Microsoft

Office 365 SharePoint Assessment: Prerequisites and Configuration

This document explains the required steps to configure the Office 365 SharePoint Assessment.

Currently the data collection process is performed using the Offline Assessment Client, that requires a data collection machine.

Data collection machine

This scenario can be used when the data collection machine can connect to the Office 365 tenant directly. It requires one computer that will be designated as the data collection machine which must be able to access the Internet to collect configuration data pertaining to an Office 365 tenant.

The data collection machine does not have a requirement to be domain joined, it can be a standalone machine. Internet Connection is required for this data collection machine.

Detailed information on these configurations and requirements are listed later in this document.

This document was last updated on December 8, 2020. To ensure you have the latest version of this document, check here:
https://www.microsoft.com/en-us/download/details.aspx?id=54778

Contents

Supported Versions 3
Account Requirements 3
Azure Requirements 3
Data Collection Machine Requirement 3
Data Collection Machine Setup 4
Configure Microsoft Unified Support Solutions 4
Download and install the Microsoft Monitoring Agent setup file from Azure Log Analytics 8
Setup Microsoft Assessment Azure AD Application 14
With the enabled MFA account 14
With the disabled MFA account 23
Setting permission to show Classic Workflows (if workflow report needed) 26
Install Azure Active Directory (MSOnline) ..... **Error! Bookmark not defined.**
Install Microsoft Graph 32
Install Azure AD Preview ..... **Error! Bookmark not defined.**
Install PnP (Patterns and Practices) PowerShell ..... **Error! Bookmark not defined.**
Setting up the SharePoint Online Assessment 32
With the enabled MFA account 32
With the disabled MFA account 37
Appendix 42
Data Collection Methods 42
Microsoft Graph API 42
Microsoft PowerShell 42
SharePoint Modernization Scanner 42
Office 365 Assessment – Authentication Model 43
Graph API 43
PowerShell Cmdlets 43
SharePoint Modernization Scanner 44
View Prerequisite Errors 44

System Requirements and Configuration at Glance

According to the scenario you want to use, review the following details to ensure that you meet the necessary requirements.

Supported Versions

- Office 365 SharePoint Online

Account Requirements

- User account rights:
    - Global Administrator for Office 365

Permissions:

Engineer and TAM Assignment to Log Analytic Workspace and Services Hub

- TAM invites the engineer to the customer's Services Hub to access information in the hub. Invitation email comes from Microsoft Services – Subject: Invitation to Microsoft Services Hub.
- Granting "**Read Access"** to the customer's Log Analytic workspace is a manual process that is managed and controlled by the customer. The access needs to be manually removed after the review by the customer.

    Manage log data and workspaces in Azure Monitor
    https://docs.microsoft.com/en-us/azure/azure-monitor/platform/manage-access

Azure Requirements

- Have an Azure Subscription. If your company does not have an Azure Subscription please click here to subscribe.
- Be able to link your Service Hub, and Azure Subscriptions Accounts

Data Collection Machine Requirement

- Data collection machine hardware: Minimum 4 gigabytes (GB) of RAM, 2 gigahertz (GHz dual-core processor, minimum 2 GB of free disk space.
    - High End Workstation: Windows 10 – 64bit only
    - Server: Windows Server 2019, Windows Server 2016 – 64bit only
    - PowerShell version: 5.0 or greater
- Data collection machine software requirement: A standalone or domain joined machine.
- The data collection machine must be able to connect to the Internet using HTTPS to connect to the Office 365 tenant.
- A local Admin account or Domain account with Local Admin right for Task setup.

Data Collection Machine Setup

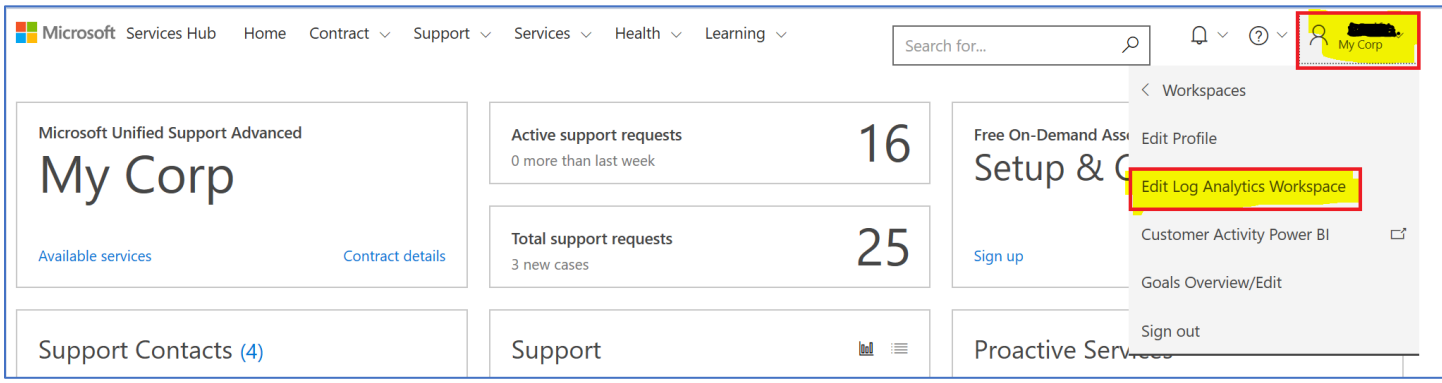
Configure Microsoft Unified Support Solutions

To begin the Office 365 SharePoint Assessment you will need to:

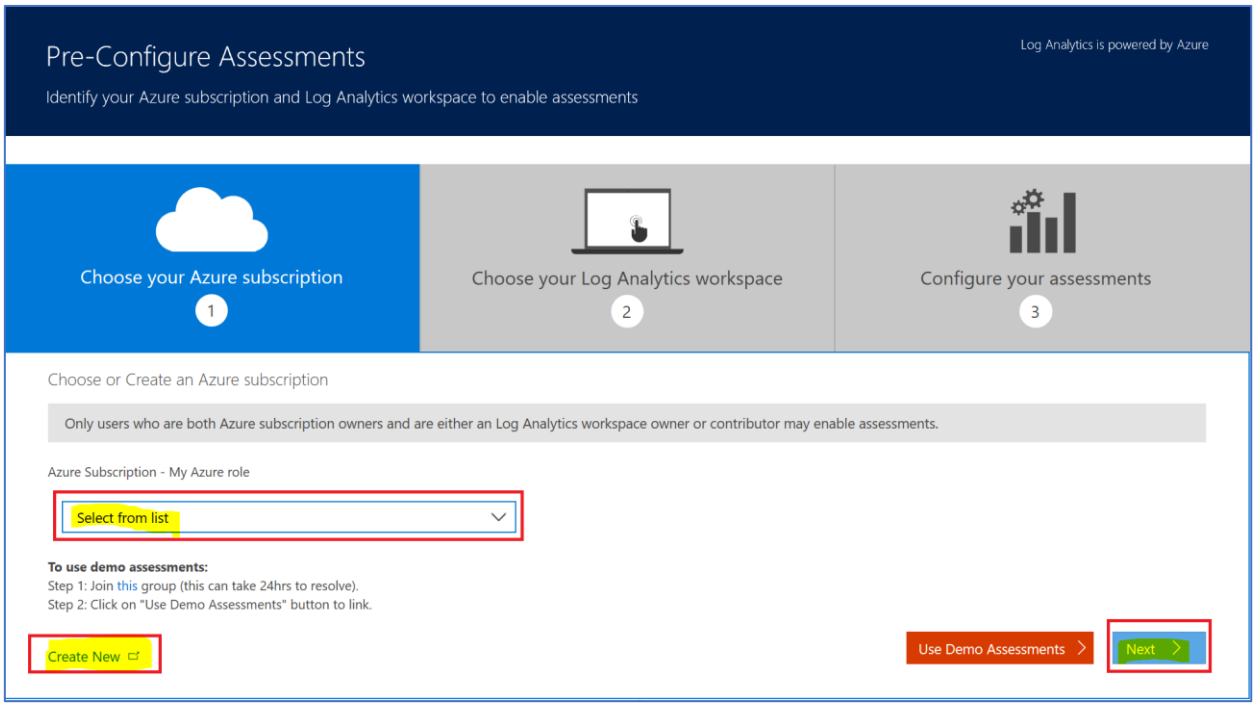
1. Navigate to https://serviceshub.microsoft.com and then go to **Health** -> **Assessments**

2. If haven't done yet, you need to connect the Service Hub to your azure subscription. If you don't have Azure subscription, you need to create one.

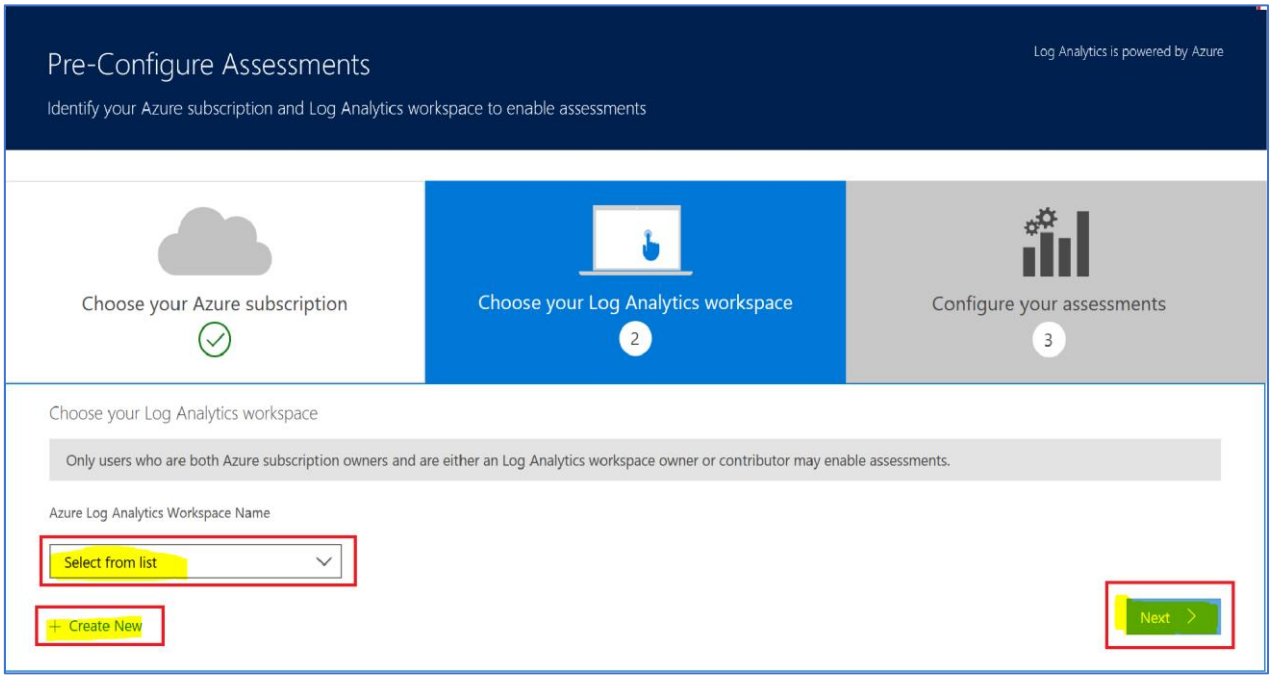
3. Click the drop-down menu for the account (this account must Azure Subscription Owner/Contributor role on the target subscription) and select **Edit Log Analytics Workspace**



4. Select the target Azure subscription (the drop-down list will list only the Azure subscriptions that your account is having access to). If you don't have Azure subscription, you can click the **Create New** link to create new subscription. After having the Azure Subscription is selected click **Next**.

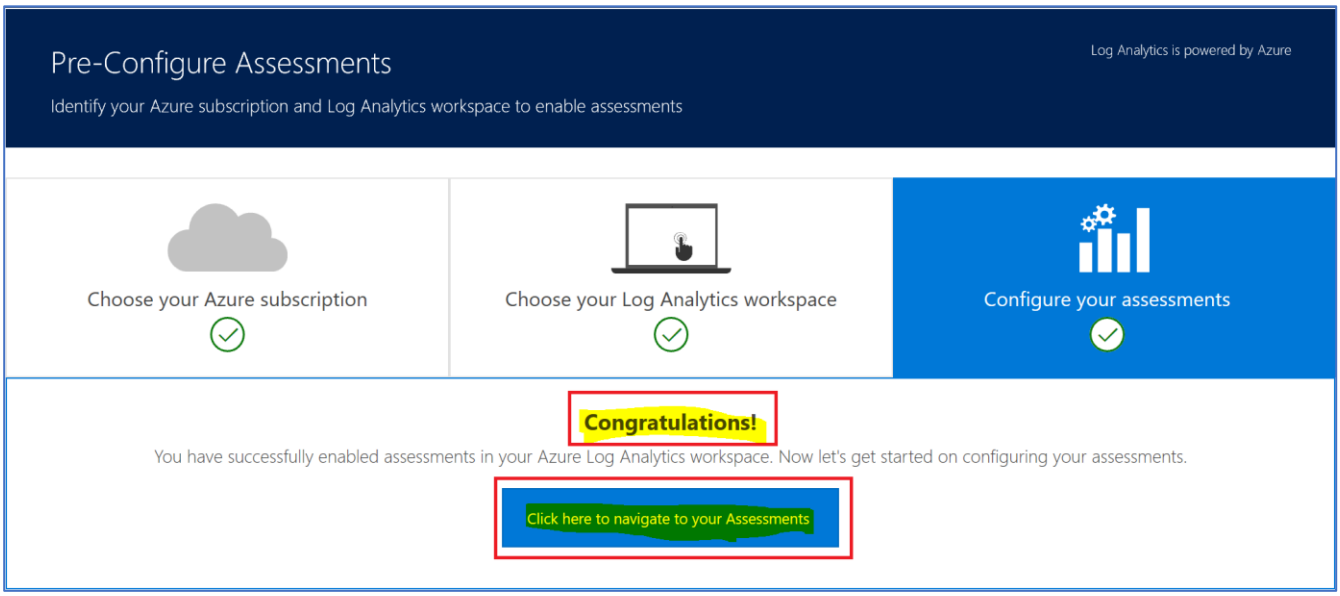


5. Select the **Azure Log Analytics Workspace** you want to use for the assessment purposes from the drop-down list, if you do not have one already created click **Create New** link to create new one. After having the workspace is selected click **Next**.

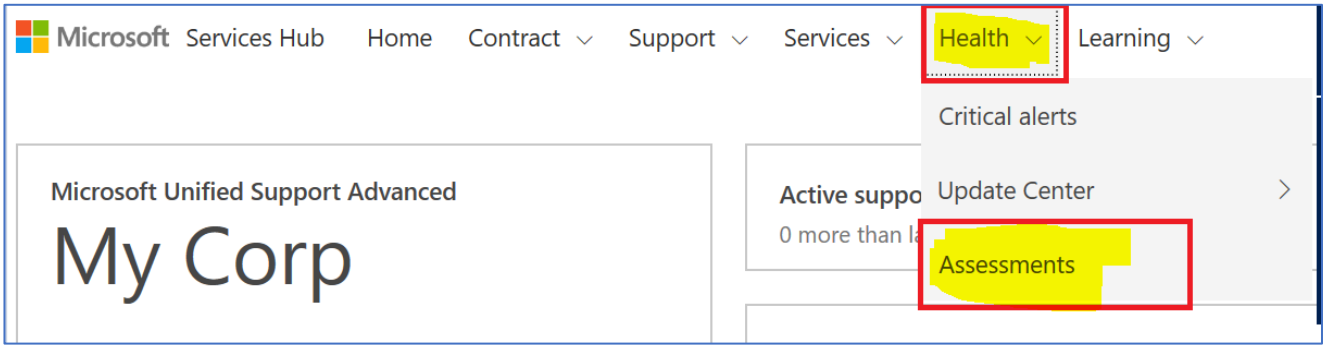


You should get the Congratulations screen as an indication that the link between the Services Hub and Azure Log Analytics workspace is established successfully.

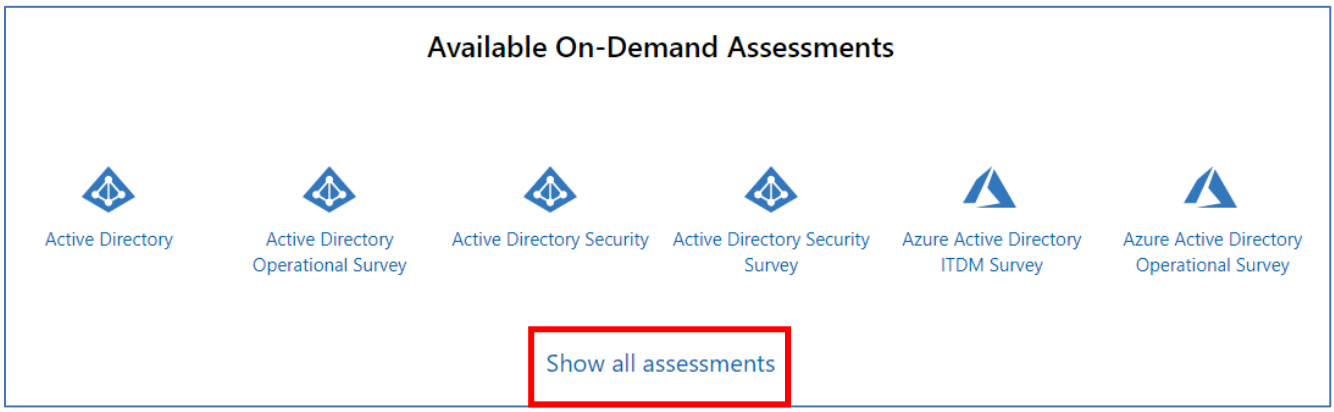
6. Click the **Click here to navigate to your Assessment** to create your SharePoint Online On-Demand assessment



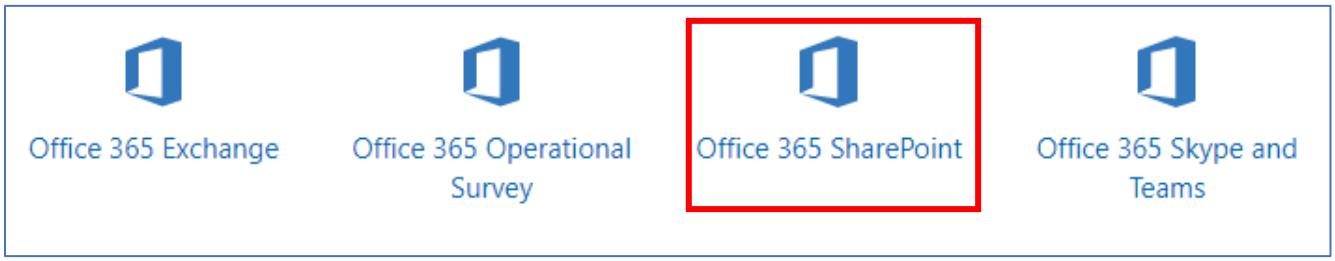
7. If you have the connection already prepared ahead of time, then you click the **Health** drop-down menu from the Services Hub portal and select **Assessments** to navigate to your Assessment to create your SharePoint Online On-Demand assessment or manage the existing assessments



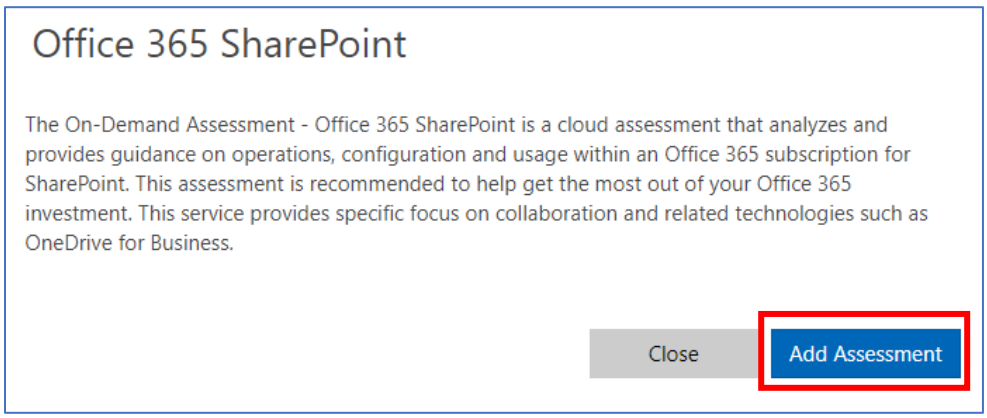
8. You will need to click **Show all assessments** to see all the assessments



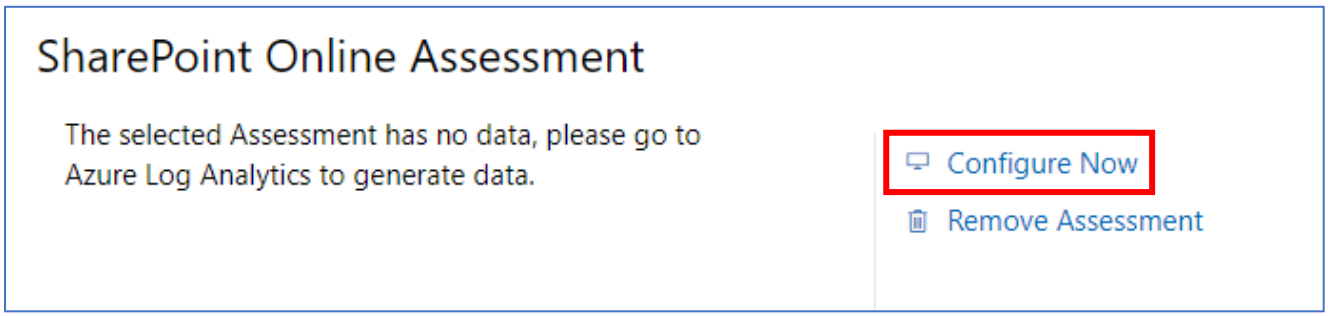
9. Click on the **Office 365 SharePoint**.



