# Securing privileged access

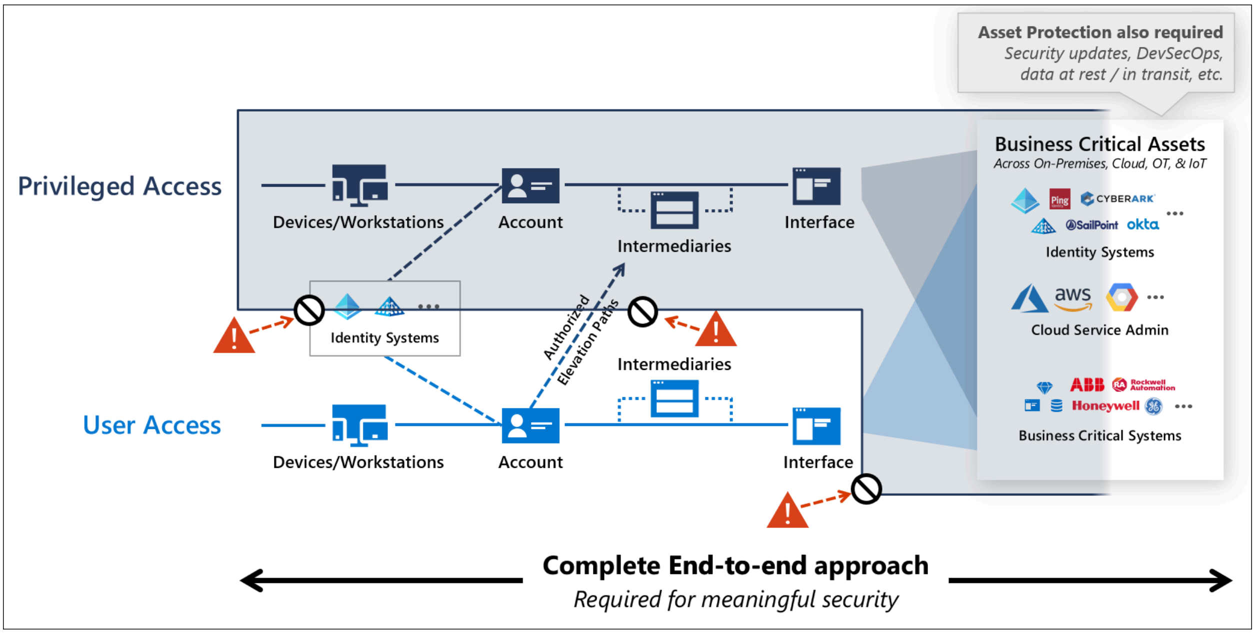
Article • 06/20/2024

Organizations should make securing privileged access the top security priority because of the significant potential business impact, and high likelihood, of attackers compromising this level of access.

Privileged access includes IT administrators with control of large portions of the enterprise estate and other users with access to business-critical assets.

Attackers frequently exploit weaknesses in privileged access security during human-operated ransomware attacks and targeted data theft. Privileged access accounts and workstations are so attractive to attackers because these targets allow them to rapidly gain broad access to the business assets in the enterprise, often resulting in rapid and significant business impact.

The following diagram summarizes the recommended privileged access strategy to create an isolated virtual zone that these sensitive accounts can operate in with low risk.



Securing privileged access effectively seals off unauthorized pathways completely and leaves a select few authorized access pathways that are protected and closely monitored. This diagram is discussed in more detail in the article, Privileged Access Strategy.

Building this strategy requires a holistic approach combining multiple technologies to protect and monitor those authorized escalation paths using Zero Trust principles including explicit validation, least privilege, and assume breach. This strategy requires multiple complementary initiatives that establish a holistic technology approach, clear processes, and rigorous operational execution to build and sustain assurances over time.

## Get started and measure progress

⛶ Expand table

| Image | Description | Image | Description |
|---|---|---|---|
| | Rapid Modernization Plan (RaMP) - Plan and implement the most impactful quick wins | | Best practices Videos and Slides |

## Industry references

Securing privileged access is also addressed by these industry standards and best practices.

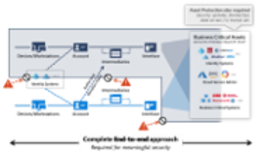
⛶ Expand table

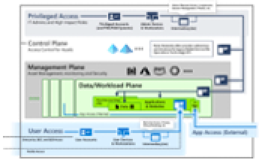
| | | |
|---|---|---|
| **UK National Cyber Security Center (NCSC)** | **Australian Cyber Security Center (ACSC)** | **MITRE ATT&CK** |

## Next steps

Strategy, design, and implementation resources to help you rapidly secure privileged access for your environment.

⛶ Expand table

| Image | Article | Description |
|---|---|---|
|  Devices/Workstations<br>Account<br>Intermediaries<br>Interface<br>Identity Systems<br>Business Critical Assets<br>Complete End-to-end approach<br>Required for meaningful security | Strategy | Overview of privileged access strategy |
| Defender's cost<br>$$$<br>$$<br>$<br>Attacker's cost<br>$$$<br>$$<br>$ | Success criteria | Strategic success criteria |

| Image | Article | Description |
|---|---|---|
| | Security levels | Overview of security levels for accounts, devices, intermediaries, and interfaces |
| | Accounts | Guidance on security levels and controls for accounts |
| | Intermediaries | Guidance on security levels and controls for intermediaries |
| | Interfaces | Guidance on security levels and controls for interfaces |
| | Devices | Guidance on security levels and controls for devices and workstations |
|  | Enterprise access model | Overview of Enterprise Access Model (successor to legacy tier model) |
| | ESAE Retirement | Information on retirement of legacy administrative forest |

# Privileged access: Strategy

Article • 06/20/2024

Microsoft recommends adopting this privileged access strategy to rapidly lower the risks to your organization from high impact and high likelihood attacks on privileged access.

***Privileged access should be the top security priority at every organization.*** Any compromise of these users has a high likelihood of significant negative impact to the organization. Privileged users have access to business critical assets in an organization, nearly always causing major impact when attackers compromise their accounts.

This strategy is built on Zero Trust principles of explicit validation, least privilege, and assumption of breach. Microsoft provides implementation guidance to help you rapidly deploy protections based on this strategy

> ⓘ **Important**
>
> There is no single "silver bullet" technical solution that will magically mitigate privileged access risk, you must blend multiple technologies together into a holistic solution that protects against multiple attacker entry points. Organizations must bring the right tools for each part of the job.

## Why is privileged access important?

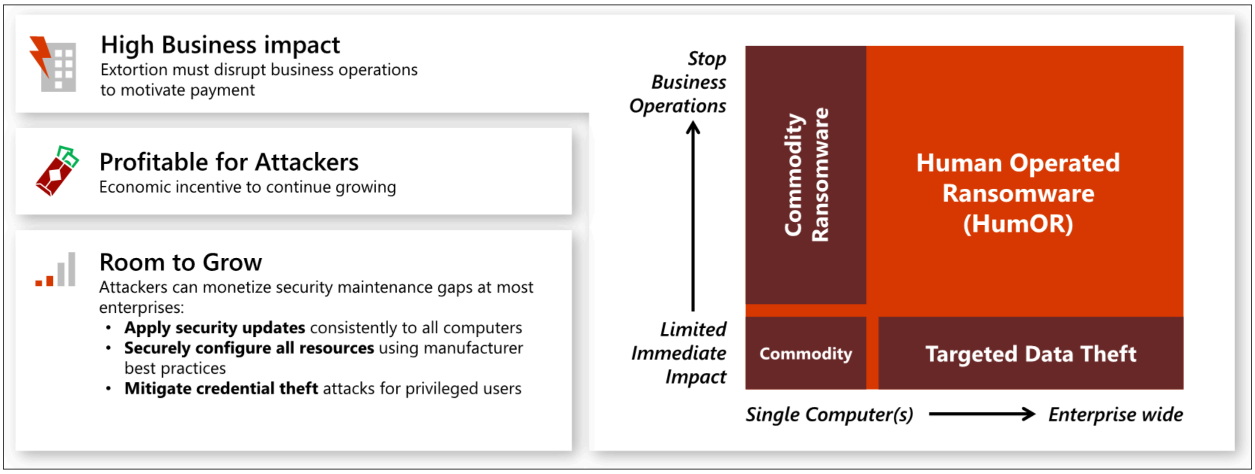
Security of privileged access is critically important because it's foundational to all other security assurances, an attacker in control of your privileged accounts can undermine all other security assurances. From a risk perspective, loss of privileged access is a high impact event with a high likelihood of happening that is growing at an alarming rate across industries.

These attack techniques were initially used in targeted data theft attacks that resulted in many high profile breaches at familiar brands (and many unreported incidents). More recently these techniques were adopted by ransomware attackers, fueling an explosive growth of highly profitable human operated ransomware attacks that intentionally disrupt business operations across industry.

> ⓘ **Important**

Human operated ransomware is different from commodity single computer ransomware attacks that target a single workstation or device.

This graphic describes how this extortion based attack is growing in impact and likelihood using privileged access:



**High Business impact**
Extortion must disrupt business operations to motivate payment

**Profitable for Attackers**
Economic incentive to continue growing

**Room to Grow**
Attackers can monetize security maintenance gaps at most enterprises:

- **Apply security updates** consistently to all computers
- **Securely configure all resources** using manufacturer best practices
- **Mitigate credential theft** attacks for privileged users

- High business impact
  - It's difficult to overstate the potential business impact and damage of a loss to privileged access. Attacker's with privileged access effectively have full control of all enterprise assets and resources, giving them the ability to disclose any confidential data, stop all business processes, or subvert business processes and machines to damage property, hurt people, or worse. Massive business impact has been seen across every industry with:
    - **Targeted data theft** - attackers use privileged access to access and steal sensitive intellectual property for their own use it or to sell/transfer to your competitors or foreign governments
    - **Human-operated ransomware (HumOR)** - attackers use privileged access to steal and/or encrypt all data and systems in the enterprise, often stopping all business operations. They then extort the target organization by demanding money to not disclose the data and/or providing the keys to unlock it.
- High likelihood of occurrence
  - The prevalence of privileged access attacks has grown since the advent of modern credential theft attacks starting with pass the hash techniques. These techniques first jumped in popularity with criminals starting with the 2008 release of the attack tool "Pass-the-Hash Toolkit" and have grown into a suite of reliable attack techniques (mostly based on the Mimikatz toolkit). This weaponization and automation of techniques allowed the attacks (and their subsequent impact) to grow at a rapid rate, limited only by the target organization's vulnerability to the attacks and the attacker's monetization/incentive models.

- Prior to the advent of human-operated ransomware (HumOR), these attacks were prevalent but often unseen or misunderstood because of:
  - **Attacker monetization limits** - Only groups and individuals who knew how to monetize sensitive intellectual property from target organizations could profit from these attacks.
  - **Silent impact** - Organizations often missed these attacks because they didn't have detection tools, and also had a hard time seeing and estimating the resulting business impact (for example, how their competitors were using their stolen intellectual property and how that affected prices and markets, sometimes years later). Additionally, organizations who saw the attacks often stayed silent about them to protect their reputations.
- Both the silent impact and attacker monetization limitations on these attacks are disintegrating with the advent of human operated ransomware, which is growing in volume, impact, and awareness because it's both:
  - **Loud and disruptive** - to business processes to payment of extortion demands.
  - **Universally applicable** - Every organization in every industry is financially motivated to continue operations uninterrupted.

For these reasons, privileged access should be the top security priority at every organization.

# Building your privileged access strategy

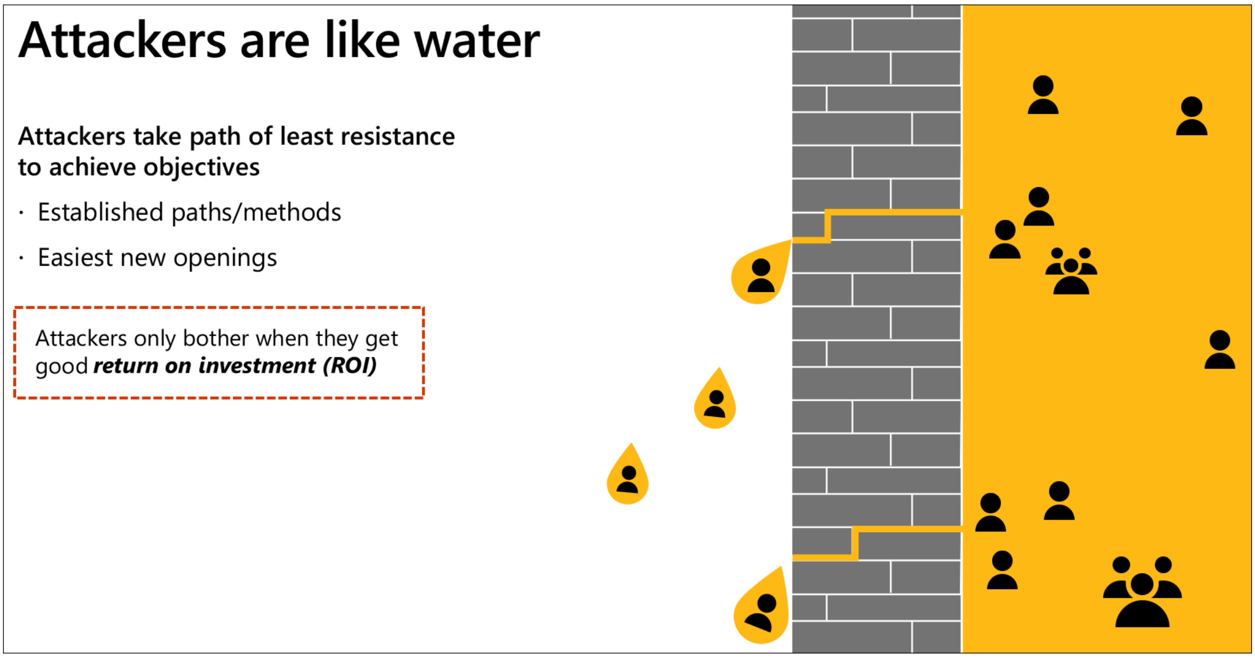
Privileged access strategy is a journey that must be composed of quick wins and incremental progress. Each step in your privileged access strategy must take you closer to "seal" out persistent and flexible attackers from privileged access, who are like water trying to seep into your environment through any available weakness.

This guidance is designed for all enterprise organizations regardless of where you already are in the journey.

## Holistic practical strategy

Reducing risk from privileged access requires a thoughtful, holistic, and prioritized combination of risk mitigations spanning multiple technologies.

Building this strategy requires recognition that attackers are like water as they have numerous options they can exploit (some of which can appear insignificant at first), attackers are flexible in which ones they use, and they generally take the path of least resistance to achieve their objectives.


Attackers are like water
Attackers take path of least resistance to achieve objectives
· Established paths/methods
· Easiest new openings
Attackers only bother when they get good ***return on investment (ROI)***

The paths attackers prioritize in actual practice are a combination of:

- Established techniques (often automated into attack tools)
- New techniques that are easier to exploit

Because of the diversity of technology involved, this strategy requires a complete strategy that combines multiple technologies and follows Zero Trust principles.

> ⓘ Important
>
> You must adopt a strategy that includes multiple technologies to defend against these attacks. Simply implementing a privileged identity management / privileged access management (PIM/PAM) solution is not sufficient. For more information, see, Privileged access Intermediaries.

- The attackers are goal-oriented and technology agnostic, using any type of attack that works.
- The access control backbone you're defending is integrated into most or all systems in the enterprise environment.

Expecting you can detect or prevent these threats with just network controls or a single privileged access solution will leave you vulnerable to many other types of attacks.

## Strategic assumption - Cloud is a source of security

This strategy uses cloud services as the primary source of security and management capabilities rather than on-premises isolation techniques for several reasons:

- **Cloud has better capabilities** - The most powerful security and management capabilities available today come from cloud services, including sophisticated tooling, native integration, and massive amounts of security intelligence like the 8+ trillion security signals a day Microsoft uses for our security tools.
- **Cloud is easier and faster** - Adopting cloud services requires little to no infrastructure for implementing and scaling up, enabling your teams to focus on their security mission rather than technology integration.
- **Cloud requires less maintenance** - The cloud is also managed, maintained, and secured consistently by vendor organizations with teams dedicated to that single purpose for thousands of customer organizations, reducing the time and effort for your team to rigorously maintain capabilities.
- **Cloud keeps improving** - Features and functionality in cloud services are constantly being updated without a need for your organization to invest ongoing.

## Building the recommended strategy

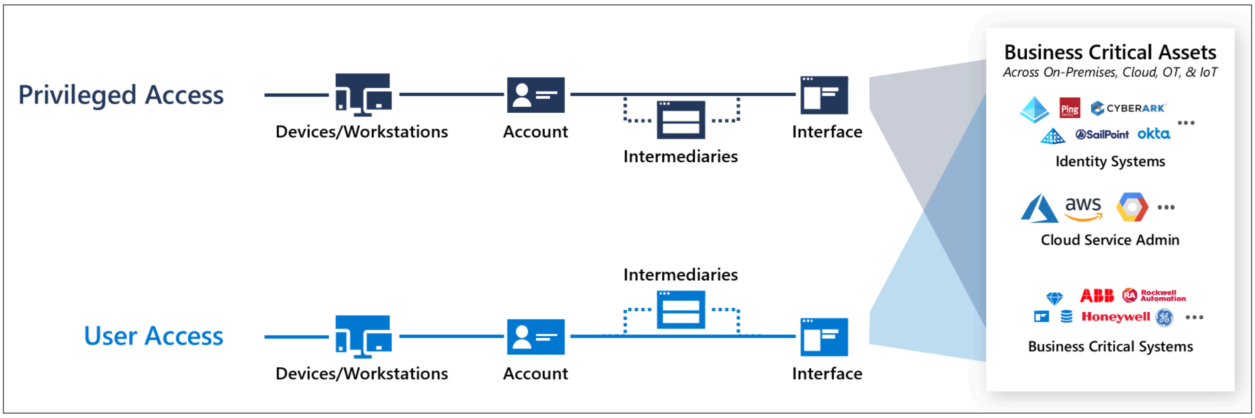
Microsoft's recommended strategy is to incrementally build a 'closed loop' system for privileged access that ensures only trustworthy 'clean' devices, accounts, and intermediary systems can be used for privileged access to business sensitive systems.

Much like waterproofing something complex in real life, like a boat, you need to design this strategy with an intentional outcome, establish and follow standards carefully, and continually monitor and audit the outcomes so that you remediate any leaks. You wouldn't just nail boards together in a boat shape and magically expect a waterproof boat. You would focus first on building and waterproofing significant items like the hull and critical components like the engine and steering mechanism (while leaving ways for people to get in), then later waterproofing comfort items like radios, seats, and the like. You would also maintain it over time as even the most perfect system could spring a leak later, so you need to keep up with preventive maintenance, monitor for leaks, and fix them to keep it from sinking.

