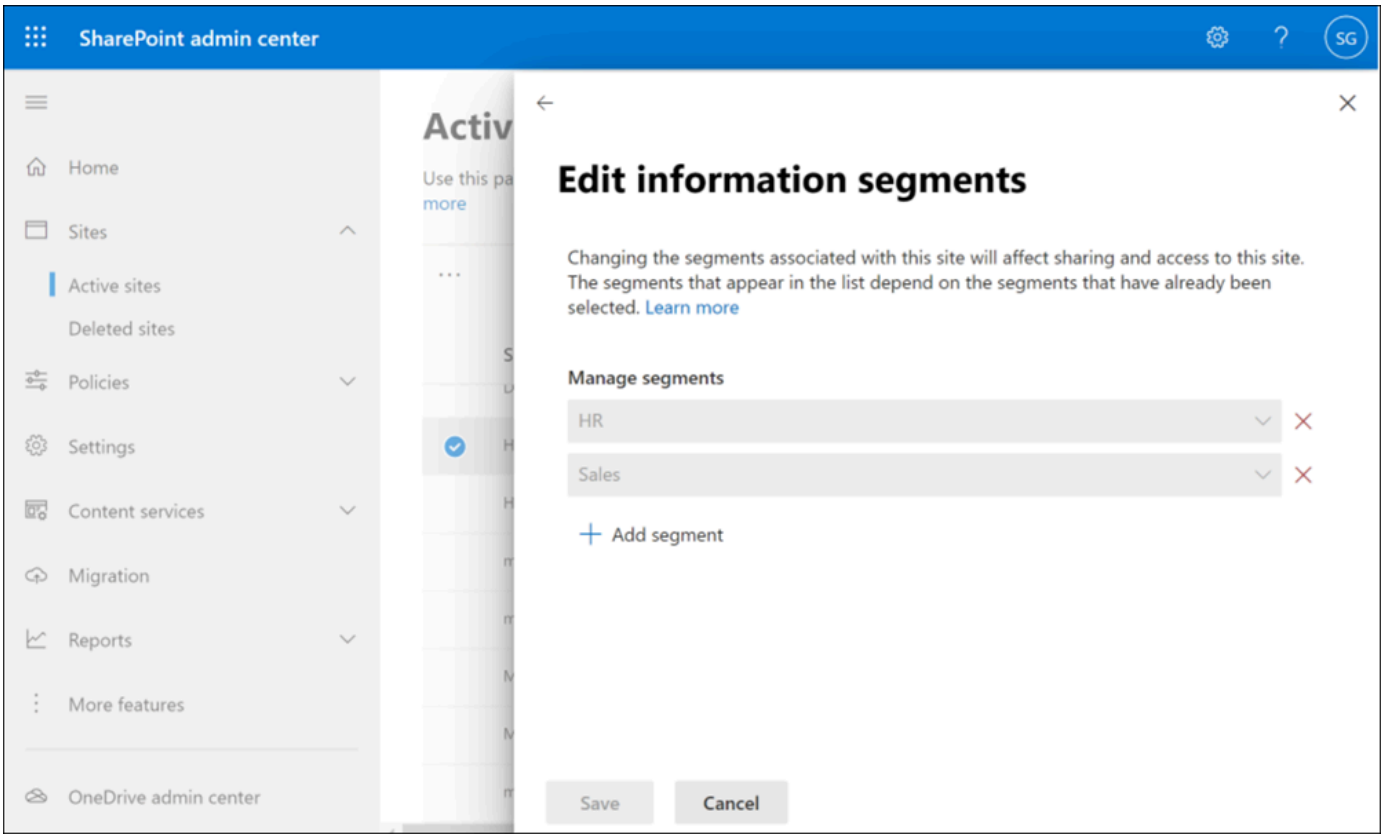
To view, edit, or remove information segments for a site, use **Active sites** in the SharePoint admin center.

The Segments column lists the first segment associated with the site and shows whether the site has other segments associated. Learn how to show or move this column.



To view the complete list of segments associated with a site, select the site name to open the details panel, and then select the **Settings** tab.

To edit the segments associated with the site, select **Edit**, add or remove segments, and then select **Save**.



2. Use SharePoint PowerShell to view and manage information segments on a site

> **Important**
>
> Microsoft recommends that you use roles with the fewest permissions. Minimizing the number of users with the Global Administrator role helps improve security for your organization. Learn more about Microsoft Purview roles and permissions.

1. Connect to Security & Compliance PowerShell as a Global Administrator.

2. Run the following command to get the list of segments and their GUIDs.

   PowerShell

   ```
   Get-OrganizationSegment | ft Name, EXOSegmentID
   ```

3. Save the list of segments.

Expand table

Name	EXOSegmentId
Sales	a9592060-c856-4301-b60f-bf9a04990d4d
Research	27d20a85-1c1b-4af2-bf45-a41093b5d111
HR	a17efb47-e3c9-4d85-a188-1cd59c83de32

4. You must use the latest version of the SharePoint Online Management Shell. If you installed a previous version of the SharePoint Online Management Shell, go to **Add or remove programs** and uninstall *SharePoint Online Management Shell*. Then, install the latest version. To learn more, see Get started with SharePoint Online Management Shell.

5. Connect to SharePoint Online as a Global Administrator or SharePoint Administrator in Microsoft 365. For more information, see Getting started with SharePoint Online Management Shell.

6. Run the following command:

   PowerShell
   ```
   Set-SPOSite -Identity <site URL> -AddInformationSegment <segment GUID>
   ```

   For example:

   PowerShell
   ```
   Set-SPOSite -Identity https://contoso.sharepoint.com/sites/ResearchTeamSite -
   AddInformationSegment 27d20a85-1c1b-4af2-bf45-a41093b5d111
   ```

You see an error message if you attempt to associate a segment that isn't compatible with the site's existing segments.

> **Note**
>
> When you add a segment to a site, the site's IB mode is automatically updated to *Explicit*.

To remove a segment from a site, run the following command:

PowerShell
```
Set-SPOSite -Identity <site URL> -RemoveInformationSegment <segment GUID>
```

For example:

PowerShell

```
Set-SPOSite -Identity https://contoso.sharepoint.com/sites/ResearchTeamSite -
RemoveInformationSegment 27d20a85-1c1b-4af2-bf45-a41093b5d111
```

> **Note**
>
> When you remove all segments from a site, the site's IB mode is automatically updated to *Open*.

To view the segments of a site, run the following command to return the GUIDs of any segments associated with the site.

PowerShell

```
Get-SPOSite -Identity <site URL> | Select InformationSegment
```

3. Use the SharePoint REST API to view and manage information segments on a site

SharePoint includes a Representational State Transfer (REST) service that you can use to manage segments on a site. To access SharePoint resources and manage site segments by using REST, construct a RESTful HTTP request by using the OData standard. This request corresponds to the desired client object model application programming interface (API).

For more information about the SharePoint REST service, see Get to know the SharePoint REST service.

View and manage IB modes as an administrator with SharePoint PowerShell

To view the IB mode of a site, run the following command:

PowerShell

```
Get-SPOSite -Identity <site URL> | Select InformationBarriersMode
```

Owner Moderated mode scenario

You want to allow a Sales and Research user to collaborate on a SharePoint site in the presence of an HR user.

Owner Moderated is a mode applicable to sites (Teams-connected sites, non-group connected sites) that grants incompatible segment users access to the site. Only the site owner can invite incompatible segment users to the same site.

To update a site's mode to *Owner Moderated*, run the following PowerShell command:

PowerShell

```
Set-SPOSite -Identity <siteurl> -InformationBarriersMode OwnerModerated
```

You can't set the Owner Moderated IB mode on a site with segments. Remove the segments first before setting IB mode as Owner Moderated. Users who have site access permissions can access an Owner Moderated site. Only the site owner can share an Owner Moderated site and its contents according to their IB policy.

Auditing

You can view audit events in the Microsoft Purview portal to monitor IB activities. The system logs audit events for the following activities:

- Enabling Information Barriers for SharePoint and OneDrive
- Applying a segment to a site
- Changing the segment of a site
- Removing the segment of a site
- Applying Information Barriers mode to a site
- Changing Information Barriers mode of a site
- Disabling Information Barriers for SharePoint and OneDrive

For more information about SharePoint segment auditing in Microsoft 365, see Search the audit log in the Microsoft Purview portal.

Site creation and management by site owners

When a segmented user creates a SharePoint site, the site associates with the user's segment and the site's Information Barriers mode automatically sets to *Explicit*.

Site owners can add more segments to a SharePoint site that already has segments with the site's mode set as *Explicit*. Site owners can't remove added segments from sites. SharePoint

Administrators need to remove added segments in your organization if needed.

When a non-segmented user creates a SharePoint site, the site doesn't associate with any segment and the site's Information Barriers mode automatically sets to *Open*.

When a SharePoint Administrator creates a SharePoint site from the SharePoint admin center, the site doesn't associate with any segment and the site's IB mode sets to *Open*.

To help site owners add a segment to a site, share the Associate information segments with SharePoint sites article with your SharePoint site owners.

Microsoft Teams sites

When you create a team in Microsoft Teams, you also automatically create a SharePoint site for the team's files. To protect the Microsoft Teams sites by using Information Barriers control, enable Information Barriers in SharePoint for your tenant.

Within 24 hours, the site's Information Barriers mode is automatically set to *Implicit* and segments associated with the team's members are associated with the site.

Microsoft Teams sites with the IB mode set to *Implicit* have site access and sharing based on Microsoft 365 group membership.

For example, users have access to the Microsoft Teams site if they're members of the Microsoft 365 group connected to the site. The Microsoft 365 group connected to the Team is IB compliant.

> **Note**
>
> If you enabled Information Barriers for SharePoint in your organization before March 15, 2022, the Teams-connected site's access and sharing is based on the segments of the site. For example:

- You can share the site and its content with users whose segment matches that of the site.
- Users can access the site and its content if they have the same segment as that of the site and have site access permissions.

To enable Microsoft 365 group membership-based access and sharing control for all *Implicit* mode sites in your organization, see Enable SharePoint and OneDrive Information Barriers in your organization.

Private channel and Information Barriers

When you enable SharePoint Information Barriers in your organization, any new private channel site automatically inherits its parent Microsoft Team's IB mode within 24 hours. The mode for a private channel is assigned as follows:

Expand table

Parent Team's IB mode	Private channel site's IB mode
Open	Open
Implicit or Owner Moderated	Implicit

The private channel site's IB mode governs access and sharing for the private channel site:

- Private channel site with *Open* Information Barriers mode
  - Access anyone with site access permissions
  - Sharing links are allowed per the site's existing sharing policy
  - People picker allows discoverability of user per the sharer's IB policy
- Private channel site with *Implicit* Information Barriers mode
  - Access only to users who are currently members of the private channel
  - Sharing by using **People with existing access link**

Private channel sites already configured in your organization have their Information Barriers mode set as *Open*. To configure existing private channel sites to *Implicit* mode, run the following cmdlet in the SharePoint PowerShell module:

PowerShell

```
Set-Sposite -Identity <site URL> -InformationBarriersMode Implicit
```

Learn more about managing Microsoft Teams connected teams sites.

Search

Users see search results from:

- **Segment associated sites**: When the site's segment matches the user's segment and the user has site access permission. For example, a site with *Explicit* mode.

- **Non-segmented sites**: When the user has existing access to the content or site. For example, sites with *Open*, *Owner Moderated*, or *Implicit* mode. When the user selects the search result to open the content in the site, the user is denied access if they don't match the site's IB policy.

Tenant wide search and Copilot experience

Users experience is as follows:

- **Segment associated sites**: When the site's segment matches the user's segment and the user has site access permission. For example, a site with *Explicit* mode.
- **Open mode sites:** When the user has existing access to the content or site.
- **Implicit and Owner moderated mode sites:**
  - When the user has existing access to the content or site.
  - If the user had access to the site and content prior to the policy application, they continue to see the site and its contents in search and Copilot results. However, when attempting to open the content, they're denied access if they don't comply with the site's IB policy.

Effects of changes to user segments

If a SharePoint site owner or site member's segment changes, they retain access to the site or content according to the site's IB mode:

- **Open mode**: User can access the site if they have existing site access permissions.
- **Owner Moderated**: User can access the site if they have existing site access permissions.
- **Implicit Mode**: If the user is a member of the Microsoft 365 group, they retain access to the site.
- **Explicit Mode**: If the user's new segment matches the site's segment and user has site access permissions, they retain access to the site.

Effects of changes to existing IB policies

If a compliance administrator changes an existing IB policy, the change might affect the compatibility of the segments associated with a site (in *Explicit* or *Implicit* mode*). For example, segments that were once compatible might no longer be compatible.

By using the Information Barriers policy compliance report, the SharePoint Administrator can view the list of sites where segments are no longer compatible. For more information, see Learn how to create an Information Barriers policy compliance report in PowerShell.

To manage out of compliance sites:

- In *Explicit* mode, a SharePoint Administrator must change the associated segments to bring them into IB compliance.
- In *Implicit* mode, a SharePoint Administrator can't manage segments directly. The Teams admin should manage the Team's membership to bring the Teams membership roster and segments into IB compliance.

How to suspend SharePoint and OneDrive Information Barriers in your organization

If your organization wants to temporarily suspend Information Barriers on SharePoint, use SharePoint Online Management Shell and the Set-Spotenant cmdlet.

To suspend Information Barriers, run the following command:

PowerShell

```
Set-SPOTenant -InformationBarriersSuspension $true
```

> **Note**
>
> If you have Microsoft 365 Multi-Geo, run this command for each of your geo-locations.

Allow sharing of Open mode sites with mail-enabled security groups

IB supports an opt-in capability available in the SharePoint PowerShell module for sites in *Open* mode to be shared with mail-enabled security groups for site permissions, sharing, and audience targeting. This capability is only supported in *Open* mode sites. SharePoint admins can enable this support in your organization. Ensure the security group membership is IB compliant.

Before enabling group support, verify that you meet the following prerequisites:

- Your organization has only IB *Block* policies.

- Your organization is enabled for SharePoint IB (see this section in this article).

To configure mail-enabled security group support in *Open* mode sites, run the following command:

PowerShell

```
Set-SPOTenant -ShowPeoplePickerGroupSuggestionsForIB $true
```

Next steps

- Use Information Barriers with OneDrive: Configure IB modes and segments for OneDrive accounts in your organization.
- SharePoint and OneDrive insights reports: Run reports to identify top sites by IB mode and usage patterns.
- Create an Information Barriers policy compliance report: Identify noncompliant sites after policy changes.
- Information Barriers compliance assistant: Automatically remove noncompliant users from group-connected SharePoint sites.

ⓘ **Note:** The author created this article with assistance from AI. Learn more

---

Last updated on 03/30/2026

Use Information Barriers with OneDrive

Microsoft Purview Information Barriers are policies that prevent users from communicating and collaborating with each other. This article covers IB behavior in OneDrive.

For OneDrive, Information Barriers can determine and prevent the following kinds of unauthorized collaborations:

- User access to OneDrive or stored content
- Sharing OneDrive or stored content with other users

Information Barriers modes and OneDrive

When you enable Information Barriers on SharePoint and OneDrive, you automatically protect the OneDrive of segmented users with IB policies. Information Barriers modes help strengthen access, sharing, and membership of a OneDrive site based on its IB mode and segments associated with the OneDrive.

When you use Information Barriers with OneDrive, the following IB modes apply:

- **Open**: The OneDrive has no segments. This mode is the default when a non-segmented user provisions their OneDrive.
- **Owner Moderated**: The OneDrive is used for collaboration with incompatible users in the presence of the site owner/moderator. See this section for details.
- **Explicit**: The user's segment and other compatible segments are associated with the OneDrive. This mode is the default when a segmented user provisions their OneDrive within 24 hours of enablement.
- **Mixed**: The segmented user's OneDrive is allowed to be shared with unsegmented users. This mode is an opt-in mode that the SharePoint admin can set on a OneDrive of a segmented user.

> **Note**
>
> Starting July 12, 2022, *Inferred* mode changed to *Mixed* mode. The functionality for the mode remains the same.

Open mode

Open mode sharing behavior

When a OneDrive has no segments and IB mode as *Open*:

- The user can share files and folders based on the IB policy applied to the user and the sharing setting for the OneDrive.

Open mode access behavior

For a user to access content in a OneDrive with no segments and IB mode as *Open*:

- The files must be shared with the user.

Owner Moderated mode

Owner Moderated sharing behavior

When a OneDrive has Information Barriers mode set to *Owner Moderated*:

- The option to share with *Anyone with the link* is disabled.
- The option to share with *Company-wide link* is disabled.
- You can share the site and its content with existing members.
- Only the OneDrive owner can share the site and its content, following their IB policy.

Owner Moderated access behavior

For a user to access a OneDrive with Information Barriers mode set to *Owner Moderated*:

- The user has site access permissions.

Explicit mode

Explicit mode sharing behavior

When a OneDrive has Information Barriers segments and the mode is set to *Explicit*:

- The option to share with *Anyone with the link* is disabled.
- The option to share with *Company-wide link* is disabled.
- You can share files and folders only with users whose segment matches that of the OneDrive.

Explicit mode access behavior

For a user to access content in a OneDrive with segments and IB mode set to *Explicit*:

1. The user's segment matches a segment associated with the OneDrive.

   AND

2. The files are shared with the user.

> **Note**
>
> By default, non-segment users can access shared OneDrive files only from other non-segment users with IB modes set to *Open*. They can't access shared files from OneDrive that have segments applied and the IB mode is *Explicit*.

Mixed mode

Mixed mode sharing behavior

When a OneDrive uses Information Barriers segments and the mode is set to *Mixed*:

- The option to share with *Anyone with the link* is disabled.
- The option to share with *Company-wide link* is disabled.
- You can share files and folders with users whose segment matches that of the OneDrive and unsegmented users in the tenant.

Mixed mode access behavior

For a segmented user to access content in a OneDrive with segments and IB mode set to *Mixed*:

1. The user's segment matches a segment associated with the OneDrive.

   AND

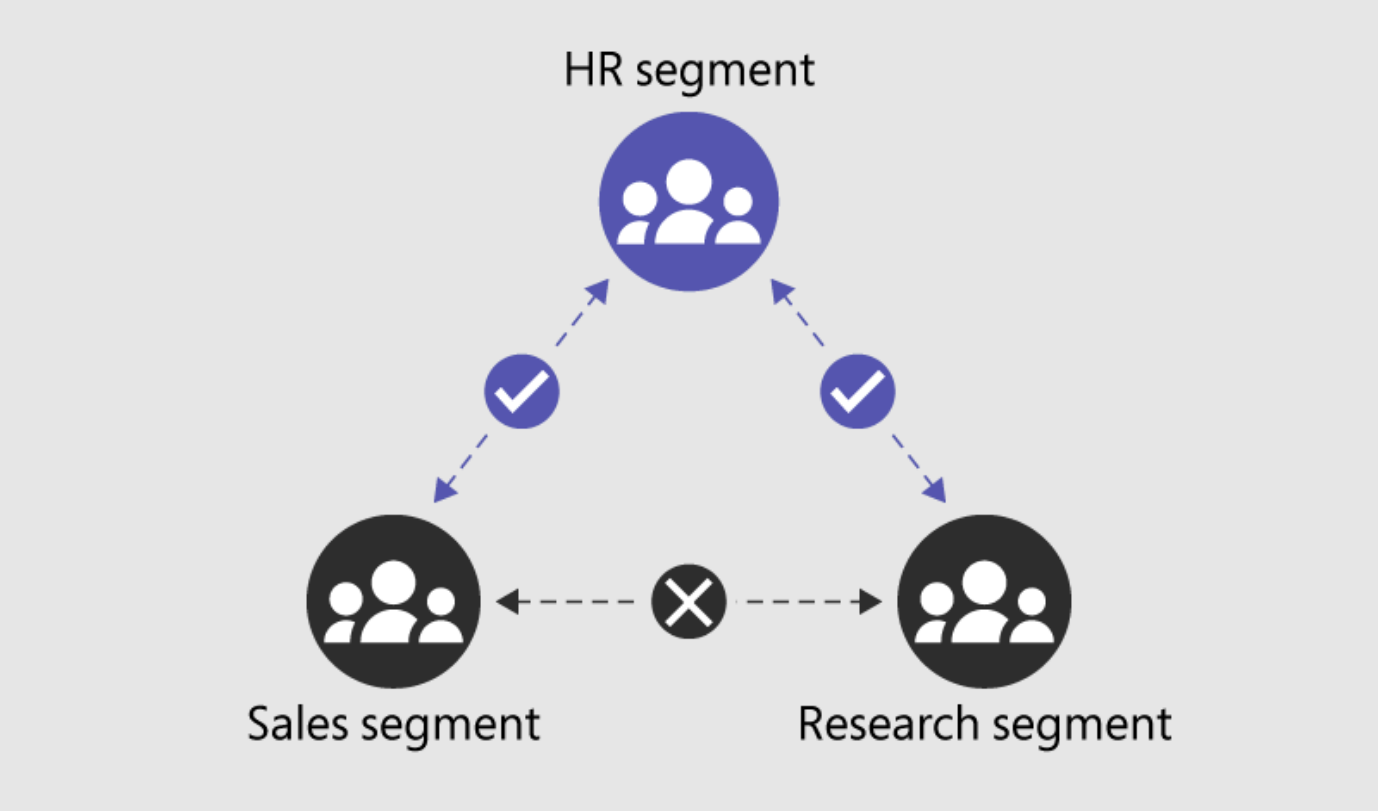
2. The files are shared with the user.

For an unsegmented user to access content in a OneDrive with segments and IB mode set to *Mixed*:

- The user has site access permissions.

Example scenario

The following example illustrates three segments in an organization: HR, Sales, and Research. You define an IB policy that blocks communication and collaboration between the Sales and Research segments.



By using Information Barriers in OneDrive, when you apply a segment to a user, the segment automatically associates with the user's OneDrive within 24 hours. The OneDrive also associates with other segments that are compatible with the user's segment and with each other. A OneDrive can have up to 100 associated segments. A global or SharePoint admin can manage these segments by using PowerShell, as described later in the section Associate or remove additional segments on a user's OneDrive.

The following table shows the effects of this example configuration:

Expand table

Components	HR users	Sales users	Research users	Non-segment users
Segments associated with OneDrive	HR	Sales, HR	Research, HR	None
IB mode on OneDrive	Explicit	Explicit	Explicit	Open

Components	HR users	Sales users	Research users	Non-segment users
OneDrive content can be shared with	HR only	Sales and HR	Research and HR	Anyone based on the sharing settings selected
OneDrive content can be accessed by	HR only	Sales and HR	Research and HR	Anyone with whom the content is shared

Enable SharePoint and OneDrive Information Barriers in your organization

You configure enabling Information Barriers for SharePoint and OneDrive in a single action. You can't enable Information Barriers for the services separately. For more information, see Enable SharePoint and OneDrive Information Barriers in your organization. After you enable Information Barriers for SharePoint and OneDrive, continue with the OneDrive guidance in this article.

Prerequisites

1. Make sure you meet the licensing requirements for Information Barriers.
2. Create IB policies that allow or block communication between the segments and activate the policies. Create segments and define the users in each.
3. After you configure and activate your IB policies, wait 24 hours for the changes to propagate through your organization.
4. Enable Information Barriers for OneDrive. You configure enabling Information Barriers for SharePoint and OneDrive in a single action. You can't enable these services separately. For more information, see the guidance and steps in the Use Information Barriers with SharePoint article.
5. Complete the steps in the following sections to customize and manage Information Barriers for OneDrive in your organization.

Use PowerShell to view the segments associated with a OneDrive

> **Important**

Microsoft recommends that you use roles with the fewest permissions. Minimizing the number of users with the Global Administrator role helps improve security for your organization. Learn more about Microsoft Purview roles and permissions.

A global admin or SharePoint admin can view and change the segments associated with a user's OneDrive. Your organization can have up to 5,000 segments, and users can be assigned to multiple segments.

> **Important**
>
> Support for 5,000 segments and assigning users to multiple segments is only available when your organization isn't in *Legacy* mode. Assigning users to multiple segments requires extra steps to change the Information Barriers mode for your organization. For more information, see Use multi-segment support in Information Barriers.
>
> For organizations in *Legacy* mode, the maximum number of segments supported is 250, and users are restricted to being assigned to only one segment. Organizations in *Legacy* mode are eligible to upgrade to the newest version of Information Barriers in the future. For more information, see the Information Barriers roadmap.

1. Connect to Security & Compliance PowerShell as a global admin.
2. Run the following command to get the list of segments and their GUIDs.

PowerShell

```
Get-OrganizationSegment | ft Name, EXOSegmentID
```

3. Save the list of segments.

Expand table

Name	EXOSegmentId
Sales	a9592060-c856-4301-b60f-bf9a04990d4d
Research	27d20a85-1c1b-4af2-bf45-a41093b5d111
HR	a17efb47-e3c9-4d85-a188-1cd59c83de32

4. You must use the latest version of the SharePoint Online Management Shell. If you installed a previous version of the SharePoint Online Management Shell, go to **Add or remove programs** and uninstall *SharePoint Online Management Shell*. Then, install the latest version. To learn more, see Get started with SharePoint Online Management Shell.

5. Connect to SharePoint as a global admin or SharePoint admin in Microsoft 365. For more information, see Getting started with SharePoint Online Management Shell.

6. Run the following command:

   PowerShell

   ```
   Get-SPOSite -Identity <site URL> | Select InformationSegment
   ```

   For example:

   PowerShell

   ```
   Get-SPOSite -Identity https://contoso-my.sharepoint.com/personal/John_contoso_onmicrosoft_com | Select InformationSegment
   ```

Manage segments on a user's OneDrive

> ⚠ **Warning**
>
> If the segments associated with a user's OneDrive don't match the segment you apply to the user, the user can't access their OneDrive. Don't associate any segments with the OneDrive of a non-segment user.

> ⓘ **Note**
>
> Any changes you make are overwritten if the user's segment changes.

To associate a segment with a OneDrive, run the following command in the SharePoint Online Management Shell.

PowerShell

```
Set-SPOSite -Identity <site URL> -AddInformationSegment <segment GUID>
```

For example:

PowerShell

```
Set-SPOSite -Identity https://contoso-
my.sharepoint.com/personal/John_contoso_onmicrosoft_com -AddInformationSegment
27d20a85-1c1b-4af2-bf45-a41093b5d111
```

When you add segments to a OneDrive, the site's IB mode automatically updates to *Explicit*. An error appears if you attempt to associate a segment that isn't compatible with the existing segments on the OneDrive.

To remove a segment from a OneDrive, run the following command.

PowerShell

```
Set-SPOSite -Identity <site URL> -RemoveInformationSegment <segment GUID>
```

For example:

PowerShell

```
Set-SPOSite -Identity https://contoso-
my.sharepoint.com/personal/John_contoso_onmicrosoft_com -RemoveInformationSegment
27d20a85-1c1b-4af2-bf45-a41093b5d111
```

If you remove all the segments of a OneDrive site, the IB mode of the OneDrive automatically updates to *Open*.

Manage the IB mode of a user's OneDrive (preview)

> **Important**
>
> Microsoft recommends that you use roles with the fewest permissions. Minimizing the number of users with the Global Administrator role helps improve security for your organization. Learn more about Microsoft Purview roles and permissions.

To view the IB mode of a OneDrive site, run the following command in the SharePoint Online Management Shell as a SharePoint admin or global administrator:

PowerShell

```
Get-SPOSite -Identity <site URL> | Select InformationBarriersMode
```

For example:

PowerShell

```
Get-SPOSite -Identity https://contoso-
my.sharepoint.com/personal/John_contoso_onmicrosoft_com | Select
InformationBarriersMode
```

A SharePoint admin or global administrator can also manage the IB mode of a OneDrive site to meet the needs of your organization by using new IB modes:

Owner Moderated mode example

Allow an incompatible segment user access to a OneDrive. For example, you want to allow HR user's OneDrive to be accessed by both Sales and Research segment users in your tenant.

Owner Moderated is a mode applicable to OneDrive sites that allows incompatible segment users to access OneDrive in the presence of a moderator/owner. Only the site owner has the capability to invite incompatible segment users on the same site.

To update a OneDrive site IB mode to *Owner Moderated*, run the following PowerShell command:

PowerShell

```
Set-SPOSite -Identity <siteurl> -InformationBarriersMode OwnerModerated
```

You can't set the Owner Moderated IB mode on a site with segments. Remove the segments before setting the IB mode as Owner Moderated. Users with site access permissions can access an Owner Moderated site. Only the site owner can share an Owner Moderated OneDrive and its contents per their IB policy.

Mixed mode example

Allow unsegmented users to access OneDrive associated with segments. For example, you want to allow HR users' OneDrive to be accessed by HR segment and unsegmented users in your tenant. Mixed mode applies to OneDrive sites that allow segmented and unsegmented users to access OneDrive.

To update a OneDrive site's IB Mode to Mixed, run the following PowerShell command:

PowerShell

```
Set-SPOSite -Identity <siteurl> -InformationBarriersMode Mixed
```

You can't set mixed IB mode on a site without segments. Add segments before setting the IB mode as mixed.

Effects of changes to user segments

If a user's segment changes, the OneDrive segment and IB mode automatically update within 24 hours as described in the OneDrive Information Barriers section.

Example 1: User's segment updated from Research to Sales, the user's OneDrive updates as follows within 24 hours:

- Segment: Sales, HR
- IB mode: *Explicit*

Example 2: User's segment updated from HR to None

- Segment: None
- IB mode: *Open*

Effects of changes to IB policies

If a compliance administrator changes an existing policy, the change might affect the compatibility of the segments associated with the OneDrive.

For example, segments that were once compatible might no longer be compatible. A SharePoint admin must change the segments associated with an affected site. For more information, see create an Information Barriers policy compliance report in PowerShell.

If you change a policy after users share files, the sharing links work only if the user attempting to access the shared files has a segment applied that matches a segment associated with the OneDrive.

Auditing

Audit events are available in the Microsoft Purview portal to help you monitor IB activities. The system logs audit events for the following activities:

- Enabling Information Barriers for SharePoint and OneDrive

- Applying segment to site
- Changing segment of site
- Removing segment of site
- Applying Information Barriers mode to site
- Changing Information Barriers mode of site
- Disabling Information Barriers for SharePoint and OneDrive

For more information about OneDrive segment auditing in Microsoft 365, see Search the audit log.

Next steps

- Use Information Barriers with SharePoint: Configure IB modes and segments for SharePoint sites in your organization.
- SharePoint and OneDrive insights reports: Run reports to identify OneDrive accounts by IB mode and usage patterns.
- Create an Information Barriers policy compliance report: Identify noncompliant OneDrive accounts after policy changes.

ⓘ **Note:** The author created this article with assistance from AI. Learn more

---

Last updated on 03/30/2026

Information Barriers compliance assistant (preview)

This article explains how to enable the Information Barriers (IB) compliance assistant for group-connected SharePoint sites. These sites are sites that don't have an associated team in Microsoft Teams. When you enable the IB compliance assistant, it automatically removes users who don't match the segments specified on this site to ensure group membership honors configured IB policies. This configuration helps ensure your organization remains compliant with standards, policies, and compliance regulations.

Prerequisites

1. Make sure you define policies for Information Barriers.
2. Configure IB segments on a SharePoint Site.
3. Install the Azure PowerShell module.
4. Install the Microsoft Graph PowerShell SDK.
5. PowerShell account must have directory administrator access for the tenant.

Enable the background compliance assistant

These steps create a new application in your organization's enterprise applications. For the compliance assistant to function properly, you must have explicitly added segments to a SharePoint site. Complete the following steps to enable the compliance assistant:

1. Run the following PowerShell cmdlets.

   PowerShell

   ```
   Connect-MgGraph
   Connect-AzAccount
   $appId="00001111-aaaa-2222-bbbb-3333cccc4444"
   $sp=Get-AzADServicePrincipal -ServicePrincipalName $appId
   if ($sp -eq $null) {New-AzADServicePrincipal -ApplicationId $appId}
   Start-Process "https://login.microsoftonline.com/common/adminconsent?
   client_id=$appId"
   ```

2. When prompted, sign in by using your Microsoft 365 work or school account.

3. In the **Permissions requested** dialog box, review the information, and select **Accept**. This action configures admin consent for the compliance assistant.

Verify you created a new application

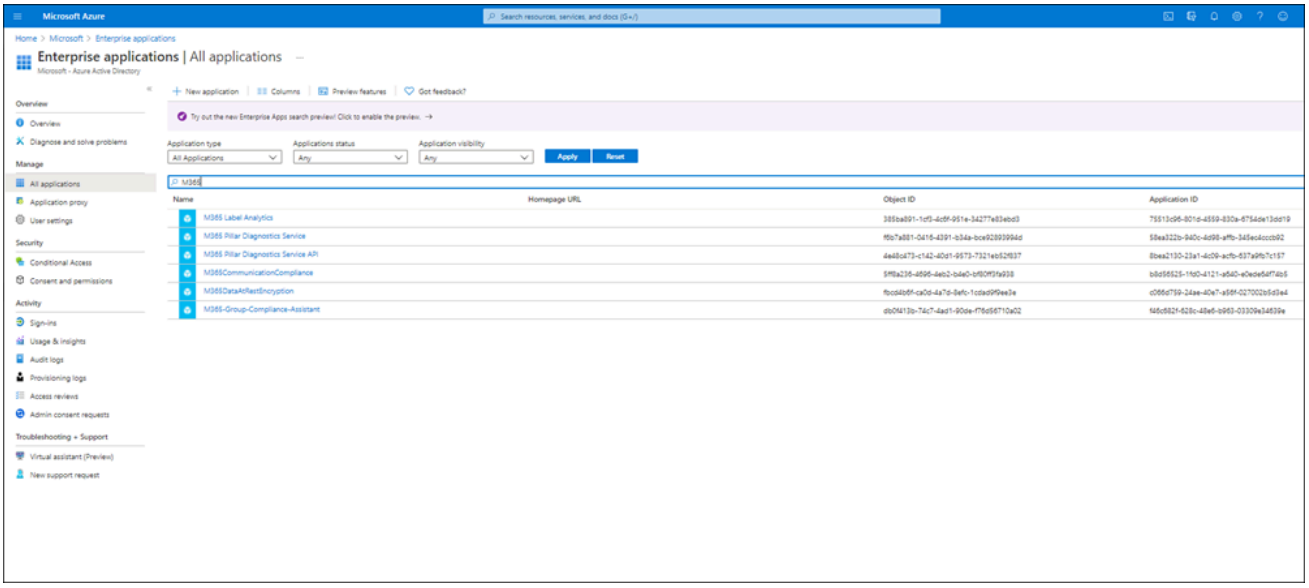
To verify you created a new application in your organization's enterprise applications, complete the following steps:

1. Sign in to portal.azure.com with directory administrator credentials.

2. Select **Manage Microsoft Entra ID**.

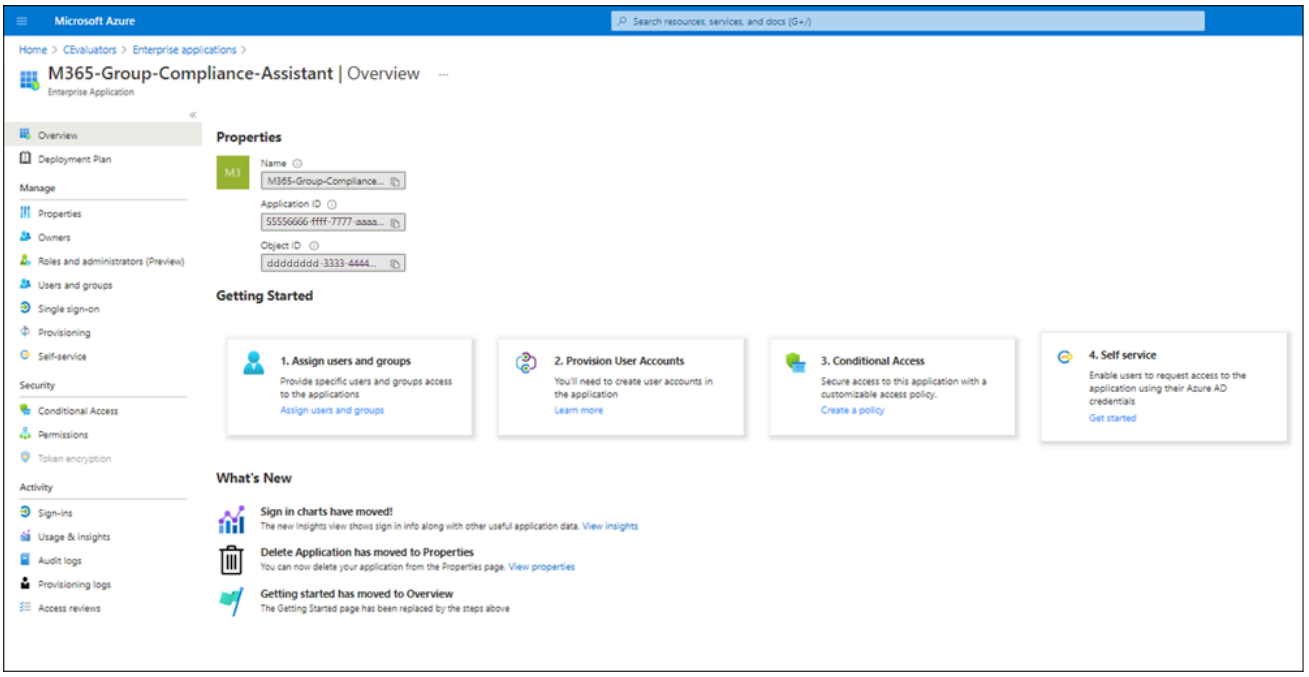
3. Select **Enterprise Applications** in the left navigation.

4. Search for the compliance assistant by using 'M365' as the search term.

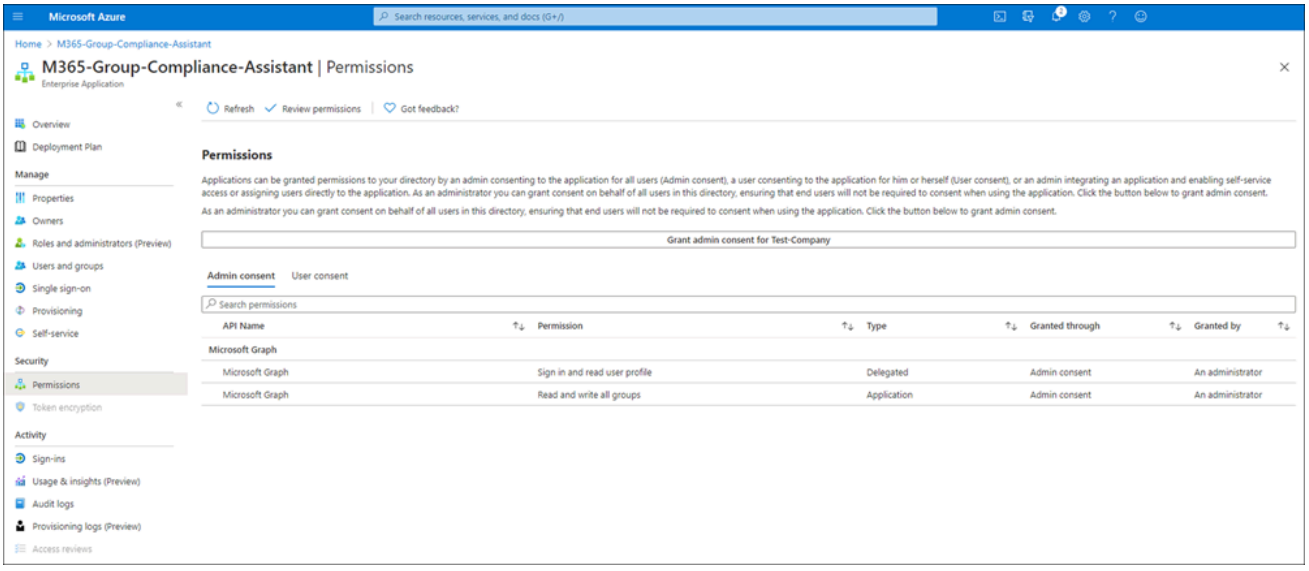


5. Select **M365-Group-Compliance-Assistant** from the list of search results.

6. On the **M365-Group-Compliance-Assistant overview** page, review the application properties.



7. Select **Permissions** in the left navigation to review the permissions that the application is authorized for.



8. In this example, the **M365-Group-Compliance-Assistant** is authorized to add or remove noncompliant IB users from your Microsoft 365 groups.

You can use audit log search in the Microsoft Purview portal to search, review, and track audit log events for the M365-Group-Compliance-Assistant application. The audit activities associated with the compliance assistant are:

- **IB assistant removed group member**: The IB noncompliant group member was removed from the group by the compliance assistant.
- **IB assistant removed group owner**: The IB noncompliant owner was removed from the group by the compliance assistant.

- **Identified as IB non-compliant group**: The segments on the group are non-IB compliant with each other.

To search the audit log for Microsoft 365 Groups activities, see Search the audit log.

> **Note**
>
> The compliance assistant runs periodically (every 24 hours). The assistant runs on group-connected SharePoint sites that don't have an associated team in Microsoft Teams. To enable the compliance assistant for SharePoint sites connected to Microsoft Teams, follow the instructions in the **Define IB policies** article.

Next steps

- Use Information Barriers with SharePoint: Manage IB segments and modes on the SharePoint sites the assistant monitors.
- Create an Information Barriers policy compliance report: Identify noncompliant sites that need manual remediation beyond the assistant.
- Manage Information Barriers policies: Update segments or policies to resolve recurring compliance issues.

Note: The author created this article with assistance from AI. Learn more

---

Last updated on 04/14/2026

Create an Information Barriers policy compliance report

If a compliance administrator changes an existing Information Barriers policy, the change might affect the compatibility of segments already associated with a site.

For example, a policy might allow communication and collaboration between the Sales and Research segments. Later, the policy might not allow communication and collaboration between these segments. The segments are incompatible and shouldn't be associated with the same site.

By using the SharePoint Information Barriers policy compliance report, SharePoint administrators can view the list of sites that don't comply with existing policies. The report covers these sites:

- Microsoft 365 group-connected team sites that aren't connected to Microsoft Teams
- Communication sites
- Modern team sites that aren't connected to Microsoft 365 groups
- OneDrive
- User-owned SharePoint Embedded containers

The report displays the list of sites that don't comply with the existing policies that you recently updated. For each noncompliant site, it shows compatible segments, incompatible segments, and invalid segments (those segments that no longer exist).

If a OneDrive or user-owned SharePoint Embedded container doesn't comply, this report lets you update its segments to be compliant with the latest IB policies in your organization.

> **Note**
>
> You only need to run this report if you change Information Barriers policies. Depending on the number of sites in your organization, it can take a long time for this report to run.

Run the report

> **Important**
>
> Microsoft recommends that you use roles with the fewest permissions. Minimizing the number of users with the Global Administrator role helps improve security for your

organization. Learn more about Microsoft Purview roles and permissions.

1. You must use the latest version of the SharePoint Online Management Shell. If you installed a previous version of the SharePoint Online Management Shell, go to **Add or remove programs** and uninstall *SharePoint Online Management Shell*. Then, install the latest version. To learn more, see Get started with SharePoint Online Management Shell.

2. Connect to SharePoint Online as a Global Administrator or SharePoint Administrator in Microsoft 365. For more information, see Getting started with SharePoint Online Management Shell.

3. Run the following command to build the report:

   PowerShell
   ```
   Start-SPOInformationBarriersPolicyComplianceReport
   ```

   Or, to automatically update any noncompliant OneDrive accounts when you build the report, run:

   PowerShell
   ```
   Start-SPOInformationBarriersPolicyComplianceReport -UpdateOneDriveSegments
   ```

   Or, to automatically update any noncompliant user-owned SharePoint Embedded containers when you build the report, run:

   PowerShell
   ```
   Start-SPOInformationBarriersPolicyComplianceReport -
   UpdateUserOwnedContainerSegments
   ```

4. Run the following command to view the status of the task:

   PowerShell
   ```
   Get-SPOInformationBarriersPolicyComplianceReport
   ```

   The command returns the following set of information:

   text

```
State: Completed
Id: beedfc3e-850c-4ca2-9ae0-7eacbe529d77
StartTimeInUtc: 9/21/2026 1:11:32 AM
CompleteTimeInUtc: 9/21/2026 1:11:33 AM
QueuedTimeInUtc: 9/21/2026 1:07:11 AM
UpdateOneDriveSegments: False
UpdateUserOwnedContainerSegments: True
```

5. Run the following command to view the report:

PowerShell

```
Get-SPOInformationBarriersPolicyComplianceReport -reportid <ID>
```

(Where *ID* is the report's ID from the previous step.)

The command returns the following set of information for each site:

text

```
Content: {8d7c4a12-5f6e-4b8d-9a31-c7e2f4a9d6b5}
HasNonCompliantSites: True
State: Completed
Id: beedfc3e-850c-4ca2-9ae0-7eacbe529d77
StartTimeInUtc: 9/21/2026 1:11:32 AM
CompleteTimeInUtc: 9/21/2026 1:11:33 AM
QueuedTimeInUtc: 9/21/2026 1:07:11 AM
UpdateOneDriveSegments: False
UpdateUserOwnedContainerSegments: True
```

The **Content** row lists the sites that aren't compliant. If all sites are compliant, the **Content** row is empty and **HasNonCompliantSites** is `False`.

6. Run the following command to view details about the noncompliant segments associated with each site:

PowerShell

```
$report = Get-SPOInformationBarriersPolicyComplianceReport -reportid <ID>
$report.Content
```

(Where *ID* is the report's ID from the previous step.)

The command returns the following set of information for each site:

text

```
SiteId: 3ef21e8a-69d9-4bf0-a70f-0328e5a18087
SiteUrl: https://contoso.sharepoint.com/sites/Research
SiteType: Group
ComplianceState: NonCompliant
CurrentSegments: Sales, Research
OriginalSegments: Sales, Research
InvalidIBSegments:
IncompatibleSegmentsPairs: <Sales, Research>
FailedToBeProcessed: False
```

> **Note**
>
> For info about removing incompatible segments, see Use Information Barriers with SharePoint. When you finish with a report, delete it by using `Remove-SPOInformationBarriersPolicyComplianceReport -reportid <>`.

Next steps

- Use Information Barriers with SharePoint: Remove incompatible segments from noncompliant SharePoint sites identified in the report.
- Use Information Barriers with OneDrive: Update segments on noncompliant OneDrive accounts identified in the report.
- Manage Information Barriers policies: Edit policies to resolve widespread compliance issues across sites.

Note: The author created this article with assistance from AI. Learn more

---

Last updated on 10/02/2026

Control notifications in the SharePoint mobile app

Article • 07/19/2024

By default, SharePoint mobile app users can receive notifications about site activity. The service sends these notifications through the Firebase Cloud Messaging service for Android or the Apple Push Notification service for iOS. As a SharePoint Administrator and above in Microsoft 365, you can turn off these notifications for all users for compliance purposes. If you allow these notifications, users can select to turn them off.

Currently, notifications are sent for the following activities:

- SharePoint news published (users receive these based on relevancy)
- Page comment (sent to the page author)
- Page comment reply (sent to the page author and the author of the comment that is being replied to)
- Page comment mention (sent to person @ mentioned)
- Page like (sent to the page author)

Other notifications might be added in the future.

> **Note**
>
> Notifications aren't available for the US government environments or Office 365 operated by 21Vianet (China).

Allow or block notifications

1. Go to **Settings** in the SharePoint admin center, and sign in with an account that has admin permissions for your organization.

2. Select the **Notifications** setting for SharePoint.

3. Select or clear **Allow notifications**.

You can also control this setting in PowerShell by using Set-SPOTenant -NotificationsInSharePointEnabled.

See also

For info about controlling OneDrive notifications, see Control notifications.

To control whether sharing emails include "At a glance" content, see Set-SPOTenant -IncludeAtAGlanceInShareEmails.

Feedback

Was this page helpful? Yes No

Provide product feedback

Use Microsoft Purview risk and compliance solutions instead of the older information management and records management features in SharePoint for Microsoft 365

> **Important**
>
> Read the overview to get a summary of the plan to deprecate the applicable older features from SharePoint for Microsoft 365 records management. For more information and links to important articles and pages, see migration strategies.
>
> Review the older information management and records management features in SharePoint for Microsoft 365 deprecation timeline for dates that have been announced and for updates on new deprecation announcements.

Overview

If you need to retain or delete content in Microsoft 365, we recommend using Microsoft Purview Data Lifecycle Management and Microsoft Purview Records Management features instead of older information management and records management features in SharePoint for Microsoft 365

We have a long-term deprecation plan for these older features. More information, including dates, is in the deprecation timeline. Feature deprecations are communicated in advance to give customers time to prepare and perform any applicable migration activities.

The following older information management and records management features in SharePoint for Microsoft 365 are under consideration for deprecation:

- Record Center
  - Create a record center site
  - Submit records to the record center (commonly referred to as "send to" location)
  - Content Organizer
- Information management policies
- In-place records management, including vault abilities.
- Document deletion policies (deletion only)

- Policies for site closure and deletion (deletion only)

Deprecation summary

The following key points summarize how deprecation works:

- Microsoft won't automatically migrate your older information management and records management features in SharePoint for Microsoft 365. If you choose not to migrate to supported features, the older features might no longer be supported.
- Between now and the deprecation date of the feature, you have the flexibility to migrate your scenarios on your own schedule.
- If you have configured SharePoint sites for content type policies or information management policies, those policies continue to be ignored while a retention policy or retention label policy is in effect.
- Deprecation for features might include some or all the following outcomes:
  - Microsoft might not support the feature.
  - It might no longer be visible in the user interface.
  - Configurations might not be available through the user interface or programmatically, including enable and disable actions.
  - When fully deprecated, backend services supporting behaviors for the feature might no longer function as expected.

Deprecation timeline

> **Note**
>
> Any future dates and timelines are approximate and might change as we develop our plans further.

Worldwide service

Upcoming

November 2023 – Announcement of the first set of features in the deprecation plan and timelines.

January 2025 - The following features will no longer be supported by Microsoft and configurations will no longer be available:

- Record Center site template, used to create a new Record Center site.

- Configure systems to submit files to a site using the Record Center programmable interface (commonly referred to as "send to" location).
- Content Organizer.

April 2026 - The following features will no longer be supported by Microsoft and configurations will no longer be available:

- Information Management Policies for targeting policy to library, folders & content Types, Name & Admin Description, Policy Statement, Retention, Auditing, Barcodes, Labels.
- In-Place Records Management for Vault abilities, Record Restrictions, Record Declaration Availability, Declaration Roles
- Document deletion policies, Policies for site closure and deletion

Government clouds (GCC, GCC-H, DoD)

Upcoming

November 2023 – Announcement of the first set of features in the deprecation plan and timelines.

January 2025 - The following features will no longer be supported by Microsoft and configurations will no longer be available:

- Record Center site template, used to create a new Record Center site.
- Configure systems to submit files to a site using the Record Center programmable interface (commonly referred to as "send to" location).
- Content Organizer.

April 2026 - The following features will no longer be supported by Microsoft and configurations will no longer be available:

- Information Management Policies for targeting policy to library, folders & content Types, Name & Admin Description, Policy Statement, Retention, Auditing, Labels.
- In-Place Records Management for Vault abilities, Record Restrictions, Record Declaration Availability.
- Document deletion policies, Policies for site closure and deletion

Migrating from older features to modern features

Modern Microsoft Purview features have flexible configuration options to help meet your data lifecycle and records management needs. The specific configuration that works best for your

organization depends on your organization's governance strategy and applicable requirements.

To identify what works best for your scenarios and understand options for migrating your organization's older features to modern Purview solutions, see migration strategies.

Last updated on 01/27/2026

Migration strategies for moving to Microsoft Purview risk and compliance solutions from older information management and records management for SharePoint for Microsoft 365

Article • 01/29/2025

Before you begin, it's important to plan your migration. You might need to interact with multiple stakeholders within your organization depending on the use case. It's important for you to carefully design your migration strategy. We've provided a few examples to help guide your next steps.

Prepare for using Purview risk and compliance solutions

1. Review your existing older policies and decide which ones you need to recreate in the modern features. Confirm your goals for compliance and which of the features you're using today to meet those needs. For example, you might have a business requirement to keep your content in some SharePoint sites for one year and are using information management policies today to accomplish this requirement. This review can also be an opportunity to audit your retention schedule and identify if there are any duplicate, outdated, or conflicting policies that you might not want to recreate.

2. Use this guide to understand what you need to do, identify the older feature and behavior you're migrating from, and decide which modern feature to use. It's also recommended to confirm that you have the applicable licenses for the modern features. Learn more about licensing for Purview Data Lifecycle Management and Purview Records Management.

   You might be eligible for a free trial of Microsoft Purview risk and compliance solutions, including premium Purview Data Lifecycle Management and Purview Records Management features. See free trial.

3. Configure your modern features. Implement the strategies defined in your plan and set up the modern features that meet your requirements.

4. Verify that your new features are working as expected:

    - Wait for the applicable time period for your new features to take effect
    - Confirm policies applied to a location using policy lookup
    - Use activity explorer to review actions related to labeling content
    - Use content explorer to review labeled items
    - Check the policy status for errors

Older features and using Purview features instead

Record center site

Expand table

Older feature	Purview feature suggestion

Record Center site templates helps organizations implement their records management and retention programs.	• Create a communication site to replace the records center.
	• Use Purview Data Lifecycle Management for retention policies that retain or delete content.
	• Use Purview Records Management for retention labels that:
	  ◦ Apply by default to items within a library, folder, or document set.
	  ◦ Auto-apply to content
	  ◦ Classify contents as records

Submit records to the record center

Expand table

Older feature	Purview feature suggestion
The record collection programmable interface (commonly referred to as "send to" location) enables organizations to automatically submit files to a SharePoint site.	Configure PowerAutomate to route records automatically to your new communication site.

Content Organizer

Expand table

Older feature	Purview feature suggestion
Content Organizer automatically routes content to a location in a SharePoint site.	To route content, including records, to locations within your sites: • Configure PowerAutomate to route content automatically to your sites. • Create a rule in Microsoft Syntex that moves or copies files in document libraries. • Use Audit (Standard) to maintain logs.

Information Management policies

Expand table

Older feature	Purview feature suggestion

Information Management policies allow for schedules to be defined on a library and its folders, or to site content types.	• Use Purview Data Lifecycle Management for retention policies that retain or delete content.
	• Use Purview Data Lifecycle Management or Purview Records Management for:
	  ○ Retention labels that are applied by default to content in a folder or library.
	  ○ Automatically apply to specified content types.
	  ○ Customizing what happens at the end of the retention period.
	  ○ Managing single and multi-stage disposition of content.
	• Use PowerAutomate to route content automatically using custom flow.
	• Use Audit (Standard). to maintain logs of events and operations performed.
	• To include information on a file (policy labels), create and publish sensitivity labels that apply content marking.

Document deletion policies

Expand table

Older feature	Purview feature suggestion
Document deletion policies permanently delete content from a site after a specified period of time.	Use Purview Data Lifecycle Management for retention policies that retain or delete content.

In-place records management

Expand table

Older feature	Purview feature suggestion

In-place records management specifies restrictions on documents declared as records. Vault abilities allow administrators to prevent the direct tampering with records, track version changes, and audit actions.	• Use Purview Records Management for retention labels that:
	  ◦ Are published for users to manually apply.
	  ◦ Auto-apply to content.
	  ◦ Classify contents as records to prevent tampering and add more audit activities.
	  ◦ Take action during and at the end of the content lifecycle.
	• Use Audit (Standard) to maintain logs.

Feedback

Was this page helpful? Yes No

Provide product feedback

Introduction to managed metadata

Metadata is information about information. For example, a book's title and author is metadata. Metadata can be many kinds of information -- a location, a date, or a catalog item number. When you use SharePoint products, you can manage the metadata centrally. You can organize the metadata in a way that makes sense in your business and use the metadata to make it easier to find what you want.

This article describes some important terminology of managed metadata, and gives you a quick look at how you can use the tools in SharePoint to manage metadata.

Important terminology

This section contains definitions of some key terminology. These terms and concepts appear frequently in articles about managed metadata.

Taxonomy

A taxonomy is a formal classification system. A taxonomy groups the words, labels, and terms that describe something, and then arranges the groups into a hierarchy.

People construct taxonomies for almost any kind of information, from biological systems to organizational structures. For example, biologists group living organisms into four major classifications: animal, plant, fungus, and microbe. Each of these major groups has many subdivisions. Together, the whole system is a taxonomy.

Organizations create taxonomies in too many ways to list. They create Chart of Accounts taxonomies to manage accounting systems, organization charts and job classifications to manage employees, product catalogs and so on. All these taxonomies are structured hierarchies of information; formal classification systems that help people handle information.

Folksonomy

A folksonomy is an informal classification system. It evolves gradually as web site users collaborate on words, labels, and terms on a site. Originally, folksonomies developed from popular applications such as bookmarking.

If you have ever seen a tag cloud on a website, then you have seen a visualization of a folksonomy. The following figure shows a tag cloud on a SharePoint site.

A folksonomy-based approach to metadata can be useful. It creates a way to share the knowledge and expertise of site users. By using a folksonomy, content classification can evolve together with changing business needs and user interests.

Term Set

A Term set is a group of related terms.

Terms sets can have different scope, depending on where you create the term set.

- **Local term sets** are created within the context of a site collection, and are available for use (and visible) only to users of that site collection. For example, when you create a term set for a metadata column in a list or library, then the term set is local. It is available only in the site collection that contains this list or library. For example, a media library might have a metadata column that shows the kind of media (diagram, photograph, screenshot, video, etc.). The list of permitted terms is relevant only to this library, and available for use in the library.

- **Global term sets** are available for use across all sites that subscribe to a specific Managed Metadata Service application. For example, an organization might create a term set that lists names of business units in the organization, such as Human Resources, Marketing, Information Technology, and so on.

In addition, you can configure a term set as closed or open. In a closed term set, users can't add new terms unless they have appropriate permissions. In an open term set, users can add new terms in a column that is mapped to the term set.

Terms

A term is a specific word or phrase that you associated with an item on a SharePoint site. It is a single item in a term set. A term has a unique ID and it can have many text labels (synonyms). If you work on a multilingual site, the term can have labels in different languages.

There are two types of terms:

- **Managed terms** Managed terms are terms that are pre-defined. Term Store administrators organize managed terms into a hierarchical term set.
- **Enterprise keywords** An enterprise keyword is a word or phrase that a user adds to items on a SharePoint site. The collection of enterprise keywords is known as the Keywords set. Typically, users can add any word or phrase to an item as a keyword. This means that you can use enterprise keywords for folksonomy-style tagging. Sometimes, Term Store administrators move enterprise keywords into a specific managed term set. When they are part of a managed term set, keywords become available in the context of that term set.

To learn more about how to create and manage terms, see Create and manage terms in a term set.

Group

In SharePoint products, group is a security term. With respect to managed metadata, a group is a set of term sets that all share common security requirements. Only users who have contributor permissions for a specific group can manage term sets that belong to the group or create new term sets within it. Organizations should create groups for term sets that will have unique access or security needs.

To learn more about how to create a group for term sets, see Set up a new group for term sets.

Term Store management tool

The Term Store management tool is the tool that people who manage taxonomies use to create or manage term sets and the terms within them. The Term Store management tool displays all the global term sets and any local term sets available for the site collection from which you access the Term Store management tool.

Managed Metadata column

A Managed Metadata column is a special kind of column that you can add to lists or libraries. It enables site users to select terms from a specific term set. A Managed Metadata column can map to an existing term set, or you can create a local term set specifically for the column.