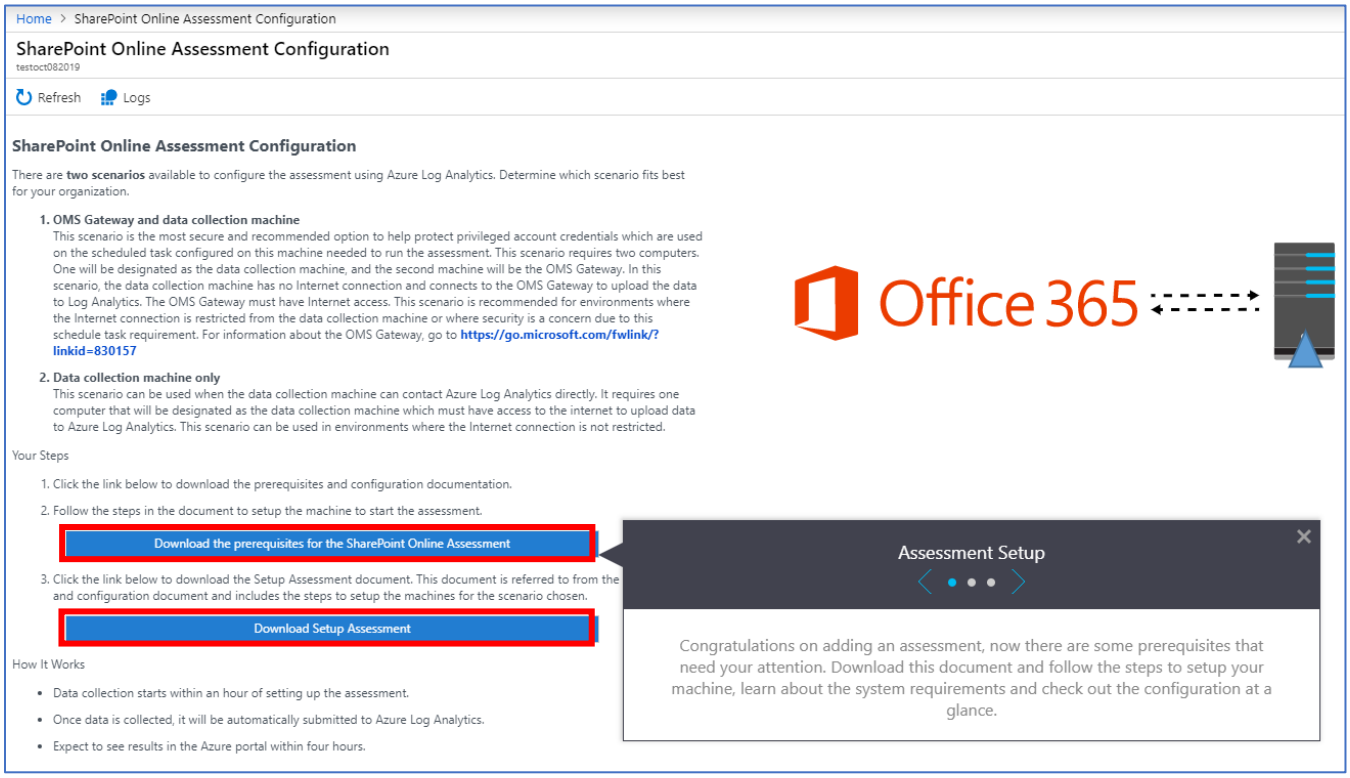
10. Click **Add Assessment**.



11. Setup the assessment by following the steps in the **Configure Now** page



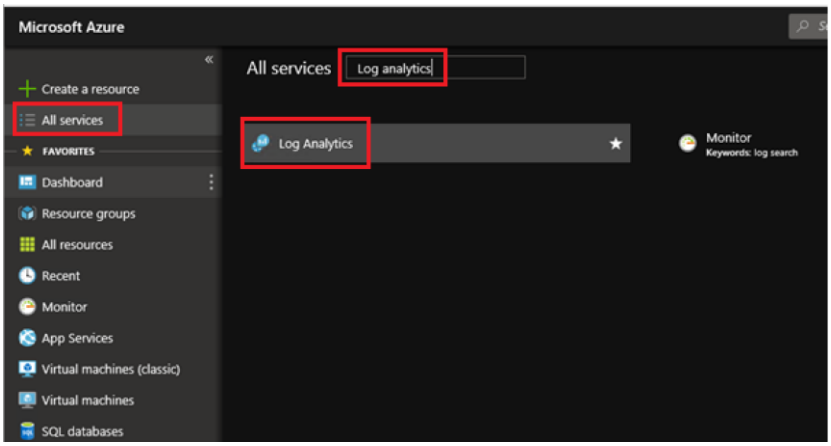
12. Download the **prerequisites** and the **setup** documents and go through them both to setup the assessment and start collecting the data from your environment.



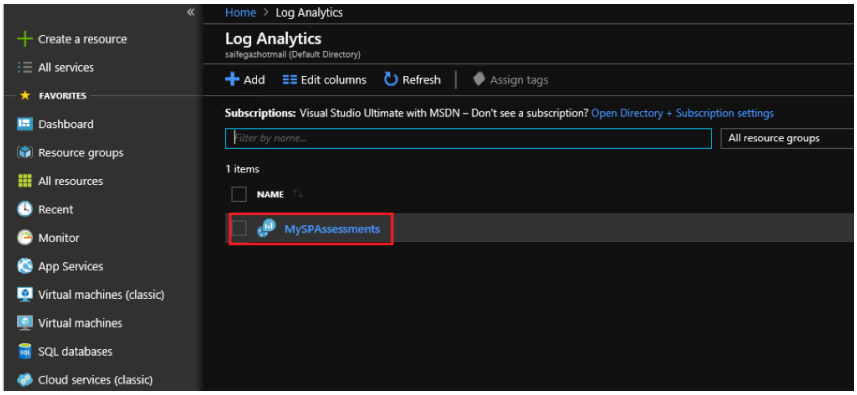
Download and install the Microsoft Monitoring Agent setup file from Azure Log Analytics

On the designated data collection machine complete the following:

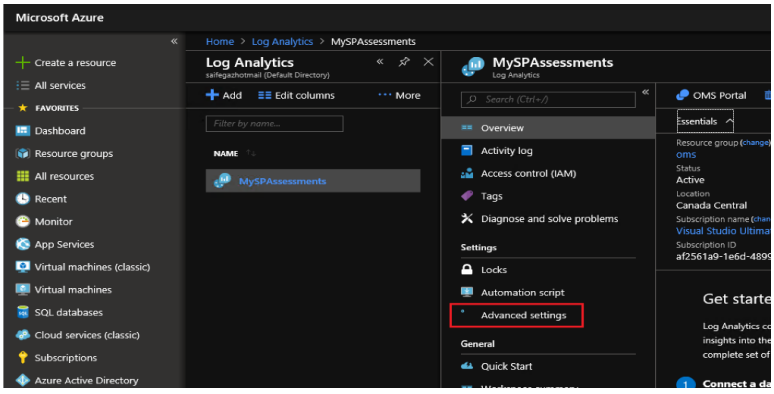
1. In the Azure portal, go to **log analytics**; to find it, you can click on the **All Services** > type **Log analytics** in the filter field



select your workspace if it exists or create new one.

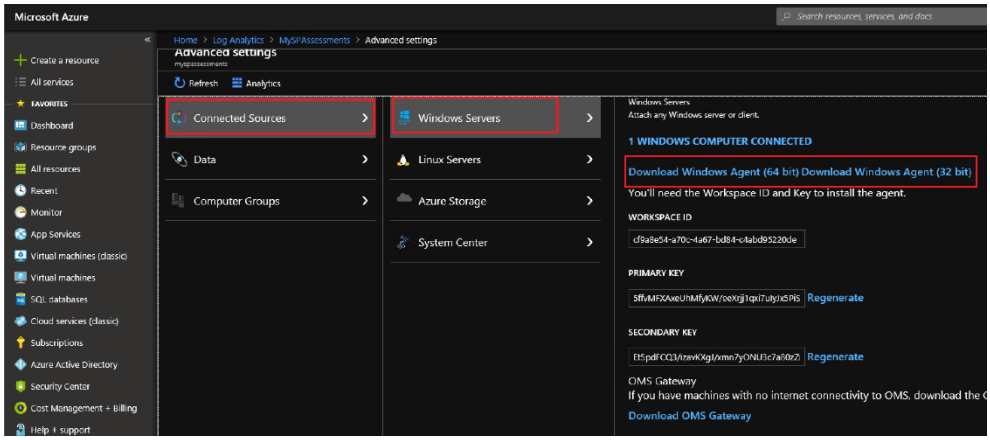


2. click the **Advanced Settings** Icon.

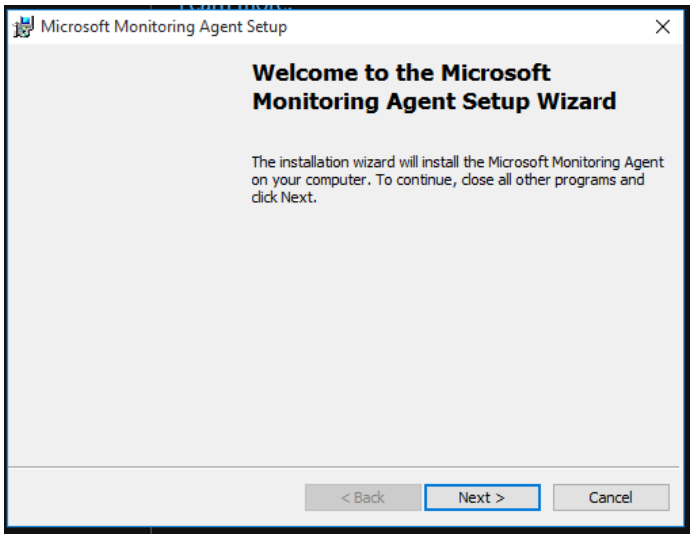


3. Click **Connected Sources**, and then select **Windows Servers**.
4. Click the **Download Windows Agent** link that is applicable to your computer processor type to download the setup file. If the agent is downloaded on another machine, copy the Setup file over to the data collection machine.

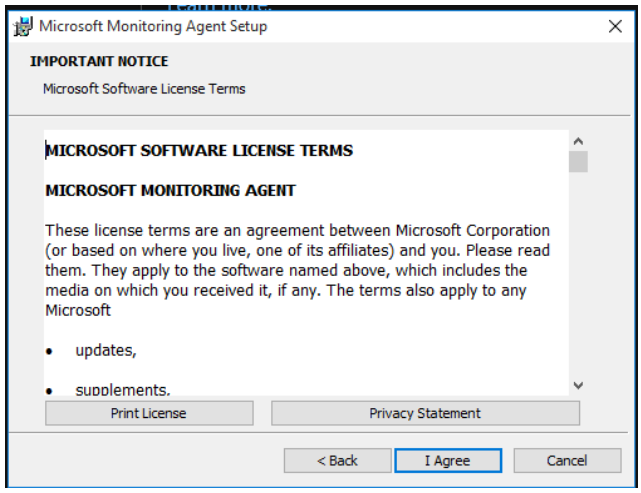
> **Note:** *If a monitoring client was installed for System Center Operations Manager (SCOM), the setup only offers to Upgrade the agent, preserving existing settings. The upgrade does not include any of the configuration steps below.*



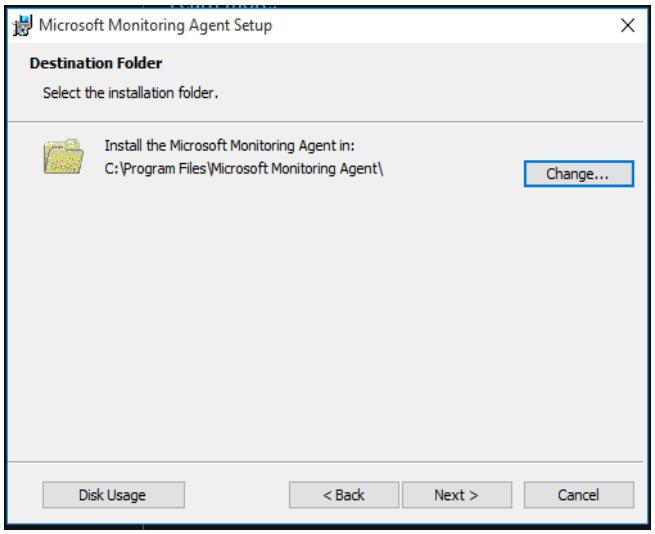
5. Run Setup to install the agent.
6. On the **Welcome** page, click **Next**.



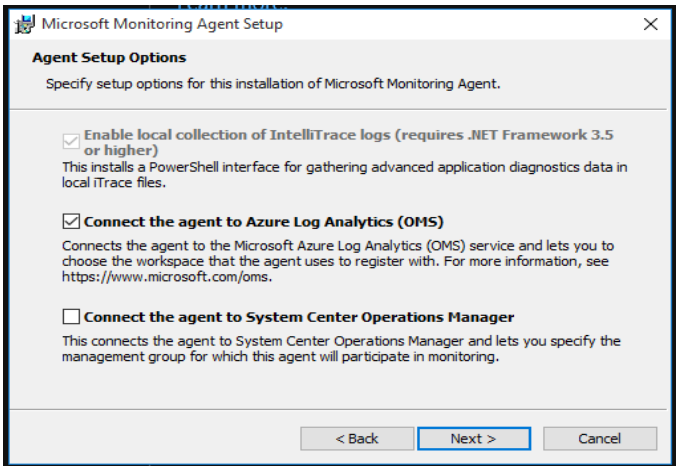
7. On the **License Terms** page, read the license and then click **I Agree**



8. On the **Destination Folder** page, change or keep the default installation folder and then click **Next**.

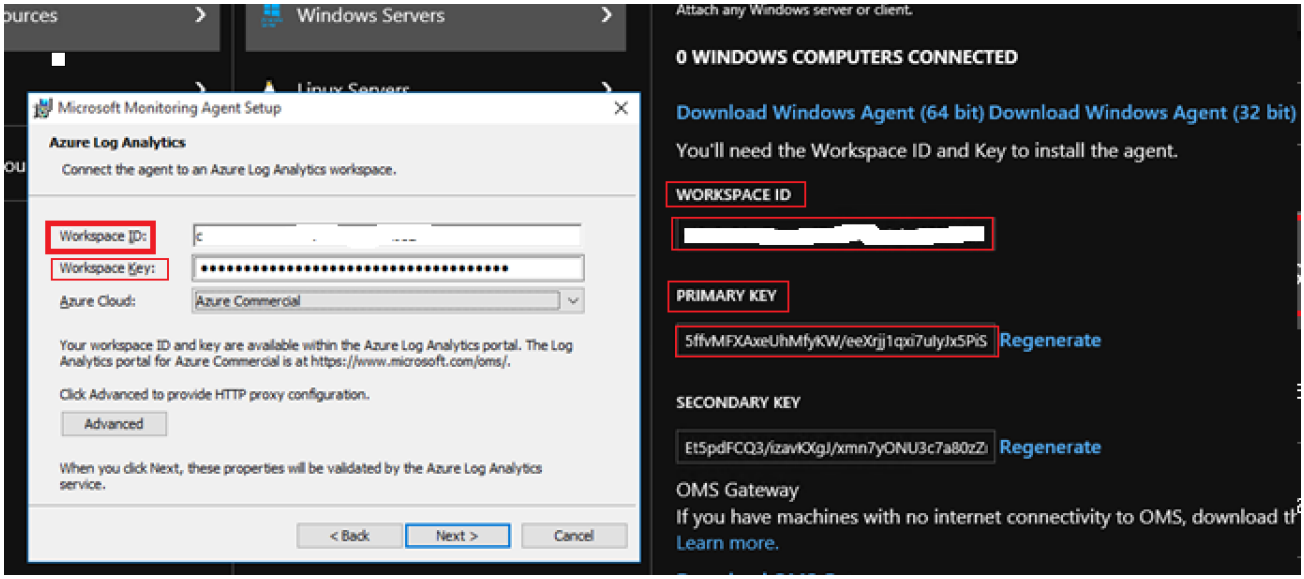


9. On the **Agent Setup Options** page, choose the **Connect the agent to Azure Log Analytics (OMS)** option. Click **Next**.

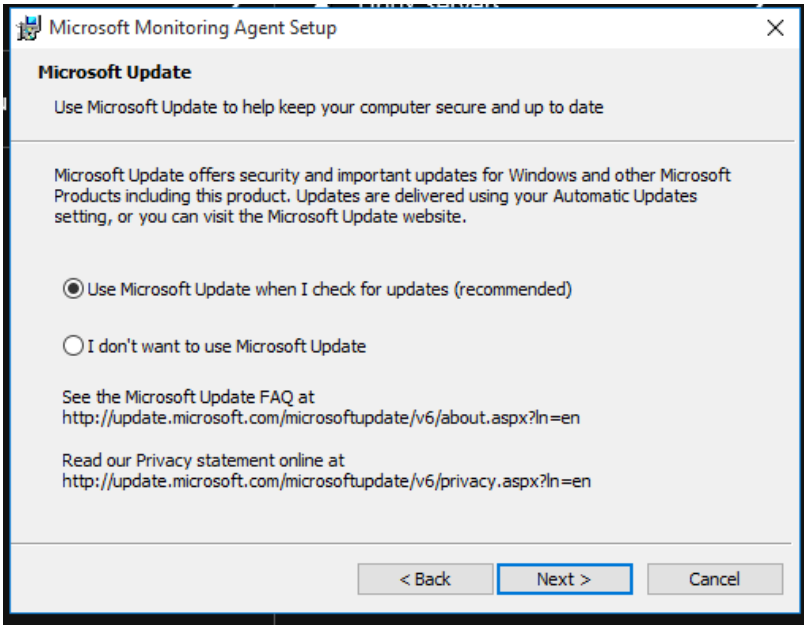


10. On the Overview, Settings Dashboard page, click **Connected Sources**, and then copy and paste the **Workspace ID** and **Workspace Key (Primary Key)** from the log analytics portal. (Hint: Click the copy button then paste in the corresponding **Agent Setup** field).

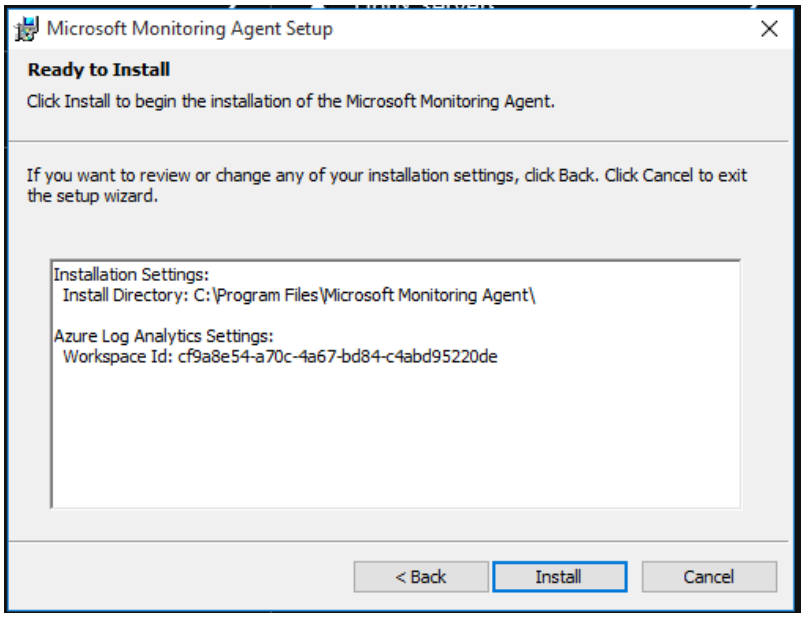
11. Select **Azure Commercial** or if you are using an Azure US Government cloud select **Azure US Government** from the **Azure Cloud** drop down menu and click **OK**.



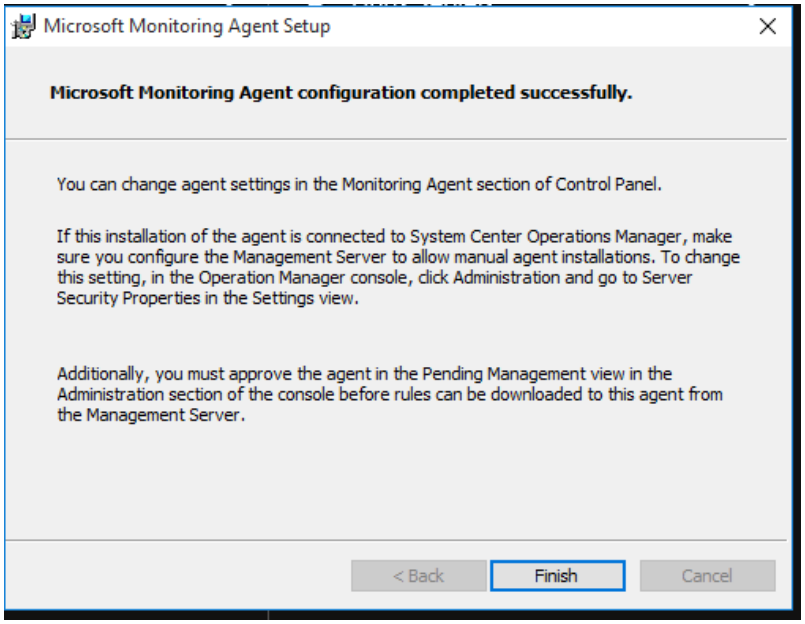
12. On the **Microsoft Update** page, optionally select **Use Microsoft Update when I check for updates (recommended)**, then click **Next**.



13. On the **Ready to Install** page, review your choices, and then click **Install**.



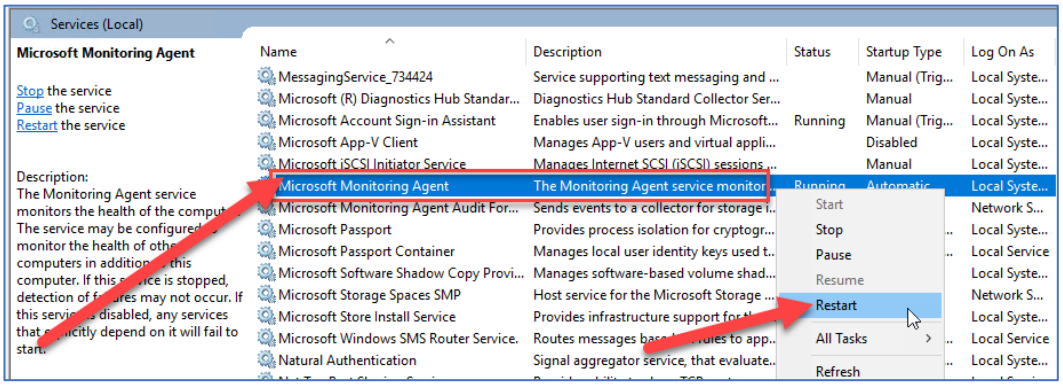
14. On the **Microsoft Monitoring Agent configuration successfully completed** page, click **Finish**.



15. When complete, the **Microsoft Monitoring Agent** appears in **Control Panel**. You can review your configuration there and verify that the agent is connected to log analytics. When connected to log analytics, the agent displays a message stating: **The Microsoft Monitoring Agent has successfully connected to the log analytics service**.