Securing Privileged Access has two simple goals

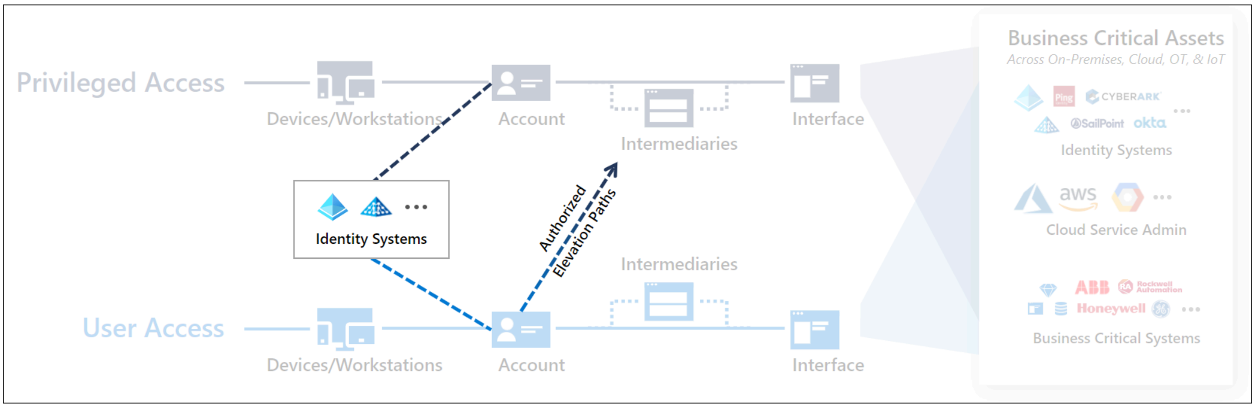
1. Strictly limit the ability to perform privileged actions to a few authorized pathways
2. Protect and closely monitor those pathways

There are two types of pathways to accessing the systems, user access (to use the capability) and privileged access (to manage the capability or access a sensitive capability)



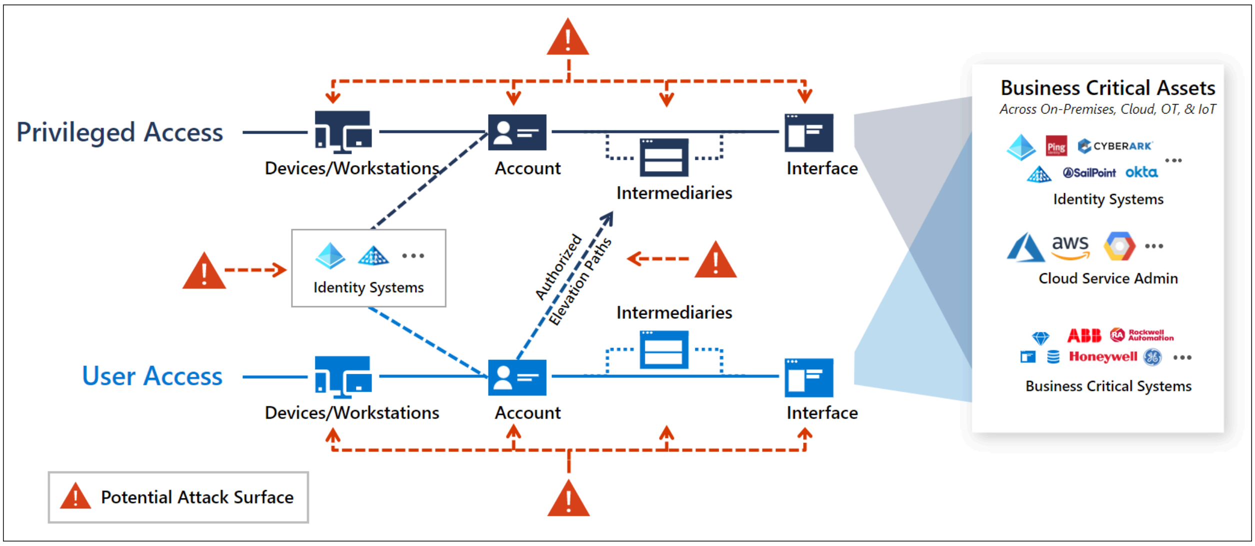
- User Access - the lighter blue path on the bottom of the diagram depicts a standard user account performing general productivity tasks like email, collaboration, web browsing, and use of line-of-business applications or websites. This path includes an account logging on to a device or workstation, sometimes passing through an intermediary like a remote access solution, and interacting with enterprise systems.
- Privileged Access - the darker blue path on the top of the diagram depicts privileged access, where privileged accounts like IT Administrators or other sensitive accounts access business-critical systems and data or perform administrative tasks on enterprise systems. While the technical components may be similar in nature, the damage an adversary can inflict with privileged access is much higher.

The full access management system also includes identity systems and authorized elevation paths.



- Identity Systems - provide identity directories that host the accounts and administrative groups, synchronization and federation capabilities, and other identity support functions for standard and privileged users.
- Authorized Elevation Paths - provide means for standard users to interact with privileged workflows, such as managers or peers approving requests for administrative rights to a sensitive system through a just-in-time (JIT) process in a Privileged Access Management / Privileged Identity management system.

These components collectively comprise the privileged access attack surface that an adversary may target to attempt to gain elevated access to your enterprise:



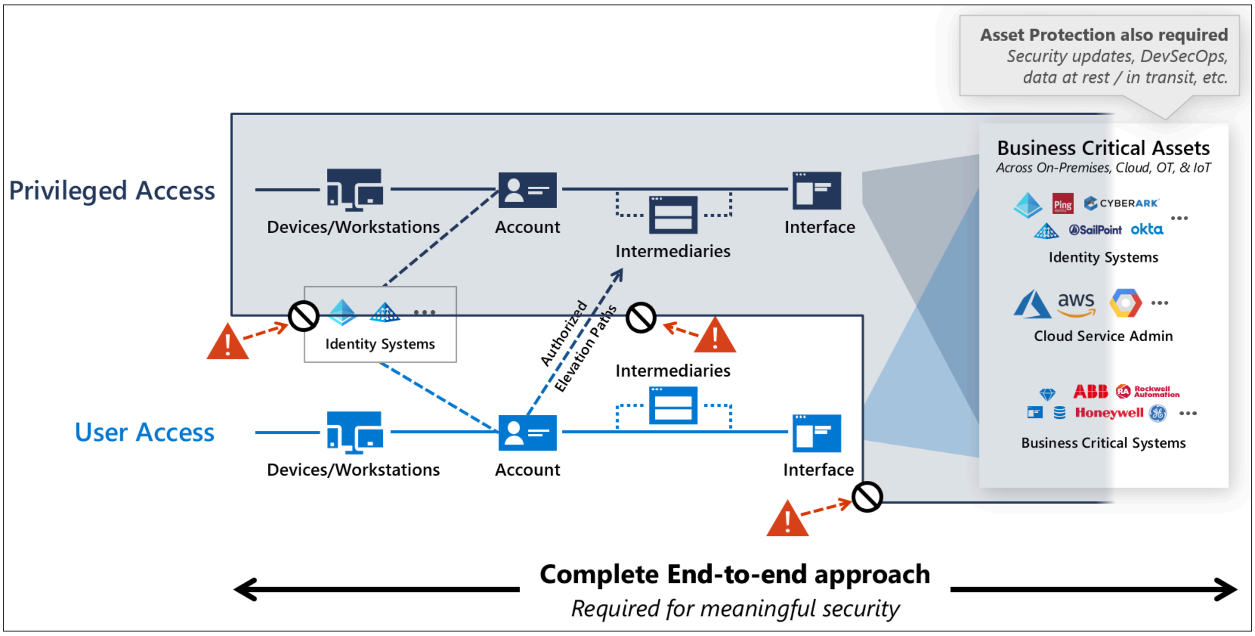
ⓘ Note

For on-premises and infrastructure as a service (IaaS) systems hosted on a customer-managed operating system, the attack surface dramatically increases with management and security agents, service accounts, and potential configuration issues.

Creating a sustainable and manageable privileged access strategy requires closing off all unauthorized vectors to create the virtual equivalent of a control console physically attached to a secure system that represents the only way to access it.

This strategy requires a combination of:

- **Zero Trust access control** described throughout this guidance, including the rapid modernization plan (RAMP)
- **Asset protection** to protect against direct asset attacks by applying good security hygiene practices to these systems. Asset protection for resources (beyond access control components) is out of scope of this guidance, but typically includes rapid application of security updates/patches, configuring operating systems using manufacturer/industry security baselines, protecting data at rest and in transit, and integrating security best practices to development / DevOps processes.


Asset Protection also required
Security updates, DevSecOps, data at rest / in transit, etc.
Privileged Access
Devices/Workstations
Account
Intermediaries
Interface
Identity Systems
Authorized Elevation Paths
Intermediaries
User Access
Devices/Workstations
Account
Interface
Business Critical Assets
Across On-Premises, Cloud, OT, & IoT
Identity Systems
Cloud Service Admin
Business Critical Systems
Complete End-to-end approach
Required for meaningful security

## Strategic initiatives in the journey

Implementing this strategy requires four complementary initiatives that each have clear outcomes and success criteria

1. End-to-end Session Security - Establish explicit Zero Trust validation for privileged sessions, user sessions, and authorized elevation paths.
   a. Success Criteria: Each session validates that each user account and device are trusted at a sufficient level before allowing access.
2. Protect & Monitor Identity Systems including Directories, Identity Management, Admin Accounts, Consent grants, and more
   a. Success Criteria: Each of these systems is protected at a level appropriate for the potential business impact of accounts hosted in it.
3. Mitigate Lateral Traversal to protect against lateral traversal with local account passwords, service account passwords, or other secrets
   a. Success Criteria: Compromising a single device won't immediately lead to control of many or all other devices in the environment
4. Rapid Threat Response to limit adversary access and time in the environment
   a. Success Criteria: Incident response processes impede adversaries from reliably conducting a multi-stage attack in the environment that would result in loss of privileged access. (Measured by reducing the mean time to remediate (MTTR) of incidents involving privileged access to near zero and reducing MTTR of all incidents to a few minutes so adversaries don't have time to target privileged access.)

# Next steps

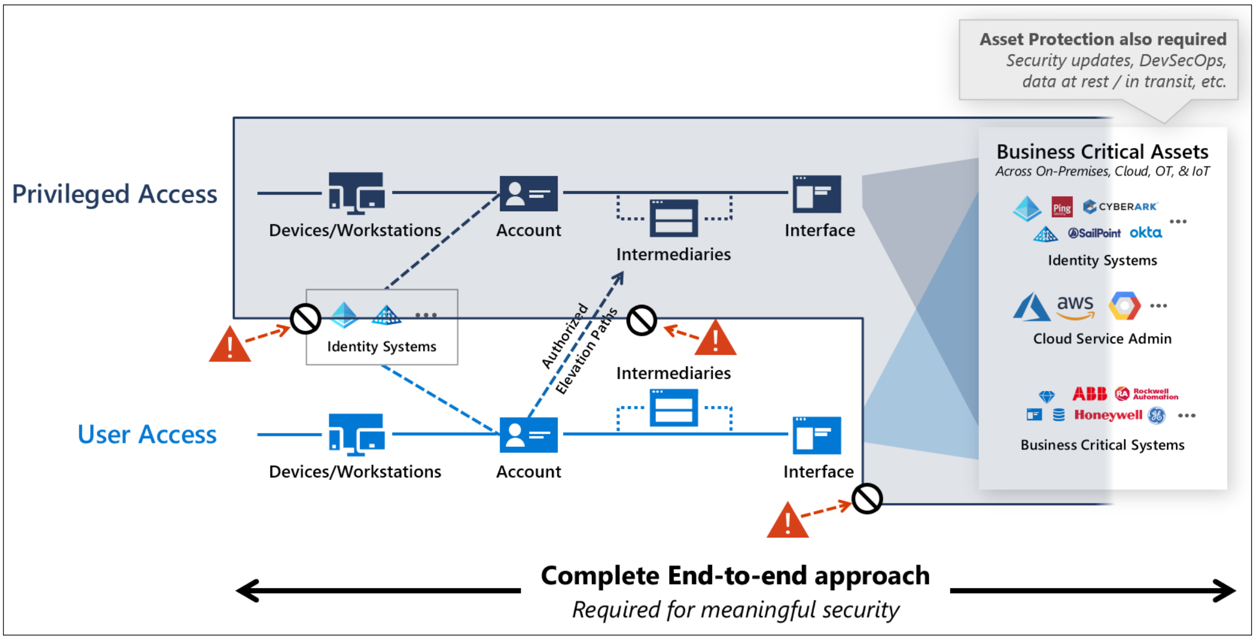
- Securing privileged access overview
- Measuring success
- Security levels
- Privileged access accounts
- Intermediaries
- Interfaces
- Privileged access devices
- Enterprise access model
- Enhanced Security Admin Environment (ESAE) retirement

# Success criteria for privileged access strategy

Article • 01/29/2024

This document describes the success criteria for a privileged access strategy. This section describes strategic perspectives of success for a privileged access strategy. For a roadmap on how to adopt this strategy, see the rapid modernization plan (RaMP). For implementation guidance, see privileged access deployment

Implementing a holistic strategy using Zero Trust approaches creates a "seal" of sorts over the access control for privileged access that makes it resistant to attackers. This strategy is accomplished by limiting pathways to privileged access only a select few, and then closely protecting and monitoring those authorized pathways.



A successful strategy must address the all points attackers can use to intercept privileged access workflows including four distinct initiatives:

- **Privileged Access workflow** elements of the privileged access workflow including underlying devices, operating systems, applications, and identities
- **Identity systems** hosting the privileged accounts and the groups, and other artifacts that confer privilege on the accounts
- **User access workflow** and authorized elevation paths that can lead to privileged access
- **Application interfaces** where zero trust access policy is enforced and role-based access control (RBAC) is configured to grant privileges

ⓘ Note

A complete security strategy also includes asset protections that are beyond the scope of access control, such as data backups and protections against attacks on the application itself, the underlying operating system and hardware, on service accounts used by the application or service, and on data while at rest or in transit. For more information on modernizing a security strategy for cloud, see **Define a security strategy**.

An attack consists of human attackers leveraging automation and scripts to attack an organization is composed of humans, the processes they follow, and the technology they use. Because of this complexity of both attackers and defenders, the strategy must be multi-faceted to guard against all the people, process, and technology ways that the security assurances could inadvertently be undermined.

Ensuring sustainable long-term success requires meeting the following criteria:

- Ruthless prioritization
- Balance security and productivity
- Strong partnerships within the organization
- Disrupt attacker return on investment
- Follow clean source principle

## Ruthless prioritization

Ruthless prioritization is the practice of taking the most effective actions with the fastest time to value first, even if those efforts don't fit pre-existing plans, perceptions, and habits. This strategy lays out the set of steps that have been learned in the fiery crucible of many major cybersecurity incidents. The learnings from these incidents form the steps we help organizations take to ensure that these crises don't happen again.

While it's always tempting for security professionals to try to optimize familiar existing controls like network security and firewalls for newer attacks, this path consistently leads to failure. Microsoft's Detection and Response Team (DART) has been responding to privileged access attacks for nearly a decade and consistently sees these classic security approaches fail to detect or stop these attacks. While network security provides necessary and important basic security hygiene, it's critical to break out of these habits and focus on mitigations that will deter or block real world attacks.

Ruthlessly prioritize the security controls recommended in this strategy, even if it challenges existing assumptions and forces people to learn new skills.

# Balance security and productivity

As with all elements of security strategy, privileged access should ensure that both productivity and security goals are met.

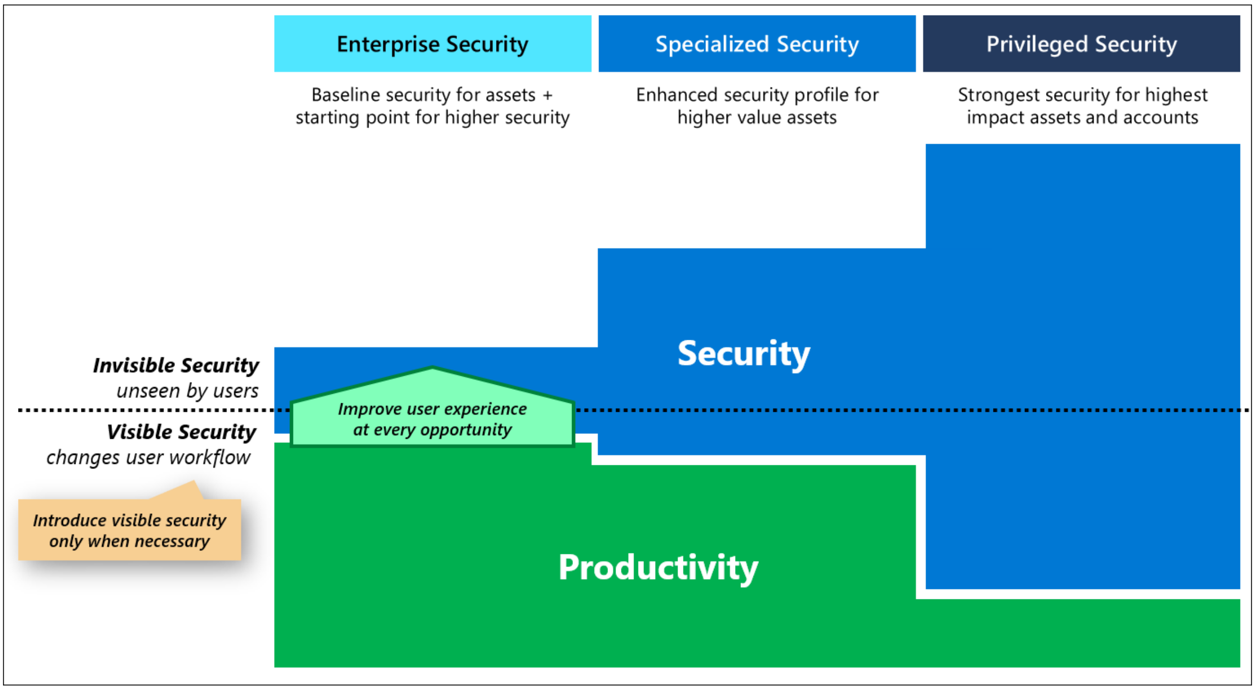
Balancing security avoids the extremes that create risk for the organization by:

- Avoiding overly strict security that causes users to go outside the secure policies, pathways, and systems.
- Avoiding weak security that harms productivity by allowing adversaries to easily compromise the organization.

For more information about security strategy, see Defining a security strategy.

To minimize negative business impact from security controls, you should prioritize invisible security controls that improve user workflows, or at least don't impede or change user workflows. While security sensitive roles may need visible security measures that change their daily workflows to provide security assurances, this implementation should be done thoughtfully to limit the usability impact and scope as much as possible.