To learn how to work with a Managed Metadata column, see Create a managed metadata column

Enterprise Keywords column

The enterprise Keywords column is a column that you can add to content types, lists, or libraries to enable users to tag items with words or phrases that they choose. By default, it is a multi-value column. When users type a word or phrase into the column, SharePoint presents type-ahead suggestions. Type-ahead suggestions might include items from managed term sets and the Keywords term set. Users can select an existing value, or enter something new.

List or library owners can enable or disable metadata publishing by updating the **Enterprise Metadata and Keywords Settings** for a list or library.

To learn how to add a special keywords column, see Add an enterprise keywords column to a list or library.

Tagging

In a general sense, tagging refers to the act of applying managed metadata to an item.

Metadata scenarios: from taxonomies to folksonomies

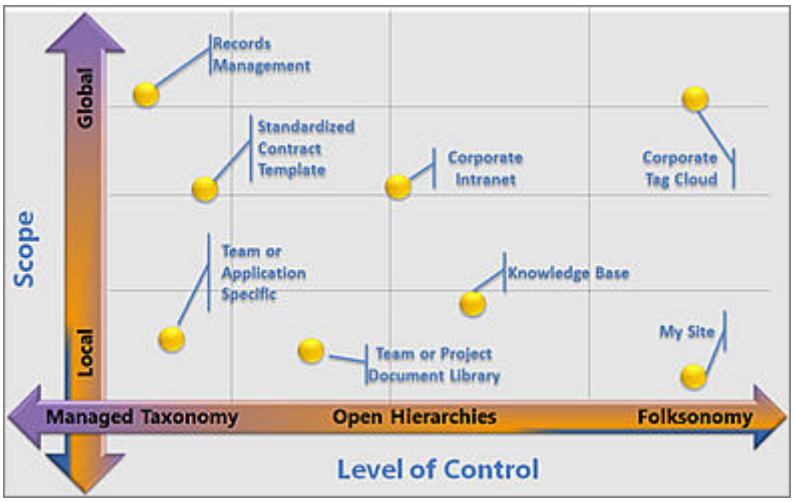
SharePoint metadata management supports a range of approaches to metadata, from formal taxonomies to user-driven folksonomies. You can implement formal taxonomies through managed terms and term sets. You can also use enterprise keywords which enable site users to tag content with keywords that they choose.

In addition, SharePoint products offer flexibility. You can choose how much structure and control to use with metadata, and you can choose the scope of control and structure. For example:

- You can apply control globally across sites, or make local to specific sites.
- You can configure term sets to be closed or open to user contributions.
- You can choose to use enterprise keywords with managed terms, or not.

SharePoint products enable organizations to combine the advantages of formal, managed taxonomies with the dynamic benefits of user-driven tagging in customized ways.

The following diagram shows how different requirements might use different levels of scope and control.



Benefits of managed metadata

There are several advantages to using managed metadata across the sites in an organization:

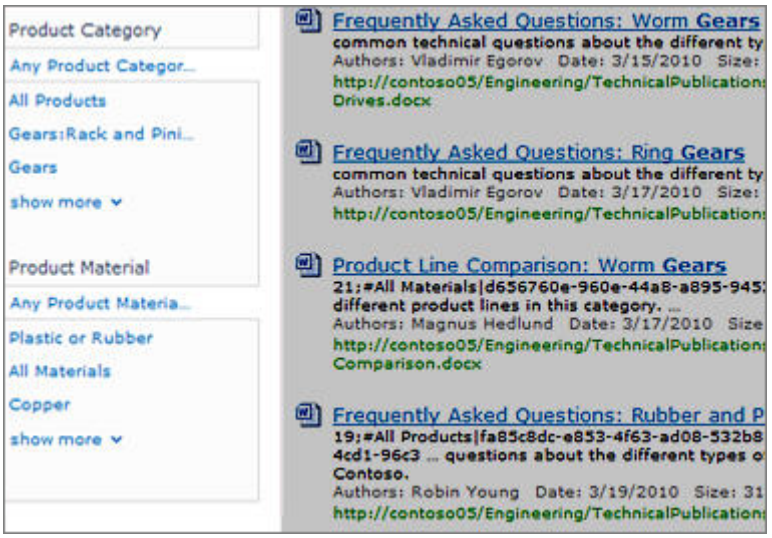
Consistent use of metadata

The managed metadata features in SharePoint products enable you to control how users add metadata to content. For example, by using term sets and managed terms, you can control which terms users can add to content, and you can control who can add new terms. You can also limit enterprise keywords to a specific list by configuring the Keywords term set as closed.

When the same terms are used consistently across sites, it is easier to build robust processes or solutions that rely on metadata. Additionally, it is easier for site users to apply metadata consistently to their content.

Improved content discoverability

When the content across sites in an organization has consistent metadata, it is easier to find business information and data by using search. Search features such as the refinement panel, which displays on the left-hand side of the search results page, enable users to filter search results based on metadata.



Metadata navigation for sites

Metadata navigation for sites enables a site administrator to create navigation elements based on metadata terms. For more information including performance recommendations, see Navigation options for SharePoint.

Metadata navigation for lists and libraries

Metadata navigation enables users to create views of information dynamically, based on specific metadata fields. Then, users can locate libraries by using folders or by using metadata pivots, and refine the results by using additional Key Filters. To learn how to set this up, see Set up metadata navigation for a list or library and Use grouping to modify a SharePoint view.

Increased flexibility

Managed metadata makes it easier for Term Store Administrators to maintain and adapt your metadata as business needs evolve. You can update a term set easily. And, new or updated terms automatically become available when you associate a Managed Metadata column with that term set. For example, if you merge multiple terms into one term, content that is tagged with these terms is automatically updated to reflect this change. You can specify multiple synonyms (or labels) for individual terms. If your site is multilingual, you can also specify multilingual labels for individual terms.

Managing metadata

Managing metadata effectively requires careful thought and planning. Think about the kind of information that you want to manage the content of lists and libraries, and think about the way

that the information is used in the organization. You can create term sets of metadata terms for lots of different information.

For example, you might have a single content type for a document. Each document can have metadata that identifies many of the relevant facts about it, such as these examples:

- Document purpose - Is it a sales proposal? An engineering specification? A Human Resources procedure?
- Document author, and names of people who changed it
- Date of creation, date of approval, date of most recent modification
- Department responsible for any budgetary implications of the document
- Audience

Here are some important activities that are involved with managing metadata:

- Planning and configuring
- Managing terms, term sets, and groups
- Specifying properties for metadata

Planning and configuring managed metadata

Your organization may want to do careful planning before you start to use managed metadata. The amount of planning that you must do depends on how formal your taxonomy is. It also depends on how much control that you want to impose on metadata.

If you want to let users help develop your taxonomy, then you can just have users add keywords to items, and then organize these into term sets as necessary.

If your organization wants to use managed term sets to implement formal taxonomies, then it is important to involve key stakeholders in planning and development. After the key stakeholders in the organization agree upon the required term sets, you can use the Term Store management tool to import or create your term sets. To learn how to access the tool, see Open the Term Store management tool

Managing terms, term sets, and groups

The Term Store management tool provides a tree control that you can use to perform most tasks. Your user role for this tool determines the tasks that you can perform. To work on global terms in the Term Store management tool, you must be a SharePoint Administrator and above in Microsoft 365, or a Term Store Administrator in SharePoint. To work on terms for a site, you can be a designated Group Manager or Contributor for term sets.

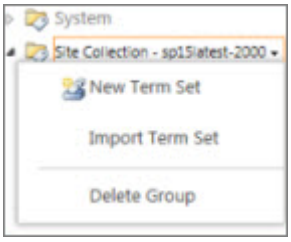
For more information, see Create and manage groups and term sets.

To take actions on an item in the hierarchy, follow these steps.

1. Point to the name of the Managed Metadata Service application, group, term set, or term that you want to change, and then click the arrow that appears.

2. Select the actions that you want from the menu.

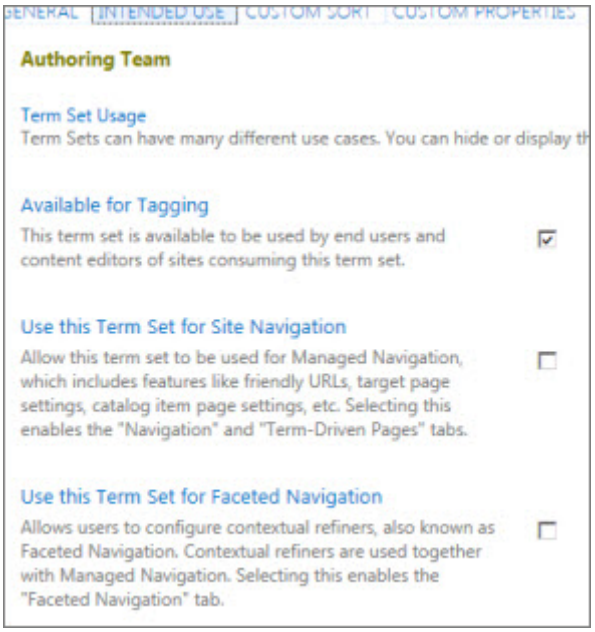
For example, if you are a Term Store Administrator or a Group Manager you can create, import, or delete term sets in a group. Term set contributors can create new term sets.



Properties for terms and term sets

At each level of the hierarchy, you can configure specific properties for a group, term set, or term by using the properties pane in the Term Store management tool. For example, if you are configuring a term set, you can specify information such as Name, Description, Owner, Contact, and Stakeholders in pane available on the **General** tab. You can also specify whether you want a term set to be open or closed to new submissions from users. Or, you can choose the **Intended Use** tab, and specify whether the term set should be available for tagging or site navigation.

> ⓘ **Note**
>
> These characters are not allowed in Taxonomy property names: `[` `]` `;` `"`, `<` `>` `|` `&` `\` `t`.



See also

Introduction to managed metadata in SharePoint Server

Set up metadata navigation for a list or library

Configure metadata navigation for a list or library

Add an enterprise keywords column to a list or library

Create a Managed Metadata column

Import term sets

Last updated on 06/25/2026

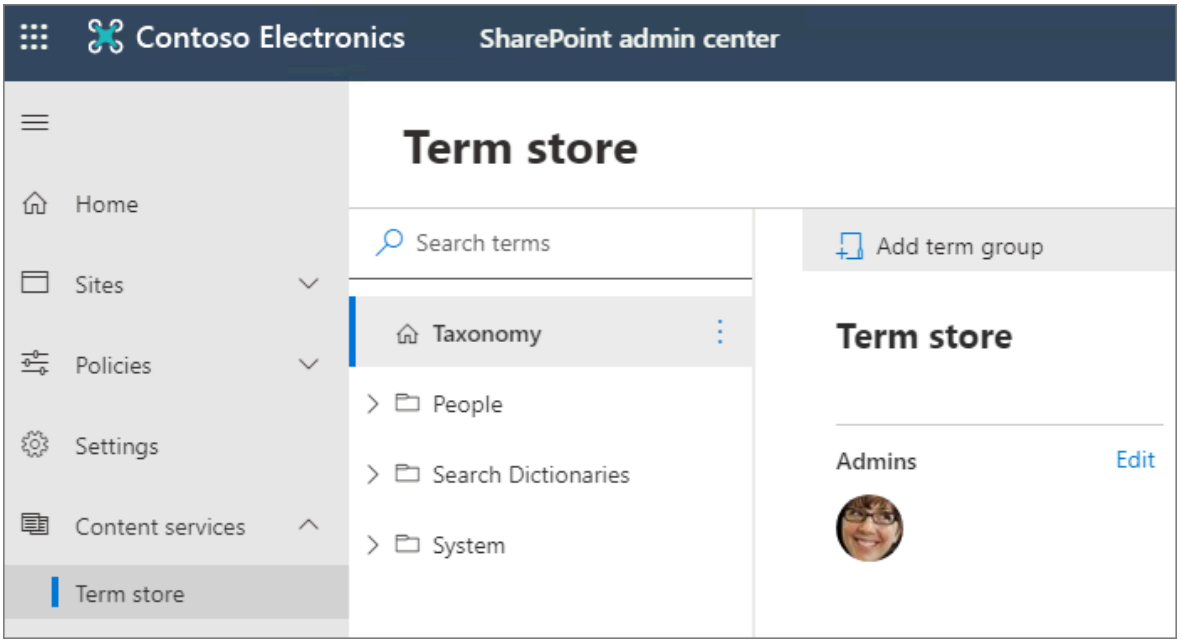
Open the Term Store Management Tool

Article • 07/22/2024

If you're a SharePoint Administrator and above in Microsoft 365, you can access the Term Store Management Tool from the SharePoint admin center.

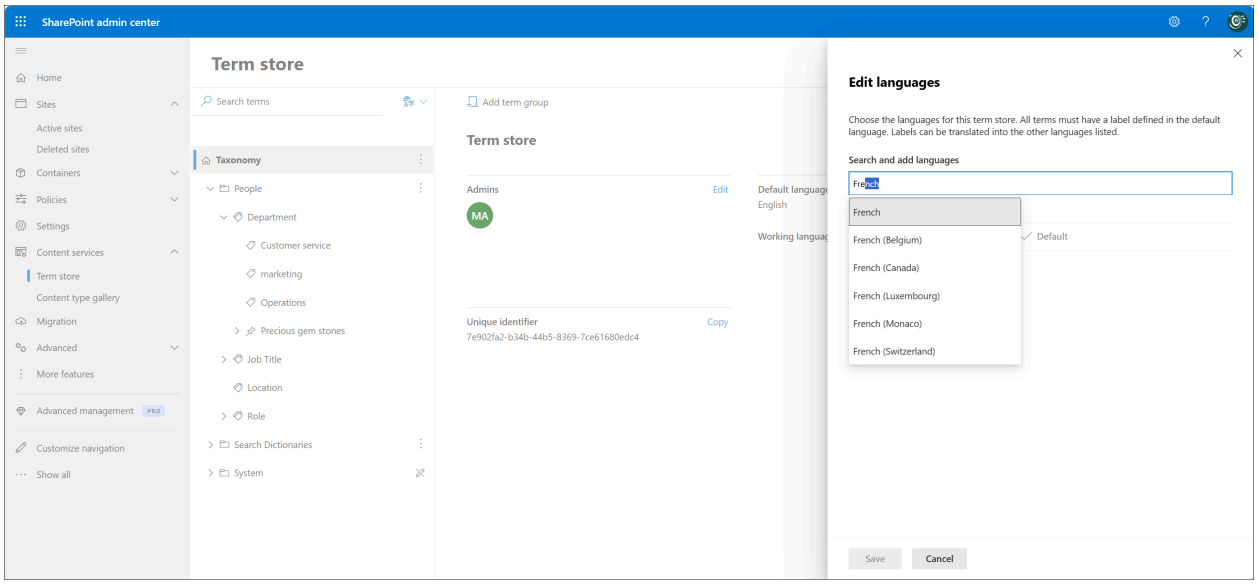
1. Open the SharePoint admin center.

2. In the left navigation, under **Content services**, choose Term store.



Manage the default language and working languages

If you need more than your default language for the terms, you can add working languages by selecting **Edit** next to **Default language**. The **Edit languages** panel shows up. You can type to search and add languages. You can also change the default language here.



Open term store management for a site

If you need to edit the local taxonomy for a site, you can open the term store management tool from the site.

1. For a site that you own, go to the **Site Settings** page.
2. Under **Site Administration**, select **Term store management**.

Feedback

Was this page helpful? Yes No

Provide product feedback

Set up a new group for term sets

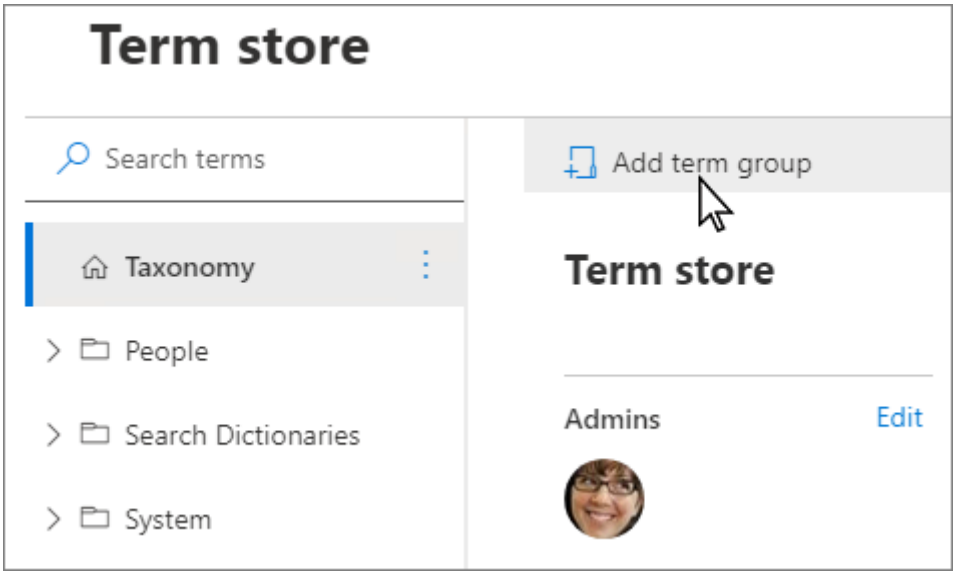
Article • 02/21/2023

A term group is a set of term sets that all share common security requirements. Only users who are designated as contributors to a specific group can manage term sets that belong to the group or create new term sets within it. Organizations should create unique groups for term sets that will have unique access or security needs. For information about how to create a term set, see Set up a new term set.

> **Important**
>
> To create a new term set group, you must be a term store admin.

To set up a new group for term sets, follow these steps.

1. In the SharePoint admin center, under **Content services**, select Term store.
2. In the right pane, click **Add term group**.



3. Enter a name for your new group, and then press ENTER.
4. To edit the Term group **name** and **description**, select **Edit** next to the group name. The **Edit name and description** panel appears. Enter a description to help users understand the purpose of this term group. Select **Save**.
5. To edit the group managers or contributors, select **Edit** next to **Group managers**. The **Edit admins** panel appears. Enter the names or email addresses of the people you want to add, assign them to a role, and then click **Save**.
6. To copy the unique identifier for this term group, select **Copy**.

Feedback

Was this page helpful? Yes No

Provide product feedback

Create and manage terms in a term set

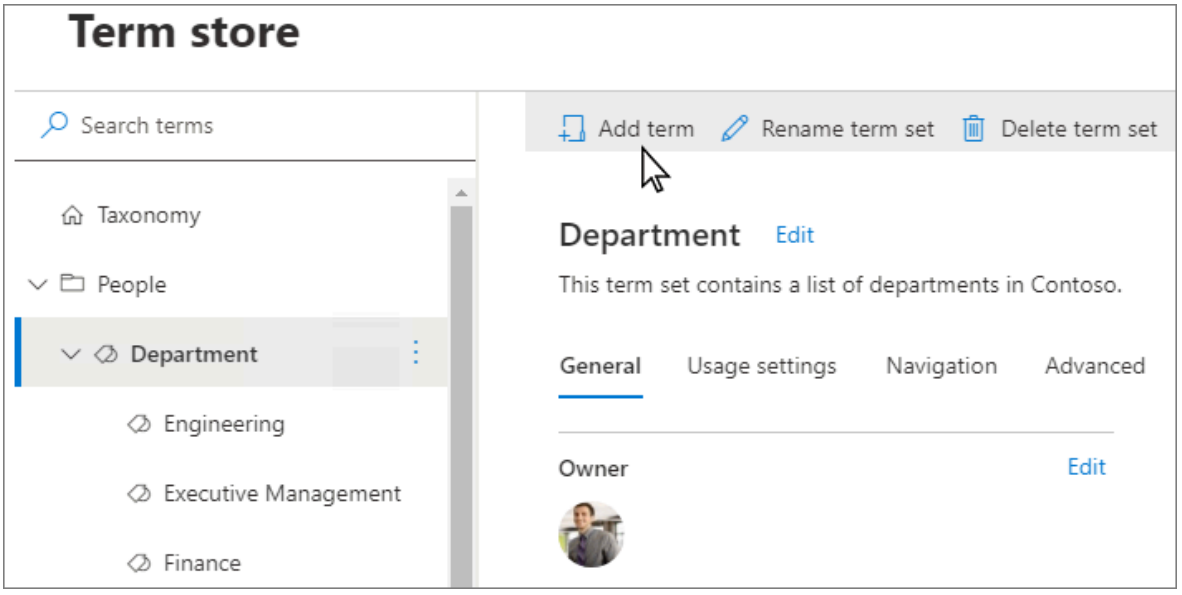
Article • 05/28/2024

To create and manage terms, you must be a contributor, a group manager, or a term store admin. (If you have many terms that you want to add, consider importing them.)

> **Note**
>
> If you are adding a term to a local term set, you must open term store management at the site level.

To create a term in a term set

1. In the SharePoint admin center, under **Content services**, select **Term store**.
2. In the tree-view pane, select the term set to which you want to add a term.
3. Select **Add term**.



4. Type a name for the term and press ENTER.
5. Update the term settings as needed:
   - On the **General** tab, to add languages, translations, and synonyms, select **+Add**. The **Add translation and synonyms** panel appears. Select your language, translation, description, and add synonyms. Select **Save**.

> **Note**

> If you don't see **+Add**, that's probably because you have only one working language, which is your default language. You can add more working languages by selecting **Taxonomy**, then selecting **Edit** next to **Default language**

- On the **Usage settings** tab, to make the term available to the users and content editors of sites consuming this term set, select **Edit**. The **Available for tagging** panel appears. By default, the term is enabled for tagging. To disable, select the **Enable** checkbox. Select **Save**.

- On the **Advanced** tab, to use shared or local custom properties to store more data about term sets, select **Edit**. The **Edit shared custom properties** panel appears. Add property names and values. Select **Save**.

Take another action with terms

There are several actions that you can take on terms that help you build and manage term sets as the business needs of your organization evolve.

To take any of the following actions, first select the term that you want to update.

Rename term

- Select **Rename term**.

Copy term

- Select **Copy term**. This action shows the name of the new term as **<original term name> - Copy**. No child terms for the source term are copied.

Copy term with children

Select **Copy term with children**. This action is only available on terms having at least one child term. This action shows the name of the new term as **<original term name> - Copy**. Children terms of the source term are also copied. Names of children terms are preserved as they are in the source term.

Move term

1. Select **Move term**. The **Move to** panel appears.

2. Select the target term set or term.

3. Select **Move**.

Delete term

If you delete this term, any terms below it will also be deleted. Terms that are shared with other term sets will be placed in the Orphaned terms set under System.

1. Select **Delete term**.

2. Select **Delete**.

Pin term

Pinning a term makes linked copies of the term and its children available at the destination. You can only create or edit the children of a pinned term at the source and the changes reflect everywhere the term is used.

1. Select **Pin term**. The **Pin term to** panel appears.

2. Select the target term set or term where you want to pin the term.

3. Select **Pin**.

Reuse term

Reusing a term makes linked copies of the term and its children available at the destination. You can create children for a reused term anywhere it's used but will exist only in the term set they were created.

1. Select **Reuse term**. The **Reuse term to** panel appears.

2. Select the target term set or term where you want to reuse the term.

3. Select the term, and then select **Reuse**.

Merge term

Merging this term with another will collapse its synonyms, translations, and custom properties into the other term.

1. Select **Merge term**. The **Merge to** panel appears.

2. Select the target term set or term where you want to merge the term.

3. Select **Merge**.

Deprecate term

This action makes any instances of this term in any term set to which it belongs unavailable for tagging. Child terms of the term aren't deprecated.

- Select **Deprecate term**.

Feedback

Was this page helpful? Yes No

Provide product feedback

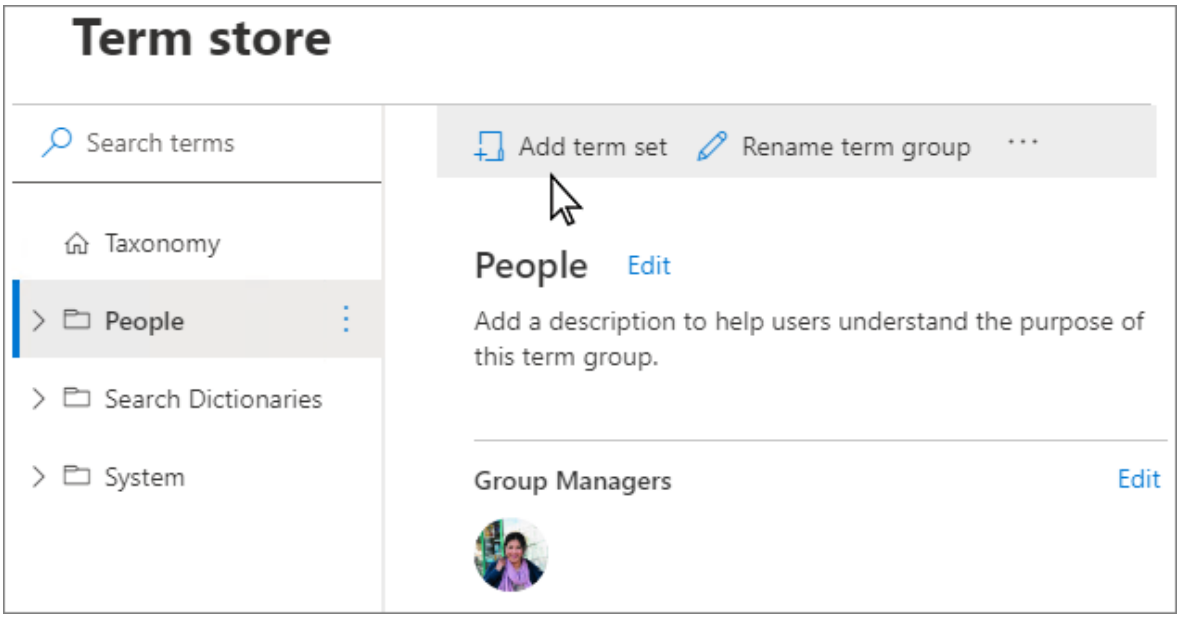
Set up a new term set

Article • 02/21/2023

To add a term set, you must be a contributor, group manager or a term store admin.

To set up a new term set

1. In the SharePoint admin center, under **Content services**, select Term store .
2. In the tree-view navigation pane, expand the groups to select the group to which you want to add a term set.
3. Click **Add term set**.



.

4. Type a name for the term set and press ENTER.

General tab

1. On the **General** tab, for **Owner**, select **Edit**. The **Edit Properties** panel appears. Specify the following information about who owns and maintains this term set:
   - **Term Set owner**: If you want the owner of the term set to be someone other than you, enter the person, group, or email address for who will maintain this term set.
   - **Stakeholders**: Add the names of users, groups, or email addresses that should be notified before major changes are made to the term set.
   - **Contact**: If you want site users to be able to provide feedback on the term set, enter an email address.

2. Click **Save**.

Usage settings tab

To configure the term submission policy

1. On the **Usage settings** tab, for **Submission policy**, select **Edit**. The **Edit submission policy** panel appears.

2. Specify whether you want the term set to be **Closed** or **Open**. If you select **Closed**, only people with contribute permissions can add terms to this term set. If you select **Open**, users can add terms from a tagging application.

3. Click **Save**.

To configure the tagging policy

1. Under the **Usage settings** tab, for **Available for tagging**, select **Edit**. The **Available for tagging** panel appears.

2. Select the **Enable** check box to make the terms in the term set available for tagging. If you clear the **Enable** check box, this term set won't be visible to most users. If the term set is still in development, or is not otherwise ready for use, you might want to clear the **Enable** check box.

3. Select **Save**.

Navigation tab

Enabling site navigation means you can use the terms in this term set for site navigation links with friendly URLs and dynamic content. Enabling faceted navigation means users can use refiners based on managed metadata from the search index to quickly browse to specific content

1. Under the **Navigation** tab, for **Use term set for site navigation**, select **Edit**. The **Edit Properties** panel appears.

2. Click the **Enable** check boxes to use this term set for site or faceted navigation.

3. Click **Save.**

Enabling either using the term set for site or faceted navigation enables options to set a custom target page and a custom catalog item page.

You can choose a custom target page if you want to display a specific page. Custom target pages that you set for individual terms will override this setting.

To set a custom target page

1. For **Custom target page**, select **Edit**. The **Edit term set target page** panel appears.
2. Move the toggle switch to enable **Use a custom target page**.
3. Click **Select**, and then select **Save**. The target page appears when users navigate to a friendly URL in this term set.

If terms in this term set are used as catalog categories, you can select the page used to render catalog data for items under those categories.

To set a custom catalog item page

1. For **Custom catalog item page**, select **Edit**. The **Edit term set catalog item page** panel appears.
2. Move the toggle switch to enable **Use a custom catalog item page**.
3. Click **Select** and then select **Save**.

Advanced tab

You can use machine translation to translate your terms, or you can export and import XLIFF files. You must repeat the translation each time you update the term set.

To configure translations

1. Under the **Advanced** tab, for **Translation**, select **Manage**. The **Translation** panel appears.
2. To use machine translation to translate this term set into the working languages for the term store, select **Start**. The **Machine translation** panel appears.
3. For the terms you want to translate, select either **All terms**, or **Only the terms updated since the last translation**.
4. From both the **Translate from** and **Translate to** dropdowns, select a language.
5. Click **Translate.**

You can use custom properties to store additional data about a term set.

To edit custom properties

1. For **Custom properties**, select **Edit**. The **Edit Custom properties** panel appears.
2. Enter a **Property name** and **Value**, and then select **Add**.\
3. Click **Save.**

To learn how to add a term to the new term set, see Create and manage terms in a term set.

Feedback

Was this page helpful? Yes No

Provide product feedback

Assign roles and permissions to manage term sets

Article • 02/21/2023

The tasks that you can do in the term store are determined by the specific role that you're assigned.

To be able to create or change a term, you must have one of three specific roles: term store admin, group manager, or contributor.

A term store admin can do these tasks:

- Create or delete term set groups.
- Add or remove group managers or contributors, or other term store admins
- Change the working languages for the term store.
- Any task that a group manager or contributor can do.

When you set up a term set, you can designate a group or a person as an Owner, Contact, or Stakeholders for the term set. These labels do not grant any specific permission to work with the term set. Instead, they provide a useful way to track the business owners or stakeholders for a term set.

Add term store admins

1. In the SharePoint admin center, under **Content services**, select Term store .
2. In the tree view pane on the left, select the taxonomy.
3. In the **Term store** page, for **Admins**, select **Edit**. The **Edit term store admin** panel appears. Enter the names or email addresses of the people who you want to add as term store admins. Select **Save**.

Add group managers

A group manager can do these tasks:

- Add or remove contributors.
- Any task that a contributor can do.

> **Important**
>
> You must be a term store admin to add new Group Managers.

To add a group manager:

1. In the SharePoint admin center, under **Content services**, select Term store.
2. In the tree view pane on the left, select the Group for which you want to add a Group Manager.
3. From the **People** page, select **Edit**. The **Edit name and description** panel appears. Add a term group name and description to help users understand the purpose of this term group. Select **Save**.
4. For **Group Managers**, to add people who can create new term groups, set and assign users to the group manager and contributor role, select **Edit**. The **Edit admins** panel appears. Enter the names or email addresses of the people who you want to add as Group Managers. Select **Save**.

Add contributors

A contributor can create or change a term set.

You must be either a term store admin or a group manager of a specific group to add contributors to that group.

1. In the SharePoint admin center, under **Content services**, select Term store.
2. In the tree view pane on the left, select the Group to which you want to add a Contributor.
3. For **Contributors**, set and assign users to the group manager and contributor role, select **Edit**. The **Edit contributors** panel appears. Enter the names or email addresses of the people who you want to add as Contributors. Select **Save**.

Metadata tasks that site users can perform

Site users who do not have an assigned role in the term store can use terms and terms sets in other ways.

Site members can do the following tasks with managed metadata:

- Update values in managed metadata columns (if terms sets associated with the columns are open and if the column lets fill-in choices).
- Add new terms to a term set when they update the value for a managed metadata column.
- Create new enterprise keywords when they update the enterprise keywords column for a list or library.
- Use metadata navigation in lists or libraries to filter the display of items.
- Use managed terms or enterprise keywords in search queries, and then refine search results based on these terms.

In addition, site users who have appropriate permissions (such as site owners) can create new managed metadata columns for lists, libraries, or content types. When site users create these columns, they can create new term sets that apply only to the site (previously called "site collection"), and they can manage the terms within these term sets.

Feedback

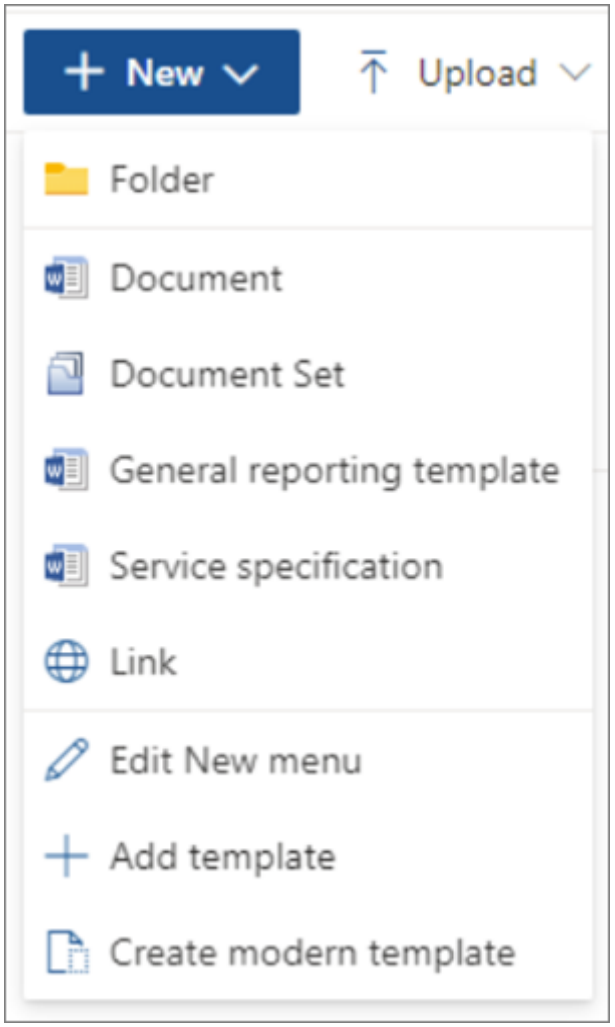
Was this page helpful? Yes No

Provide product feedback

Create or customize a content type

Article • 01/13/2025

Content types help make it easy to provide consistency across a site. You create or customize a content type with the characteristics that you want, such as a certain template, specific metadata, and so on. For example, when a user chooses an item from the **New Item** or **New Document** menu, you can ensure that customized content is used.



Content types created in the SharePoint admin center are saved to the SharePoint content type hub located at /sites/ContentTypeHub.

To learn more about content types, see Introduction to content types and content type publishing.

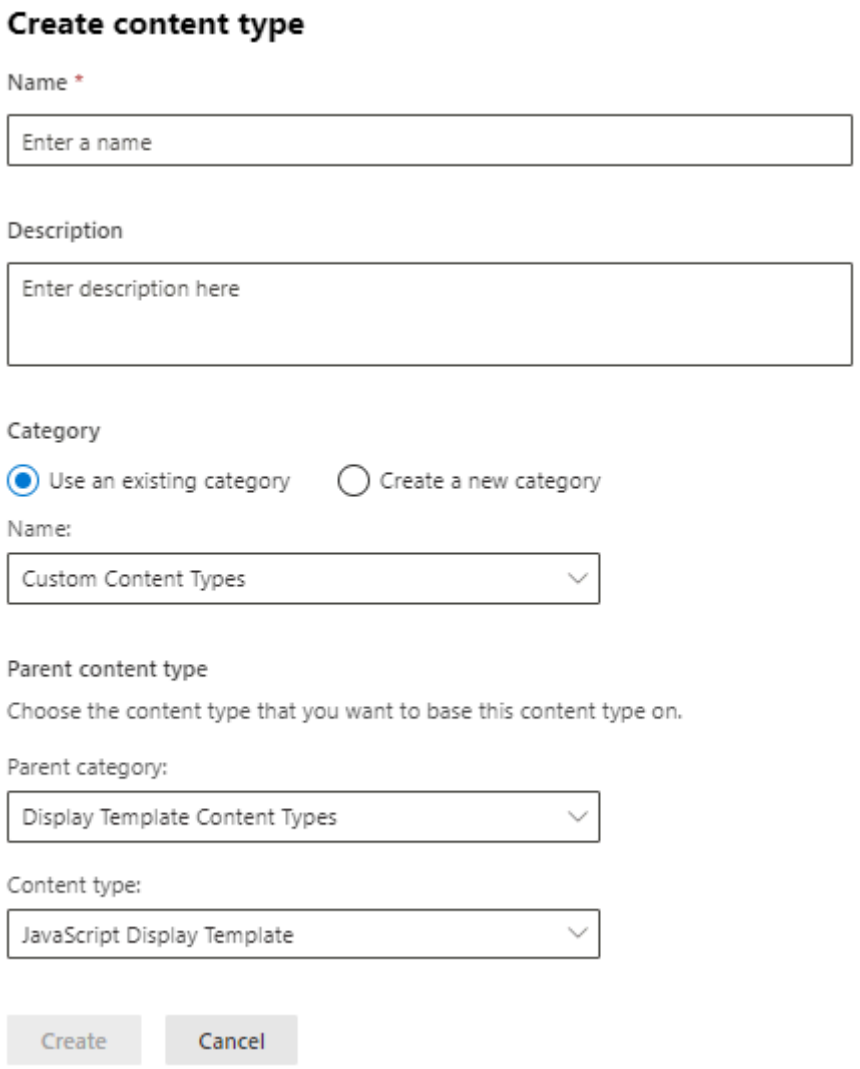
To understand how the built-in content types relate to each other, see SharePoint in Microsoft 365 default content type hierarchy.

Create a content type

1. Go to the **Content type gallery** in the SharePoint admin center, and sign in with an account that has admin permissions for your organization. The Content type gallery page isn't available if you have the global reader role.

2. Select **Create content type**. The **Create content type** panel appears.

3. On the **Create content type** panel, provide a name and description for the new content type.



4. In the **Category** section, you have two choices:

   - To put the new content type in an existing category, select **Use an existing category**, and from the **Name** dropdown, select a category.

   - To put the content in a new category, select **Create a new category**, and in the **Category name** box, provide a name.

5. In the **Parent content type** section, from the **Parent category** and **Content type** dropdowns, select the content type that you want to base this content type on.

6. Select **Create**.

The new content type appears in the **Content type gallery**.

Change the name of a content type

1. Go to the **Content type gallery** in the SharePoint admin center, and sign in with an account that has admin permissions for your organization. The Content type gallery page isn't available if you have the global reader role.

2. Under the **Site content type** column, select the name of the site content type that you want to change.

3. On the content type page, on the menu bar, select **Edit**. The **Edit content type** panel appears.

4. In the **Name** text box, change the name of the content type.

5. Select **Save**.

Associate a document template with a content type

To make sure that documents have consistent content across a site, you can associate a Word, Excel, or PowerPoint template with a site content type.

For example, you might want employees to use a standard Excel template when they create a weekly time sheet. If you associate the template with a Timesheet content type, every time someone uses the Timesheet content type, the correct template is automatically loaded in the worksheet.

You can make it even easier for users by adding the Timesheet content type to a library. Then, users can open the correct timesheet just by selecting **Timesheet** on the **New Documents** menu. To learn how to do this, see Add a content type to a list or library.

To associate a template with a content type

1. Go to the **Content type gallery** in the SharePoint admin center, and sign in with an account that has admin permissions for your organization. The Content type gallery page isn't available if you have the global reader role.

2. Under the **Site content type** column, select the name of the document-based content type that you want to change by associating a Word, Excel, or PowerPoint template.

3. In the menu bar, under **Settings**, select **Advanced Settings**. The **Advanced Settings** panel appears.

4. Enter the location of the template:

    - If the template is stored on your site, select **Use an existing template**, and then enter the URL for the template that you want to use. To edit the template, select **Edit template**.

    - If the document template is stored on your local computer, select **Upload a new document template**, and then select **Upload**. From the explorer page, locate the file that you want to use, select it, and then select **Open**.

5. Under **Permissions**, to select whether the content type can be modified, select either **Read** or **Edit**. You can change this setting later from this page by anyone with permissions to edit this content type.

6. Under **Update site and lists**, if you want to update all site and list content types that inherit from this content type with the settings on this page, select **Enable**.

7. Select **Save**.

Related topics

Add columns to a content type

Create or customize a site content type

Feedback

Was this page helpful? Yes No

Provide product feedback

Add columns to a content type

Article • 02/21/2023

The columns for a content type represent metadata. To add a metadata element, add a new column.

For example, your organization might want to track specific metadata for purchase orders, such as account number, project number, and project manager. If you add columns for this information to the purchase order content type, SharePoint prompts users to provide the information when they save their work. In addition, if you add the content type to a list or library, you can define a view to display the columns.

You can customize content types by adding columns of the types you need. You can also change the order of columns and specify if they are required fields.

Add a column to a content type

To add a column to a content type, follow these steps:

1. Go to Content type gallery in the SharePoint admin center, and sign in with an account that has admin permissions for your organization. The Content type gallery page isn't available if you have the global reader role.

2. Under the **Site content type** column, select the name of the site content type to which you want to add a column.

3. Under **Site columns**, from the **Add site column** dropdown, select **Add from existing site columns**. The **Add from existing site columns** panel appears.

4. In the **Select site columns from existing category** section, select **Add** or **Remove** to add or remove columns from the choices that appear. You can choose a category to narrow the list of available columns.

5. In the **Update List and Site Content Types** section, decide whether you want to update all site and content types that inherit from this content type with the settings on this page.

6. Select **Save**.

Change column order

To change column order for a content type, follow these steps.

To change column order on a content type

1. Go to Content type gallery in the SharePoint admin center, and sign in with an account that has admin permissions for your organization. The Content type gallery page isn't available if you have the global reader role.
2. Under the **Site content type** column, select the name of the site content type to which you want to change a column's order. That site content type page appears.
3. Under **Site columns**, in the **Name** column, select the column that you want to change its order.
4. Select the vertical ellipsis to the right of the site column name you selected, and from the dropdown, select **Reorder site columns** and then select from the following four choices:
    - **Move to top**
    - **Move up**
    - **Move down**
    - **Move to bottom**

Make a column required, optional, or hidden

To make a column required, optional, or hidden, follow these steps.

To make a column required, optional, or hidden

1. Go to Content type gallery in the SharePoint admin center, and sign in with an account that has admin permissions for your organization. The Content type gallery page isn't available if you have the global reader role.
2. Under the **Site content type** column, select the name of the site content type that you want to change a site content type by adding a column. That site content type page appears.
3. Under **Site columns**, in the **Name** column, select the name of the column that you want to make optional, required, or hidden.
4. Select **Edit site column settings**. The **Edit site column settings** panel appears.
5. In the **Show or hide site column** section, do one of the following:

- To show or hide this column in lists, check or clear **Show this column in lists**, respectively.
- To make it optional for users to specify information for a column, select **Optional (may contain information)**.
- To require users to specify information for a column, select **Required (must contain information)**.

6. Under **Update sites and lists**, if you want to update all site and list content types that inherit from this content type with the settings on this page, check the box.
7. Select **Save**.

> **Note**
>
> When you update the column name of an existing site column that is part of a published content type from the content type hub, ensure that the language of the target site and the language of the browser are the same for the latest site column name to appear correctly after the sync completes.

Related topics

Remove columns from a content type

Add columns to a content type

Add a content type to a list or library

Create, change, or delete a view of a list or library

Feedback

Was this page helpful? Yes No

Provide product feedback

Remove columns from a content type

Article • 02/21/2023

Columns can be added and removed from content types as necessary. To remove a column from a content type, follow these steps:

To remove a column from a content type

1. Go to the **Content type gallery** in the SharePoint admin center, and sign in with an account that has admin permissions for your organization. The Content type gallery page isn't available if you have the global reader role.
2. Under the **Site content type** column, select the name of the site content type to which you want to remove a column.
3. Under **Site columns**, select the column name you want to remove.
4. Select the vertical ellipsis to the right of the site column name you selected, and from the dropdown, select **Delete**. A **Delete site column** dialog box appears prompting you that this action will remove the column from the content type.
5. Select **Delete** to confirm.

Related topics

Add columns to a content type

Create or customize a site content type

Add a content type to a list or library

Remove columns from a content type

Feedback

Was this page helpful? Yes No

Provide product feedback

Publish a content type

Article • 02/21/2023

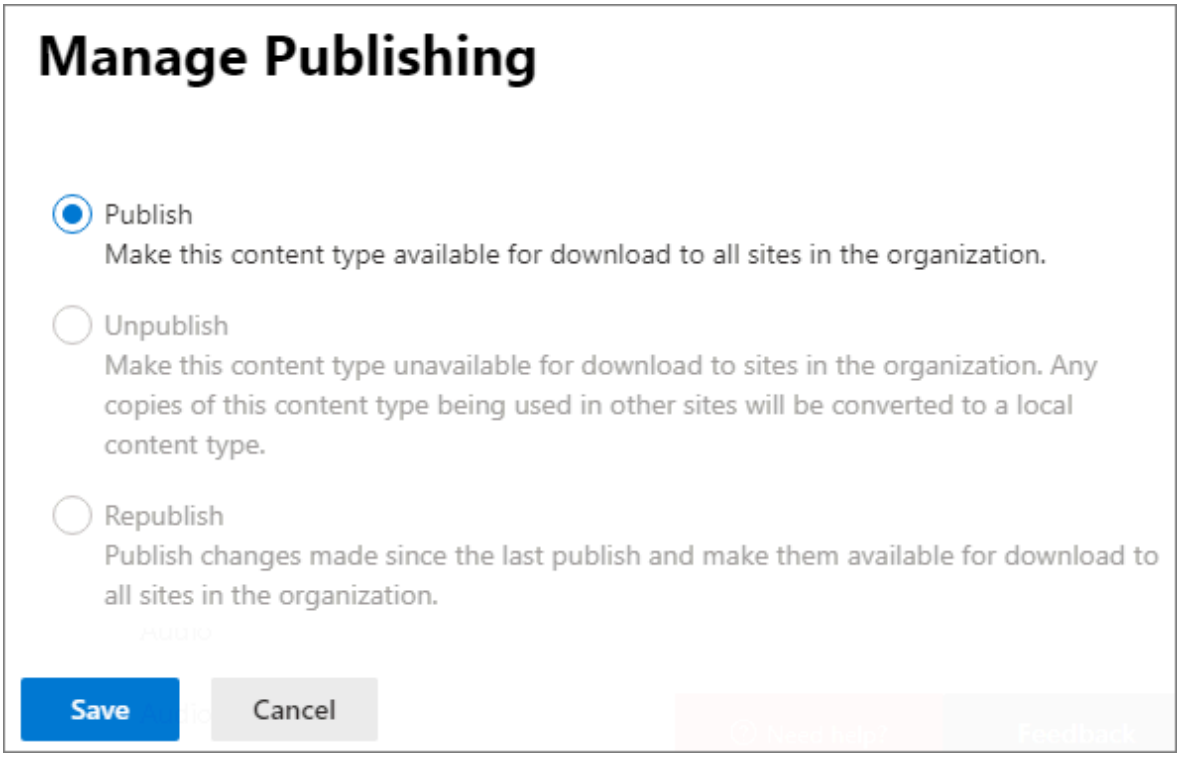
You can publish, unpublish, or republish content types in the content type hub at /sites/ContentTypeHub or from the SharePoint admin center.

To publish, republish, or unpublish a content type

1. Go to the **Content type gallery** in the SharePoint admin center, and sign in with an account that has admin permissions for your organization. The Content type gallery page isn't available if you have the global reader role.

2. Under the **Site content type** column, select the name of the site content type for which you want to manage updates. That site content type page appears.

3. In the menu bar, select **Publish**. The **Manage Publishing** panel appears.



4. On the **Manage Publishing** page, do one of the following:

   - To make this content type available for download to all sites in the organization, select **Publish**.

   - To publish updates to this content type, select **Republish**.

   - To make this content type unavailable for download to sites in the organization, select **Unpublish**. Any copies of this content type being used in other sites will be converted to a local content type.

5. Select **Save**.

Related topics

Publish a content type from a content publishing hub

Introduction to content types and content type publishing

Feedback

Was this page helpful? Yes No

Provide product feedback

Search experiences in SharePoint

Article • 02/21/2023

Microsoft Search is the modern search experience in SharePoint in Microsoft 365 and is a personalized experience. It uses the insights of the Microsoft Graph to show results that are relevant to you. Routine tasks such as finding the right version of a document, getting back to a presentation you were editing, or a document you were collaborating with others on, are easy. Learn more about Microsoft Search for users. The classic search experience, on the other hand, can be tailored more to your organization. Learn about the differences between the search experiences.

Both search experiences are turned on by default and as a search administrator you can't turn either search experience off. Which search experience your users see depends on where they search from:

- Users get the classic search experience on publishing sites, classic team sites, and in the Search Center.
- Users get the Microsoft Search experience on the SharePoint start page, hub sites, communication sites, and modern team sites. Learn about classic and modern sites.

  If you're in a document library, the search box shows **Search this library**. If you're in the home page of the site, the box shows **Search this site**. In all other locations, the search box shows **Search**.

Benefits of Microsoft Search in SharePoint

Easy to search - Microsoft Search suggests results based on users' previous activity in Microsoft 365, right in the search box. On the search results page the results are ordered by relevance.

Find shared files - Microsoft Search uses advanced query understanding to make finding shared files simple. Users can easily find files they're collaborating on.

Show relevant content - Promote the information and answers your users need to complete tasks, for example policies, benefits, resources, tools, and more. You can also target specific groups, like new hires or remote workers.

Administer across all apps - Microsoft Search is on by default and any administration you do applies to Microsoft Search in all the apps.

Easy to explore results - Users can explore results without leaving search. They can for example browse through a presentation directly in the search results page and quickly assess if it's the right result.

Mobile friendly - The Microsoft Search results page is mobile friendly.

User friendly interface - Microsoft Search offers a great user interface without a search administrator configuring anything. Learn more

Microsoft Search evolves - The set of content types users can search for and the intelligence of the search box will grow over time. Learn what's coming next in Microsoft Search

When to use which search experience?

Which experience your users see depends on whether your organization mostly uses classic or modern sites. If you believe that Microsoft Search gives your users the best experience, learn how to get started with Microsoft Search in SharePoint.

Should you use the Search Center or the SharePoint start page as your portal?

If you need custom refiners or search verticals for organization-specific content, or you need to display results for organization-specific content differently than other content. Use the Search Center (classic search) as your portal. If not, we recommend promoting the SharePoint start page (Microsoft Search) to your users.

Is the search experience impacted if you migrate from classic to modern sites?

Yes, if you have customized search. A classic site has a classic search box. For example, you've set up the search box to redirect to a custom Search Center in order show results that are filtered and formatted for organization-specific content types. The modern site has the Microsoft Search box. You can't customize the Microsoft Search experience like that. If you don't need to customize search, we recommend using modern sites.

Can users search across all sites of an administrative unit?

It's possible, but it takes some effort to do this with classic search. It's better to use a hub site to organize the sites. Hub sites use Microsoft Search, which is scoped to search

for news, people, files, and sites across all sites that are associated with the hub. Learn more about hub sites

Can you use Microsoft Search in combination with cloud hybrid search?

Yes. With cloud hybrid search, both on-premises and online content go into the same index, which both the classic and Microsoft Search experiences use.

Feedback

Was this page helpful? Yes No

Provide product feedback

Overview of search in SharePoint

Article • 04/25/2024

If you're responsible for search in your organization, learn how you can tailor the search experience to your organization and make search even better for your users.

SharePoint in Microsoft 365 has both a classic and a modern search experience, where Microsoft Search in SharePoint is the modern search experience. As a search admin, you can't enable or disable either search experience, both are enabled by default.

Users get the classic search experience on publishing sites, classic team sites, and in the Search Center. Users get the Microsoft Search experience on the SharePoint start page, hub sites, communication sites, and modern team sites. The most visible difference is that the Microsoft Search box is placed at the top of SharePoint, in the header bar. Another difference is that Microsoft Search is personal. The results one user sees are different from what other users see, even when they search for the same words. Users see results before they start typing in the search box, based on their previous activity and trending content in Microsoft 365, and the results update as they type. The search results are easy to explore without any effort from you as an admin. Learn more about the Microsoft Search experience for users in Find what you need with Microsoft Search.

Both search experiences use the same search index to find search results. You can customize and tailor the classic search experience more than Microsoft Search in SharePoint. Some classic search settings can impact both experiences, learn how to avoid impacting Microsoft Search. Read When to use which search experience to decide which experience is best for your organization.

See the following main areas where you can customize and impact the search experience and make sure that search is performing the way you want. The high-level overview of How search works can also help you understand where and how you can impact the search experience in SharePoint.

Many of the classic search features are available on the search administration page in the SharePoint admin center.

1. Make sure the content can be found

The content must be crawled and added to the search index for your users to find what they're looking for when they search in SharePoint. Microsoft Search uses the same index of SharePoint content as classic search does.

See how you can make content searchable, and how you can crawl content to get it into the search index. Also, see how you can help users search for content across Microsoft 365 and on-premises SharePoint Server at the same time. Learn more

2. Make the search results look great

Presenting the search results the right way makes content easier to find.

See how you can manage the classic experience in the Search Center in SharePoint, and how you can use the different search Web Parts to help each user find what they're looking for. See Make the search results look great

3. Show relevant search results

All search results are not relevant to everyone all the time.

See how you can show each user exactly the results they're looking for. See Show the right search results

4. Check logs, limits and reports

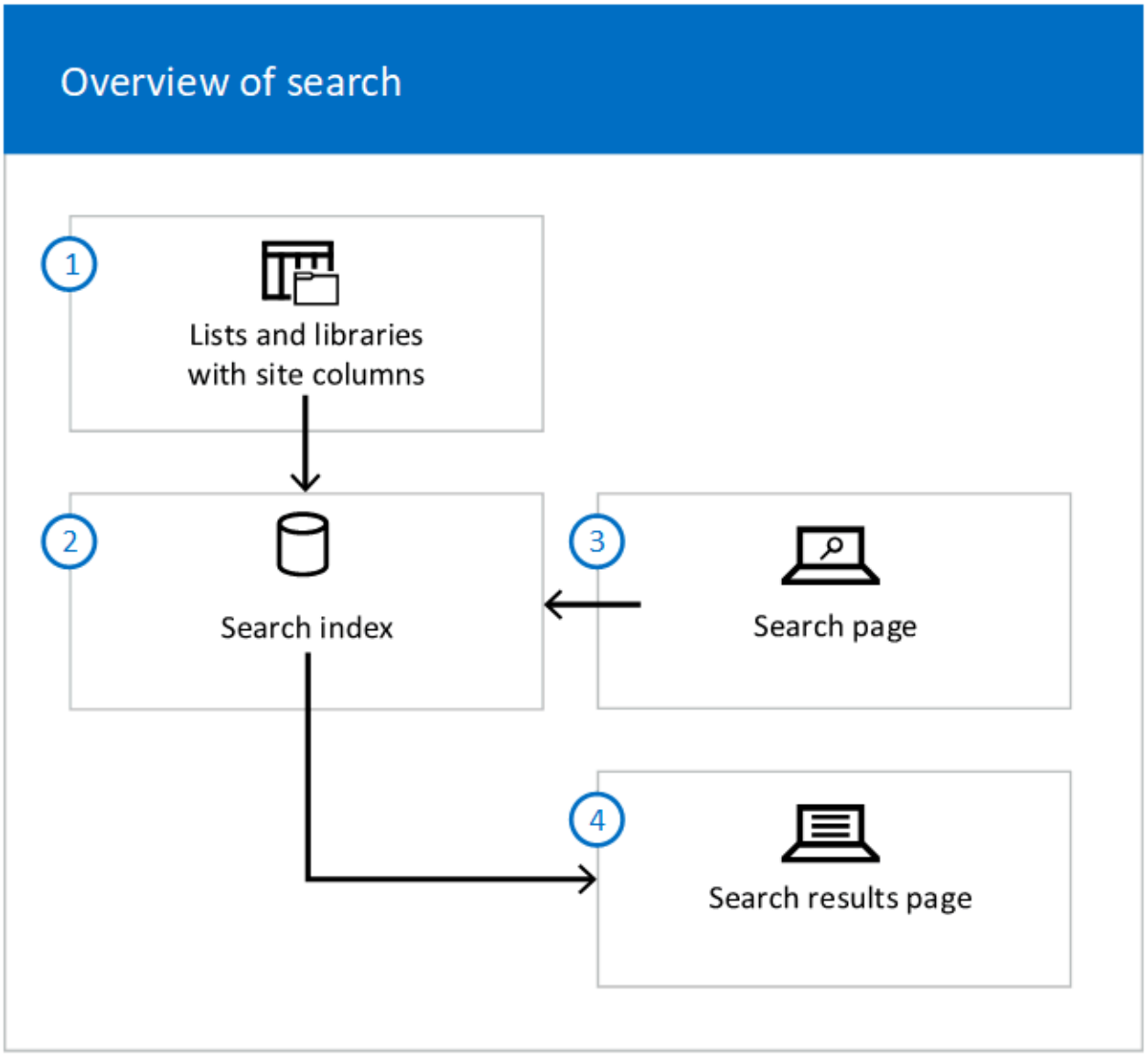
See how you can check if the crawler has added content to the search index, and if your users are finding what they're looking for. Look up the limits for search, for example how many entries you can have in a custom search dictionary. See Check logs, limits and reports

How search works

This high-level overview of how search works can help you understand where and how you can customize the search in SharePoint.

In lists and libraries, site columns store detailed information about each document.

1. Search **crawls** the lists and libraries and adds the site columns and values to the search index.
2. In the **search index**, site columns are mapped to managed properties.
3. When a user enters a **query** in a search box, the query is sent to the search index.
4. The search engine finds **matching results**, and sends them to a search results page.