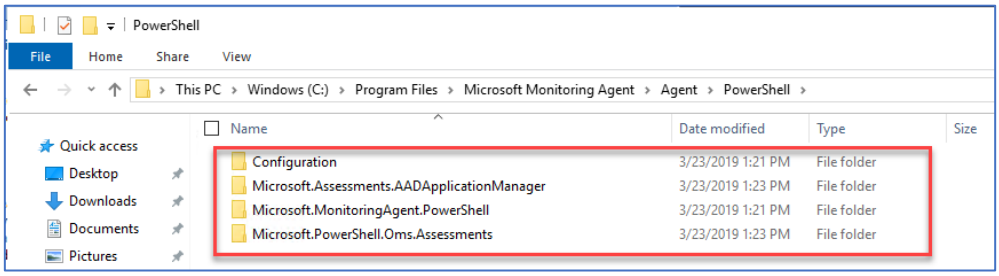
After setting up the data collection machine, continue with the setup of the Assessment as outlined in the prerequisites and configuration documentation for each technology.

16. Restart **MMA** Service



17. Confirm the below folders exist in

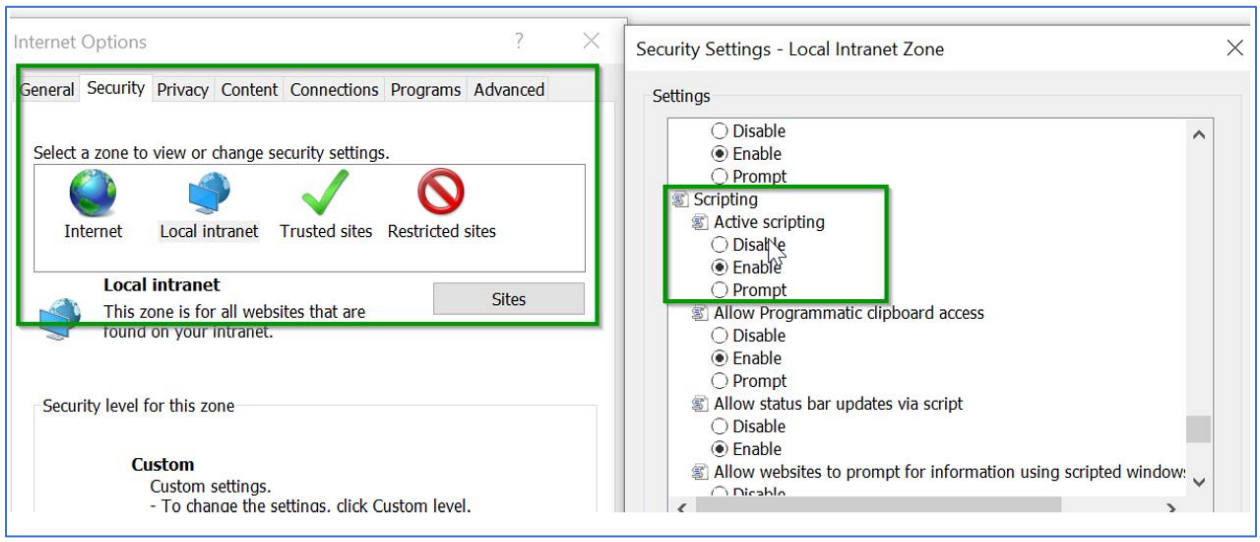
    C:\Program Files\Microsoft Monitoring Agent\Agent\PowerShell



Confirm the folders are available before continuing to setup the new MS application in Azure

Note: *While executing New-MicrosoftAssessmentsApplication command, you may need to enable the following settings to enable the Authentication popup prompt.*

18. Go to Internet options and Enable JavaScript:



19. Add your SharePoint Online admin center URL to the trusted sites e.g. https://tenantname-admin.sharepoint.com or https://admin.tenantname.com if friendly admin URL configured

Setup Microsoft Assessment Azure AD Application

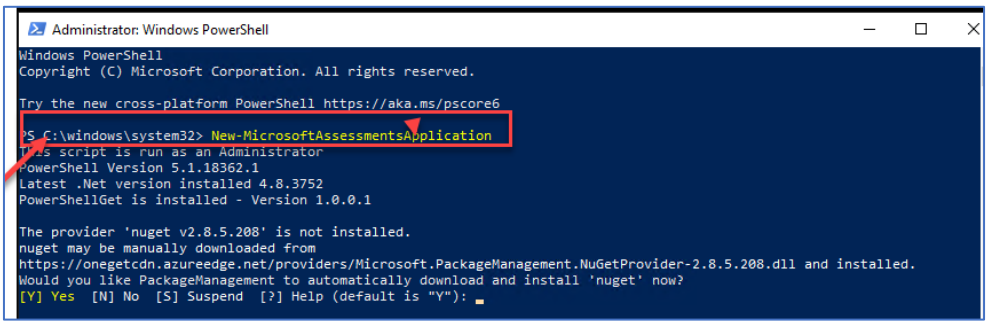
With the enabled MFA account

1. Open PowerShell as an Administrator and then run the following on the Data Collection Machine.

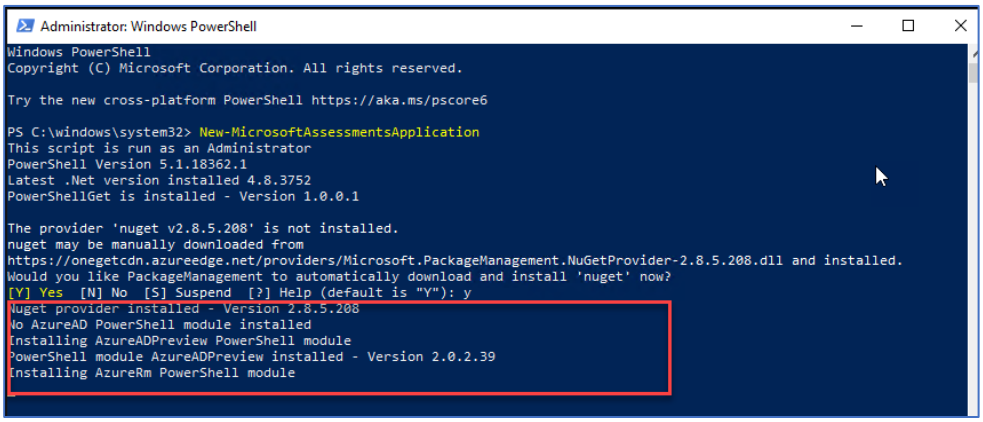
   ```
   New-MicrosoftAssessmentsApplication
   ```

   This script will run and then prompt for Global Administrator Credentials

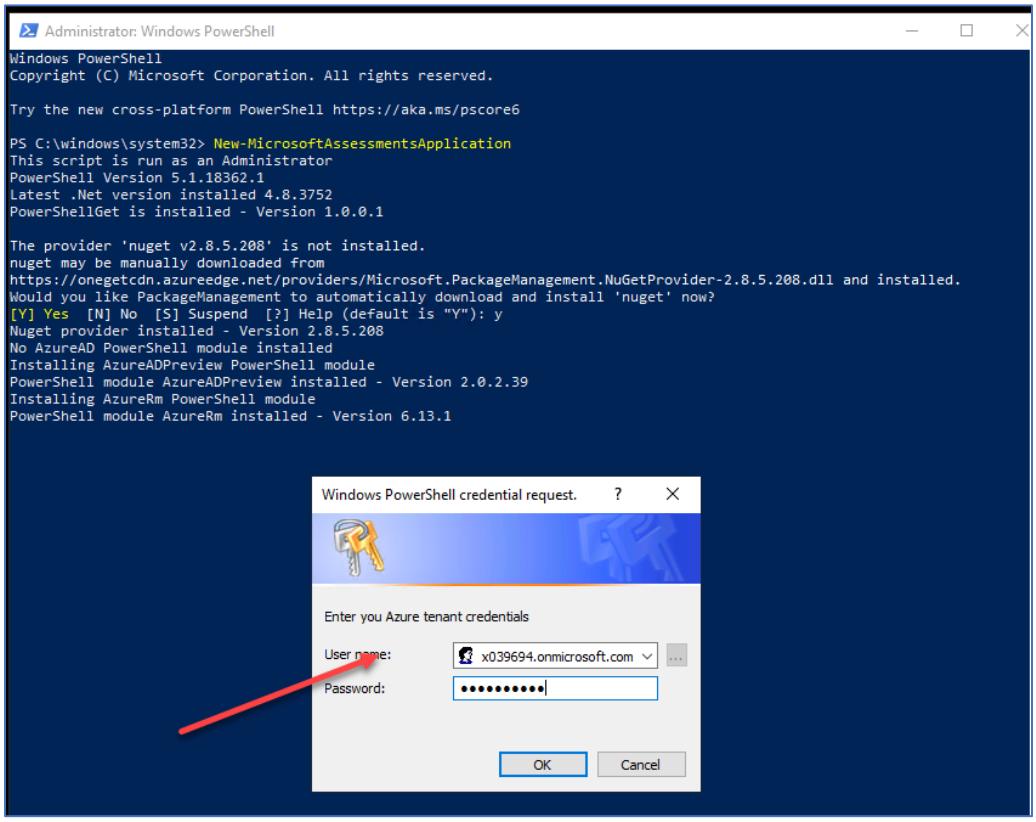
2. Type "**Y**" to install package.



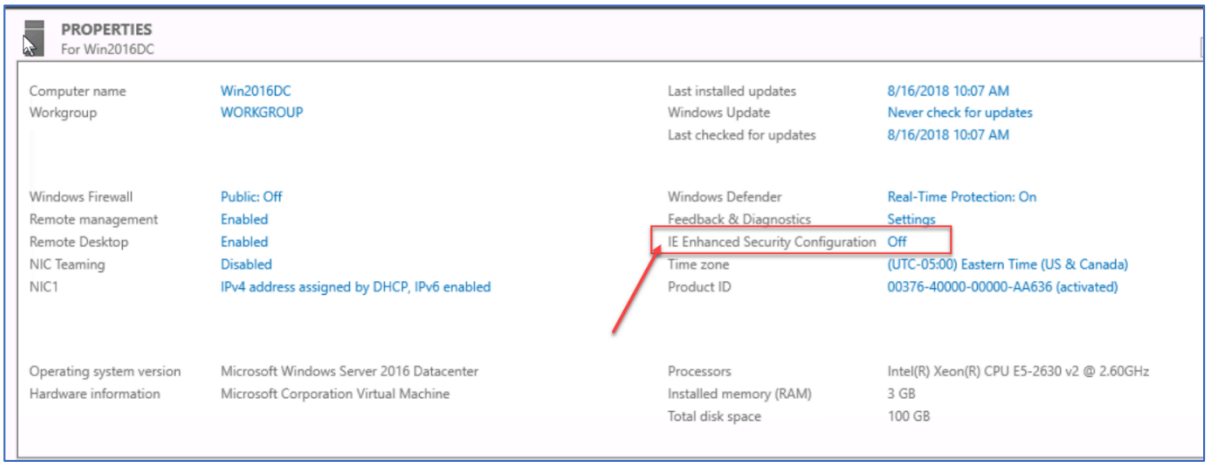
This will install the AzureAD Preview Module



3. At the credential prompt, please enter an account with Global Administrator access rights.

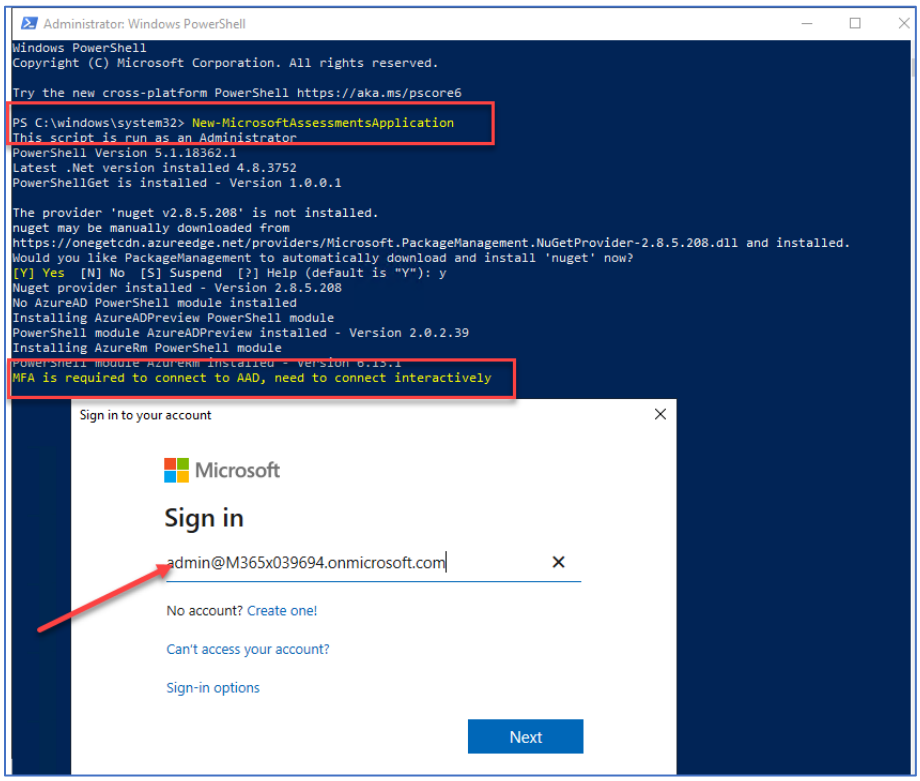


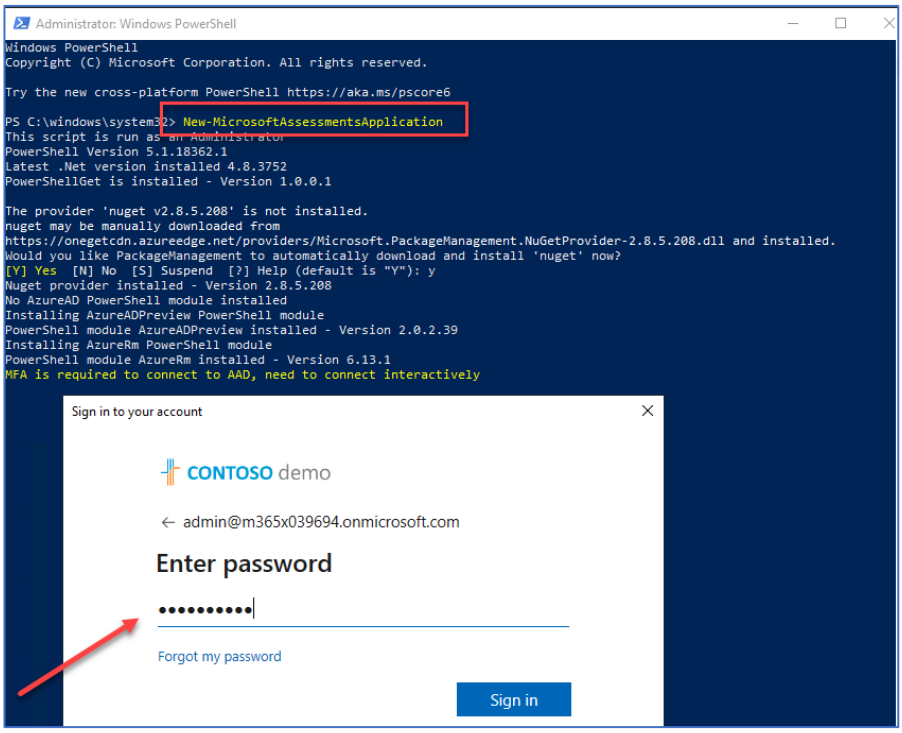
4. PS: for Windows Server 20** , you may be needed to disable IE Enhanced Security



5. You will be prompted to Logging, please use the Global Administrator Account, Password and MFA Code

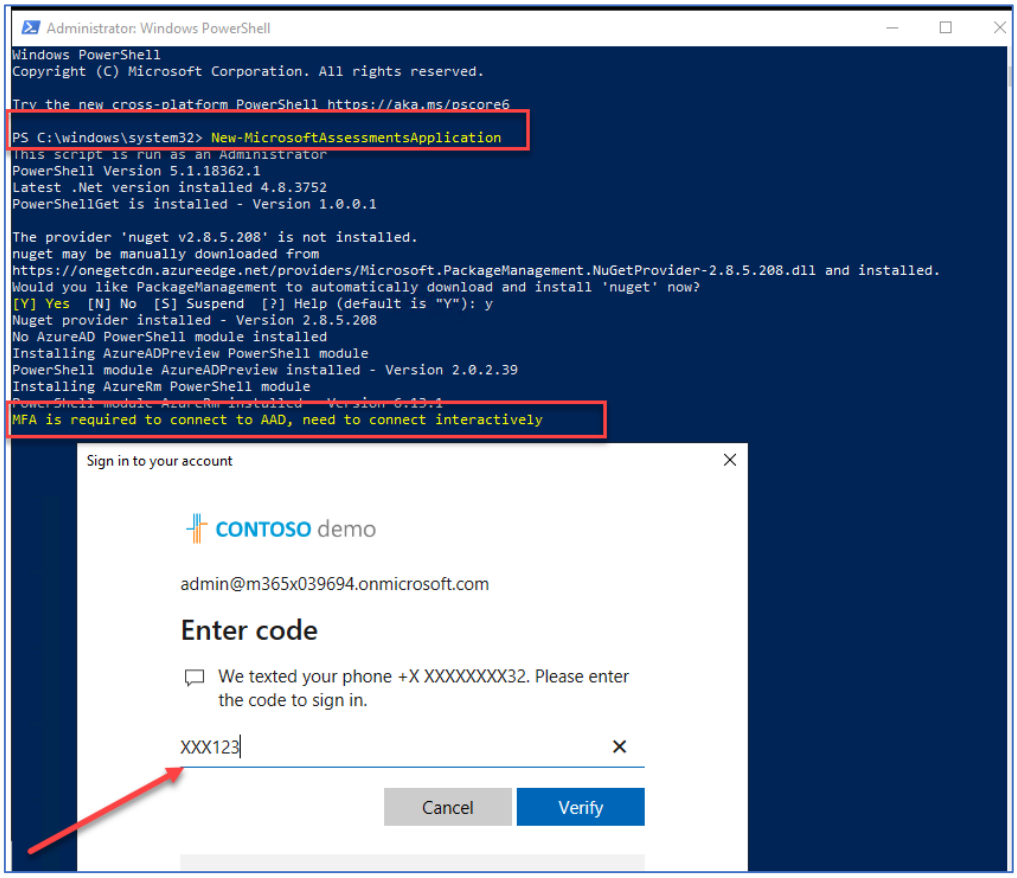
6. You will be prompted so Sign-in again after the MFA Requirement message. Use the Global Admin credentials and MFA code





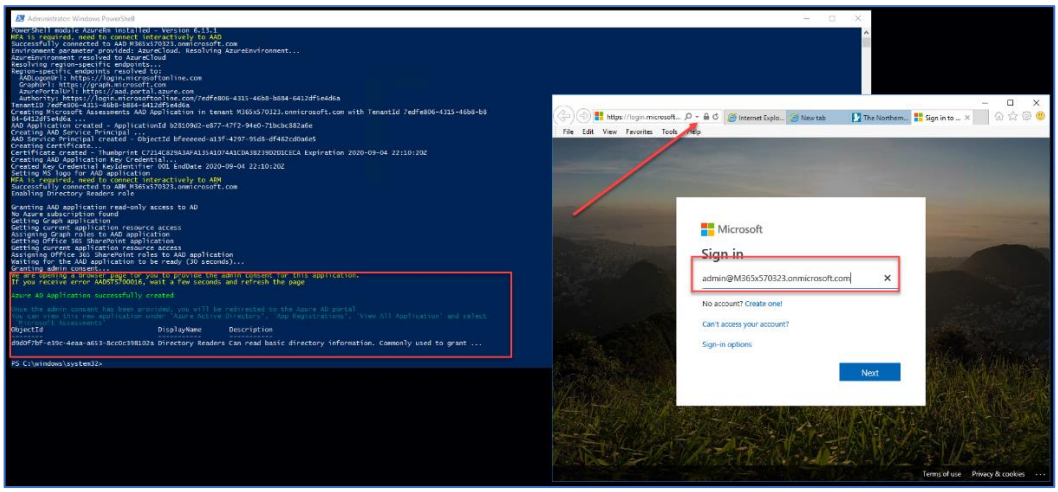
7. Enter your MFA code

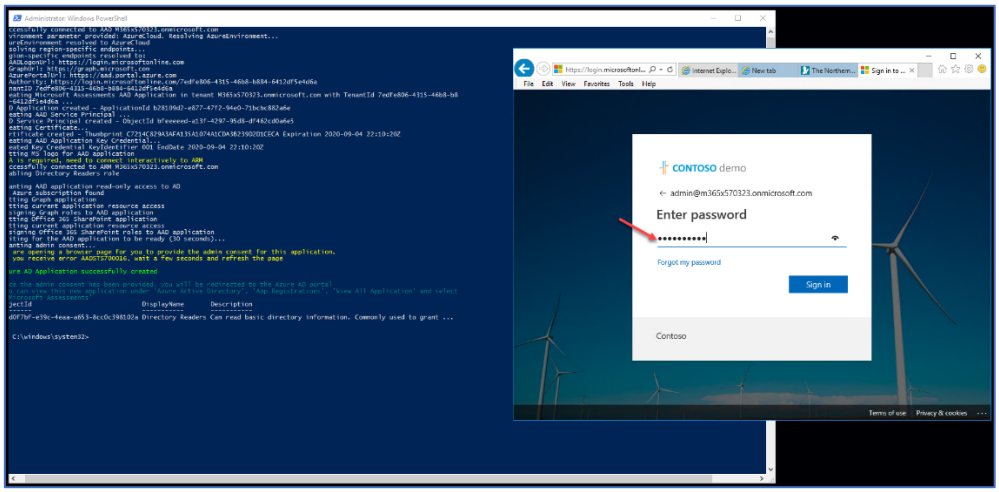
8. You will be prompted to logging again with your GA account, Password and MFA Code

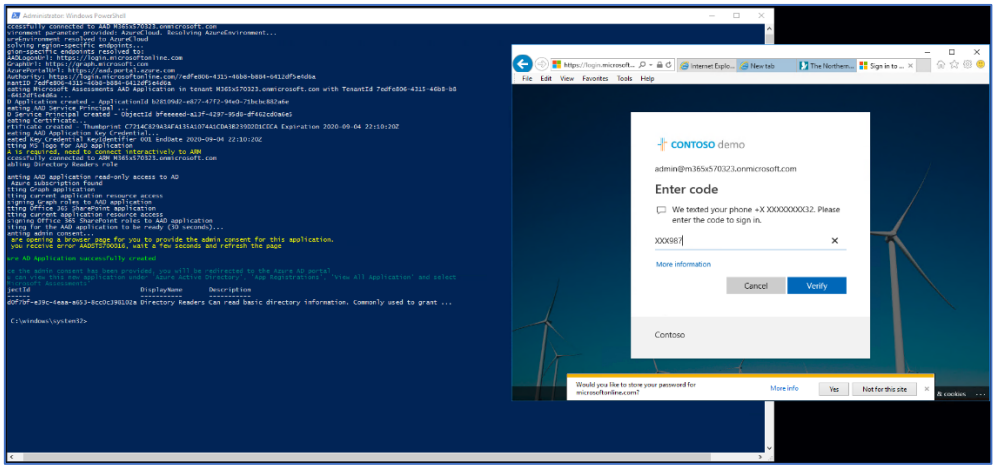


9. After the successful creation of the Azure Application, a browser will be launch and you will be prompted to logging again with your Global Admin Account, Password and MFA Code,

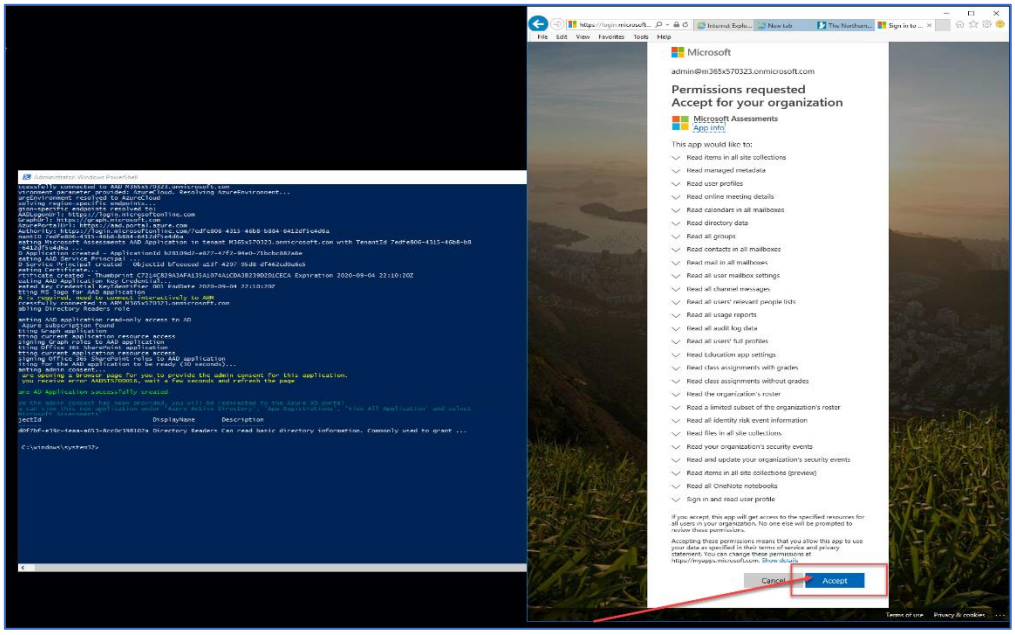
   PS: All prompts will be in the browser.