This strategy follows this guidance by defining three profiles (detailed later in Keep it Simple - Personas and Profiles)



Enterprise Security
Baseline security for assets + starting point for higher security
Specialized Security
Enhanced security profile for higher value assets
Privileged Security
Strongest security for highest impact assets and accounts
Invisible Security
unseen by users
Visible Security
changes user workflow
Introduce visible security only when necessary
Improve user experience at every opportunity
Security
Productivity

# Strong partnerships within the organization

Security must work to build partnerships within the organization to be successful. In addition to the timeless truth that "none of us is as smart as all of us," the nature of security is to be a support function to protect someone else's resources. Security isn't accountable for the resources they help protect (profitability, uptime, performance, etc.), *security is a support function that provides expert advice and services* to help protect the intellectual property and business functionality that is important to the organization.

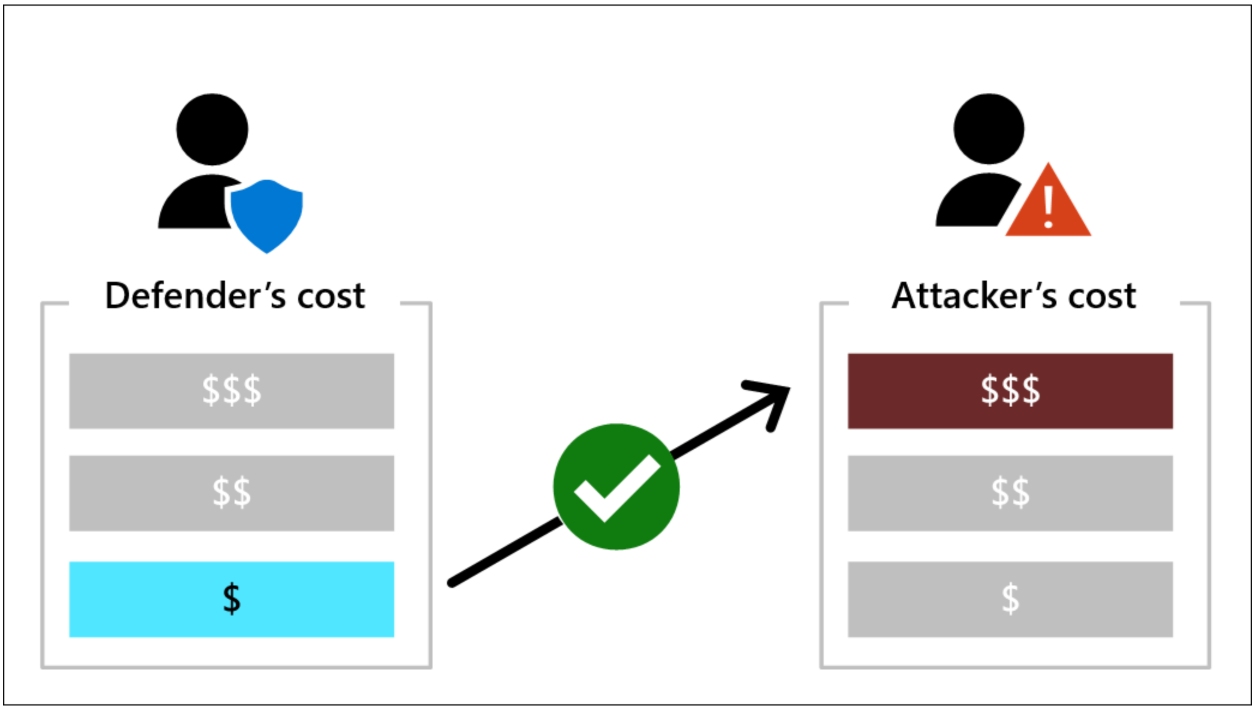
Security should **always work as a partner** in support of business and mission objectives. While security should not shy away from giving direct advice like recommending against accepting a high risk, security should also always frame that advice in terms of the business risk relative to other risks and opportunities managed by the resource owners.

While some parts of security can be planned and executed successfully mostly within security organization, many like securing privileged access require working closely with IT and business organizations to understand which roles to protect, and help update and redesign workflows to ensure they are both secure and allow people to do their jobs. For more information on this idea, see the section Transformations, mindsets, and expectations in the security strategy guidance article.

# Disrupt attacker return on investment

Maintain focus on pragmatism by ensuring that defensive measures are likely to meaningfully disrupt the attacker value proposition of attacking you, increasing cost and friction on the attacker's ability to successfully attack you. Evaluating how defensive measures would impact the adversary's cost of attack provides both a healthy reminder to focus on the attackers perspective as well as a structured mechanism to compare the effectiveness of different mitigation options.

Your goal should be to increase the attackers cost while minimizing your own security investment level:



Disrupt attacker return on investment (ROI) by increasing their cost of attack across the elements of the privileged access session. This concept is described in more detail in the article Success criteria for privileged access strategy.

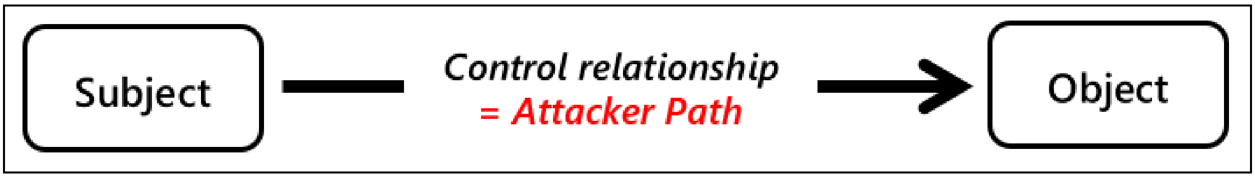
ⓘ **Important**

A privileged access strategy should be comprehensive and provide defense in depth, but must avoid the Expense in depth fallacy where defenders simply pile on more same (familiar) type controls (often network firewalls/filters) past the point where they add any meaningful security value.

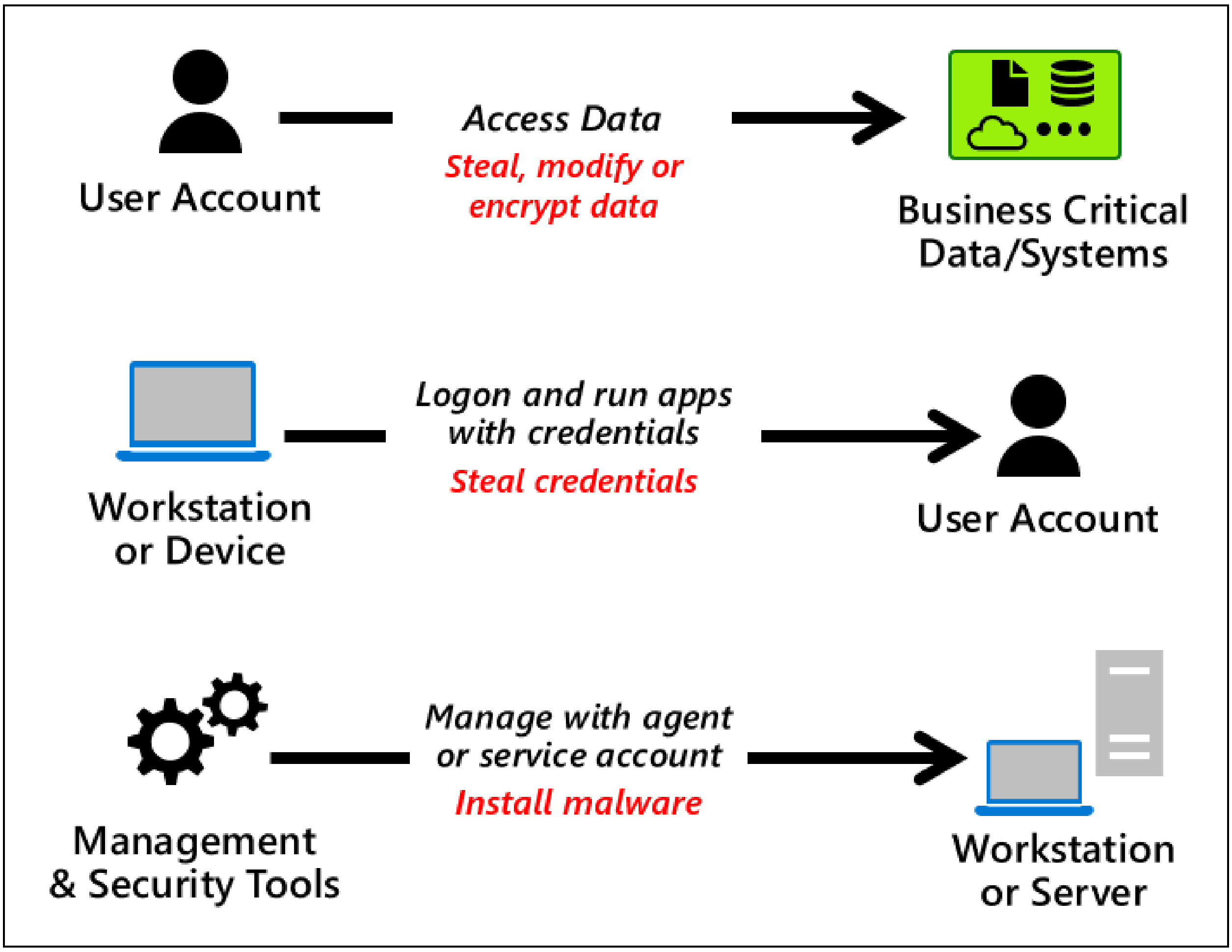
For more information on attacker ROI, see the short video and in-depth discussion Disrupting attacker return on investment.

# Clean source principle

The clean source principle requires all security dependencies to be as trustworthy as the object being secured.



Any subject in control of an object is a security dependency of that object. If an adversary can control anything in control of a target object, they can control that target object. Because of this threat, you must ensure that the assurances for all security dependencies are at or above the desired security level of the object itself. This principle applies across many types of control relationships:


User Account
Access Data
Steal, modify or encrypt data
Business Critical Data/Systems
Workstation or Device
Logon and run apps with credentials
Steal credentials
User Account
Management & Security Tools
Manage with agent or service account
Install malware
Workstation or Server

While simple in principle, this concept gets complex easily in the real world as most enterprises grew organically over decades and have many thousands of control relationships recursively that build on each other, loop back on each other, or both. This web of control relationships provides many access paths that an attacker can discover and navigate during an attack, often with automated tools.

Microsoft's recommended privileged access strategy is effectively a plan to untangle the most important parts of this knot first using a Zero Trust approach, by explicitly validating that the source is clean before allowing access to the destination.

In all cases, the trust level of the source must be the same or higher than the destination.

- The only notable exception to this principle is allowing the use of unmanaged personal devices and partner devices for enterprise scenarios. This exception enables enterprise collaboration and flexibility and can be mitigated to an acceptable level for most organizations because of the low relative value of the enterprise assets. For more context on BYOD security, see the blog post How a BYOD policy can reduce security risk in the public sector.
- This same exception cannot be extended to specialized security and privileged security levels however because of the security sensitivity of these assets. Some PIM/PAM vendors may advocate that their solutions can mitigate device risk from

> lower-level devices, but we respectfully disagree with those assertions based on our experience investigating incidents. The asset owners in your organization may choose to accept risk of using enterprise security level devices to access specialized or privileged resources, but Microsoft does not recommend this configuration. For more information, see the intermediary guidance for Privileged Access Management / Privileged Identity management.

The privileged access strategy accomplishes this principle primarily by enforcing Zero Trust policy with Conditional Access on inbound sessions at interfaces and intermediaries. The clean source principle starts with getting a new device from an OEM that is built to your security specifications including operating system version, security baseline configuration, and other requirements such as using Windows Autopilot for deployment.

Optionally, the clean source principle can extend into a highly rigorous review of each component in the supply chain including installation media for operating systems and applications. While this principle would be appropriate for organizations facing highly sophisticated attackers, it should be a lower priority than the other controls in this guidance.

# Next steps

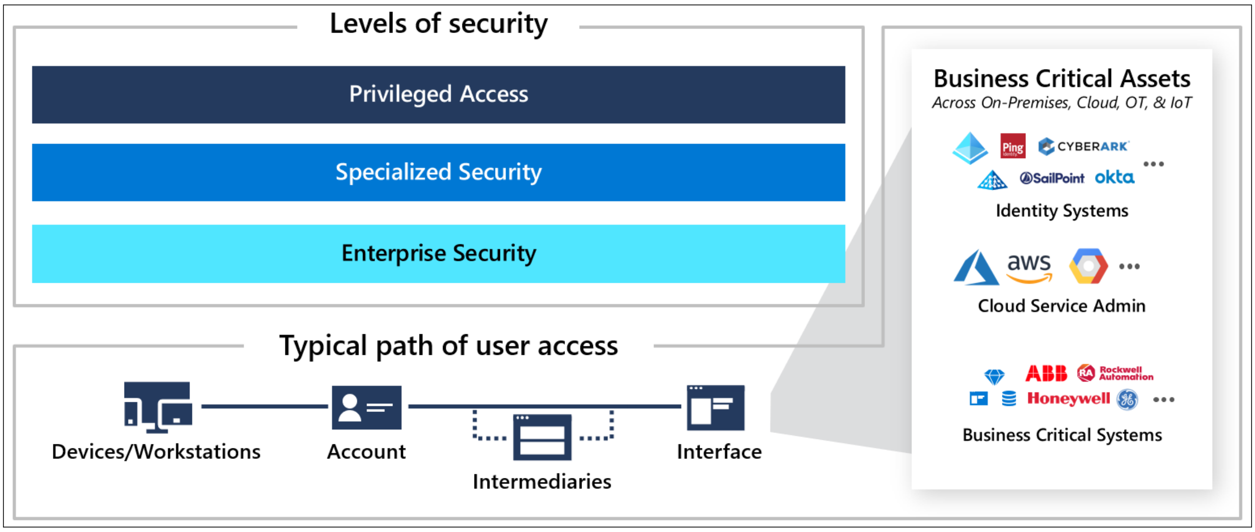
- Securing privileged access overview
- Privileged access strategy
- Security levels
- Privileged access accounts
- Intermediaries
- Interfaces
- Privileged access devices
- Enterprise access model

# Privileged access security levels

Article • 01/29/2024

This document describes the security levels of a privileged access strategy For a roadmap on how to adopt this strategy, see the rapid modernization plan (RaMP). For implementation guidance, see privileged access deployment

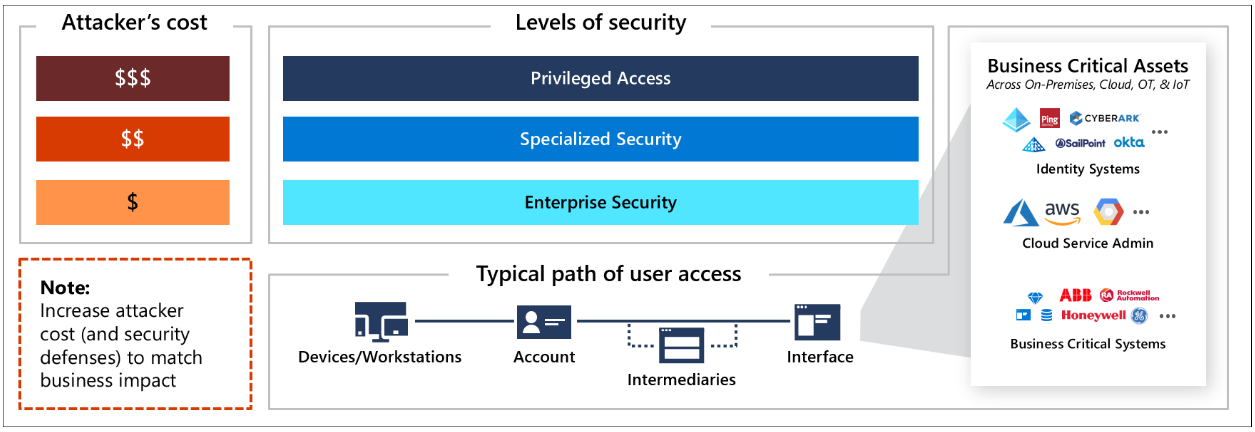
These levels are primarily designed to provide simple and straightforward technical guidance so that organizations can rapidly deploy these critically important protections. The privileged access strategy recognizes that organizations have unique needs, but also that custom solutions create complexity that results in higher costs and lower security over time. To balance this need, the strategy provides firm prescriptive guidance for each level and flexibility through allowing organizations to choose when each role will be required to meet the requirements of that level.



Making things simple helps people understand it and lowers the risk they will be confused and make mistakes. While the underlying technology is almost always complex, it is critical to keep things simple rather than creating custom solutions that are difficult to support. For more information, see Security design principles.

Designing solutions that are focused on the needs of the administrators and end users, will keep it simple for them. Designing solutions that are simple for security and IT personnel to build, assess, and maintain (with automation where possible) leads to less security mistakes and more reliable security assurances.

The recommended privileged access security strategy implements a simple three level system of assurances, that span across areas, designed to be easy to deploy for: accounts, devices, intermediaries, and interfaces.



Each successive level drives up attacker costs, with additional level of Defender for Cloud investment. The levels are designed to target the 'sweet spots' where defenders get the most return (attacker cost increase) for each security investment they make.

Each role in your environment should be mapped to one of these levels (and optionally increased over time as part of a security improvement plan). Each profile is clearly defined as a technical configuration and automated where possible to ease deployment and speed up security protections. For implementation details see the article, Privileged access roadmap.

# Security levels

The security levels used throughout this strategy are:

## Enterprise

- **Enterprise security** is suitable for all enterprise users and productivity scenarios. In the progression of the rapid modernization plan, enterprise also serves as the starting point for specialized and privileged access as they progressively build on the security controls in enterprise security.

> ⓘ Note
>
> Weaker security configurations do exist, but aren't recommended by Microsoft for enterprise organizations today because of the skills and resources attackers have available. For information on what attackers can buy from each other on the dark markets and average prices, see the video **Top 10 Best Practices for Azure Security**

## Specialized

- **Specialized security** provides increased security controls for roles with an elevated business impact (if compromised by an attacker or malicious insider).

  Your organization should have documented criteria for specialized and privileged accounts (for example, potential business impact is over $1M USD) and then identify all the roles and accounts meeting that criteria. (used throughout this strategy, including in the Specialized Accounts)

  Specialized roles typically include:
  - **Developers** of business critical systems.
  - **Sensitive business roles** such as users of SWIFT terminals, researchers with access to sensitive data, personnel with access to financial reporting prior to public release, payroll administrators, approvers for sensitive business processes, and other high impact roles.
  - **Executives** and personal assistants / administrative assistants that that regularly handle sensitive information.
  - **High impact social media accounts** that could damage the company reputation.
  - **Sensitive IT Admins** with a significant privileges and impact, but are not enterprise-wide. This group typically includes administrators of individual high impact workloads. (for example, enterprise resource planning administrators, banking administrators, help desk /tech support roles, etc.)

  Specialized Account security also serves as an interim step for privileged security, which further builds on these controls. See privileged access roadmap for details on recommended order of progression.

# Privileged

- **Privileged security** is the highest level of security designed for roles that could easily cause a major incident and potential material damage to the organization in the hands of an attacker or malicious insider. This level typically includes technical roles with administrative permissions on most or all enterprise systems (and sometimes includes a select few business critical roles)

  Privileged accounts are focused on security first, with productivity defined as the ability to easily and securely perform sensitive job tasks securely. These roles will not have the ability to do both sensitive work and general productivity tasks (browse the web, install and use any app) using the same account or the same device/workstation. They will have highly restricted accounts and workstations with increased monitoring of their actions for anomalous activity that could represent attacker activity.