See also

Learn about Microsoft Search

Get started with Microsoft Search in SharePoint

Feedback

Was this page helpful? Yes No

Provide product feedback

View search usage reports in modern sites

Article • 11/28/2022

If you're a SharePoint Administrator in your organization, you're probably asked questions about search usage, such as:

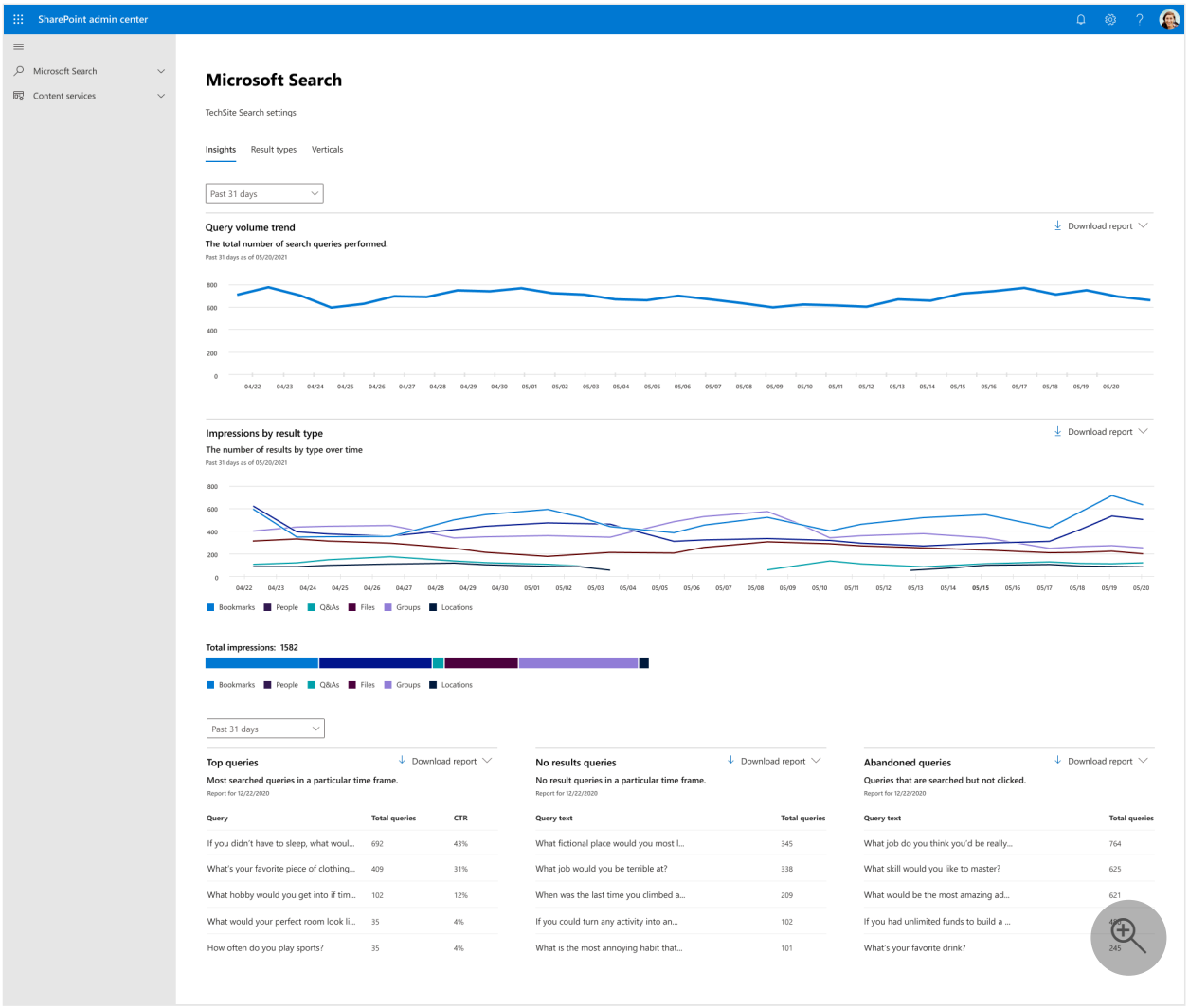
- What are the top queries on my site per day or per month?
- How many search queries are users performing on average?
- Which queries are getting low clicks as they're not showing up in any results?
- How often are query rules firing and how often are people clicking promoted results?

To view a report

To view search usage reports in modern sites, navigate to **Site settings** > **Site collection administration** > **Microsoft Search** > **Configure search settings** > **Insights**.

Modern search usage reports with Microsoft Search provide a few graphs and tables generated from searches that are executed from search in modern sites. You can see data from the past 31 days (about one month), per day, or monthly for the previous year.

The first date picker lets you pick past 31 days (about one month) or past 12 months for the first two graphs. The second date picker lets you select a particular day or month for the bottom three tables (top, abandoned, no results). Downloading a report will allow you to see reports from a broader range of time. Click on the download arrow and select past 31 days (about one month) or past 12 months. The report is downloaded as an Excel spreadsheet. If you selected the past 31 days (about one month), the spreadsheet will have an individual tab for each day. The past 12 months download will have a tab for each month.



Overview of search reports

Expand table

Report	Description
Query Volume	This report shows the number of search queries performed. Use this report to identify search query volume trends and to determine periods of high and low search activity.
Top Queries	This report shows the most popular search queries. A query is added to this report when it's searched at least three times with a click on a result. Use this report to understand what types of information your users are searching for.
Abandoned Queries	This report shows popular search queries that receive low click-through. Use this report to identify search queries that might create user dissatisfaction and to improve the finding of content.
No Results Queries	This report shows popular search queries that returned no results. Use this report to identify search queries that might create user dissatisfaction and to improve the finding of content.

Report	Description
Impression distribution	This report shows impressions over various time frames. The timeline shows the daily number of impressions for a result type. Determine which result type is most frequently, or infrequently, used. Use this report to understand what result types users are using and any changes in user behavior over a period of time.

Related topics

Microsoft 365 Reports in the Admin Center - SharePoint site usage

Microsoft 365 Reports in the Admin Center - SharePoint activity

Feedback

Was this page helpful? Yes No

Provide product feedback

SharePoint classic search administration overview

Article • 02/21/2023

As a SharePoint Administrator and above in Microsoft 365, you can customize and impact the search experiences for your users. You can define searchable managed properties in the search schema, identify high-quality pages to improve relevance, manage query rules and result sources, and remove individual results. You can also evaluate any changes by viewing reports about usage and search.

The changes you make from the search administration page are valid for the whole tenant, but you can also customize search on site collection level and on site level.

You can customize and tailor the classic search experience more than Microsoft Search in SharePoint. Some classic search settings can impact both experiences, learn how to avoid impacting Microsoft Search.

How to get to the classic search administration page

1. Go to **More features** in the SharePoint admin center, and sign in with an account that has admin permissions for your organization.

   > **Note**
   >
   > If you have Office 365 operated by 21Vianet (China), sign in to the Microsoft 365 admin center, then browse to the SharePoint admin center and open the More features page.

2. Under **Search**, select **Open**.

What do you want to do?

Expand table

Choose this option:	To do this:
Manage the search schema	Learn how to create a customized search experience by changing the search schema. In the search schema, you can view, create, or change

Choose this option:	To do this:
	managed properties, and map crawled properties to managed properties.
Manage search dictionaries	Learn how to manage search dictionaries for classic search. You can use search dictionaries to include or exclude company names to be extracted from the content of your indexed documents, or you can include or exclude words for query spelling correction.
Manage authoritative pages	Influence the pages or documents that should appear at the top of the search results by identifying high-quality pages, also known as authoritative pages, for the classic search experience.
Manage query suggestion settings	Learn how to add phrases that you want the system to suggest to users as they search for an item using classic search, and how to add phrases that you don't want the system to suggest to users. Also, learn how to turn this feature on or off.
Manage result sources	Result sources limit searches to certain content or to a subset of search results. Learn how to create your own result sources, or change the predefined result sources.
Manage query rules	Improve search results in the classic search experience by creating and managing query rules. Query rules can help searches respond to the intent of users.
Manage query client types	Learn how query client types decide in which order queries are performed in the classic search experience.
Remove search results	Learn how you can temporarily remove items from the search results with immediate effect. These items can be documents, pages, or sites that you don't want users to see when they search.
View usage and search reports	View usage reports and search reports and see how often your users search, what their top queries are, and which queries they're having trouble getting answers for.
Manage Search Center settings	Choose where searches in the classic search experience should go by specifying the URL of your Search Center.
Import and export customized search configuration settings	Learn how to export and import customized search configuration settings between tenants, site collections, and sites.
Manage crawl log permissions	Learn how to grant users or groups read access to crawl log information for the tenant. A typical use case is in eDiscovery, where users may need to check whether crawled content was in fact added to the search index.

Note

Thesaurus isn't available in SharePoint in Microsoft 365.

See also

Search limits for SharePoint

Feedback

Was this page helpful? Yes No

Provide product feedback

Make sure content can be found

Article • 10/03/2022

The content must be crawled and added to the search index for your users to find what they're searching for in Microsoft SharePoint. SharePoint in Microsoft 365 has both a classic and a modern search experience, both use the same search index. Learn about the differences between the classic and modern search experiences in SharePoint

Make site content searchable

When users search on a site, results can come from many places such as columns, libraries, and pages. A site owner can change search settings to decide whether or not content should appear in search results.

Users only see search results for content they have access to. Setting the right permissions for content ensure that people can see the right documents and sites in the search results. Learn more.

Crawl site content

In SharePoint, content is automatically crawled based on a defined crawl schedule. The crawler picks up content that has changed since the last crawl and updates the index.

In some cases, you may want to manually request crawling and full re-indexing of a site, a document library, or a list. Learn more.

Search across on-premises and online content

Hybrid search in SharePoint lets your users search for files and documents across SharePoint Server and Microsoft 365 at the same time. With cloud hybrid search, both on-premises and online content go into the index that both the classic and Microsoft Search experiences use.

Remove search results temporarily

You can **temporarily** remove documents, pages and sites from search results with immediate effect. Learn more.

Feedback

Was this page helpful? Yes No

Provide product feedback

Enable content on a site to be searchable

When users search on a site, results can come from many places such as columns, libraries, and pages. A site owner can change search settings to decide whether content is allowed to appear in search results. Permissions on content also affect whether users are allowed to see the content in search results. A good understanding of how permissions and search settings work can help you ensure that users can see the right documents and sites in the search results.

> **Note**
>
> Search results are always security trimmed, so users will only see content they have permission to see. The search settings only define what content is included in the search index.
>
> There are specific scenarios where users have permissions to see the content but are still unable to find it in the search results. For more details, see Search results don't appear for group owners after creating a new Office 365 group.

Plan to make your content available in search results

As a site owner, you can use settings to control whether content can appear in search results. Content is stored in many places including sites, lists, libraries, Web Parts, and columns. By default, most content contained in a site, list, library, Web Part page, or column will be crawled and added to the search index. What's in the search index decides what content can appear in search results both in the **classic** and **modern** search experiences. The permissions that are set on items, lists, libraries, sites, and so forth, also affect whether users can see the content in search results.

Site owners and site collection administrators can choose whether content can appear in search results. By default, the content of a site can appear in search results. If a site owner or site collection administrator specifies that the content from a particular site can't appear in search results, then the other search results settings such as those for lists, libraries, ASPX pages, and columns set on that site wouldn't have any effect.

Similarly, if a site owner or site collection administrator prevents list or library content from appearing in search results, then excluding columns wouldn't have any effect. It's important to know what settings are inherited from higher levels in order to plan search effectively.

Understand search settings and permissions

One of the responsibilities of a site owner is to control who has access to content. You can give some people permission to read and change content, allow others to only read content, and prevent others from viewing content entirely. In order to accommodate this flexibility, you use permissions groups, which are assigned specific permission levels. To allow users access to the site or to content on that site, a site owner assigns users to one or more security groups. By using permissions settings in conjunction with search results settings, the site owner can manage whether users can see content in search results.

For example, let's say Joe is working on a Request for Proposal (RFP) in Microsoft Office Word and is collaborating with a team of 10 people. His team site has 50 users, all of whom are Site Members. Joe isn't ready for the whole team to view the RFP. Therefore, when he uploads it to the team site, he sets the permissions so that only the team of 10 can view and edit it. Until he grants all 50 people read permissions, only the 10 people who have permission to view the document will see it listed in search results.

Permissions can be applied to lists, sites, views, and Web Parts. Also, permissions can be dependent on other permissions. All of this can affect what the user sees in search results. Therefore, before adding any content to your site, you may want to familiarize yourself with SharePoint's permissions model, the permissions model of your site or organization, or to plan what the permissions model will be for your site.

See also: Default SharePoint Groups in SharePoint

Show content on a site in search results

As a site owner, you can choose whether the content on your site can appear in search results. By default, all site content can appear in search results. The person who's viewing search results must have permission to view the content.

> ⓘ **Note**
>
> To change this setting, you must have the Manage Permissions permission level. This permission level is included in the " *Site Name* " Owner group.

1. On the site, select **Settings** , and then select **Site settings**. If you don't see **Site settings**, select **Site information**, and then select **View all site settings**.

2. Under **Search**, click **Search and offline availability**.

3. In the **Indexing Site Content** section, under **Allow this site to appear in Search results**, select **Yes** to allow the content of the site to appear in search results.

To prevent the content from appearing in search results, select **No**.

Show content from lists or libraries in search results

As a site owner, you can decide whether items in lists and libraries on your site are included in search results. By default every list and library is set to include all items in search results.

> **Note**
>
> To change this setting, you must have the Manage Lists permission level. The Designer and " *Site Name* " Owner groups contain this permission level. When you do not have Manage Lists permissions, the menus described in this procedure aren't available.

1. On the site, find and click the list or library you want to customize.

2. Select **Settings**, and then select **Site settings**. If you don't see **Site settings**, select **Site information**, and then select **View all site settings**.

3. Under **Site Administration**, click **Site Libraries and lists**.

4. Click an item from the list, for example, **Customize "Shared Documents."**

5. On the List Settings page, under **General Settings**, click **Advanced settings**.

6. In the **Search** section, under **Allow items from this document library to appear in search results**, select **Yes** to include all of the items in the list or library in search result.

To prevent items from the list or library to appear in search results, select **No**.

Show contents of ASPX pages in search results

You can control whether the content of ASPX pages is included in search results. When you create a site, many content pages are created automatically. For example, default.aspx, allitems.aspx for your Web Part gallery, and several others are automatically created pages. You can also create custom ASPX pages.

By default, when a Web Part displayed on an ASPX page uses information from a list or library that contains restricted permissions, also known as fine-grained permissions, none of the content in any of the ASPX pages on the site is included in search results. This prevents non-authorized users from viewing content.

For example, let's say five documents are displayed in a Shared Documents Web Part on a team site with 50 members. One of the documents has restricted permissions; only a few people are allowed to see it. Content is automatically hidden from that site in search results so that the content from that document does not appear when users search. This prevents the content of the ASPX page from unintentionally being exposed to people who are not supposed to see it.

You have the option of ignoring this setting to display all content in search results regardless of permissions. In this case, all content can appear in the search results, but unauthorized users will not be able to access the actual documents. Another option is to not include any ASPX content in search results, regardless of permissions.

> **Note**
>
> To change this setting, you must have the Manage Permissions permission level. This permission level is included in the " *Site Name* " Owner group.

1. On the site, select **Settings**, and then select **Site settings**. If you don't see **Site settings**, select **Site information**, and then select **View all site settings**.
2. Under **Search**, click **Search and offline availability**.
3. In the **Indexing ASPX Page Content** section, select one of the following options:

Expand table

Option	Description
Do not index Web Parts if this site contains fine-grained permissions	When permissions of the ASPX page are different from the parent site, no content on the site appears in search results.
Always index all Web Parts on this site	Show content of all ASPX pages on the site in search results regardless of permissions.
Never index any Web Parts on this site	Hide content of all ASPX pages on the site from search results regardless of permissions.

Exclude content in columns from search results

As a site owner you can control whether the content in specific columns in lists or libraries appears in search results. By default, all content is included in search results. This setting is useful when you want to prevent sensitive data from appearing in search results.

> **Note**
>
> To change this setting, you must have the Manage Permissions permission level. This permission level is included in the "*Site Name*" Owner group.

1. On the site that contains the list or library, select **Settings**, and then select **Site settings**. If you don't see **Site settings**, select **Site information**, and then select **View all site settings**.

2. Under **Search**, click **Searchable columns**.

   The option is only visible for sites with the classic publishing feature enabled. If the option is not visible navigate directly to `<Site URL>>/_layouts/15/NoCrawlSettings.aspx`.

3. In the **Excluded Columns from Search Indexing** section, under **Excluded**, check the box next to the Column Name for the column you want to exclude in search results.

> **Note**
>
> Columns that appear are those that belong to the current site.

Crawl and re-index a site

When people search for content on your SharePoint sites, what's in your search index decides what they'll find. The search index contains information from all documents and pages on your site. In SharePoint, content is automatically crawled based on a defined crawl schedule. The crawler picks up content that has changed since the last crawl and updates the index.

For cases in which the Search schema has changed where a managed property has been added/removed/changed, you will want to specifically request a full re-indexing of a site. See Manually request crawling and re-indexing of a site for more information.

Last updated on 06/25/2026

Manually request crawling and reindexing of a site, a library or a list

Article • 04/15/2025

In SharePoint, content is automatically crawled based on a defined crawl schedule. The crawler picks up content that has changed since the last crawl and updates the index. You'll want to manually request crawling and full reindexing of a site, a document library, or a list after a schema change has occurred.

> **Caution**
>
> Reindexing a site can cause a massive load on the search system. Don't reindex your site unless you've made changes that require all items to be reindexed.

Reindex after changing managed properties

When people search for content on your SharePoint sites, what's in your search index decides what they find. The search index contains information from all documents and pages on your site.

The search index is built up by crawling the content on your SharePoint site. The crawler picks up content and metadata from the documents in the form of crawled properties. To get the content and metadata from the documents into the search index, the crawled properties must be mapped to managed properties. Only managed properties are kept in the index. This means that users can only search on managed properties.

When you change a managed property, or when you change the mapping of crawled and managed properties, the site must be recrawled before your changes are reflected in the search index. Because your changes are made in the search schema, and not to the actual site, the crawler won't automatically reindex the site. To make sure that your changes are crawled and fully reindexed, you must request a reindexing of the site. The site content is recrawled so that you can start using the managed properties in queries, query rules and display templates.

You can also choose to only reindex a document library or a list. When you've changed a managed property that's used in a library or list, or changed the mapping of crawled and managed properties, you can specifically request a reindexing of that library or list only. All of the content in that library or list is marked as changed, and the content is picked up during the next scheduled crawl and reindexed.

Learn more about search and crawled and managed properties in Manage the search schema in SharePoint.

See also: Enable content on a site to be searchable

Reindex a site

1. On the site, select **Settings**, and then select **Site settings**. If you don't see **Site settings**, select **Site information**, and then select **View all site settings**.
2. Under **Search**, select **Search and offline availability**.
3. In the **Reindex site** section, select **Reindex site**.
4. A warning appears, check the box before **Please check this box to acknowledge and agree to the statement above.** Select **Reindex site** again to confirm. The content is reindexed during the next scheduled crawl.

Reindex a document library or a list

1. On the site, go to the list or library that you want to reindex.
2. In the upper right corner, select **Settings**, and then choose **Library Settings** or **List Settings**.
3. On the Settings page, under **General Settings**, choose **Advanced settings**. If you don't see the **Settings** page, you may need to choose **More library settings** or **More List settings**.
4. Scroll down to **Reindex Document Library** or **Reindex List**, and select the button. A warning appears. Select the button again to confirm. The content is reindexed during the next scheduled crawl.

Remove search results

Article • 07/19/2024

As a user who has SharePoint administrator or above permissions in Microsoft 365, you can temporarily remove items from search results with immediate effect. The items that you can remove can be documents or pages that you don't want users to see. An example of this could be a Word document containing an invitation to an event that has been canceled, but the organizer has not removed the document from the site yet. Removing a result removes it from both classic and modern search results.

> **Important**
>
> This is only a quick fix! Unless you delete the items or change the permissions of items manually, they will show up again in your search results after the next crawl.

1. Go to **More features** in the SharePoint admin center, and sign in with an account that has admin permissions for your organization.

   > **Note**
   >
   > If you have Office 365 operated by 21Vianet (China), sign in to the Microsoft 365 admin center, then browse to the SharePoint admin center and open the More features page.

2. Under **Search**, select **Open**.

3. On the **search administration** page, select **Remove Search Results**.

4. On the **Remove Search Results** page, in the **URLs to remove** box, enter the URLs that you want to remove from the search results, for example, https://contoso.sharepoint.com/sites/site1. URLs cannot contain a wildcard (*) character. Enter one URL on each line.

5. Select **Remove Now**. The URLs are immediately removed from your search results.

Feedback

Was this page helpful? Yes No

Provide product feedback

Make the search results look great

Presenting the search results the right way makes content easier to find for users.

SharePoint has both a classic and a modern search experience, where Microsoft Search in SharePoint is the modern search experience. Learn about the differences between the search experiences in SharePoint.

If you're responsible for search in your organization, you can customize how results are presented on classic search results pages. Read about how you can use the search web parts in SharePoint to make it easier for users find what they're looking for in the classic search experience.

Manage the Search Center

A Search Center is a classic site where users can enter search queries and view search results. Learn more.

Specify the default Search Center URL

Choose where searches should go by specifying the URL of your default Search Center. Learn more.

Specify the Search Center URL for a site or subsite

For each site or subsite, you can specify the URL of the Search Center where you want the search results from the site to be displayed. Learn more.

The Search Box Web Part

The Search Box Web Part shows a text box where users can enter words or phrases to search for information. Learn more.

The Search Results Web Part

The Search Results Web Part shows the search results of a query that was entered in a Search Box Web Part. Change settings for the Search Results Web Part

The Search Navigation Web Part

The Search Navigation Web Part lets users move quickly between search verticals, for example between **People** and **Videos**. Learn more.

The Refinement Web Part

The Refinement Web Part filters search results into categories called refiners. The refiners help users drill into the search results to find what they're looking for. About configuring the Refinement Web Part.

The Content Search Web Part

When visitors browse to a page that contains a Content Search Web Part, the Web Part automatically issues a query. The search results are displayed within the Web Part. Configure a Content Search Web Part in SharePoint.

Use result types and display types to change how search results look

To help users quickly distinguish between different types of results, you can use *result types* and *display templates* to show important information directly in the search results. Users don't have to click on each result to see if they've found what they're looking for. Learn more.

Last updated on 06/25/2026

Manage the Search Center in SharePoint

Article • 10/03/2022

The Search Center is a classic search experience. The Search Center is a site or site collection that has a starting page where users enter search queries and a search results page where users can drill into and refine search results, or run a new query.

SharePoint offers two types of Search Centers: the **Basic** Search Center and the **Enterprise** Search Center. By default, SharePoint is set up with the Basic Search Center.

Both Search Centers search the same content and show the same search results. The main difference is that the Enterprise Search Center comes with the search verticals People, Conversations, and Videos. Search verticals are pages that are tailored for displaying search results that are filtered and formatted for a specific content type or class. Search verticals help users move quickly between such different types and classes of content. Also, as a search administrator you have more options for tailoring the look and feel of the Enterprise Search Center.

If your organization needs an enterprise-wide search experience, evaluate first whether the modern search experience covers your needs. Modern search also comes with verticals, it doesn't require any set up, and the results are personal. Learn about the modern search experience for users .

If modern search doesn't cover you needs, you can switch from the Basic Search Center to an Enterprise Search Center.

Search Center pages

These pages are located in the **Pages** library, and they contain predefined Web Parts that you can customize to improve the end user's search experience.

Expand table

Page	Description
default.aspx	The home page for Search Centers, and the page where users enter their queries.
results.aspx	The default search results page for the Search Centers. If you have an Enterprise Search Center, this is also the search results page for the **Everything** search vertical.

Page	Description
peopleresults.aspx	If you have an Enterprise Search Center, this is the search results page for the **People** search vertical.
conversationresults.aspx	If you have an Enterprise Search Center, this is the search results page for the **Conversations** search vertical.
videoresults.aspx	If you have an Enterprise Search Center, this is the search results page for the **Videos** search vertical.
advanced.aspx	This is the search page where users can apply some restrictions to their search phrases — for example, they can limit the search to an exact phrase.

As a SharePoint Administrator and above, you can also create your own search pages and add them to the Enterprise Search Center as search verticals, see Add a search vertical to the Search Navigation Web Part.

About the Web Parts used on Search Center pages

The Search Center pages contain the following predefined Web Parts: Search Box Web Part, Search Results Web Part, Search Navigation Web Part, and Refinement Web Part.

If you have an Enterprise Search Center, the Web Parts on the search result pages are by default set up the same way. The only difference is that the query in the **Search Results** Web Part is directed to different result sources for each search vertical page. For example, for the **People** search vertical page, the query in the **Search Results** Web Part is limited to the **Local People Results** result source. For the **Videos** search vertical page, the query in the **Search Results** Web Part is limited to the **Local Video Results**.

For information about how to customize the Search Center Web Parts, see the following articles:

- Change settings for the Search Box Web Part
- Change settings for the Search Results Web Part
- Change settings for the Search Navigation Web Part
- Change settings for the Refinement Web Part

Feedback

Was this page helpful? Yes No

Provide product feedback

Search Center settings

Article • 07/22/2024

As a SharePoint Administrator or above in Microsoft 365, you specify where searches should go for your classic site collection or site by specifying the URL of your Search Center. For example, if you've created an Enterprise Search Center which users can use to search everything in your company, you must enter the URL of that site here.

Enter the address of your Search Center

1. Go to **More features** in the SharePoint admin center, and sign in with an account that has admin permissions for your organization.

> **Note**
>
> If you have Office 365 operated by 21Vianet (China), sign in to the Microsoft 365 admin center, then browse to the SharePoint admin center and open the More features page.

2. Under **Search**, select **Open**.
3. On the **search administration** page, select **Search Center Settings**.
4. In the **Search Center URL** box, enter the URL of the Search Center site.

   Example: http://companyportal/searchcenter/pages.

5. Select **OK**.

> **Note**
>
> It may take up to 30 minutes before changes take effect.

Feedback

Was this page helpful? Yes No

Provide product feedback

Specify search settings for a site collection or a site

Article • 10/03/2022

As a SharePoint Administrator and above in Microsoft 365, you can specify how search should behave for a classic site collection or a site. The shared Search Box at the top of most classic pages uses these search settings. Any settings you specify on site collection level applies to all sites within that site collection, unless you specify other settings for the site.

You can specify where searches should go for your classic site collection or site by specifying the URL of your Search Center. For example, if you have created an Enterprise Search Center on your site where users can search everything in your company, you can enter the URL of that site here. If you do not enter a Search Center URL, searches will go to the default Search Center, available at <host_name>/search/.

When you create an Enterprise Search Center site collection SharePoint creates a default search home page and a default search results page. In addition, several pages known as search verticals are also created. Search verticals are customized for searching specific content, such as People, Conversations, and Videos, and they display search results that are filtered and formatted for a specific content type or class.

For more on creating and customizing a search center for your site, see Manage the Search Center in SharePoint.

You can change which search results page queries are sent to. By default, queries are sent to the same search results page as the parent, but you can override this for a site collection or a site.

You can also configure search navigation for a site. With search navigation, users can move quickly between different search vertical pages. Navigation links are shown in the Search Navigation Web Part on search result pages, and can also be shown as a drop-down menu in the search box.

> **Note**
>
> It may take up to 30 minutes before changes take effect.

Specify search settings for a site collection

1. On the site, select **Settings**, and then select **Site settings**. If you don't see **Site settings**, select **Site information**, and then select **View all site settings**.

2. Under **Site Collection Administration**, click **Search Settings**.

3. To specify a Search Center, in the **Search Center URL** box, type the URL of the Search Center site.

4. To change which search result page queries are sent to, in the section **Which search results page should queries be sent to?**, clear **Use the same results page settings as my parent**, and then select one of the following:

   - **Send queries to a custom results page URL**. Enter the URL. Custom URLs can be relative or absolute, and can also include special tokens, such as {SearchCenterURL}.

     Example: /SearchCenter/Pages/results.aspx or http://server/sites/SearchCenter/Pages/results.aspx.

   - **Turn on the drop-down menu inside the search box, and use the first Search Navigation node as the destination results page**. If you choose this option, users can choose search vertical in the search box when they enter a query.

5. Click **OK**.

Specify search settings for a site

By default, a site has the same search settings as the site collection that the site belongs to. You can, however, override these settings by defining specific search settings for the site.

1. On the site, select **Settings**, and then select **Site settings**. If you don't see **Site settings**, select **Site information**, and then select **View all site settings**.

2. Under **Search**, click **Search Settings**.

3. To specify a Search Center, in the **Search Center URL** box, type the URL of the Search Center site.

4. To change which search result page queries are sent to, in the section **Which search results page should queries be sent to?**, clear **Use the same results page settings as my parent**, and then select one of the following:

- **Send queries to a custom results page URL**. Enter the URL. Custom URLs can be relative or absolute, and can also include special tokens, such as {SearchCenterURL}.

  Example: /SearchCenter/Pages/results.aspx or http://server/sites/SearchCenter/Pages/results.aspx.

- **Turn on the drop-down menu inside the search box, and use the first Search Navigation node as the destination results page**. Make sure that the search vertical you want as a default is the first option in the **Configure Search Navigation** section.

5. To configure search navigation, edit settings in the **Configure Search Navigation** section as required. You can, for example:

   - Change the display name or the URL of a search vertical
   - Change the order of the search vertical links
   - Add a search vertical

     See Change settings for the Search Navigation Web Part for steps.

6. Click **OK**.

Feedback

Was this page helpful? Yes No

Provide product feedback

Change settings for the Search Box Web Part

The Search Box Web Part shows a text box where users can enter words or phrases to search for information. By default, the Search Box Web Part is used on the home page for the Search Center (default.aspx), and all default search results pages (**Everything**, **People**, **Conversations**, and **Videos**).

As a SharePoint Administrator or above in Microsoft 365, you can change settings in the Search Box Web Part. You can:

- Change where the search results should be displayed — for example, show results in a custom Search Results Web Part or a custom search results page.
- Turn off query suggestions.
- Show links to a search preference page and an advanced search page.
- Change the display template that is used for the Web Part.

Change where search results are displayed

1. On the Search Center site home page, click the **Settings** menu, and then click **Edit Page**.
2. In the Web Part, click the **Search Box Web Part Menu** arrow, and then click **Edit Web Part**.
3. In the **Search Box** tool pane, under **Properties for Search Box**, expand **Which search results page should queries be sent to**.

- To use the settings that are defined on the **Search Settings** page, select the **Use this site's Search Settings** check box.
- To override the settings that are defined on the **Search Settings** page, clear the **Use this site's Search Settings** check box.
- To show search results in a Web Part on the page, in the section **Send queries to other Web Parts on this page**, select a Web Part.

> ⓘ Note

If there are no other Web Parts on a page, search results will be sent to the search results page that is specified on the **Search Settings** page.

- To send queries to a different search results page, select **Send queries to a custom results page URL**, and then type the URL of the custom search results page.

> **Note**
>
> You can't send queries to a custom search results page that uses a friendly URL.

4. Click **OK**.

Change settings for query suggestions

As a SharePoint Administrator or above in Microsoft 365, you can turn off or on query suggestions or edit the different settings for query suggestions. Query suggestions are turned on by default.

1. On the Search Center site home page, click the **Settings** menu, and then click **Edit Page**.
2. In the Web Part, click the **Search Box Web Part Menu** arrow, and then click **Edit Web Part**.
3. In the **Search Box** tool pane, under **Properties for Search Box**, expand the **Query Suggestions** section.

- To turn off query suggestions, clear the **Show suggestions** check box.
- To change how many query suggestions to show, type the maximum number in the **Number of query suggestions** box.
- To change how many characters the user must type before query suggestions are shown, edit the number in the **Minimum number of characters** box.
- To change how many milliseconds elapse before query suggestions are shown, edit the number in the **Suggestions delay (in milliseconds)** box.

4. Click **OK**.

Show links or change the display template

1. On the Search Center site home page, click the **Settings** menu, and then click **Edit Page**.

2. In the Web Part, click the **Search Box Web Part Menu** arrow, and then click **Edit Web Part**.

3. In the **Search Box** tool pane, under **Properties for Search Box**, expand the **Settings** section:

- To show a link to a search preference page, select **Show preferences link**.
- To show a link to an advanced search page, select **Show advanced link**, and then in the **Advanced search page URL** box, type the URL of the advanced search page that you want to link to.
- To apply another display template, in the **Search box control Display Template** list, select the display template that you want to apply to the Web Part.
- Select the **Make the search box have focus when the page is loaded** check box so that users can immediately type a query in the search box when the page is loaded without first having to click the search box. This option is selected by default.

4. Click **OK**.

See also

Manage the Search Center in SharePoint

Change settings for the Search Navigation Web Part

Change settings for the Refinement Web Part

Change settings for the Search Results Web Part

Last updated on 06/25/2026

Change settings for the Search Navigation Web Part

The Search Navigation Web Parts shows links that let users move quickly between the different search pages, known as search verticals. Search verticals are predesigned to give users different search experiences depending on what they are looking for. For example, if users click the **People** link, they are taken to the people search vertical, which is a search page specifically set up to display people information.

By default, the Search Navigation Web Part is set up to show links to the search verticals **Everything**, **People**, **Conversations** and **Videos**. The Search Navigation Web Part uses search results from the Search Results Web Part so that when users click a search vertical link, the search results are filtered and displayed according to how the search vertical is set up.

As a SharePoint Administrator or above in Microsoft 365, you can change how the Search Navigation Web Part is set up by specifying a different Web Part to get the results from, change how many links to show, and change the appearance and layout of the Web Part. You make these changes by editing the properties in the Web Part tool pane.

To make other changes, such as changing display names for the links, or change their order, go to the **Search Settings** for the corresponding site. Here, you can also add a link to a new search vertical to be shown in the Web Part.

Change the settings for the Search Navigation Web Part

Here's how you can change the set-up of the Search Navigation Web Part. You can specify a different Web Part to get the results from, change how many links to show, and change the appearance and layout of the Web Part.

1. On the search results page, click the **Settings** menu, and then click **Edit Page**.

2. In the Search Navigation Web Part, click the **Search Navigation Web Part** menu arrow, and then click **Edit Web Part**.

3. In the Web Part tool pane, in the **Control** section:

- To receive search results from another Web Part on the page, in the **Use Current Query from** list, select a Web Part.
- To change the number of search vertical links to display before overflowing, in the **Maximum Links Before Overflow** box, type a number.

4. To change how the Web Part looks, edit the settings in the **Appearance** and **Layout** sections.
5. Click **OK**.

Change the display name or the URL of a search vertical

1. On the site, select **Settings**, and then select **Site settings**. If you don't see **Site settings**, select **Site information**, and then select **View all site settings**.
2. On the **Site Settings** page, in the **Search** section, click **Search Settings**.
3. On the **Search Settings** page, in the **Configure Search Navigation** section, click to select the search vertical that you want to change, and then click **Edit**.
4. In the **Navigation Link** dialog:

- To change the display name of a search vertical, in the **Title** field, type a display name.
- To change the URL of the search vertical, in the **URL** field, type a URL.

> **Note**
>
> You can't use a page that uses a friendly URL for your search vertical.

5. Click **OK**.

Change the order of the search vertical links

1. On the site, select **Settings**, and then select **Site settings**. If you don't see **Site settings**, select **Site information**, and then select **View all site settings**.
2. On the **Site Settings** page, in the **Search** section, click **Search Settings**.
3. On the **Search Settings** page, in the **Configure Search Navigation** section, click to select a search vertical.

4. Click **Move Up** or **Move Down** to change the display order.

5. Click **OK**.

Add a search vertical to the Search Navigation Web Part

As a SharePoint Administrator or above, you can create a new search vertical page and add it to the Search Navigation Web Part. When you create a new page, we recommend that you copy one of the existing search vertical pages — for example, **results.aspx**, and then modify the copy to create a new page.

Here's how you can add a link to the new search vertical page in the Web Part:

1. On the site, select **Settings**, and then select **Site settings**. If you don't see **Site settings**, select **Site information**, and then select **View all site settings**.

2. On the **Site Settings** page, in the **Search** section, click **Search Settings**.

3. On the **Search Settings** page, in the **Configure Search Navigation** section, click **Add Link**.

4. In the **Navigation Link** dialog:

- In the **Title** field, type a display name.

- In the **URL** field, type the URL of the new search vertical.

- Click **OK** to save the new search vertical.

5. To change the display order, use the **Move Up** or **Move Down** buttons.

6. Click **OK**.

See also

Manage the Search Center in SharePoint

Change settings for the Search Box Web Part

Change settings for the Refinement Web Part

Change settings for the Search Results Web Part

Last updated on 06/25/2026

Change settings for the Refinement Web Part

The Refinement Web Part filters search results into categories called refiners. Users can click these refiners to narrow search results to find what they're looking for more easily.

By default, the Refinement Web Part is used on all default search vertical pages in the Enterprise Search Center, which are the search results pages for **Everything**, **People**, **Conversations**, and **Videos**.

As a user who has SharePoint site administrator or above permissions in Microsoft 365, you can change how the Refinement Web Part is set up. You can:

- Filter search results from a different Search Results Web Part.
- Specify which refiners to show.

  > **Note**
  >
  > Any managed properties that you want to use as refiners must be set to refinable and queryable in the search schema. Also, the content source that contains the managed properties must have been crawled before the properties can be used as refiners.

- Change the display template for a refiner.
- Change display names for refiners.
- Add counts to refiners.

Change how the Refinement Web Part behaves and looks

1. On the page that contains the Refinement Web Part, on the **Settings** menu, click **Edit Page**.
2. In the Web Part, click the **Refinement Web Part Menu** arrow, and then click **Edit Web Part**.
3. In the Web Part tool pane, in the **Refinement Target** section, select the Web Part that you want to filter search results from. By default, the Search Results Web Part is selected.

4. In the Web Part tool pane, verify that the **Choose Refiners in this Web Part** is selected.

5. Click **Choose Refiners**.

6. On the **Refinement configuration** page, from the **Available refiners** section, use the buttons to choose which refiners to show in the Web Part, and also in what order to show them. If you have specified an **Alias** for a refinable managed property, this alias is shown in the **Configuration for** section.

7. In the **Configuration for** section, choose how you want each refiner to look.

   > **Note**
   >
   > If you've a single language site, you can change the refiner display name in the **Display name** section. For multilingual sites, change the refiner display language as described under Change the display name for a refiner.

8. Click **OK**.

Change the display name for a refiner in the classic search experience

By default, the name of the managed property will be used as a display name for the refiner. In many cases, the managed property name is hard to understand—for example, **RefinableString00** or **ColorOWSTEXT**. You can fix this by changing the name of the refiner in a JavaScript file.

1. On the page that contains the Refinement Web Part, select **Settings**, and then select **Site settings**. If you don't see **Site settings**, select **Site information**, and then select **View all site settings**.

2. On the **Site Settings** page, in the **Web Designer Galleries** section, click **Master pages and page layouts**.

3. On the **Master Page Gallery** page, click **Display Templates**.

4. On the **Display Templates** page, click **Language Files**.

5. On the **Language Files** page, click the folder for the relevant language.

6. Open the **CustomStrings.js** file.

7. Add one line for each managed property that you want to change the display name for. Use this syntax:

   `"rf_RefinementTitle_ManagedPropertyName": "Sample Refinement Title for ManagedPropertyName"`

   For example, add this line to change the display name for the managed property **RefinableInt00** to **Price**:

   `"rf_RefinementTitle_RefinableInt00": "Price"`

8. Save the file.

Add refiner counts

By default, the Refinement Web Part doesn't show refiner counts — that is, the number of results for each refiner value. For example, if you've enabled the managed property Color as a refiner, the refiner values will be colors, such as Red, Green, and Blue. You can add refiner counts by changing a value in an HTML file so that the refiner values are shown as Red (10), Green (12), and Blue (8).

1. On the page that contains the Refinement Web Part, select **Settings**, and then select **Site settings**. If you don't see **Site settings**, select **Site information**, and then select **View all site settings**.

2. On the **Site Settings** page, in the **Web Designer Galleries** section, click **Master pages and page layouts**.

3. On the **Master Page Gallery** page, click **Display Templates**.

4. On the **Display Templates** page, click **Filters**.

5. Open the **Filter_Default.html** file.

6. Change the value for **ShowCounts** to **true**.

7. Save the file.

See also

Manage the Search Center in SharePoint

Change settings for the Search Box Web Part

Change settings for the Search Navigation Web Part

Change settings for the Search Results Web Part

Last updated on 06/25/2026

Change how search results look by using result types and display templates

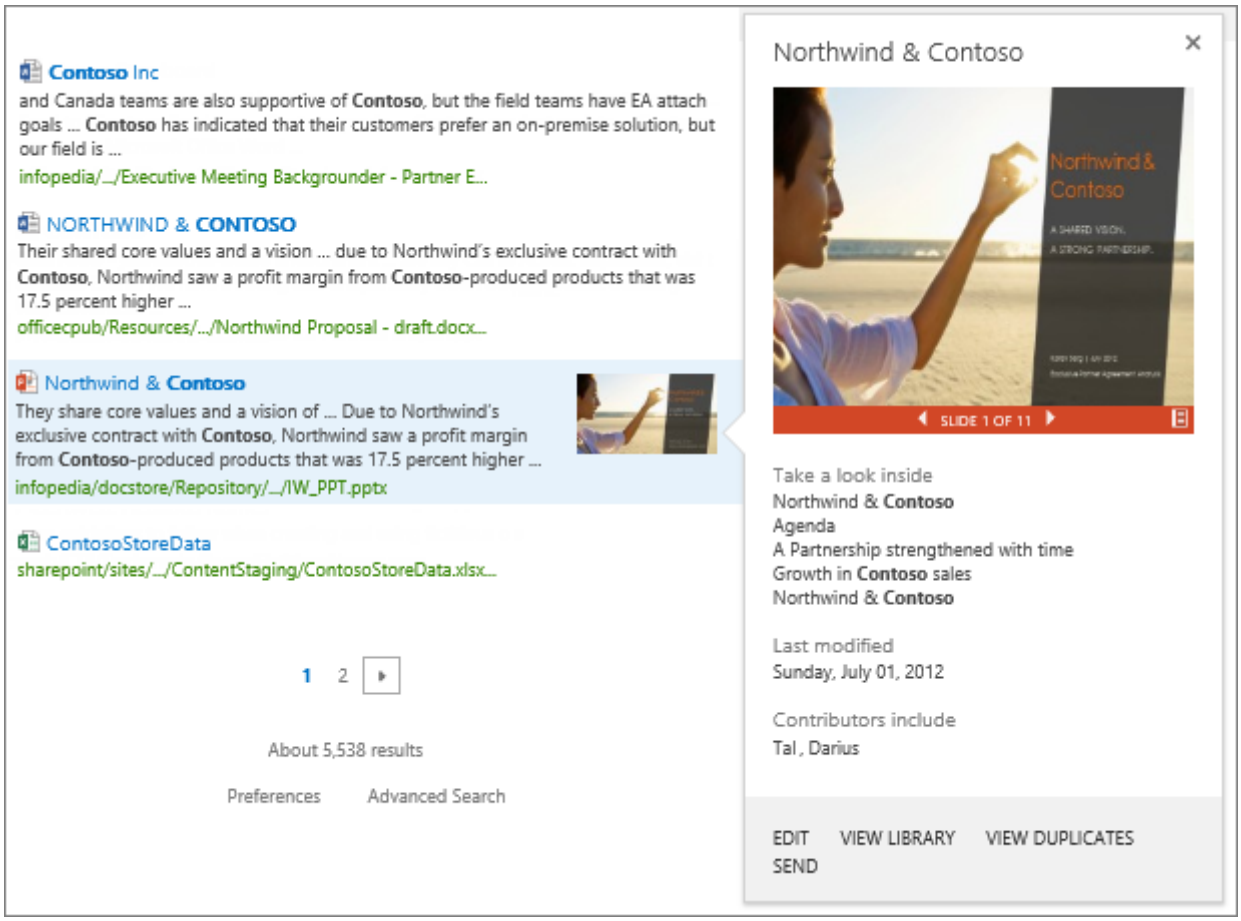
Article • 10/03/2022

To help users quickly distinguish between different types of results when they search for something in the classic search experience, we use *result types* and *display templates*. Important information is shown directly in the search results, so that users don't have to click on each result to see if they've found what they're looking for.

By default, the Search Results Web Part in your Search Center is set up to use different display templates according to the result type of the search result. Result types define when to use which display template, and the *display template* defines what information to show in the search results.

For example, there's a display template for PowerPoint files and another display template for Word documents. A result type says that if the search term is found in a PowerPoint file, then use the PowerPoint display template when showing that result. The users can see right away that this result is a PowerPoint file, and they can also see other information that helps them see whether this result is what they're looking for. When users hover over the result, they'll see a preview of the PowerPoint in the hover panel, together with more details about it. The hover panel also lets users perform *actions,* such as **Edit** or **Send**. The same way, the result type for Word documents uses a Word display template to show information.

Results look different based on result type and display template. This picture shows item display templates for Word, PowerPoint and Excel on the left side, and a hover panel display template for PowerPoint on the right side.



Types of display templates used in the Search Results Web Part

The default Search Center on your site consists of different Web Parts: a Search Box Web Part, a Search Results Web Part, a Search Navigation Web Part, and a Refinement Web Part. The actual search results are shown in the **Search Results Web Part**, All these Web Parts can also be added to any of your site's pages.

For the Search Results Web Part, there are three main types of display templates you should know about, Control display templates, Item result templates, and Hover panel templates.

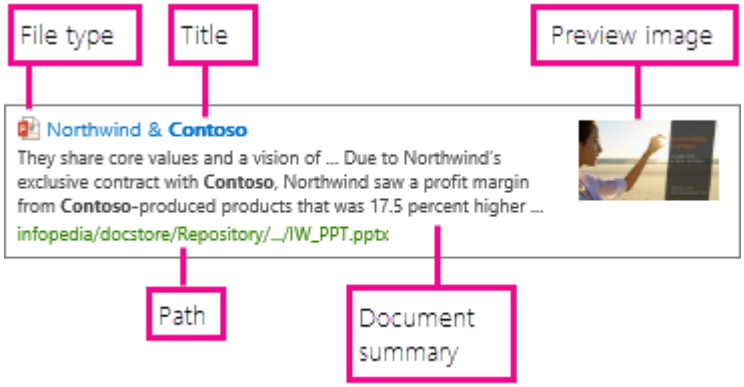
The *Control display template* decides the overall structure of how the results are presented. It contains the things "around" the individual results, such as a heading, numbering, next and previous page buttons, and a "no results found" message.

An *Item display template* defines how each result is displayed. It defines the managed properties you want to show and how they're displayed. You can have different item display templates for different result types.

The *Hover panel display template* typically shows a preview of the item or document when the users hover over the search result. The hover panel display template also contains actions such as **Edit** or **Send**, and other information about the search result.

How display templates show information about search results

The search results contain information that'll help users identify whether the result is what they're looking for. The display templates show this information by surfacing *managed properties* . Managed properties are content and metadata stored in the search index, for example the author and the title of a document. The display templates show a selection of the managed properties in the search results, such as file type, title, document summary, path, and image.



You can create your own display templates that show information that's important to your users, for specific types of results.

- For more information about managed properties, see Manage the search schema in SharePoint.
- For information about the Search Center and how to set it up, see Manage the Search Center in SharePoint.
- For a full list of available display templates, see **Display templates for the Search Results Web Part** in Display template reference in SharePoint Server 2013.

Feedback

Was this page helpful? Yes No

Provide product feedback

About display templates in the Content Search Web Part and other search-driven Web Parts

The Content Search Web Part and the other search-driven Web Parts use display templates to control how the search results appear in the Web Part. By using display templates, you can control the ways in which search results appear and behave in search-driven Web Parts.

Display templates are HTML files that specify which managed properties from the search result to display, and also how these properties should be displayed. For example, a display template could specify that the managed property PublishingImage displays a 100x100 pixel picture, and the managed property Title appears in bold to the left of the image. You can use any of the pre-configured display templates, or create your own.

The different search-driven Web Parts have different default display template settings that are optimized for the intended use of that Web Part. For example, by default, the Content Search Web Part displays a list of items where each item has a picture on the left side and three lines of text on the right.

To change display template settings

1. In the **Control** list, select a display template to control the organization and layout of your search results and the overall look of the Web Part.

2. In the **Item** list, select a display template for the individual items that are displayed in the search results within the Web Part.

3. Select the **Don't show anything when there are no results** check box if you don't want to display the Web Part at all if there are no search results returned by the query in that Web Part.

   If you clear the check box, the Web Part is displayed even if there are no search results, and the Web Part will show the "No results" message in the selected Control display template.

To change which managed properties are displayed in the fields in the Item Display Template

By default, display templates have a set of property mappings in them that were defined when the display template was created. However, you can override these settings in a particular Content Search Web Part.

1. Under **Property Mappings**, select the check box **Change the mapping of managed properties for the fields in the Item Display Template**.

2. In the different lists below the check box, enter the managed property to use for that field in the Item Display Template.

   If you enter multiple managed property names in a list, separate the managed properties by using semicolon. When displaying content, SharePoint will use the first property that isn't empty.

For more information, see:

- About search criteria for the Content Search Web Part and other search-driven Web Parts

---

Last updated on 06/24/2026

Make pages load faster with caching in the Content Search Web Part

Configure a Content Search Web Part in SharePoint (CSWP) offers much flexibility for configuring the query it contains. However, if you configure the Web Part to use a complex query, or if you have many CSWPs on a page, the page can take longer time to load. To make the page load faster, you can configure the CSWP to cache search results for users who belong to the same AD security groups. Because it's faster to look up search results in the cache than in the search index, the page loads faster.

When you have configured a CSWP to use caching, it will first look in the cache for existing search results that match the query and the AD security group. If it doesn't find any search results in the cache, it looks in the search index.

We recommend that you use caching only in CSWPs that are on pages that have more than 10 page loads per 15 minutes, for example of popular home pages or on category pages that are starting points for navigating to more detailed catalog pages.

> **Tip**
>
> See **Configure a Content Search Web Part in SharePoint** for other things you can do to make pages load faster.

Configure a Content Search Web Part (CSWP) to use caching

1. Make sure that you're a member of the Designers SharePoint group on the site that contains the CSWP.
2. Go to the page that contains the CSWP.
3. From **Settings**, select **Edit Page**.
4. Select the CSWP that you want to configure.
5. In the Web Part tool pane, in the **Properties** section, in the **Search Criteria** section, select **Change query**.

6. Go to the **SETTINGS** tab.

7. In the **Caching** section, select **Group: Everyone except external users**, or select **Group:** and then enter the name of the AD security group you want to use.

> **Note**
>
> To test that the CSWP returns the expected results, you have to be member of the AD security group that you select.

> **Tip**
>
> You can't look up the name of your AD security groups from the CSWP. To look up your AD security groups, go to your Azure classic portal. For more information, see Managing groups in Microsoft Entra ID

When should I use caching?

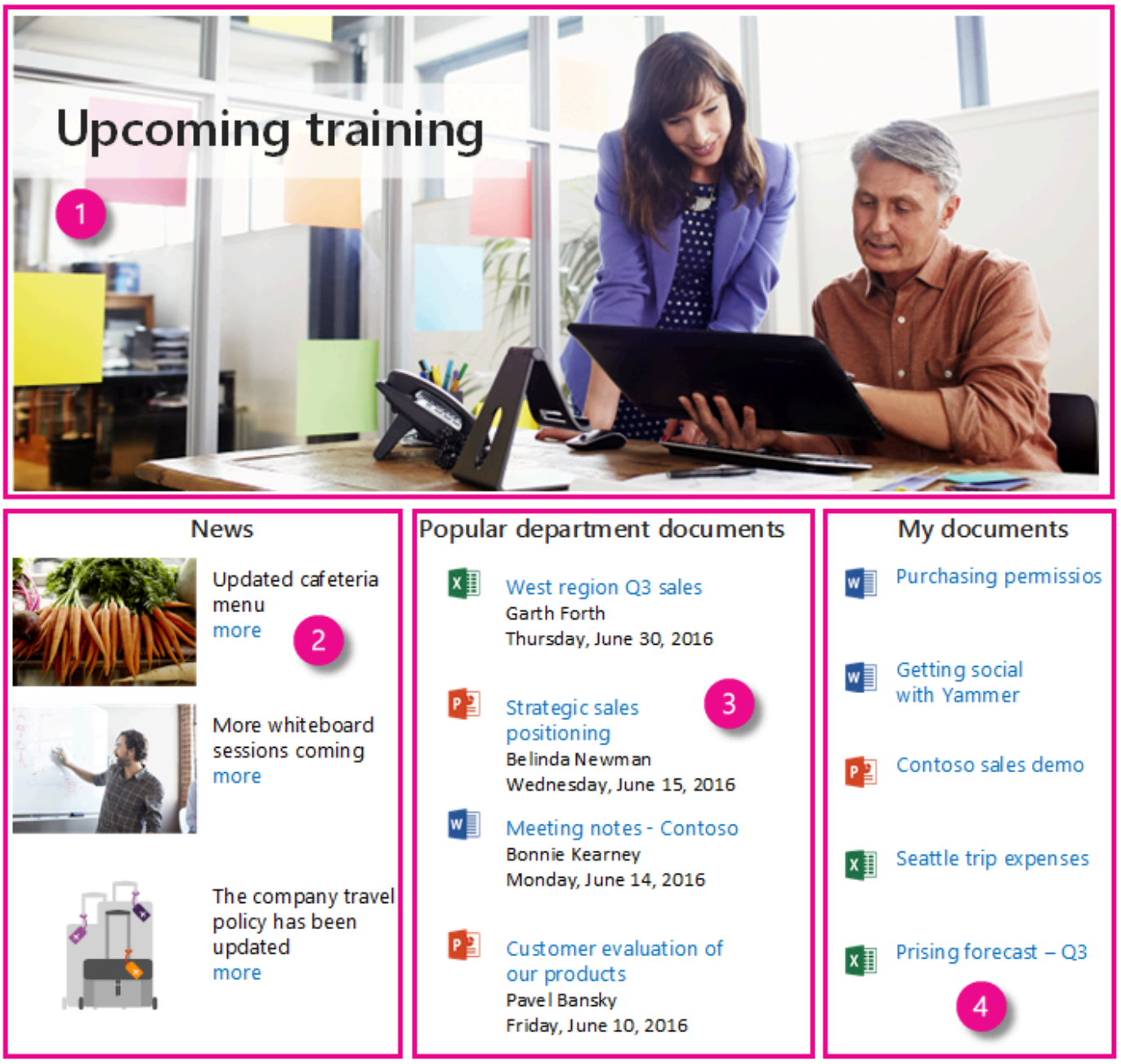
Before you change all your Content Search Web Parts (CSWP) to use caching, you should consider the characteristics of the page where the CSWPs are used:

- **What type of page is the CSWP on?** Caching works great in CSWPs that are on home pages or pages that many users have as a starting point when they browse for information. CSWPs on category pages that are starting points for navigating to more detailed catalog pages, can also benefit from caching.

- **How many page loads does the page have?** We recommend that you use caching only in CSWPs that are on pages with more than 10 page loads per 15 minutes.

- **Is the CSWP configured to show different results to different users?** If the CSWP query involves too many user groups, the search result combinations can overload the cache, and the page load time won't be reduced, or may even increase.

The example below shows an intranet page with four CSWPs. On average, the page has 38 page loads per 15 minutes. These page characteristics suggest that the page can load faster if you configure some of the CSWPs to use caching.



Let's look at the individual CSWPs:

- CSWP 1 shows a featured company news story, in this case a news story about upcoming training.
- CSWP 2 shows other company news stories.
- CSWP 3 shows popular documents in your department.
- CSWP 4 shows the documents you have been working on recently.

The queries in **CSWP 1 and 2** are configured to **show the same results to all users**. That means you can probably make the page load faster by configuring these two CSWPs to use caching.

The queries in **CSWP 3 and 4** are configured to **show different results to different users**.

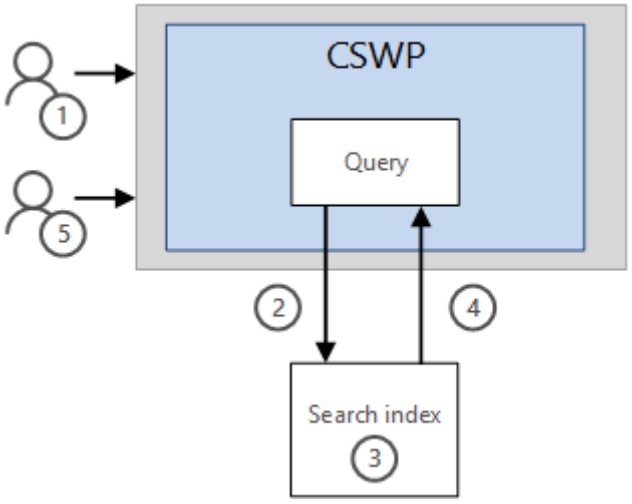
CSWP 3 shows one set of results to people who work in the HR department, and another set of results to people who work in the Sales department. In most cases, you can make the page load faster by using caching in this Web Part. However, if you have many small departments with only a few employees in each department, the number of search results that will be stored in the cache could overload the cache and actually increase the page load time.

CSWP 4 shows which documents the logged-in user has worked on recently. You shouldn't use caching in this Web Part. Because the query is tailored to each user, all individual search results are stored in the cache. This overloads the cache and might increase the page load time.

How does caching make web pages load faster?

First, let's look at how search results are displayed in a Content Search Web Part (CSWP) **without** caching:

1. A user goes to a page that has a CSWP.
2. The query in the CSWP is sent to the search index.
3. Search finds results in the search index, and removes any search results that the users in the assigned AD security group aren't allowed to see.
4. The search results are sent from the search index to the CSWP, where the user sees the results.
5. A second user goes to the same page, and steps 2 - 4 are repeated.



Now let's look at how results are displayed in a Content Search Web Part (CSWP) **with** caching:

1. A user goes to a page that has a CSWP.

2. An AD security group, for example **Everyone except external users**, is assigned in the CSWP. This example assumes that the user who visits the page belongs to the assigned AD security group.

3. The query and the assigned AD security group in the CSWP is combined, and search first looks for a matching query and security group in the cache. If it doesn't find any matching results in the cache, the query is sent to the search index.

4. Search finds results in the search index, and removes any results that the users in the assigned AD security group aren't allowed to see.

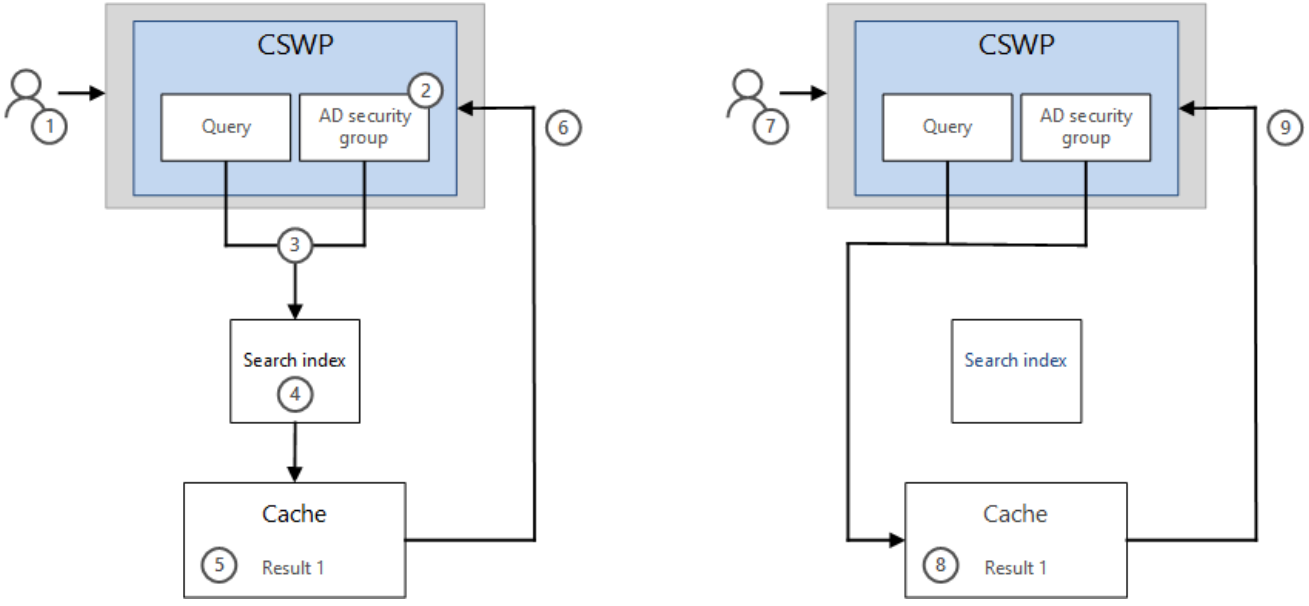
5. The search result is sent from the search index to the cache where it's stored (Result 1).

6. The search result is served from the cache to the CSWP, where the user sees the result.

7. A second user goes to the same page. The second user belongs to the same AD security group as the first user.

8. Search finds existing search results for the combination of the query and the AD security group in the cache.

9. The search result is served from the cache to the CSWP where the users see the result.



Because it's quicker to look up search results in the cache than in the search index, the page loads faster.