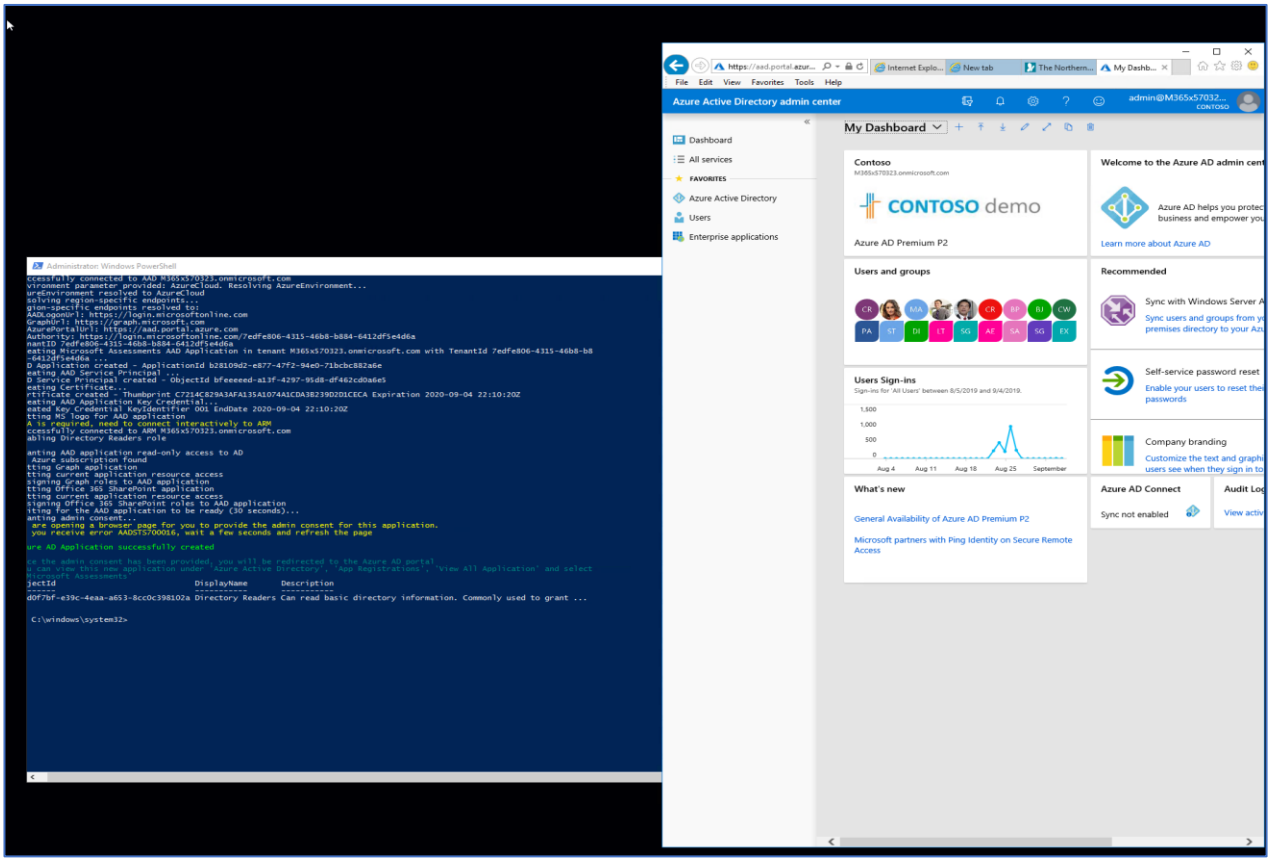




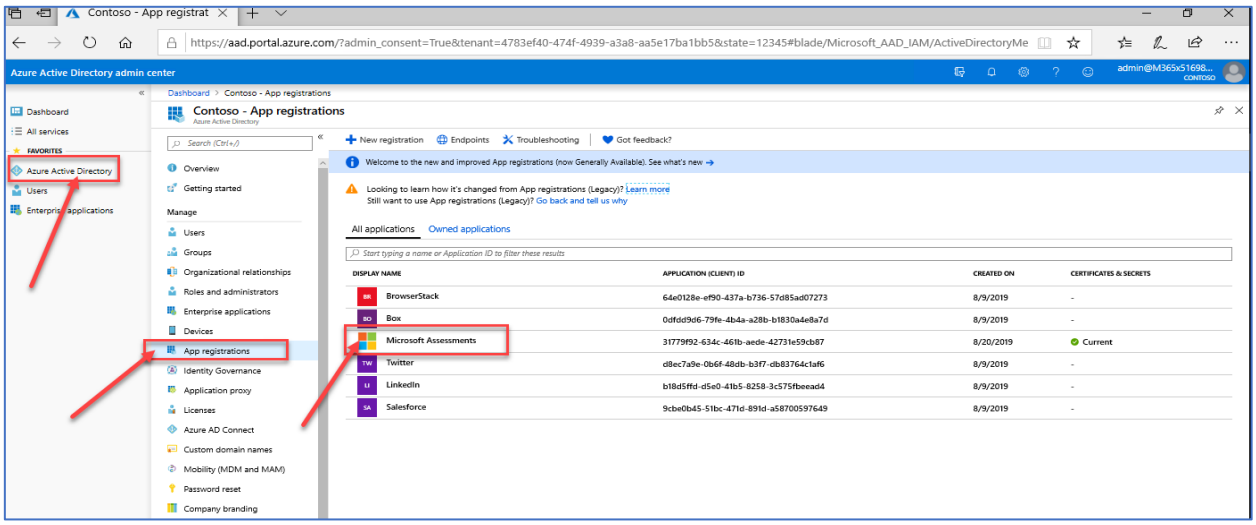
10. You will be prompted to accept the permission request



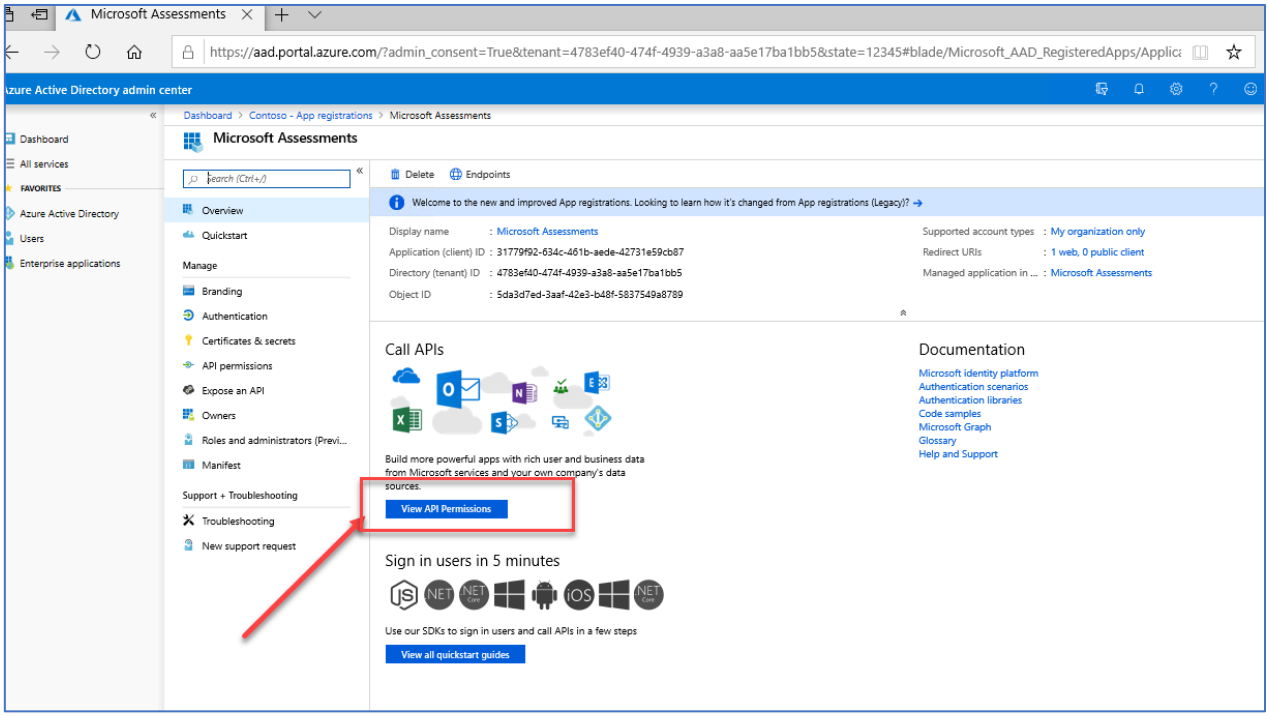
11. And you be logging into your Azure Environment.



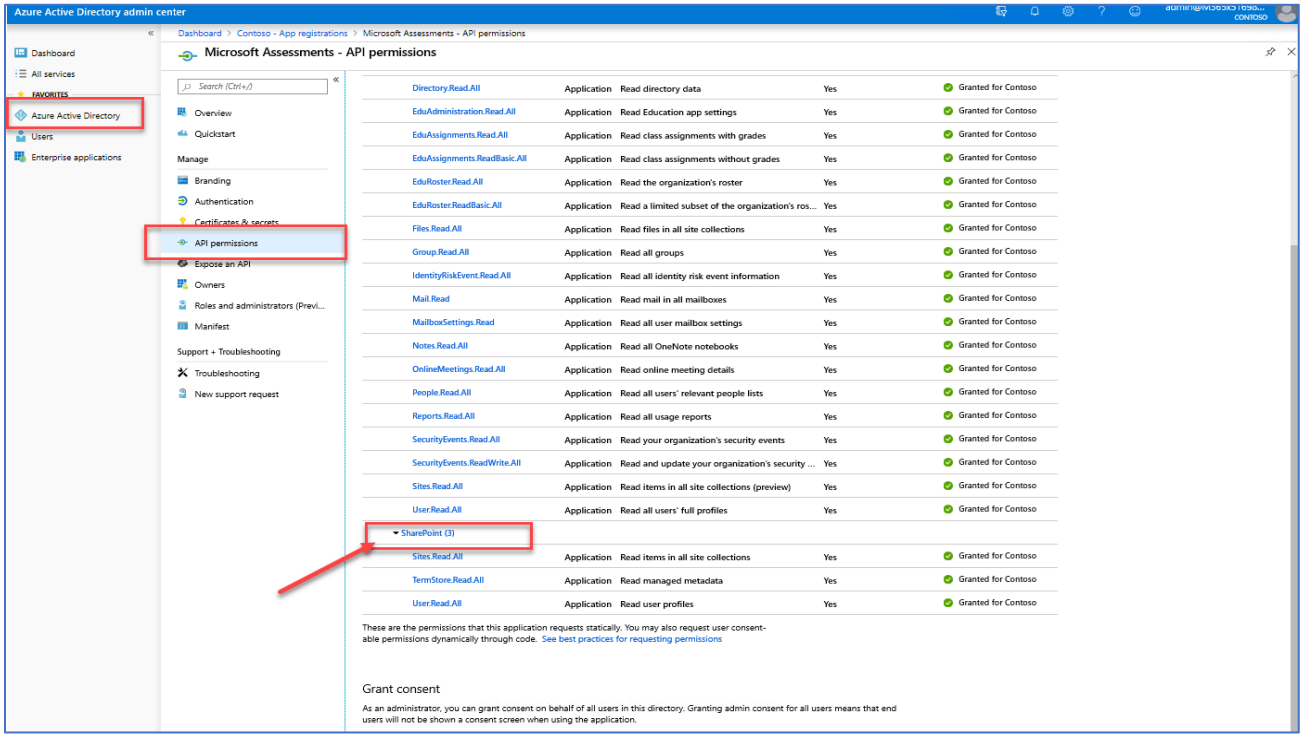
12. In Azure Select “Azure Active Directory” → “App Registrations”→ and confirm the “Microsoft Assessments” app is present



13. Click on the Microsoft Assessment Application to open it and click on “View API Permissions”



14. Confirm the SharePoint App Permissions section was also created.


Azure Active Directory admin center
Dashboard
All services
FAVORITES
Azure Active Directory
Users
Enterprise applications
Dashboard > Contoso - App registrations > Microsoft Assessments - API permissions
Microsoft Assessments - API permissions
Search (Ctrl+/)
Overview
Quickstart
Manage
Branding
Authentication
Certificates & secrets
API permissions
Expose an API
Owners
Roles and administrators (Previ...
Manifest
Support + Troubleshooting
Troubleshooting
New support request
Directory.Read.All Application Read directory data Yes Granted for Contoso
EduAdministration.Read.All Application Read Education app settings Yes Granted for Contoso
EduAssignments.Read.All Application Read class assignments with grades Yes Granted for Contoso
EduAssignments.ReadBasic.All Application Read class assignments without grades Yes Granted for Contoso
EduRoster.Read.All Application Read the organization's roster Yes Granted for Contoso
EduRoster.ReadBasic.All Application Read a limited subset of the organization's ros... Yes Granted for Contoso
Files.Read.All Application Read files in all site collections Yes Granted for Contoso
Group.Read.All Application Read all groups Yes Granted for Contoso
IdentityRiskEvent.Read.All Application Read all identity risk event information Yes Granted for Contoso
Mail.Read Application Read mail in all mailboxes Yes Granted for Contoso
MailboxSettings.Read Application Read all user mailbox settings Yes Granted for Contoso
Notes.Read.All Application Read all OneNote notebooks Yes Granted for Contoso
OnlineMeetings.Read.All Application Read online meeting details Yes Granted for Contoso
People.Read.All Application Read all users' relevant people lists Yes Granted for Contoso
Reports.Read.All Application Read all usage reports Yes Granted for Contoso
SecurityEvents.Read.All Application Read your organization's security events Yes Granted for Contoso
SecurityEvents.ReadWrite.All Application Read and update your organization's security ... Yes Granted for Contoso
Sites.Read.All Application Read items in all site collections (preview) Yes Granted for Contoso
User.Read.All Application Read all users' full profiles Yes Granted for Contoso
SharePoint (3)
Sites.Read.All Application Read items in all site collections Yes Granted for Contoso
TermStore.Read.All Application Read managed metadata Yes Granted for Contoso
User.Read.All Application Read user profiles Yes Granted for Contoso
These are the permissions that this application requests statically. You may also request user consent-able permissions dynamically through code. See best practices for requesting permissions
Grant consent
As an administrator, you can grant consent on behalf of all users in this directory. Granting admin consent for all users means that end users will not be shown a consent screen when using the application.

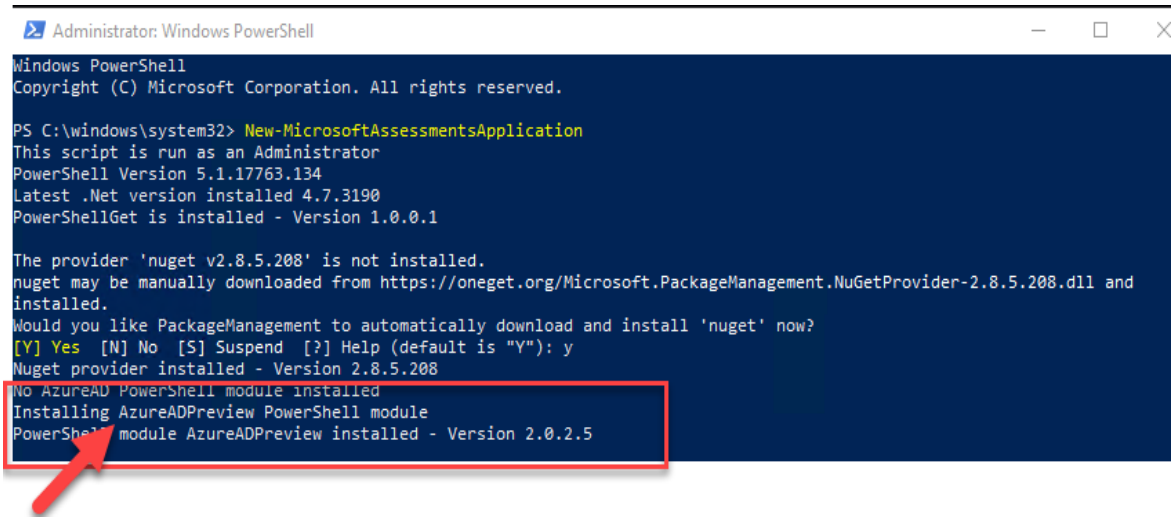
With the disabled MFA account

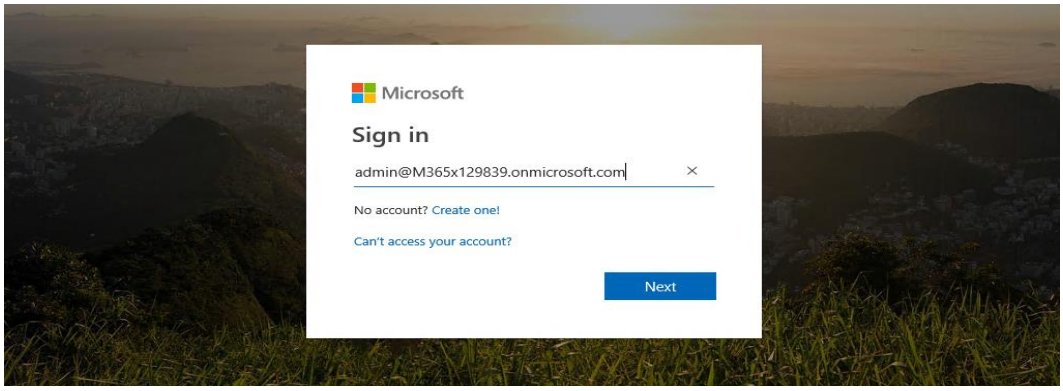
1. Open PowerShell as an Administrator and then run the following on the Data Collection Machine.