Privileged access security roles typically include:

- Microsoft Entra Global Administrators and related roles
- Other identity management roles with administrative rights to an enterprise directory, identity synchronization systems, federation solution, virtual directory, privileged identity/access management system, or similar.
- Roles with membership in these on-premises Active Directory groups
  - Enterprise Admins
  - Domain Admins
  - Schema Admin
  - BUILTIN\Administrators
  - Account Operators
  - Backup Operators
  - Print Operators
  - Server Operators
  - Domain Controllers
  - Read-only Domain Controllers
  - Group Policy Creator Owners
  - Cryptographic Operators
  - Distributed COM Users
  - Sensitive on-premises Exchange groups (including Exchange Windows Permissions and Exchange Trusted Subsystem)
  - Other Delegated Groups - Custom groups that may be created by your organization to manage directory operations.
  - Any local administrator for an underlying operating system or cloud service tenant that is hosting the above capabilities including
    - Members of local administrators group
    - Personnel who know the root or built in administrator password
    - Administrators of any management or security tool with agents installed on those systems

## Next steps

- Securing privileged access overview
- Privileged access strategy
- Measuring success
- Privileged access accounts
- Intermediaries
- Interfaces
- Privileged access devices
- Enterprise access model

# Privileged access: Accounts

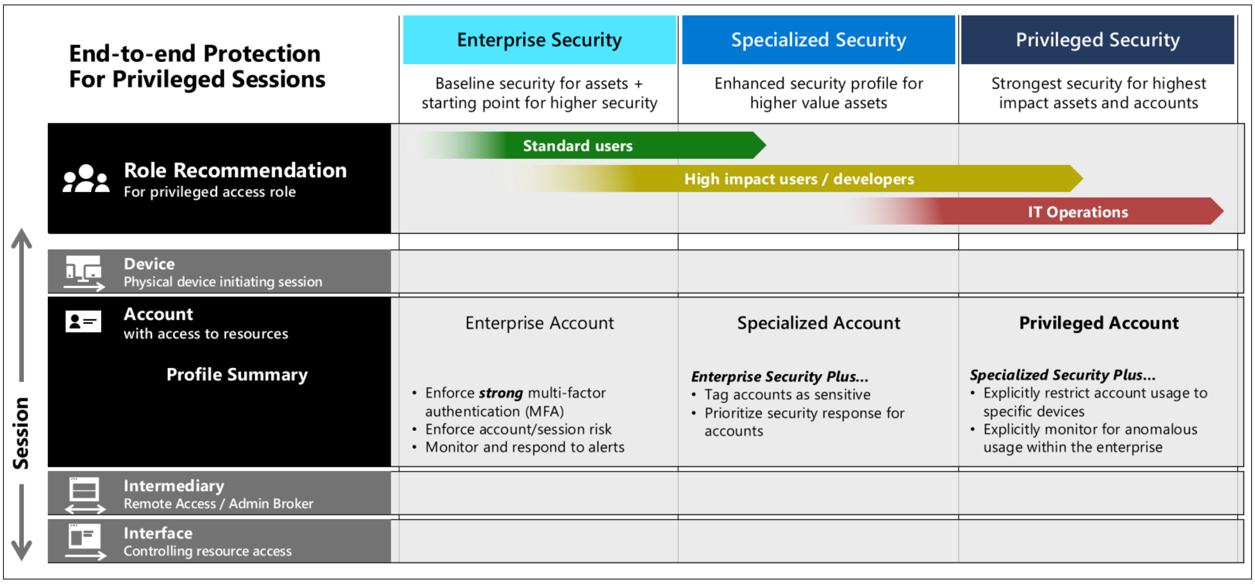
Article • 01/29/2024

Account security is a critical component of securing privileged access. End to end Zero Trust security for sessions requires strongly establishing that the account being used in the session is actually under the control of the human owner and not an attacker impersonating them.

Strong account security starts with secure provisioning and full lifecycle management through to deprovisioning, and each session must establish strong assurances that the account isn't currently compromised based on all available data including historical behavior patterns, available threat intelligence, and usage in the current session.

## Account security

This guidance defines three security levels for account security that you can use for assets with different sensitivity levels:



| End-to-end Protection For Privileged Sessions | Enterprise Security<br>Baseline security for assets + starting point for higher security | Specialized Security<br>Enhanced security profile for higher value assets | Privileged Security<br>Strongest security for highest impact assets and accounts |
|---|---|---|---|
| Role Recommendation<br>For privileged access role | Standard users<br>High impact users / developers | High impact users / developers<br>IT Operations | IT Operations |
| Device<br>Physical device initiating session | | | |
| Account<br>with access to resources<br>Profile Summary | Enterprise Account<br>• Enforce ***strong*** multi-factor authentication (MFA)<br>• Enforce account/session risk<br>• Monitor and respond to alerts | Specialized Account<br>***Enterprise Security Plus...***<br>• Tag accounts as sensitive<br>• Prioritize security response for accounts | **Privileged Account**<br>***Specialized Security Plus...***<br>• Explicitly restrict account usage to specific devices<br>• Explicitly monitor for anomalous usage within the enterprise |
| Intermediary<br>Remote Access / Admin Broker | | | |
| Interface<br>Controlling resource access | | | |

These levels establish clear and implementable security profiles appropriate for each sensitivity level that you can assign roles to and scale out rapidly. All of these account security levels are designed to maintain or improve productivity for people by limiting or eliminating interruption to user and admin workflows.

## Planning account security

This guidance outlines the technical controls required to meet each level. Implementation guidance is in the privileged access roadmap.

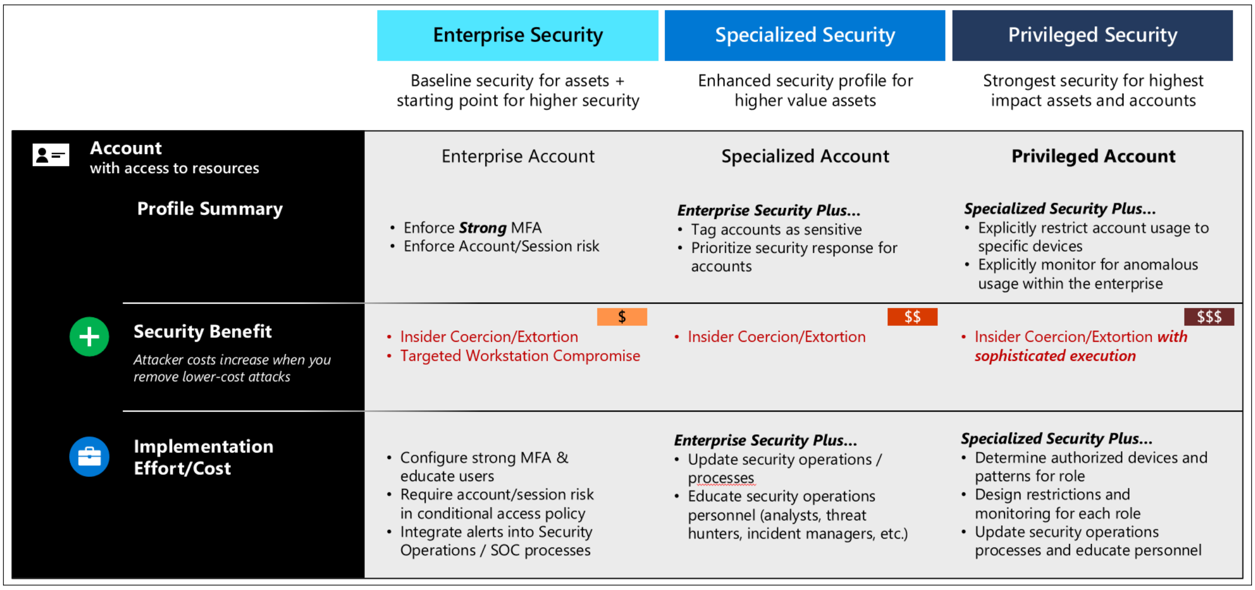
# Account security controls

Achieving security for the interfaces requires a combination of technical controls that both protect the accounts and provide signals to be used in a Zero Trust policy decision (see Securing Interfaces for policy configuration reference).

The controls used in these profiles include:

- Multi-factor authentication - providing diverse sources of proof that the (designed to be as easy as possible for users, but difficult for an adversary to mimic).
- Account risk - Threat and Anomaly Monitoring - using UEBA and Threat intelligence to identify risky scenarios
- Custom monitoring - For more sensitive accounts, explicitly defining allowed/accepted behaviors/patterns allows early detection of anomalous activity. This control is not suitable for general purpose accounts in enterprise as these accounts need flexibility for their roles.

The combination of controls also enables you to improve both security and usability - for example a user who stays within their normal pattern (using the same device in same location day after day) does not need to be prompted for outside MFA every time they authenticate.



| | Enterprise Security | Specialized Security | Privileged Security |
|---|---|---|---|
| | Baseline security for assets + starting point for higher security | Enhanced security profile for higher value assets | Strongest security for highest impact assets and accounts |
| **Account** with access to resources<br>**Profile Summary** | Enterprise Account<br>• Enforce ***Strong*** MFA<br>• Enforce Account/Session risk | **Specialized Account**<br>***Enterprise Security Plus…***<br>• Tag accounts as sensitive<br>• Prioritize security response for accounts | **Privileged Account**<br>***Specialized Security Plus…***<br>• Explicitly restrict account usage to specific devices<br>• Explicitly monitor for anomalous usage within the enterprise |
| **Security Benefit**<br>*Attacker costs increase when you remove lower-cost attacks* | $<br>• Insider Coercion/Extortion<br>• Targeted Workstation Compromise | $$<br>• Insider Coercion/Extortion | $$$<br>• Insider Coercion/Extortion ***with sophisticated execution*** |
| **Implementation Effort/Cost** | • Configure strong MFA & educate users<br>• Require account/session risk in conditional access policy<br>• Integrate alerts into Security Operations / SOC processes | ***Enterprise Security Plus…***<br>• Update security operations / processes<br>• Educate security operations personnel (analysts, threat hunters, incident managers, etc.) | ***Specialized Security Plus…***<br>• Determine authorized devices and patterns for role<br>• Design restrictions and monitoring for each role<br>• Update security operations processes and educate personnel |

# Enterprise security accounts

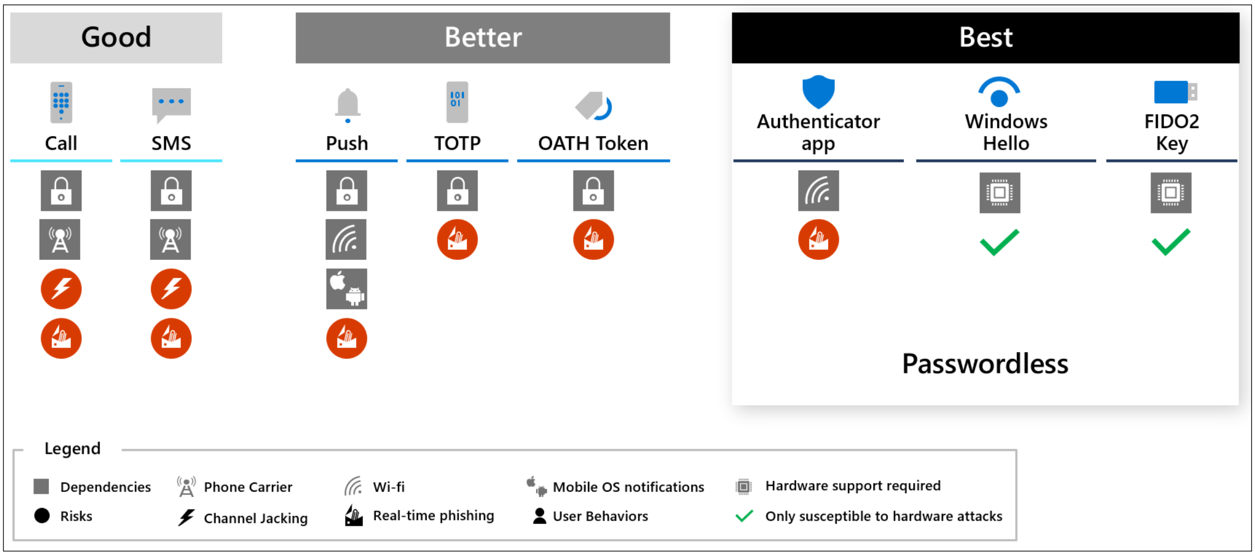
The security controls for enterprise accounts are designed to create a secure baseline for all users and provide a secure foundation for specialized and privileged security:

- Enforce strong multi-factor authentication (MFA) - Ensure that the user is authenticated with strong MFA provided by an enterprise-managed identity system (detailed in the diagram below). For more information about multi-factor authentication, see Azure security best practice 6.

> ⓘ Note
>
> While your organization may choose to use an existing weaker form of MFA during a transition period, attackers are increasingly evading the weaker MFA protections, so all new investment into MFA should be on the strongest forms.

- Enforce account/session risk - ensure that the account is not able to authenticate unless it is at a low (or medium?) risk level. See Interface Security Levels for details on conditional enterprise account security.
- Monitor and respond to alerts - Security operations should integrate account security alerts and get sufficient training on how these protocols and systems work to ensure they are able to rapidly comprehend what an alert means and react accordingly.
  - Enable Microsoft Entra ID Protection
  - Investigate risk Microsoft Entra ID Protection
  - Troubleshoot/Investigate Conditional Access Sign-in failures

The following diagram provides a comparison to different forms of MFA and passwordless authentication. Each option in the best box is considered both high security and high usability. Each has different hardware requirements so you may want to mix and match which ones apply to different roles or individuals. All Microsoft passwordless solutions are recognized by Conditional Access as multi-factor authentication because they require combining something you have with either biometrics, something you know, or both.



> ⓘ Note
>
> For more information on why SMS and other phone based authentication is limited, see the blog post **It's Time to Hang Up on Phone Transports for Authentication** .

## Specialized accounts

Specialized accounts are a higher protection level suitable for sensitive users. Because of their higher business impact, specialized accounts warrant additional monitoring and prioritization during security alerts, incident investigations, and threat hunting.

Specialized security builds on the strong MFA in enterprise security by identifying the most sensitive accounts and ensuring alerts and response processes are prioritized:

1. Identify Sensitive Accounts - See specialized security level guidance for identifying these accounts.
2. Tag Specialized Accounts - Ensure each sensitive account is tagged
   a. Configure Microsoft Sentinel Watchlists to identify these sensitive accounts
   b. Configure Priority account protection in Microsoft Defender for Office 365 and designate specialized and privileged accounts as priority accounts -
3. Update Security Operations processes - to ensure these alerts are given the highest priority
4. Set up Governance - Update or create governance process to ensure that
   a. All new roles to are evaluated for specialized or privileged classifications as they are created or changed
   b. All new accounts are tagged as they are created
   c. Continuous or periodic out of band checks to ensure that roles and accounts didn't get missed by normal governance processes.

## Privileged accounts

Privileged accounts have the highest level of protection because they represent a significant or material potential impact on the organization's operations if compromised.

Privileged accounts always include IT Admins with access to most or all enterprise systems, including most or all business critical systems. Other accounts with a high business impact may also warrant this additional level of protection. For more information about which roles and accounts should be protected at what level, see the article Privileged Security.

In addition to specialized security , privileged account security increases both:

- Prevention - add controls to restrict the usage of these accounts to the designated devices, workstations, and intermediaries.
- Response - closely monitor these accounts for anomalous activity and rapidly investigate and remediate the risk.

## Configuring privileged account security

Follow the guidance in the Security rapid modernization plan to both increase the security of your privileged accounts and decrease your cost to manage.

## Next steps

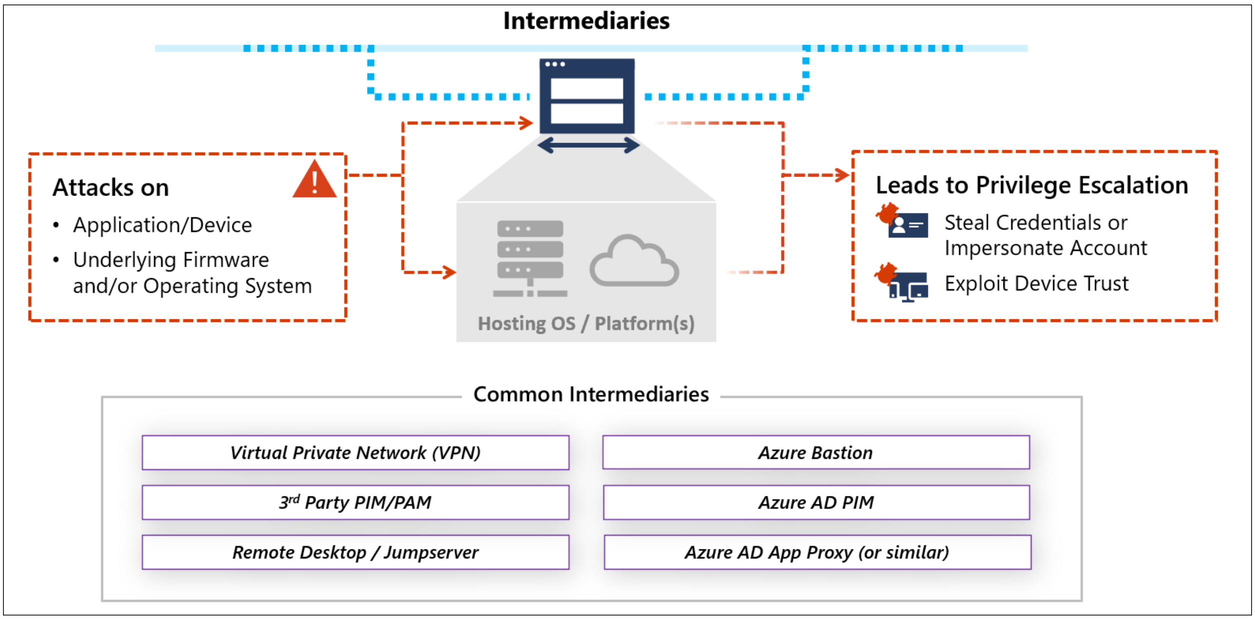
- Securing privileged access overview
- Privileged access strategy
- Measuring success
- Security levels
- Intermediaries
- Interfaces
- Privileged access devices
- Enterprise access model

# Privileged access: Intermediaries

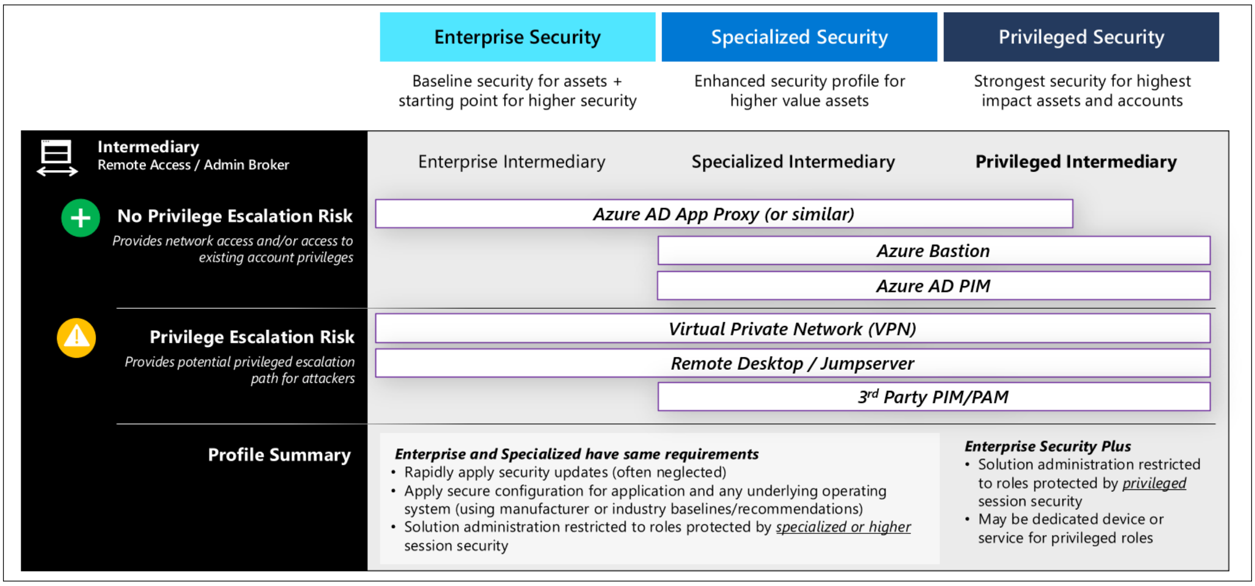
Article • 01/29/2024

Security of intermediary devices is a critical component of securing privileged access.