> **Important**

The cache expires after 15 minutes. It's repopulated by the first user that goes to the page after the cache has expired, so page load time might be longer for the first user that repopulates the cache after an expiration.

Troubleshooting: newly added content doesn't show up in CSWP results

The Content Search Web Part (CSWP) shows search results from content that has been crawled and added to the search index. When you configure the CSWP to use caching, it shows matching results from the cache, and not from the search index. Search results, **also empty search results**, are stored in the cache for a maximum of 15 minutes before the cache expires.

If you search for newly added content before the content has been crawled and included in the search index, the cache contains an **empty search result** for the query until the cache expires, and the content won't show up in the CSWP results.

If newly added content doesn't show up in the CSWP:

1. Make sure that the content has been crawled and added to the search index. Search for the content in a search box, or in a CSWP that doesn't use caching, until you can find the content.

2. Wait for at least 15 minutes to let the CSWP cache expire, and try again.

3. If you still don't see any results, check that you're a member of the AD security group that has been assigned to the CSWP. If you're not a member of the AD security group, you won't see any search results.

> **Note**
>
> SharePoint automatically crawls and adds new content to the search index at scheduled intervals, but you can also manually request crawling and re-indexing of a site, a library or a list.

Last updated on 06/25/2026

Switch from an Enterprise Search Center to Basic in SharePoint

Article • 10/08/2024

The Basic Search Center is a classic search experience. To offer your users a richer search experience, you can do one of the two things:

- Switch from a Basic Search Center to an Enterprise Search Center
- Rely on the modern search experience that SharePoint comes with. Learn about differences between classic and modern search and when to choose which search experience for your organization.

If you're currently using the Enterprise Search Center, you can easily replace (swap) it with the Basic Search Center if needed. The swap results in your users seeing the classic search experience in their default search home page and default search results page. You can use the Invoke-SPOSiteSwap PowerShell cmdlet to swap.

How to use Invoke-SPOSiteSwap to swap your Search Center sites

1. Download the latest SharePoint Online Management Shell.

   > **Note**
   >
   > If you installed a previous version of the SharePoint Online Management Shell, go to Add or remove programs and uninstall "SharePoint Online Management Shell."

2. Connect to SharePoint as a SharePoint Administrator or above in Microsoft 365. To learn how, see Getting started with SharePoint Online Management Shell.

3. Run the Invoke-SPOSiteSwap cmdlet.

   PowerShell

   ```
   Invoke-SPOSiteSwap
     -SourceUrl <string>
     -TargetUrl <string>
     -ArchiveUrl <string>
   ```

Expand table

Parameter	Description
-SourceUrl	The site you want to promote.
-TargetUrl	The site you want to replace.
-ArchiveUrl	URL that the target site is archived to.

Here's an example of how to use these parameters when swapping an existing Enterprise Search Center to Basic:

- **For your -SourceUrl**, you need the URL of your Basic Search Center site. The site must exist before running the cmdlet. For our example, we use <spam> <spam>https://contoso.sharepoint.com/sites/SiteSearch<spam><spam>.

You can create a Basic Search Center site from an Enterprise site template.

- **For your -TargetUrl**, you need the URL of your Enterprise Search Center site that you want to replace. For our example, we use <spam> <spam>https://contoso.sharepoint.com/search<spam><spam>.

- **For your -ArchiveUrl**, use a Url that doesn't currently exist at the location. Your Enterprise Search Center site is archived to this site location. For our example, we use <spam> <spam>https://contoso.sharepoint.com/sites/ArchivedEntSearch<spam><spam>.

Here's how to use the examples in the Invoke-SPOSiteSwap cmdlet:

PowerShell

```
Invoke-SPOSiteSwap -SourceUrl
https://contoso.sharepoint.com/sites/SearchSite -TargetUrl
https://contoso.sharepoint.com/search -ArchiveUrl
https://contoso.sharepoint.com/sites/ArchivedEntSearch
```

Successfully running the cmdlet would result in:

- Basic Search is the default Search Center experience. When users go to <spam> <spam>https://contoso.sharepoint.com/search<spam><spam>, they're now using the Basic Search Center.
- The Enterprise Search Center site is no longer available as the default Search Center experience.

See also

Manage the Search Center in SharePoint

Feedback

Was this page helpful? Yes No

Provide product feedback

Show the right search results

Article • 02/21/2023

All search results are not relevant to everyone all the time. Learn how you can help users find exactly the results they're looking for in SharePoint. SharePoint has both a classic and a modern search experience, learn about the differences between the classic and modern search experiences in SharePoint.

Manage the search schema

The search schema controls what users can search for, how they can search it, and how the results get presented on your search websites. In the search schema, you can view, create, or change managed properties, and map crawled properties to managed properties. Learn about the search schema.

Manage query rules

Query rules apply to the classic search experience. They consist of conditions and associated actions. When a query meets the conditions in a query rule, the search system performs the actions specified in the rule. Query rules can be used to promote results to the top of the result list.Learn about managing query rules.

Manage query suggestions

Query suggestions are words that appear below the search box as a user types a query. SharePoint automatically creates a query suggestion when you've clicked a search result for a query at least six times. In the classic search experience you can also import your own lists of query suggestions to SharePoint. Learn about managing query suggestions.

Using query transforms

Query transforms apply to the classic search experience. You can configure a query transform to replace properties of a query, such as the result source that the query will use to get search results, or the sort order that it will use when it displays search results. Read Understanding query transforms to learn more.

Manage result sources

Result sources limit searches to certain content, or to a subset of search results. You can also use result sources to send queries to external providers such as Bing. Learn about managing result sources

Manage result types

Results types apply to the classic search experience. A result type specifies one or more conditions to compare search results against, and an action to take if a search result meets those conditions. The action specifies the display template to use for the search result. Learn about managing result types.

Manage search dictionaries

Search dictionaries apply to the classic search experience. You can use search dictionaries to include or exclude words for query spelling correction, and you can include or exclude company names to be extracted from the content of indexed documents. Learn about managing search dictionaries.

Manage authoritative pages

You can influence the pages or documents that should appear at the top of your list of search results by identifying authoritative pages - high-quality pages that link to the most relevant information. Authoritative pages apply to the classic search experience. Learn about managing authoritative pages.

Export and import search settings

You can export and import customized search configuration settings between tenants, site collections, and sites. The settings include all customized query rules, result sources, result types, ranking models and site search settings. Learn about exporting and importing search settings.

Feedback

Was this page helpful? Yes No

Provide product feedback

Manage the search schema in SharePoint

Article • 05/29/2025

The search schema controls what users can search for, how users can search it, and how you can present the results on your search websites. By changing the search schema, you can customize the search experience in SharePoint in Microsoft 365.

See Overview of crawled and managed properties in SharePoint Online for a list of crawled and managed properties specific to SharePoint Online.

See Overview of crawled and managed properties in SharePoint Server for a list of existing crawled and managed properties in SharePoint.

About the search schema

When a user searches for content on SharePoint sites, search only finds what's in the **search index**, and only shows results that the user has permission to see.

Search discovers information by crawling items on your site. The discovered content and metadata are called **properties** of the item. The **search schema** has a list of **crawled properties** that helps the crawler decide what content and metadata to extract.

Not all crawled content or metadata is useful to have in the search index, so the search schema has a list of useful types of content and metadata, called **managed properties**. The index only includes content and metadata from the managed properties. Examples of useful metadata for the index are the author and the title of a document.

Search comes with relevant crawled properties mapped to managed properties. For example, crawled properties related to author map to a managed property related to author. If you add a managed property, you must map it to a crawled property to get content into the index. After the site, library, or list is crawled, users can search for the content and metadata of new, or changed managed properties. See Introducing Search Schema for SharePoint for more info.

> **Note**
>
> Numeric data in Microsoft Excel files isn't indexed. For example, the number "123456789" isn't indexed, but the string "PO123456789" is indexed.

Managed properties and search

Each managed property has settings that determine how users can search for the content of that managed property, and how the content can be shown in the search results.

You can create new, **custom** managed properties, but this type of properties can only contain text or Yes/No. If you need other content types in your custom managed property, then use one of the unused, **built-in** managed properties that search comes with. These managed properties can contain information in integer, decimal, date and time, double precision float, or binary format. You can "rename" these unused managed properties by using the alias setting.

For the built-in managed properties, you can change their mappings to crawled properties, but the only setting you can change is the alias.

> ⓘ **Important**
>
> If an alias is added to a managed property, ensure a managed property with the same name as the alias does not already exist. Aliased managed properties take precedence during search and Microsoft 365 experiences relying on specific properties and values may break as a result.
>
> It is not advisable to change the mapping or mapping order of crawled properties for existing managed properties outside of the default unused managed properties provided for reuse, or for managed properties manually created. Changing crawled property mappings may break Microsoft 365 experiences relying on specific properties and values.

Define which content that users can search and get results for

If you set a managed property to be **searchable**, the content is added to the index. This means that a simple query for "Smith" returns items that contain the word "Smith" and also items whose "author" property contains "Smith". If you want users to be able to "only search for items that have this specific author", set the author property to be **queryable**. Then, to find only items that have an author named Smith, users can query for "author:Smith".

If you want to prevent the content in a managed property from showing up as search results, you can disable the **retrievable** setting for the managed property.

If you don't want anonymous users to see the information in a managed property, for example who authored an item, disable the "Safe for Anonymous" setting for the managed property.

Get better search results when you have multi-lingual content and metadata with special characters

When search indexes content or when it processes queries, it breaks a stream of text into smaller parts such as words, phrases, symbols, or other meaningful elements. These parts are called tokens. When users enter a query, search tries to find tokens in the index that match the tokens of the query.

For most languages, search changes text to lower-case, removes diacritics, replaces special characters, such as punctuation, with white space, and then breaks on white spaces.

Breaking on white spaces works fine for a language like English, but not so well for East Asian languages. Let's say you have a document library that contains product datasheets both in English and Chinese. Each datasheet has a product identifier with non-alphanumerical characters, such as "11.132-84-115#4". When search processes the datasheet, it **detects** its language, and tokenizes everything in it according to that language. So, the product identifier in a Chinese data sheet is tokenized as if it was Chinese text. In an English data sheet, the product identifier is tokenized as if it was English text. When users search for a product identifier, search tokenizes their query according to the language setting of the SharePoint site they're on. If the site is set to English, and the user searches for a product identifier that was tokenized as Chinese text, the tokens might not match, and the users get no results.

Here's how you can make results better for users: When search crawls the datasheet, it extracts the product identifier. Map the crawled property for the product identifier to a new managed property, "ProductID". Enable **language neutral tokenization** for the "ProductID" managed property, and instruct users to search for product identifiers against the "ProductID" managed property, like this: *ProductID:"11.132-8*" . Because you enabled language neutral tokenization for "ProductID", search uses language neutral tokenization for the query and can find matching results for the query.

Get better search results when you have metadata with special characters

To help users get better search results when they search in managed properties that contain metadata with non-alphanumeric characters, you can enable the **finer tokenization** setting for the managed property.

Let's look at the example with a product datasheet library again.

Users who prefer to quickly enter a query and then browse the results to find the datasheet they're looking for, typically enter queries like ProductID:"132-884". Because search breaks content for the **search index** into smaller parts than it does for **queries**, search might not find matches for these queries. When the query is tokenized finer, it's more likely that there are matches between the tokens in the search index and in the query. Users can also query for the middle or last part of the product identifier.

Users who search for a datasheet and expect to only get results that match the full product identifier, typically write queries like *ProductID:"11.132-884-115#4*" . Finer query tokenization doesn't make a difference for such queries.

Determine which title to show in results

A single crawled property can be mapped to multiple managed properties. Or, multiple crawled properties can be mapped to a single managed property, for example both the "Writer" and "Author" crawled properties can be mapped to the "Author" managed property.

For example, a document in a library can have a SharePoint title, a title in the file metadata, and the content can have a title formatted with the style "Title". All these are mapped to the "Title" managed property. It's the title from the crawled property that's highest on the mapping list and that has a value that's included in the index.

Auto-generated managed properties

Some managed properties are generated automatically. One example is when you add a site column to a SharePoint library or list. When search crawls that list it automatically generates a crawled and a managed property for the site column, and a mapping between them. Another example is when crawling finds metadata in a document you've uploaded to SharePoint. If there isn't already a mapping to a managed property for that metadata, such as 'Title', search auto-generates a managed property. The type of crawled property determines the settings of the auto-generated managed property.

The search schema displays the name of auto-generated managed properties and their mappings to crawled properties in grey in the search schema. The search schema doesn't hold the settings of the managed auto-generated managed properties. The settings exist, but they're hidden from the search schema. You can add mappings to other managed properties for the crawled properties, but if you change any other setting, you override the other (hidden) settings and the auto-generated managed property is converted to a regular managed property. If you decide to **change** an auto-generated managed property, review **all** the settings carefully, just as you would when you create a new property manually.

> ⓘ **Important**
>
> Auto-generated managed properties are case-sensitive. When accessing auto-generated managed properties, such as through a REST query, verify that the casing is correct. If the casing is incorrect, no value will be returned.
>
> When the implicit mapping between an auto-generated crawled property and its corresponding auto-generated managed property is modified, the implicit mapping is disrupted. For example, when the auto-generated crawled property is mapped to another explicit managed property or the auto-generated managed property is mapped to another explicit crawled property, the implicit mapping is disrupted. Following a reindex, both the auto-generated crawled property and auto-generated managed property are removed.

Refine on managed properties

If you want to use a managed property as a refiner on the search results page, use the setting **refinable**. This setting is only available on the built-in managed properties, and only affects the classic search experience. If you need to use a new managed property, or an auto-generated managed property, as a refiner, rename an existing, unused managed property (that's refinable) by

using an alias. There are quite a few managed properties available for this purpose. They have names such as "RefinableString00" and "RefinableDate19."

For example, you create a new site column called "NewColors", and you want users to be able to use "NewColors" as an option when they refine on the search results. In the search schema, you choose an unused managed property, for example "RefinableString00", and rename the property to "NewColors" by using the Alias setting. Then, you map this new managed property to the relevant crawled property.

Change the search schema on tenant level or on site collection level

Usually, you don't have to change the default search schema for the tenant unless you want to create a more advanced or customized search experience.

You can change the search schema for the whole tenant or for a specific site collection only. The search schema for the site collection is based on the search schema for the tenant, so typically, you would make changes on the tenant level first, and then on the site collection level. Any changes you make on a site collection, only apply to that site collection.

Crawling and re-indexing

When you change managed properties or add new ones, the changes take effect only after the content is re-crawled. In SharePoint in Microsoft 365, crawling happens automatically based on the defined crawl schedule.

When you have added a new property to a list or to a library, or when you have changed properties that are used in a list or library, search has to re-crawl the content before your changes are reflected in the search index. Because your changes are made in the search schema, and not to the actual site, the search doesn't automatically re-crawl the list or the library. To make sure that your changes are crawled, you can specifically request a re-indexing of the list or library. When you do this, the list or library content is re-crawled so that you can start using your new managed properties in queries, query rules and display templates. When working with built-in managed properties (like refinablestring##), we recommend updating/mapping properties at the tenant-level. This approach is easier to manage, creates a more consistent user experience, and performs better in the long run.

Create a new managed property

> **Note**

Not all options are available in SharePoint in Microsoft 365. Refinable Managed Properties cannot be created. Instead use the existing Refinable Managed Properties, for example, RefinableString00 or RefinableInt00. Searching "Refinable" shows all of the usable Refinable Managed Properties available.

In SharePoint in Microsoft 365, when you create a new managed property, it has some limitations. For example, the property can only be of type **Text** or **Yes/No**, and it can't be refinable or sortable.

> **Important**
>
> Consider using only letters and digits in managed property names. Although it is possible to create custom managed properties with special characters (such as hyphens, dots, and underscores), many of those characters act as operator characters in the query syntax. For example, a hyphen means negation. Such property names have to be enclosed in double quotation marks when used in queries. Many tools and applications that create queries don't handle this correctly, and therefore it is better to use only letters and digits in managed property names.

If you need a property of a different type, or one that has different characteristics than what is available, follow the steps under Create a managed property by renaming an existing one.

Go to the Search Schema page for the tenant

1. Go to **More features** in the SharePoint admin center, and sign in with an account that has admin permissions for your organization.

   > **Note**
   >
   > If you have Office 365 operated by 21Vianet (China), sign in to the Microsoft 365 admin center, then browse to the SharePoint admin center and open the More features page.

2. Under **Search**, select **Open**.

3. On the search administration page, select **Manage Search Schema**.

Go to the Search Schema page for a site collection

1. On the site, select **Settings**, and then select **Site settings**. If you don't see **Site settings**, select **Site information**, and then select **View all site settings**.

2. Under **Site Collection Administration**, select **Search Schema**.

3. Select **Managed Properties**.

4. On the **Managed Properties** page, select **New Managed Property**.

5. In the **Name and description** section, in the **Property name** box, enter the name of the new managed property. Optionally, enter a description.

6. In the **Type** section, select one of the available options for the property:

   - Yes/No.
   - Text.

7. In the **Main characteristics** section, select one or several of the available options.

8. In the **Mappings to crawled properties** section, select **Add a mapping**.

9. In the **crawled property selection** dialog, select a crawled property to map to the managed property, and then select **OK**. If you want to map more crawled properties to the same managed property, repeat this step.

10. In the **Mappings to crawled properties** section, specify if you want to include:

- All content from all crawled properties mapped to this managed property.

- Content from the first crawled property that contains a value and, optionally, in which order.

11. Select **OK**.

Create a managed property by renaming an existing one

Go to the Search Schema page for the tenant

1. Go to **More features** in the SharePoint admin center, and sign in with an account that has admin permissions for your organization.

   > **Note**
   >
   > If you have Office 365 operated by 21Vianet (China), sign in to the Microsoft 365 admin center, then browse to the SharePoint admin center and open the More features page.

2. Under **Search**, select **Open**.

3. On the search administration page, select **Manage Search Schema**.

Go to the Search Schema page for a site collection

1. On the site, select **Settings**, and then select **Site settings**. If you don't see **Site settings**, select **Site information**, and then select **View all site settings**.

2. Under **Site Collection Administration**, select **Search Schema**.

3. On the **Managed Properties** page, find an unused managed property. By unused, we mean that the property is not mapped to a crawled property: the **Mapped Crawled Properties** column is empty. See the Default unused managed properties table for more details.

   > **Important**
   >
   > To be able to use the property as a refiner later, choose a managed property that is marked with **Refine**.

4. Point to the managed property, select the arrow, and then select **Edit/Map property**.

5. On the **Edit Managed Property** page, under **Main characteristics**, in the **Alias** section, in the **Alias** box, enter the new name for the property.

6. In the **Mappings to crawled properties** section, select **Add a mapping**.

7. On the **Crawled property selection** page, select a crawled property to map to the managed property, and then select **OK**. Repeat this step to map more crawled properties to this managed property.

8. Select **OK**.

   > **Important**
   >
   > When you create a new managed property this way, the library or list that uses the refiner must be re-crawled and re-indexed before the property appears as an option in the refinement configuration. See Request re-indexing of a document library or list.

View crawled properties and managed properties

Go to the Search Schema page for the tenant

1. Go to **More features** in the SharePoint admin center, and sign in with an account that has admin permissions for your organization.

   > **Note**

> If you have Office 365 operated by 21Vianet (China), sign in to the Microsoft 365 admin center, then browse to the SharePoint admin center and open the More features page.

2. Under **Search**, select **Open**.

3. On the search administration page, select **Manage Search Schema**.

Go to the Search Schema page for a site collection

1. On the site, select **Settings**, and then select **Site settings**. If you don't see **Site settings**, select **Site information**, and then select **View all site settings**.

2. Under **Site Collection Administration**, select **Search Schema**.

3. On the **Managed Properties** tab, you see all the managed properties, the settings on the managed properties, and the crawled properties they are mapped to.

4. To view crawled properties and the managed properties they are mapped to, select **Crawled Properties**.

5. To view crawled property categories, select **Categories**.

Edit a managed property

> **Note**
>
> Not all options are available in SharePoint.

Go to the Search Schema page for the tenant

1. Go to **More features** in the SharePoint admin center, and sign in with an account that has admin permissions for your organization.

   > **Note**
   >
   > If you have Office 365 operated by 21Vianet (China), sign in to the Microsoft 365 admin center, then browse to the SharePoint admin center and open the More features page.

2. Under **Search**, select **Open**.

3. On the search administration page, select **Manage Search Schema**.

Go to the Search Schema page for a site collection

1. On the site, select **Settings**, and then select **Site settings**. If you don't see **Site settings**, select **Site information**, and then select **View all site settings**.
2. Under **Site Collection Administration**, select **Search Schema**.
3. On the **Managed Properties** tab, in the **Property Name** column, find the managed property that you want to edit, or in the **Filter** box, enter the name.
4. Point to the managed property in the list, select the arrow, and then select **Edit/Map property**.
5. On the **Edit Managed Property** page, edit the settings, and then select **OK**.

Delete a managed property

Go to the Search Schema page for the tenant

1. Go to **More features** in the SharePoint admin center, and sign in with an account that has admin permissions for your organization.

   > **Note**
   >
   > If you have Office 365 operated by 21Vianet (China), sign in to the Microsoft 365 admin center, then browse to the SharePoint admin center and open the More features page.

2. Under **Search**, select **Open**.
3. On the search administration page, select **Manage Search Schema**.

Go to the Search Schema page for a site collection

1. On the site, select **Settings**, and then select **Site settings**. If you don't see **Site settings**, select **Site information**, and then select **View all site settings**.
2. Under **Site Collection Administration**, select **Search Schema**.
3. On the **Managed Properties** tab, find the managed property that you want to delete, or in the **Filter** box, enter its name.
4. Point to the managed property that you want to delete, select the arrow, and then select **Delete**.
5. Select **OK**.

> **Important**
>
> If you delete a managed property: > Users can't search on the property. > A query rule that uses the property no longer works. > A custom web part that uses the property no longer works.

Map a crawled property to a managed property

Go to the Search Schema page for the tenant

1. Go to **More features** in the SharePoint admin center, and sign in with an account that has admin permissions for your organization.

   > **Note**
   >
   > If you have Office 365 operated by 21Vianet (China), sign in to the Microsoft 365 admin center, then browse to the SharePoint admin center and open the More features page.

2. Under **Search**, select **Open**.

3. On the search administration page, select **Manage Search Schema**.

Go to the Search Schema page for a site collection

1. On the site, select **Settings**, and then select **Site settings**. If you don't see **Site settings**, select **Site information**, and then select **View all site settings**.

2. Under **Site Collection Administration**, select **Search Schema**.

3. Choose **Crawled Properties**.

4. On the **Crawled Properties** page, find the crawled property that you want to map to a managed property, or under **Filters**, enter its name in the **Crawled properties** box.

5. Point to the crawled property that you want to map, select the arrow, and then select **Edit/Map property**.

6. On the **Edit Crawled Property** page, in the **Mappings to managed properties** section, select **Add a Mapping**.

7. In the **managed property selection** dialog, select a managed property to map to the crawled property, and then select **OK**. Repeat this step to map more managed properties to this crawled property.

8. In the **Include in full-text index** section, if you want to include the content of this crawled property in the full-text index, select the box.

9. Select **OK**.

> **Note**
>
> To help clarify the the scope of Managed and Crawled Property mappings, Crawled Properties list **Scope** and **Override** values whose values are the scope at which the property was discovered or created and if the property overrides a property at a higher scope. If crawled properties with same name and property set Id exist in different scopes, the lower scope's value (for example, Site Collection) overrides the higher scope (e.g., System). The scope override precedence from low to high is **Site Collection** -> **Tenant** -> **System**. An overridden property is greyed out and can only be modified at the scope at which it was created.

View or edit crawled property categories

Go to the Search Schema page for the tenant

1. Go to **More features** in the SharePoint admin center, and sign in with an account that has admin permissions for your organization.

   > **Note**
   >
   > If you have Office 365 operated by 21Vianet (China), sign in to the Microsoft 365 admin center, then browse to the SharePoint admin center and open the More features page.

2. Under **Search**, select **Open**.

3. On the search administration page, select **Manage Search Schema**.

Go to the Search Schema page for a site collection

1. On the site, select **Settings**, and then select **Site settings**. If you don't see **Site settings**, select **Site information**, and then select **View all site settings**.

2. Under **Site Collection Administration**, select **Search Schema**.

3. Select **Categories**.

4. On the Categories page, find the crawled property category that you want to view or edit.

5. Do one of the following:

- To view which crawled properties belong to a category, and which managed properties they are mapped to, click the crawled property category in the Categories page.
- To edit a category, point to the crawled property category that you want to edit, click the arrow, and then click **Edit category**.

Default unused managed properties

The following table provides an overview of the default unused managed properties that you can reuse and rename using an Alias.

Expand table

Managed property type	Count	Multi	Query	Search	Retrieve	Refine	Sort	Managed property name range	Notes
Date	10	-	Query	-	-	-	-	Date00 to Date09	
Date	20	Multi	Query	-	Retrieve	Refine	Sort	RefinableDate00 to RefinableDate19	
Date	2	-	Query	-	Retrieve	Refine	Sort	RefinableDateInvariant00 to RefinableDateInvariant01	*
Date	5	-	Query	-	Retrieve	Refine	Sort	RefinableDateSingle00 to RefinableDateSingle04	
Decimal	10	-	Query	-	-	-	-	Decimal00 to Decimal09	
Decimal	10	Multi	Query	-	Retrieve	Refine	Sort	RefinableDecimal00 to RefinableDecimal09	
Double	10	-	Query	-	-	-	-	Double00 to Double09	
Double	10	Multi	Query	-	Retrieve	Refine	Sort	RefinableDouble00 to RefinableDouble09	
Integer	50	-	Query	-	-	-	-	Int00 to Int49	
Integer	50	Multi	Query	-	Retrieve	Refine	Sort	RefinableInt00 to RefinableInt49	
String	200	Multi	Query	-	Retrieve	Refine	Sort	RefinableString00 to RefinableString199	
String	40	Multi	Query	-	Retrieve	Refine	Sort	RefinableStringFirst00 to RefinableStringFirst39	*
String	10	Multi	Query	-	Retrieve	Refine	Sort	RefinableStringLn00 to RefinableStringLn09	**

Managed property type	Count	Multi	Query	Search	Retrieve	Refine	Sort	Managed property name range	Notes
String	50	-	Query	-	Retrieve	Refine	Sort	RefinableStringWbOff00 to RefinableStringWbOff49	***
String	50	Multi	Query	-	Retrieve	Refine	Sort	RefinableStringWbOffFirst00 to RefinableStringWbOffFirst49	*, ***

* Mappings to crawled properties - Include content from the first crawled property that is not empty, based on the specified order.

** Language neutral word breaker

*** Complete Matching

Request re-indexing of a document library or list

1. On your site, go to the list or library where you added the new property, and select the title. The **Library** or **List** tabs appear.
2. On the ribbon, select the **Library** tab or the **List** tab.
3. Under the **Settings** section, select **Library settings** or **List settings**.
4. On the **Settings** page, under **General Settings**, select **Advanced settings**.
5. Scroll down to **Reindex Document Library** or **Reindex List**, and select the button. All of the content in the document library or list is re-indexed during the next scheduled crawl.

> ⓘ **Note**
>
> This may cause a massive load on the search system, so be sure to re-index only after you've made all the changes you want to be re-indexed.

Related Topics

Overview of crawled and managed properties in SharePoint Online

Overview of crawled and managed properties in SharePoint Server

Overview of the search schema in SharePoint Server

Manually request crawling and re-indexing of a site

Manage query rules

As a SharePoint Administrator or other administrator in Microsoft 365, you can improve search results in the classic search experience by creating and managing query rules. Query rules help searches respond to the intent of users.

In a query rule, you specify conditions and associated actions. When a query meets the conditions in a query rule, the search system performs the actions specified in the rule to improve the relevance of the search results. This improvement could be by narrowing results or changing the order in which results are displayed. When the query rule condition is met, an associated action could be to show a specific item at the top of the search results. For example, say you have an intranet site where all company events are maintained in a library, and you want to promote a first-aid seminar. To do this, create a query rule that boosts the first-aid seminar to the top of the search results when someone searches for "seminar" or "event."

A query rule can specify the following three types of actions:

- Promote a search result to appear above ranked results. For example, for the query "sick leave", a query rule could specify a particular result, such as a link to a site that has a statement of company policy regarding time off work.
- Add one or more groups of search results, called result blocks. For example, for a query that contains "Fabrikam sales report", a query rule might recognize "Fabrikam" as a customer, and then display a result block with pertinent results about Fabrikam from your customer relationship management (CRM) system.
- Change the ranking of search results. For example, for a query that contains "download toolbox", a query rule could recognize the word "download" as an action term and boost search results that point to a particular download site on your intranet.

You can create query rules at different levels: for the whole tenant, for a site collection, or for a site. When you create query rules at tenant level, all site collections can use the query rules. When you create query rules at site collection level, all sites in the site collection can use the rules. When you create query rules at site level, only that site can use the rules.

You can configure query rules for one or more result sources, and you can specify a time period for when the query rule is active.

SharePoint has both a classic and a modern search experience. Only query rules that return promoted results can affect the modern search experience. Query rules that do query rewrites aren't supported for modern experiences. Users might see such promoted results on the **All** tab on the search results page when they search across all of SharePoint. Learn more about the differences between the classic and modern search experiences in SharePoint.

> **Important**
>
> In December 2021, Microsoft deprecated query rules with promoted results for organization-scoped queries in favor of Bookmark and Q&A answers in modern search experiences. Examples of organization-scoped queries are SharePoint Home and Office.com.
>
> Promoted results continue to work for all classic search experiences and for sites and hub sites with modern search experiences. Promoted results also continue to work for environments where Bookmark and Q&A answers aren't available.

Promote a search result

You can add several individual promoted results. When there's more than one promoted result, you can specify the relative ranking.

1. Go to the **Manage Query Rules** page for the tenant, a site collection, or a site:
    - For a tenant, in the new SharePoint admin center, select **More features**. Under **Search**, select **Open**. On the search administration page, select **Manage Query Rules**.
    - For a site collection, in your site collection, select **Settings**, and then select **Site settings**. If you don't see **Site settings**, select **Site information**, and then select **View all site settings**. Under **Site Collection Administration**, select **Search Query Rules**.
    - For a site, select **Settings**, and then select **Site settings**. If you don't see **Site settings**, select **Site information**, and then select **View all site settings**. Under **Search**, select **Query Rules**.
2. On the **Manage Query Rules** page, in the **Select a Result Source** list, select a result source for the new query rule.
3. Select **New Query Rule**.

4. On the **Add Query Rule** page, in the **General Information** section, in the **Rule name** field, type the name for the query rule.

5. Select to expand the **Context** section.

6. In the **Context** section, do one of the following:

   - To apply the query rule to all result sources, select **All sources**.

   - To apply the query rule to one or more specific result sources, select **One of these sources**. By default, the result source that you specified earlier is selected. To add a result source to the query rule, select **Add Source**, select a result source in the dialog, and then select **Save**.

7. In the **Query Conditions** section, do one of the following:

   - Select one of the conditions listed in Overview of conditions that make a query rule fire.

     > ⓘ **Note**
     >
     > The rule fires when any condition is true.

     To add more conditions, select **Add Alternate Condition**.

   - Select **Remove Condition** to configure this query rule to fire for every query that users type at the level at which you're creating the rule, and then go to the next step. For example, if you're creating this rule for a site collection, select **Remove Condition** if you want this rule to fire for every query that users type inside any search box in the site collection.

8. In the **Actions** section, specify the action to take when the query rule fires. Specify one of the following:

   - To promote individual results so they appear towards the top of search results, select **Add Promoted Result** (in SharePoint 2010 Products this option was called Best Bets). In the dialog, in the **Title** field, type the name that you want to give this promoted result. In the **URL** field, type the URL of the result that should be promoted. Select **Render the URL as a banner instead of as a hyperlink**. Select **Save**.

You can add several individual promoted results. When there's more than one promoted result, specify the relative ranking.

- To promote a group of search results, select **Add Result Block**. For more information, see Create and display a result block.
- To change ranked search results, select **Change ranked results by changing the query**. For more information, see Change ranked search results by changing the query.

9. To make the query rule active during a particular time period, select **Publishing**, and then specify the period.
10. Select **Save**.

Create and display a result block

A result block contains a small subset of results that are related to a query in a particular way. Like individual results, you can promote a result block or rank it with other search results.

When you configure a query condition for a result block, use *query variables*. Query variables are like placeholders for values that you don't yet know when you specify the query. However, when the query runs, this information is available and the system uses it to send the query to the index. For example, {User.Name} stands for the display name of the user who typed in the query. Another one is {searchBoxQuery}, which stands for the query a user typed in a search box. When you use the Query Builder to configure the query, a list of query variables is shown. (See step 3 in the procedure right below.)

1. In step 9 of the procedure Create a query rule, on the **Add Query Rule** page, in the **Actions** section, click **Add Result Block**.
2. Enter the title that appears in the result block in the **Title** field in the **Block Title** section.
3. Configure the query that gives results for the block. In the **Query** section, click **Launch Query Builder** and on the **BASICS** tab, complete the following steps:
   - Select which content to search by selecting a result source from the drop-down list in the **Select a query** section.
   - Specify your query. See Query variables in SharePoint Server 2013 for a list of available query variables. You can select predefined query variables from the **Keyword filter** drop-down list, and then add them to the Query text box by clicking **Add keyword filter**.

- If relevant, use property filters to query the content of managed properties that are set to queryable in the search schema. You can select managed properties from the **Property filter** drop-down list. Select **Add property filter** to add the filter to the query.

> ⓘ **Note**
>
> Custom managed properties don't appear in the **Property filter** list. To add a custom managed property to your query, in the **Query text** box, enter the name of your custom managed property followed by the query condition, for example *MyCustomColorProperty:Green*.

4. Specify how the search results within your result block should be sorted. Sorting of search results is case sensitive. On the **SORTING** tab, in the **Sort by** drop-down list, select a managed property, and then select **Descending** or **Ascending**. The list only contains managed properties that are set as sortable in the search schema. You can also sort by rank. To add more sorting levels, click **Add sort level**.

5. If you choose to sort by rank, you can optionally define rules for dynamically changing the ordering of results. In the **Dynamic ordering** section, define when to change ranking by selecting a condition from the drop-down list and then specifying whether to **promote** or **demote** the result. To add more rules, click **Add dynamic ordering rules**.

6. Preview the final query that the Content Search Web Part runs, on the **TEST** tab. The preview is based on the original query template where dynamic variables are substituted with current values. Other changes to the query might be made as part of query rules. Click **Show more** to display additional information.

   - The **Query text** shows the final query that the Content Search Web Part runs. It's based on the original query template where dynamic variables are replaced with current values. You might end up making other changes to the query as part of query rules.

   - The **Query template** box shows the content of the query template that is applied to the query.

   - The **Query template variables** section shows the query variables that are applied to the query, and the values of the variables that apply to the current page. You can type other values to test the effect they have on the query. Click the **Test Query** button to preview the search results.

7. Click **OK** to close the **build your query** dialog.

8. Define which result source this result block should apply to. Use the **Search this Source** drop-down list in the **Query** section.

9. In the **Items** drop-down list, select how many results to show in the result block.

10. Expand the **Settings** section.

    The result block only displays the number of search results that you specified in the previous step. However, you can add a **Show more** link at the bottom of the result block that shows all search results for the result block.

    To add a **Show more** link, select **"More" link goes to the following URL**, and then type a URL. You can use query variables in this URL, like this example: `http://www.\<site\>/search/results.aspx?k={subjectTerms}`.

11. Select **OK**.

Change ranked search results by changing the query

The ranking model calculates a ranking order of search results. You can change this ranking by promoting or demoting items within the search results. For example, for a query that contains "download toolbox", you can create a query rule that recognizes the word "download" as an action term. Once you add this rule, you can change the ranked search results to promote the URL of a specific download site on your intranet.

You can also dynamically change the sorting order of the search results, based on several variables such as file name extension or specific keywords. When you change ranked search results by changing the query, you see that your results are security trimmed and refinable. Moreover, the search results don't show up if the document is no longer there.

1. In step 9 of the procedure Create a query rule, on the **Add Query Rule** page, in the **Actions** section, select **Change ranked results by changing the query**. The **build your query** dialog appears.

2. On the **BASICS** tab, complete the following steps:

    - Select which content to search by selecting a result source from the drop-down list in the **Select a query** section.

    - Specify your query. See Query variables in SharePoint Server 2013 for a list of available query variables. You can select predefined query variables from the **Keyword filter**

drop-down list, and then add them to the Query text box by clicking **Add keyword filter**.

- If relevant, use property filters to query the content of managed properties that are set to queryable in the search schema. You can select managed properties from the **Property filter** drop-down list. Select **Add property filter** to add the filter to the query.

3. Specify how the search results within your result block should be sorted. Sorting of search results is case sensitive. On the **SORTING** tab, in the **Sort by** drop-down list, select a managed property, and then select **Descending** or **Ascending**. The list only contains managed properties that are set as sortable in the search schema. You can also sort by rank. To add more sorting levels, select **Add sort level**.

4. If you choose to sort by rank, you can optionally define rules for dynamically changing the ordering of results. In the **Dynamic ordering** section, define when to change ranking by selecting a condition from the drop-down list and then specifying whether to **promote** or **demote** the result. To add more rules, select **Add dynamic ordering rules**.

5. Preview the final query that the Content Search Web Part runs, on the **TEST** tab. The preview is based on the original query template where dynamic variables are substituted with current values. Other changes to the query might be made as part of query rules. Select **Show more** to display additional information.

   - The **Query text** shows the final query that the Content Search Web Part runs. It's based on the original query template where dynamic variables are replaced with current values. You might end up making other changes to the query as part of query rules.

   - The **Query template** box shows the content of the query template that is applied to the query.

   - The **Query template variables** section shows the query variables that are applied to the query, and the values of the variables that apply to the current page. You can type other values to test the effect they have on the query. Click the **Test Query** button to preview the search results.

6. Select **OK** to close the **Build Your Query** dialog.

7. Select **Save**.

Make a query rule inactive on a site

Site collections and sites inherit query rules that you create at the tenant level. Similarly, sites in the site collection inherit query rules that you create at the site collection level. If you don't want a query rule to apply to a site that inherits it, you can make the query rule inactive for the site.

1. On your site, select **Settings**, and then select **Site settings**. If you don't see **Site settings**, select **Site information**, and then select **View all site settings**.

2. On the **Site Settings** page, in the **Search** section, select **Query Rules**.

3. On the **Manage Query Rules** page, on the **Select a Result Source** menu, select the result source that contains the query rule that you want to make inactive.

4. In the **Name** column, point to the query rule that you want to make inactive, select the arrow that appears, and then select **Make Inactive**.

Rank query rules for a site collection

When multiple query rules are active for a tenant, a site collection, or a site, more than one rule can fire for a query that you perform at that level. By default, the rules don't fire in a specific order. However, if you want to control the order in which the rules fire, add the query rules that you create to query groups. To do this, select rules to add to a group, and then specify the order in which the rules in the group fire if they're triggered. You can also prevent query rules that rank lowest in a group from firing even if they do get triggered.

1. In the site collection, select **Settings**, and then select **Site settings**. If you don't see **Site settings**, select **Site information**, and then select **View all site settings**.

2. On the **Site Settings** page, in the **Site Collection Administration** section, select **Search Query Rules**.

3. On the **Manage Query Rules** page, on the **Select a Result Source** menu, select the result source that contains the query rules that you want to group.

4. For each query rule that you created that you want to add to a group, point to the rule and select the check box.

> **Note**
>
> The **Defined for this site collection** section lists query rules that you created for this site collection.

5. Select **Order Selected Rules**.

6. In the **Order Selected Rules** dialog, do either of the following, and then select **OK**:

   - Select **Move rules to new group with this name**, and then type a name for the group.
   - Select **Move rules to existing group** and select a group in the list.

7. On the **Manage Query Rules** page:

   - To change the order in which a rule in a group fires if it's triggered, change the number ordering of the rule.
   - To prevent query rules that are ranked lowest in the group from firing, go to the row for the group's query rule that should fire last, and then in the **Actions** column, in the **Continue/Stop** list, select **Stop**.

Overview of conditions that make a query rule fire

Expand table

Query condition	Description	Configuration	Example
Query Matches Keyword Exactly	The query rule fires when a query exactly matches a word or phrase that you specify.	In the **Query exactly matches one of these phrases** text box, type one or more phrases separated by semicolons.	Type "picture; pic" in the box. The query rule fires when a user types "picture" or "pic" in a search box. The rule doesn't fire if a user types "pictures" or "sunny picture."
Query Contains Action Term	The query rule fires when a query contains a term for something that the user wants to do. The term must be at the beginning or end of the query.	Enter the action term that causes the query rule to fire by doing one of the following: Select **Action term is one of these phrases**, and type one or more phrases.	Type the word "download" in the **Action term is one of these phrases** box. When a user types "download Contoso Electronics datasheet" in a search box, there are chances the user isn't searching for a document that contains the words "download," "Contoso," "Electronics," and "datasheet." Instead, the user most likely wants to download a Contoso Electronics datasheet. The query rule fires, and only the words "Contoso," "Electronics," and "datasheet" are sent to the search index.
Query More Common in	The query rule fires if users frequently sent	In the **Query is more likely to be used in**	You selected **Local Video Results** in the list. The query rule fires if a user types the word

Query condition	Description	Configuration	Example
Source	this query from another source that you already specified.	**this source** list, select a result source.	"training" in a search box and if that word is already frequently typed in a search box in the Videos vertical.
Result Type Commonly Clicked	The query rule fires if other users frequently clicked a particular result type after typing the same query.	In the **Commonly clicked results match result type** list, select a result type.	You selected **SharePoint MicroBlog Post** in the list. If users frequently click a microblog post in search results, consider configuring the most recent microblog post as the first promoted result, and the next most recent microblog post as the second promoted result (in the **Actions** section).
Advanced Query Text Match	You want to use a phrase or a dictionary entry that causes the query rule to fire, and then define more detailed conditions for when the query rule fires.	Enter the phrase or term that causes the query rule to fire by doing one of the following: Select **Query contains one of these phrases**, and type one or more phrases.	You selected **Query contains one of these phrases**, and then chose **Start of query matches, but not entire query**. The query rule fires only if the phrase is at the beginning of a query, not if it's at the end.

Last updated on 06/25/2026

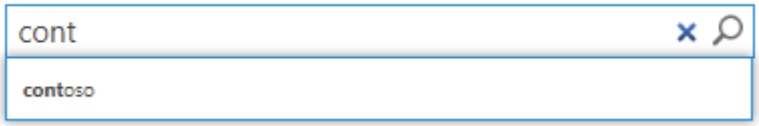
Customize query suggestions in SharePoint search

Article • 02/21/2023

Query spelling suggestions are words that appear below the search box as a user types a query. SharePoint automatically creates query suggestions from frequently entered queries that resulted in a click on a search result. For example, if you've repeatedly entered the query word "coffee" and then clicked a search result each time, "coffee" automatically becomes a query suggestion.

Automatic query suggestions are generated periodically for each result source and each site collection, so the query suggestions can be different for different result sources and site collections.

For example, in the following screenshot, "contoso" is automatically suggested.



SharePoint has both a classic and a modern search experience, learn about the differences between the classic and modern search experiences in SharePoint. The modern search experience uses the same default result source as the classic search experience. Automatic query suggestions for the default result source appear only in the classic search experience.

As an admin you can manually create your own lists of queries that always shall be suggested or phrases that never shall be suggested, and import them to SharePoint.

- Your list of queries that shall always be suggested only applies to modern search and only in tenant-wide scope.
- Your list of phrases that never shall appear apply to both classic and modern search, to all result sources and all site collections.

To create query suggestions for multiple languages, you'll need to create a separate file for each language. The language determines how the query suggestions are processed internally in the search system. All manual query suggestions are always displayed for **all** languages. Add each phrase as a separate line in the text file that you create and save the file in UTF-8 encoding.

Query suggestions are turned on by default. To turn them off, go to **Search Suggestions**, and clear **Show search suggestions**.

To create query suggestions in SharePoint search

1. Go to **More features** in the SharePoint admin center, and sign in with an account that has admin permissions for your organization.

   > **Note**
   >
   > If you have Office 365 operated by 21Vianet (China), sign in to the Microsoft 365 admin center, then browse to the SharePoint admin center and open the More features page.

2. Under **Search**, select **Open**.

3. On the search administration page, select **Query Suggestion Settings**.

4. Open a text editor of your choice, and enter a list of terms that you want the system to always suggest to users. Only add one term per line to the text file, and don't mix languages in the text file.

5. Save the text file to a location that's accessible from SharePoint.

6. To import a list of query suggestions to SharePoint search, go to **Always suggest phrases** > **Import from text file**. When you import query suggestions, any existing ones will be overwritten.

7. Browse to the file that you want to import.

8. Go to **Language for suggestion phrases**, and select the processing language of your query suggestions. It should match the language of the terms in the text file.

9. Select **Save Settings**.

Related tasks

You can edit a list of query suggestions that you've manually created. To edit a list that you've already imported into SharePoint, choose **Export to text file**, update the text file with your changes, and then re-import it. After you've uploaded your query suggestions file, it might take up to a week until your query suggestions are displayed. You can check that they're working properly by entering a phrase from your list of query suggestions in the search box. The query suggestion should appear below the search box.

To get rid of a list of query terms, you must overwrite it. Do this by importing an empty text file.

To prevent terms from appearing in the search box, create a text file with the query terms that you never want users to see below the search box, and then import it to **Never suggest phrases**.

Feedback

Was this page helpful? Yes No

Provide product feedback

Manage result sources

Article • 10/17/2024

Result sources limit searches to certain content or to a subset of search results. You can also use result sources to send queries to external providers such as Bing.

A SharePoint Administrator or above can manage result sources for all site collections and sites in the tenant. A site collection administrator or a site owner can manage result sources for a site collection or a site, respectively.

SharePoint has both a classic and a modern search experience. The modern search experience gets results from the default result source. If you change the default result source, this impacts both the classic and modern search experiences. Learn more about the differences between the classic and modern search experiences in SharePoint.

For the classic search experience, you can create your own result sources, or use the predefined result sources. After you create a result source, you configure Search Web Parts and query-rule actions to use it.

Create a new result source

1. Go to the **Manage Result Sources** page for the tenant, for a site collection, or a site:

    - For a tenant, in the new SharePoint admin center, select **More features**. Under **Search**, select **Open**, and then on the search administration page, select **Manage Result Sources**.

    - For a site collection, in your site collection, select **Settings**, and then select **Site settings**. If you don't see **Site settings**, select **Site information**, and then select **View all site settings**. Under **Site Collection Administration**, select **Search Result Sources**.

    - For a site, select **Settings**, and then select **Site settings**. If you don't see **Site settings**, select **Site information**, and then select **View all site settings**. Under **Search**, select **Result Sources**.

2. On the **Manage Result Sources** page, select **New Result Source**.

3. In the **General Information** section, type a name and a description for the new result source.

4. In the **Protocol** section, select one of the following protocols for retrieving search results:

    - **Local SharePoint**, the default protocol, provides results from the search index of this tenant (Search Service).
    - **Remote SharePoint** (retired) provides results from the index of a search service in a different farm (external source). In the **Remote Service URL** box, type the address of the root site collection of the remote SharePoint farm.
    - **OpenSearch 1.0/1.1** (retired) provides results from a search engine that uses the OpenSearch 1.0/1.1 protocol.
    - **Exchange** provides results from Microsoft Exchange Server. Select **Use AutoDiscover** to have the search system find an Exchange Server endpoint automatically, or type the URL of the Exchange web service to retrieve results from — for example, https://contoso.com/ews/exchange.asmx

> **Important**
>
> As of September 2024, for SharePoint Online Microsoft 365 Result Sources, the OpenSearch and Remote SharePoint protocol options have been retired and will soon be removed from the Result Source configuration UI. Any SharePoint Online Result Source currently configured to use these options will have zero results returned.

> **Note**
>
> The Exchange Web Services Managed API must be installed on the computer where the search service is running.

5. If you choose **Local SharePoint** or **Remote SharePoint** for protocol, choose a **Type**:

    - **SharePoint Search Results** to search the whole index.
    - **People Search Results** to search in people profiles and enable query processing that is specific to people search, such as phonetic name matching or nickname matching.

6. In the **Query Transform** section, you can change incoming queries to use a new query text instead. Choose one of these options:

- Leave the default query transform (**searchTerms**) as is. The query will be unchanged since the previous transform.
- Type a different query transform in the box. See Understanding query transforms .
- Build your own query. Select **Launch Query Builder** and build your query by specifying filters on the **BASICS**, sorting on the **SORTING** tab, and then testing the query on the **TEST** tab. Each of these tabs are described in the following sections.

7. In the **Credentials Information** section, choose an authentication type for users to connect to the result source.
8. Select **Save**.

The BASICS tab

Expand table

Choose this option	To do this
Keyword filter	Use keyword filters to add predefined query variables to the query transform. Select query variables from the list, and add them to the query by clicking **Add keyword filter**.
Property filter	Use property filters to query the content of managed properties that are set to **queryable** in the search schema. Select managed properties from the **Property filter** list. Click **Add property filter** to add the filter to the query. **NOTE**: Custom managed properties are not shown in the **Property filter** list. To add a custom managed property to your query, in the **Query text** box, enter the name of your custom managed property followed by the query condition, for example *MyCustomColorProperty:Green*

The SORTING tab

Expand table

Choose this option	To do this
Sort results	Define sorting for results. The **Sort by** list contains managed properties that are set as sortable in the search schema. Select a property to sort by, and then select **Descending** or **Ascending**. To sort by relevance, select **Rank**. Click **Add sort level** if you want to specify more levels of sorting.
Dynamic ordering	Click **Add dynamic ordering rule** to specify additional ranking by adding rules that change the order of results within the result block when certain conditions are met. You can add conditions by choosing from the lists that appear.

The TEST tab

Expand table

Choose this option	To do this
Query text	See the final query text, which is based on the original query template, the applicable query rules, and the variable values.
Show more	Click the link to show more options.
Query template	See the query as it is defined in the **BASICS** tab or in the text box in the **Query transform** section on the Add Result Source page.
Query template variables	Test the query template by specifying values for the query variables. Click **Test query** to see the results.

Set a result source as default

The default result source is **Local SharePoint Results**, but you can choose to set a different one as the default. By doing this, it will be easier to edit the query in Search Web Parts. For example, when you add a Content Search Web Part to a page, the Web Part automatically uses the default result source.

1. Go to the **Manage Result Sources** page for the tenant, for a site collection, or a site:

    - For a **tenant**, in the new SharePoint admin center, select More features. Under **Search**, select **Open**, and then on the search administration page, select **Manage Result Sources**.

- For a site collection, in your site collection, select **Settings**, and then select **Site settings**. If you don't see **Site settings**, select **Site information**, and then select **View all site settings**. Under **Site Collection Administration**, select **Search Result Sources**.
- For a site, select **Settings**, and then select **Site settings**. If you don't see **Site settings**, select **Site information**, and then select **View all site settings**. Under **Search**, select **Result Sources**.

2. On the **Manage Result Sources** page, point to the result source that you want to set as the default, select the arrow that appears, and then select **Set as Default**.

Delete a result source

A result source might be no longer needed. The following procedure provides the steps for removing a result source.

1. Go to the **Manage Result Sources** page for the tenant, for a site collection, or a site:
   - For a **tenant**, in the new SharePoint admin center, select More features. Under **Search**, select **Open**, and then on the search administration page, select **Manage Result Sources**.
   - For a site collection, in your site collection, select **Settings**, and then select **Site settings**. If you don't see **Site settings**, select **Site information**, and then select **View all site settings**. Under **Site Collection Administration**, select **Search Result Sources**.
   - For a site, select **Settings**, and then select **Site settings**. If you don't see **Site settings**, select **Site information**, and then select **View all site settings**. Under **Search**, select **Result Sources**.
2. On the **Manage Result Sources** page, point to the result source that you want to remove, select the arrow that appears, select **Delete**, and then select **Ok** in the confirmation dialog.

See also

Understanding result sources

Understanding query transforms

Feedback

Was this page helpful? Yes No

Provide product feedback

Manage result types

Article • 10/03/2022

As a site collection administrator or site owner, you can create and use result types to customize how results are displayed for particular types of documents.

SharePoint has both a classic and a modern search experience. For the classic search experience, you use a result type to specify a display template that the search system should use for a particular type of document or search result. As documents aren't all the same, search results shouldn't be either. By using result types and display templates, it's much easier for users to find the results they are looking for. You can't customize how results are displayed for the modern search experience. Learn about the differences between the classic and modern search experiences in SharePoint.

A result type specifies one or more conditions to compare search results against, such as the type or the result source of the search result, and an action to take if a search result meets those conditions. The action specifies the display template to use for the search result.

For example, a preconfigured result type named **Person** specifies that if a search result comes from the result source **Local People Results**, then use the **People Item** display template. The **People Item** display template shows information in the hover panel such as documents the person's authored and gives you quick access to those documents.

Another example is to have a result type that fires if the **ContentType** property **contains** *Sales Report* , and then have a specific display template for sales reports. Users will identify the search result as a sales report right away.

See Change how search results look by using result types and display templates for more information.

There are many preconfigured result types to choose from, and you can also create new custom result types. You can configure result types at site collection level and at site level.

Add a new result type

1. Go to the **Manage Result Types** page for a site collection or a site:

- For a site collection, in your site collection, select **Settings** , and then select **Site settings**. If you don't see **Site settings**, select **Site information**, and then select

View all site settings. Under **Site Collection Administration**, select **Search Result Types**.

- For a site, select **Settings** , and then select **Site settings**. If you don't see **Site settings**, select **Site information**, and then select **View all site settings**. Under **Search**, select **Result Types**.

2. On the **Manage Result Types** page, do one of the following:

- Click **New Result Type**, or
- In the list of existing result types, click the name of a result type, such as **Person**, and then click **Copy** so that you can modify the copy to create a new result type.

3. In the **General Information** section, in the **Give it a name** box, type a name for the result type.
4. In the **Conditions** section, in the first list, choose a result source that the results should match.
5. In the **Conditions** section, in the second list, choose which types of content should match. To match all content, skip the rule. To add more content types, click **Add value**.
6. To add more advanced conditions related to managed properties, expand **Show more conditions**.
7. In the first list, choose a property to match.
8. Choose how the property should relate to one or more values.
9. Enter one or more values for the property in the box. Separate by using semicolons.
10. To add more properties to match, click **Add property**.
11. In the **Actions** section, select a display template. The URL of the display template is shown under **Display template URL**.
12. Check the **Optimize for frequent use** box if the result type will be among the most frequently used result types.
13. Click **Save**.

Feedback

Was this page helpful? Yes No

Provide product feedback

Manage search dictionaries

Article • 02/21/2023

APPLIES TO: ✓ 2013 ✓ 2016 ✓ 2019 ✓ Subscription Edition ✗ SharePoint in Microsoft 365

In SharePoint Server, you can use search dictionaries to include or exclude company names to be extracted from the contents of your indexed documents, or you can include or exclude words for query spelling correction.

Manage company name extraction

> **Note**
>
> Beginning on November 15th, 2019, we'll be removing Company Name Extraction from SharePoint in Microsoft 365. This will only impact you if you have configured company name extraction to be surfaced in the classic Enterprise Search Center as a refiner. Learn more about the specifics and other options by reading Changes to company name extraction in SharePoint.

For company name extraction to work, that is, for a company name to be pulled from your content and for it to be mapped to the managed property **companies**, you have to make sure that:

- The managed property setting **Company name extraction** is enabled on the managed property that you want to extract company names from. This setting is available for the managed properties **Title**, **Body** and **Notes**. See also Manage the search schema in SharePoint.
- The name of the company that you want to extract is in the prepopulated company name dictionary or in the **Company Inclusions** list.

After you have done this, you can then use the managed property **companies** to create refiners based on the extracted company name in the **Refinement Web Part**, on the search results page.

Include company names

1. Go to **More features** in the SharePoint admin center, and sign in with an account that has admin permissions for your organization.

> **Note**
>
> If you have Office 365 operated by 21Vianet (China), sign in to the Microsoft 365 admin center, then browse to the SharePoint admin center and open the More features page.

2. Under **Search**, select **Open**, and to open the term store, select **Manage Search Dictionaries**.
3. On the **Site Settings: Term Store Management Tool** page, to expand the **Search Dictionaries** menu, select the arrow.
4. Select **Company Inclusions**, then select the arrow, and then select **Create Term**.
5. Enter the name of the company that you want to include in the box that appears.
6. To add the term to the **Company Inclusions** list, select anywhere on the page.

Exclude company names

1. Go to **More features** in the SharePoint admin center, and sign in with an account that has admin permissions for your organization.

> **Note**
>
> If you have Office 365 operated by 21Vianet (China), sign in to the Microsoft 365 admin center, then browse to the SharePoint admin center and open the More features page.

2. Under **Search**, select **Open**.
3. To open the term store, select **Manage Search Dictionaries**.
4. On the **Taxonomy Term Store** page, to expand the **Search Dictionaries** menu, select the arrow.
5. Select **Company Exclusions**, then select the arrow, and then select **Create Term**.
6. Enter the name of the company that you want to exclude in the box that appears.
7. To add the term to the **Company Exclusions** list, select anywhere on the page.

Manage query spelling correction

> **Note**
>
> Beginning on December 8, 2020, we'll be removing Query Spelling Inclusions and Query Spelling Exclusions from SharePoint in Microsoft 365. This will only impact you if you have configured Query Spelling Suggestions.

If you or another user enters a word in a search query that appears to be misspelled, the search results page helps you out by displaying query spelling corrections. This is also known as "Did you mean?".

For example, if you enter a query that contains the word "ampitheater", the query spelling correction would show "amphitheater" if this term is available in many places in your indexed documents. You can add terms such as the one just shown to the **Query Spelling Inclusions** list, or to the **Query Spelling Exclusions** list to influence how you want query spelling corrections to be applied or not. It takes up to 10 minutes for any changes to the **Query Spelling Inclusions** or the **Query Spelling Exclusions** list to take effect.

Include a term in query spelling corrections

1. Go to **More features** in the SharePoint admin center, and sign in with an account that has admin permissions for your organization.

> **Note**
>
> If you have Office 365 operated by 21Vianet (China), sign in to the Microsoft 365 admin center, then browse to the SharePoint admin center and open the More features page.

2. Under **Search**, select **Open**.
3. To open the term store, select **Manage Search Dictionaries**.
4. On the **Site Settings: Term Store Management Tool** page, to expand the **Search Dictionaries** menu, select the arrow.
5. Select **Query Spelling Inclusions**, then select the arrow, and then select **Create Term**.

6. Enter the query spelling that you want to include in the box that appears.
7. To add the term to the **Query Spelling Inclusions**, select anywhere on the page.

Exclude a term from query spelling corrections

1. Go to **More features** in the SharePoint admin center, and sign in with an account that has admin permissions for your organization.

> **Note**
>
> If you have Office 365 operated by 21Vianet (China), sign in to the Microsoft 365 admin center, then browse to the SharePoint admin center and open the More features page.

2. Under **Search**, select **Open**.
3. To open the term store, select **Manage Search Dictionaries**.
4. On the **Site Settings: Term Store Management Tool** page, to expand the **Search Dictionaries** menu, select the arrow.
5. Select **Query Spelling Exclusions**, then select the arrow, and then select **Create Term**.
6. Enter the query spelling that you want to exclude in the box that appears.
7. To add the term to the **Query Spelling Exclusions** list, select anywhere on the page.

Edit query spelling corrections or company names

1. Go to **More features** in the SharePoint admin center, and sign in with an account that has admin permissions for your organization.