New-MicrosoftAssessmentsApplication

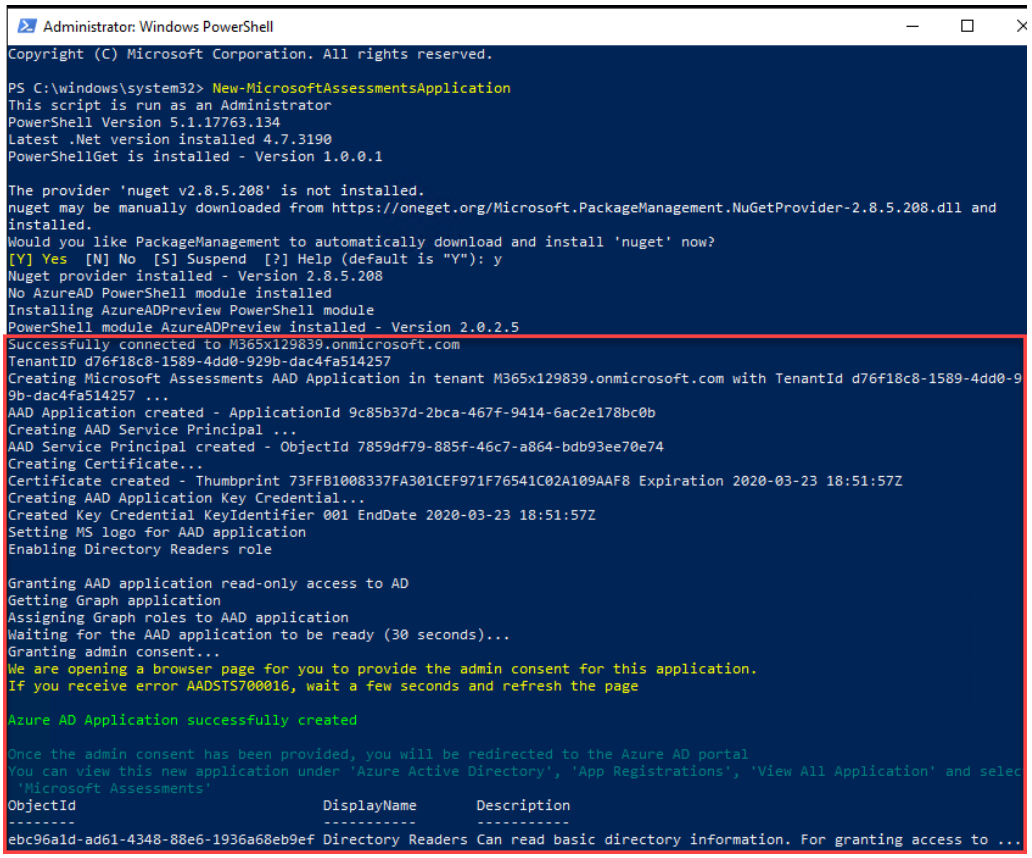
This script will run and then prompt for Global Administrator Credentials:

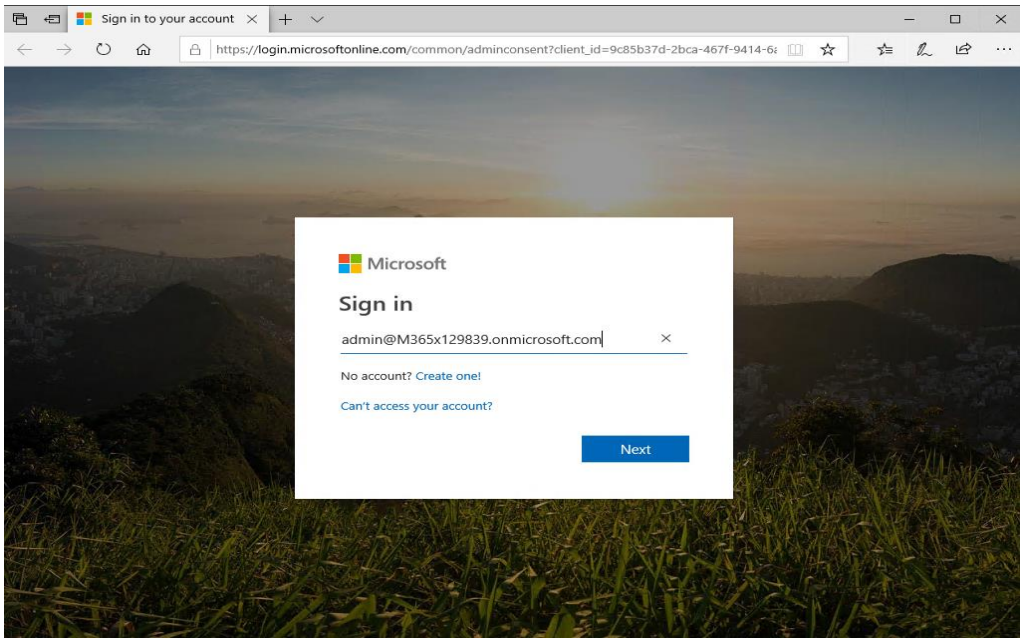
2. Type “Y” to install package. PS: This command will install the AzureADPreview module. **If it doesn’t get installed as part of this step, make sure you install the Azure AD Preview Module.**

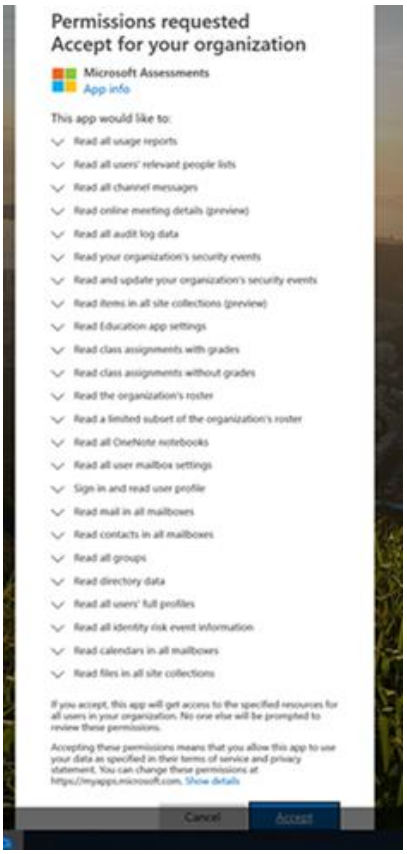




3. Once credentials have been setup, a browser will open that will ask for **Read** access to several objects, check the access requests, and then click **Accept**.

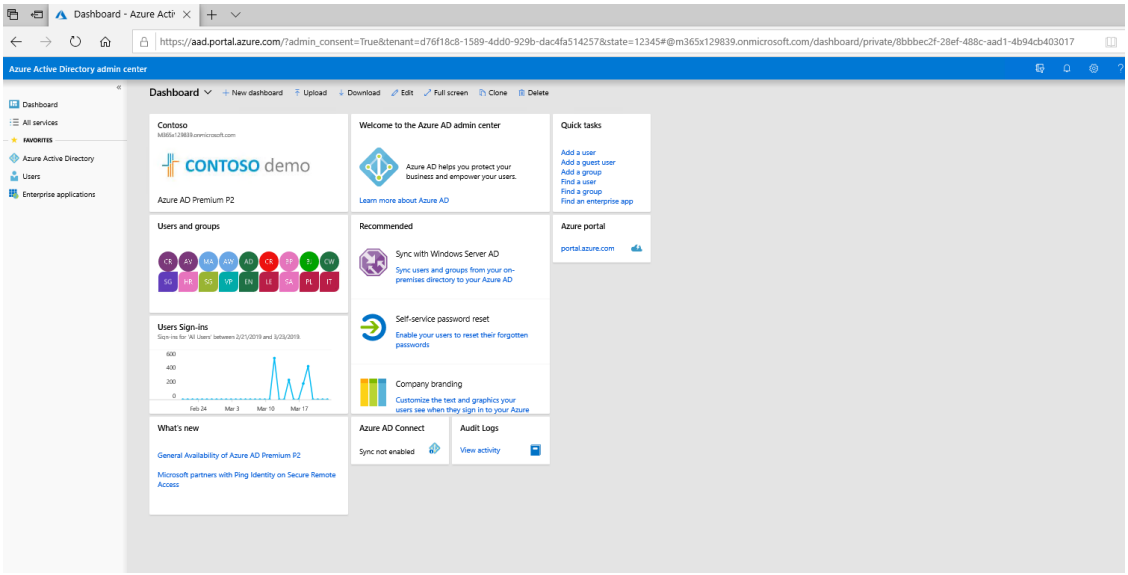

Administrator: Windows PowerShell
Copyright (C) Microsoft Corporation. All rights reserved.
PS C:\windows\system32> New-MicrosoftAssessmentsApplication
This script is run as an Administrator
PowerShell Version 5.1.17763.134
Latest .Net version installed 4.7.3190
PowerShellGet is installed - Version 1.0.0.1
The provider 'nuget v2.8.5.208' is not installed.
nuget may be manually downloaded from https://oneget.org/Microsoft.PackageManagement.NuGetProvider-2.8.5.208.dll and installed.
Would you like PackageManagement to automatically download and install 'nuget' now?
[Y] Yes [N] No [S] Suspend [?] Help (default is "Y"): y
Nuget provider installed - Version 2.8.5.208
No AzureAD PowerShell module installed
Installing AzureADPreview PowerShell module
PowerShell module AzureADPreview installed - Version 2.0.2.5
Successfully connected to M365x129839.onmicrosoft.com
TenantID d76f18c8-1589-4dd0-929b-dac4fa514257
Creating Microsoft Assessments AAD Application in tenant M365x129839.onmicrosoft.com with TenantId d76f18c8-1589-4dd0-99b-dac4fa514257 ...
AAD Application created - ApplicationId 9c85b37d-2bca-467f-9414-6ac2e178bc0b
Creating AAD Service Principal ...
AAD Service Principal created - ObjectId 7859df79-885f-46c7-a864-bdb93ee70e74
Creating Certificate...
Certificate created - Thumbprint 73FFB1008337FA301CEF971F76541C02A109AAF8 Expiration 2020-03-23 18:51:57Z
Creating AAD Application Key Credential...
Created Key Credential KeyIdentifier 001 EndDate 2020-03-23 18:51:57Z
Setting MS logo for AAD application
Enabling Directory Readers role
Granting AAD application read-only access to AD
Getting Graph application
Assigning Graph roles to AAD application
Waiting for the AAD application to be ready (30 seconds)...
Granting admin consent...
We are opening a browser page for you to provide the admin consent for this application.
If you receive error AADSTS700016, wait a few seconds and refresh the page
Azure AD Application successfully created
Once the admin consent has been provided, you will be redirected to the Azure AD portal
You can view this new application under 'Azure Active Directory', 'App Registrations', 'View All Application' and select 'Microsoft Assessments'
ObjectId DisplayName Description
ebc96a1d-ad61-4348-88e6-1936a68eb9ef Directory Readers Can read basic directory information. For granting access to ...


Sign in to your account
https://login.microsoftonline.com/common/adminconsent?client_id=9c85b37d-2bca-467f-9414-6a
Microsoft
Sign in
admin@M365x129839.onmicrosoft.com
No account? Create one!
Can't access your account?
Next

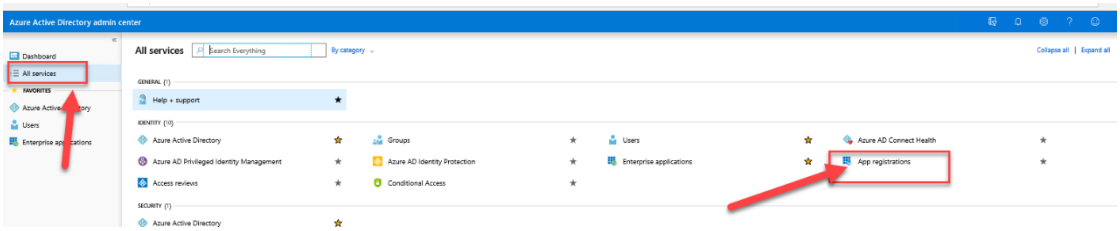


4. Now that the App has been setup. After you click on “Accept” the Azure Portal will open.

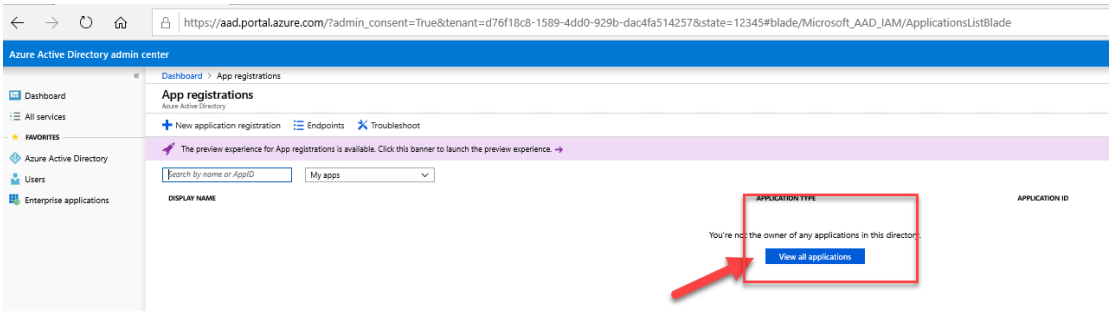
5. In the Azure Portal navigate to **Azure Active Directory** on the left navigation



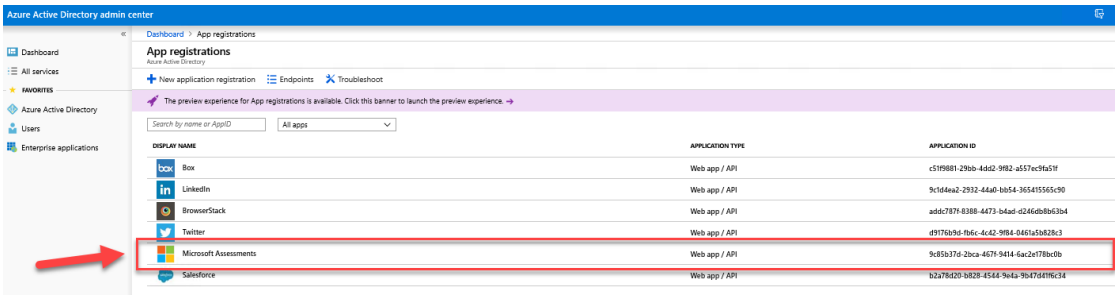
6. Click on “**All Services**” → “**App Registration**”



7. Click on "**View All Applications**"

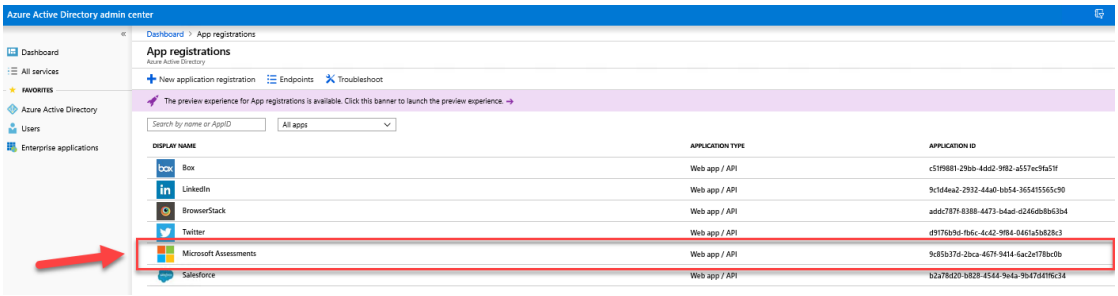


8. The new Microsoft Assessment Application will be listed

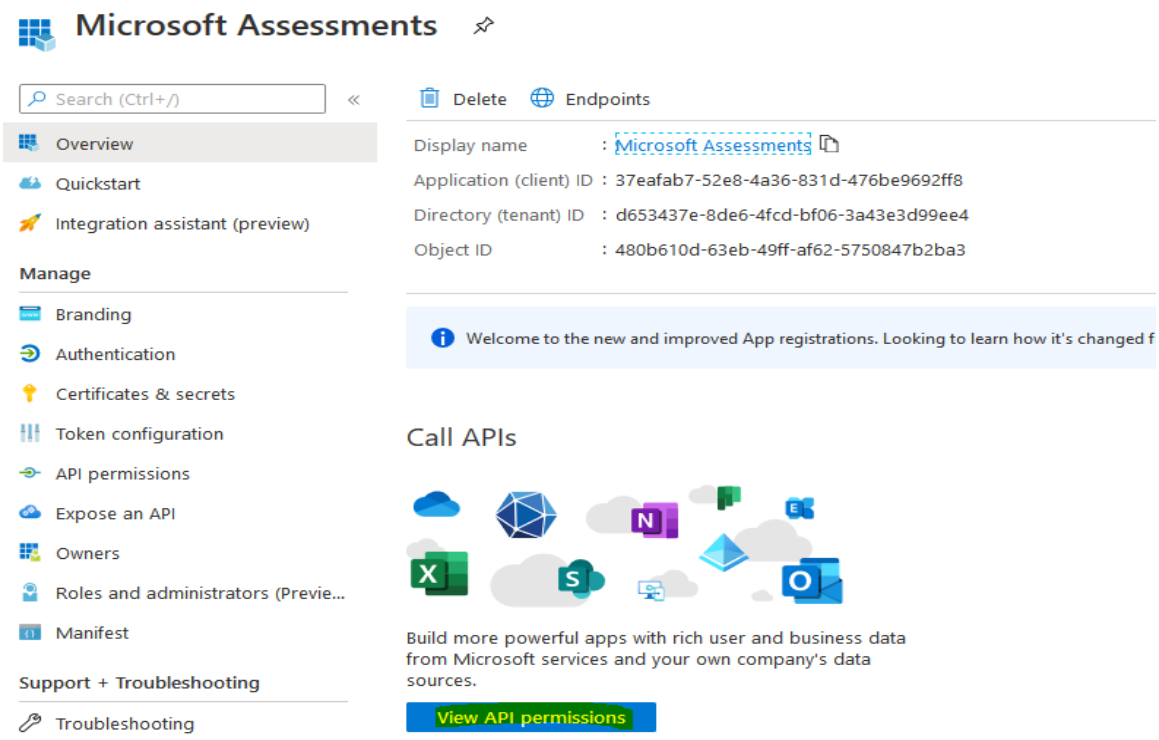


Setting permission to show Classic Workflows (if workflow report needed)

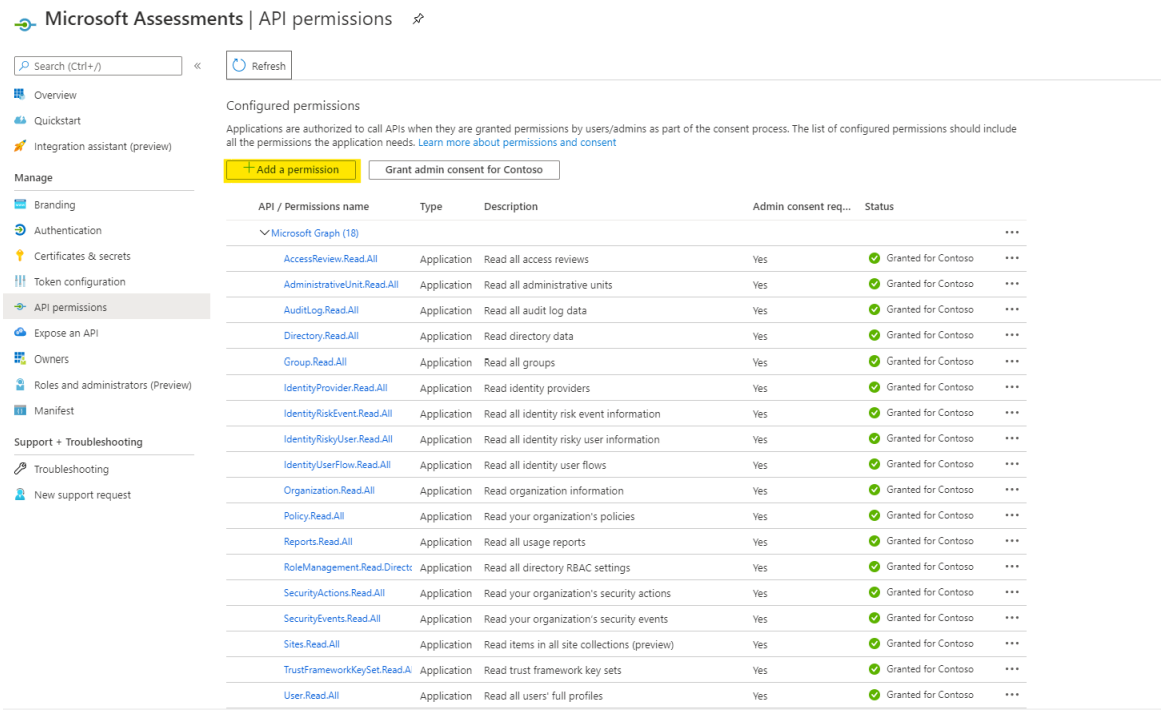
1. On the Azure portal, select ***[Azure Active Directory]*** > ***[App Registrations]*** and confirm the **"Microsoft Assessments"** app is present on the right pane.

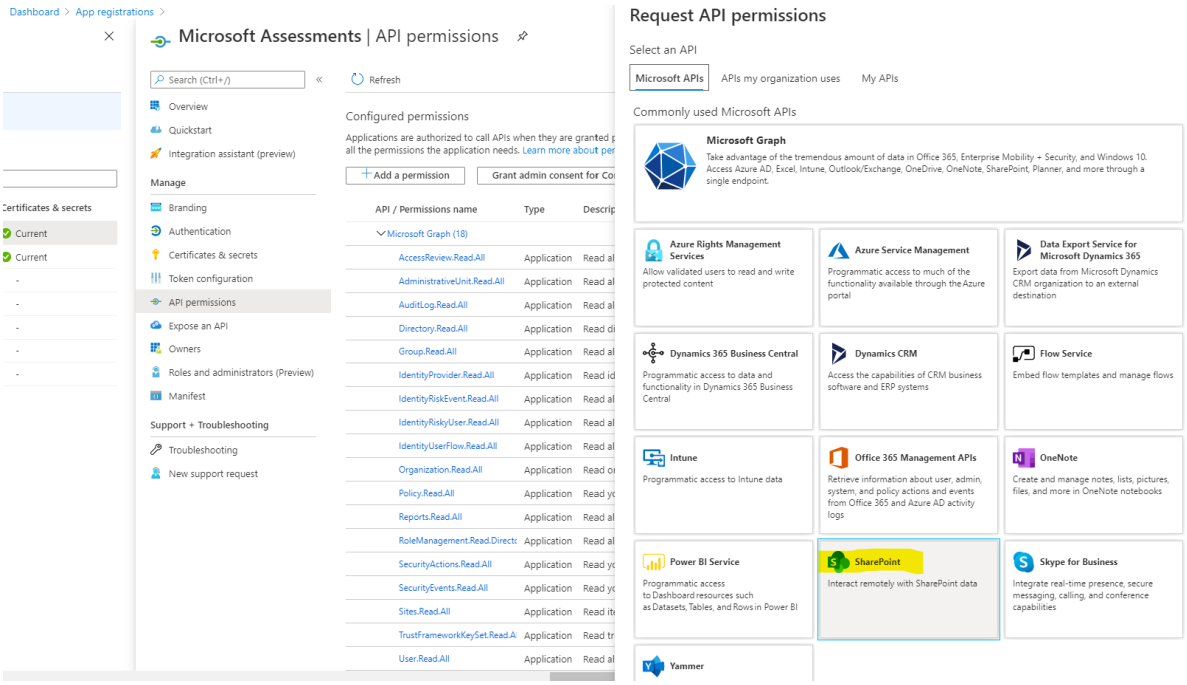


2. Click on the **Microsoft Assessment** Application to open it and click on **"View API Permissions"**.

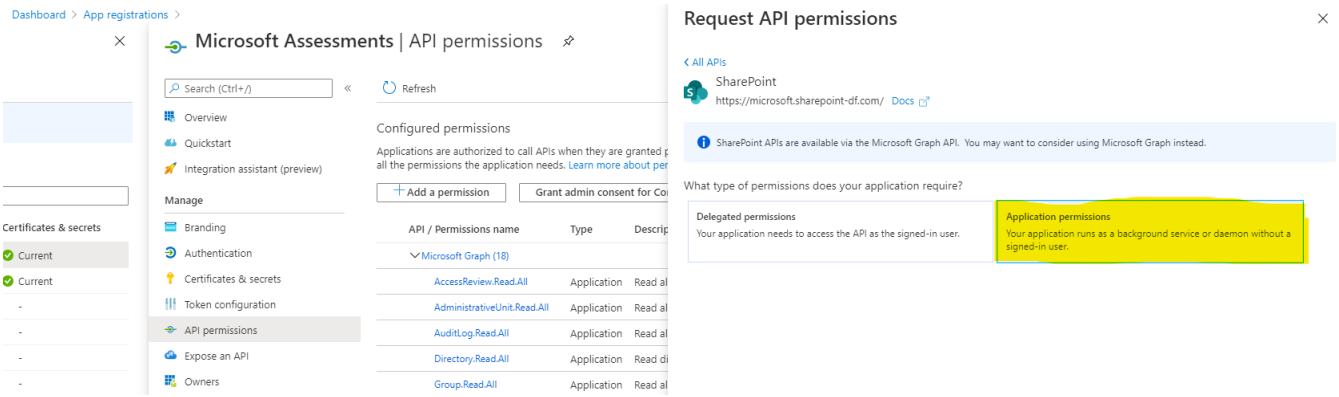


3. Under configured permissions in the middle of the page, click on "**Add a permission**" button, on the right pane select "**SharePoint**" under the Microsoft APIs tab.