Intermediaries add link to the chain of Zero Trust assurance for the user or administrator's end to end session, so they must sustain (or improve) the Zero Trust security assurances in the session. Examples of intermediaries include virtual private networks (VPNs), jump servers, virtual desktop infrastructure (VDI), as well as application publishing through access proxies.


Intermediaries
Attacks on
• Application/Device
• Underlying Firmware and/or Operating System
Hosting OS / Platform(s)
Leads to Privilege Escalation
Steal Credentials or Impersonate Account
Exploit Device Trust
Common Intermediaries
Virtual Private Network (VPN)
Azure Bastion
3rd Party PIM/PAM
Azure AD PIM
Remote Desktop / Jumpserver
Azure AD App Proxy (or similar)

An attacker can attack an intermediary to attempt to escalating privileges using credentials stored on them, get network remote access to corporate networks, or exploit trust in that device if being used for Zero Trust access decisions. Targeting intermediaries has become an all too common, especially for organizations that don't rigorously maintain the security posture of these devices. For example, credentials collected from VPN devices .



Enterprise Security

Baseline security for assets + starting point for higher security

Specialized Security

Enhanced security profile for higher value assets

Privileged Security

Strongest security for highest impact assets and accounts

**Intermediary**
Remote Access / Admin Broker

Enterprise Intermediary

Specialized Intermediary

**Privileged Intermediary**

**No Privilege Escalation Risk**

*Provides network access and/or access to existing account privileges*

*Azure AD App Proxy (or similar)*

*Azure Bastion*

*Azure AD PIM*

**Privilege Escalation Risk**

*Provides potential privileged escalation path for attackers*

*Virtual Private Network (VPN)*

*Remote Desktop / Jumpserver*

*3rd Party PIM/PAM*

**Profile Summary**

***Enterprise and Specialized have same requirements***

- Rapidly apply security updates (often neglected)
- Apply secure configuration for application and any underlying operating system (using manufacturer or industry baselines/recommendations)
- Solution administration restricted to roles protected by *specialized or higher* session security

***Enterprise Security Plus***

- Solution administration restricted to roles protected by *privileged* session security
- May be dedicated device or service for privileged roles

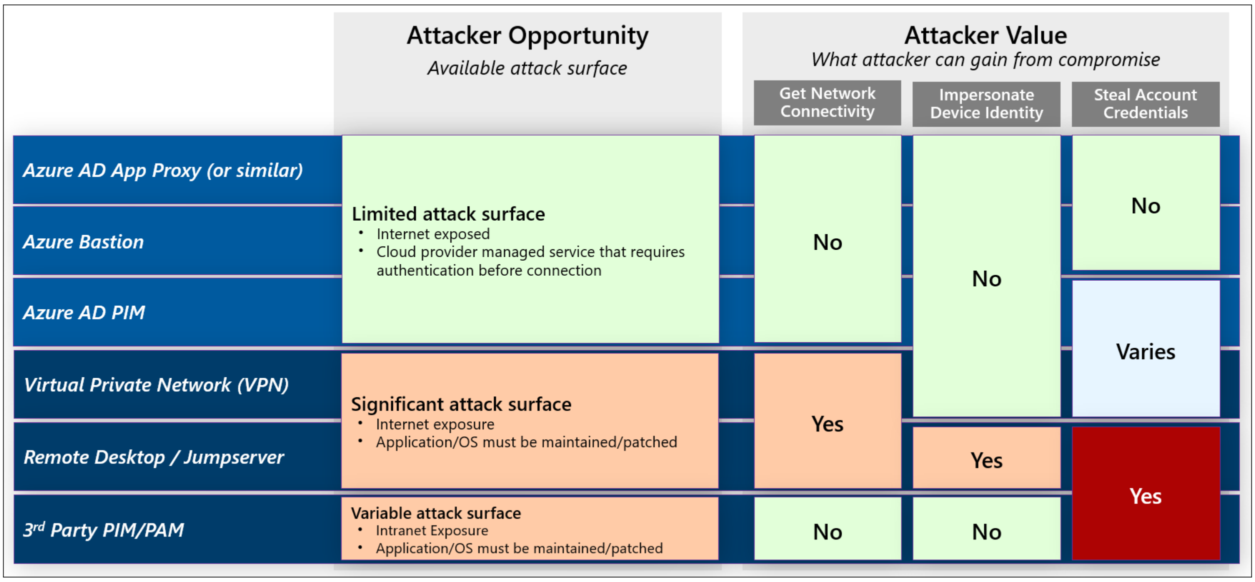
Intermediaries vary in purpose and technology, but typically provide remote access, session security, or both:

- **Remote access** - Enable access to systems on enterprise networks from the internet
- **Session security** - Increase security protections and visibility for a session
  - **Unmanaged device scenario** - Providing a managed virtual desktop to be accessed by unmanaged devices (for example, personal employee devices) and/or devices managed by a partner/vendor.
  - **Administrator security scenario** - Consolidate administrative pathways and/or increase security with just in time access, session monitoring and recording, and similar capabilities.

Ensuring security assurances are sustained from the originating device and account through to the resource interface requires understanding the risk profile of the intermediary and mitigation options.

# Attacker opportunity and value

Different intermediary types perform unique functions so they each require a different security approach, though there are some critical commonalities like rapidly applying security patches to appliances, firmware, operating systems, and applications.



| | Attacker Opportunity<br>*Available attack surface* | Attacker Value<br>*What attacker can gain from compromise* | | |
|---|---|---|---|---|
| | | Get Network Connectivity | Impersonate Device Identity | Steal Account Credentials |
| *Azure AD App Proxy (or similar)* | Limited attack surface<br>• Internet exposed<br>• Cloud provider managed service that requires authentication before connection | No | No | No |
| *Azure Bastion* | | | | |
| *Azure AD PIM* | | | | Varies |
| *Virtual Private Network (VPN)* | Significant attack surface<br>• Internet exposure<br>• Application/OS must be maintained/patched | Yes | | |
| *Remote Desktop / Jumpserver* | | | Yes | Yes |
| *3rd Party PIM/PAM* | Variable attack surface<br>• Intranet Exposure<br>• Application/OS must be maintained/patched | No | No | |

The **attacker opportunity** is represented by the available attack surface an attack operator can target:

- **Native cloud services** like Microsoft Entra PIM, Azure Bastion, and Microsoft Entra application proxy offer a limited attack surface to attackers. While they are exposed to the public internet, customers (and attackers) have no access to underlying operating systems providing the services and they are typically maintained and monitored consistently via automated mechanisms at the cloud provider. This smaller attack surface limits the available options to attackers vs. classic on-premises applications and appliances that must be configured, patched, and monitored by IT personnel who are often overwhelmed by conflicting priorities and more security tasks than they have time to complete.
- **Virtual Private Networks (VPNs)** and **Remote Desktops** / **Jump servers** frequently have a significant attacker opportunity as they are exposed to the internet to provide remote access and the maintenance of these systems is frequently neglected. While they only have a few network ports exposed, attackers only need access to one unpatched service for an attack.
- **Third-party PIM/PAM** services are frequently hosted on-premises or as a VM on Infrastructure as a Service (IaaS) and are typically only available to intranet hosts. While not directly internet exposed, a single compromised credential may allow attackers to access the service over VPN or another remote access medium.

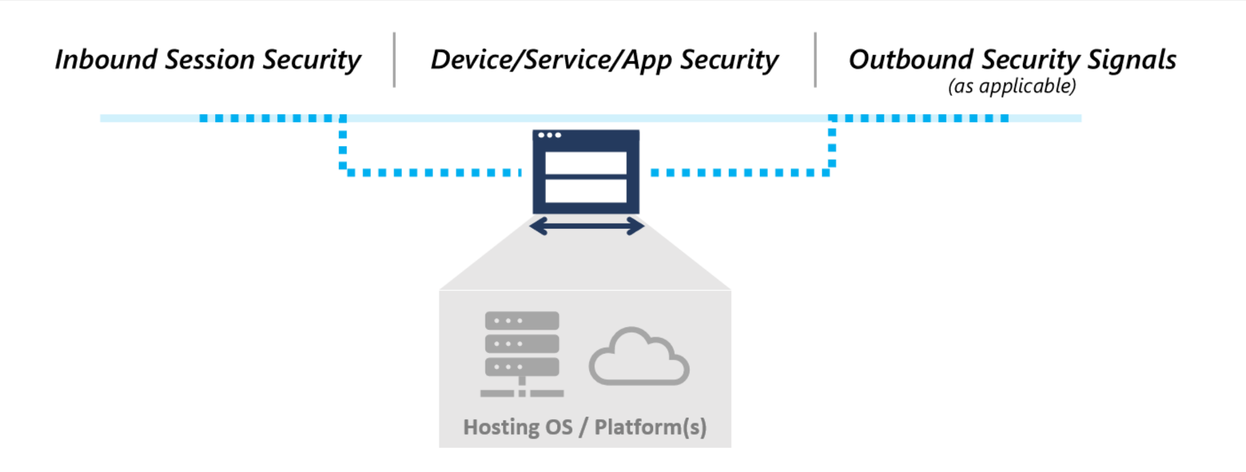
**Attacker value** represents what an attacker can gain by compromising an intermediary. A compromise is defined as an attacker gaining full control over the application/VM and/or an administrator of the customer instance of the cloud service.

The ingredients that attackers can collect from an intermediary for the next stage of their attack include:

- **Get network connectivity** to communicate with most or all resource on enterprise networks. This access is typically provided by VPNs and Remote Desktop / Jump server solutions. While Azure Bastion and Microsoft Entra application proxy (or similar third-party solutions) solutions also provide remote access, these solutions are typically application or server-specific connections and don’t provide general network access
- **Impersonate device identity** - can defeat Zero Trust mechanisms if a device is required for authentication and/or be used by an attacker to gather intelligence on the targets networks. Security Operations teams often don't closely monitor device account activity and focus only on user accounts.
- **Steal account credentials** to authenticate to resources, which are the most valuable asset to attackers as it offers the ability to elevate privileges to access their ultimate goal or the next stage in the attack. Remote Desktop / Jump servers and third-party PIM/PAM are the most attractive targets and have the “All your eggs in one basket” dynamic with increased attacker value and security mitigations:
  - **PIM/PAM** solutions typically store the credentials for most or all privileged roles in the organization, making them a highly lucrative target to compromise or to weaponize.
  - **Microsoft Entra PIM** doesn't offer attackers the ability to steal credentials because it unlocks privileges already assigned to an account using MFA or other workflows, but a poorly designed workflow could allow an adversary to escalate privileges.
  - **Remote Desktop / Jump servers** used by administrators provide a host where many or all sensitive sessions pass through, enabling attackers to use standard credential theft attack tools to steal and reuse these credentials.
  - **VPNs** can store credentials in the solution, providing attackers with a potential treasure trove of privilege escalation, leading to the strong recommendation to use Microsoft Entra ID for authentication to mitigate this risk.

## Intermediary security profiles

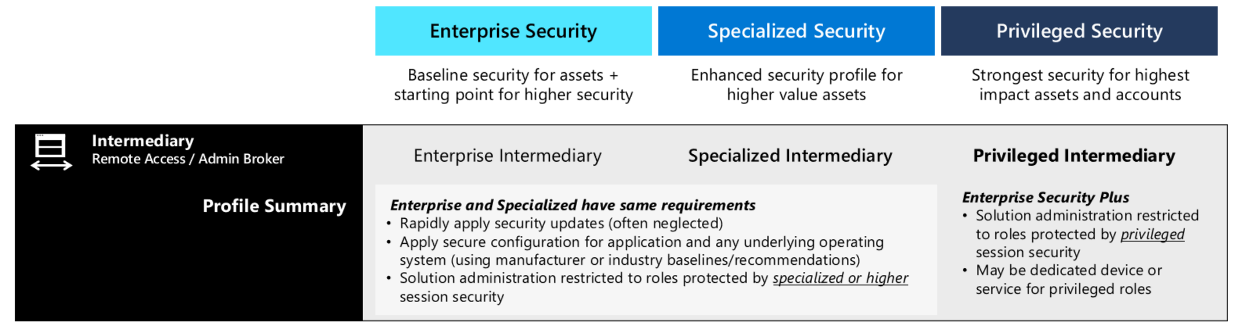
Establishing these assurances requires a combination of security controls, some of which are common to many intermediaries, and some of which specific to the type of intermediary.



An intermediary is a link in the Zero Trust chain that presents an interface to users/devices and then enables access to the next interface. The security controls must address inbound connections, security of the intermediary device/application/service itself, and (if applicable) provide Zero Trust security signals for the next interface.

## Common security controls

The common security elements for intermediaries are focused on maintaining good security hygiene for enterprise and specialized levels, with additional restrictions for privilege security.



| | Enterprise Security | Specialized Security | Privileged Security |
|---|---|---|---|
| | Baseline security for assets + starting point for higher security | Enhanced security profile for higher value assets | Strongest security for highest impact assets and accounts |
| **Intermediary**<br>Remote Access / Admin Broker | Enterprise Intermediary | **Specialized Intermediary** | **Privileged Intermediary** |
| **Profile Summary** | ***Enterprise and Specialized have same requirements***<br>• Rapidly apply security updates (often neglected)<br>• Apply secure configuration for application and any underlying operating system (using manufacturer or industry baselines/recommendations)<br>• Solution administration restricted to roles protected by *specialized or higher* session security | | ***Enterprise Security Plus***<br>• Solution administration restricted to roles protected by *privileged* session security<br>• May be dedicated device or service for privileged roles |

These security controls should be applied to all types of intermediaries:

- **Enforce inbound connection security** - Use Microsoft Entra ID and Conditional Access to ensure all inbound connections from devices and accounts are known, trusted, and allowed. For more information, see the article Secuiting privileged interfaces for detailed definitions for device and account requirements for enterprise and specialized.
- **Proper system maintenance** - All intermediaries must follow good security hygiene practices including:
  - **Secure configuration** - Follow manufacturer or industry security configuration baselines and best practices for both the application and any underlying

    operating systems, cloud services, or other dependencies. Applicable guidance from Microsoft includes the Azure Security Baseline and Windows Baselines.
  - **Rapid patching** - Security updates and patches from the vendors must be applied rapidly after release.
- **Role-Based Access Control (RBAC)** models can be abused by attackers to escalate privileges. The RBAC model of the intermediary must be carefully review to ensure that only authorized personnel that are protected at a specialized or privileged level are granted administrative privileges. This model must include any underlying operating systems or cloud services (root account password, local administrator users/groups, tenant administrators, etc.).
- **Endpoint detection and response (EDR) and outbound trust signal** - Devices that include a full operating system should be monitored and protected with an EDR like Microsoft Defender for Endpoint. This control should be configured to provides device compliance signals to Conditional Access so that policy can enforce this requirement for interfaces.

Privileged Intermediaries require additional security controls:

- **Role-Based Access Control (RBAC)** - Administrative rights must be restricted to only privileged roles meeting that standard for workstations and accounts.
- **Dedicated devices (optional)** - because of the extreme sensitivity of privileged sessions, organizations may choose to implement dedicated instances of intermediary functions for privileged roles. This control enables additional security restrictions for these privileged intermediaries and closer monitoring of privileged role activity.

# Security guidance for each intermediary type

This section contains specific security guidance unique to each type of intermediary.

## Privileged Access Management / Privileged Identity management

One type of intermediary designed explicitly for security use cases is privileged identity management / privileged access management (PIM/PAM) solutions.

### Use cases and scenarios for PIM/PAM

PIM/PAM solutions are designed to increase security assurances for sensitive accounts that would be covered by specialized or privileged profiles, and typically focus first on IT administrators.

While features vary between PIM/PAM vendors, many solutions provide security capabilities to:

- Simplify service account management and password rotation (a critically important capability)
- Provide advanced workflows for just in time (JIT) access
- Record and monitor administrative sessions

> ⓘ **Important**
>
> PIM/PAM capabilities provide excellent mitigations for some attacks, but do not address many privielged access risks, notably risk of device compromise. While some vendors advocate that their PIM/PAM solution is a 'silver bullet' solution that can mitigate device risk, our experience investigating customer incidents has consistently proven that this does not work in practice.
>
> An attacker with control of a workstation or device can use those credentials (and privileges assigned to them) while the user is logged on (and can often steal credentials for later use as well). A PIM/PAM solution alone cannot consistently and reliably see and mitigate these device risks, so you must have discrete device and account protections that complement each other.

### Security risks and recommendations for PIM/PAM

The capabilities from each PIM/PAM vendor vary on how to secure them, so review and follow your vendor's specific security configuration recommendations and best practices.

> ⓘ **Note**
>
> Ensure you set up a second person in business critical workflows to help mitigate insider risk (increases the cost/friction for potential collusion by insider threats).

## End-user Virtual Private Networks

Virtual Private Networks (VPNs) are intermediaries that provide full network access for remote endpoints, typically require the end user to authenticate, and can store credentials locally to authenticate inbound user sessions.

> ⓘ Note
>
> This guidance refers only to "point to site" VPNs used by users, not "site to site" VPNs that are typically used for datacenter/application connectivity.

## Use cases and scenarios for VPNs

VPNs establish remote connectivity to enterprise network to enable resource access for users and administrators.