> **Note**
>
> If you have Office 365 operated by 21Vianet (China), sign in to the Microsoft 365 admin center, then browse to the SharePoint admin center and open the More features page.

2. Under **Search**, select **Open**.
3. To open the term store, select **Manage Search Dictionaries**.
4. On the **Site Settings: Term Store Management Tool** page, to expand the **Search Dictionaries** menu, select the arrow.
5. Depending on which dictionary the term is in, select **Company Exclusions**, **Company Inclusions**, **Query Spelling Exclusions**, or **Query Spelling Inclusions**.
6. Double-click the term that you want to edit.
7. Enter the new name for the term.
8. To save the edited term, select anywhere on the page.

Feedback

Was this page helpful? Yes No

Provide product feedback

Manage authoritative pages

Article • 02/21/2023

APPLIES TO: ✓ 2013 ✓ 2016 ✓ 2019 ✓ Subscription Edition ✗ SharePoint in Microsoft 365

As a SharePoint Administrator and above in Microsoft 365, you can influence the pages or documents that should appear at the top of your list of search results by identifying high-quality pages, also known as authoritative pages. Authoritative pages link to the most relevant information. A typical example of an authoritative page could be the home page of your company portal.

Authoritative pages only work for **classic** search and only for web parts that use the **default** ranking model.

If you have specific knowledge of an area, you can influence the relative importance of pages by adding more levels of authoritative pages (second-level and third-level).

In the same way, you can also add non-authoritative pages. A typical example of a non-authoritative page could be the URL of a site that contains outdated information.

Specify authoritative or non-authoritative pages

1. Go to **More features** in the SharePoint admin center, and sign in with an account that has admin permissions for your organization.

   > **Note**
   >
   > If you have Office 365 operated by 21Vianet (China), sign in to the Microsoft 365 admin center, then browse to the SharePoint admin center and open the More features page.

2. Under **Search**, select **Open**.

3. On the search administration page, select **Manage Authoritative Pages**.

4. In the **Authoritative Web Pages** section, in the **Most authoritative pages** box, enter the URLs of pages that are the most important. Separate the URLs with returns so that there is one URL per line.

5. In the **Second-level authoritative pages** box, enter the URLs of any pages that should be seen as second-level.

6. In the **Third-level authoritative pages** box, enter the URLs of any pages that should be seen as third-level.

7. In the **Non-authoritative Sites** section, in the **Sites to demote** box, enter the URLs of any sites that you want to be ranked lower than all of the other sites. Type one URL per line.

   > **Tip**
   >
   > All URLs whose prefix matches the prefix of a URL in the **Sites to demote** box are demoted. Example: Entering http://archive/ demotes the rank of all URLs that begin with http://archive/.

8. Select **OK**.

How results are ranked

Classic search uses the list of authoritative pages to calculate the ranking of results. Static rank determines the relative importance of a page. Static rank is calculated as the smallest number of clicks that it would take a user to navigate from an authoritative page to a document. The closer a document is to the most authoritative page, the higher the static rank of the page is.

Feedback

Was this page helpful? Yes No

Provide product feedback

Export and import customized search configuration settings

Article • 02/21/2023

As a SharePoint Administrator and above in Microsoft 365, you can export and import customized search configuration settings between tenants, site collections, and sites. The settings that you export and import include all customized query rules, result sources, result types, ranking models and site search settings. It's also possible to export customized search configuration settings from a Search service application and import the settings to tenants, site collections, or sites. You can't export the default configuration settings.

Overview

When you export customized search configuration settings, SharePoint creates a search configuration file in XML format. This search configuration file includes all exportable customized search configuration settings at the tenant, site collection, or site level from where you start the export. A search configuration file for a site collection doesn't contain search configuration settings from the individual sites within the site collection.

When you import a search configuration file, SharePoint creates and enables each customized search configuration setting in the tenant, site collection or site from where you start the import.

This table shows the settings that you can export or import. For each setting, you'll find dependencies on other customized search configuration settings. If the customized search configuration settings depend on a customized search configuration setting at a different level, for example, if a site query rule depends on a result source at site collection level, you must export and import settings at all of the relevant levels.

Expand table

Customized search configuration setting	Dependency on other customized search configuration settings
Query rules. These include result blocks, promoted results, and user segments.	Result sources, result types, search schema, ranking model.
Result sources	Search schema
Result types	Search schema, result sources, display

Customized search configuration setting	Dependency on other customized search configuration settings
	templates
Search schema	None
Ranking model	Search schema

Conditions that can cause the import to fail

If the search configuration file and the target for your import have settings with the same name, the import of the search configuration file fails when it encounters this setting. There are exceptions however:

- If you reimport a search configuration file, the settings that have the same name in the search configuration file and on the target do not cause the import to fail.
- Managed properties with the same name do not cause an import to fail if the individual managed property settings are the same on the property in the search configuration file and on the target property.
- Managed properties with the same name do not cause an import to fail if the aliases and mappings to crawled properties are different on the managed property in the search configuration file and on the target managed property. The import adds the aliases and mappings on the managed property in the search configuration file to the aliases and mappings on the target managed property.

If the search configuration file contains managed property names or aliases that contain invalid characters, the import fails when it encounters that managed property name or alias.

The managed property names and aliases of a search schema must be unique for a site and its parent site collection. This means:

- If your search configuration file has a managed property that has the same name as an alias for a managed property on your target site or the parent site collection of your target site, then the import fails.
- If your search configuration file has a managed property with an alias that has the same name as a managed property on your target site or the parent site collection of your target site, then the import fails.

Note

Any customized search settings that were created and enabled by SharePoint before the import failed, remain enabled.

If the import fails, remove the condition that caused the failure and reimport the search configuration file. For example, if the Notes column states that there is already a query rule with the same name as the query rule that you are trying to import, then you should remove that query rule either from the target or from the import file, and then reimport the file. See Invalid characters causing your import to fail later in this article.

Export customized search configuration settings from a tenant

1. Go to **More features** in the SharePoint admin center, and sign in with an account that has admin permissions for your organization.

   > **Note**
   >
   > If you have Office 365 operated by 21Vianet (China), sign in to the Microsoft 365 admin center, then browse to the SharePoint admin center and open the More features page.

2. Under **Search**, select Open.
3. Select **Export Search Configuration**.
4. In the dialog, select **Save**.

Export customized search configuration settings from a site

1. On the site, select **Settings**, and then select **Site settings**. If you don't see **Site settings**, select **Site information**, and then select **View all site settings**.
2. On the **Site Settings** page, in the **Search** section, select **Configuration Export**.
3. In the dialog, select **Save**.

Export customized search configuration settings from a site collection

1. On the site, select **Settings**, and then select **Site settings**. If you don't see **Site settings**, select **Site information**, and then select **View all site settings**.

2. On the **Site Settings** page, in the **Site Collection Administration** section, select **Search Configuration Export**.

3. In the dialog, select **Save**.

Import customized search configuration settings to a tenant

1. Go to **More features** in the SharePoint admin center, and sign in with an account that has admin permissions for your organization.

   > **Note**
   >
   > If you have Office 365 operated by 21Vianet (China), sign in to the Microsoft 365 admin center, then browse to the SharePoint admin center and open the More features page.

2. Under **Search**, select **Open**.

3. On the **Import Search Configuration** page, browse to the file you want to import.

4. Select **Import**.

5. On the **Search Config List** page, verify that:

6. The search configuration file you imported is in the list, and that its status is **Imported Successfully**.

   If the file hasn't been imported successfully, then the **Notes** column provides more details about what happened.

7. The **Scope** column shows that the settings you imported are at the right level, that is, at the level you meant to import the file to. For example, if you imported your settings at the site collection level instead of at the site level, you'd see this information in the **Scope** column. The **Scope** column shows at which level the search configuration settings were enabled. The levels are: tenant (Tenant), site collection (SPSite), or site level (SPWeb).

Import customized search configuration settings to a site

1. On the site, select **Settings**, and then select **Site settings**. If you don't see **Site settings**, select **Site information**, and then select **View all site settings**.

2. On the **Site Settings** page, in the **Search** section, select **Configuration Import**.

3. On the **Import Search Configuration** page, browse to the file you want to import.

4. Select **Import**.

5. On the **Search Config List** page, verify that:

6. The search configuration file you imported is in the list, and that its status is **Imported Successfully**.

   If the file hasn't imported successfully, then the **Notes** column provides more details about what happened.

7. The **Scope** column shows that the settings you imported are at the right level, that is, at the level you meant to import the file to. For example, if you imported your settings at the site collection level instead of at the site level, you'd see this information in the **Scope** column. The **Scope** column shows at which level the search configuration settings were enabled. The levels are: tenant (Tenant), site collection (SPSite), or site level (SPWeb).

Import customized search configuration settings to a site collection

1. On the site, select **Settings**, and then select **Site settings**. If you don't see **Site settings**, select **Site information**, and then select **View all site settings**.

2. On the **Site Settings** page, in the **Site Collection Administration** section, select **Search Configuration Import**.

3. On the **Import Search Configuration** page, browse to the file you want to import.

4. Select **Import**.

5. On the **Search Config List** page, verify that:

6. The search configuration file you imported is in the list, and its status is **Imported Successfully**.

If the file hasn't imported successfully, then the **Notes** column provides more details about what happened.

7. The **Scope** column shows that the settings you imported are at the right level, that is, at the level you meant to import the file to. For example, if you imported your settings at the site collection level instead of at the site level, you'd see this information in the **Scope** column. The **Scope** column shows at which level the search configuration settings were enabled. The levels are: tenant (Tenant), site collection (SPSite), or site level (SPWeb).

Invalid characters causing your import to fail

If managed properties or aliases contain any of the listed characters, the import of the customized search schema that contains these properties will fail.

Expand table

Character	Name
	space
:	colon
;	semicolon
,	comma
(	opening parenthesis
)	closing parenthesis
[	opening bracket
]	closing bracket
{	opening brace
}	closing brace
%	percent
$	dollar sign
_	underscore
+	plus sign
!	exclamation point

Character	Name
*	asterisk
=	equal sign
&	ampersand
?	question mark
@	at sign
#	number sign
\	backslash
~	tilde
<	opening angle bracket
>	closing angle bracket
|	pipe
`	grave accent
^	caret
'	escape sequence
"	escape sequence

Known issue

Unable to load Search Configuration List

When you import search configuration files into the tenant admin search settings page, you might encounter an issue that the **Search Configuration List** could not display properly and you might receive a "File not found" error.

This issue only blocks the UI from displaying the list of search configuration files you imported and would not break the **Import** functionality. Your search configuration will be imported properly.

Since you are unable to check the status of the search configuration file you imported from the UI, you could choose an alternative way to access the list, like SharePoint CSOM API or SharePoint Online REST API.

Unable to import stale search configuration XML file

If the search configuration file was exported a long time ago, the import might fail.

If the exported search configuration file is stale, you should export a new search configuration first and then use it to import the list of search configuration files.

Feedback

Was this page helpful? Yes No

Provide product feedback

Check logs, limits and reports

Article • 10/03/2022

See if the crawler has added content to the search index, and if your users are finding what they're looking for in SharePoint.

View search usage reports

This article describes how you can use search reports in the SharePoint admin center to find answers to questions about how search is being used in your organization. You can for example see the number of queries and the top queries. Learn more.

Query throttling

In SharePoint, you can't turn query throttling on or off, but you can use client-type information to make sure lower-priority clients like automated queries don't squeeze out higher-priority clients like UI. Learn more.

Set crawl log permissions

Use the crawl log to see if crawled content was successfully added to the search index, if it was excluded because of a crawl rule, or if indexing failed because of an error. Learn more.

Search limits

Look up the limits to SharePoint search. For example, there are limits to the number of entries you can have in a custom search dictionary and the number of results that can be returned for a query. Learn more.

Feedback

Was this page helpful? Yes No

Provide product feedback

Crawl log permissions

Article • 07/22/2024

As a SharePoint Administrator or above in Microsoft 365, you can grant users read access to crawl log information for the tenant. The crawl log tracks information about the status of crawled content.

A typical use case is in eDiscovery, where you can grant a security group permission to view the crawl log information for the tenant. The users in the security group can view the crawl log data via the eDiscovery portal to check whether crawled content was successfully added to the search index, or whether indexing failed because of an error. For more information, see Get started with eDiscovery (Standard) in Microsoft Purview and Investigating partially indexed items in eDiscovery.

Grant users permission to view the crawl log information

1. Go to **More features** in the SharePoint admin center, and sign in with an account that has admin permissions for your organization.

> **Note**
>
> If you have Office 365 operated by 21Vianet (China), sign in to the Microsoft 365 admin center, then browse to the SharePoint admin center and open the More features page.

2. Under **Search**, select **Open**.
3. On the **search administration** page, select **Crawl Log Permissions**.
4. In the **Crawl Log Permissions** box, enter names or email addresses. The names of valid users or user groups appear in the list as you enter letters in the box.
5. Select **OK**.

Feedback

Was this page helpful? Yes No

Provide product feedback

Manage query client types

Article • 02/21/2023

APPLIES TO: ✓ 2013 ✓ 2016 ✓ 2019 ✓ Subscription Edition ✗ SharePoint in Microsoft 365

Learn how query client types decide in which order queries are performed.

A query client type is how a client performing a query tells the system what type of client it is. For example, a client might tell us it is UI, or an automated query. Query throttling monitors the use of resources and protects the search system. Administrators can use client-type information for throttling, to make sure lower-priority clients like automated queries don't squeeze out higher-priority clients like UI. Query client types are also used for things like logging, reports, and determining relevance.

The client sets the client type as a label in the query. The administrator configures the valid client types (though some are default and mandatory), and the client chooses one for each query.

> **Note**
>
> You can't turn query throttling on or off.

Add a query client type

> **Note**
>
> You can change the name of a client type that has been created for your tenant only.

1. Go to **More features** in the SharePoint admin center, and sign in with an account that has admin permissions for your organization.

> **Note**
>
> If you have Office 365 operated by 21Vianet (China), sign in to the Microsoft 365 admin center, then browse to the SharePoint admin center and open the More features page.

2. Under **Search**, select **Open**.

3. On the search administration page, select **Manage Query Client Types**.

4. To add a client type, select **New Client Type**.

5. On the **Edit a client type** page, in the **Query Client Type** field, for the client type, enter a name.

6. From the **Throttling Tier** list, select either **Top**, **Middle**, or **Bottom**.

> **Note**
>
> Lower priority queries are throttled first. The search system processes queries from top tier to bottom tier.

7. Select **OK**.

Prioritize a client query type

You can use throttling tiers to prioritize query processing. When the resource limit is reached, query throttling kicks in, and the search system processes queries, starting from the top tier, right through to the bottom tier.

1. Go to **More features** in the SharePoint admin center, and sign in with an account that has admin permissions for your organization.

> **Note**
>
> If you have Office 365 operated by 21Vianet (China), sign in to the Microsoft 365 admin center, then browse to the SharePoint admin center and open the More features page.

2. Under **Search**, select **Open**.

3. On the search administration page, select **Manage Query Client Types**.

4. Go to the **Client Type** section, and select the **System Type** that you want to change.

5. From the **Throttling Tier** list, select either **Top**, **Middle**, or **Bottom**.

> **Note**
>
> Lower priority queries are throttled first. The search system processes queries from top tier to bottom tier.

6. Select **OK**.

Feedback

Was this page helpful? Yes No

Provide product feedback

Search limits for SharePoint

Article • 11/18/2024

As an admin who manages SharePoint (for more info, see SharePoint search administration overview), you should also be aware of limits to search. For example, there are limits to the number of entries you can have in a custom search dictionary or the number of rows that are returned as part of a search.

There are two types of limits:

- **Boundary** A number that can't be exceeded.
- **Supported** A recommended number, based on testing that Microsoft has done, that shouldn't be exceeded. If you exceed a supported limit, you might encounter unexpected results or see a significant decrease in performance.

These limits apply to all SharePoint plans.

The following table lists the limits for SharePoint search.

Expand table

Limit	Maximum value	Limit type	Notes
Size of document that can be downloaded by the crawl components	All File Types: 150 MB PDF, PPTX, PPT, DOC, DOCX: 512 MB	Boundary	Crawl processing supports files up to 150 MB for all types, with an extended limit of 512 MB for PDF, PPTX, PPT, DOC, and DOCX formats. For files exceeding these limits, only document metadata is downloaded, while the full content is NOT downloaded and remains unavailable for search.
Parsed content size	2 million characters	Boundary	Search stops parsing an item after it has parsed up to 2 million characters of content from it, including the item's attachments. The actual number of parsed characters can be lower than this limit because search uses a maximum of 30 seconds on parsing a single item and its attachments. When search stops parsing an item, the item is marked as partially processed. Any unparsed content isn't processed and therefore isn't indexed.
Characters processed by the	1,000,000	Boundary	Search breaks content into individual words (tokens). The word breaker produces tokens

Limit	Maximum value	Limit type	Notes
word breaker			from the first 1,000,000 characters of a single item, including the item's attachments. The actual amount of tokens can be lower than this limit because search uses a maximum of 30 seconds on word breaking. Any remaining content isn't processed.
Indexed managed property size	512 KB per managed property that is set to either "searchable" or "queryable"	Boundary	
Retrievable managed property size	64 KB per managed property	Boundary	
Sortable and refinable managed property size	16 KB per managed property	Boundary	
Token size	Variable - the size depends on the word breaker, and the word-breaker is language-dependent.	Boundary	Search can index tokens of any length but the word breaker that is used to produce tokens can limit the token length. Word breakers are language-aware components that break content into single words (tokens).
Unique indexed tokens per managed property	10,000	Boundary	This is the maximum number of unique tokens that can be added to the search index per managed property. If the limit is exceeded, the index contains the first 10,000 tokens from the managed property and the file will be marked as partially processed by setting the IsPartiallyProcessed property to true.
Distinct users or Active Directory / Microsoft Entra security groups having access to an item	10,000	Boundary	When more than 10,000 distinct users or Active Directory / Microsoft Entra security groups have access to an item, the item isn't searchable by any user. Such items will only be returned as part of an eDiscovery query through the Security & Compliance center.

Limit	Maximum value	Limit type	Notes
Number of entries in a custom search dictionary	5,000 terms per tenant	Boundary	This limits the number of terms allowed for inclusions and exclusions dictionaries for query spelling correction and company extraction. You can store more terms than this limit in the term store, but search only uses 5,000 terms per tenant.
Managed property mappings	100 per managed property	Supported	Crawled properties can be mapped to managed properties. Exceeding this limit may decrease crawl speed and query performance.
Values per managed property	1,000	Boundary	A managed property can have multiple values of the same type. This is the maximum number of values per managed multi-valued managed property per document. If this number is exceeded, the remaining values are discarded.
Number of bytes in a multi-valued string property	32 KB	Boundary	If you reach this limit, the multi-valued property is truncated.
Unique contexts used for ranking	15 unique contexts per rank model	Boundary	
Authoritative pages	1 top level and minimal second- and third-level pages per tenant	Supported	Use as few second- and third-level pages as possible while still achieving the desired relevance. If you add additional pages, you may not achieve the desired relevance. Add the key site to the first relevance level. Add more key sites at either second or third relevance levels, one at a time. Evaluate relevance after each addition to ensure that you have achieved the desired relevance effect.
Text length for queries using Keyword Query Language	4 KB (4,096 characters)	Boundary	
Number of rows in a result set	500	Boundary	To display the entire result set, issue more paging queries. For Discovery queries the maximum number of rows in a result set is 10,000.

Limit	Maximum value	Limit type	Notes
User-defined full-text indexes	3	Boundary	
Maximum number of on-premises items indexed in Microsoft 365	20 million items	Threshold	For each 1 TB of storage space your tenant has in Microsoft 365, you can index 1 million items of on-premises content in your tenant's search index in Office 365 with the cloud hybrid search solution. This quota is by default limited upwards to 20 million items. To increase the number of items that can be indexed beyond 20 million items, contact Microsoft Support.

See also

- SharePoint Limit
- SharePoint Service Description
- Overview of the search schema in SharePoint Server 2013
- SharePoint feature availability across Office 365 plans

Feedback

Was this page helpful? Yes No

Provide product feedback

View Popularity Trends and Most Popular Items

To identify usage trends and find out at what times activity is high or low, you can view **Popularity Trends** reports for a site or a site collection. The reports show historical usage information, such as number of views (hits) and unique users per day or month. Popularity Trends for a page or item in a library in a library show how many views the page or item has had recently.

You can also view the most popular items in a library. You'll see which items have the most views, either recently or ever (from the first time the item became available.)

> **Note**
>
> For SharePoint Modern sites, please see View usage data for your SharePoint site.

View Popularity Trends for a site

1. On the site, select **Settings**, and then select **Site settings**. If you don't see **Site settings**, select **Site information**, and then select **View all site settings**.
2. Under **Site Administration**, click **Popularity Trends**.
3. Click **Usage**.
4. Click Open to open the report in Excel.

View Popularity Trends for a site collection

1. On the site, select **Settings**, and then select **Site settings**. If you don't see **Site settings**, select **Site information**, and then select **View all site settings**.
2. Under **Site Collection Administration**, click **Popularity and Search Reports**.
3. Under **Usage Reports**, click **Usage**.
4. Click Open to open the report in Excel.

You can also view other reports for the site collection, see View usage and search reports.

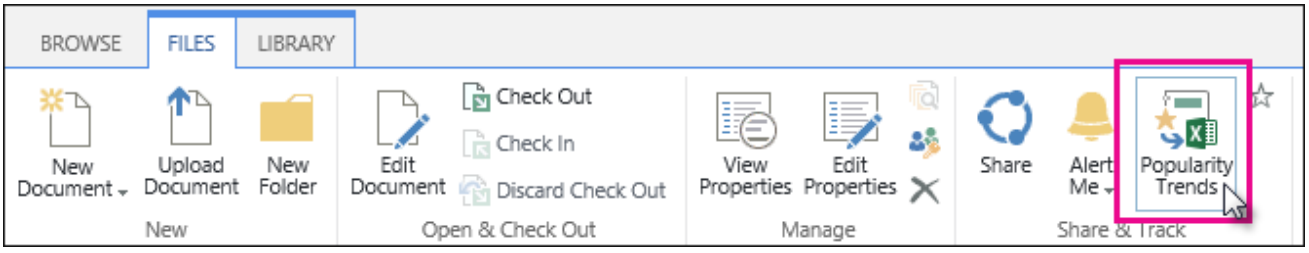
View Popularity Trends for a page or item in a library

1. On your site, navigate to the relevant document library.

2. Select one or more pages or items that you want to look at trends for.

3. Click the **FILES** tab.

4. On the ribbon, click **Popularity Trends**.



5. Click Open to open the **Usage Details** report in Excel. There's one tab in the report for each item you selected.

You can also see popularity trends for a page or item from the **Most Popular Items** view.

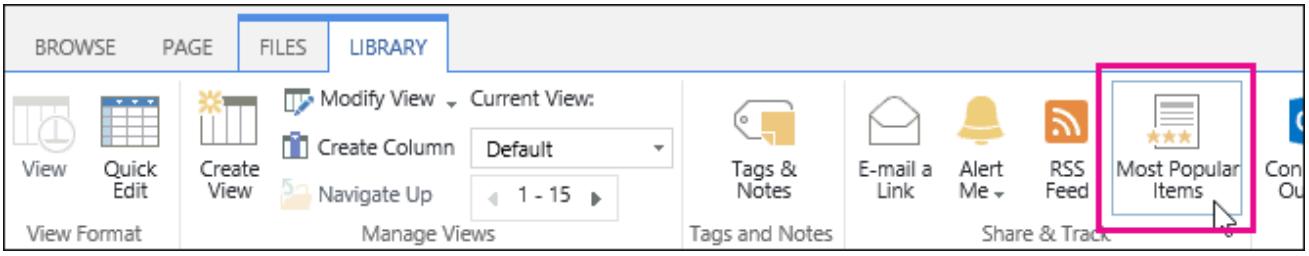
Or, you can go to an individual page and select the **PAGE** tab > **Popularity Trends**.

View the Most Popular Items in a library

1. On your site, go to the relevant document library.

2. Click the **LIBRARY** tab.

3. On the ribbon, click **Most Popular Items**.



You can sort the list by **Recent** (views the last 14 days), or **Ever** (views from the first time the item became available).

To see more details for each item, click the **Popularity Trends** link under each item URL.

View Usage and Search reports for all sites

If you're a SharePoint Administrator or above in Microsoft 365, you can view search usage reports for the whole organization. See View usage and search reports.

Last updated on 06/25/2026

Manage user profiles in the SharePoint admin center

Article • 04/30/2025

This article is for SharePoint Administrators and above in Microsoft 365.

- If you're running SharePoint Server, see Administer the User Profile service in SharePoint Server.
- If you're not an admin, see View and update your profile in Office Delve for info about changing your profile.

Most organizations don't need to change any user profile settings in the SharePoint admin center. For the organizations that do need to work with user profile settings, this article describes the most common tasks.

Create and edit custom user properties

In Microsoft 365, identity is managed by Microsoft Entra ID. For info about this, see Understanding Microsoft 365 identity and Microsoft Entra ID. SharePoint receives this profile information as described in About user profile synchronization. If you need to store additional info about your users, you can create custom properties in the classic SharePoint admin center. For info about doing this, see Add and edit user profile properties in SharePoint.

> **Note**
>
> Instead of creating user sub-types in the SharePoint admin center, we recommend using the Microsoft 365 admin center to Compare groups or using the Microsoft Entra admin center to create groups with dynamic membership.

Add and remove admins for a user's OneDrive

Follow these steps to transfer ownership of a OneDrive to a different user, or give a user full control over another user's OneDrive.

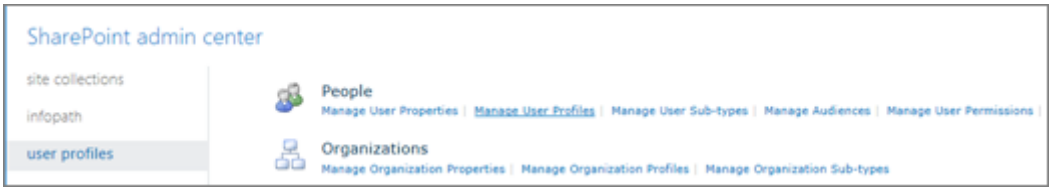
1. Go to **More features** in the SharePoint admin center, and sign in with an account that has admin permissions for your organization.

> **Note**

If you have Office 365 operated by 21Vianet (China), sign in to the Microsoft 365 admin center, then browse to the SharePoint admin center and open the More features page.

2. Under **User profiles**, select **Open**.

3. Under **People**, select **Manage User Profiles**.



4. Enter the user's name and select **Find**.

5. Right-click the user, and then select **Manage site collection owners**.

6. Add and remove admins for the OneDrive, and then select **OK**.

> ⚠ **Warning**
>
> Do not remove a user as the admin of their own OneDrive. Doing this causes many experiences to break.

For info about automatically transferring ownership of OneDrive to a user's manager when the user account is marked for deletion, see Set up access delegation.

Manage audiences (classic experience)

Audiences let you customize content on pages so that it appears only to particular people based on their:

- Membership in a distribution list or security group
- Location in the reporting structure or public info in the user profile

For example, you can display a navigational link to only people in a particular geographic location. For info about using audiences and information about using audience targeting in the modern experience, see Target content to specific audiences.

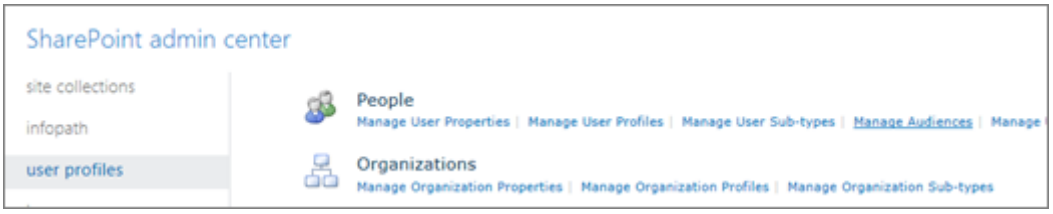
> **Note**
>
> Only sites that use classic templates can be customized based on audience. Audiences are not a security feature. They help you deliver relevant content to specific groups of people, but don't prevent content from being available to anyone with the appropriate permissions.

To add, edit, or delete an audience or an audience rule, go to the Manage Audiences page:

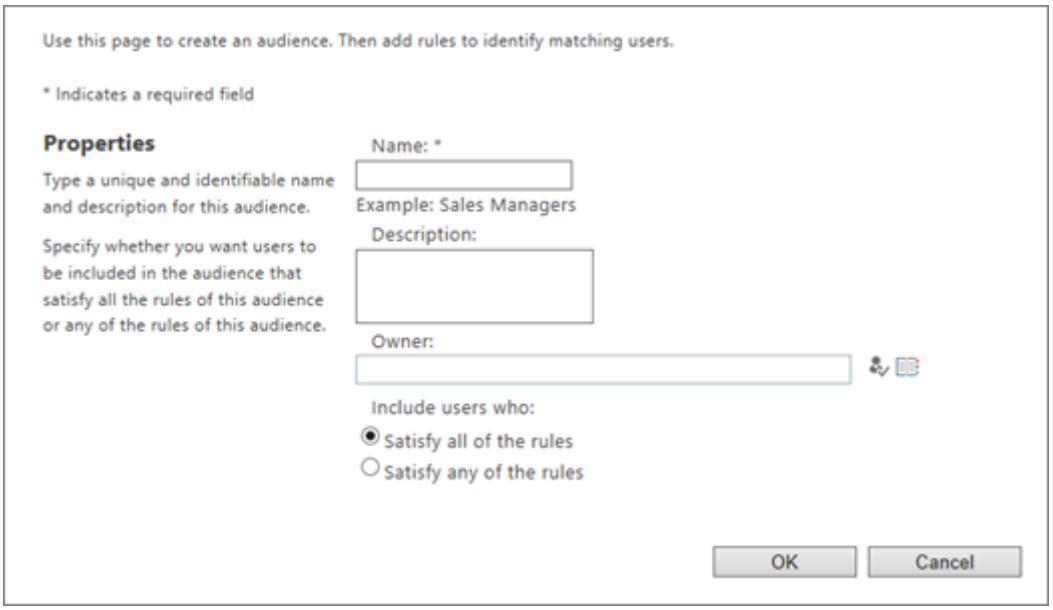
1. Go to **More features** in the SharePoint admin center, and sign in with an account that has admin permissions for your organization.

> **Note**
>
> If you have Office 365 operated by 21Vianet (China), sign in to the Microsoft 365 admin center, then browse to the SharePoint admin center and open the More features page.

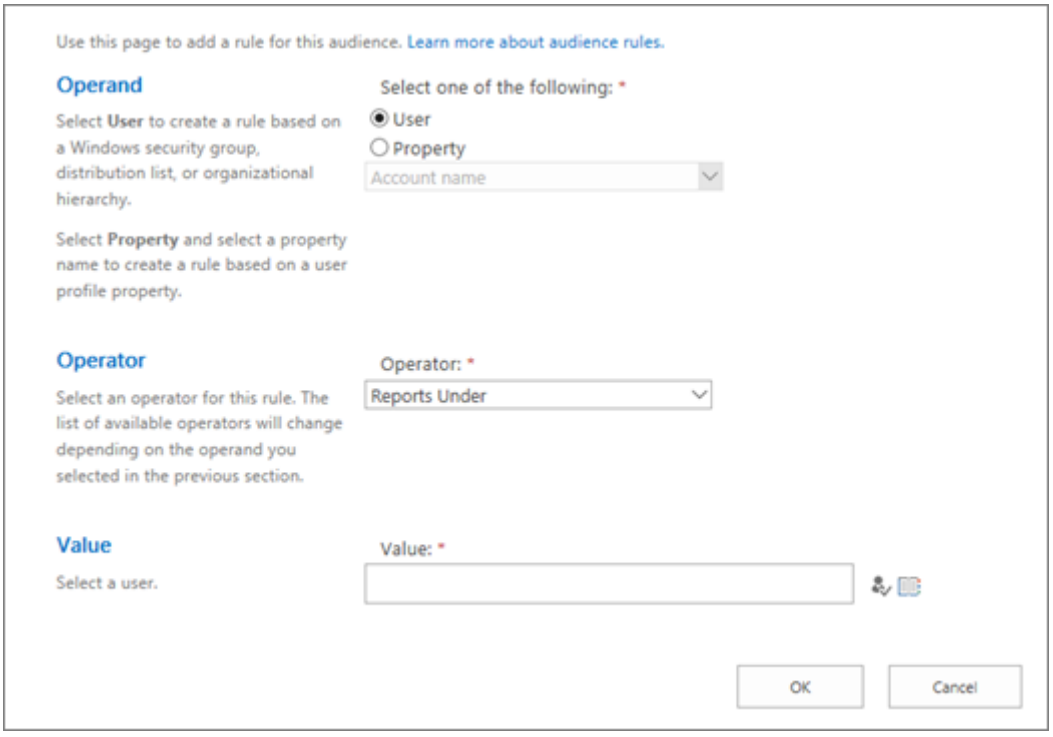
2. Under **User profiles**, select **Open**.
3. Under **People**, select **Manage Audiences**.



Creating a new audience:



Creating a new rule for the audience:



Audiences compile approximately weekly, and you can only view audience members after the audience compiles. The user profiles page shows the number of audiences, the number of uncompiled audiences, and the compilation status and time.

Disable OneDrive creation for some users

If some users are licensed to use OneDrive, but you don't want them to create a OneDrive (perhaps for regulatory reasons), you can prevent them from doing so.

> **Note**

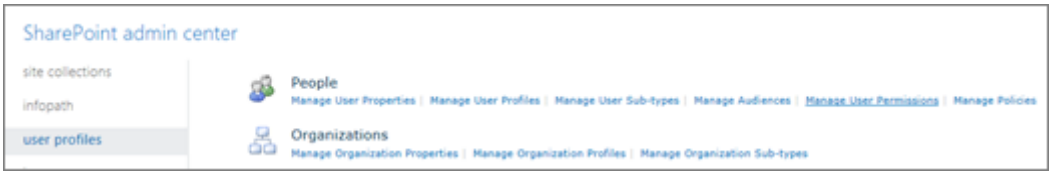
If a user already created a OneDrive, changing the following setting won't delete it.

1. Go to **More features** in the SharePoint admin center, and sign in with an account that has admin permissions for your organization.

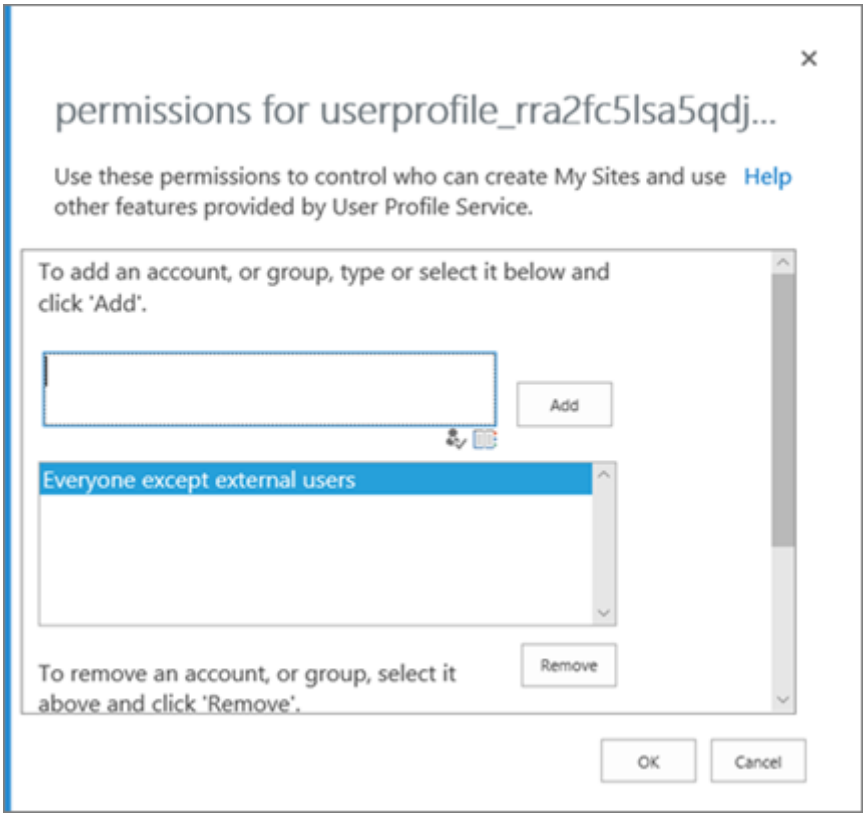
> **Note**
>
> If you have Office 365 operated by 21Vianet (China), sign in to the Microsoft 365 admin center, then browse to the SharePoint admin center and open the More features page.

2. Under **User profiles**, select **Open**.

3. Under **People**, select **Manage User Permissions**.



4. By default, "Everyone except external users" has permission to "Create Personal Site" (which includes creating a OneDrive and saving user data such as followed and frequent sites). Remove that group and add specific groups to allow only a subset of licensed users to create a OneDrive.



5. Select **OK**.

Add and edit user profile properties in SharePoint

Article • 01/16/2025

If your organization uses the cloud identity model, your user accounts are stored in Microsoft Entra ID and you can manage most user profile info in the Microsoft 365 admin center. For info, see Edit or change a user in Microsoft 365. You can also manage user profiles (including adding user pictures and defining user managers) in the Microsoft Entra admin center. For info, see Add or change profile information for a user in Microsoft Entra ID. If you need to create custom user profile properties, such as languages spoken, emergency contact info, or sales account, you can use user properties in SharePoint. Note that these properties are NOT synced back to Microsoft Entra ID.

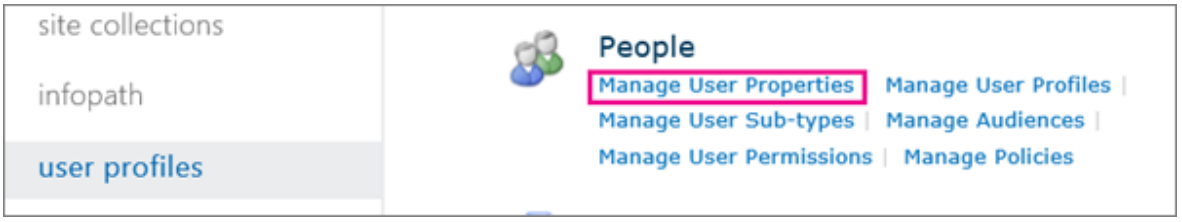
Add a property for a user profile

1. Go to **More features** in the new SharePoint admin center, and sign in with an account that has admin permissions for your organization.

> **Note**
>
> If you have Office 365 operated by 21Vianet (China), sign in to the Microsoft 365 admin center, then browse to the SharePoint admin center and open the More features page.

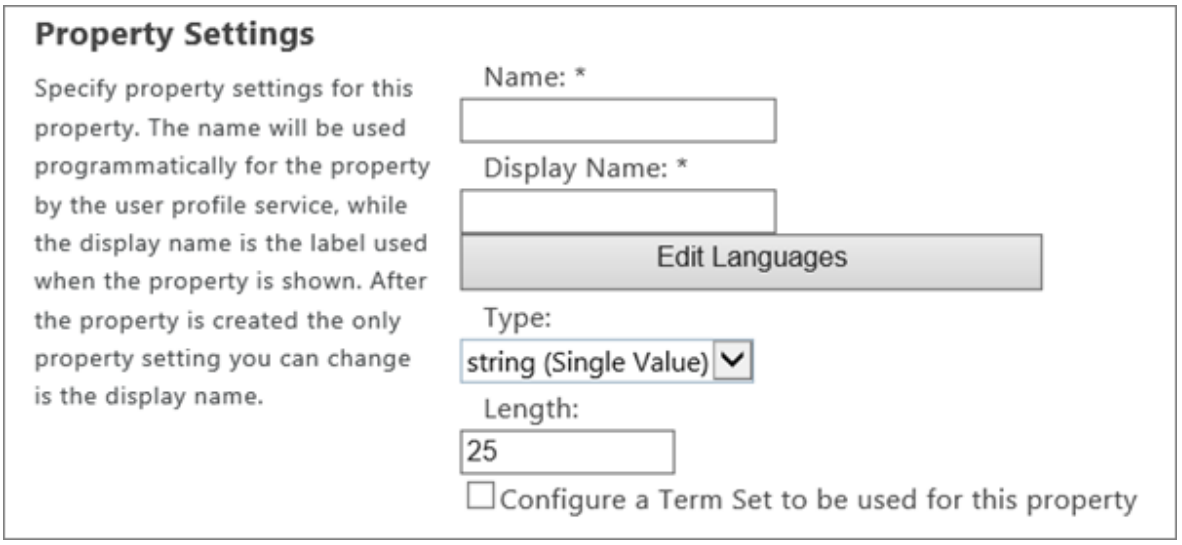
2. Under **User profiles**, select **Open**.

3. Under **People**, select **Manage User Properties**.



4. Select **New Property**.

5. In the **Name** box, enter a unique name for the property.



6. In the **Display Name** box, enter the profile property name that will be displayed to all users. (This name doesn't have to be unique.)

7. In the **Type** list, select the data type for the property.

> ⓘ **Note**
>
> If you select **string (Multi Value)**, the property will be permanently set as a multi-valued property. You can't change this setting after you select **OK**. You can only delete the property and add it again as a new single-value property.

8. If you selected binary, HTML, or string, use the **Length** box to enter the maximum number of characters allowed for property values.

9. If you selected string and want to associate the profile property with a managed metadata term set, select **Configure a Term Set to be used for this property**. Then select a term set from the list.

10. Make sure **Default User Profile Subtype** is selected so the default user profile subtype is associated with this user profile property.

11. In the **Description** box, enter the instructions or information that is displayed to users about this profile property.

12. In the **Policy Settings** section, select the policy setting and default privacy setting that you want for this property. Select the **User can override** box to enable users to override these settings.

13. If you want users to be able to change this profile information for themselves, select **Allow users to edit values for this property**.

14. In the **Display Settings** section, specify whether and how the property will be viewed by users.

15. In the **Search Settings** section, select **Alias** if the property is the equivalent of a user's name. For example, you might do this if you create a property for a "Stage name" and want searches for all documents by John Kane to return the same results as searches for the user's real name. Select the **Indexed** if you want searches to return all the user profiles matching that property. For example, if you have a property for "University," a search for that value would return all alumni from that university.

> **Note**
>
> The **Alias** check box is available only if you set the **Default Privacy Setting** > **Everyone**.

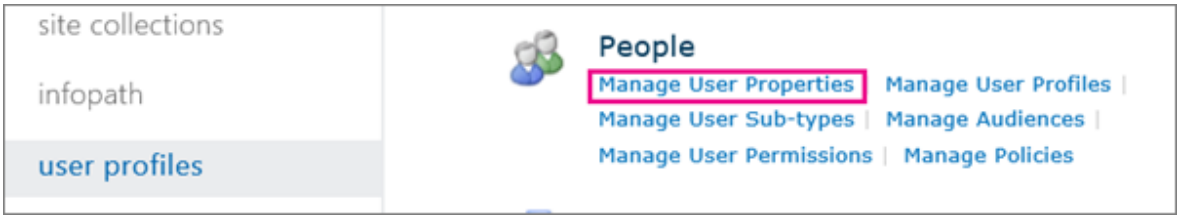
16. Select **OK**.

Edit or delete a property you added

1. Go to **More features** in the new SharePoint admin center, and sign in with an account that has admin permissions for your organization.

> **Note**
>
> If you have Office 365 operated by 21Vianet (China), sign in to the Microsoft 365 admin center, then browse to the SharePoint admin center and open the More features page.

2. Select **User profiles**, and then select **Open**. Under **People**, choose **Manage User Properties**.



3. In the **Property Name** column, select the profile property that you want to change, and then select **Edit** or **Delete**.

4. Edit the elements you want to change.

> **Note**
>
> Some elements of profile properties, such as the **Type** element, are unavailable because they can't be edited. To define these elements, create a new property. The exception is the Source Data Connection property. It's predefined in SharePoint and can't be changed.

5. When you're done, select **OK**.

Synchronize custom properties

Custom properties from Active Directory or Microsoft Entra ID aren't synchronized with SharePoint. For info about bulk updating custom user profile properties by using PowerShell, see Call the import API from PowerShell.

Need more help?

If you have technical questions about this topic, you might find it helpful to post them on the SharePoint discussion forum. It's a great resource for finding others who have worked with similar issues or who have encountered the same situation.

Feedback

Was this page helpful? Yes No

Provide product feedback

User profile synchronization

Article • 01/15/2025

Microsoft SharePoint uses the Active Directory synchronization job to import user and group attribute information into the User Profile Application (UPA). When a new user is added to Microsoft Entra ID, the user account information is sent to the SharePoint directory store and the UPA sync process creates a profile in the User Profile Application based on a predetermined set of attributes. Once the profile has been created, any modifications to these attributes will be synced as part of regularly scheduled sync process.

> **Note**
>
> The profile properties that are synced by the UPA sync process aren't configurable. Synchronization times vary based on workloads.

Sync process

There are four steps in the sync process.

Expand table

Step	Description
1. Active Directory to Microsoft Entra ID	Microsoft Entra Connect syncs data from on-premises Active Directory to Microsoft Entra ID. For more info, see What is hybrid identity with Microsoft Entra ID? and Attributes synchronized.
2. Microsoft Entra ID to SharePoint	Microsoft Entra ID syncs data from Microsoft Entra ID to the SharePoint directory store.
3. SharePoint to UPA	The UPA sync process syncs user account information in SharePoint directory store to the User Profile Application (UPA).
4. UPA to sites	User account information from the UPA is synced to SharePoint sites (previously called "site collections").

Typically, user profiles are created automatically for all accounts that are created in Microsoft 365. For organizations that have a Microsoft 365 Education subscription, user profiles aren't created for new accounts by default. The user must access SharePoint once, at which time a basic stub profile will be created for the user account. The stub profile will be updated with all remaining data as part of the sync process.

If block sign-in is set on the user account in Microsoft Entra ID or disabled accounts are synced from Active Directory on premises, those user accounts won't be processed as part of the UPA sync process. The user must be enabled and licensed for changes to be processed.

Properties that are synced into SharePoint user profiles

The following Microsoft Entra user attributes are synced to the UPA.

Expand table

Microsoft Entra attribute	User profile property display names	Notes	Sync to sites
UserPrincipalName	Account Name User Name User Principal Name	Example: `i:0#.f <|> membership <|>` gherrera@contoso.com gherrera@contoso.com	Yes
DisplayName	Name		Yes
GivenName	FirstName		Yes
sn	LastName		Yes
telephoneNumber	Work phone	Example: (123) 456-7890	Yes
proxyAddresses	Work Email SIP Address	Work Email is set to the value prefixed with SMTP. (SMTP:gherrera@contoso.com) Example: gherrera@contoso.com	Yes
PhysicalDeliveryOfficeName	Office		Yes
Title	Title Job Title	Job Title contains the same value as Title and is connected to a term set.	Yes
Department	Department	Department is connected to a term set.	Yes
WWWHomePage	Public site redirect		No
PreferredLanguage	Language Preferences	Used by SharePoint to determine language for the user when the	Yes

Microsoft Entra attribute	User profile property display names	Notes	Sync to sites
		multilingual user interface (MUI) feature is enabled.	
msExchHideFromAddressList	SPS-HideFromAddressLists		No
Manager	Manager	User Manager for organization hierarchy	Yes

> **Note**
>
> To update more or custom properties, see Bulk update custom user profile properties. Some property names could differ between Azure AD Graph and Microsoft Graph, see Property differences between Azure AD Graph and Microsoft Graph.

Frequently asked questions (FAQs)

How often are changes synced into the User Profile Application?

User account attribute changes are collected in batches and processed for UPA synchronization. Times vary based on the amount of changes requested in a single batch. The UPA synchronization is schedule to run at regular intervals.

Will UPA synchronization overwrite existing properties in SharePoint user profiles?

For the default properties that are synced by UPA synchronization, values are overwritten to align with Microsoft Entra ID.

Does UPA synchronization update only properties that have changed?

UPA synchronization is driven primarily by changes that are made Microsoft Entra ID, including adding new users. A full import can occur under certain maintenance events.

Why isn't it possible to map additional properties for UPA synchronization to sync from Microsoft Entra ID to the User Profile Application?

UPA synchronization is limited to a preconfigured set of properties to guarantee consistent performance across the service.

Feedback

Was this page helpful? Yes No

Provide product feedback

Troubleshoot user profile removal issues in SharePoint

Article • 05/29/2025

This article describes how to remove users so they no longer appear in SharePoint. It should be used to troubleshoot Profile Property synchronization or mismatched ID issues only as advised by Microsoft Customer Support Services.

- **Scenario 1: Someone is deleted from the Microsoft 365 admin center but still appears in SharePoint.**

  When a user or guest browses to a SharePoint site, their user information is cached in the UserInfo list. When the user or guest is deleted, their related UserInfo information isn't removed. Their profile still appears, which may cause confusion when people view the people picker.

- **Scenario 2: Site User ID Mismatch.**

  This issue most frequently occurs when a user is deleted and the account is then re-created with the same user name. The account in the Microsoft 365 admin center or Active Directory (in directory synchronization scenarios) is deleted and re-created with the same user principal name (UPN). The new account is created by using a different ID value. When the user tries to access a site collection or their OneDrive, the user has an incorrect ID. A second scenario involves directory synchronization with an Active Directory organizational unit (OU). If users have already signed in to SharePoint, and then are moved to a different OU and resynced with SharePoint, they may experience this problem.

Delete a user from the Microsoft 365 admin center

For the steps to delete a user in the Microsoft 365 admin center, see Delete a user from your organization.

> **Note**
>
> If you're using directory synchronization, you must remove the user from the on-premises Active Directory environment.

After you delete a user, a series of jobs will remove the user from SharePoint. After the next incremental profile import job, the user (or users) will be marked as deleted, the user's profile

page will be deleted, and the user's OneDrive will be marked for deletion by the MySite cleanup job.

Delete a guest from the Microsoft 365 admin center

1. Sign in to https://admin.microsoft.com as a SharePoint Administrator and above in Microsoft 365. (If you see a message that you don't have permission to access the page, you don't have Microsoft 365 admin permissions in your organization.)

   > **Note**
   >
   > If you have Office 365 operated by 21Vianet (China), sign in at https://login.partner.microsoftonline.cn/. Then select the Admin tile to open the admin center.

2. In the left pane, select **Users** > **Guest users**.

3. Select the user, then select **Delete a user**.

Delete a guest user using Microsoft Graph PowerShell

1. **Install Microsoft Graph PowerShell Module:**

   - Open PowerShell with elevated permissions (right-click on your Start menu or press Windows key + X).
   - Type the following command and press Enter:

     PowerShell

     ```
     Install-Module -Name Microsoft.Graph
     ```

   - When prompted, type "Y" to install the NuGet provider.

2. **Connect to Microsoft Graph:**

   - Now that the Microsoft Graph module is installed, connect to Microsoft Graph using the following command:

```
PowerShell
Connect-MgGraph -Scopes "User.ReadWrite.All", "Group.ReadWrite.All"
```

- Enter your admin credentials when prompted.

3. **Get the Guest User's UPN/Object ID:**

   - Once connected, run the following command to get a list of all user accounts in your tenant:

```
PowerShell
Get-MgUser -All | Format-List  ID, DisplayName, Mail, UserPrincipalName
```

   - Note down the UPN or Object ID of the guest user you want to remove.

4. **Remove the Guest User:**

   - Run the following command to remove the specified guest user (replace `TestUser@example.com` with the actual UPN or Object ID):

```
PowerShell
Remove-MgUser -UserId
"TestUser@contoso.com#EXT#@contoso.onmicrosoft.com"
```

   - This command will permanently remove the user from Azure AD.

Remove people from the UserInfo list

The preceding steps removed access to Microsoft 365 and SharePoint. However, the user or guest still appears in people searches and in the SharePoint Online Management Shell when you use the Get-SPOUser cmdlet. To completely remove people from SharePoint, you must remove them from the UserInfo list. There are two ways to do this:

Browsing site by site in SharePoint

You have to browse to each site collection that the user or guest visited, and then follow these steps:

> ⓘ **Note**

This option is available only if the user previously browsed to the site collection. They won't be listed if they were granted access but never visited the site.

1. Browse to the site and edit the URL by adding the following string to the end of it: **/_layouts/15/people.aspx?MembershipGroupId=0**

   For example, the full URL resembles the following: `https://fabrikam.sharepoint.com/_layouts/15/people.aspx?membershipGroupId=0`.

2. Select the person from the list, and then on the **Actions** menu, select **Delete Users from Site Collection**.

Using the SharePoint Online Management Shell

1. Install the SharePoint Online Management Shell.

2. Connect to SharePoint as a SharePoint Administrator or above in Microsoft 365. To learn how, see Getting started with SharePoint Online Management Shell.

3. Run the following command for each site collection that the user or guest visited:

   PowerShell

   ```
   Remove-SPOUser -Site https://fabrikam.sharepoint.com/sites/sc1 -LoginName
   jondoe@fabrikam.com
   ```

   > **Note**
   >
   > Replace the *jondoe@fabrikam.com* placeholder with the person in question.

Clear browser history

SharePoint uses browser caching in several scenarios, including in the people picker. Even when a user is fully removed, he or she may still remain in the browser cache. Clearing the browser history resolves this issue. For info about doing this in Microsoft Edge, see View and delete browser history in Microsoft Edge.

When you clear the browser history, make sure that you also select to clear cookies and website data.

Business Connectivity Services (BCS) retirement in Microsoft 365

Article • 10/05/2023

SharePoint has a long history of helping users work with external data inside the SharePoint user experience, starting with the Business Data Catalog feature in SharePoint Server 2007. As SharePoint has evolved into a cloud-first service, so too have the options to integrate with external data sources. To simplify these options and provide the best experience for these scenarios going forward, Microsoft is announcing its plan to retire Business Connectivity Services (BCS) in Microsoft 365 and focus on Microsoft Power Apps as its replacement technology.

Impacted features and scenarios

All Business Connectivity Services features will be retired in SharePoint in Microsoft 365. This includes features such as:

- External lists
- External columns
- External content types
- Business Connectivity Services hybrid solutions

Recommended replacement technology: Microsoft Power Apps

We encourage you to explore using Power Apps to replace their Business Connectivity Services solutions in SharePoint in Microsoft 365. Although there's no direct migration from Business Connectivity Services to Power Apps, it supports a modern, cloud-first external data connectivity experience. Power Apps can integrate with various Microsoft 365 services and external data sources through its extensible connector technology, including SharePoint, Dynamics 365, SQL Server, and others. It also supports integrating with on-premises data sources through the on-premises data gateway.

To learn more about Power Apps, see the links in the More information section.

Retirement schedule

- October 2, 2023: Retirement announcement and you can proactively set a property to block Business Connectivity Services features within their tenant.
- October 30, 2023: Microsoft will begin blocking Business Connectivity Services features based on the tenant property you set.
- January 8, 2024: Microsoft will block Business Connectivity Services features in new Microsoft 365 tenants by default, and in tenants who haven't used the feature since October 30, 2023.
- September 30, 2024: Business Connectivity Services is fully retired in Microsoft 365.

Blocking Business Connectivity Services features within your tenant

You can prepare for the Business Connectivity Services retirement by setting a property that will block this feature in their tenant. This will ensure that users within your tenant won't start using this feature if it isn't already in use.

You should only set this property once you've confirmed there's no business need to use the Business Connectivity Services features. You can confirm Business Connectivity Services usage by following these instructions:

1. Go to **More features** in the SharePoint admin center, and sign in with an account that has admin permissions for your organization.

   > **Note**
   >
   > If you have Microsoft 365 operated by 21Vianet (China), sign in to the Microsoft 365 admin center, then browse to the SharePoint admin center and open the **More features** page.

2. Under **BCS**, select **Open**.

3. On the **BCS Home Page**, select **Manage BDC Models and External Content Types**.

4. In the **View** dropdown selector, select each of views including **BDC Models**, **External Systems**, and **External Content Types**. Confirm that no BDC models, external systems, or external content types have been added.

5. Return to the **BCS Home Page** and select **Manage connections to online services**.

6. Confirm that no connections have been added.

7. Return to the **BCS Home Page** and select **Manage connections to on-premises services**.

8. Confirm that no connections have been added.

To proceed with setting the property that will block this feature, tenant administrators can download and launch SharePoint Online Management Shell version 16.0.24120.12000 or higher and then run the following commands:

PowerShell

```
Connect-SPOService -Url https://<tenant>-admin.sharepoint.com
Set-SPOTenant -BusinessConnectivityServiceDisabled $true
```

SharePoint in Microsoft 365 will begin blocking features based on this tenant property on October 30, 2023.

Blocking Business Connectivity Services in new tenants by default

Starting January 8, 2024, Microsoft will block Business Connectivity Services in new tenants by default by automatically setting this property to true in those new tenants. In addition, Microsoft will also set this property to true on existing tenants who haven't used the Business Connectivity Services feature since October 30, 2023.

If you want to re-enable Business Connectivity Services, you can do so by setting this property to false as follows:

PowerShell

```
Connect-SPOService -Url https://<tenant>-admin.sharepoint.com
Set-SPOTenant -BusinessConnectivityServiceDisabled $false
```

Note that re-enabling Business Connectivity Services in your tenant isn't recommended unless you have a specific need.

Business Connectivity Services is retired in Microsoft 365

Starting September 30, 2024, Business Connectivity Services will be retired in Microsoft 365. Its features will no longer be available and can't be re-enabled through the `Set-SPOTenant` PowerShell cmdlet. This applies to all environments including Government Clouds and Department of Defense.

Impact to SharePoint Server

This announcement has no impact on Business Connectivity Services in SharePoint Server.

This feature will remain supported in SharePoint Server 2016 and SharePoint Server 2019 until those products reach their end of support date of July 14, 2026.

Microsoft has no plans to retire Business Connectivity Services in SharePoint Server Subscription Edition at this time. Deprecation and removal announcements for SharePoint Server Subscription Edition are announced in the What's deprecated or removed from SharePoint Server Subscription Edition article.

More information about Power Apps

For more information about Power Apps and its integration capabilities with external data sources, see:

What is Power Apps?

What is an on-premises data gateway?

Scenarios for integrating SharePoint with Power Apps

Overview of connectors for canvas apps

Related topics

BCS retirement announcement on Tech Community

Feedback

Was this page helpful? Yes No

Provide product feedback

Secure Store Service (SSS) retirement in Microsoft 365

Article • 04/08/2025

SharePoint has a long history of helping users securely work with external data inside the SharePoint user experience, starting with the Business Data Catalog feature in SharePoint Server 2007. SharePoint has been evolving into a cloud-first service and along with it the options for managing credentials and secrets for external data access have also evolved. To simplify these options and provide the best experience for these scenarios going forward, Microsoft is announcing its plan to retire Secure Store Service (SSS) in Microsoft 365 and focus on Azure Key Vault as its replacement technology.

This announcement follows the discontinuation of Business Connectivity Services (BCS), which was the primary use case for Secure Store Service.

Impact on SharePoint Server

This announcement has no immediate impact on Secure Store Service in SharePoint Server 2016, 2019, and Subscription Edition.

Until SharePoint Server 2016 and SharePoint Server 2019 reach their end of support date of July 14, 2026, SSS will be supported. For SharePoint Server Subscription Edition, there are no current and immediate plans to retire SSS. For any deprecation or feature support removal announcements, see What's deprecated or removed from SharePoint Server Subscription Edition

Impacted features and scenarios

All Secure Store Service features will be retired in SharePoint in Microsoft 365. This includes features such as:

- Secure Store Target Applications
- Credential storage
- Mapping for external data sources

Retirement schedule

Expand table

Date	Milestone
April 10, 2025	Retirement is announced and transition period begins.
May 31, 2025	Adding new Target Applications or credentials in Secure Store Service is restricted.
September 30, 2025	Secure Store Service is fully retired in Microsoft 365.