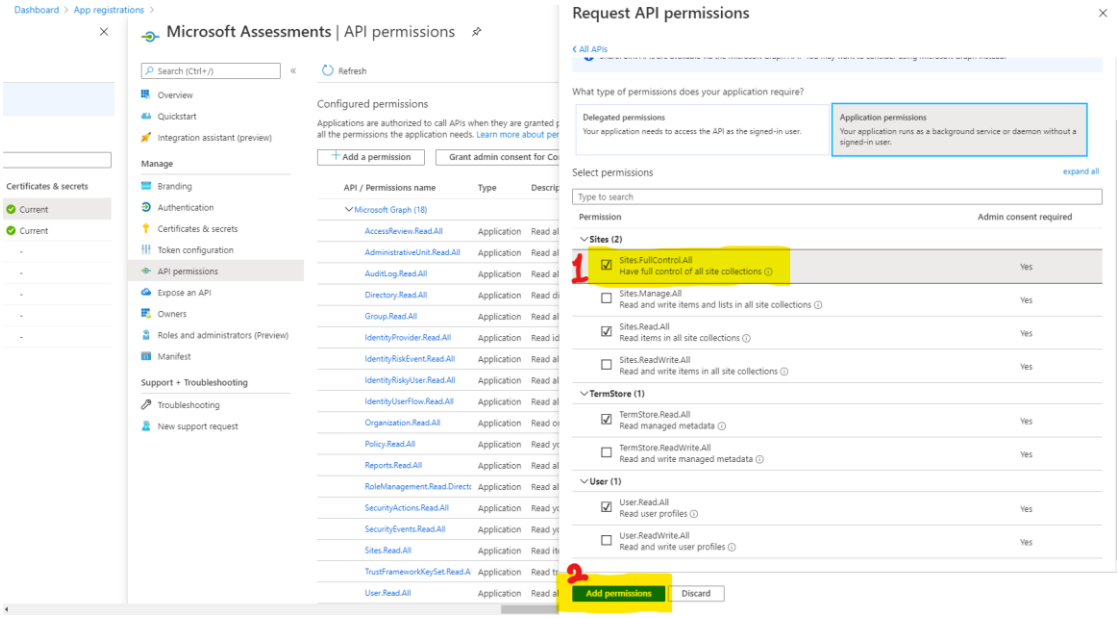




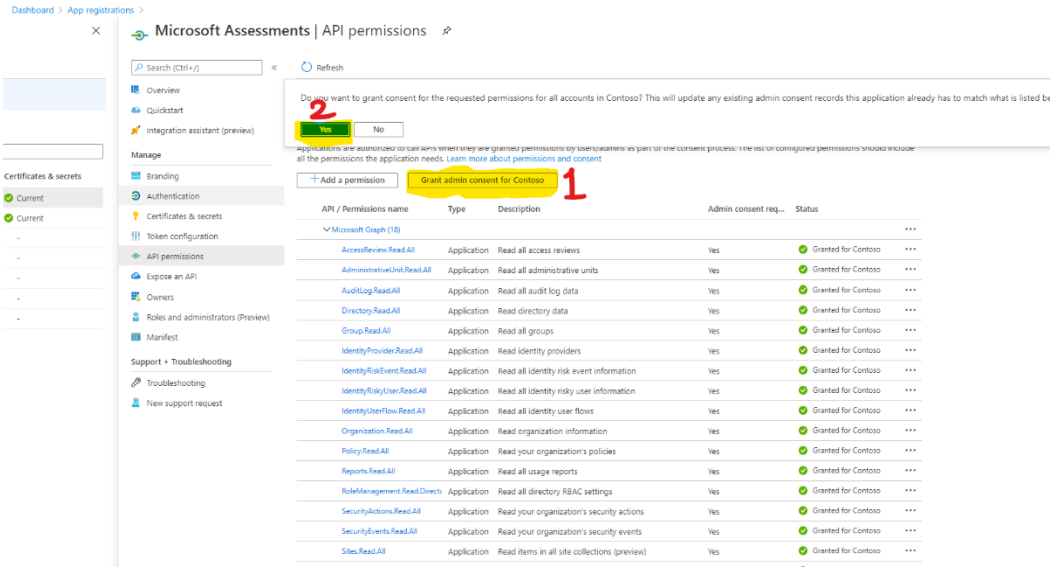
4. Select "**Application permissions**" for the type of permissions, this should open bottom part with list of permissions to select.



5. Select "**Sites.FullControl.All**" option and click on the "Add permissions" button on the bottom. You should receive notification that updating permissions.

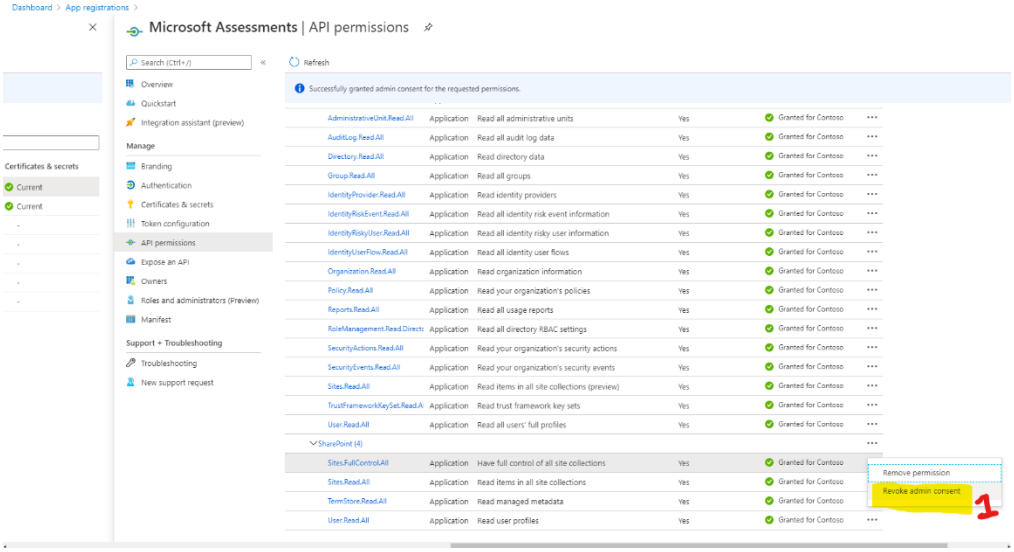


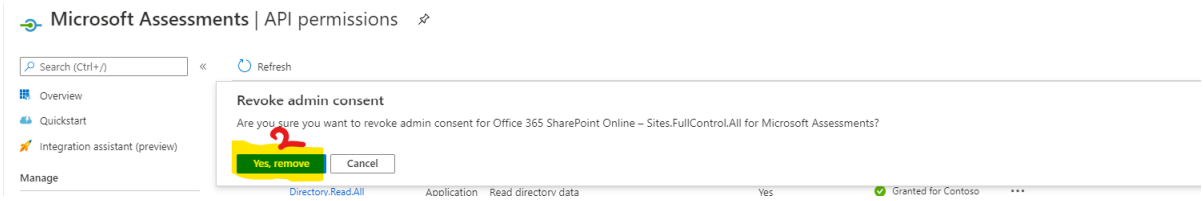
6. Since this permission requires Admin consent, scroll to the top of the screen, and click the "**Grant admin consent**" button on the middle. Ensure to click the confirmation prompt "**Yes**" for granting admin consent.



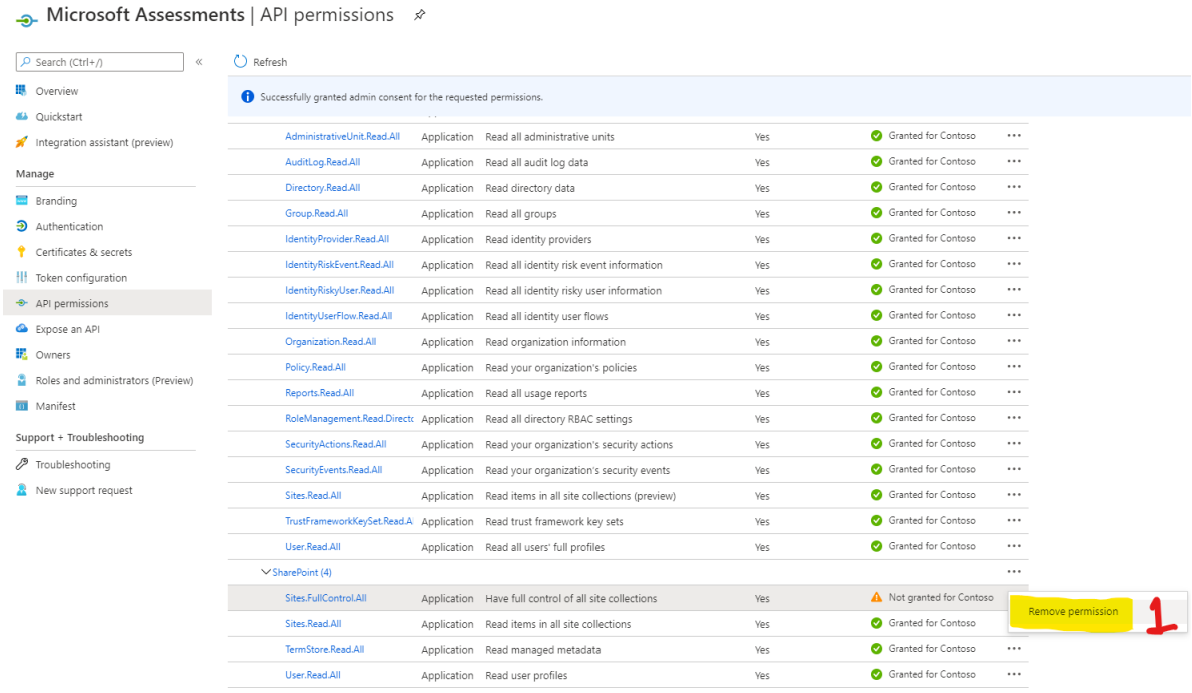
7. If you need to remove this permission after the assessment run is complete, you can certainly remove it, but any later runs will not report classic workflows.
8. To revoke admin consent "**Sites.FullControl.All**" permissions, within API permissions, scroll to bottom under SharePoint category of permissions, select the ellipsis(…) on the right corresponding to "**Sites.FullControl.All**" and click "**Revoke admin consent**" and confirm

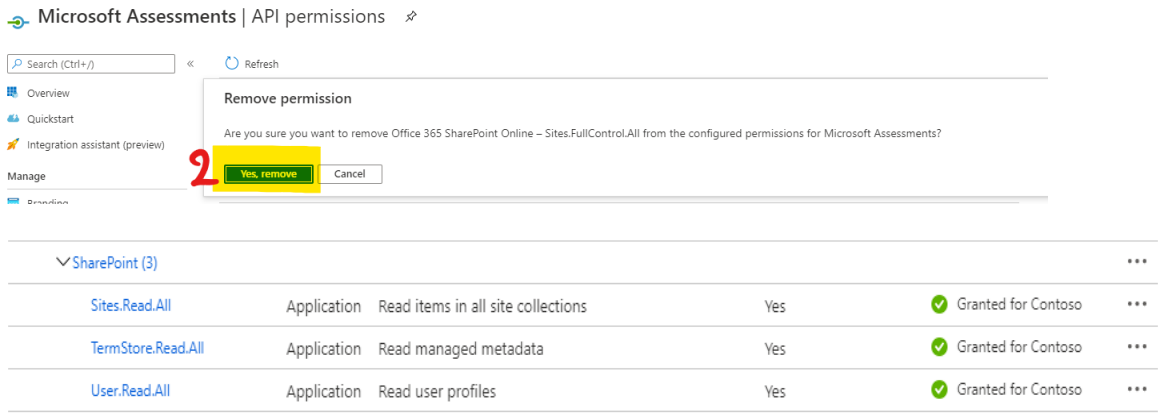
prompt “**Yes, remove**”.





9. To remove “**Sites.FullControl.All**” permissions, within API permissions, scroll to bottom under SharePoint category of permissions, select the ellipsis(…) on the right corresponding to “**Sites.FullControl.All**” and click “**Remove permission**” and confirm prompt “**Yes, remove**”.





10. Ensure final permissions of the SharePoint category looks like the above permissions list after revoking and removing "**Sites.FullControl.All**" permission.

Install Prerequisite Cmdlets

The Azure AD Preview Module is supported on the following Windows operating systems with the default version of Microsoft .NET Framework and Windows PowerShell: Windows 8.1, Windows 8, Windows 7, Windows Server 2012 R2, Windows Server 2012, or Windows Server 2008 R2.

If your computer has all the prerequisites for the installation, the module can be installed with the Install-Module cmdlet via PowerShell 5.0 or greater while Run as Administrator:

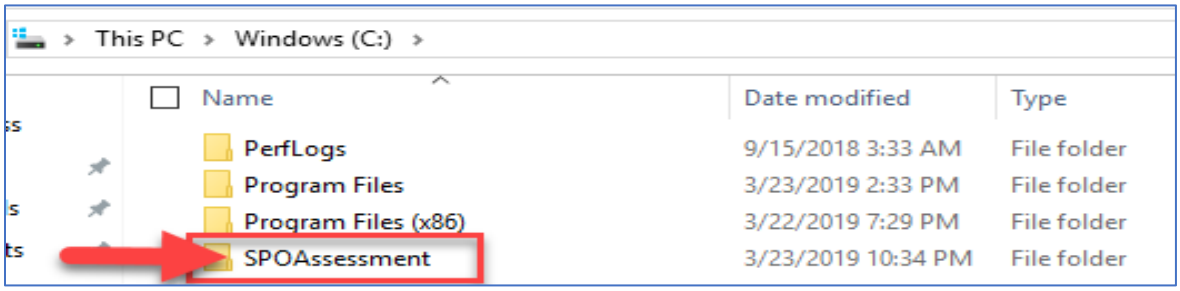
```
Set-ExecutionPolicy -ExecutionPolicy RemoteSigned
Install-Package Microsoft.Graph -Version 3.20.0
Install-Module SharePointPnPPowerShellOnline -Verbose -AllowClobber -Force
```

Setting up the SharePoint Online Assessment

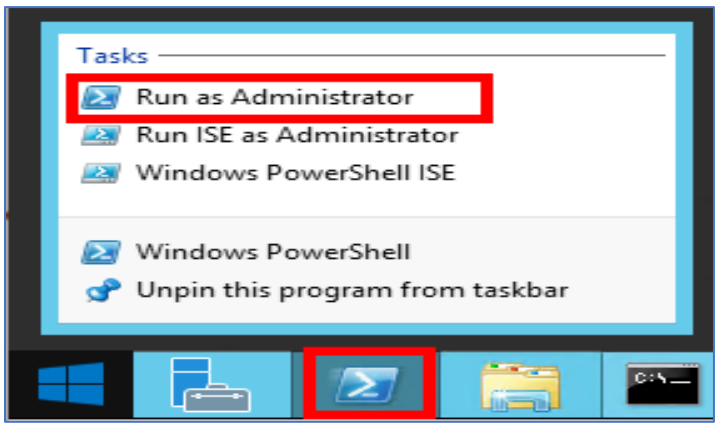
With the enabled MFA account

On the designated data collection machine, complete the following:

1. Create the working directory for the Assessment data. i.e. C:\SPOAssessment



2. Open the Windows PowerShell command prompt as an Administrator



3. Run the following command:
4. Where <Directory> is the path to an existing directory used to store the files created while collecting and analyzing the data from the environment.

```
Add-SharePointOnlineAssessmentTask -WorkingDirectory <Directory>
```

Example:

Add-SharePointOnlineAssessmentTask –WorkingDirectory “C:\SPOOA”

```
PS C:\windows\system32> Add-SharePointOnlineAssessmentTask -WorkingDirectory "C:\SPOOA"

cmdlet Add-SharePointOnlineAssessmentTask at command pipeline position 1
Supply values for the following parameters:
(Type !? for Help.)
ScheduledTaskUsername: Administrator
ScheduledTaskPassword: ************
[SharePointOnlineAssessment]Performing Credentials Validation
[SharePointOnlineAssessment]Detected agent configuration for Management Group AOI-b88c58fa-f16f-4bdc-adc4-829bb231f1ea
[SharePointOnlineAssessment][2812]To start an SharePointOnlineAssessment the Administrator user must have the 'Log on as
 a batch job' right. Please verify using Local Security Policy manager.

[SharePointOnlineAssessment]Creating Windows Schedule task to run assessment...
[SharePointOnlineAssessment]Task Creation Successful
[SharePointOnlineAssessment]SharePointOnlineAssessment setup successful.
[SharePointOnlineAssessment]Detailed log is at: C:\Users\Administrator\AppData\Local\Temp\Assessments_Configuration_2019
1008_041053.log
[SharePointOnlineAssessment][2804]To receive continued assessment updates, please close this Powershell window
```

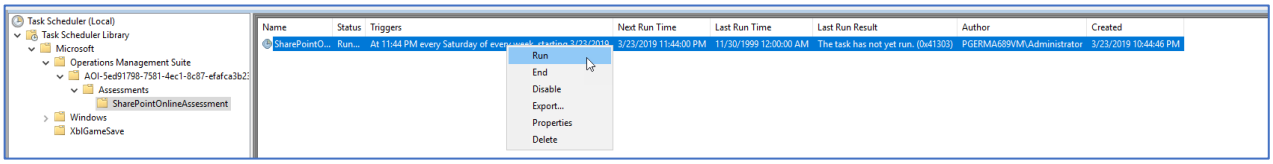
5. You will be promoted to enter an account that will be able to run a scheduled task on the Tools machine. Supply the required user account credentials to tun the Scheduled Task. These credentials are used to run the SharePoint Online Assessment.

> Note:
> *1. The account used to setup the assessment task needs to be a local admin in the Tool Machine, it can a local account or a Domain account with full admin right on the Tool Machine. if using local account just enter the account name and password, if using a domain account use the format Domain\Account.*
> *2. Ensure that when setting up the assessment task, the account that will be used to run the scheduled task is the account that is used to log in and setup the assessment task.*

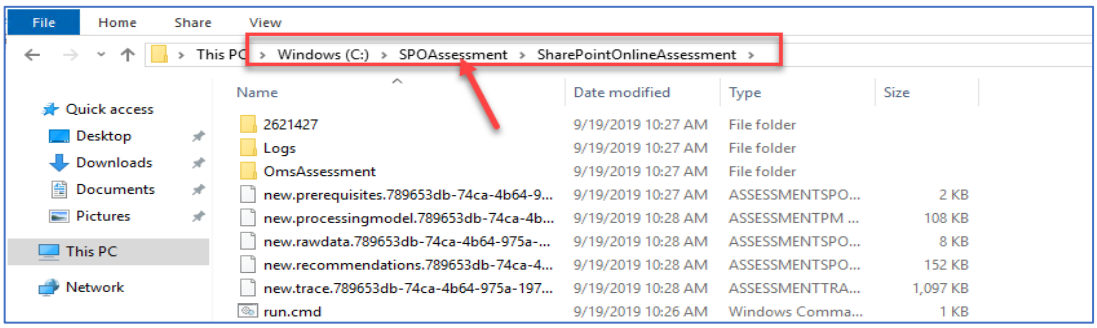
6. The script will continue with the necessary configuration. It will create a scheduled task that will trigger the data collection.

7. Data collection is triggered by the **scheduled task** named **SharePointOnlineAssessment** within an hour of running the previous script and then every 7 days. The task can be changed to run on a different date/time or even forced to run at once.

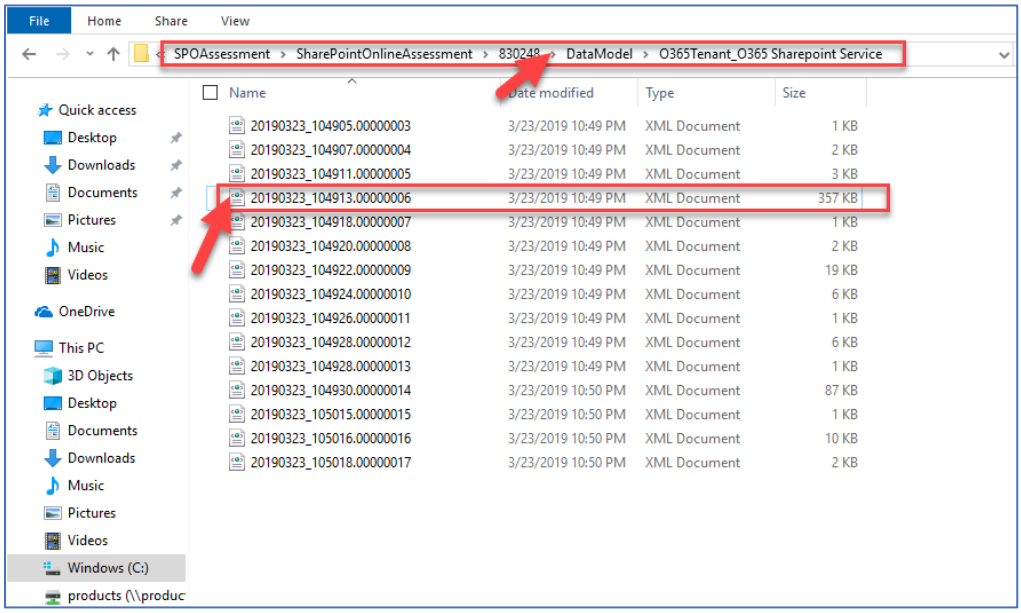
8. You can confirm the Task is created in **Task Scheduler** and you can “Right Click” on the Task to **Run** it.