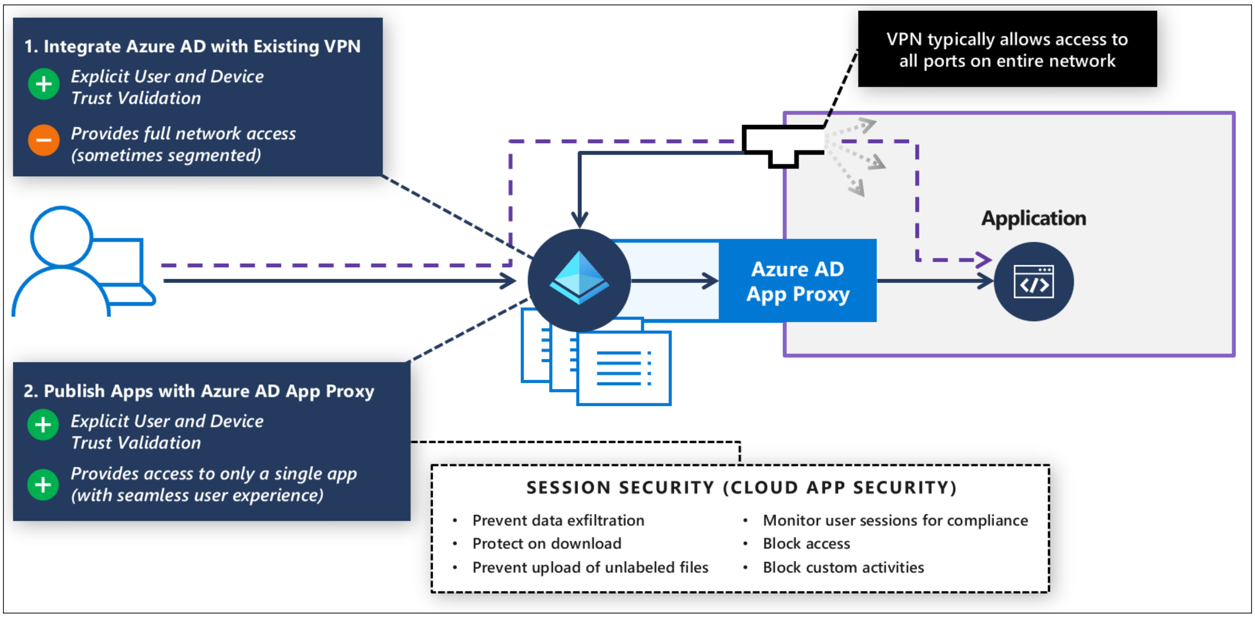
## Security risks and recommendations for VPNs

The most critical risks to VPN intermediaries are from maintenance neglect, configuration issues, and local storage of credentials.

Microsoft recommends a combination of controls for VPN intermediaries:

- **Integrate Microsoft Entra authentication** - to reduce or eliminate risk of locally stored credentials (and any overhead burden to maintain them) and enforce Zero Trust policies on inbound accounts/devices with conditional access. For guidance on integrating, see
  - Azure VPN Microsoft Entra integration
  - Enable Microsoft Entra authentication on the VPN gateway
  - Integrating third-party VPNs
    - Cisco AnyConnect
    - Palo Alto Networks GlobalProtect and Captive Portal
    - F5
    - Fortinet FortiGate SSL VPN
    - Citrix NetScaler
    - Zscaler Private Access (ZPA)
    - and more
- **Rapid patching** - Ensure that all organizational elements support rapid patching including:
  - **Organizational sponsorship** and leadership support for requirement
  - **Standard technical processes** for updating VPNs with minimal or zero downtime. This process should include VPN software, appliances, and any underlying operating systems or firmware
  - **Emergency processes** to rapidly deploy critical security updates
  - **Governance** to continually discover and remediate any missed items

- **Secure configuration** - The capabilities from each VPN vendor vary on how to secure them, so review and follow your vendor's specific security configuration recommendations and best practices
- **Go beyond VPN** - Replace VPNs over time with more secure options like Microsoft Entra application proxy or Azure Bastion as these provide only direct application/server access rather than full network access. Additionally Microsoft Entra application proxy allows session monitoring for additional security with Microsoft Defender for Cloud Apps.



1. Integrate Azure AD with Existing VPN
+ Explicit User and Device Trust Validation
− Provides full network access (sometimes segmented)
VPN typically allows access to all ports on entire network
Application
Azure AD App Proxy
2. Publish Apps with Azure AD App Proxy
+ Explicit User and Device Trust Validation
+ Provides access to only a single app (with seamless user experience)
SESSION SECURITY (CLOUD APP SECURITY)
• Prevent data exfiltration
• Protect on download
• Prevent upload of unlabeled files
• Monitor user sessions for compliance
• Block access
• Block custom activities

## Microsoft Entra application proxy

Microsoft Entra application proxy and similar third-party capabilities provide remote access to legacy and other applications hosted on-premises or on IaaS VMs in the cloud.

### Use cases and scenarios for Microsoft Entra application proxy

This solution is suitable for publishing legacy end-user productivity applications to authorized users over the internet. It can also be used for publishing some administrative applications.

### Security risks and recommendations for Microsoft Entra application proxy

Microsoft Entra application proxy effectively retrofits modern Zero Trust policy enforcement to existing applications. For more information, see Security considerations for Microsoft Entra application proxy

Microsoft Entra application proxy can also integrate with Microsoft Defender for Cloud Apps to add Conditional Access App Control session security to:

- Prevent data exfiltration
- Protect on download
- Prevent upload of unlabeled files
- Monitor user sessions for compliance
- Block access
- Block custom activities

For more information, see Deploy Defender for Cloud Apps Conditional Access App Control for Microsoft Entra apps

As you publish applications via the Microsoft Entra application proxy, Microsoft recommends having application owners work with security teams to follow least privilege and ensure access to each application is made available to only the users that require it. As you deploy more apps this way, you may be able to offset some end-user point to site VPN usage.

## Remote Desktop / jump server

This scenario provides a full desktop environment running one or more applications. This solution has a number of different variations including:

- **Experiences** - Full desktop in a window or a single application projected experience
- **Remote host** - may be a shared VM or a dedicated desktop VM using Windows Virtual Desktop (WVD) or another Virtual Desktop Infrastructure (VDI) solution.
- **Local device** - may be a mobile device, a managed workstation, or a personal/partner managed workstation
- **Scenario** - focused on user productivity applications or on administrative scenarios, often called a 'jump server'

### Use cases and security recommendations for Remote Desktop / Jump server

The most common configurations are:

- Direct Remote Desktop Protocol (RDP) - This configuration is not recommended for internet connections because RDP is a protocol that has limited protections against modern attacks like password spray. Direct RDP should be converted to either:

    - RDP through a gateway published by Microsoft Entra application proxy
    - Azure Bastion
- RDP through a gateway using
    - Remote Desktop Services (RDS) included in Windows Server. Publish with Microsoft Entra application proxy.
    - Windows Virtual Desktop (WVD) - Follow Windows Virtual Desktop security best practices.
    - Third-party VDI - Follow manufacturer or industry best practices, or adapt WVD guidance to your solution
- Secure Shell (SSH) server - providing remote shell and scripting for technology departments and workload owners. Securing this configuration should include:
    - Following industry/manufacturer best practices to securely configure it, change any default passwords (if applicable), and using SSH keys instead of passwords, and securely storing and managing SSH keys.
    - Use Azure Bastion for SSH remoting to resources hosted in Azure - Connect to a Linux VM using Azure Bastion

## Azure Bastion

Azure Bastion is an intermediary that is designed to provide secure access to Azure resources using a browser and the Azure portal. Azure Bastion provides access resources in Azure that support Remote Desktop Protocol (RDP) and Secure Shell (SSH) protocols.

### Use cases and scenarios for Azure Bastion

Azure Bastion effectively provides a flexible solution that can be used by IT Operations personnel and workload administrators outside of IT to manage resources hosted in Azure without requiring a full VPN connection to the environment.

### Security risks and recommendations for Azure Bastion

Azure Bastion is accessed through the Azure portal, so ensure that your Azure portal interface requires the appropriate level of security for the resources in it and roles using it, typically privileged or specialized level.

Additional guidance is available in the Azure Bastion Documentation

# Next steps

- Securing privileged access overview

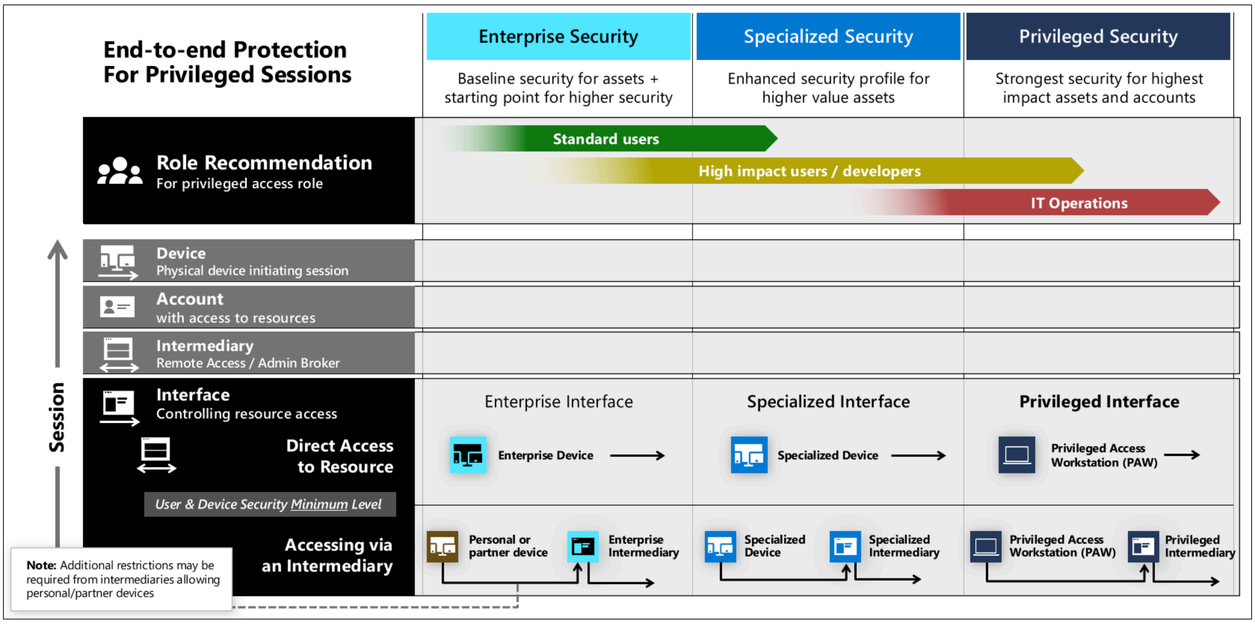
- Privileged access strategy
- Measuring success
- Security levels
- Privileged access accounts
- Interfaces
- Privileged access devices
- Enterprise access model

# Privileged access: Interfaces

Article • 06/20/2024

A critical component of securing privileged access is the application of zero trust policy to ensure that devices, accounts, and intermediaries meet security requirements before providing access.

This policy ensures users and devices initiating the inbound session are known, trusted, and allowed to access the resource (via the interface). The policy enforcement is performed by the Microsoft Entra Conditional Access policy engine that evaluates policy assigned to the specific application interface (such as Azure portal, Salesforce, Office 365, AWS, Workday, and others).



End-to-end Protection For Privileged Sessions
Enterprise Security
Baseline security for assets + starting point for higher security
Specialized Security
Enhanced security profile for higher value assets
Privileged Security
Strongest security for highest impact assets and accounts
Role Recommendation
For privileged access role
Standard users
High impact users / developers
IT Operations
Session
Device
Physical device initiating session
Account
with access to resources
Intermediary
Remote Access / Admin Broker
Interface
Controlling resource access
Direct Access to Resource
User & Device Security Minimum Level
Accessing via an Intermediary
Enterprise Interface
Enterprise Device
Specialized Interface
Specialized Device
Privileged Interface
Privileged Access Workstation (PAW)
Personal or partner device
Enterprise Intermediary
Specialized Device
Specialized Intermediary
Privileged Access Workstation (PAW)
Privileged Intermediary
Note: Additional restrictions may be required from intermediaries allowing personal/partner devices

This guidance defines three security levels for interface security that you can use for assets with different sensitivity levels. These levels are configured in the securing privileged access rapid modernization plan (RAMP) and correspond to security levels of accounts and devices.

The security requirements for inbound sessions to interfaces apply to accounts and the source device, whether it’s a direct connection from physical devices or a Remote Desktop / Jump server intermediary. Intermediaries can accept sessions from personal devices to provide enterprise security level (for some scenarios), but specialized or privileged intermediaries shouldn't allow connections from lower levels because of the security sensitive nature of their roles.

ⓘ Note

These technologies provide strong end to end access control to the application interface, but the resource itself must also be secured from out of band attacks on the application code/functionality, unpatched vulnerabilities or configuration errors in the underlying operating system or firmware, on data at rest or in transit, supply chains, or other means.

Ensure to assess and discover risks to the assets themselves for complete protection. Microsoft provides tooling and guidance to help you with that including Microsoft Defender for Cloud, Microsoft Secure Score, and threat modelling guidance.

## Interface examples

Interfaces come in different forms, typically as:

- Cloud service/application websites such as Azure portal, AWS, Office 365
- Desktop Console managing an on-premises application (Microsoft Management Console (MMC) or custom application)
- Scripting/Console Interface such as Secure Shell (SSH) or PowerShell

While some of these directly support Zero Trust enforcement via the Microsoft Entra Conditional Access policy engine, some of them will need to be published via an intermediary such as Microsoft Entra application proxy or Remote Desktop / jump server.

## Interface security

The ultimate goal of interface security is to ensure that each inbound session to the interface is known, trusted, and allowed:

- Known – User is authenticated with strong authentication and device is authenticated (with exceptions for personal devices using a Remote Desktop or VDI solution for enterprise access)
- Trusted – Security health is explicitly validated and enforced for accounts and devices using a Zero Trust policy engine
- Allowed – Access to the resources follows least privilege principle using a combination of controls to ensure it can only be accessed
    - By the right users
    - At the right time (just in time access, not permanent access)
    - With the right approval workflow (as needed)
    - At an acceptable risk/trust level

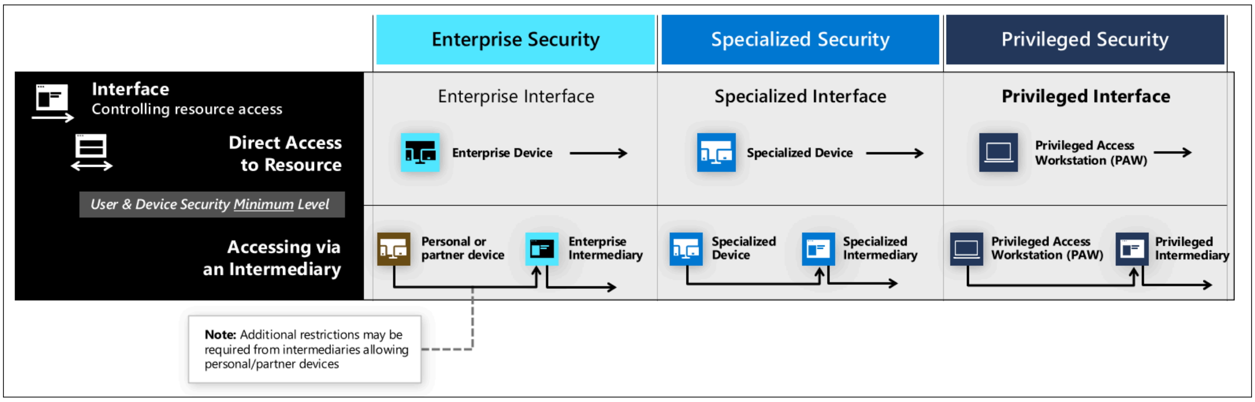
# Interface security controls

Establishing interface security assurances requires a combination of security controls including:

- Zero Trust policy enforcement - using Conditional Access to ensure that the inbound sessions meet the requirements for:
  - Device Trust to ensure the device at minimum:
    - Is managed by the enterprise
    - Has endpoint detection and response on it
    - Is compliant with organizations configuration requirements
    - Isn't infected or under attack during the session
  - User Trust is high enough based on signals including:
    - Multifactor authentication usage during initial sign in (or added later to increase trust)
    - Whether this session matches historical behavior patterns
    - Whether the account or current session triggers any alerts based on threat intelligence
    - Microsoft Entra ID Protection risk
- Role-based access control (RBAC) model that combines enterprise directory groups/permissions and application-specific roles, groups, and permissions
- Just in time access workflows that ensure specific requirements for privileges (peer approvals, audit trail, privileged expiration, etc.) are enforced before allowing privileges the account is eligible for.

# Interface security levels

This guidance defines three levels of security. For more information on these levels, see Keep it Simple - Personas and Profiles. For implementation guidance, see the rapid modernization plan.



**Note:** Additional restrictions may be required from intermediaries allowing personal/partner devices

## Enterprise interface

Enterprise interface security is suitable for all enterprise users and productivity scenarios. Enterprise also serves as a starting point for higher sensitivity workloads that you can incrementally build on to reach specialized and privileged access levels of assurance.

- Zero Trust policy enforcement - on inbound sessions using Conditional Access to ensure that users and devices are secured at the enterprise or higher level
  - To support, bring your own device (BYOD) scenarios, personal devices, and partner-managed devices may be allowed connect if they use an enterprise intermediary such as a dedicated Windows Virtual Desktop (WVD) or similar Remote Desktop / Jump server solution.
- Role-Based Access Control (RBAC) - Model should ensure that the application is administered only by roles at the specialized or privileged security level

## Specialized interface

Security controls for specialized interfaces should include

- Zero Trust policy enforcement - on inbound sessions using Conditional Access to ensure that users and devices are secured at the specialized or privileged level
- Role-Based Access Control (RBAC) - Model should ensure that the application is administered only by roles at the specialized or privileged security level
- Just in time access workflows (optional) - that enforce least privilege by ensuring privileges are used only by authorized users during the time they're needed.

## Privileged interface

Security controls for privileged interfaces should include

- Zero Trust policy enforcement - on inbound sessions using Conditional Access to ensure that users and devices are secured at the privileged level
- Role-Based Access Control (RBAC) - Model should ensure that the application is administered only by roles at the privileged security level
- Just in time access workflows (required) that enforce least privilege by ensuring privileges are used only by authorized users during the time they're needed.