Automatic retirement

Microsoft will manage the retirement process automatically. Administrators don't need to take any manual steps to disable Secure Store Service. Once retired, the service will no longer be available, and any existing configurations will be removed.

Recommended replacement technology: Azure Key Vault

We encourage you to explore using Azure Key Vault to replace Secure Store Service solutions in SharePoint in Microsoft 365. Although there's no direct migration from Secure Store Service to Azure Key Vault, it supports a modern, cloud-first credential and secret management experience. Azure Key Vault can integrate with various Microsoft 365 services and external data sources through its secure and scalable architecture.

To learn more about Azure Key Vault, see the links in the More information section.

More Information about Azure Key Vault

For more information about Azure Key Vault and its capabilities, see:

- Azure Key Vault (AKV) Documentation

Manage Business Connectivity Service Applications

Article • 02/21/2023

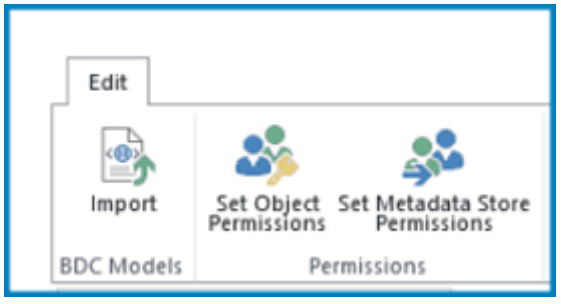
In SharePoint in Microsoft 365, you can create Business Connectivity Services (BCS) connections to data sources, such as SQL Azure databases or Windows Communication Foundation (WCF) web services, that are outside the SharePoint site. Once you've created these connections, you can manage or edit BCS information in the SharePoint admin center. Microsoft SharePoint uses BCS together with Secure Store Services to access and retrieve data such as BDC Models from external data systems. See also Deploy a Business Connectivity Services hybrid solution in SharePoint.

> **Note**
>
> Business Connectivity Services (BCS) in Microsoft 365 is a deprecated feature. On January 8, 2024, it will be disabled in new tenants as well as existing tenants that haven't used the feature since October 30, 2023. It will be retired and removed from all tenants on September 30, 2024. Customers are encouraged to explore using Microsoft Power Apps to replace their Business Connectivity Services solutions in Microsoft 365.
>
> For more information, see Business Connectivity Services (BCS) Retirement in Microsoft 365.

Manage BCS permissions

After setup is complete, user permissions control access to the data that the connection provides. BCS has two types of permissions:

- Object permissions
- Metadata Store permissions



Object permissions

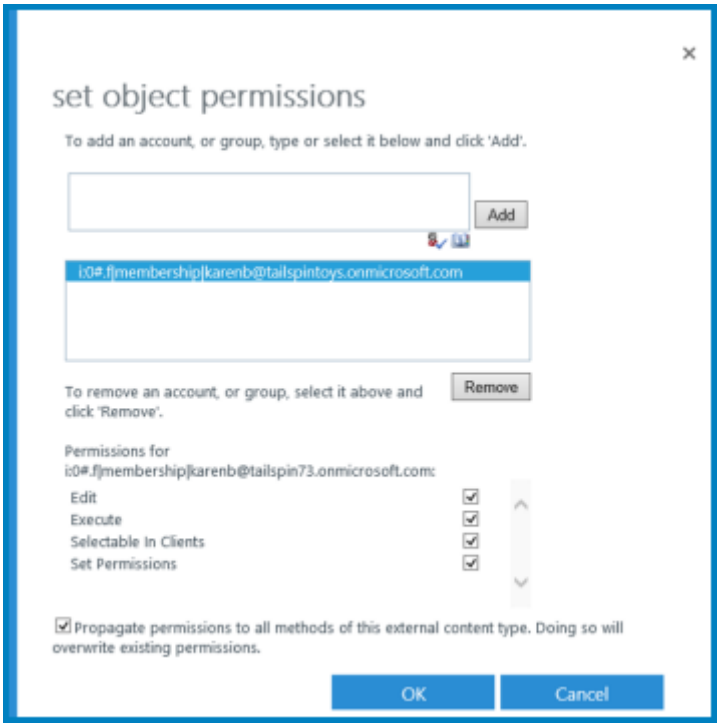
Object permissions apply only to a specific External System, BDC Model, or External Content Type (ECT). Each ECT is a securable object. For example, if you have an ECT called WCFBookSales, object permissions apply only to the WCFBookSales object, and not to any other ECT that might be defined.

To set object permissions for an object, follow these steps.

1. Go to **More features** in the SharePoint admin center, and sign in with an account that has admin permissions for your organization.

> **Note**
>
> If you have Office 365 operated by 21Vianet (China), sign in to the Microsoft 365 admin center, then browse to the SharePoint admin center and open the More features page.

2. Under **BCS**, select **Open**.
3. In the **business data catalog** section, select **Manage BDC Models and External Content Types**.
4. Select the check box next to the name of the ECT or external system that you want to manage.
5. On the ribbon, select **Set Object Permissions**.



6. Enter a user account or group name in the text box, and then select **Add**. You can also select **Browse** to look for the name that you want.

7. Select the name of the account or group for which you want to set access to the ECT or external system. You can set permissions for only one account at a time. If you have multiple accounts or groups, you have to set levels of access for each account separately, by selecting them one at a time.

   The following table describes the permissions and their associated access levels.

Expand table

Permission	Notes
Edit	Allows the user or group to create External Systems and BDC Models, to import BDC Models, and to Export BDC Models. This setting should be reserved for highly privileged users.
Execute	Allows the user or group to execute operations (create, read, update, delete, or query) on ECTs.
Selectable in clients	Allows the user or group to create external lists for any ECTs, and to view the ECTs in the external item picker.
Set permissions	Allows the user, group, or claim to set permissions on the Metadata Store. At least one user or group must have this permission on every BCS connection so that permissions management can occur. With this permission, a user can grant **Edit** permissions to the Metadata Store. This setting should be reserved for highly privileged users

Metadata Store Permissions

Metadata Store permissions apply globally to the whole BCS store. That is, they apply to all BDC Models, external systems, ECTs, methods, and methods instances that are defined for that external data system. You can set permissions on the metadata store to determine who can edit items and set permissions for the store.

Metadata Store permissions apply to many objects, such as BDC Models, ECTs, and external systems. Because Metadata Store permissions can replace object permissions, they must be managed carefully. When applied with forethought, Metadata Store permissions can grant access quickly and completely.

To set Metadata Store permissions, follow these steps.

1. In the left pane of the new SharePoint admin center, select More features.
2. Under **BCS**, select **Open**.
3. Select **Manage BDC Models and External Content Types**.
4. On the ribbon, select **Set Metadata Store Permissions**.
5. Enter a user account or group into the text box, and then select **Add**. You can also select **Browse** to look for the account that you want.
6. The account or group will appear in the second text box. If you have multiple accounts or groups, you must select them one at a time to set the level of access.

Expand table

Permission	Notes
Edit	Allows the user or group to create External Systems and BDC Models, to import BDC Models, and to export BDC Models. This setting should be reserved for highly privileged users.
Execute	Allows the user or group to execute operations (create, read, update, delete, or query) on ECTs.
Selectable in clients	Allow the user or group to create external lists for any ECTs, and to view the ECTs in the external item picker.
Set Permissions	Allows the user, group, or claim to set permissions on the Metadata Store. At least one user or group must have this permission on every BCS connection so that permissions management can occur.

Permission	Notes
	With this permission, a user can grant Edit permissions to the Metadata Store. This setting should be reserved for highly privileged users.

7. To propagate permissions to all items in the Metadata Store, select **Propagate permissions to all BDC Models, External Systems and External content types in the BDC Metadata Store**. If you select this option, you'll replace all existing permissions (including object permissions) that you may have set anywhere else in your selected BCS Application.

Import or export a Business Data Connectivity (BDC) Model

The BDC Model view allows a user to import and export the underlying framework for the business data connection. This is very useful if you have to re-create the connection in a new environment. A BDC Model file can be imported to create an ECT connection to an external system.

You can import or export two types of model files:

Model Exports the XML metadata for a selected system.

Resource Exports the localized names, properties, and permissions for a selected system.

> ⓘ **Note**
>
> You can create a BDC Model using XML code. If you do so, it's important to know that you cannot use the authentication modes **RevertToSelf** and **PassThrough** with SharePoint. Although you might be able to import a BDC Model that was written in XML, the connection will not be usable.

Import a BDC Model

When you import a BDC Model, you also import its specified permissions. Before you import a BDC Model, it's a good idea to understand how imported permissions interact with existing permissions.

Imported permissions for a BDC Model are added to the store of existing permissions in the BDC service. If an entry for an object already exists in the access control list, the

existing value is overwritten with the permissions information from the imported file.

To import a BDC Model, follow these steps:

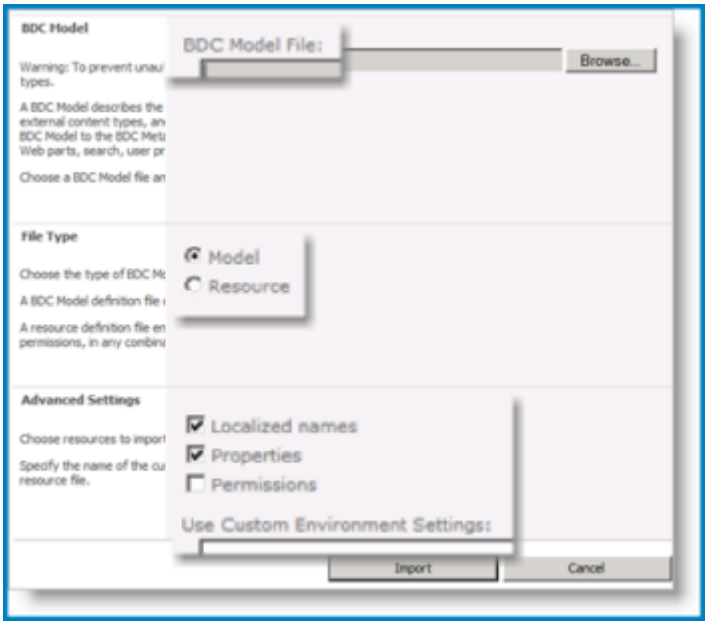
1. In the left pane of the new SharePoint admin center, select **More features**.

2. Under **BCS**, select **Open**.

3. In the business connectivity services section, select **Manage BDC Models and External Content Types**.

4. On the ribbon, select **Import**.

5. In the **BDC Model** section, enter the name of the BDC Model File. The Model name must not include any special characters, such as ~ " # % & * : < > ? \ { | } or the character 0x7f. You can also select **Browse** to locate the *.bdcm file for a BDC Model.



6. In the **File Type** section, select **Model** or **Resource** as the file type that you want to import.

7. In the **Advanced Settings** section, select one or more of the following resources to import:

8. **Localized names** to import localized names for the ECTs in a particular locale. Imported localized names are merged with the existing localized names by Business Data Connectivity.

9. **Properties** to import properties for ECTs. Imported properties are merged with the existing property descriptions by Business Data Connectivity.

10. **Permissions** to import permissions for ECTs and other securable objects in the model.

11. (Optional) To save the resource settings in a file for later use, type a name for the resource file in the **Use Custom Environment Settings** text box.

12. Select **Import**.

Export a BDC Model

You can export a BDC Model and then read its contents to determine differences between connections. This can be useful if you are troubleshooting. You can also import an exported BDC Model file into another environment for testing or reuse.

To export a BDC Model or Resource file, follow these steps:

1. In the left pane of the new SharePoint admin center, select **More features**.

2. Under **BCS**, select **Open**.

3. Select **Manage BDC Models and External Content Types**.

4. Select the dropdown, and in the **View** group, select **BDC Model**.

5. Select the name of the BDC Model that you want to export, on the ribbon, select **Export**.

6. On the Business Data Connectivity Models page, select the model or resource file to export.

7. On the Export page, in the **File Type** section, to specify the type of file that you want to export, select **Model** or **Resource**.

8. In the **Advanced Settings** section, to further refine the data export, select one or more of the following:

- To export localized names for the ECTs in a particular locale, select**Localized names**.

- To export properties for ECTs, select **Properties**.

- To export permissions for ECTs, select **Permissions**.

- To export an implementation-specific proxy that is used to connect to the external system, select **Proxies**. .

9. If you saved a file of resource settings for later use, enter the name of the file to export in the **Use Custom Environment Settings** field.

10. Select **Export** to start a dialog that enables you to save a *.bdcm file to your local drive. You can open the *.bdcm file in a text editor.

Add actions to external content types

By adding actions to ECTs, administrators associate a uniform resource locator (URL) with an ECT. This automatically starts a specified program or opens a specified web page.

Actions can specify parameters that are based on one or more fields in an ECT. For example, you can create an action for an ECT that specifies a Search page URL. The parameter for this action might be the ID of an item in the external data source. This would allow you to specify a custom action for the ECT that automates search for this item.

> **Note**
>
> When you add a new action to an ECT, that action is not added to existing external lists for that ECT. The action is only available in new external lists for the ECT.

To add an action to an ECT, follow these steps.

1. In the left pane of the new SharePoint admin center, select **More features**.

2. Under **BCS**, select **Open**.

3. Select **Manage BDC Models and External Content Types**.

4. Point to the name of the ECT to which you want to add an action, and then select the arrow that appears. From the menu, to open the **Add Action** page, select **Add Action**.

5. In the **Name** field, give the action a meaningful name.

6. In the URL field, for the action you want to open, enter the URL.

   > **Note**
   >
   > Under the control, you can find an example URL. The example shows how to add one (or more) parameter place-holders such as {0}, or {1}

```
(http://www.adventure-works.com/sample.aspx?p0={0}&amp;p1={1} ).
```

7. If you want web parts on the site to be able to use this new action, select one of the following options:

Expand table

Command	Action
Yes	Starts the action in a new browser window (preserves the page context).
No	Starts the action in the same browser window.

8. In the **URL Parameters** field, specify any parameters that are required by the URL. These are numbered in the interface starting at 0.

9. Decide if you want to use an **Icon** or not. This field also allows you to use Standard icons.

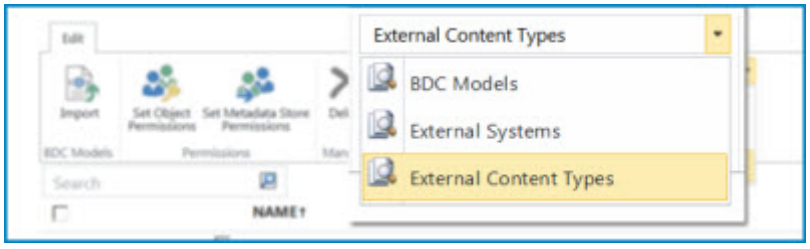
10. If you want the action to be the default action, select the **Default Action** check box.

> **Important**
>
> Parameters can contain personally identifying information such as names and Social Security numbers. When you design an action, be careful not to use fields that display personally identifying information.

View external data and external data settings

You use the **View** section of the ribbon to choose different views of BCS connections. The three views display information about the BCS connection in different ways, and give you access to different actions. It is important to become familiar with these views because some tasks are available only in specific views.

The three view options are BDC Models, External Systems, and External Content Types, as shown in the following illustration.

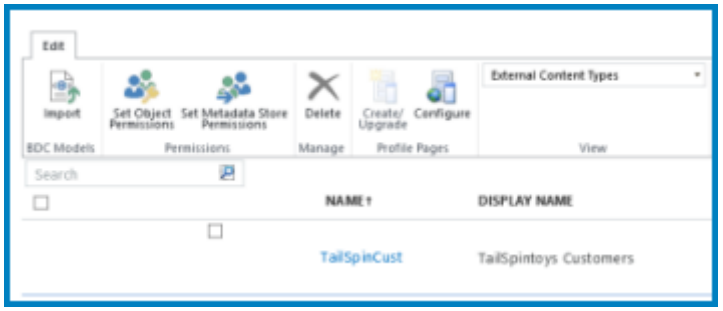


For more information about how you can use these views to help manage BCS, see the sections that follow.

External Content Types view

By default, the BCS connection uses the **External Content Types** view. This view shows Service Application Information, and lists the following information:

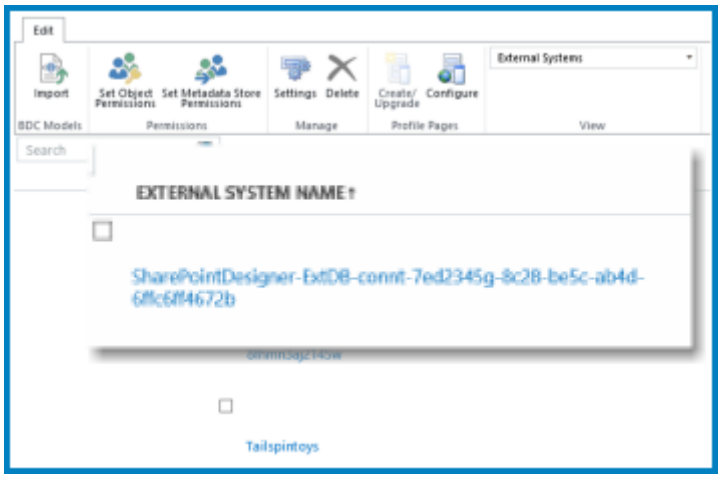
- ECT name
- ECT display name
- ECT type namespace
- Namespace version
- External system name



For most processes in BCS, this view is sufficient. However, if there are many ECTs, this view can be difficult to navigate.

External Systems view

The **External Systems** view shows a BCS connection in terms of its system of origin. This view is useful if you want to know the BCS connection information after you create the BCS. In this view, you can see the property settings for a named External System. In addition, you can configure some of the property settings.



View property settings

The name of the External System appears on this page as a selectable link (a navigable URL). You can select the URL to open a window that shows the original property settings for that store. In addition, if you are connected to SQL Azure, you can see the database server name and database, in this view.

Depending on the type of BCS connection, the property settings can include any combination of the following items:

- Access Provider (such as WCF Service)
- Authentication Mode (such as User's Identity)
- Database Server
- Impersonation Level (such as None, Anonymous, Identification, Impersonation, Delegation)
- Initial Database name
- Integrated Security (such as SSPI)
- Secure Store Implementation
- Secure Store Target Application ID (as the ID entered in Secure Store)
- Service EndPoint Address (such as the URL pointing to SomeWCFService.svc)
- Connection Pooling (Active/Inactive)
- Secondary Secure Store Target Application ID
- Secure Store Implementation

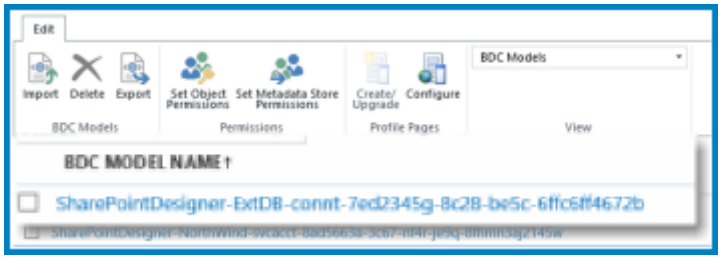
Configure property settings

If you point to an External System Name, you can open a shortcut menu that includes a **Settings** command. This is useful for SharePoint connections that use Windows Communication Foundation (WCF) Web Services. By selecting the **Settings** option from the menu, you can configure any of the following settings:

- Metadata Exchange URL
- Metadata Exchange Discovery Mode
- Web Services Description Language (WDSL) Authentication Mode
- WSDL Secure Store Target Application Id
- Secure Store Implementation.

BDC Model view

The **BDC Model** view offers ribbon commands that enable you to import or export BDC Models. In addition, the BDC Model view can make it easier to move around in a very large collection of ECTs. Because the BDC Model shows hyperlinks for each distinct connection, rather than showing all ECTs for each connection, it can make a more manageable list.



If you want to see all the ECTs for a BDC Model, select the name of the Model. If you select the name of an ECT, open a table that shows the fields that are defined for the ECT. It resembles the following table.

Expand table

Name	Type	Display by Default
Order Id	System.String	No
Employee Id	System.String	No
Freight	System.Nullable '1[[System.Decimal, ...	No

This display can closely mirror the layout of the data source connected via an ECT, and give better insight into the structure of the underlying data.

Also, at the bottom of the page, any Associations, Actions, or Filters for this ECT appear.

Feedback

Was this page helpful? Yes No

Provide product feedback

Create or edit a Secure Store Target Application

Article • 02/21/2023

When you want to use external data (such as data from your other business applications or partner resources) in SharePoint, you can use Business Connectivity Services (BCS) together with Secure Store. And, you can manage BCS and Secure Store right in the SharePoint admin center. The external data source that you can connect to is called a Secure Store Target Application, or just a Target Application.

BCS makes it possible for you to set up a connection to the Target Application, and the Secure Store enables you to manage the credentials that are required by the external data source.

> **Note**
>
> To access the Secure Store, you must have at least the SharePoint Administrator role.

How the Secure Store Service Works

This SharePoint service makes access to external business application data easier. In order to understand why the Secure Store Service offers this benefit, it's important to understand that the username and password used to access external data stores may not be the same as the username and password used to access SharePoint. When a user accesses a SharePoint page that displays information from an external data system, SharePoint must make a separate request to retrieve information from the external data system. This must be made with credentials that are known to the external data system in order for the request for content to be successful. Only then can SharePoint display the information from the external data system on the page. The Secure Store Service stores the external data system credentials for this reason.

The Secure Store Service is designed to create a background mapping between a group of users in SharePoint, and a single user known to the external data system. When the Secure Store Service is properly configured, the following occurs:

- A user authenticates through Internet Information Services (the web server technology underlying SharePoint technologies) to SharePoint via valid credentials.

- Inside SharePoint, the Secure Store Service uses mapped credentials known to the external business application to render any necessary external data on the site for the authenticated user.

Another benefit of the Secure Store Service is that it eliminates authentication prompts for users. When users navigate to SharePoint pages that access external data systems, the Secure Store Service is active in the background, checking user rights and providing mapped credentials to the external data when appropriate. This allows users to access the required data without prompting them to enter usernames and passwords specific to the external application.

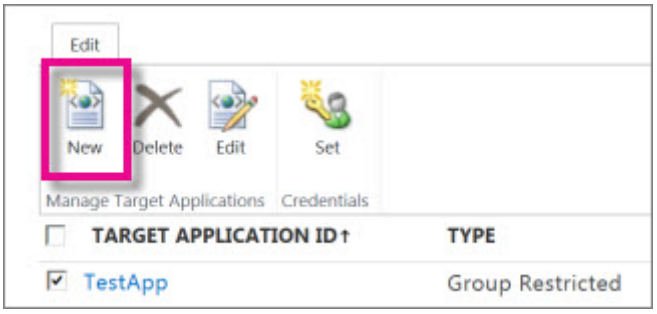
Create a Target Application

1. Go to **More features** in the SharePoint admin center, and sign in with an account that has admin permissions for your organization.

> **Note**
>
> If you have Office 365 operated by 21Vianet (China), sign in to the Microsoft 365 admin center, then browse to the SharePoint admin center and open the More features page.

2. Under **Secure store**, select **Open**.

3. In the **Manage Target Applications** group on the ribbon, select **New**.



4. In the **Target Application Settings** section, enter values for the following fields:

5. **Target Application ID**. You might find it useful to assign a meaningful name. For example, if you are connecting to source that contains employee data, you might enter EmployeeTargetApp.

6. Display Name. This field should be a user-friendly name for the Target Application. For example, you might use Employee Data.

7. **Contact E-mail** Enter a valid email address for people to use when they have questions.

8. **Target Application Type**. By default, SharePoint uses type **Group Restricted**.

9. In the **Credential Fields** section, for the credentials that are required to access data in the Target Application, enter the **Field Names** and **Field Types**. These fields determine how you will map identity in the Secure Store Service. By default, the Credential Fields list the Windows User Name and Windows Password with matching Field Types (User Name and Password), and specifies that the password is masked.

10. In the **Target Application Administrators** section, enter a list of users, or to search for the name of a group, select **Browse**. This section usually contains the account of the SharePoint Administrator, or a Global Administrator.

11. In the **Members** section, enter a list of users or SharePoint groups of users who need to access the target app. Or, to search for the name of a group that you want to map to the Target Application, select **Browse**.

12. Select **OK** to accept this configuration and return to the Secure Storage Service page. The new Target Application appears on the page.

Edit settings for a Target Application

1. Go to **More features** in the SharePoint admin center, and sign in with an account that has admin permissions for your organization.

> **Note**
>
> If you have Office 365 operated by 21Vianet (China), sign in to the Microsoft 365 admin center, then browse to the SharePoint admin center and open the More features page.

2. Under **Secure store**, select **Open**.

3. From the list of Target Applications, select an existing Target Application.

4. On the ribbon, select **Edit**.

> **Note**

Some fields on the Edit page are not available. These elements cannot be edited. After you create a Target Application, you can't change the **Target Application ID**, **Target Application Type**, or **Credentials Fields**.

5. Select any of the following to edit the contents:

- Display Name
- Contact E-mail
- Target Application Administrators
- Members

6. Select **OK**.

Set credentials for a Target Application

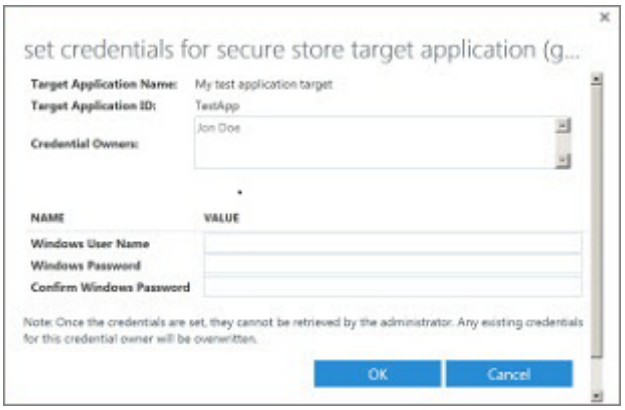
1. Go to **More features** in the SharePoint admin center, and sign in with an account that has admin permissions for your organization.

> **Note**
>
> If you have Office 365 operated by 21Vianet (China), sign in to the Microsoft 365 admin center, then browse to the SharePoint admin center and open the More features page.

2. Under **Secure store**, select **Open**.

3. Select a single Target Application from the list if you have created more than one.

4. In the **Credentials** group on the ribbon, select **Set**. This opens the **Set Credentials for Secure Store Target Application (Group)** dialog. When you set credentials, you map a Target Application Group to a single set of credentials for an external data system.



5. In the **Set Credentials for Secure Store Target Application (Group)** dialog, enter the credential values that you want. The credential fields that you enter apply to the external data system.

> **Note**
>
> The following fields cannot be edited. These fields specify the Secure Store mapping for the Target Application: **Target Application Name**, **Target Application ID**, and **Credential Owners**.

> **Important**
>
> Be careful when you enter the password. If you enter a password that is incorrect, you won't see a message about the error. Instead, you'll be able to continue with configuration. However, errors can occur later, when you attempt to access data through BCS. Also, if the password for the external data source is updated, you have to return to this page to manually update the password credentials.

6. When you finish entering values for credential fields, select **OK**.

Feedback

Was this page helpful? Yes No

Provide product feedback

Overview of apps in SharePoint

Article • 07/22/2024

Apps are small, easy-to-use web applications that add functionality to SharePoint sites. They offer unlimited possibilities for customizing your sites in ways that are specific to your organization. For example, you can add apps that perform general tasks such as time and expense tracking, or apps that make it easy for customers to contact you, or productivity apps that enable you to establish data connections and develop reports for your stakeholders.

Some apps are included with SharePoint, others might be developed by your organization, and still others are created by third-party developers and available for purchase from the SharePoint Store.

Only those users who have the appropriate permission level can add apps to a site. Typically, Full Control permission (or membership in the Site Owners group) is the minimum requirement. But some apps require access to data sources or web services to read data required for the app. This kind of app has permissions associated with it.

When the app requires organization-level permissions, the requestor will need approval from a Microsoft 365 admin to continue with the installation. The approval process includes a workflow, called the permission request flow, which ensures installation requests are directed to the right person.

This article is intended for SharePoint Administrators and above in Microsoft 365 at the organization level who receive requests for app installation.

Make the application available

Once the status has been changed to **Approved**, go to the SharePoint Store and acquire the app. This is done by clicking the link next to **View App Details** on the App Request entry.

At this point, site owners can check the **Your Requests** list to view the status of their request. After the application has been acquired and approved, it will show up in the **Apps you've requested** list.

Delegate approval authority

As a SharePoint Administrator or above in Microsoft 365 in your organization, you can delegate app approval authority as a way of spreading the approval workaround, or

alleviating approval bottlenecks. Remember that apps are stored and managed in the Apps site. To grant app approval permission to select users, you can add them as site admins on the Apps site.

> **Caution**
>
> When you add users as site admins on the Apps site, you are giving them the ability to approve the installation of apps that have organization-wide impact. Consider this decision carefully.

To add site collection admins to the Apps site:

1. Go to the Active sites page of the new SharePoint admin center, and sign in with an account that has admin permissions for your organization.
2. Select the Apps site, and then select **Membership** on the command bar to open the details panel.
3. Make the appropriate selection based on the type of member and provide input and select the name of the person who you want to manage apps, and then select **Save**.

Feedback

Was this page helpful? Yes No

Provide product feedback

Manage apps using the Apps site

As a SharePoint Administrator or above in Microsoft 365, you can acquire solutions from the SharePoint Store or distribute custom apps that can be used across SharePoint, Microsoft Teams, and Viva Connections.

For information about your options for developing custom apps for SharePoint, see Overview of the SharePoint Framework and SharePoint add-ins.

> **Important**
>
> Starting April 2, 2026, SharePoint add-ins will be retired for SharePoint in Microsoft 365 and users will no longer be able to use SharePoint add-ins. Installing SharePoint add-ins from the SharePoint Store will not be possible as of July 1, 2024. Learn more about the retirement of add-ins.

Add apps from the SharePoint Store

When you add an app from the SharePoint Store to the Apps site, you make it available for site owners to add from the My apps page.

1. Go to the More features page in the SharePoint admin center and select **Open** under **Apps**.
2. On the Manage apps page, select **SharePoint Store** in the left pane.
3. Search for an app or select a category to scroll through available apps.
4. Select an app you want to add. In some cases, adding the app might be supported in the SharePoint Store classic experience only.
5. Select **Add to Apps site**.
6. Some apps can be added to all sites in the organization so that site owners don't have to. If you want to do this, select **Enable this app and add it to all sites**.
7. Select **Add**.

8. If the app requires additional permissions, a message appears. Go to **API access page** in SharePoint admin Center to approve the permission requests.

Add custom apps

When you upload a custom app to the Apps site, it's available for users to install when they browse apps under **From Your Organization**.

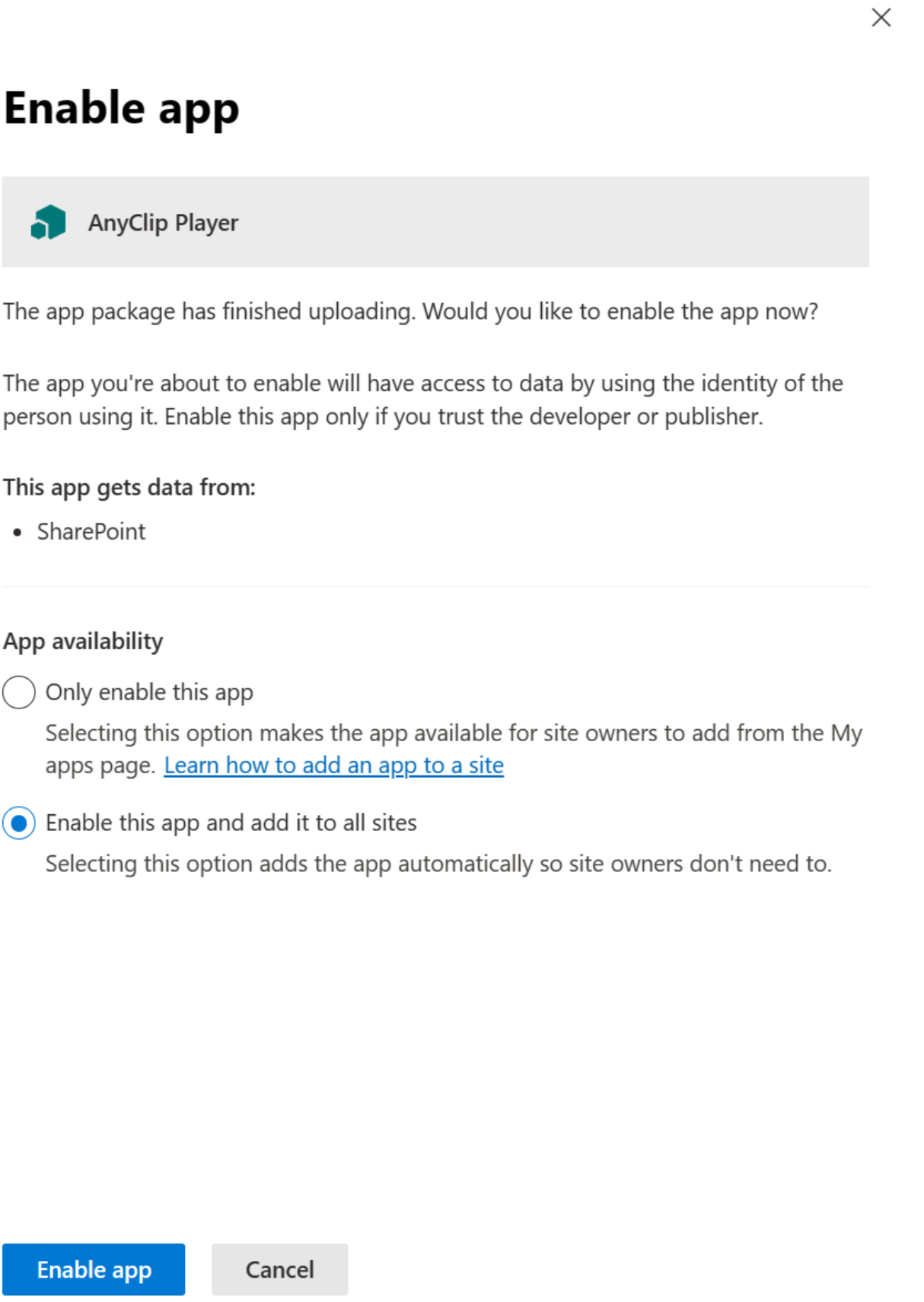
1. Go to **More features** in the SharePoint admin center, and sign in with an account that has admin permissions for your organization.

   > **Note**
   >
   > If you have Office 365 operated by 21Vianet (China), sign in to the Microsoft 365 admin center, then browse to the SharePoint admin center and open the More features page.

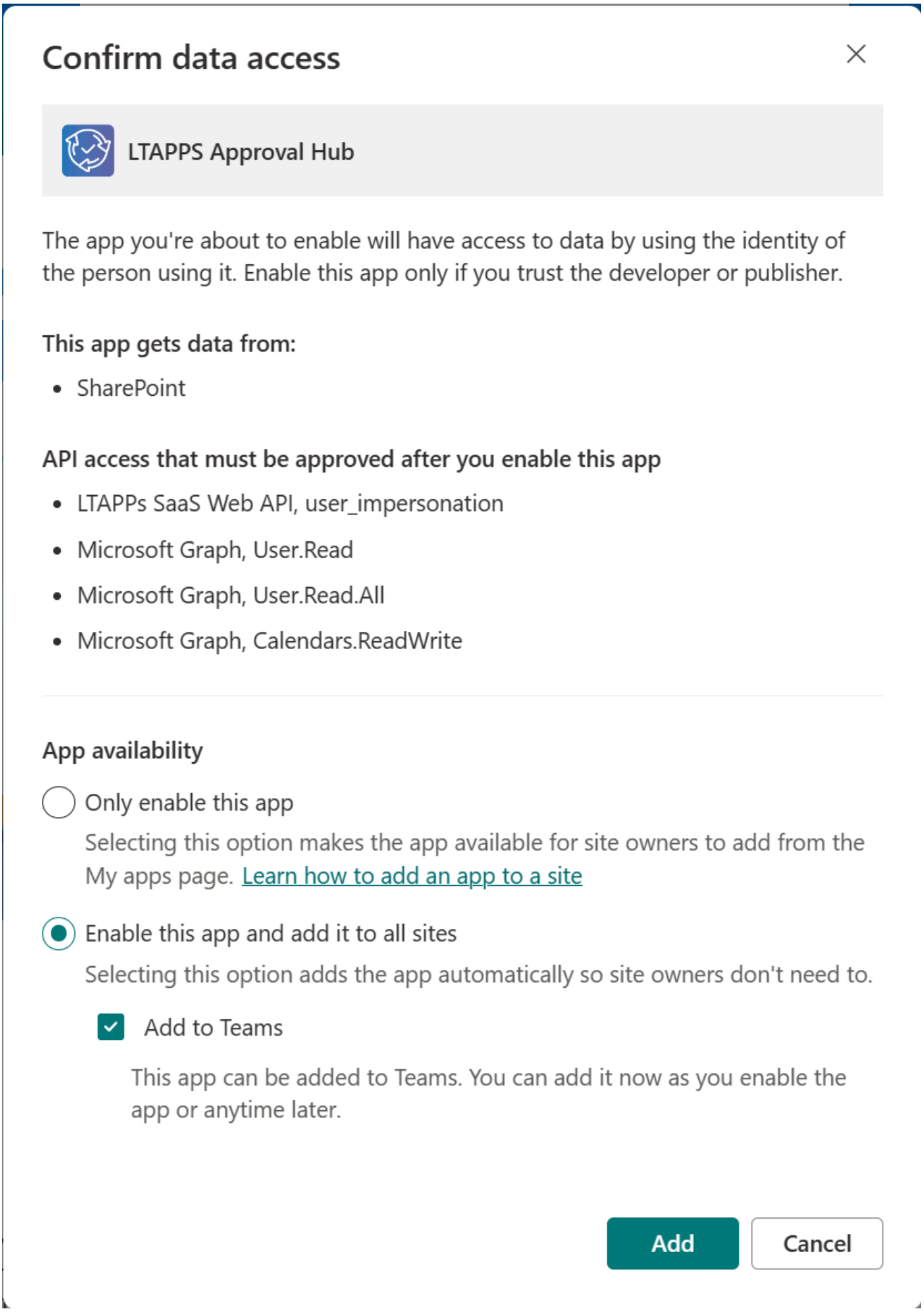
2. Under **Apps**, select **Open**.

3. On the Manage apps page, select **Upload**, and browse to the app you want upload, or drag the app into the library. SharePoint Framework solutions have the file name extension .sppkg.

4. Review the info in the **Enable app** panel. Depending on the functionality that the app provides, the developer can set a flag that allows you to add the app to all sites in the organization. To do this, select **Enable this app and add it to all sites**.



If the app can be added to Teams, you can check the **Add to Teams** option that appears under **Enable this app and add it to all sites**.

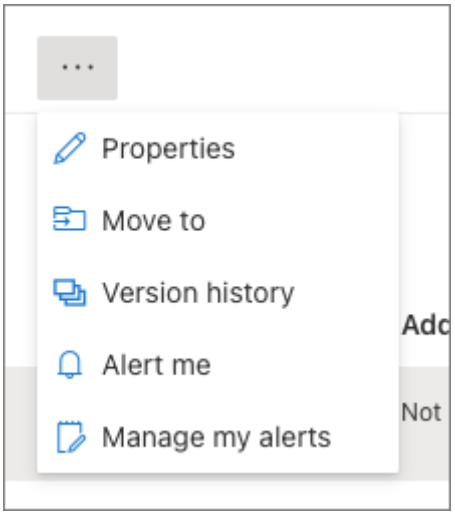


> **Note**
>
> We recommend testing solutions before deploying them broadly.

5. Select **Enable app** or **Add** for apps that can be added to Teams.

6. Select **Close**.

7. To help site owners identify and use the app, select the app, and then select **Properties**.



8. Review and edit the **Name** for the app and enter optional information like a description, images, category, publisher, and support URL. Follow the instructions on the screen for details like image size.

9. Make sure the **Enabled** checkbox is selected so that users are able to add this app to sites.

10. If it appears, in the **Hosting Licenses** box, specify the number of licenses you think you need.

11. Close the panel.

Add an app to all sites

App developers can choose to allow administrators to automatically add an app to all sites. This makes the app available for site owners.

If you didn't choose to add an app to all sites when you enabled it, you can do so later on the Apps site.

To add an app to all sites:

1. On the **Manage apps page**, select the app that you want to add to all sites.

2. Select **Add to all sites**.

3. Select **Confirm**.

4. Select **Close**.

Stop automatically adding an app to new sites

If you chose to have an app automatically added to all sites, you can stop adding it to new sites by changing the setting on the Apps site.

To stop adding an app to new sites:

1. On the Manage apps page, select the app that you want to stop adding to new sites.

2. Select **Stop adding to new sites**.

3. Select **Save**.

4. Select **Close**.

Add an app to Teams

Some apps can be added to Teams. You can add them on the Apps site.

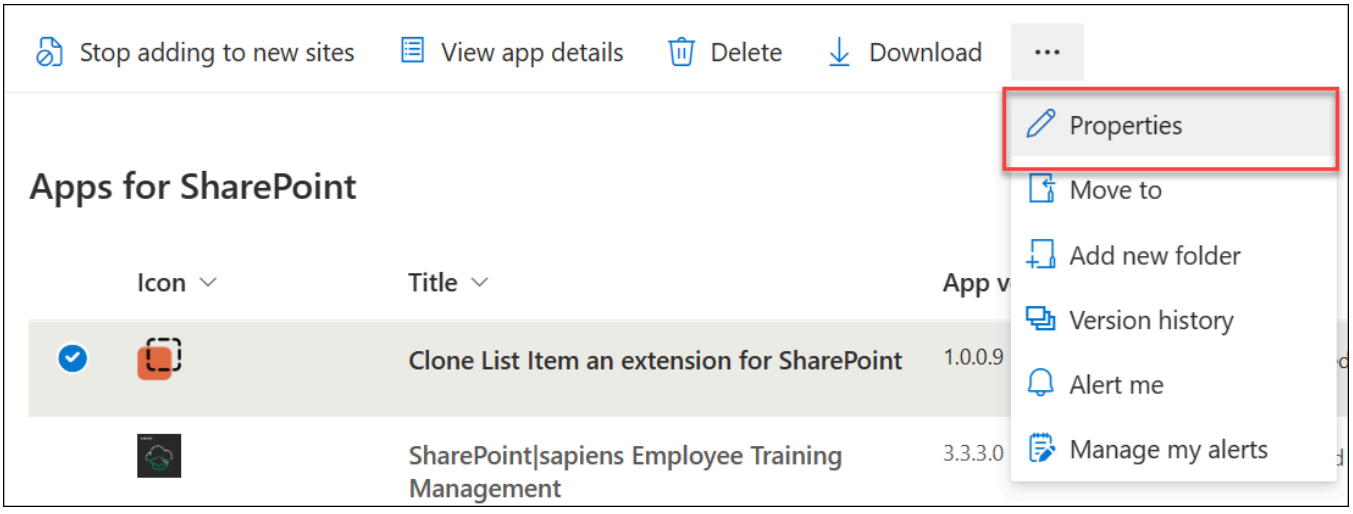
To add an app to Teams:

1. On the Manage apps page, select the app that you want to add to Teams.

2. Select **Add to Teams**.

Disable an app

If you want to prevent users from using an app that you've already enabled, you can disable it.



1. On the Manage apps page, select the app that you want to disable, and then select **Properties**.
2. Clear the **Enabled** check box.
3. Close the panel.

Delete an app from the Manage apps page

If you just want to remove an app from a specific site, see Remove an app from a site .

If you no longer want a specific app to be available for users to add, you can delete it from on the Manage apps page. Any instances of the app that have already been added to sites by users remain, but the app is no longer available for users to add to more sites.

> **Important**
>
> If you delete an app, existing instances of the app will no longer work.

1. On the Manage apps page, select the app that you want to delete.
2. Select **Delete**.
3. Select **Delete** to confirm that you want to send the app to the recycle bin.

Related articles

Configure settings for the SharePoint Store

Add an app to a site

Last updated on 04/03/2026

Manage app requests

Article • 02/10/2025

When users request an app, they are requesting that an admin get that app on their behalf. In an app request, users can request a specific number of licenses, and they can provide a business justification for why they need the app. App requests are saved to the App Requests list in the Apps site.

To manage app requests

1. Go to the More features page of the new SharePoint admin center, and sign in with an account that has admin permissions for your organization.

   > **Note**
   >
   > If you have Office 365 Germany, sign in to the Microsoft 365 admin center, then browse to the SharePoint admin center and open the More features page.
   >
   > If you have Office 365 operated by 21Vianet (China), sign in to the Microsoft 365 admin center, then browse to the SharePoint admin center and open the More features page.

2. Under **Apps**, select **Open**, and then select **More features**.

3. Select **Configure store settings**.

4. Select **Click here to view app requests**. Then select **Active requests**.

To approve an app

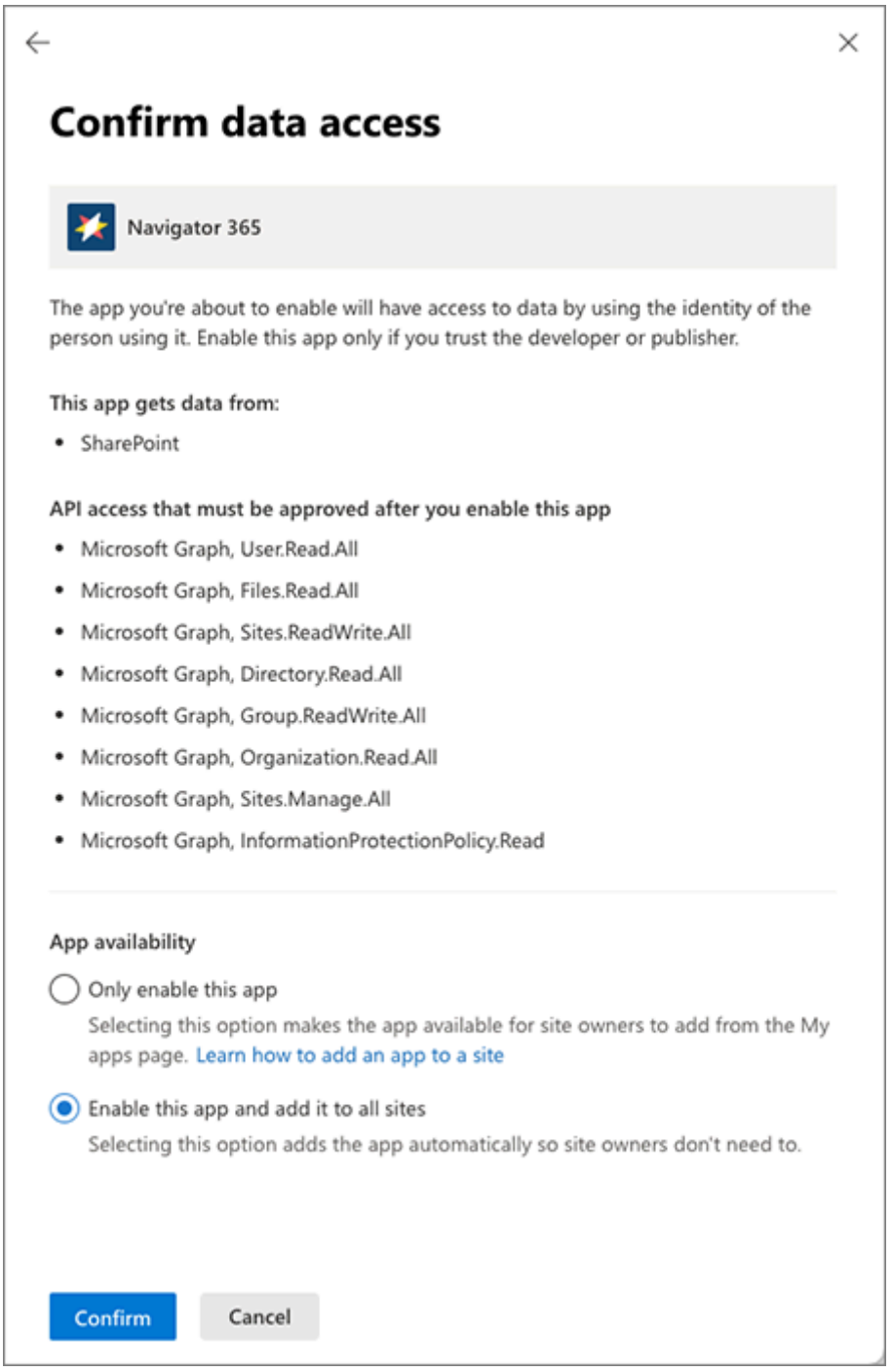
1. In the **Active Requests** list, select a request.

2. On the app request form, add any comments in the **Comments** field.

3. Select **Approve and add this app**.

4. If the app allows you to automatically add it to all sites, choose if you want to add it to all sites.

5. Confirm the data access required by the app by selecting **Confirm**.



6. If the app requires additional permissions, go to the API access page to approve those permissions.

7. Close the panel.

To decline an app

1. In the **App Requests** list, select a request.

2. On the app request form, add any comments in the **Comments** field.

3. Select **Decline request**.

4. On the confirmation panel, select **Decline request**.

If you didn't add the app to all sites in the approval process, users need to add it to the site. See Add an app to a site.

Site users who request apps can view their requests by going to **Settings** > **Add an app** > **Your Requests**.

Related topics

Add an app to a site

Office Store and SharePoint Store Terms of Use

Feedback

Was this page helpful? Yes No

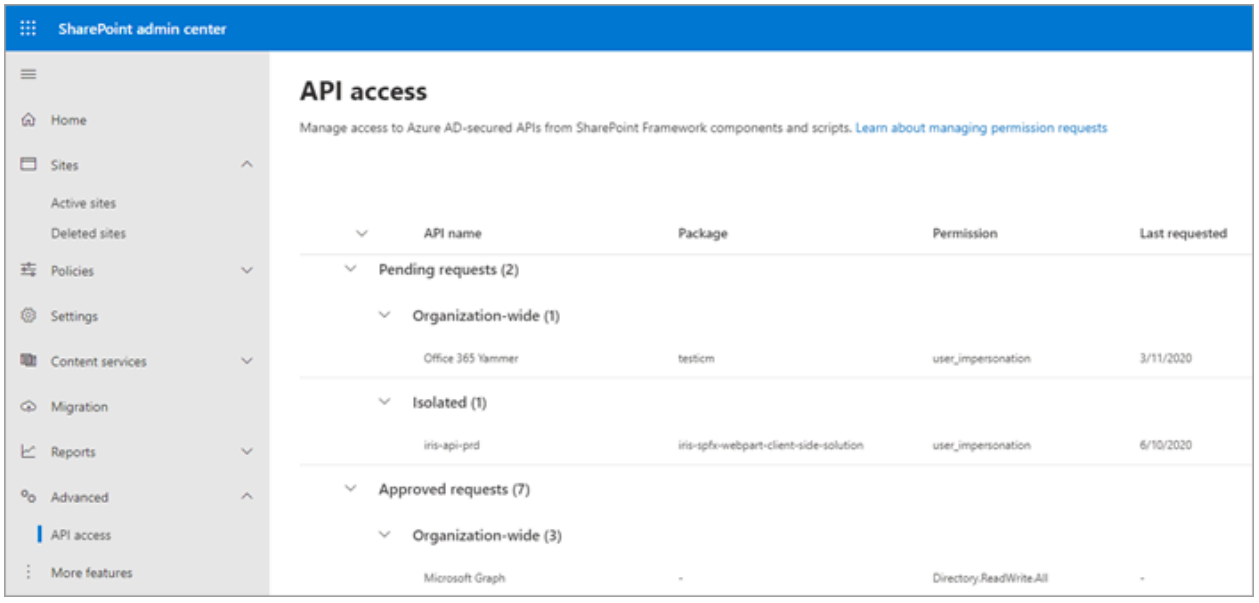
Provide product feedback

Manage access to Microsoft Entra ID-secured APIs

Article • 09/25/2024

When developers build SharePoint Framework solutions, they might need to connect to an API that's secured through Microsoft Entra ID. Developers can specify which Microsoft Entra applications and permissions their solution requires, and an administrator can manage the permission request from **API access** in the SharePoint admin center.

Learn more about building SharePoint Framework solutions that connect to Azure-AD secured APIs.



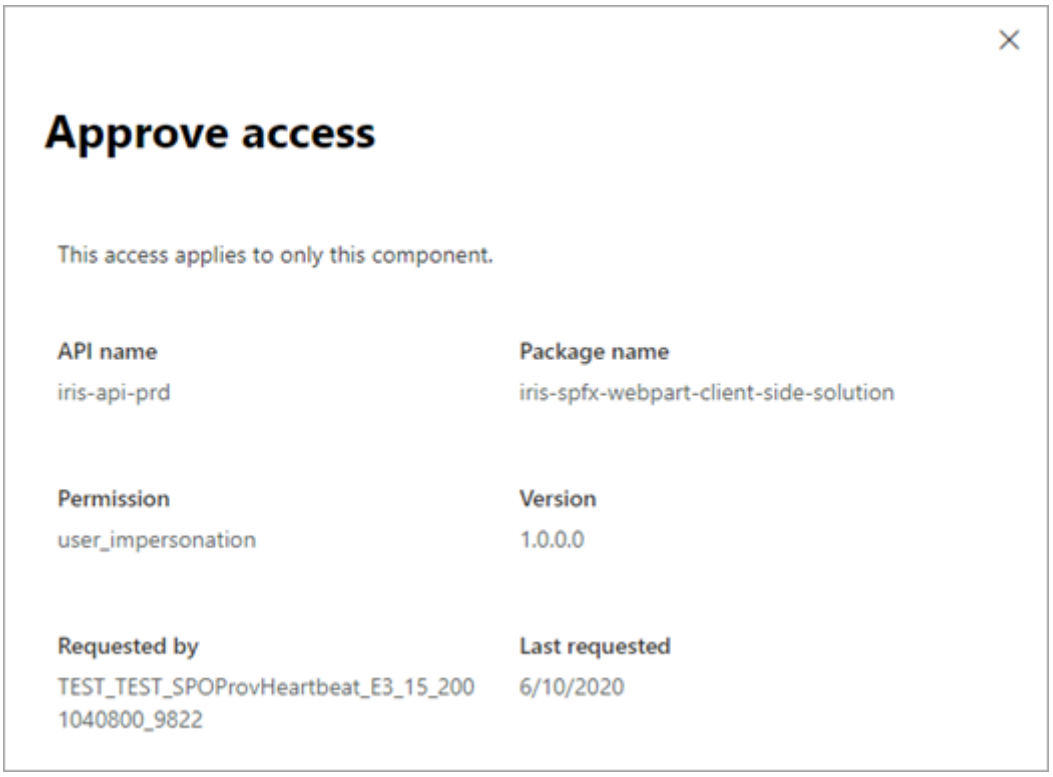
The API access page shows pending and approved requests. It also shows which requests apply to any SharePoint Framework component or custom script in your organization (organization-wide) and which requests apply to only the specific component (isolated).

> **Note**
>
> The admin role that's required to approve permissions depends on the API. To approve permissions to any of the third-party APIs registered in the tenant, the application administrator role is sufficient. To approve permissions for Microsoft Graph or any other Microsoft API, the Global Administrator role is required. The API access page is not available for people signed in with the global reader role.

Approve a pending request

1. Select the request, and then select **Approve** to see details about the request.

2. In the **Approve access** panel, select **Approve**.



After you approve a request, it moves to the Approved requests list.

> **Note**
>
> Permissions of type delegated are added to the *SharePoint Online Client Extensibility Web Application Principal* in Microsoft Entra ID.
>
> If you try to approve a permission request for a resource that already has some permissions granted (for example, granting additional permissions to the Microsoft Graph), the requested scopes are added to the previously granted permissions.

Reject a pending request

1. Select the request, and select **Reject**.

2. Select **Reject** again to confirm.

Rejecting access doesn't remove the app from the Apps site. If the app is used on any sites, it might not work as expected. After you reject the request, it's removed

from the page and the developer will need to issue a new request with the same resource and scope.

Remove access to a previously approved request

1. Select the request, and then select **Remove access**.
2. Select **Remove** again to confirm.

   When you remove access, solutions and custom scripts that rely on the permission might not work as expected. After you remove access, the request is removed from the page and the developer will need to issue a new request with the same resource and scope.

Manage access by using Microsoft PowerShell

You can also use PowerShell to manage permission requests.

- To view pending requests, use the cmdlet Get-SPOTenantServicePrincipalPermissionRequests.
- To approve a request, use the cmdlet Approve-SPOTenantServicePrincipalPermissionRequest.
- To reject a request, use the cmdlet Deny-SPOTenantServicePrincipalPermissionRequest.
- To remove access to a previously approved request, use the cmdlet Revoke-SPOTenantServicePrincipalPermission.

Feedback

Was this page helpful? Yes No

Provide product feedback

Allow or prevent custom script

As a SharePoint Administrator in Microsoft 365, you can temporarily allow the use of custom scripts in SharePoint sites. By using custom scripts, users can operate with some classic features, like using the script editor web part. Users can also change the look, feel, and behavior of sites and pages to meet organizational objectives or individual needs.

If you allow custom script, all users who have *Add and Customize Pages* permission to a site or page can add any script they want. By default, users who create sites are site owners and, therefore, have this permission.

> **Note**
>
> For simple ways for users to change the look and feel of a site, see Change the look of your SharePoint site.

By default, SharePoint doesn't allow script on most sites that administrators create by using the SharePoint admin center and on all sites that are created by using the New-SPOSite PowerShell command. The same restriction also applies to OneDrive, sites that users create themselves, modern team and communication sites, and the root site for your organization. For more information about the security implications of custom script, see Security considerations of allowing custom script.

> **Important**
>
> If your organization's SharePoint deployment was done before 2015, your custom script settings might still be set to *Not Configured*, even if, in the SharePoint admin center, they appear to be set to prevent users from running custom script. In this case, users can't copy items between SharePoint sites and between OneDrive and SharePoint. On the Settings page in the SharePoint admin center, to accept the custom script settings as they appear, select **OK**, and enable cross-site copying. For more information about copying items between OneDrive and SharePoint, see Copy files and folders between OneDrive and SharePoint sites.

How do I temporarily allow custom script on SharePoint sites?

> **Caution**

Before you allow custom script on sites in your organization, make sure you understand the security implications.

To allow custom script on a particular site (previously called a *site collection*) immediately, follow these steps:

1. Download the latest SharePoint Online Management Shell.

   > **Note**
   >
   > If you installed a previous version of the SharePoint Online Management Shell, go to **Add or remove programs** and uninstall **SharePoint Online Management Shell**.

2. Connect to SharePoint as a SharePoint Administrator in Microsoft 365. To learn how, see Getting started with SharePoint Online Management Shell.

3. Run the following command.

   PowerShell
   ```
   Set-SPOSite <SiteURL> -DenyAddAndCustomizePages 0
   ```

   Or, use the Set-PnPSite PowerShell cmdlet as follows:

   PowerShell
   ```
   Set-PnPSite -Identity <SiteURL> -NoScriptSite $false
   ```

Changes to allow custom scripts are overridden to *Not allowed* within 24 hours.

> **Note**
>
> You can't allow custom scripts on an individual user's OneDrive.