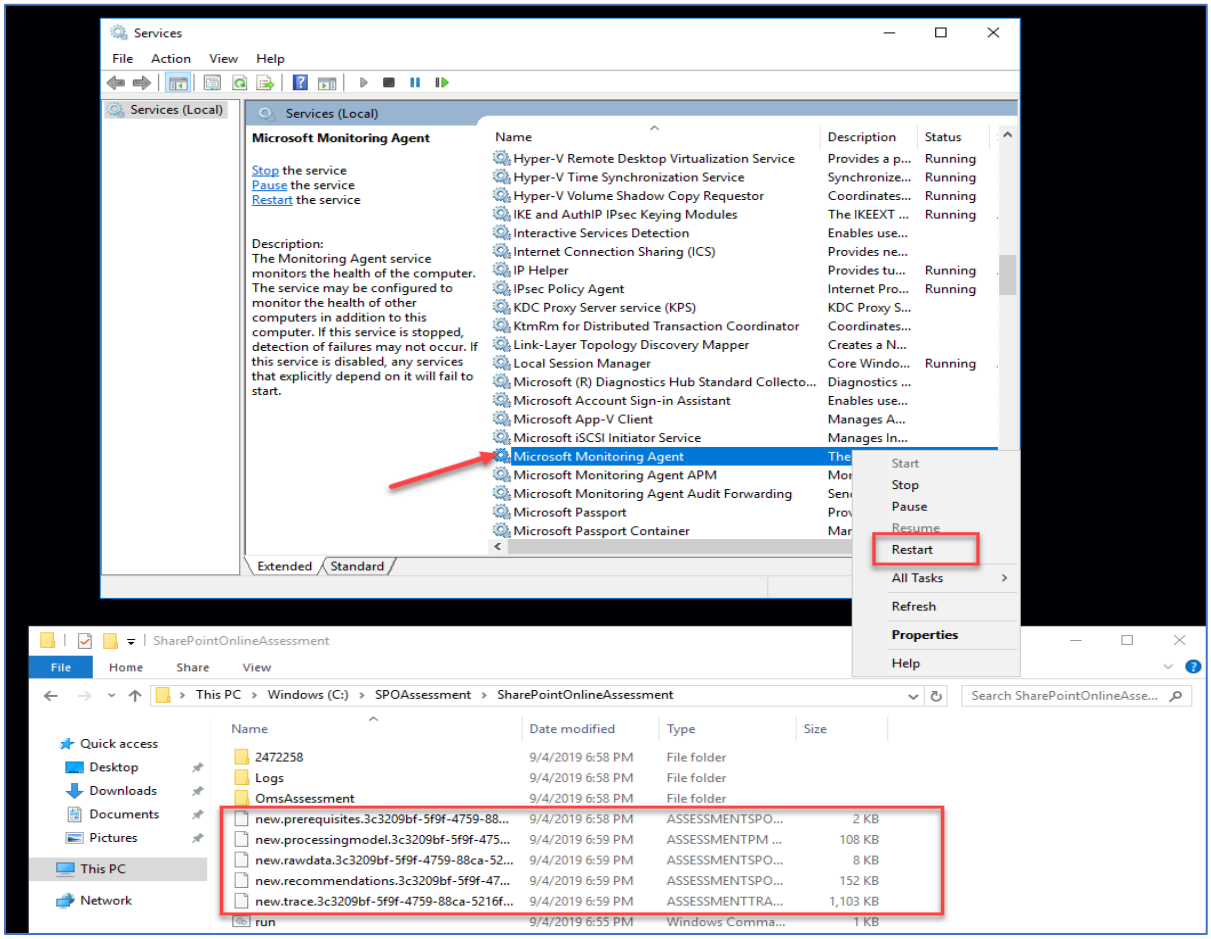
9. During collection and analysis, data is temporarily stored under the **WorkingDirectory** folder that was configured during setup, using the following structure:



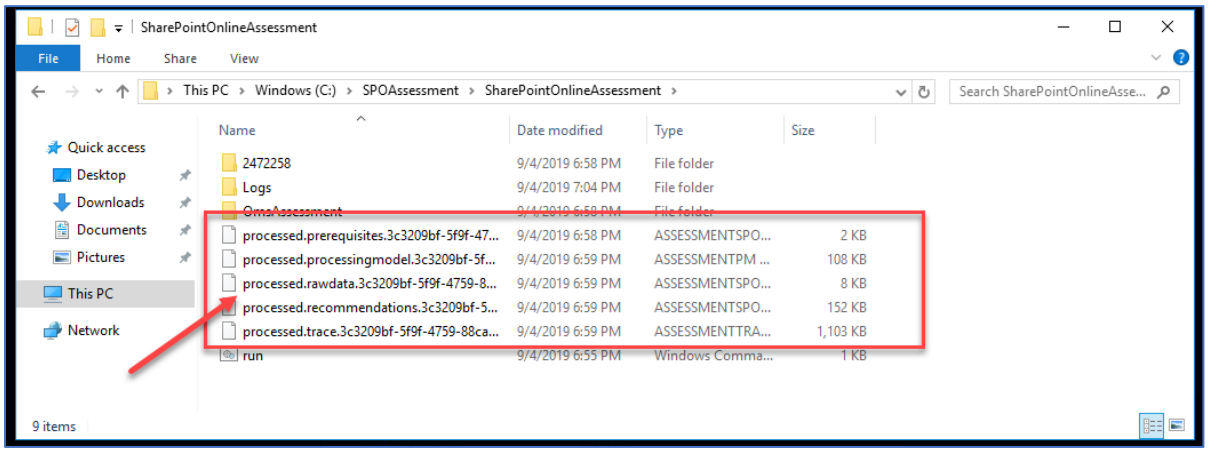
10. After the completion of the task, you can Verify the XML files are created under the DataModel folder,



11. Restart the **MMA** service, you will notice under the **SharePointAssessment** Folder file with prefix of “new”



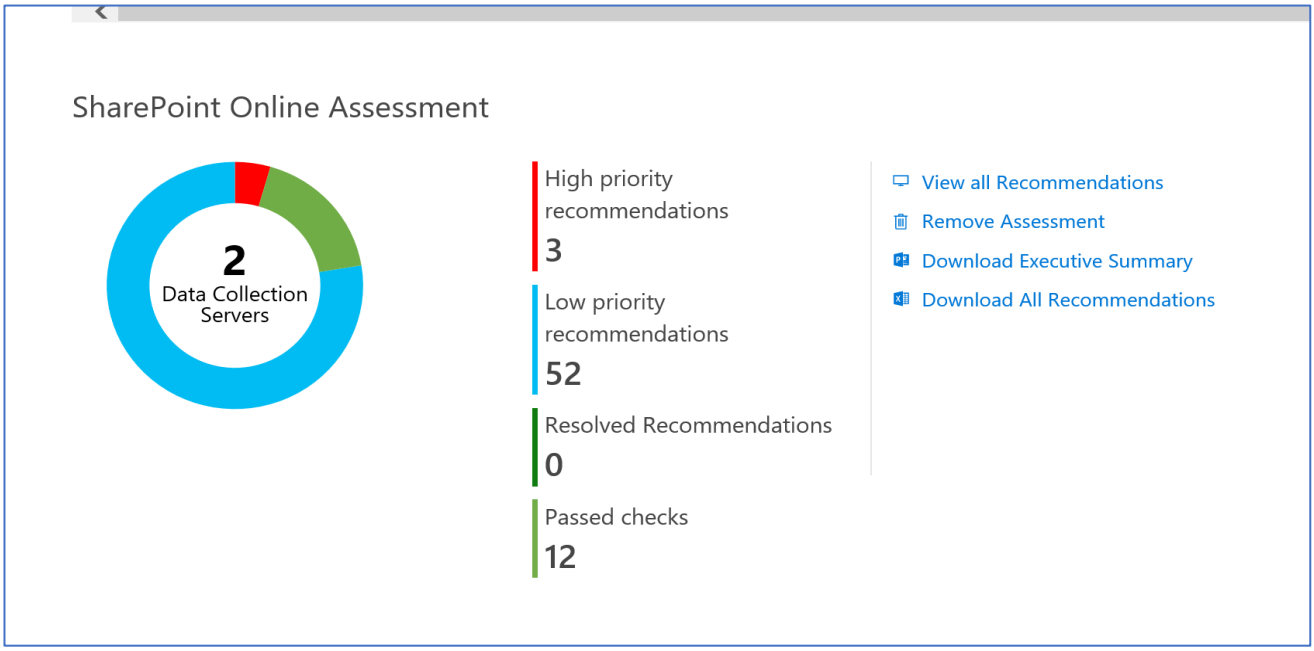
12. After Restarting the MMA Agent, the prefix of “new” will be changed to “processed”



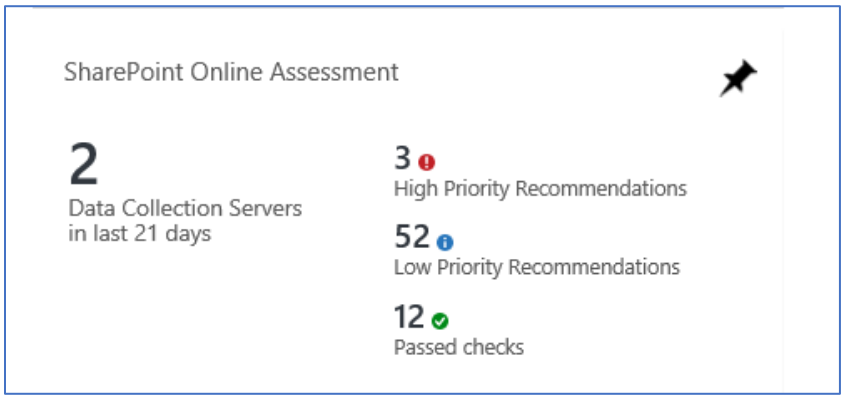
13. After data collection and analysis is completed on the tools machine, it will be submitted to your Azure Log Analytics workspace.

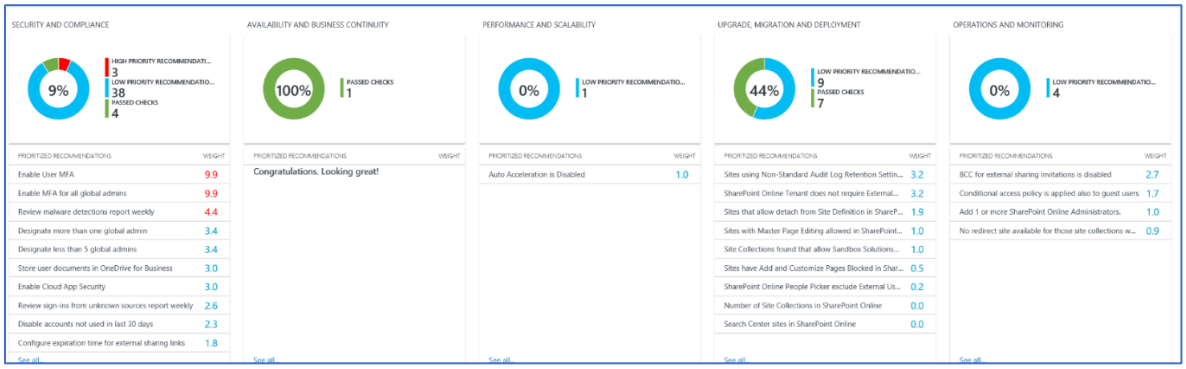
Note: *Data Collection takes approximately 30 to 60 minutes.*

14. Your assessment results will be available to view on your **Service hub** Dashboard. Click the **SharePoint Online Assessment** and click on “View All Recommendations” to review:



15. You will then be presented with findings grouped by the focus area.

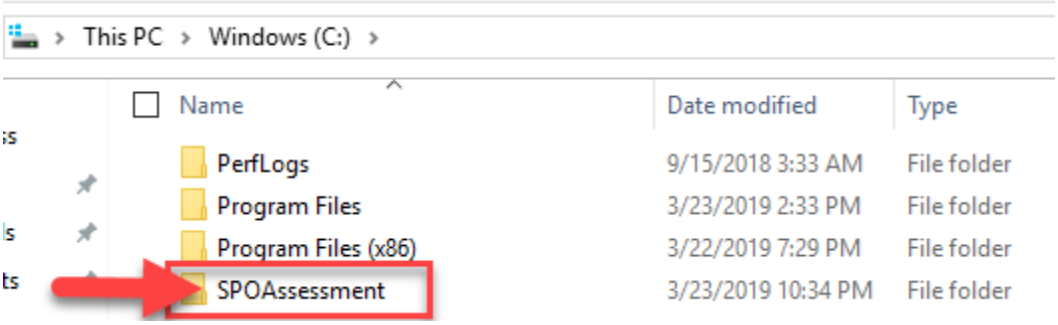




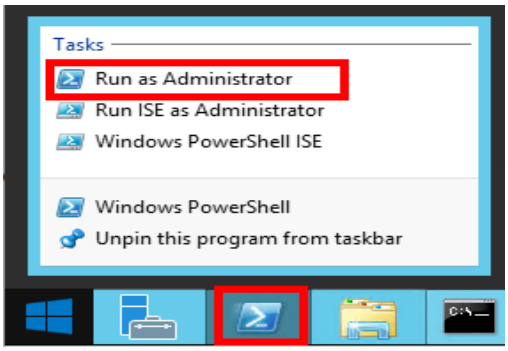
With the disabled MFA account

On the designated data collection machine, complete the following:

1. Create the working directory for the Assessment data. i.e. **C:\SPOAssessment**

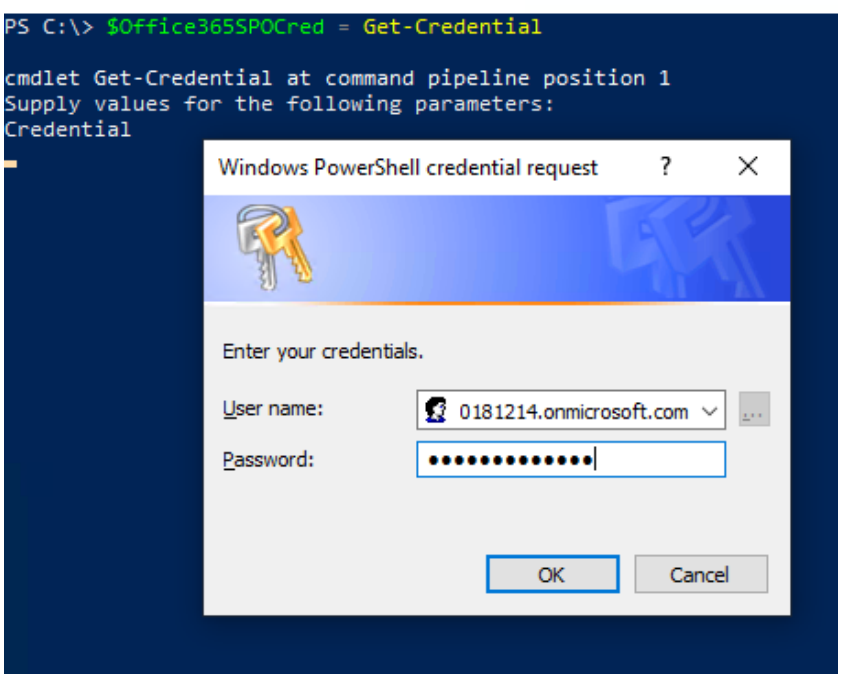


2. Open the Windows PowerShell command prompt as an Administrator



3. Define the Credentials for the assessment to use:
   - Ex. `$Office365SPOCred = Get-Credential`

   You will be prompted to enter the GA account and password

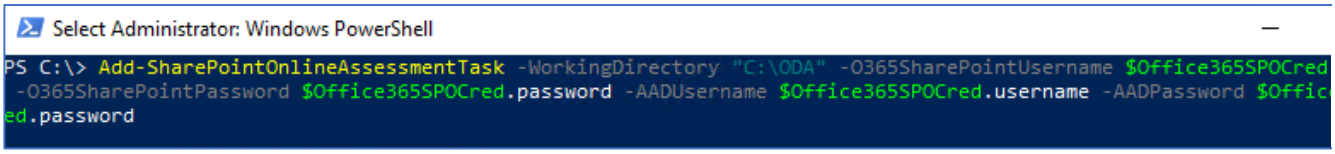


4. Run the following command:
   Where *<Directory>* is the path to an existing directory used to store the files created while collecting and analyzing the data from the environment.

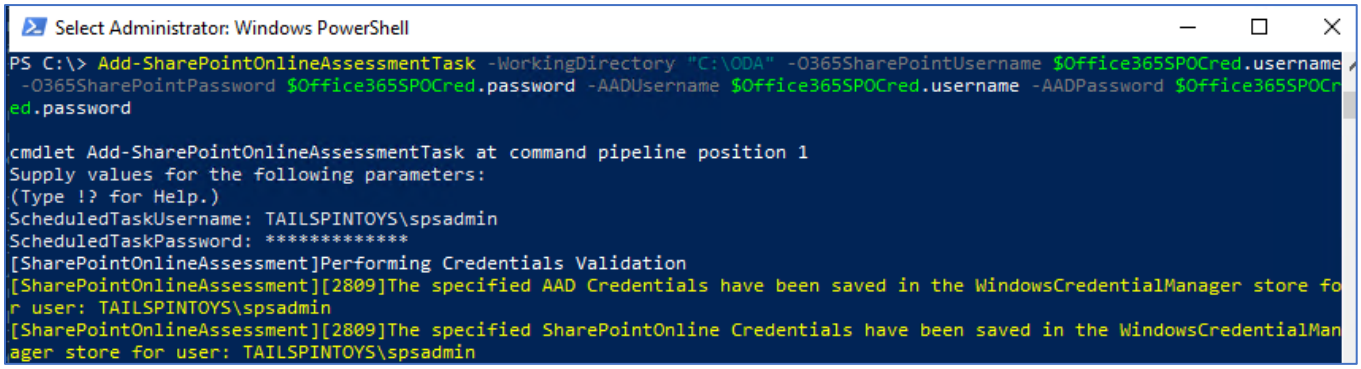
```
Add-SharePointOnlineAssessmentTask -WorkingDirectory <Directory> -O365SharePointUsername
$Office365SPOCred.username -O365SharePointPassword $Office365SPOCred.password -AADUsername
$Office365SPOCred.username -AADPassword $Office365SPOCred.password
```

   Example:

```
$Office365SPOCred = Get-Credential
Add-SharePointOnlineAssessmentTask -WorkingDirectory "C:\ODA" -O365SharePointUsername
$Office365SPOCred.username -O365SharePointPassword $Office365SPOCred.password -AADUsername
$Office365SPOCred.username -AADPassword $Office365SPOCred.password
```



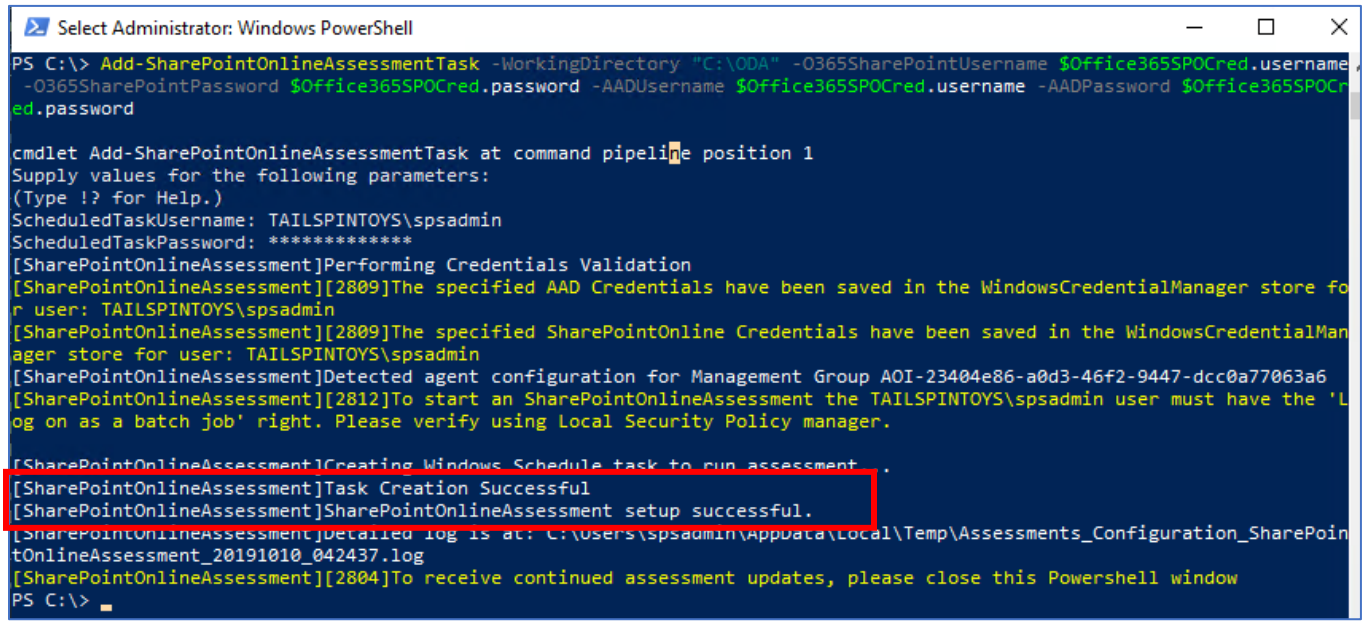
5. You will be promoted to enter an account that will be able to run a scheduled task on the Tools machine. Provide the required user account credentials to tun the Scheduled Task. These credentials are used to run the SharePoint Online Assessment.