# Next steps

- Securing privileged access overview
- Privileged access strategy
- Measuring success
- Security levels

- Privileged access accounts
- Intermediaries
- Privileged access devices
- Enterprise access model

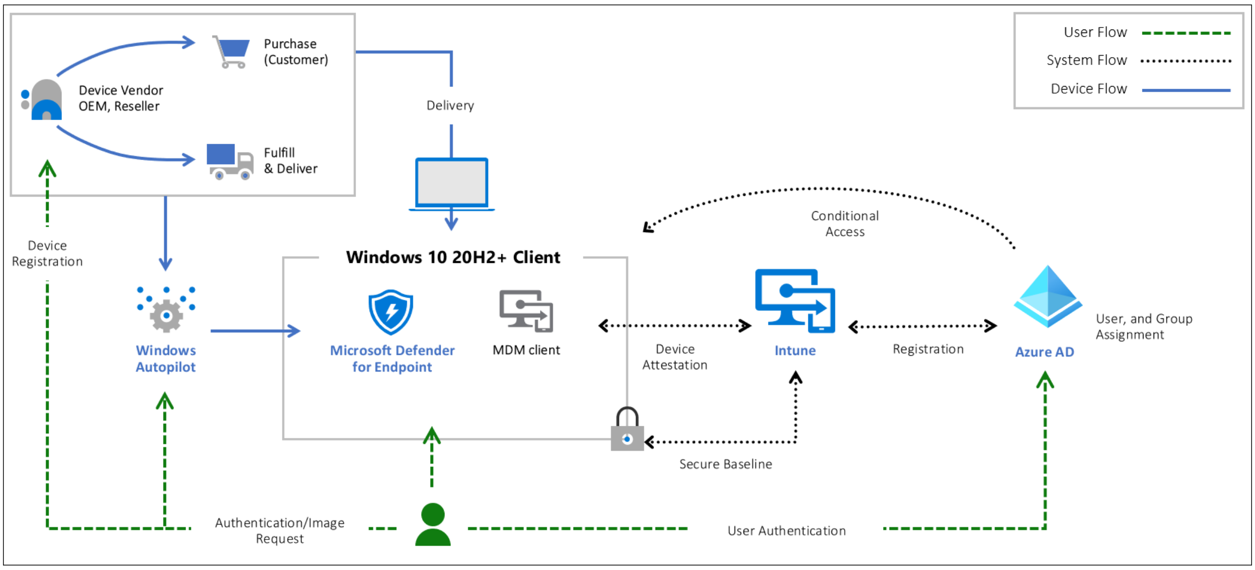
# Securing devices as part of the privileged access story

Article • 01/29/2024

This guidance is part of a complete privileged access strategy and is implemented as part of the Privileged access deployment

End to end zero trust security for privileged access requires a strong foundation of device security upon which to build other security assurances for the session. While security assurances may be enhanced in the session, they will always be limited by how strong the security assurances are in the originating device. An attacker with control of this device can impersonate users on it or steal their credentials for future impersonation. This risk undermines other assurances on the account, intermediaries like jump servers, and on the resources themselves. For more information, see clean source principle

The article provides an overview of security controls to provide a secure workstation for sensitive users throughout its lifecycle.



This solution relies on core security capabilities in the Windows 10 operating system, Microsoft Defender for Endpoint, Microsoft Entra ID, and Microsoft InTune.

## Who benefits from a secure workstation?

All users and operators benefit from using a secure workstation. An attacker who compromises a PC or device can impersonate or steal credentials/tokens for all accounts that use it, undermining many or all other security assurances. For administrators or sensitive accounts, this allows attackers to escalate privileges and increase the access they have in your organization, often dramatically to domain, global, or enterprise administrator privileges.

For details on security levels and which users should be assigned to which level, see Privileged access security levels

# Device Security Controls

The successful deployment of a secure workstation requires it to be part of an end to end approach including devices, accounts, intermediaries, and security policies applied to your application interfaces. All elements of the stack must be addressed for a complete privileged access security strategy.

This table summarizes the security controls for different device levels:

Expand table

| Profile | Enterprise | Specialized | Privileged |
|---|---|---|---|
| Microsoft Endpoint Manager (MEM) managed | Yes | Yes | Yes |
| Deny BYOD Device enrollment | No | Yes | Yes |
| MEM security baseline applied | Yes | Yes | Yes |
| Microsoft Defender for Endpoint | Yes* | Yes | Yes |
| Join personal device via Autopilot | Yes* | Yes* | No |
| URLs restricted to approved list | Allow Most | Allow Most | Deny Default |
| Removal of admin rights | | Yes | Yes |
| Application execution control (AppLocker) | | Audit -> Enforced | Yes |
| Applications installed only by MEM | | Yes | Yes |

ⓘ Note

The solution can be deployed with new hardware, existing hardware, and bring your own device (BYOD) scenarios.

At all levels, good security maintenance hygiene for security updates will be enforced by Intune policies. The differences in security as the device security level increases are focused on reducing the attack surface that an attacker can attempt to exploit (while preserving as much user productivity as possible). Enterprise and specialized level devices allow productivity applications and general web browsing, but privileged access workstations do not. Enterprise users may install their own applications, but specialized users may not (and are not local administrators of their workstations).

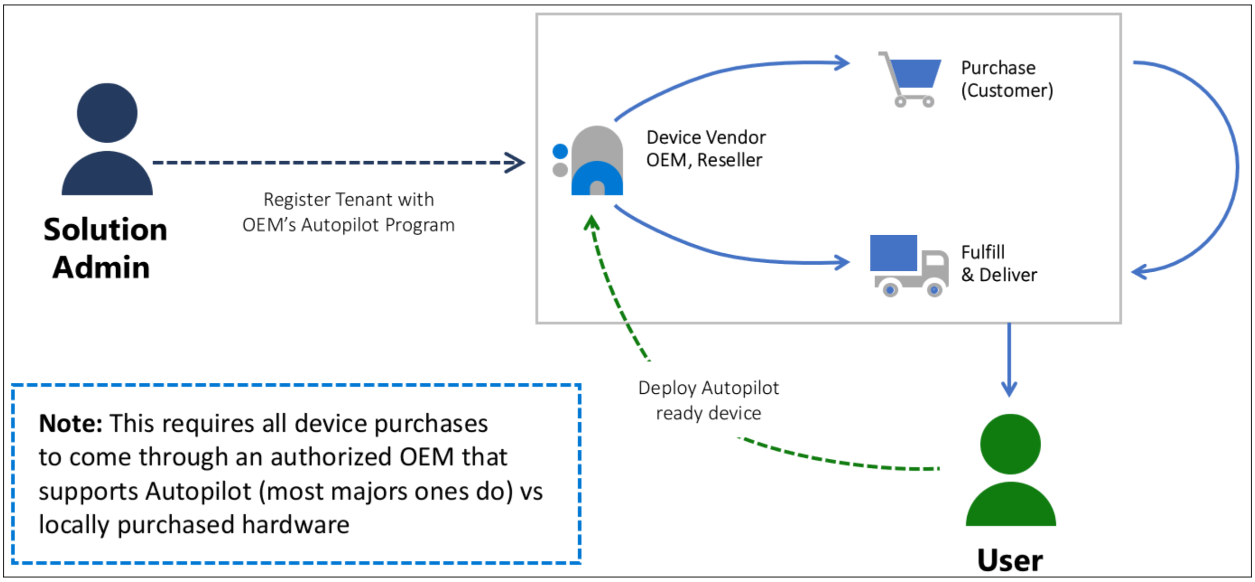
> ⓘ Note
>
> Web browsing here refers to general access to arbitrary websites which can be a high risk activity. Such browsing is distinctly different from using a web browser to access a small number of well-known administrative websites for services like Azure, Microsoft 365, other cloud providers, and SaaS applications.

## Hardware root of trust

Essential to a secured workstation is a supply chain solution where you use a trusted workstation called the 'root of trust'. Technology that must be considered in the selection of the root of trust hardware should include the following technologies included in modern laptops:

- Trusted Platform Module (TPM) 2.0
- BitLocker Drive Encryption
- UEFI Secure Boot
- Drivers and Firmware Distributed through Windows Update
- Virtualization and HVCI Enabled
- Drivers and Apps HVCI-Ready
- Windows Hello
- DMA I/O Protection
- System Guard
- Modern Standby

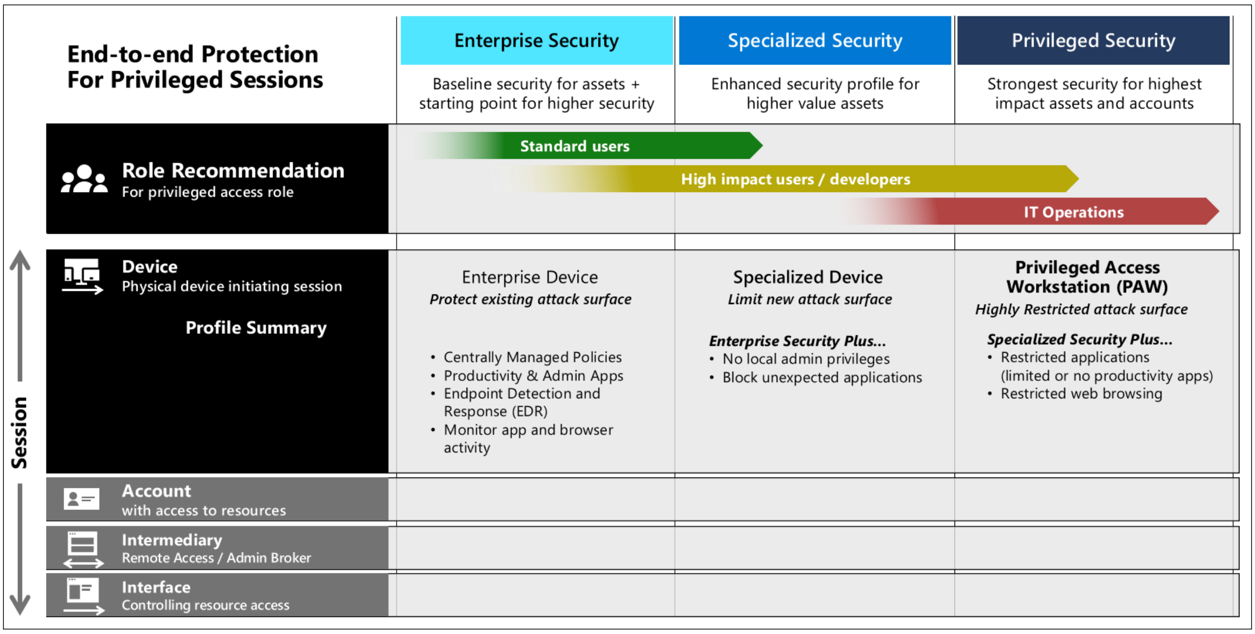
For this solution, root of trust will be deployed using Windows Autopilot technology with hardware that meets the modern technical requirements. To secure a workstation, Autopilot lets you leverage Microsoft OEM-optimized Windows 10 devices. These devices come in a known good state from the manufacturer. Instead of reimaging a potentially insecure device, Autopilot can transform a Windows 10 device into a “business-ready” state. It applies settings and policies, installs apps, and even changes the edition of Windows 10.


Solution Admin
Register Tenant with OEM's Autopilot Program
Device Vendor OEM, Reseller
Purchase (Customer)
Fulfill & Deliver
Deploy Autopilot ready device
User

**Note:** This requires all device purchases to come through an authorized OEM that supports Autopilot (most majors ones do) vs locally purchased hardware

# Device roles and profiles

This guidance shows how to harden Windows 10 and reduce the risks associated with device or user compromise. To take advantage of the modern hardware technology and root of trust device, the solution uses Device Health Attestation. This capability is present to ensure the attackers cannot be persistent during the early boot of a device. It does so by using policy and technology to help manage security features and risks.



| End-to-end Protection For Privileged Sessions | Enterprise Security<br>Baseline security for assets + starting point for higher security | Specialized Security<br>Enhanced security profile for higher value assets | Privileged Security<br>Strongest security for highest impact assets and accounts |
|---|---|---|---|
| **Role Recommendation**<br>For privileged access role | Standard users | Standard users<br>High impact users / developers | High impact users / developers<br>IT Operations |
| **Device**<br>Physical device initiating session<br>**Profile Summary** | Enterprise Device<br>*Protect existing attack surface*<br>• Centrally Managed Policies<br>• Productivity & Admin Apps<br>• Endpoint Detection and Response (EDR)<br>• Monitor app and browser activity | **Specialized Device**<br>***Limit new attack surface***<br>***Enterprise Security Plus...***<br>• No local admin privileges<br>• Block unexpected applications | **Privileged Access Workstation (PAW)**<br>***Highly Restricted attack surface***<br>***Specialized Security Plus...***<br>• Restricted applications (limited or no productivity apps)<br>• Restricted web browsing |
| **Account**<br>with access to resources | | | |
| **Intermediary**<br>Remote Access / Admin Broker | | | |
| **Interface**<br>Controlling resource access | | | |

- **Enterprise Device** – The first managed role is good for home users, small business users, general developers, and enterprises where organizations want to raise the minimum security bar. This profile permits users to run any applications and browse any website, but an anti-malware and endpoint detection and response (EDR) solution like Microsoft Defender for Endpoint is required. A policy-based approach to increase the security posture is taken. It provides a secure means to work with customer data while also using productivity tools like email and web browsing. Audit policies and Intune allow you to monitor an Enterprise workstation for user behavior and profile usage.

The enterprise security profile in the privileged access deployment guidance uses JSON files to configure this with Windows 10 and the provided JSON files.

- **Specialized Device** – This represents a significant step up from enterprise usage by removing the ability to self-administer the workstation and limiting which applications may run to only the applications installed by an authorized administrator (in the program files and pre-approved applications in the user profile location. Removing the ability to install applications may impact productivity if implemented incorrectly, so ensure that you have provided access to Microsoft store applications or corporate managed applications that can be rapidly installed to meet users needs. For guidance on which users should be configured with specialized level devices, see Privileged access security levels
    - The Specialized security user demands a more controlled environment while still being able to do activities such as email and web browsing in a simple-to-use experience. These users expect features such as cookies, favorites, and other shortcuts to work but do not require the ability to modify or debug their device operating system, install drivers, or similar.

The specialized security profile in the privileged access deployment guidance uses JSON files to configure this with Windows 10 and the provided JSON files.

- **Privileged Access Workstation (PAW)** – This is the highest security configuration designed for extremely sensitive roles that would have a significant or material impact on the organization if their account was compromised. The PAW configuration includes security controls and policies that restrict local administrative access and productivity tools to minimize the attack surface to only what is absolutely required for performing sensitive job tasks. This makes the PAW device difficult for attackers to compromise because it blocks the most common vector for phishing attacks: email and web browsing. To provide productivity to these users, separate accounts and workstations must be provided for productivity applications and web browsing. While inconvenient, this is a necessary control to protect users whose account could inflict damage to most or all resources in the organization.
    - A Privileged workstation provides a hardened workstation that has clear application control and application guard. The workstation uses credential guard, device guard, app guard, and exploit guard to protect the host from malicious behavior. All local disks are encrypted with BitLocker and web traffic is restricted to a limit set of permitted destinations (Deny all).

The privileged security profile in the privileged access deployment guidance uses JSON files to configure this with Windows 10 and the provided JSON files.

## Next steps

Deploy a secure Azure-managed workstation.

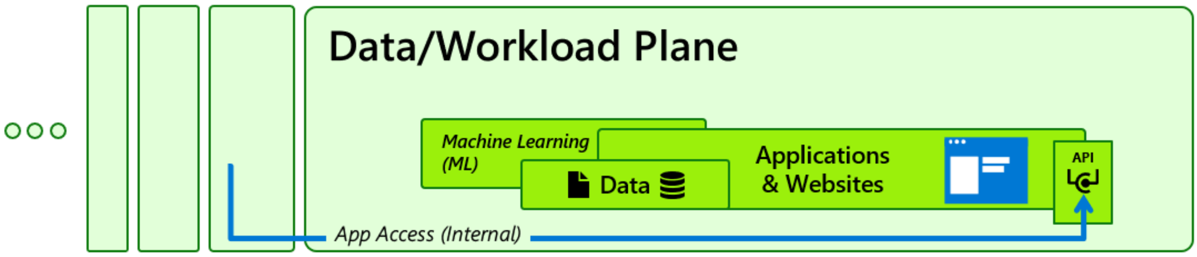
# Enterprise access model

Article • 01/29/2024

This document describes an overall enterprise access model that includes context of how a privileged access strategy fits in. For a roadmap on how to adopt a privileged access strategy, see the rapid modernization plan (RaMP). For implementation guidance to deploy this, see privileged access deployment

Privileged access strategy is part of an overall enterprise access control strategy. This enterprise access model shows how privileged access fits into an overall enterprise access model.

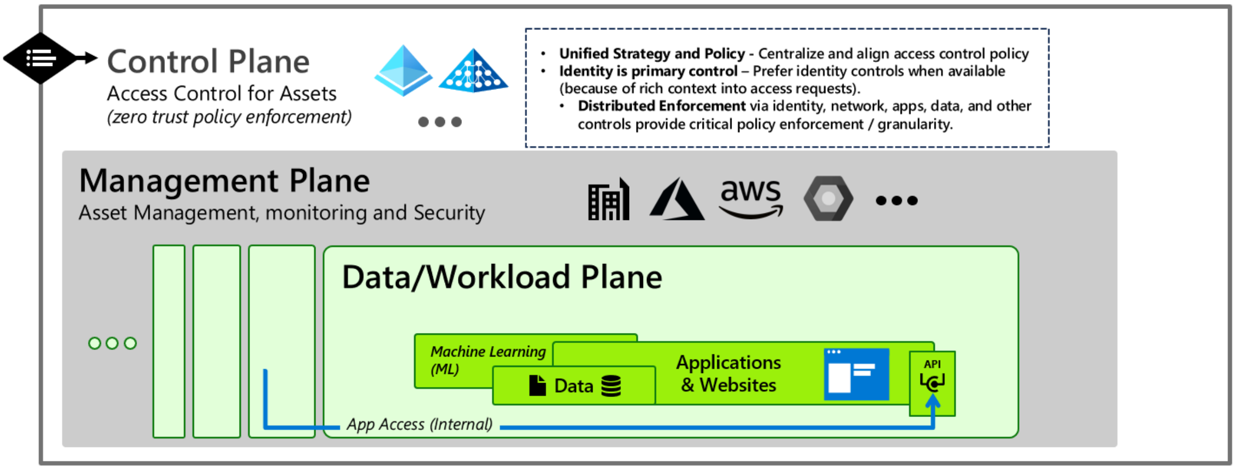
The primary stores of business value that an organization must protect are in the Data/Workload plane:



The applications and data typically store a large percentage of an organization's:

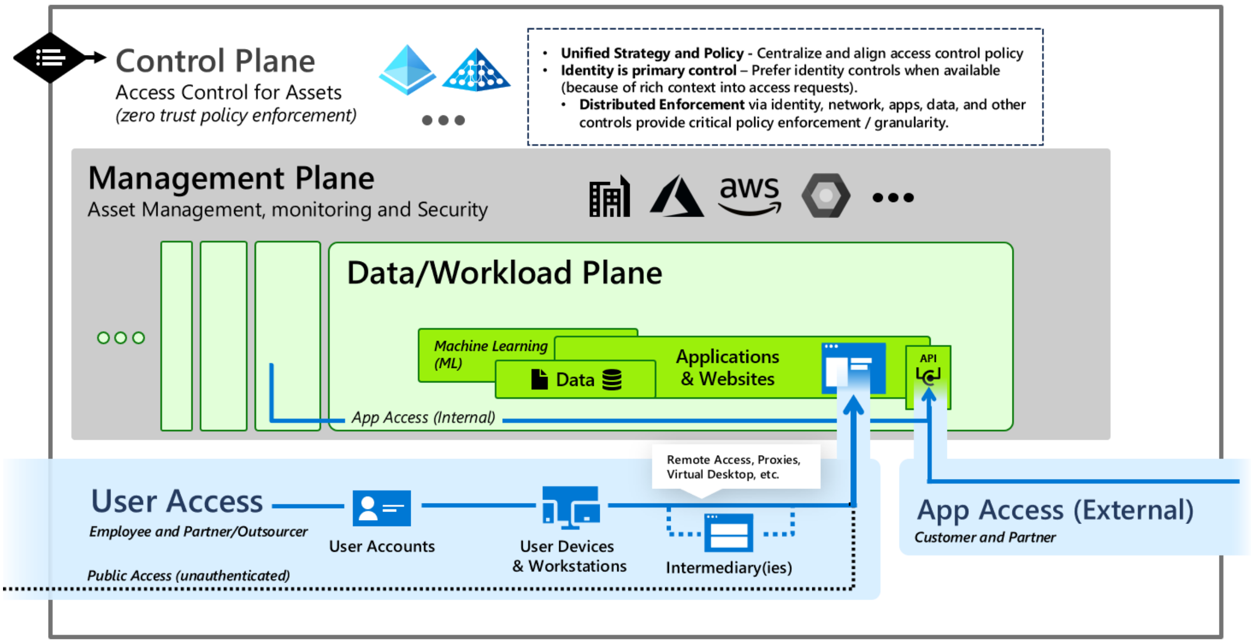
- **Business processes** in applications and workloads
- **Intellectual property** in data and applications

The enterprise IT organization manages and supports the workloads and the infrastructure they are hosted on, whether it's on-premises, on Azure, or a third-party cloud provider, creating a **management plane**. Providing consistent access control to these systems across the enterprise requires a **control plane** based on centralized enterprise identity system(s), often supplemented by network access control for older systems like operational technology (OT) devices.