How do I permanently block new custom scripts in OneDrive and SharePoint sites?

Turn on Baseline security mode settings.

How do I manage custom scripts in the SharePoint admin center?

As a SharePoint administrator, use the SharePoint admin center to manage custom scripts within your organization.

1. Identify the sites that are configured to use custom scripts.

2. Change custom script settings for each site, as appropriate for your organiztion.

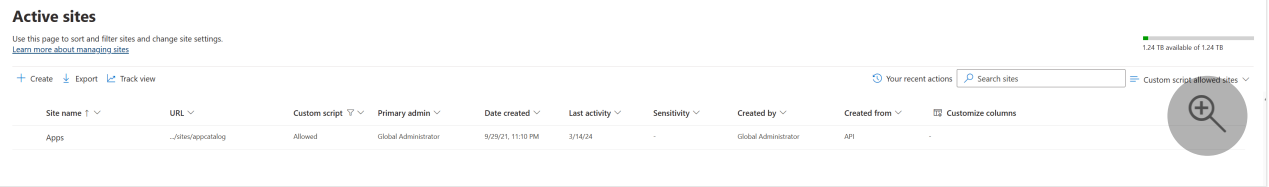
Alternately, you can turn on Baseline security mode settings and block new custom scripts across OneDrive and SharePoint sites at once.

Identify sites that allow custom scripts

Use the SharePoint admin center to identify SharePoint sites that are configured to allow custom scripts.

1. In the SharePoint admin center, under **Sites**, select **Active sites**.

2. Look for the **Custom script** column.



If you don't see the **Custom script** column in the list of sites, add it to any view.

The **Custom script allowed sites** view is also available to provide easy access to all sites where custom script is enabled:

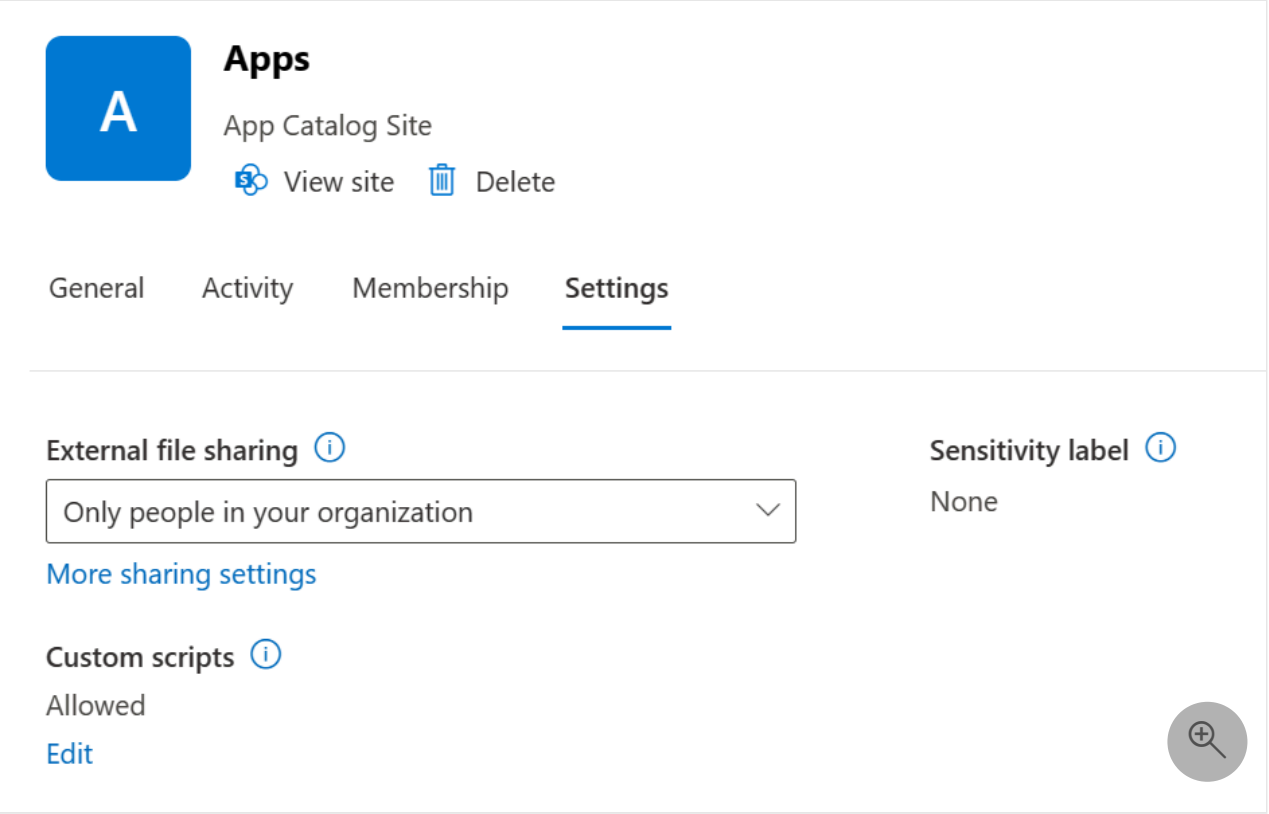
These views show which sites are configured to allow custom scripts, even if they don't actually use custom scripts.

Change custom script settings for a SharePoint site

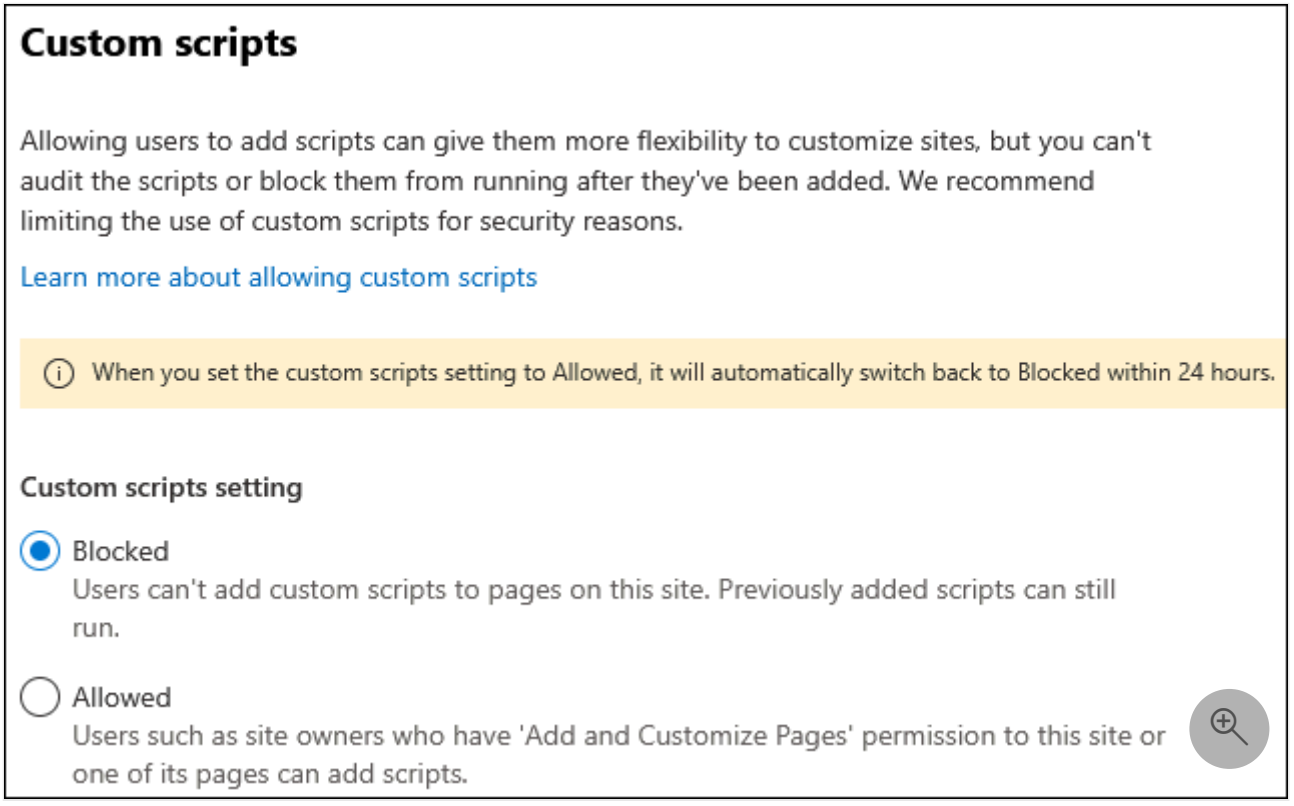
1. In the SharePoint admin center, under **Sites**, select **Active sites**.

2. On the **Active sites** page, select a site.

3. Under **Settings** > **Custom scripts**, specify whether to allow or block custom scripts.



You can control custom script settings for a specific site by deciding whether to allow or block custom script:



By default, any changes to custom script settings for a specific site last for a maximum of 24 hours. After that time, the setting resets to **Blocked** for that specific site.

> **Important**
>
> If the site is locked because it's in either the *ReadOnly* or *NoAccess* state, changes to custom scripts settings don't appear in the SharePoint admin center. However, as soon as the state of the site goes back to *Unlock*, custom script settings immediately turn to *Not allowed* before users access the site.

What features are affected when custom scripts are blocked?

When you block users from running custom scripts on OneDrive or the classic SharePoint team sites they create, site administrators and owners can't create new items, such as templates, solutions, themes, and help file collections. If you previously allowed custom script, items that were already created still work.

The following site settings aren't available when you prevent users from running custom script:

Expand table

Site feature	Behavior	Notes
Save Site as Template	No longer available in Site Settings	Users can still build sites from templates created before custom script was blocked.
Save document library as template	No longer available in Library Settings	Users can still build document libraries from templates created before custom script was blocked.
Save list as template	No longer available in List Settings	Users can still build lists from templates created before custom script was blocked.
Theme Gallery	No longer available in Site Settings	Users can still use themes created before custom script was blocked.
Help Settings	No longer available in Site Settings	Users can still access help file collections available before custom script was blocked.
Sandbox solutions	Solution Gallery is no longer available in Site Settings	Users can't add, manage, or upgrade sandbox solutions. They can still run sandbox solutions that were deployed before custom script was blocked.
SharePoint Designer	Pages that aren't HTML can no longer be updated.	Users can still open some data sources. To open a site that doesn't allow custom script in

Site feature	Behavior	Notes
	Handling List: **Create Form** and **Custom Action** no longer work. Subsites: **New Subsite** and **Delete Site** redirect to the **Site Settings** page in the browser. Data Sources: **Properties** button is no longer available.	SharePoint Designer, you must first open a site that does allow custom script.

Operating files that potentially include script	The following file types can't be uploaded, copied, moved, or opened in a library:
	`.asmx`
	`.ascx`
	`.aspx`
	`.htc`
	`.jar`
	`.master`
	`.swf`
	`.xap`
	`.xsf`
		Existing files in the library aren't impacted.

Uploading Documents to Content Types	Access denied message when attempting to attach a document template to a Content Type.	We recommend using Document Library document templates.
Publishing of SharePoint 2010 Workflows	Access denied message when attempting to publish a SharePoint 2010 Workflow.	
Custom Actions	Access denied message when attempting to create new custom actions.	Existing custom actions aren't impacted.
Design Manager	Access denied message when attempting to create new layout, master page, or design package.	Users can still use page designs created before custom script was blocked.

By default, you can't update the Site property bag when you prevent users from running custom scripts. You can change that behavior by running the following command:

PowerShell

```
Set-SPOTenant -AllowWebPropertyBagUpdateWhenDenyAddAndCustomizePagesIsEnabled
```

```
$True
```

For more information, see AllowWebPropertyBagUpdateWhenDenyAddAndCustomizePagesIsEnabeld option.

When custom scripts are blocked, the following web parts and features are unavailable to SharePoint site administrators and owners:

Expand table

Web part category	Web part
Business Data	Business Data Actions Business Data Item Business Data Item Builder Business Data List Business Data Related List Excel Web Access Indicator Details Status List Visio Web Access
Community	About This Community Join My Membership Tools What's Happening
Content Rollup	Categories Project Summary Relevant Documents RSS Viewer Site Aggregator Sites in Category Term Property Timeline WSRP Viewer XML Viewer
Document Sets	Document Set Contents Document Set Properties
Advanced	Embed
Forms	HTML Form Web Part
Media and Content	Content Editor Script Editor

Web part category	Web part
	Silverlight Web Part Page Viewer (can't set web page URL)
Search	Refinement Search Box Search Navigation Search Results
Search-Driven Content	Catalog-Item Reuse
Social Collaboration	Contact Details Note Board Organization Browser Site Feed Tag Cloud User Tasks
Master Page Gallery	Can't create or edit master pages
Publishing Sites	Can't create or edit master pages and page layouts

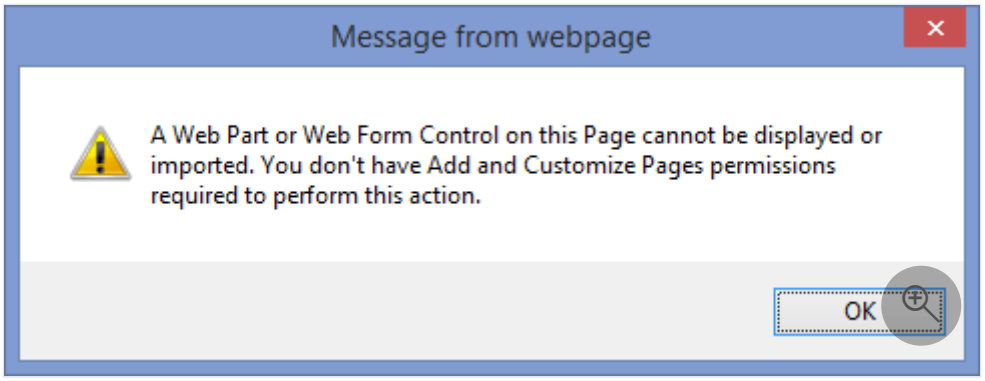
Furthermore, SharePoint Framework web parts that have the `requiresCustomScript` value set to `true` behave as follows:

- The web part isn't available in the web part picker.
- Every instance of a web part that was added to a page when custom scripts were previously allowed no longer surfaces in those pages.

SharePoint site authors can remove web parts that no longer work while editing their pages.

Best practices for communicating script setting changes

Before you prevent custom script on sites where you previously allowed it, communicate the change well in advance so users can understand the impact. Otherwise, users who are accustomed to changing themes or adding web parts on their sites suddenly can't make those changes. They see the following error message.



Communicating the change in advance reduces user frustration and support calls.

Related articles

- Baseline security mode settings

Last updated on 02/03/2026

Security considerations of allowing custom script

Article • 09/23/2024

Allowing users to customize sites and pages in SharePoint by inserting script can give them the flexibility to address different needs in your organization. However, you should be aware of the security implications of custom script.

When you allow users to run custom script, you can no longer enforce governance, scope the capabilities of inserted code, block specific parts of code, or block all custom code that has been deployed. Instead of allowing custom script, we recommend using the SharePoint Framework. For more info, see An alternative to custom script.

What custom script can do

Every script that runs in a SharePoint page (whether it's an HTML page in a document library or a JavaScript in a Script Editor Web Part) always runs in the context of the user visiting the page and the SharePoint application. This means:

- Scripts have access to everything the user has access to.
- Scripts can access content across several Microsoft 365 services and even beyond with Microsoft Graph integration.

You can't audit the insertion of script

As a SharePoint Administrator or above, you can allow or block custom script capabilities for the whole organization or for specific site collections. (For info on how to do this, see Allow or prevent custom script.) However, once you allow scripting, you can't identify:

- What code has been inserted
- Where the code has been inserted
- Who inserted the code

Any user who has "Add and Customize Pages" permission (part of the Design and Full Control permission levels) to any page or document library can insert code that can potentially have a powerful effect on all users and resources in the organization.

The script has access to more than just the page or site - it can access content across all site collections and other Microsoft 365 services in the organization. There are no boundaries for executing script. For info about site activity you can audit, see Configure audit settings for a site collection.

You can't block or remove inserted script

If you've allowed custom script, you can change the setting to later prevent users from adding custom script, but you can't block the execution of script that has already been inserted. If dangerous or malicious script is inserted, the only way you can stop it is to delete the page that hosts it. This might result in data loss.

An alternative to custom script

The SharePoint Framework is a page and web part model that provides a governed and fully supported way to build solutions using scripting technologies with support for open-source tooling. Key features of the SharePoint Framework:

- The framework runs in the context of the current user and connection in the browser.
- The controls are rendered in the normal page Document Object Model (DOM).
- The controls are responsive and accessible.
- Developers can access the lifecycle. Also to render, they can access load, serialize and deserialize, configuration changes, and more.
- You can use any browser framework you like: React, Handlebars, Knockout, Angular, and more.
- The toolchain is based on common open source client development tools like npm, TypeScript, Yeoman, webpack, and gulp.
- Admins have governance tools to immediately disable solutions regardless of the number of instances that have been used and the number of pages or sites across which they've been used.
- Solutions can be deployed in web parts and pages that use the classic experience or the new experience.
- Only Global Administrators, SharePoint Administrators, and people who have been given permission to manage the Apps site can add solutions. For info about giving

users permission to manage the Apps site, see Request app installation permissions.

Feedback

Was this page helpful? Yes No

Provide product feedback

Configure settings for the SharePoint Store

Article • 02/21/2023

The SharePoint Store is a public marketplace that offers apps for Microsoft 365, as well as Dynamics 365 and Power Platform. Site users can access the SharePoint Store directly from a SharePoint site to browse for and add third-party apps. If a SharePoint environment has been configured to prevent users from getting apps from the SharePoint Store, users can still browse for and request apps. These requests are added to the App Requests list in the SharePoint admin center.

Specify whether users can get apps from the SharePoint Store

By default, SharePoint is configured to allow users to get or request apps from the SharePoint Store. The option to change this setting will not be enabled if you have not yet created an Apps site. For information about how to create an Apps site, see Use the Apps site to make custom business apps available for your SharePoint environment.

Even if you choose not to allow users to add apps from the SharePoint Store, they will still be able to browse the SharePoint Store and request apps.

1. Go to the More features page of the SharePoint admin center, and sign in with an account that has admin permissions for your organization.

   > **Note**
   >
   > If you have Office 365 operated by 21Vianet (China), sign in to the Microsoft 365 admin center, then browse to the SharePoint admin center and open the More features page.

2. Under **Apps**, select **Open**, and then select **More features**.

3. Select **Configure store settings**.

4. Next to **App Purchases**, do one of the following:

   - If you want users to be able to add apps, select **Yes**.
   - If you do not want users to be able to get third-party apps, select **No**.

Specify whether to allow apps for Office to start in documents

Documents stored on sites may contain apps for Office from several sources. You can specify whether or not you want to allow these apps to work when documents are opened in the browser.

1. Go to the More features page of the SharePoint admin center, and sign in with an account that has admin permissions for your organization.

   > **Note**
   >
   > If you have Office 365 operated by 21Vianet (China), sign in to the Microsoft 365 admin center, then browse to the SharePoint admin center and open the More features page.

2. Under **Apps**, select **Open**, and then select **More features**.

3. Select **Configure store settings**.

4. Next to **Apps for Office from the Store**, do one of the following:

   - If you want to allow apps for Office to start when documents are opened in the browser, select **Yes**.
   - If you do not want to allow apps for Office to start when documents are opened in the browser, select **No**.

Related topics

Add an app to a site

Office Store and SharePoint Store Terms of Use

Feedback

Was this page helpful? Yes No

Provide product feedback

Required URLs and ports for OneDrive

Article • 03/27/2025

This reference article lists all endpoints used by the consumer version of Microsoft OneDrive. If your organization restricts computers on your network from connecting to the Internet, this article lists the Fully Qualified Domain Names (FQDNs) and ports that you should include in your outbound allowlist to ensure your computers can successfully use the consumer version of OneDrive.

> **Important**
>
> Filtering internet traffic requires advanced networking knowledge and isn't suitable for all customers.

If you are looking for a listing of endpoints used by OneDrive in Microsoft 365, see Microsoft 365 URLs and IP address ranges.

Supported hosts and ports for OneDrive

To use OneDrive, the following endpoints need to be accessible to client computers.

Expand table

Row	Destination host	Destination Port
1	onedrive.com *.onedrive.com onedrive.live.com login.live.com g.live.com spoprod-a.akamaihd.net *.mesh.com p.sfx.ms oneclient.sfx.ms *.microsoft.com fabric.io *.crashlytics.com vortex.data.microsoft.com posarprodcssservice.accesscontrol.windows.net redemptionservices.accesscontrol.windows.net token.cp.microsoft.com/ tokensit.cp.microsoft-tst.com/ *.office.com	TCP 80, TCP 443

Row	Destination host	Destination Port
	*.officeapps.live.com *.aria.microsoft.com *.mobileengagement.windows.net *.branch.io *.adjust.com *.servicebus.windows.net vas.samsungapps.com odc.officeapps.live.com login.windows.net login.microsoftonline.com	
2	*.files.1drv.com *.onedrive.live.com *.*.onedrive.live.com storage.live.com *.storage.live.com *.*.storage.live.com *.groups.office.live.com *.groups.photos.live.com *.groups.skydrive.live.com favorites.live.com oauth.live.com photos.live.com skydrive.live.com api.live.net apis.live.net docs.live.net *.docs.live.net policies.live.net *.policies.live.net settings.live.net *.settings.live.net skyapi.live.net snapi.live.net *.livefilestore.com *.*.livefilestore.com storage.msn.com *.storage.msn.com *.*.storage.msn.com	TCP 80, TCP 443

Feedback

Was this page helpful? Yes No

Provide product feedback

Configure InfoPath Forms Services

Article • 02/21/2023

InfoPath Forms Services in SharePoint lets you deploy your organization's forms to your sites, enabling users fill out these forms in a web browser. You can configure InfoPath Forms Services in any of several ways, depending on the needs of your organization.

> **Note**
>
> InfoPath Forms Services 2013 is the last release of InfoPath Forms Services. Microsoft Power Apps is the recommended solution for creating and delivering custom forms for SharePoint lists. Create new forms with Power Apps from the command bar or the **Customize** button on SharePoint list forms. Support for InfoPath Forms Services will match the support lifecycle for SharePoint Server 2016.

Overview

This article discusses settings that apply only to user form templates, which are form templates that are not deployed by a developer. User form templates don't require Full Trust, and they don't contain code or other business logic.

Form designers can publish user form templates to a list or a form library in a SharePoint site collection. Because user form templates can be deployed by many users, a server can potentially host thousands of user form templates. In large numbers, even form templates that contain no business logic can put a heavy load on the server.

Configure browser-enabled user form templates

When form templates are published to a server that is running InfoPath Forms Services, the designer of the form template can choose to make the form template browser-enabled. This allows a user to fill out the form in a web browser.

As an administrator, you can configure the following template settings for browser-enabled user form templates:

- **Enable or disable publishing of browser-enabled form templates.** If you disable publishing, form designers can publish only form templates that are not browser-

enabled. In this case, all browser-compatible features are disabled in the form template.

- **Enable or disable rendering of browser-enabled form templates.** If you disable rendering, users cannot use a web browser to fill out the form and must use Microsoft InfoPath Filler 2013 to open the form.

By default, browser-enabled user form templates can be published and rendered.

To configure browser-enabled user form templates:

1. Go to **More features** in the new SharePoint admin center, and sign in with an account that has admin permissions for your organization.

> **Note**
>
> If you have Office 365 operated by 21Vianet (China), sign in to the Microsoft 365 admin center, then browse to the SharePoint admin center and open the More features page.

2. Under **InfoPath**, select **Open**.
3. In the **User Browser-enabled Form Templates** section, specify how you want user form templates to be processed by InfoPath Forms Services by completing the following steps:

> **Note**
>
> These settings apply only to form templates published to form libraries. Workflow form templates and list forms are not affected.

   a. Select the **Allow users to browser-enable form templates** check box to allow users to publish browser-enabled form templates.

> **Note**
>
> Clearing this check box disables browser-enabled form templates across the entire site collection.

   b. Select the **Render form templates that are browser-enabled by users** check box to allow browser-enabled form templates that users publish to be rendered in a web browser.

> **Note**
>
> If this option is not selected, users can still publish browser-compatible form templates to form libraries, but these form templates cannot be filled out in a web browser.

4. Select **OK**.

Configure exempt user agents

To make indexing InfoPath forms faster and easier, you can specify which user agents to exempt from receiving an entire webpage to index. This means that when a user agent you've specified as exempt encounters an InfoPath form, the form will be returned as an XML file (which looks like a hierarchical text file) instead of an entire webpage. You can use the procedure below to select this option and populate the agent list.

1. Go to **More features** in the new SharePoint admin center, and sign in with an account that has admin permissions for your organization.

> **Note**
>
> If you have Office 365 operated by 21Vianet (China), sign in to the Microsoft 365 admin center, then browse to the SharePoint admin center and open the More features page.

3. Under **InfoPath**, select **Open**.
4. In the **Exempt User Agents** section, select the **Customize the list of exempt user agents** check box, and then do one of the following:
5. To add a user agent to the exempt list, in the **Name** box, enter a name, and then select **Add**.
6. To remove a user agent from the list, select the name, and then select **Remove**.
7. Select **OK**.

Feedback

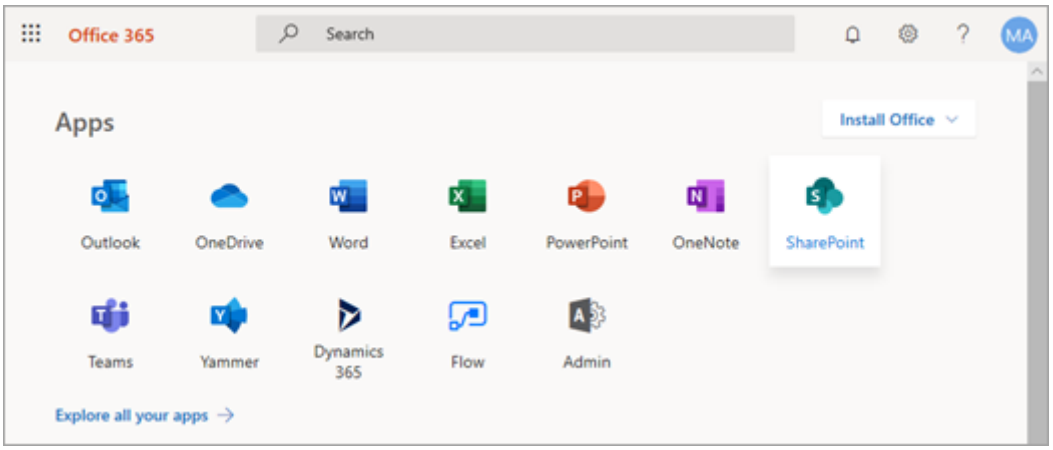
Was this page helpful? Yes No

Provide product feedback

Hide the OneDrive and SharePoint app tiles

Article • 04/16/2025

By default, the OneDrive and SharePoint app tiles appear in the app launcher and on the Microsoft 365 admin center. If your subscription doesn't include one of these services, or if you don't want users using one of them, you can hide the app tile for it.



> **Note**
>
> Hiding these services doesn't remove them for users. If users have saved the address of the service, they'll still be able to access it.
> If users select a tile for a service they don't have, they'll see an Access Denied message.

To show or hide app tiles

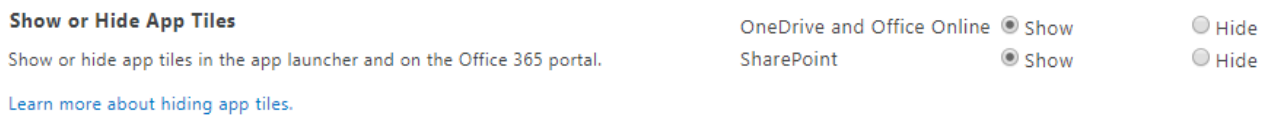
1. Go to **Settings** in the SharePoint admin center, and sign in with an account that has admin permissions for your organization.

   > **Note**
   >
   > If you have Office 365 operated by 21Vianet (China), sign in to the Microsoft 365 admin center, then browse to the SharePoint admin center and open the Settings page.

2. Open the **Settings** page.

3. At the bottom of the page, select **go to the classic settings page**.

4. In **Show or Hide App Tiles**, select the tile you want to show or hide.



> **Note**
>
> If you have an Office 365 Education subscription, you also have the option to hide **OneNote Class Notebooks** and **OneNote Staff Notebooks**.
> Hiding the OneDrive tile also hides the tiles for Word, Excel, PowerPoint, OneNote, and Visio.

5. To save the settings, select **OK**.

See also

Customize the navigation on your SharePoint site

Customize the Microsoft 365 theme for your organization

Add custom tiles to the app launcher

Allow users to create modern pages

Using modern pages in Microsoft SharePoint is a great way to share ideas using images, Office files, video, and more. Users can Add a page to a site quickly and easily, and modern pages look great on any device.

If you have at least a SharePoint Administrator role or more in Microsoft 365, you can allow or prevent users from creating modern pages. You can do this at the organization level by changing settings in the SharePoint admin center. If you allow the creation of site pages as the organization level, you can turn it on or off at the site level by using PowerShell. Site owners can also turn it on or off at the site level.

> **Note**
>
> If you want to prevent members from creating or modifying any SharePoint pages on a site, go to Site Pages, select **Settings** > **Library settings** > **Permissions for this document library**, and then set the Members group to Read.

Change page creation settings at the organization level

1. Go to **Settings** in the SharePoint admin center, and sign in with an account that has admin permissions for your organization.

   > **Note**
   >
   > If you have Office 365 operated by 21Vianet (China), sign in to the Microsoft 365 admin center, then browse to the SharePoint admin center and open the Settings page.

2. Select **Pages**.

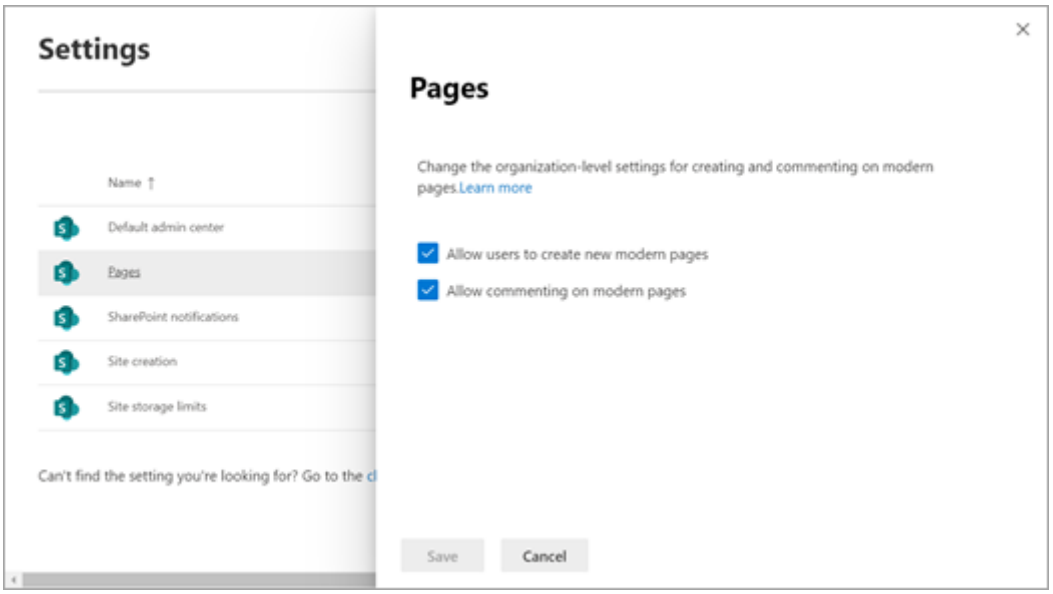
3. Select or clear **Allow users to create new modern pages**.

   > **Note**
   >
   > Preventing users from creating modern pages hides the following options:

- On the Site Pages and Site contents pages > **New** > **Page**.
- **Settings** > **Add a page**.

Users can still add pages from other modern pages, either from the New menu or from modern webparts (such as News).

4. You can also select to allow or prevent commenting on modern pages. If you allow commenting, it can be turned on or off at the page level.



Prevent users from creating modern pages on a specific site by using PowerShell

If you allow the creation of site pages as the organization level, you can turn it off at the site level by using PowerShell.

1. Download the latest SharePoint Online Management Shell.

> **Note**
>
> If you installed a previous version of the SharePoint Online Management Shell, go to Add or remove programs and uninstall "SharePoint Online Management Shell."

2. Install the SharePoint Online Client Components SDK.

3. Connect to SharePoint as a Global Administrator or SharePoint Administrator in Microsoft 365. To learn how, see Getting started with SharePoint Online Management Shell.

> ⓘ **Note**
>
> Read About Execution Policies and make sure you run the SharePoint Online Management Shell as an administrator and the correct execution policy to run unsigned scripts.

4. Copy the following code and paste it into a text editor, such as Notepad.

PowerShell

```
# Load SharePoint Online Client Components SDK Module
Import-Module 'C:\Program Files\Common Files\microsoft shared\Web Server Extensions\16\ISAPI\Microsoft.SharePoint.Client.dll'

# Set script constants
$sitePagesFeatureIdString = 'B6917CB1-93A0-4B97-A84D-7CF49975D4EC'

# Set up client context
$userName = Read-Host "Username"
$password = Read-Host "Password" -AsSecureString
$siteUrl = Read-Host "Site Url"
$webUrl = Read-Host "Server-Relative Web Url"
$context = New-Object Microsoft.SharePoint.Client.ClientContext($siteUrl)
$credentials = New-Object Microsoft.SharePoint.Client.SharePointOnlineCredentials($userName, $password)
$context.Credentials = $credentials

# Get the list of existing features
$web = $context.Site.OpenWeb($webUrl)
$features = $web.Features
$context.Load($features)
$context.ExecuteQuery()

# Verify that the Site Pages feature is present in the web
if(($features | ? { $_.DefinitionId -eq $sitePagesFeatureIdString }).Count -eq 0)
{
    Write-Host "The Site Pages feature is already disabled in this web"
    return
}

# Remove the Site Pages feature from the web
$features.Remove((new-object 'System.Guid' $sitePagesFeatureIdString), $false)
$context.ExecuteQuery()

# Verify that the Site Pages feature is no longer present in the Web
$web = $context.Site.OpenWeb($webUrl)
$features = $web.Features
$context.Load($features)
$context.ExecuteQuery()
if(($features | ? { $_.DefinitionId -eq $sitePagesFeatureIdString }).Count -eq 0)
```

```
{
    Write-Host "The Site Pages feature has been successfully disabled"
}
else
{
    throw "The Site Pages feature failed to be disabled"
}
```

5. Save the text file, and then change its extension. In this example, we name it SitePagesOut.ps1.

> **Note**
>
> You can use a different file name, but you must save the file as an ANSI-encoded text file whose extension is .ps1.

6. Change to the directory where you saved the file.

7. Run the following command:

PowerShell

```
.\SitePagesOut.ps1
```

8. The script prompts you for a **SiteUrl** and **WebUrl**.

   If you have a site such as: `https://contoso.sharepoint.com/sites/marketing/northwindcompete`

   For the **SiteUrl** you would enter: `https://contoso.sharepoint.com/sites/marketing`

   And for the **WebUrl** you would enter: `sites/marketing/northwindcompete`

Allow users to create modern pages on a specific site by using PowerShell

If you prevented users from creating modern pages on a site, follow these steps to allow it again.

1. Download the latest SharePoint Online Management Shell.

2. Install the SharePoint Client Components SDK.

3. Connect to SharePoint as a Global Administrator or SharePoint Administrator in Microsoft 365. To learn how, see Getting started with SharePoint Online Management Shell.

> ⓘ **Note**
>
> Read About Execution Policies and make sure you run the SharePoint Online Management Shell as an administrator and the correct execution policy to run unsigned scripts.

4. Copy the following code and paste it into a text editor, such as Notepad.

PowerShell

```
# Load SharePoint Online Client Components SDK Module
Import-Module 'C:\Program Files\Common Files\microsoft shared\Web Server
Extensions\16\ISAPI\Microsoft.SharePoint.Client.dll'

# Set script constants
$sitePagesFeatureIdString = 'B6917CB1-93A0-4B97-A84D-7CF49975D4EC'

# Set up client context
$userName = Read-Host "Username"
$password = Read-Host "Password" -AsSecureString
$siteUrl = Read-Host "Site Url"
$webUrl = Read-Host "Server-Relative Web Url"
$context = New-Object Microsoft.SharePoint.Client.ClientContext($siteUrl)
$credentials = New-Object
Microsoft.SharePoint.Client.SharePointOnlineCredentials($userName, $password)
$context.Credentials = $credentials

# Get the list of existing features
$web = $context.Site.OpenWeb($webUrl)
$features = $web.Features
$context.Load($features)
$context.ExecuteQuery()

# Verify that the Site Pages feature is not present in the web
if(($features | ? { $_.DefinitionId -eq $sitePagesFeatureIdString }).Count -gt 0)
{
    Write-Host "The Site Pages feature is already enabled in this web"
    return
}

# Add the Site Pages feature back to the web
$features.Add((new-object 'System.Guid' $sitePagesFeatureIdString), $false,
[Microsoft.SharePoint.Client.FeatureDefinitionScope]::None)
$context.ExecuteQuery()

# Verify that the Site Pages feature is now present in the web
$web = $context.Site.OpenWeb($webUrl)
```

```
$features = $web.Features
$context.Load($features)
$context.ExecuteQuery()
if(($features | ? { $_.DefinitionId -eq $sitePagesFeatureIdString }).Count -gt 0)
{
    Write-Host "The Site Pages feature has been successfully enabled"
}
else
{
    throw "The Site Pages feature failed to be enabled"
}
```

5. Save the text file, and then change its extension. In this example, we name it SitePagesIn.ps1.

> **Note**
>
> You can use a different file name, but you must save the file as an ANSI-encoded text file whose extension is .ps1.

6. Change to the directory where you saved the file.

7. Run the following command:

PowerShell

```
.\SitePagesIn.ps1
```

8. The script prompts you for a **SiteUrl** and **WebUrl**.

   If you have a site such as: `https://contoso.sharepoint.com/sites/marketing/northwindcompete`

   For the **SiteUrl** you would enter: `https://contoso.sharepoint.com/sites/marketing`

   And for the **WebUrl** you would enter: `sites/marketing/northwindcompete`

Last updated on 06/25/2026

Hybrid for SharePoint Server

Article • 01/25/2023

APPLIES TO: ✅ 2013 ✅ 2016 ✅ 2019 ✅ Subscription Edition ✅ SharePoint in Microsoft 365

With SharePoint Server hybrid, productivity services in SharePoint in Microsoft 365 can be integrated with on-premises SharePoint Server to provide unified functionality and access to data. For enterprises that want to gradually move their existing on-premises SharePoint Server services to the cloud, SharePoint Server hybrid provides a staged migration path by extending high-impact SharePoint Server workloads to SharePoint in Microsoft 365.

A SharePoint Server hybrid environment enables trusted communications between SharePoint in Microsoft 365 and SharePoint Server. When you have established this trust framework, you can configure integrated functionality between services and features such as Search, Follow, and user profiles.

To get started exploring hybrid, see the following articles:

- SharePoint hybrid sites and search
- Extranet for Partners with Microsoft 365

For detailed hybrid configuration information, see SharePoint Server 2016 hybrid configuration roadmaps.

Migrate your content to Microsoft 365

Moving to Microsoft 365? **Migration Manager** helps you migrate your content easily and securely.

Announcing the new Migration Admin role

A Microsoft 365 Migration Administrator role is now available to provide access to Migration Manager within the Microsoft 365 Admin Center. Previously, your migration teams must be assigned the SharePoint admin role, giving more access than needed. This new role is limited to the permissions required to migrate your content, reserving SharePoint Admin access to only users who need it.

Learn more: **Migration Admin role**.

What's new

- See what's new and coming soon to Migration Manager.
- See what's new and coming soon to the SharePoint Migration Tool (SPMT).

Mover retirement

Mover is now retired for all Admin led migrations. The ability to migrate from Google Drive, Box, Dropbox, and Egnyte is fully integrated into Migration Manager. All FastTrack-led migrations are transitioned to Migration Manager. Migration Manager doesn't support the migration of Amazon S3 or Azure blob storage.

Mover will be retired and not available for individual and students use after October 31, 2024.

- For migrating from Google Drive and Dropbox to your OneDrive (personal) account, download the OneDrive mobile app from here and follow the guidance.
- For migrating from OneDrive (work or school) to your OneDrive (personal) account, follow the guidance.
- For other migration scenarios to migrate your content to Microsoft 365, check Migration Manager learn more.

Cross-tenant migration

Tenant to tenant migration for OneDrive is now available outside of Migration Manager. To learn more:

- Cross-tenant OneDrive migration.

A cross tenant migration solution for SharePoint is currently in private preview. To learn more, see:

- How to participate in the Cross-tenant SharePoint migration preview.

Transform your classic SharePoint Server pages

If you're onboarding your classic on-premises SharePoint Server pages to Microsoft 365, we have assistance available. Learn more at: Transform classic pages to modern pages.

Where are you migrating from?

Expand table

Migrate from	Description
BOX	Collaborate all in one place by migrating your Box documents, data, and users to OneDrive, SharePoint, and Teams in Microsoft 365.
FILE SHARES	With a centralized way of connecting servers, creating tasks, and managing your migration tasks, migrate your file shares to Microsoft 365.
GOOGLE WORKSPACE	Migrate your Google Drives to Microsoft 365.
DROPBOX	Collaborate all in one place by migrating your Dropbox documents, data, and users to OneDrive, SharePoint, and Teams in Microsoft 365.
SHAREPOINT SERVER	Migrate your SharePoint Server sites and content to take advantage of the latest collaboration, intelligence, and security solutions in Microsoft 365. SharePoint Server 2010, 2013, and 2016 environments only.
SHAREPOINT SERVER WORKFLOWS	Microsoft removed **SharePoint Server 2010** workflow services from existing tenants on November 1, 2020. We recommend that you move your classic SharePoint Server workflows to Power Automate flows. With SPMT, you can migrate your **SharePoint Server 2010** out of the box (OOTB) approval and collect feedback workflows to Power

Migrate from	Description
	Automate, List and library "out-of-box" (OOTB) approval workflows, and Workflow definitions and associations.
SHAREPOINT SERVER CLASSIC PAGES	Are you onboarding your classic on-premises SharePoint Server content to Microsoft 365? Here's how: Transform classic pages to modern pages

Other resources

- **Cross-tenant OneDrive migration**. During mergers or divestitures, you commonly need the ability to move your users OneDrive accounts into a new Microsoft 365 tenant. With Cross-tenant OneDrive migration, tenant administrators can use PowerShell to transition users into their new organization. To learn more, see **Cross-tenant OneDrive migration**

- **Microsoft FastTrack**. Microsoft FastTrack services can help you get started with your migration to the cloud. When you need assistance to help you get started on your migration project.

- **Azure Data Box**. Want to remove the dependency on your WAN link to transfer data? The Microsoft Azure Data Box is a service that lets you order a device from the Microsoft Azure portal. You can then copy terabytes of data from your servers to the device, ship it back to Microsoft, and your data is copied into Azure. Once your data's in Azure, use SPMT to migrate content to SharePoint. To learn more, see Migrate using the Azure Data Box.

- **OneDrive sync app** To migrate users' Windows known folders (Desktop, Documents, Pictures, Screenshots, and Camera Roll) to OneDrive, you can use Known Folder Move. If users want to move other files from their local computer or a network file share to OneDrive or SharePoint, it's often easiest for them to use the OneDrive sync app. Users drag their files or folders to a folder they're syncing.

> **Note**
>
> When you migrate your content to Microsoft 365, you are copying the files. Your source files are not deleted.

Last updated on 04/28/2026

Multi-Geo Capabilities in OneDrive and SharePoint

Multi-Geo capabilities in OneDrive and SharePoint enable control of shared resources like SharePoint team sites and Microsoft 365 Group mailboxes stored at rest in a specified geo location.

Each user, Group mailbox, and SharePoint site have a Preferred Data Location (PDL) which denotes the geo location where related data is to be stored. Users' personal data (Exchange mailbox and OneDrive) along with any Microsoft 365 Groups or SharePoint sites that they create can be stored in the specified geo location to meet data residency requirements. You can specify different administrators for each geo location.

Users get a seamless experience when using Microsoft 365 services, including Office applications, OneDrive, and Search. See User experience in a multi-geo environment for details.

OneDrive

Each user's OneDrive can be provisioned in or moved by an administrator to a satellite location in accordance with the user's PDL. Personal files are then kept in that geo location, though they can be shared with users in other geo locations. Administrative options found under the OneDrive tab of an active user within the Microsoft 365 admin center are currently not supported for multi-geo tenants.

SharePoint Sites and Groups

Management of the Multi-Geo feature is available through the SharePoint admin center. For configuration requirements and current steps, see Microsoft 365 Multi-Geo Tenant configuration.

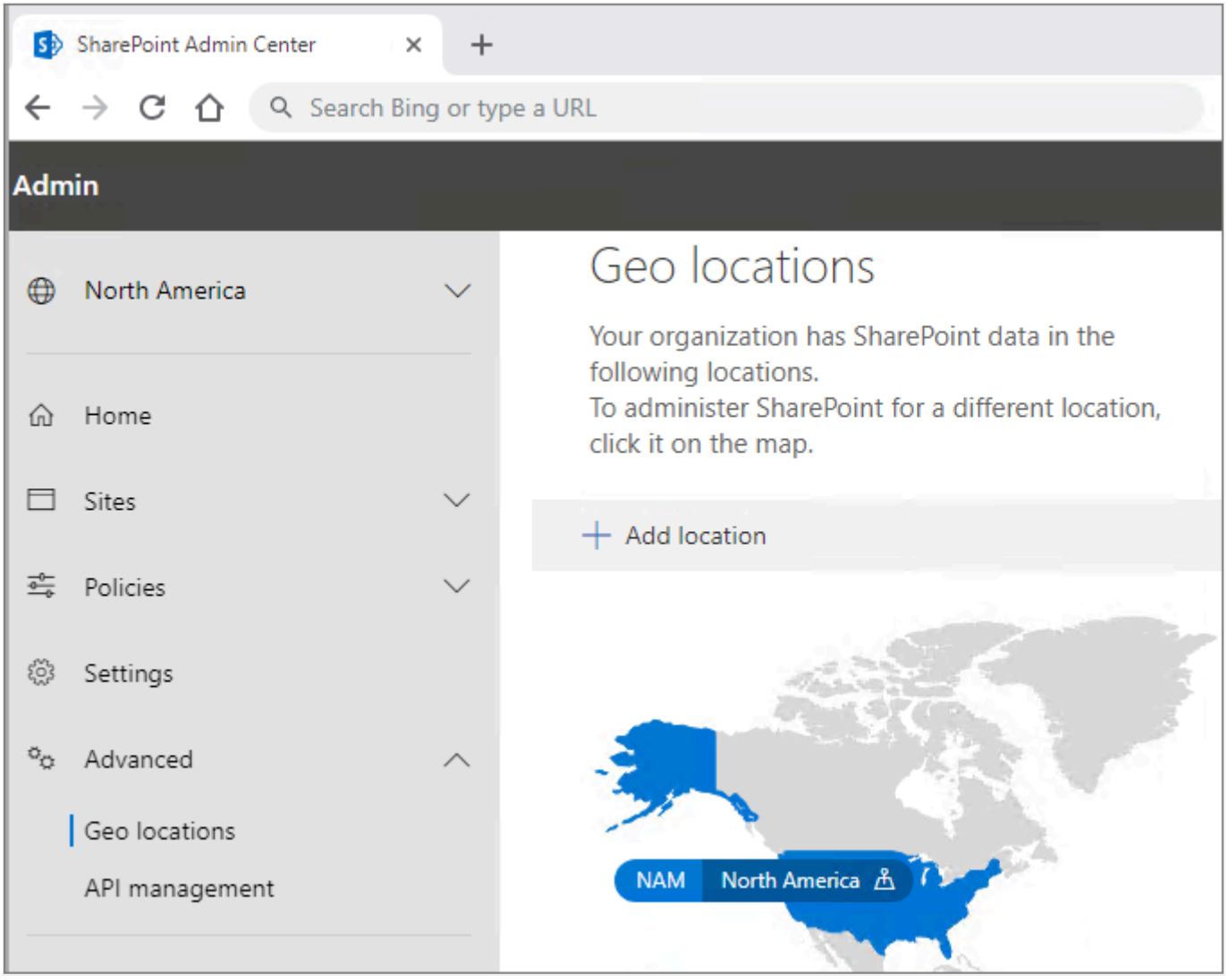
When a user creates a SharePoint group-connected site in a multi-geo environment, their PDL is used to determine the geo location where the site and its associated Group mailbox are created. (If the user's PDL hasn't been set, or if it specifies a Geography that hasn't been configured as a Satellite Geography for SharePoint and OneDrive, the site and associated group mailbox are provisioned in the Primary Provisioned Geography.)

Microsoft 365 Multi-Geo supports Exchange Online, SharePoint, OneDrive, Microsoft Teams, Microsoft 365 Copilot, and Microsoft 365 Copilot Chat. It can also be used with supported shared

resources, including SharePoint sites, Microsoft 365 Groups, shared mailboxes, Microsoft Teams teams, and eDiscovery scenarios. However, Microsoft 365 Groups that are created by these services will be configured with the PDL of the creator and their Exchange Group mailbox, and SharePoint sites are provisioned in the corresponding geo.

Managing the multi-geo environment

Setting up and managing your multi-geo environment is done through the SharePoint admin center.



Some actions, such as moving a SharePoint site or a OneDrive site require Microsoft PowerShell.

See also

Multi-Geo in SharePoint and Microsoft 365 Groups

Administering a multi-geo environment

SharePoint storage quotas in multi-geo environments

Administering Exchange Online mailboxes in a multi-geo environment

Last updated on 10/07/2026

What is SharePoint Embedded?

Applies to: All

Microsoft SharePoint Embedded is a cloud-based, API-only file and document management system you can use in any application. It lets app developers harness the Microsoft 365 file and document storage platform, and is suitable for enterprises building line-of-business applications and independent software vendors (ISVs) building multitenant applications.

SharePoint Embedded has no standalone end-user interface and doesn't offer a no-code option. You access it programmatically through Microsoft Graph, so using SharePoint Embedded always involves building or deploying an application.

SharePoint Embedded brings advanced Microsoft 365 capabilities into your app, including Office collaboration, Microsoft Purview security and compliance, and Copilot.

Is SharePoint Embedded right for you?

SharePoint Embedded fits when you're trying to do any of these tasks:

- **Store files for a multitenant SaaS app** so each customer's content stays in their own Microsoft 365 tenant.
- **Add Office co-authoring** to your app instead of building it.
- **Ground an AI agent** on enterprise content without an external vector database.
- **Run a compliant, API-only document store** with recycle bin, restore, and search.

For a full comparison with alternatives, see When to choose SharePoint Embedded.

> **Note**
>
> SharePoint Embedded isn't the same as SharePoint Online sites or document libraries, the SharePoint Framework (SPFx), OneDrive APIs, or blob storage. It's an API-only storage platform whose content lives in the customer's Microsoft 365 tenant.

> **Important**

Help us shape the future of SharePoint Embedded! Take our quick survey and share your thoughts.

Choose your path

This page is a router. Pick the row that matches what you're trying to do.

> **Tip**
>
> **Not sure which path?** Ask one question: *do you write code, or manage a tenant?* **Developers** write and deploy applications that call SharePoint Embedded APIs — start with **Build an app**. **Administrators** install, consent to, and manage SharePoint Embedded apps inside a Microsoft 365 tenant — start with **Install or manage apps**.

Expand table

I want to...	Start here
Understand SharePoint Embedded and decide if it fits	Scenarios and use cases · When to choose SharePoint Embedded
Plan a solution (architect, IT decision maker)	Plan a SharePoint Embedded solution
Build an app (developer)	Quickstart: build your first app with VS Code
Ship my app to customers (ISV / developer)	Publish and onboard customers
Install or manage apps in my tenant (admin)	Install and manage apps
Govern and secure content (compliance admin)	Apply security and compliance controls
Look something up	Reference · Graph API

Key concepts in 60 seconds

App documents stay in the customer's Microsoft 365 tenant

When a customer uses a SharePoint Embedded application, SharePoint Embedded creates a dedicated storage partition inside that customer's Microsoft 365 tenant. The partition has no user experience of its own — its documents are reachable only through Microsoft Graph APIs. Content is accessible to the developer's application, but it physically resides in the customer's tenant.

File Storage Containers

SharePoint Embedded apps store files in an entity called a **File Storage Container** (or *container*). Think of a container as an API-only document library. Your app can create many containers in each tenant that uses it, and each container can be permissioned separately and hold terabytes of content. Containers are dedicated to — and accessible only by — your app, keeping your data isolated within the tenant boundary.

To learn how containers and container types relate, see Understand container types and containers.

App-managed content experiences

By default, content stored by a SharePoint Embedded app is accessible only through that owning app, which also provides the user experience for it. You can light up rich Microsoft 365 capabilities, including:

- Core content management — any file type, folders, search, sharing, versioning, recycle bin.
- Office collaboration — view, edit, and co-author Word, Excel, and PowerPoint on the web and desktop.
- AI and agent grounding — make content discoverable to Microsoft 365 Copilot through the container type's content-discoverability setting, and search it with the Microsoft Search API scoped to your app's content.
- Low-code integration — the SharePoint Embedded connector for Power Platform (generally available February 2026).

SharePoint Embedded is used by Microsoft products (such as Loop and Designer), by ISVs embedding content management in their apps, and by enterprises storing content outside their regular Microsoft 365 entitlements.

Compliance and billing follow the tenant

Because content lives in the customer's Microsoft 365 tenant, it's subject to that tenant's settings — including Microsoft Purview compliance (eDiscovery, auditing, DLP, retention, sensitivity labels, conditional access). The SharePoint Embedded partition doesn't count against Microsoft 365 storage entitlements; it's billed separately through an Azure subscription on a pay-as-you-go, metered model based on storage and API usage. See Choose a billing model and Billing meters.

Availability

SharePoint Embedded is available in the Microsoft 365 commercial cloud, in Microsoft 365 GCC and in Microsoft 365 operated by 21Vianet for customers in China. It is not yet available in Government Community Cloud High (GCC High) or Department of Defense (DoD). See Microsoft Graph national cloud deployments.

Next steps

- New to SharePoint Embedded? Read Scenarios and use cases, then Plan a solution.
- Ready to build? Jump to the VS Code quickstart.
- Administering a tenant? Start at the Admin overview.
- See What's new for the latest releases.

ⓘ**Note:** The author created this article with assistance from AI. Learn more

---

Last updated on 08/24/2026

Service Prioritization in SharePoint

Service prioritization in SharePoint is a powerful service designed to prioritize apps within your SharePoint Online tenants, particularly those considered business-critical. By using service prioritization, organizations can ensure optimal performance, scalability, and reliability for key applications without requiring code modifications. Next, we explore what service prioritization entails and how to effectively use it within your organization.

1. What is Service Prioritization in SharePoint?

Service Prioritization in SharePoint enables businesses to assign a higher priority to their critical applications within a SharePoint environment. This prioritization ensures that these apps are the last to experience throttling in their tenant during periods of high resource usage. It allows the app to scale resource usage limits (aka.ms/SPO429) significantly—ranging from a minimum of 2x up to 10x when there are available resources. As a result, Service Prioritization enhances application reliability and delivers more consistent performance.

> **Note**
>
> Sharing limits are excluded from this offering at this time.

2. Key Benefits of Service Prioritization in SharePoint

- **Scalable Resources**: Application resource limits can exceed normal thresholds, offering up to 10 times more capacity when available.
- **No Code Changes Required**: Any app can be prioritized without requiring development or code modifications as long as they can be registered on Microsoft Graph metered APIs.
- **Pay-As-You-Go Model**: Organizations only pay for the resources they consume.

3. Metered API Classification

Service prioritization in SharePoint integrates with Azure's standard cost management experience, enabling organizations to monitor and control expenses associated with prioritized apps. For detailed reporting, refer to Microsoft’s Cost Management documentation.

To support prioritization, service prioritization in SharePoint operates on a metered API model with defined costs:

- **Standard APIs**: charged at $0.02 per 1,000 requests.
- **Heavy APIs**: charged at $0.14 per 1,000 requests.

"Heavy" APIs are those that consume a larger amount of SharePoint resources, including but not limited to resource enumeration, permissions, and downloads. If a SharePoint API is not "Heavy", it is considered "Standard".

> ⓘ **Note**
>
> All API calls to SharePoint and OneDrive are included. Price varies based on the API used per pricing above in effect as of 11/11/2025.

4. Manage Service Prioritization in SharePoint Using PowerShell

Administrators can onboard and manage service prioritization policies and app registrations using the SharePoint Online PowerShell module. Below are some key cmdlets:

- **[New-SPOServicePrioritizationBillingPolicy]**: Creates a new billing policy for service prioritization. This policy defines the billing structure for prioritized apps.
- **[Add-SPOServicePrioritizationAppRegistration]**: Registers an app for service prioritization. Requires details such as App ID, Policy ID and Quota Multiplier.
- **[Get-SPOServicePrioritizationBillingPolicies]**: Retrieves all existing billing policies for service prioritization in the tenancy.
- **[Get-SPOServicePrioritizationAppRegistrations]**: Retrieves all app registrations for service prioritization in the tenancy.
- **[Set-SPOServicePrioritizationAppRegistration]**: Updates an existing app registration for service prioritization, such as modifying the Quota Multiplier or enabling/disabling the registration.
- **[Remove-SPOServicePrioritizationAppRegistration]**: Deletes an existing app registration for service prioritization.

5. Manage Service Prioritization in SharePoint Using the Microsoft 365 Admin Center

Administrators can onboard and manage service SharePoint prioritization policies and app registrations using the Microsoft 365 admin center. Pay-as-you-go is managed in the billing in the Billing node of the Microsoft 365 admin center. Here are the main steps:

5.1. Check the pre-requisites

- To manage Service Prioritization in SharePoint, you must have the SharePoint Administrator or the Global Administrator role.
- To create a new subscription in the Microsoft 365 admin center, you must be a Billing Account Owner or a Billing Account Contributor.
- The tenant must have at least one SharePoint license, or a license that includes SharePoint.
- You must have an Azure subscription in the same tenant as Microsoft 365. If you don't have an Azure subscription, you can create one during the billing policy setup process.
- You must have an Azure resource group in that subscription. If you don't have an Azure resource group, you can create one during the billing policy setup process.
- You must have Owner or Contributor rights to the Azure subscription and resource group.

5.2. Create a billing policy

- Sign in to the Microsoft 365 admin center
- Go to Billing > Pay-as-you-go.
- On the Billing policies tab, select Add a billing policy.
- On the Billing details page, enter a name for the billing policy.
- From the Subscription drop-down list, select an existing Azure subscription, or select Create a new subscription.
- From the Resource group drop-down list, select an existing resource group, or select Create a new resource group.
- From the Region drop-down list, select a region. This selection determines where the tenant ID and usage data are stored.
- In the Choose Users screen, keep the default “all users” for the SPSP scenario.
- In the Budget screen, you can optionally create an alert when this policy reaches a limit.
- Review the pay-as-you-go billing terms of service and privacy statement, and then select the I accept the pay-as-you-go billing terms of service checkbox.

> **Note**
>
> You can't edit a subscription or resource group associated with a billing policy.

5.3. Connect the SharePoint Services Prioritization to a billing policy

- On the Review and create policy page, select a billing policy
- Select Connect your services to connect the policy
- You are redirected to the Pay-as-you-go page.
- Select the name of the service to connect (Services Prioritization in SharePoint)
- In the side panel, select the Billing policies tab.
- Find the billing policies that you want to connect to
- Select the Connection status toggle to set it to Connected.
- Select Save and then close the side panel.