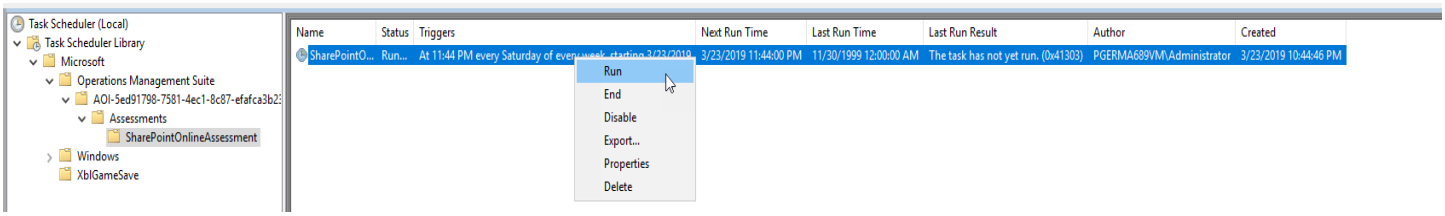
> Note:
> *1. The account used to setup the assessment task needs to be a local admin in the Tool Machine, it can a local account or a Domain account with full admin right on the Tool Machine. if using local account just enter the account name and password, if using a domain account use the format Domain\Account.*
> *2. Ensure that when setting up the assessment task, the account that will be used to run the scheduled task is the account that is used to log in and setup the assessment task.*

6. The script will continue with the necessary configuration. It will create a scheduled task that will trigger the data collection.

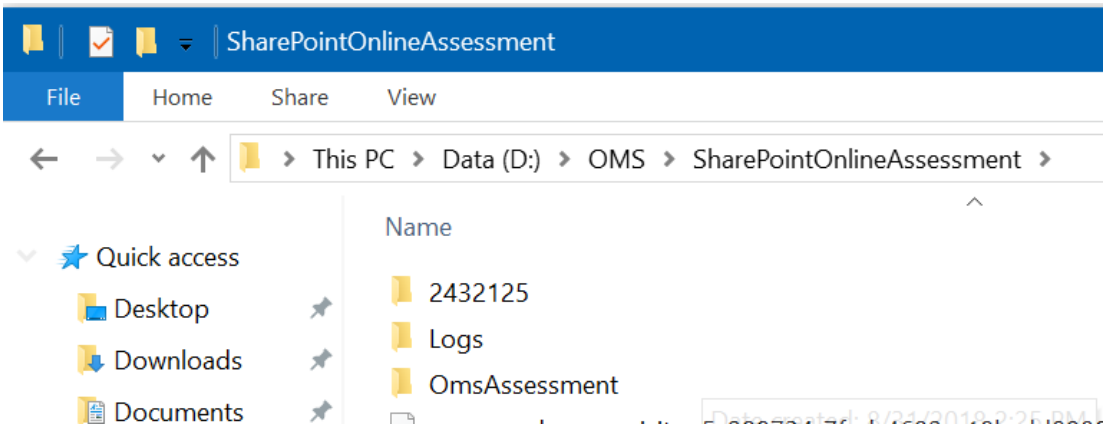
7. Data collection is triggered by the **scheduled task** named **SharePointOnlineAssessment** within an hour of running the previous script and then every 7 days. The task can be modified to run on a different date/time or even forced to run immediately.



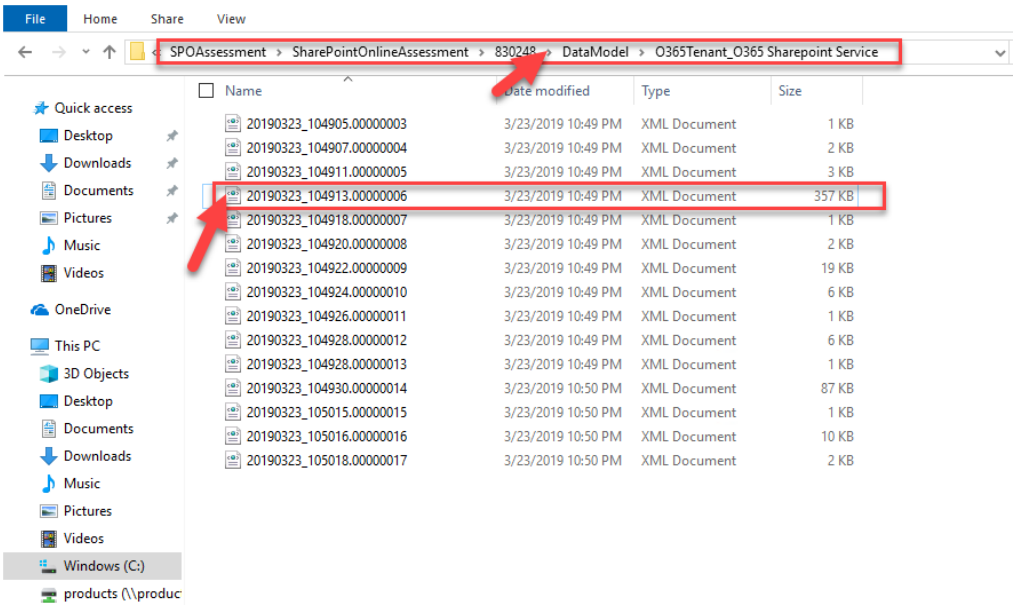
`You can confirm the Task is created in Task Scheduler and you can “Right Click” on the Task to run it.



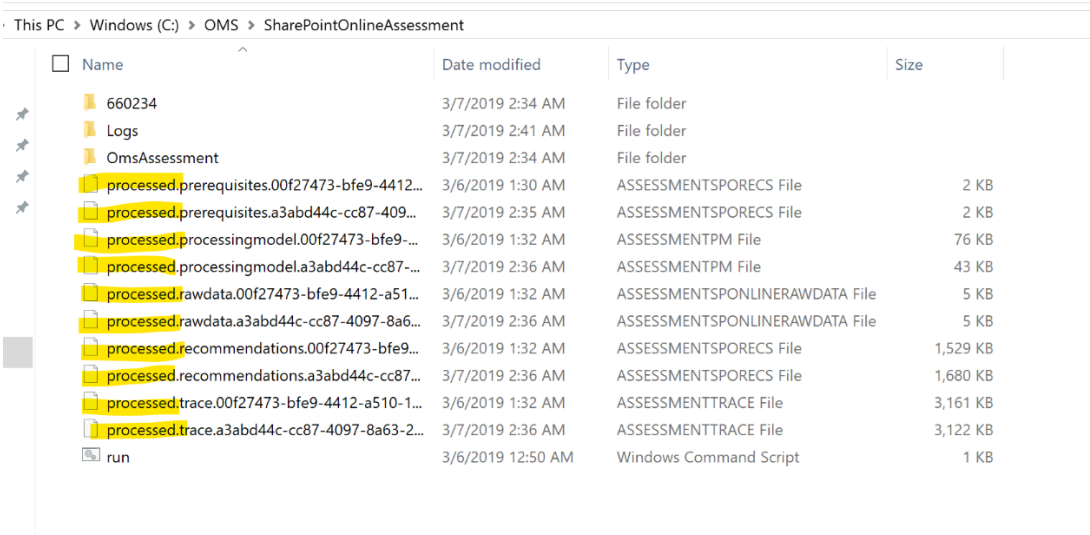
8. During collection and analysis, data is temporarily stored under the **WorkingDirectory** folder that was configured during setup, using the following structure:



After the completion of the task, you can verify that the XML files are created under the DataModel folder, for example the XML file ending on 00006, will include the SecureScore data.

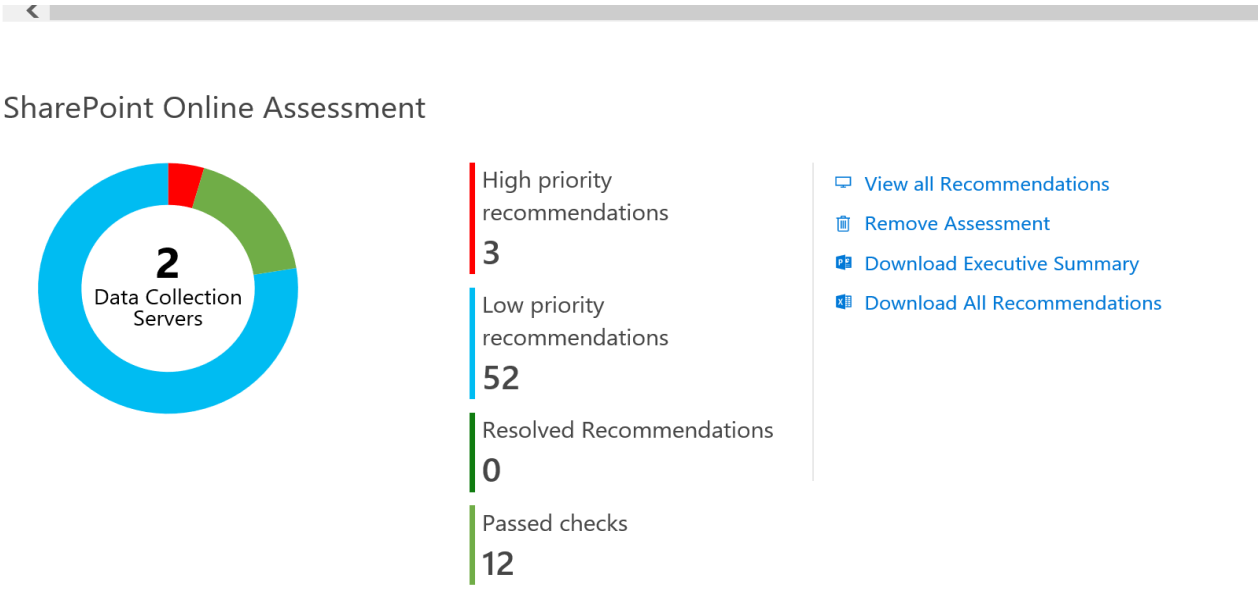


9. Once the data collection and the submission are completed on the tools machine, it will be submitted to your Azure Log Analytics workspace.
10. After collection and submission, the MMA service is restarted and the files on tools machine show a prefix “processed”.

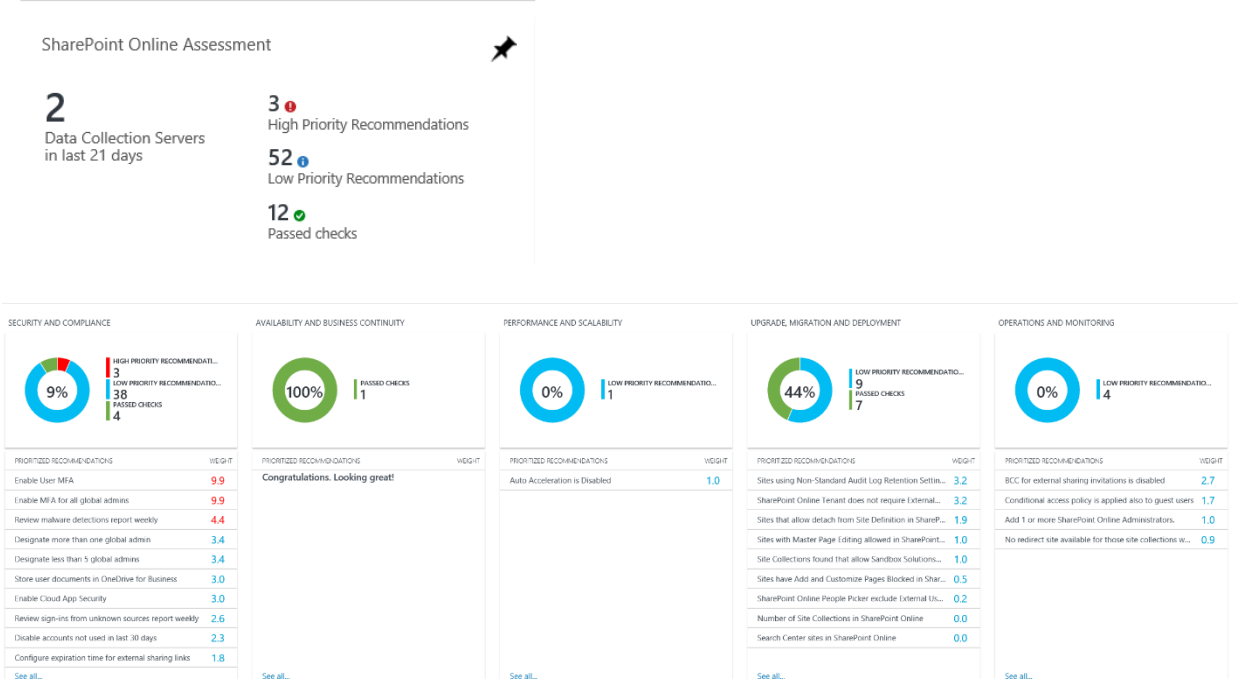


11. Data Collection takes approximately 30 to 60 minutes.

12. Your assessment results will be available on your Service Hub Dashboard. Click the **SharePoint Online Assessment** and click on “View All Recommendations” to review:



13. You will then be presented with findings grouped by the focus area.



Appendix

Data Collection Methods

The **Office 365 SharePoint Assessment** uses multiple data collection methods to collect information from your environment. This section describes the methods used to collect data from your environment. No Microsoft Visual Basic (VB) scripts are used to collect data.

Data collection uses workflows and collectors. The collectors are:

1. Microsoft Graph API
2. Microsoft PowerShell
3. SharePoint Modernization Scanner

Microsoft Graph API

The Microsoft Graph API is used to get data pertaining to Office 365 Secure Score.

Microsoft PowerShell

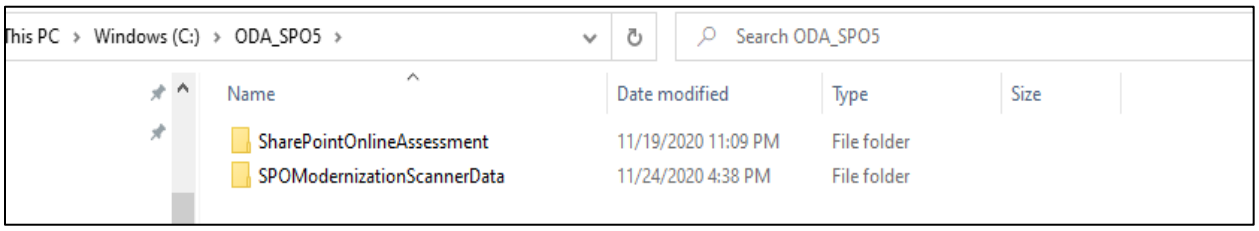
PowerShell is used to collect data from both Azure AD and Office 365. PowerShell uses the cmdlets from Azure PowerShell, SharePoint Management Shell and Patterns and Practices PnP) cmdlets to connect to and pull the required configuration settings pertaining to the tenant.

SharePoint Modernization Scanner

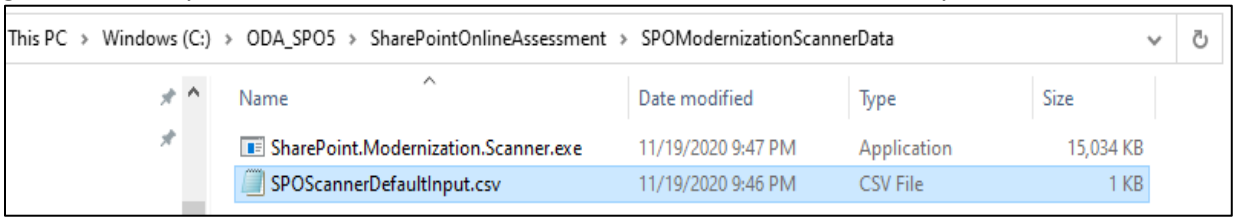
SharePoint Modernization Scanner under the covers uses SharePoint Online CSOM to collect site level configurations which will be used for analysis and recommendation towards modernizing the sites. By default, the scanner collects data only from classic sites on the tenant. If you have a need to report more than just classic sites, you can configure custom csv input file with list of site URLs for the scanner to collect data from.

Setting up Custom Input File for the scanner (Optional):

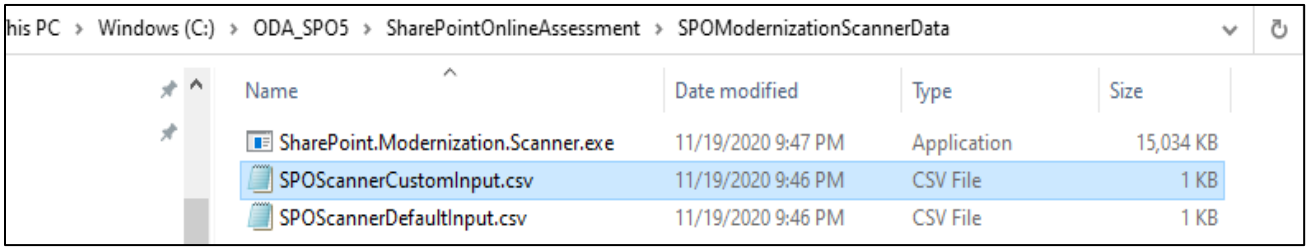
- By default, when you run the OnDemand Assessment first time, this will create a "SPOModernizationScannerData" folder under working directory (e.g.: C:\ODA_SPO5) you configured for SharePoint Online Assessment task creation under the scheduler. In the example below, "C:\ODA_SPO5" is the working directory for SharePoint Online Assessment.



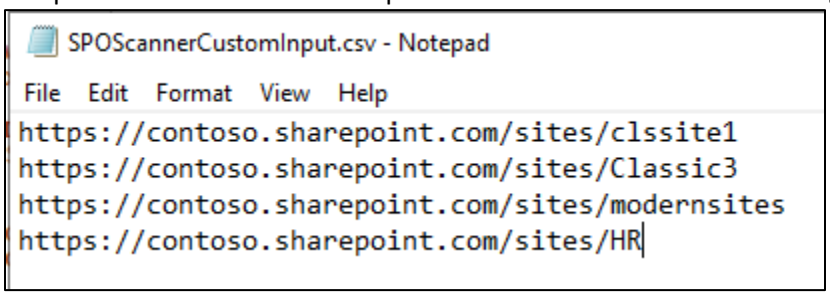
- Inside the "SPOModernizationScannerData" folder, you will see that "SPOScannerDefaultInput.csv" file is generated every time when data collection starts from Task Scheduler manually or as scheduled.



- SPOScannerDefaultInput.csv contains classic site URLs within the tenant. This will be used by the SharePoint Modernization Scanner tool by default for scanning.
- If you wish to change to different list of sites to scan, you can make a copy of the SPOScannerDefaultInput.csv or create your own file with list of URLs with the name: SPOScannerCustomInput.csv like the following:



- If you want your assessment to start the first time with custom list of sites for scanner to use, you will have to create the "SPOModernizationScannerData" folder manually and place the custom csv file with filename you see on the previous step as SPOScannerCustomInput.csv.
- Sample of SPOScannerCustomInput.csv files will look like the following:



Office 365 Assessment – Authentication Model

The Office 365 Assessment collects data using 2 methods:

1. Microsoft Graph
2. PowerShell Cmdlets
3. SharePoint Modernization Scanner

Graph API

The assessment connects to and extracts data form Microsoft Graph using an App created in Azure. The App is granted read permissions using OAuth. The data collection machine will have a certificate which is used to connect to the Azure App, which in turns gets the data from Microsoft Graph.

During the setup of the assessment, a Global Admin is required in order to create the App and grant it the relevant Read permissions so that it can query Microsoft Graph.

Once the setup is completed this part of the assessment will collect data with the App via the certificate with no account requirement. The App has only read access, which helps collect data using a least privileged model.

PowerShell Cmdlets

The assessment also collects data from Office 365 using the following cmdlets:

- Azure AD cmdlets
- SharePoint Online cmdlets

- SharePoint Online PnP cmdlets

Whilst these cmdlets currently support modern authentication to login, they are designed to run manually. This means the support of Modern Authentication is handled for accounts with MFA by a prompt to handle the authentication.

The assessment collects the data in an automated manner via a scheduled task. As this data collection is designed to run autonomously no prompts are generated. This causes an issue with account having MFA enabled, as when authenticating the account prompt for MFA does not appear and thus account cannot authenticate.

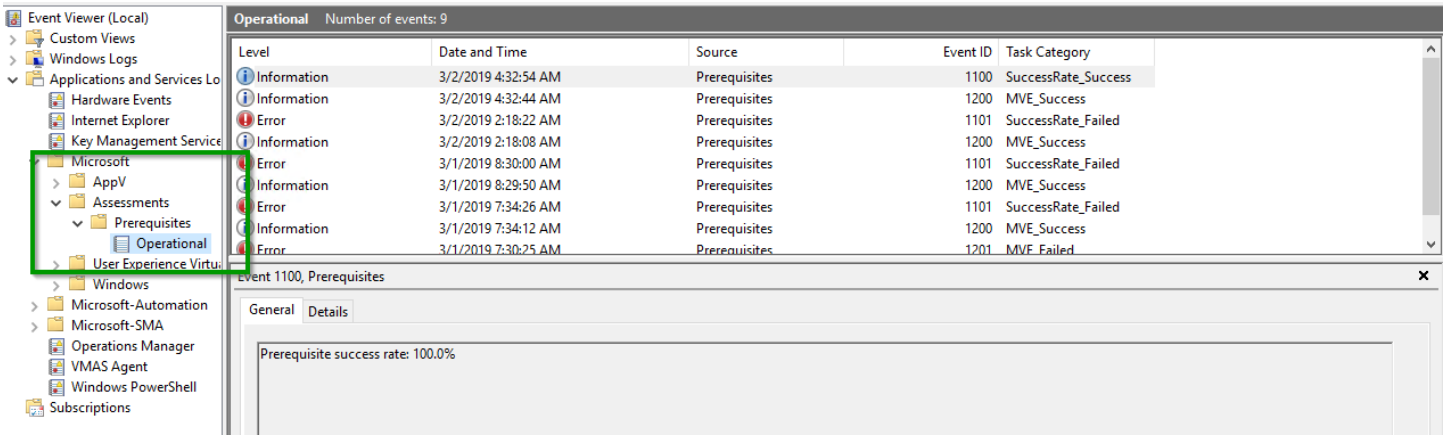
We are currently working with the PG on cmdlets that will support OAuth. With cmdlets that fully support OAuth we can use the Azure App to authenticate the requests made from the cmdlets. In doing so this will remove the requirement to use a Global Admin account, as well as the current requirement to use an account that does not have MFA.

SharePoint Modernization Scanner

SharePoint Modernization Scanner tool uses Azure AD App based authentication using OAuth authentication mechanism. As mentioned previously, SPO Scanner will by default will use only Sites.Read.All API permissions of Azure AD App for collection. Optionally, if you need to collect workflow related data, you will need to provide the Azure AD App, Sites.FullControl.All.

SharePoint Modernization Scanner will also be downloaded automatically using .NET web client when assessment is run the first time. After the first time run, the scanner version check will happen every time the assessment is run. Scanner check will ensure to check the version and download the latest only if the current version is not latest.

Download is performed the [GitHub repository] of the SharePoint Modernization Scanner. As you can see, we use only https endpoints for the downloads and on top of that we also ensure the SHA512 bit checksum matches to ensure data integrity and security.

View Prerequisite Errors

You can check the event viewer to view errors pertaining to prerequisites.