5.4. Register an app for SharePoint Services Prioritization

- Go to the Pay-as-you-go page.
- Select the "Services Prioritization in SharePoint" service.
- Go to the Settings tab.
- Use the option to add an application.
- Enter the Application ID, Quota Multiplier and Billing Policy.
- Select Save and then close the side panel.

5.5. View spending for your organization

- In the Microsoft 365 admin center, go to Billing > Pay-as-you-go.
- On the Billing policies tab, select a billing policy.
- In the billing policy side panel, select the Budget tab.
- The Spending option displays data for the current month and includes a chart that displays data for the last six months.
- You can also monitor your pay-as-you-go usage and costs in Microsoft Cost Management for Azure. Ensure you have at least read access to the billing resource group.

6. Best Practices and Considerations

- Prioritize apps that are critical to your business operations to maximize the value of service prioritization in SharePoint.
- Take time to understand the limits of the service at https://aka.ms/spo429 .
- Regularly review resource usage and adjust quotas or policies as necessary to balance performance with cost efficiency.

- Applications registered for Service Prioritization will be billed for any requests (API calls) above the regular application limits defined at https://aka.ms/spo429 .

7. Related articles

- Understanding SharePoint throttling limits
- Get started with the SharePoint Online Management Shell
- Microsoft 365 pay-as-you-go services - Overview and benefits
- Microsoft 365 pay-as-you-go pricing - SharePoint in Microsoft 365
- Set up and manage pay-as-you-go billing in the Billing node of the Microsoft 365 admin center
- Create a budget for pay-as-you-go billing
- Microsoft 365 pay-as-you-go terms of service - SharePoint in Microsoft 365
- Microsoft Cost Management documentation

Last updated on 10/15/2026

Restricted SharePoint Search

> **Important**
>
> Restricted SharePoint Search is retiring. Starting July 31, 2026, new enablement is blocked. Use comprehensive data controls such as Restricted Content Discovery (RCD) for content discoverability.

Restricted SharePoint Search is designed for customers of Microsoft 365 Copilot chat and agentic experiences. It's a short-term solution that gives your organization's administrators time to review and audit site and file permissions. It's not intended or scalable for long-term use. Comprehensive data security solutions are available, including SharePoint Advanced Management and Microsoft Purview.

What is Restricted SharePoint Search?

Restricted SharePoint Search is a setting that you, as a SharePoint Administrator or other Microsoft 365 administrator, use to maintain a list of SharePoint sites (an "allow list") for which you check permissions and apply data governance. The allow list defines which SharePoint sites can be used in organization-wide search queries. As a temporary measure, it also applies to Copilot chat and agentic experiences.

By default, the Restricted SharePoint Search setting is turned off and the allow list is empty. If you turn on Restricted SharePoint Search, users can interact with files and content they own or previously accessed in Copilot.

How to use Restricted SharePoint Search

Use Restricted SharePoint Search as a temporary measure to prevent certain content on SharePoint sites from being shared too widely. This feature lets you as an administrator decide which SharePoint sites appear in search results across your organization and Copilot chat or agentic experiences. However, it's important to note that Restricted SharePoint Search isn't a security boundary and doesn't change any permissions on SharePoint sites.

Restricted SharePoint Search doesn't guarantee that only sites on the allow list show up in search or in Copilot chat and agentic experiences. If a user recently accessed a site, or the site was

shared with that user in Teams or Outlook, the site appears in the user's results and responses, even if it's not on the allow list.

Recommended process:

1. If you use Restricted SharePoint Search, use it to temporarily help limit results in search or Copilot chat and agentic experiences. Keep in mind that it's not intended to be a long-term solution.
2. Use SharePoint Advanced Management to identify and remediate oversharing risks, such as broad access and unmanaged sharing.
3. Use Microsoft Purview to apply data security and AI governance controls with sensitivity labels, data loss prevention (DLP), and auditing.
4. After you validate permissions and governance controls, disable Restricted SharePoint Search.
5. Notify Copilot agent owners and your IT team that Copilot and agentic responses use existing SharePoint permissions. Users' search and Copilot responses can change after Restricted SharePoint Search is disabled, so it's important to keep them informed.

Why disable Restricted SharePoint Search after validation?

Restricted SharePoint Search is designed as a temporary measure, not a long-term solution. If you keep Restricted SharePoint Search enabled, the user experience is affected in the following ways:

- Restricted SharePoint Search limits to 100 sites, which isn't sustainable as your organization scales Copilot and agentic operations.
- Search results are limited to sites on the allow list, users' frequently visited sites, sites that users have permissions to, and users' recently accessed files. Restricted SharePoint Search affects the overall search experience, even for users who aren't using Copilot chat or agents.
- When Restricted SharePoint Search is enabled, Copilot has less information available to reference, which can affect its ability to provide accurate and comprehensive responses.

Disabling Restricted SharePoint Search enables Copilot chat and agentic experiences to rely on standard permission-based access, rather than a restricted hub-site scope. This configuration

helps Copilot chat and agents retrieve SharePoint content with more consistency and accuracy, while still respecting the permissions set on SharePoint sites.

Neither Copilot nor Restricted SharePoint Search prevents users from accessing content they own or previously accessed.

How does Restricted SharePoint Search work?

As a SharePoint Administrator or other Microsoft 365 administrator, you can:

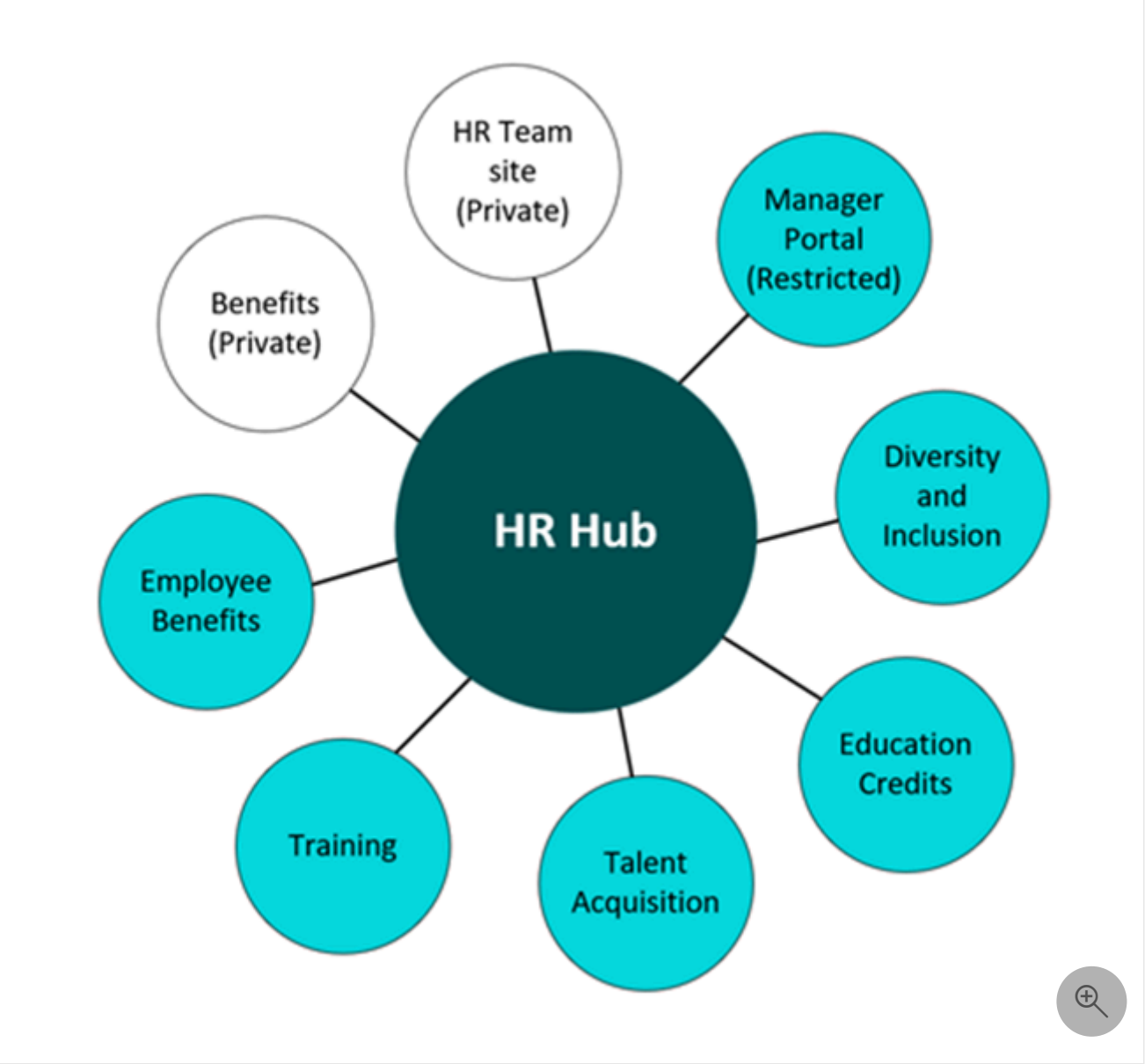
- Check the current status of Restricted SharePoint Search to see if it's enabled or disabled.
- Enable or disable Restricted SharePoint Search (it's disabled by default).
- Curate the allowed list by identifying the top 100 widely used sites.
- Add or remove sites from the allowed list by providing the site URL.
- Get the full list of sites in the allowed list.

Restricted SharePoint Search is off by default. If you decide to enable it, users who search for content or use Copilot chat and agentic experiences can expect responses to surface content from the following sources:

- An allowed list of curated SharePoint sites (with *up to 100 SharePoint sites*), honoring existing site permissions.
- Users' OneDrive files, chats, emails, and calendars they have access to.
- Files from users' frequently visited SharePoint sites.
- Files that were shared directly with users.
- Files that users viewed, edited, or created.

> **Note**
>
> - The allowed list limit of up to 100 SharePoint sites includes Hub sites, but not their associated sites. When you enable Hub sites, the associated sites of a Hub site are included in the allowed list, but they don't count towards the 100-site limit. This approach allows for greater flexibility while still adhering to the existing constraints.
> - When you're picking Hub sites, make sure all the associated sites have proper permissions.
> - The total number of files included from the last three bullet points (frequently visited sites, files shared directly with the user, and files the users viewed, edited, or created) is limited to the last 2,000 entities.

The following diagram shows an example of an HR Hub site with eight associated sites:



In the preceding diagram, all eight associated sites plus the HR Hub site are counted as one site in the allowed list.

Example: Contoso Electronics before and after using Restricted SharePoint Search

Let's consider Alex Wilber, a marketing specialist at Contoso Electronics. Before Alex's organization uses Restricted SharePoint Search, Alex can see not only his own personal contents, like his OneDrive files, chats, emails, contents that he owns or visited, but also content from some sites that haven't undergone access permission review or Access Control Lists (ACL) hygiene, and doesn't have data governance applied. For example, Contoso Electronics has a budgeting site with important business information. Most people don't know about this site, so the site owner hasn't set up proper permissions and hasn't followed correct data governance process. The site

might be open to some users who aren't allowed to see it, such as Alex. When Alex asks Copilot for some budgeting information, Copilot gets information from the budgeting site.

The IT administrator at Contoso Electronics sets up Restricted SharePoint Search to limit what sites can be searched through the allowed list. After reviewing reports, the IT administrator decides to exclude the budgeting site from the allowed list. But even though Restricted SharePoint Search is now turned on, Alex can still access things that he owns or has recently visited, or that are directly shared with him. He just can't access any other sites, unless the site is in the allowed list and he has permission to it. Now, when Alex asks Copilot the same questions about budgeting, Copilot chat and agentic experiences don't show information from that site.

From here, Contoso Electronics administrators plan to use SharePoint Advanced Management and Microsoft Purview, and eventually, disable Restricted SharePoint Search.

> **Note**
>
> Site scoped searches aren't affected by this control. This control impacts modern search and Copilot experiences.

Frequently asked questions

Can I use RSS for creating a "deny list" instead?

No, this capability isn't part of Restricted SharePoint Search. However, SharePoint Advanced Management offers a similar feature called Restricted Access Control for SharePoint sites. If you're not ready to use SharePoint Advanced Management, you can consider specifying whether to allow specific sites to show up in search results. For more information, see Allow this site to appear in Search results.

> **Note**
>
> If you turn off the "Allow this site to appear in Search results" setting, you block the site content from showing up in both the organization-wide search and the site specific search.

Does Restricted SharePoint Search affect other services that don't depend on SharePoint, such as Exchange, To Do, Planner, Loop, etc.?

Yes, any product where Enterprise Search is enabled and could have SharePoint content and/or files as search results will be impacted.

Does Restricted SharePoint Search affect other features based on the Microsoft Index, such as Purview or SharePoint Advanced Management features?

No, Restricted SharePoint Search won't affect any other features based on the Microsoft Index.

How do I enable Restricted SharePoint Search?

You can enable Restricted SharePoint Search by using PowerShell scripts. For detailed steps, see Enable or disable Restricted Search.

After enabling RSS, how long does it take to go into effect?

RSS goes into effect within an hour after it's enabled.

If I give the URL of a hub site, will it also include all of the child sites or sites associated hub sites with it? Do these other sites count towards the 100 sites in the allowed lists?

Only the hub site (the URL in the Allowed list) is included in the 100. The sub sites under the hub site aren't counted against the 100 limit but RSS is effective on the sub sites.

Next steps

1. If you decide to use Restricted SharePoint Search, start by curating the allowed list of sites. You can identify the top 100 widely used sites in your organization by using reports in the SharePoint admin center or by running the Get-SPOSite PowerShell cmdlet.

2. After curating the allowed list, enable Restricted SharePoint Search by using the Enable-SPORestrictedSearch PowerShell script.

3. Monitor the impact of Restricted SharePoint Search on your organization by evaluating the SharePoint sites activities and usage reports.

4. Work with site owners and admins to review permissions and apply data governance on the sites in the allowed list. You can use SharePoint Advanced Management to set up advanced

access policies and advanced site content lifecycle management for specific users and groups.

5. Use Microsoft Purview to apply data security and AI governance controls with sensitivity labels, data loss prevention (DLP), and auditing for the sites in the allowed list.

6. After you've validated permissions and governance controls for the sites in the allowed list, disable Restricted SharePoint Search by using the Disable-SPORestrictedSearch PowerShell script.

7. Notify Copilot agent owners and your IT team that Copilot and agentic responses now use existing SharePoint permissions without the restrictions of the allowed list. Responses can change once Restricted SharePoint Search is disabled, so it's important to keep them informed.

Last updated on 07/06/2026

Curate the allow list for Restricted SharePoint Search

> **Important**
>
> Restricted SharePoint Search is retiring. Starting July 31, 2026, new enablement is blocked. Use comprehensive data controls such as Restricted Content Discovery (RCD) for content discoverability.

Restricted SharePoint Search is designed for customers of Microsoft 365 Copilot chat and agentic experiences. It's designed as a short-term solution to allow time for your organization's administrators to thoroughly review and audit site and file permissions, but it's not intended or scalable for long-term use. Comprehensive data security solutions are available, including SharePoint Advanced Management and Microsoft Purview.

As a SharePoint Administrator or other administrator in Microsoft 365, you can set up an allow list of Restricted SharePoint Search with a maximum of 100 selected SharePoint sites. For Copilot and organization-wide search, besides the contents that users already have access to, either by direct sharing, visiting, or owning, your organization's users can only reach the sites on the allow list, honoring these sites' current permissions.

Setting up the allow list in Restricted SharePoint Search gives you time to review and audit site permissions. But which sites should you include in the allow list? This article introduces strategies and techniques for curating the allow list.

Steps to create the curated allow list

To create a curated allow list for Restricted SharePoint Search, start by creating an initial list of sites. Then work with your site admins and stakeholders to assess permissions and review the sites. Finally, apply the list with PowerShell scripts as a SharePoint Administrator or above in Microsoft 365.

Step 1: Get an initial list of sites

Every organization might have different criteria on what sites you choose to be searched across your organization and discoverable by Copilot. You can use SharePoint Admin Center (SPAC)

features to identify sites that can be part of the allow list based on your own criteria. To keep the list manageable, start with the following two types of sites for the allow list:

- **The "Known" sites**: You and your SharePoint site admins already know a set of sites from your organization that are safe to participate in organization wide search and the Copilot experience. Include these sites in the allow list.
- **The top active and shared sites**: The allow list affects what users can see in their organization-wide search results and their Copilot experience. To optimize users' search and Copilot experience, include the top active and shared sites in the allow list. Depending on your license, you can use either the SharePoint Admin Center (SPAC) or the SharePoint Admin Center Data access governance (DAG) Activity(sharing) report to identify the most active and shared sites.

Step 2: Review site permissions

Once you have the list of sites (up to 100), make sure the site permissions and content controls are implemented well enough to make them visible for search and Copilot experience. Work with your site admins and stakeholders to assess permissions and review the sites.

> ⓘ **Note**
>
> The limit of up to 100 SharePoint sites includes Hub sites, but not their sub-sites. When you enable Hub sites, the sub-sites under a Hub site are included in the allow list but don't count towards the 100-site limit. So if you're picking Hub sites, make sure all the child sites have proper permissions.

Step 3: Use PowerShell scripts to apply the allow list

After you review permissions in your curated sites, use PowerShell scripts to turn on Restricted SharePoint Search, add sites, and remove sites. You can also use PowerShell scripts to get the list of all sites in your allow list.

Find the most active and shared sites

You can find the most active sites by using the SharePoint Admin Center (SPAC). If you have either Microsoft 365 E5 licensing or Microsoft - SharePoint Advanced Management, you can also use SPAC DAG to find the most shared sites.

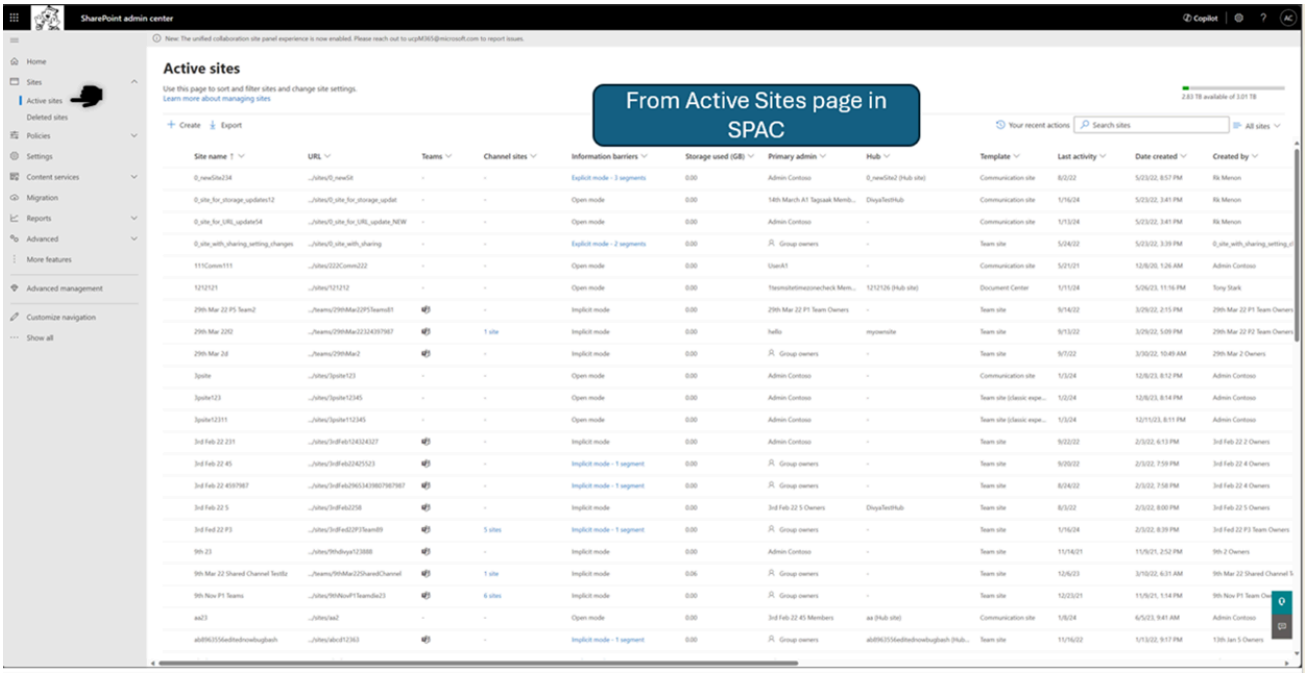
- **Using the SharePoint admin center:** If your organization has SharePoint, you have access to SharePoint admin center. Use the Active sites feature in the SharePoint admin center to get the list of sites that had the most page views and files in the last 30 days. This activity can indicate the list of sites that interest the broadest possible audience in the organization.

- **Using the data access governance activity (sharing) report** to identify sites that are shared most in the last 28 days.

Use the SharePoint admin center to find the most active sites

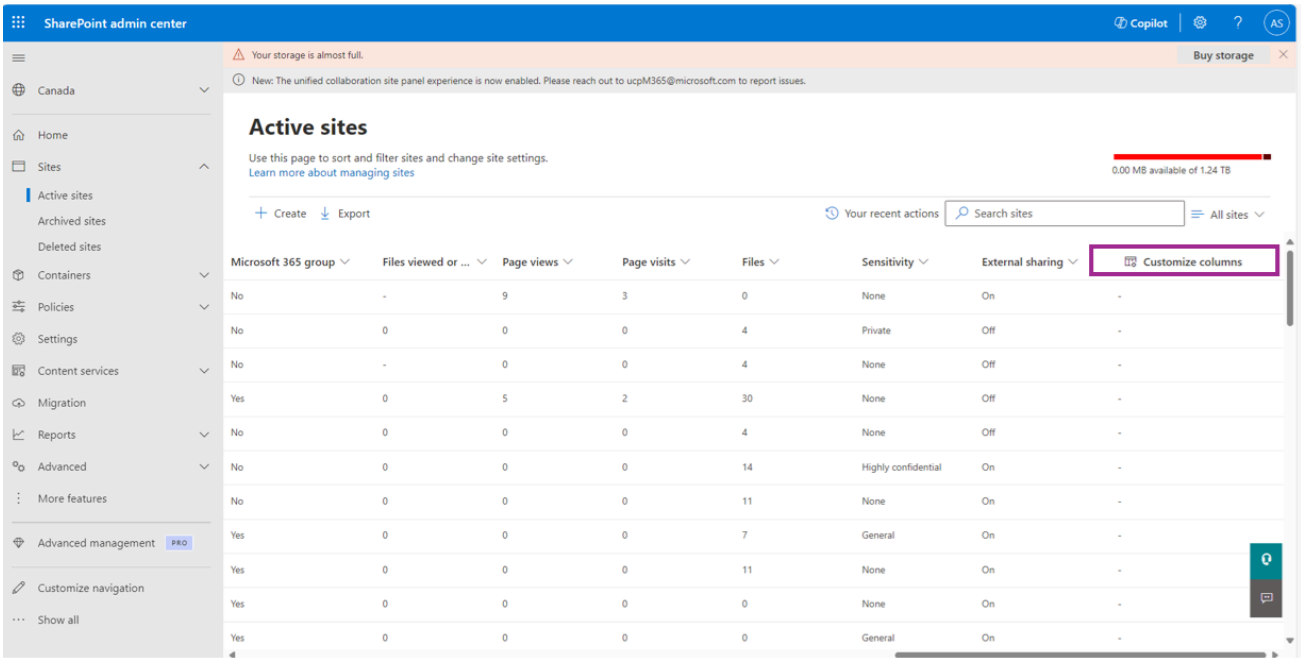
Admins can use the SharePoint admin center features to identify sites that can be part of the allow list based on their criteria. The Active sites page in the SharePoint admin center lets you view the SharePoint sites in your organization. Based on your organization's needs, you can sort and filter sites based on columns such as Last activity, Page views, and Page visits. You can search for sites, and customize the columns and views.

1. In the SharePoint admin center, in the navigation pane, select **Active Sites**.

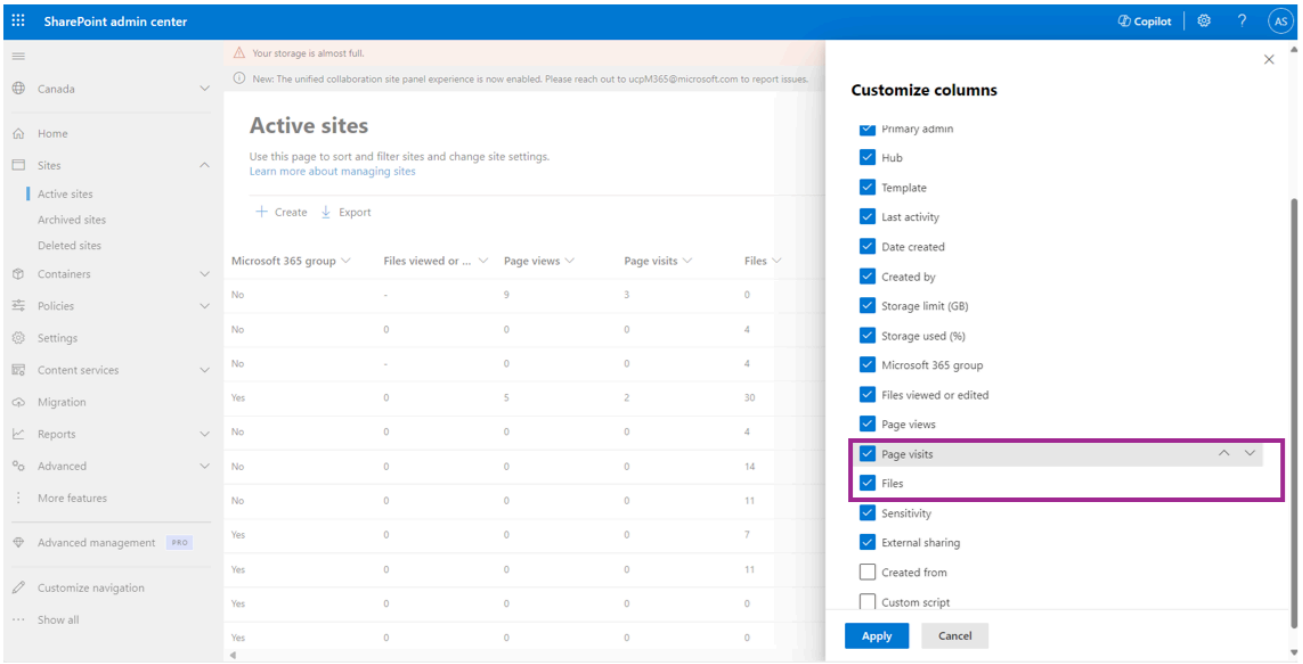


2. Using the sorting and filtering functionality of the Active sites you can curate top 100 sites based on your organization needs and create a custom view.

3. Move the columns by scrolling to right and selecting **Customize columns**.



Use the up and down arrows next to each column's name to move up the Page Views and Files columns next to the URL, so it's easy for you to see the important columns together for analysis.

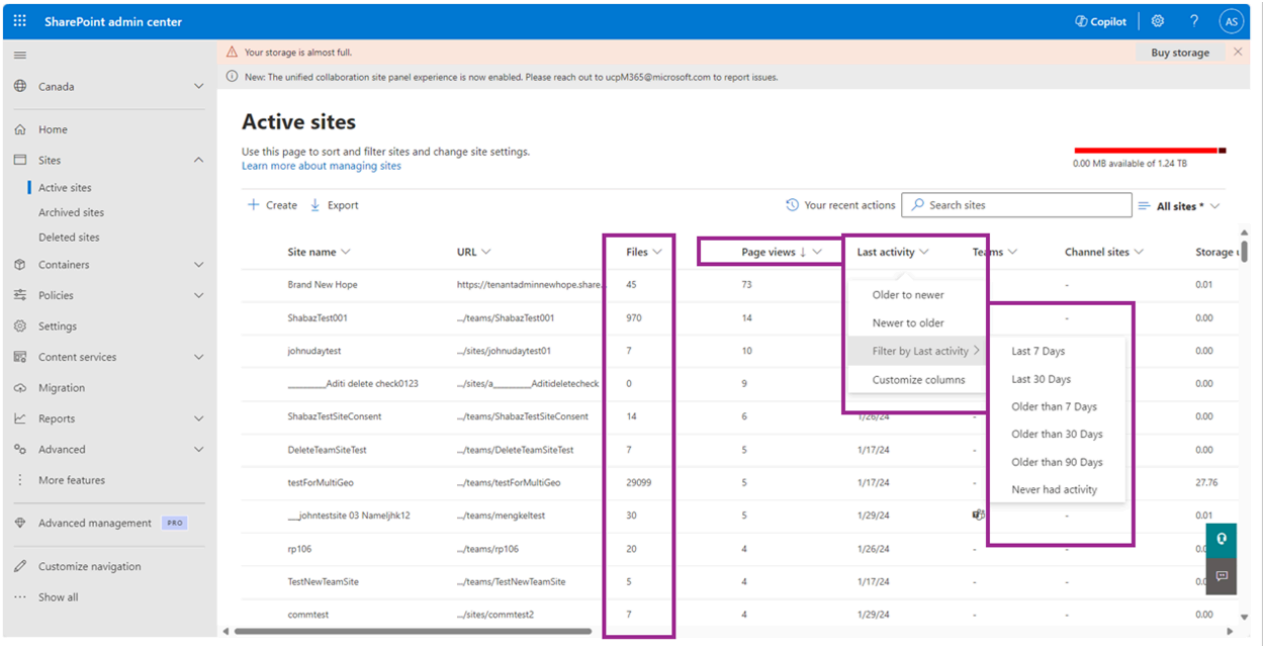


4. To create custom view of the top 100 sites sorted by **page views** for last 30 days, follow these steps:

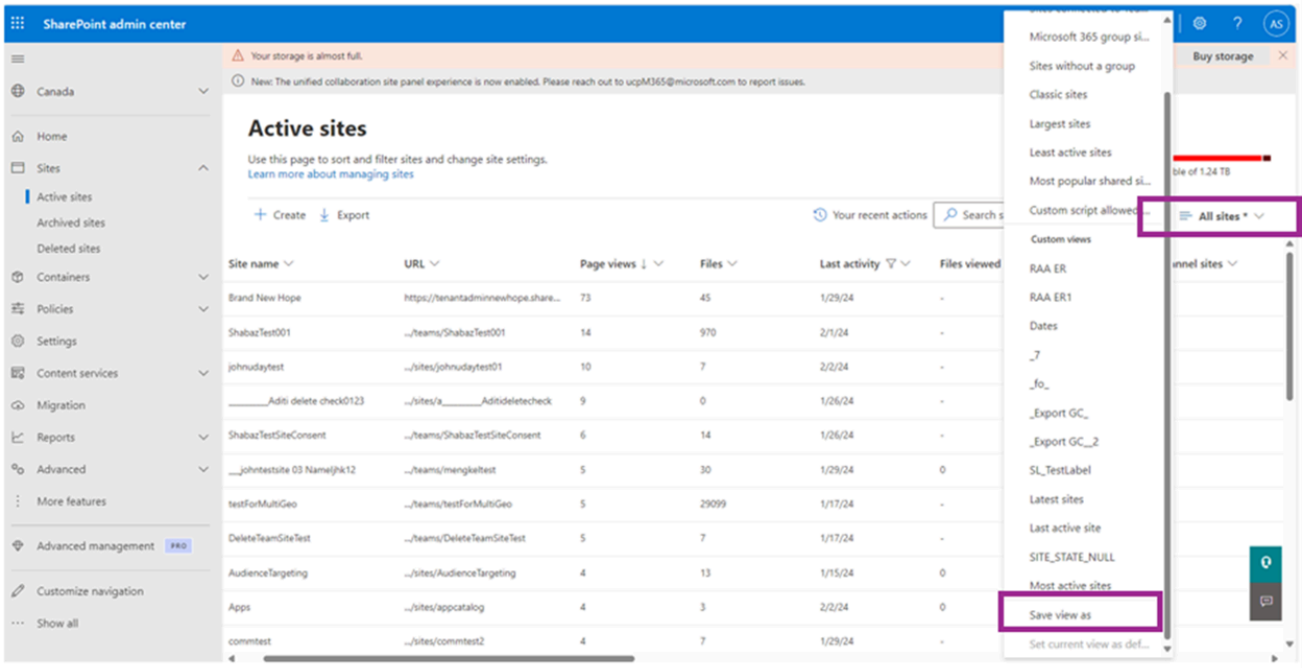
   a. Select the arrow next to the column header of **Page views** and select **Large to Small**.

   b. Select the arrow next to the column header of **Last activity** select on the **Filter by last activity** > **Last 30 days**.

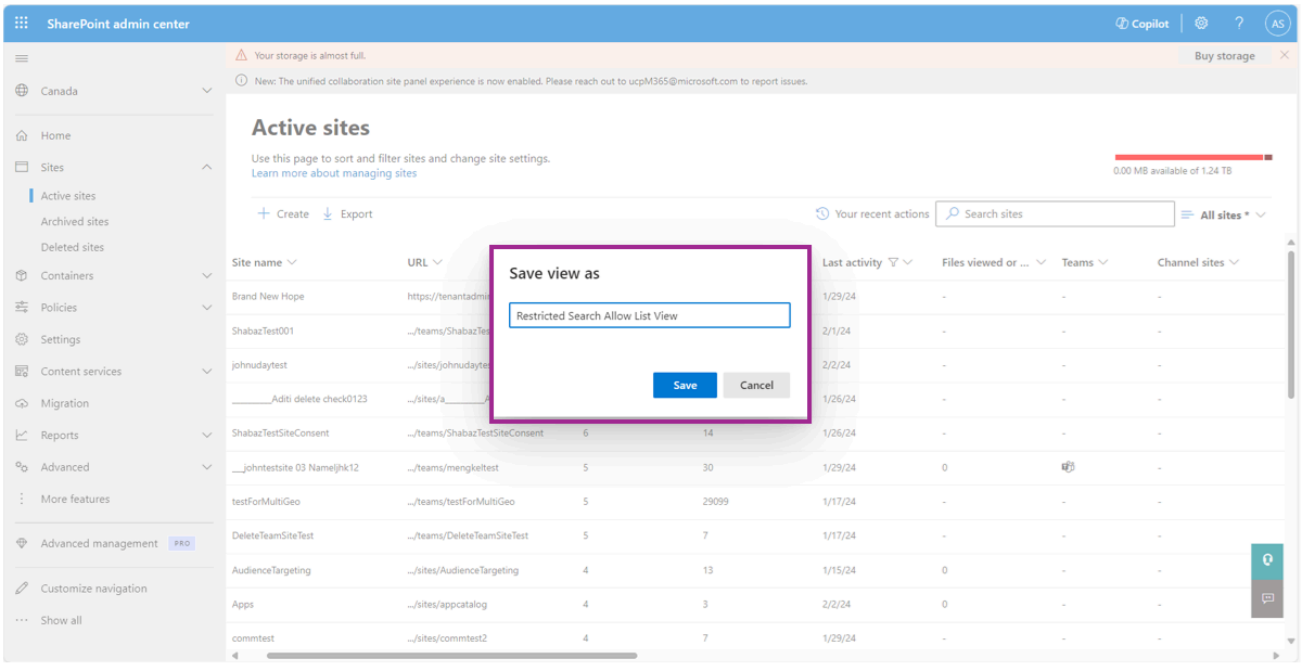
   c. Use the other columns to sort, or filter based on your needs.



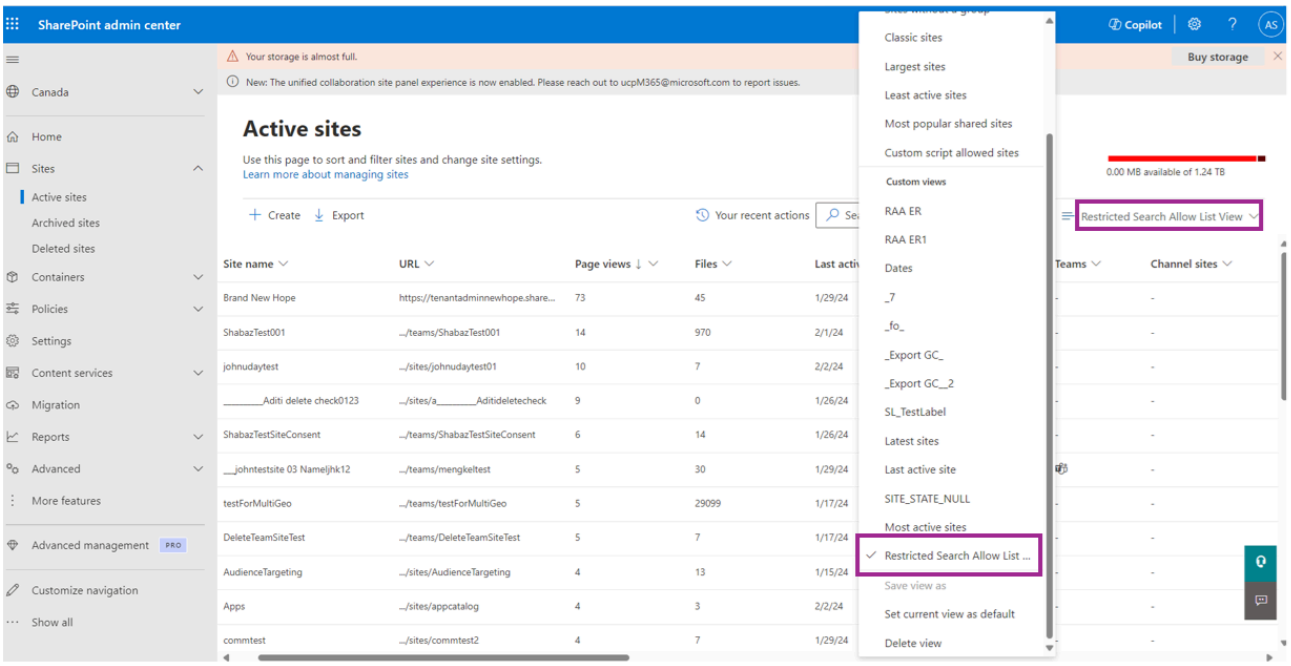
5. Create a custom view based on your current setting, and save it for future use. To create a custom view, select **All sites** > **Save view as**.



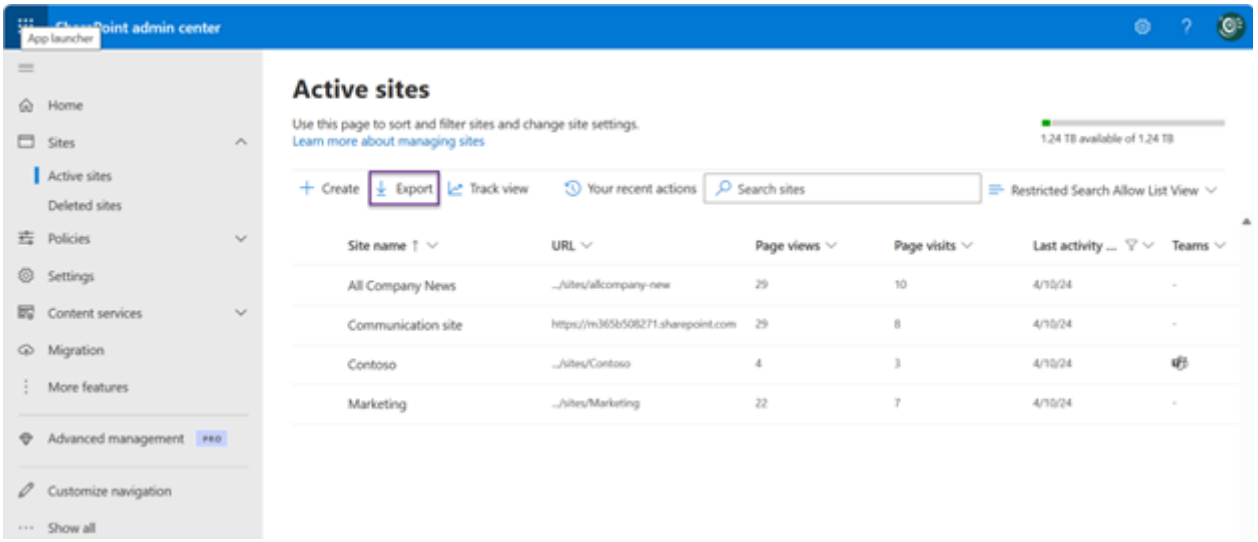
6. Specify a name for your custom view:



Your saved custom view is now available for you to choose from the drop-down menu next time.



7. Export the sites and manage the list in CSV file that you can use to add to the list by selecting the **Export** tab.



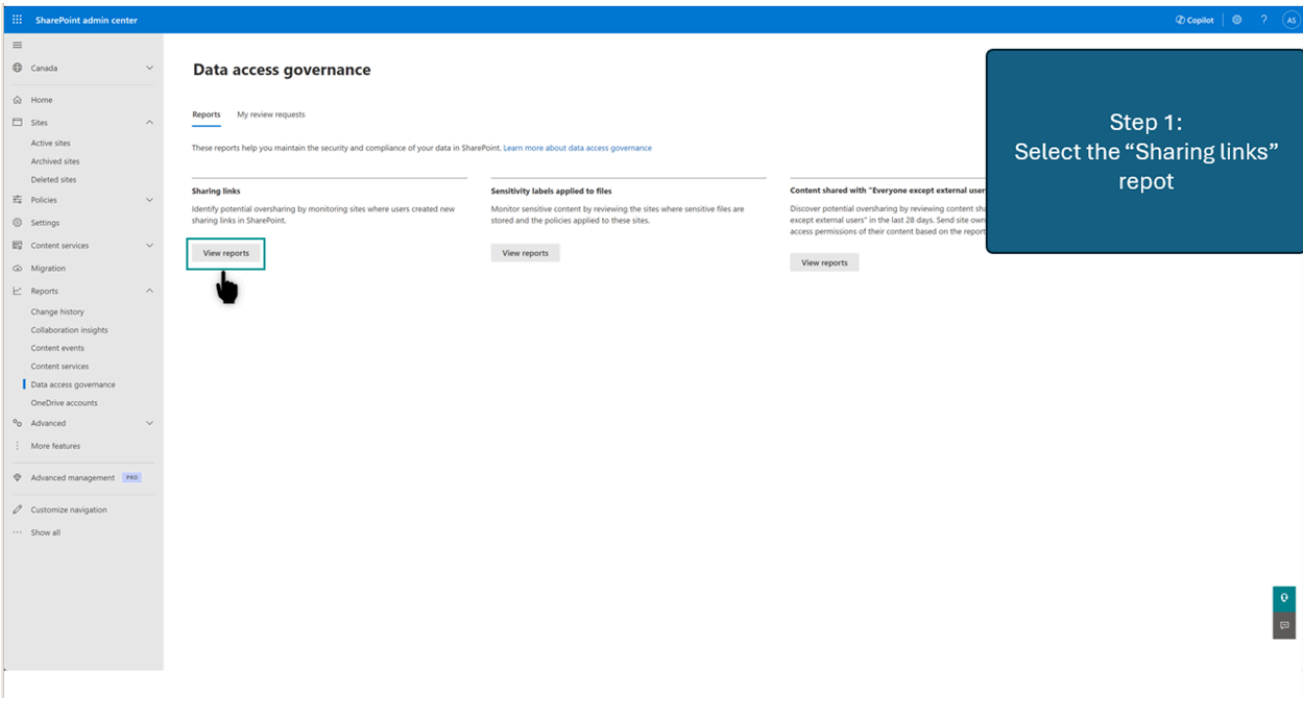
Your exported CSV file looks similar to the following CSV file:

A	B	C	D	E	F	G	H	I
"Site name'	URL	Page views	Files	Last activity (UTC)	Files viewed or edited	Teams	Channel sit	Storage
Brand New	https://tenantadminnewhope.sharepoint.com	73	45	1/29/2024 5:00		FALSE		0.
ShabazTest	https://tenantadminnewhope.sharepoint.com/teams/ShabazTest001	17	970	2/5/2024 5:00		FALSE		
johnudayte	https://tenantadminnewhope.sharepoint.com/sites/johnudaytest01	10	7	2/2/2024 5:00		FALSE		
_____A	https://tenantadminnewhope.sharepoint.com/sites/a_____Aditideletechec	9	0	1/26/2024 5:00		FALSE	0	
TestNewTe	https://tenantadminnewhope.sharepoint.com/teams/TestNewTeamSite	7	5	2/5/2024 5:00		FALSE		
ShabazTest	https://tenantadminnewhope.sharepoint.com/teams/ShabazTestSiteConsent	7	14	2/5/2024 5:00		FALSE		
__johntest	https://tenantadminnewhope.sharepoint.com/teams/mengkeltest	5	30	1/29/2024 5:00	0	TRUE		0.
testForMult	https://tenantadminnewhope.sharepoint.com/teams/testForMultiGeo	5	29099	1/17/2024 5:00		FALSE		27.
DeleteTean	https://tenantadminnewhope.sharepoint.com/teams/DeleteTeamSiteTest	5	7	1/17/2024 5:00		FALSE		
rp106	https://tenantadminnewhope.sharepoint.com/teams/rp106	5	20	2/5/2024 5:00		FALSE		0.
AudienceTa	https://tenantadminnewhope.sharepoint.com/sites/AudienceTargeting	4	13	1/15/2024 5:00	0	FALSE		
Apps	https://tenantadminnewhope.sharepoint.com/sites/appcatalog	4	3	2/2/2024 5:00	0	FALSE		
commtest	https://tenantadminnewhope.sharepoint.com/sites/commtest2	4	7	1/29/2024 5:00		FALSE		

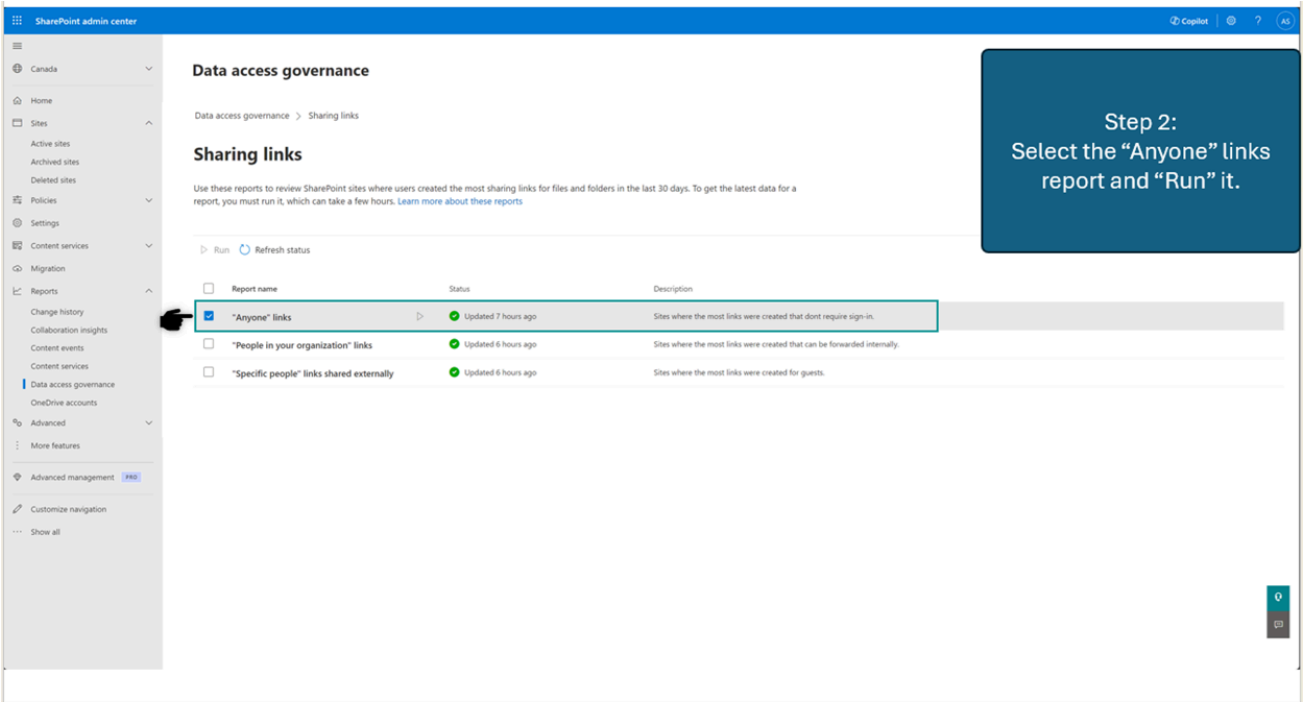
Use the data access governance activity (sharing) report to find most shared sites

SharePoint Advanced Management includes data access governance reports for SharePoint sites. This report helps you identify potential sites that are active and shared in the last 28 days.

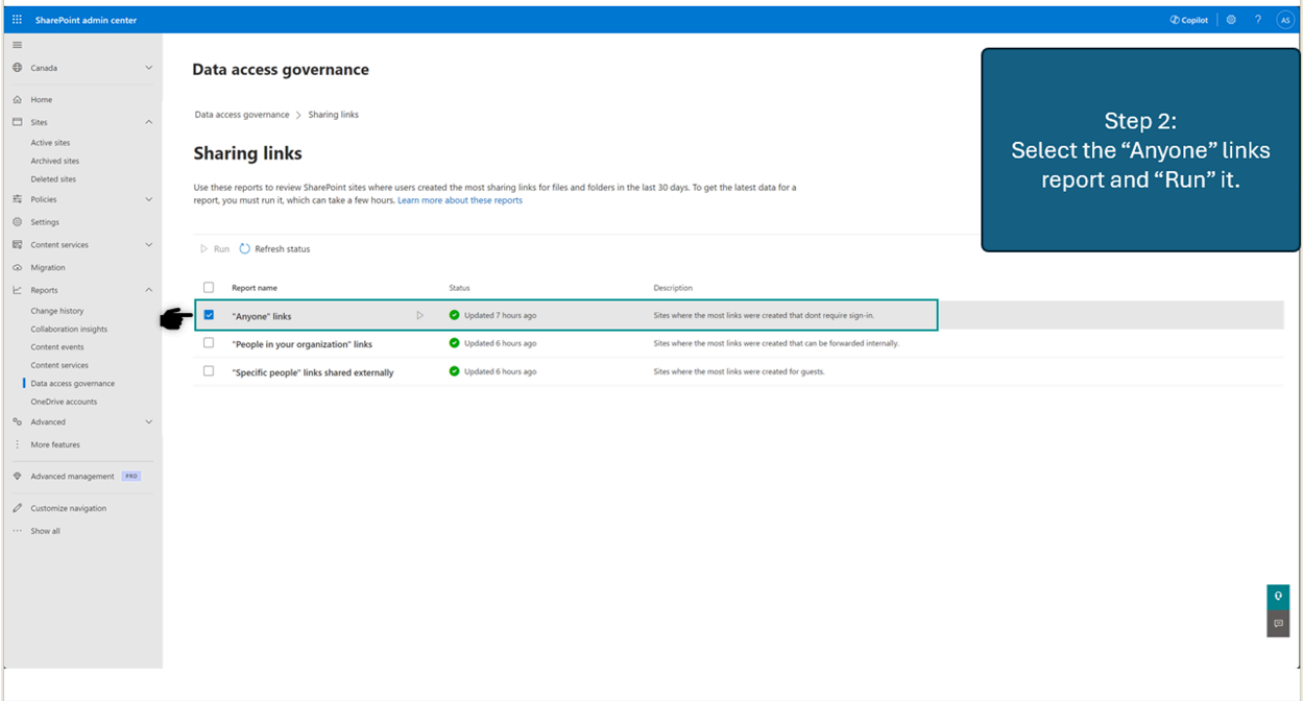
1. In the SharePoint admin center, select **Reports** > **Data access governance**. Select the **Sharing links** report.



2. In the pane of the **Sharing Links** page, select the **Anyone links** report.



3. The **"Anyone" links** report gives you a list of sites in which the highest number of **Anyone** links were created. These links let anyone access files and folders without signing in. These sites might be great candidates to allow in tenant/org wide search.



Resources

Get ready for Microsoft 365 Copilot with SharePoint Advanced Management

---

Last updated on 07/06/2026

Use PowerShell scripts for restricted SharePoint Search

> **Important**
>
> Restricted SharePoint Search is retiring. Starting July 31, 2026, new enablement is blocked. Use comprehensive data controls such as Restricted Content Discovery (RCD) for content discoverability.

Restricted SharePoint Search is designed for customers of Microsoft 365 Copilot chat and agentic experiences. It's designed as a short-term solution to allow time for your organization's administrators to thoroughly review and audit site and file permissions, but it's not intended or scalable for long-term use. Comprehensive data security solutions are available, including SharePoint Advanced Management and Microsoft Purview.

How to enable and manage restricted SharePoint Search by using PowerShell scripts

By default, Restricted SharePoint Search isn't enabled. To enable and set up restricted SharePoint Search, you need to have at least the permissions of a SharePoint Administrator in Microsoft 365. Depending on the scenario, some actions you need to take are:

- Get the current mode of restricted Search
- Enable and disable restricted Search
- Add sites to the allowed list by providing URL
- Remove sites from the allowed list by providing URL
- Get the existing list of URLs that are added in allow list

This article covers how to use admin scripts in PowerShell for these actions.

Before you begin

You must be a SharePoint Administrator or have equivalent permissions in Microsoft 365 to run the PowerShell admin scripts.

See Prerequisites for SharePoint Advanced Management.

Before you use the PowerShell scripts in this article, see SharePoint Online PowerShell module requirements.

Get the current mode of Restricted SharePoint Search

Restricted SharePoint Search is disabled by default. To verify this feature's current mode, you can run the following command:

PowerShell

```
Get-SPOTenantRestrictedSearchMode
```

Module: Microsoft.Online.SharePoint.PowerShell

Applies to: SharePoint Online

Syntax

PowerShell

```
Get-SPOTenantRestrictedSearchMode
```

Example

PowerShell

```
Get-SPOTenantRestrictedSearchMode
```

This example lets the admin get the existing allowed list in the tenant. Result can be "Enabled" or "Disabled" based on the current setting.

Enable or disable Restricted Search

Enable or disable the Restricted Search setting. The default is disabled. The first time you enable the setting, the allow list is empty. To enable or disable the Restricted SharePoint Search, run this command:

PowerShell

```
Set-SPOTenantRestrictedSearchMode
```

Module: Microsoft.Online.SharePoint.PowerShell

Applies to: SharePoint Online

Syntax

PowerShell

```
Set-SPOTenantRestrictedSearchMode
[-Mode] {Disabled | Enabled}
 [<CommonParameters>]
```

Example 1

PowerShell

```
Set-SPOTenantRestrictedSearchMode -Mode Enabled
```

> **Note**
>
> Once enabled, any new sites are excluded unless you add them to the allow list.

Example 1 sets or enables the Restricted Tenant Search mode for the tenant.

Example 2

PowerShell

```
Set-SPOTenantRestrictedSearchMode – Mode Disabled
```

Example 2 disables the Restricted Tenant Search mode for the tenant.

Parameters

`-Mode`

Sets the mode for the Restricted Tenant Search.

Expand table

Type	String
Position:	`0`
Default Value:	`Disabled`

Type	String
Required:	`True`
Accept Pipeline input:	`False`
Accept wildcard characters:	`False`

Add sites to the allow list

When you enable Restricted SharePoint Search, add site URLs to the allow list in a string or CSV file by using this command:

PowerShell

```
Add-SPOTenantRestrictedSearchAllowedList
```

Module: Microsoft.Online.SharePoint.PowerShell

Applies to: SharePoint Online

Syntax

PowerShell

```
Add-SPOTenantRestrictedSearchAllowedList -SitesList <List[string]>
[<CommonParameters>]
```

PowerShell

```
Add-SPOTenantRestrictedSearchAllowedList -SitesListFileUrl <string> [-ContainsHeader
<bool>]
 [<CommonParameters>]
```

Example 1

PowerShell

```
Add-SPOTenantRestrictedSearchAllowedList -SitesList @("
[https://contoso.sharepoint.com/sites/Marketing]
(https://contoso.sharepoint.com/sites/Marketing)", "
[https://contoso.sharepoint.com/sites/Benefits]
(https://contoso.sharepoint.com/sites/Benefits)")
```

This example shows the admin how to add the sites to the allow list.

Example 2

PowerShell

```
Add-SPOTenantRestrictedSearchAllowedList  -SitesListFileUrl
C:\Users\admin\Downloads\UrlList.csv
```

> **Note**
>
> To generate a list of all your SharePoint site URLs, go to your SharePoint online admin center, go to **Active Sites**, and select **export**. The exported list includes classic sites as well. Remove any sites from this list that you don't want indexed. You can include up to 100 URLs.

This example shows the admin how to add the sites to the allow list by providing a CSV file. Add the list of site URLs in the URL column.

Parameters

`-SitesList`

Site list for allow list.

Expand table

Type	String
Position:	`0`
Default Value:	`None`
Required:	`True`
Accept Pipeline input:	`False`
Accept wildcard characters:	`False`

`-SitesListFileURL`

File that has list of site URLs that you can add to an allow list when the tenant is set to Restricted Tenant Search Mode.

Expand table

Type	String
Position:	`0`
Default Value:	`None`
Required:	`True`
Accept Pipeline input:	`False`
Accept wildcard characters:	`False`

Remove sites from the allow list

Remove sites from the allow list by providing the site URL in a string or CSV file by using the following PowerShell command:

PowerShell

```
Remove-SPOTenantRestrictedSearchAllowedList
```

Module: Microsoft.Online.SharePoint.PowerShell

Applies to: SharePoint Online

Syntax

PowerShell

```
Remove-SPOTenantRestrictedSearchAllowedList -SitesList <List[string]>
[<CommonParameters>]
```

PowerShell

```
Remove-SPOTenantRestrictedSearchAllowedList -SitesListFileUrl <string> [-
ContainsHeader <bool>]
 [<CommonParameters>]
```

Example 1

PowerShell

```
Remove-SPOTenantRestrictedSearchAllowedList -SitesList @("
[https://contoso.sharepoint.com/sites/Marketing]
```

```
(https://contoso.sharepoint.com/sites/Marketing)", "
[https://contoso.sharepoint.com/sites/HR](https://contoso.sharepoint.com/sites/HR)")
```

Example 1 shows how the admin removes the sites from the allow list.

Example 2

PowerShell

```
Remove-SPOTenantRestrictedSearchAllowedList -SitesListFileUrl
C:\Users\admin\Downloads\UrlList.csv
```

Example 2 shows how the admin adds the sites to the allow list by providing a CSV file.

Parameters

`-SitesList`

Site list that you want to remove from the allow list.

Expand table

Type	String
Position:	`0`
Default Value:	`None`
Required:	`True`
Accept Pipeline input:	`False`
Accept wildcard characters:	`False`

`-SitesListFileURL`

File that has list of sites that you can remove from an allow list when the tenant is set to Restricted Tenant Search Mode.

Expand table

Type	String
Position:	`0`
Default Value:	`None`

Type	String
Required:	`True`
Accept Pipeline input:	`False`
Accept wildcard characters:	`False`

Get the existing list of URLs in the allow list

To get the existing list of URLs in the allow list, run the following PowerShell command:

PowerShell

```
Get-SPOTenantRestrictedSearchAllowedList
```

Module: Microsoft.Online.SharePoint.PowerShell

Applies to: SharePoint Online

Syntax

PowerShell

```
Get-SPOTenantRestrictedSearchAllowedList
```

Example

PowerShell

```
Get-SPOTenantRestrictedSearchAllowedList
```

This example shows how the admin gets the existing allow list in the tenant.

Last updated on 07/06/2026