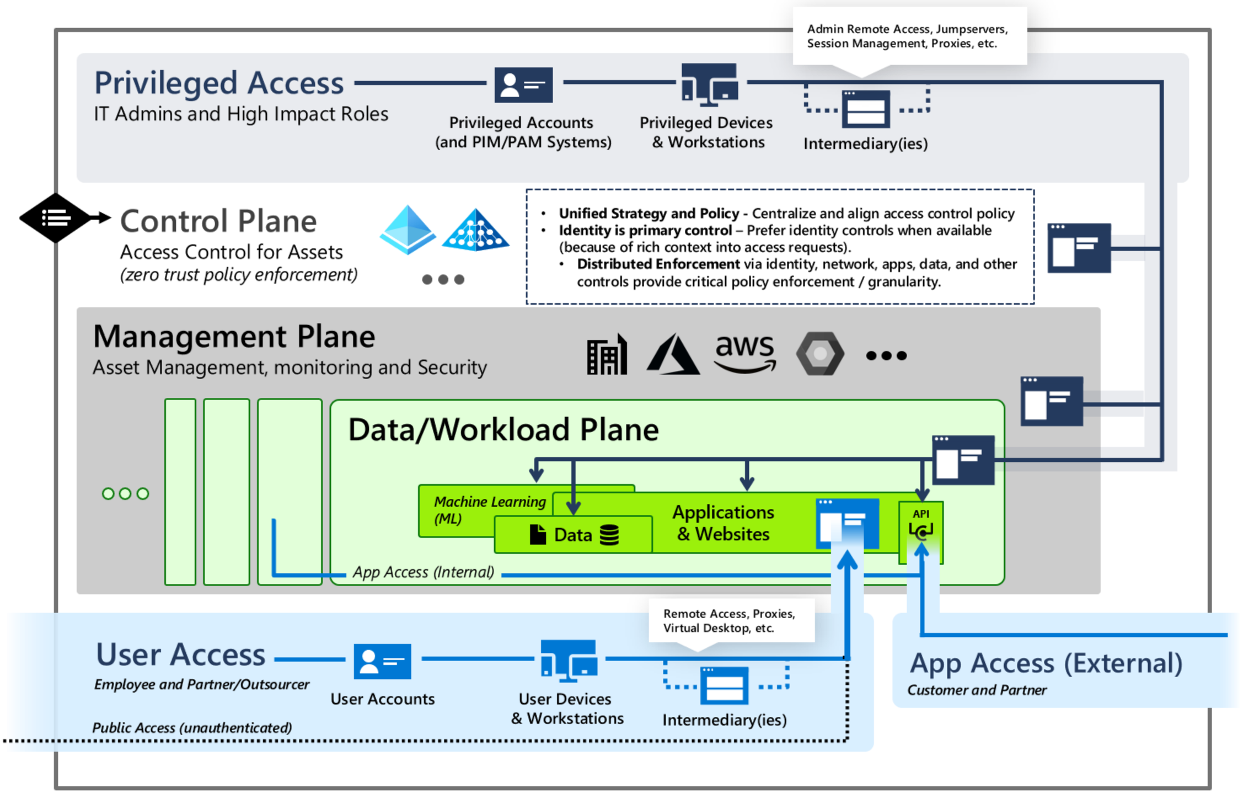

Control Plane
Access Control for Assets
(zero trust policy enforcement)
Unified Strategy and Policy - Centralize and align access control policy
Identity is primary control – Prefer identity controls when available (because of rich context into access requests).
Distributed Enforcement via identity, network, apps, data, and other controls provide critical policy enforcement / granularity.
Management Plane
Asset Management, monitoring and Security
aws
Data/Workload Plane
Machine Learning (ML)
Data
Applications & Websites
API
App Access (Internal)

Each of these planes has control of the data and workloads by virtue of their functions, creating an attractive pathway for attackers to abuse if they can gain control of either plane.

For these systems to create business value, they must be accessible to internal users, partners, and customers using their workstations or devices (often using remote access solutions) - creating **user access** pathways. They must also frequently be available programmatically via application programming interfaces (APIs) to facilitate process automation, creating **application access** pathways.


Control Plane
Access Control for Assets
(zero trust policy enforcement)
Unified Strategy and Policy - Centralize and align access control policy
Identity is primary control – Prefer identity controls when available (because of rich context into access requests).
Distributed Enforcement via identity, network, apps, data, and other controls provide critical policy enforcement / granularity.
Management Plane
Asset Management, monitoring and Security
aws
Data/Workload Plane
Machine Learning (ML)
Data
Applications & Websites
API
App Access (Internal)
User Access
Employee and Partner/Outsourcer
User Accounts
User Devices & Workstations
Remote Access, Proxies, Virtual Desktop, etc.
Intermediary(ies)
Public Access (unauthenticated)
App Access (External)
Customer and Partner

Finally, these systems must be managed and maintained by IT staff, developers, or others in the organizations, creating **privileged access** pathways. Because of the high level of control they provide over business critical assets in the organization, these pathways must be stringently protected against compromise.

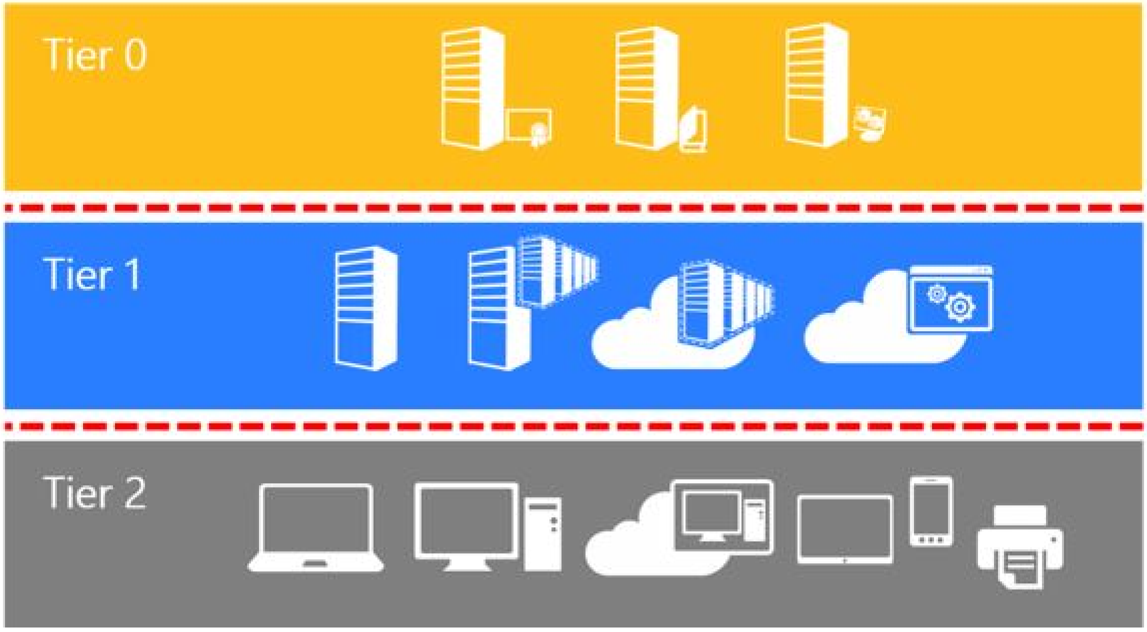

Admin Remote Access, Jumpservers, Session Management, Proxies, etc.
Privileged Access
IT Admins and High Impact Roles
Privileged Accounts (and PIM/PAM Systems)
Privileged Devices & Workstations
Intermediary(ies)
Control Plane
Access Control for Assets
(zero trust policy enforcement)
Unified Strategy and Policy - Centralize and align access control policy
Identity is primary control – Prefer identity controls when available (because of rich context into access requests).
Distributed Enforcement via identity, network, apps, data, and other controls provide critical policy enforcement / granularity.
Management Plane
Asset Management, monitoring and Security
aws
Data/Workload Plane
Machine Learning (ML)
Data
Applications & Websites
API
App Access (Internal)
Remote Access, Proxies, Virtual Desktop, etc.
User Access
Employee and Partner/Outsourcer
User Accounts
User Devices & Workstations
Intermediary(ies)
Public Access (unauthenticated)
App Access (External)
Customer and Partner

Providing consistent access control in the organization that enables productivity and mitigates risk requires you to

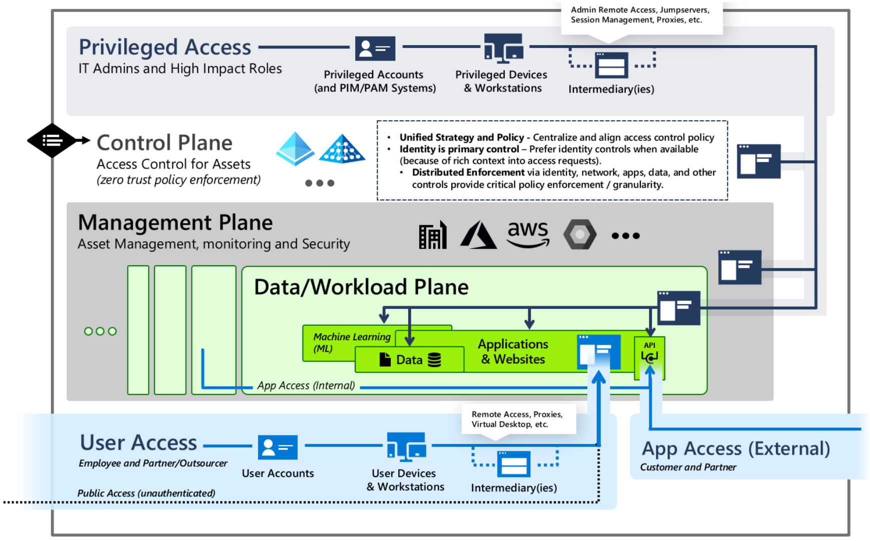
- Enforce Zero Trust principles on all access
  - Assume Breach of other components
  - Explicit validation of trust
  - Least privilege access
- Pervasive security and policy enforcement across
  - Internal and external access to ensure consistent policy application
  - All access methods including users, admins, APIs, service accounts, etc.
- Mitigate unauthorized privilege escalation
  - Enforce hierarchy – to prevent control of higher planes from lower planes (via attacks or abuse of legitimate processes)
    - Control plane
    - Management plane
    - Data/workload plane
  - Continuously audit for configuration vulnerabilities enabling inadvertent escalation
  - Monitor and respond to anomalies that could represent potential attacks

## Evolution from the legacy AD tier model

The enterprise access model supersedes and replaces the legacy tier model that was focused on containing unauthorized escalation of privilege in an on-premises Windows Server Active Directory environment.



The enterprise access model incorporates these elements as well as full access management requirements of a modern enterprise that spans on-premises, multiple clouds, internal or external user access, and more.


Admin Remote Access, Jumpservers, Session Management, Proxies, etc.
Privileged Access
IT Admins and High Impact Roles
Privileged Accounts (and PIM/PAM Systems)
Privileged Devices & Workstations
Intermediary(ies)
Control Plane
Access Control for Assets
(zero trust policy enforcement)
Management Plane
Asset Management, monitoring and Security
aws
Data/Workload Plane
Machine Learning (ML)
Data
Applications & Websites
API
App Access (Internal)
Remote Access, Proxies, Virtual Desktop, etc.
User Access
Employee and Partner/Outsourcer
User Accounts
User Devices & Workstations
Intermediary(ies)
Public Access (unauthenticated)
App Access (External)
Customer and Partner

- **Unified Strategy and Policy** - Centralize and align access control policy
- **Identity is primary control** – Prefer identity controls when available (because of rich context into access requests).
  - **Distributed Enforcement** via identity, network, apps, data, and other controls provide critical policy enforcement / granularity.

**Privileged Access**
Enables IT administrators and other high impact roles to access to sensitive systems and data.
*Stronger security for higher impact accounts*

**Control and Management Planes**
Provide unified access and management for workloads and assets *(and provide attackers shortcut for illicit objectives)*

**Data/Workloads**
Create and store business value in

- Business processes (in apps/workloads)
- Intellectual property (in data and apps)

**User and App Access**
How employees, partners, and customers access these resources

## Tier 0 scope expansion

Tier 0 expands to become the control plane and addresses all aspects of access control, including networking where it is the only/best access control option, such as legacy OT options

## Tier 1 splits

To increase clarity and actionability, what was tier 1 is now split into the following areas:

- **Management plane** – for enterprise-wide IT management functions
- **Data/Workload plane** – for per-workload management, which is sometimes performed by IT personnel and sometimes by business units

This split ensures focus for protecting business critical systems and administrative roles that have high intrinsic business value, but limited technical control. Additionally, this split better accommodates developers and DevOps models vs. focusing too heavily on classic infrastructure roles.

## Tier 2 splits

To ensure coverage for application access and the various partner and customer models, Tier 2 was split into the following areas:

- **User access** – which includes all B2B, B2C, and public access scenarios
- **App access** – to accommodate API access pathways and resulting attack surface

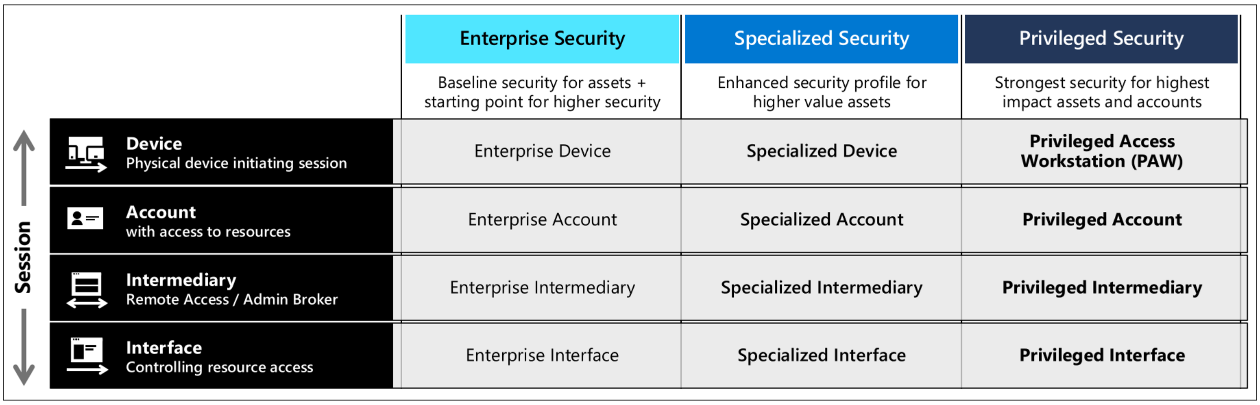
# Next steps

- Securing privileged access overview
- Privileged access strategy
- Measuring success
- Security levels
- Privileged access accounts
- Intermediaries
- Interfaces
- Privileged access devices

# Privileged access deployment

Article • 06/20/2024

This document guides you through implementing the technical components of the privileged access strategy, including secure accounts, workstations and devices, and interface security (with conditional access policy).



Session

| | Enterprise Security | Specialized Security | Privileged Security |
|---|---|---|---|
| | Baseline security for assets + starting point for higher security | Enhanced security profile for higher value assets | Strongest security for highest impact assets and accounts |
| **Device**<br>Physical device initiating session | Enterprise Device | **Specialized Device** | **Privileged Access Workstation (PAW)** |
| **Account**<br>with access to resources | Enterprise Account | **Specialized Account** | **Privileged Account** |
| **Intermediary**<br>Remote Access / Admin Broker | Enterprise Intermediary | **Specialized Intermediary** | **Privileged Intermediary** |
| **Interface**<br>Controlling resource access | Enterprise Interface | **Specialized Interface** | **Privileged Interface** |

This guidance sets up all of the profiles for all three security levels and should be assigned your organizations roles based on the Privileged access security levels guidance. Microsoft recommends configuring them in the order described in the rapid modernization plan (RAMP)

## License requirements

The concepts covered in this guide assume you have Microsoft 365 Enterprise E5 or an equivalent product. Some of the recommendations in this guide can be implemented with other licenses. For more information, see Microsoft 365 Enterprise licensing.

To automate license provisioning, consider group-based licensing for your users.

## Microsoft Entra configuration

Microsoft Entra ID manages users, groups, and devices for your administrator workstations. Enable identity services and features with an administrator account.

When you create the secured workstation administrator account, you expose the account to your current workstation. Make sure you use a known safe device to do this initial configuration and all global configuration. To reduce the attack exposure for the first-time experience, consider following the guidance to prevent malware infections.

Require multifactor authentication, at least for your administrators. See Conditional Access: Require MFA for administrators for implementation guidance.

## Microsoft Entra users and groups

1. From the Azure portal, browse to **Microsoft Entra ID** > **Users** > **New user**.

2. Create your device user by following the steps in the create user tutorial.

3. Enter:

   - **Name** - Secure Workstation User
   - **User name** - `secure-ws-user@contoso.com`
   - **Directory role** - **Limited administrator** and select the **Intune Administrator** role.
   - **Usage Location** - For example **United Kingdom**, or your desired location from the list.

4. Select **Create**.

Create your device administrator user.

1. Enter:

   - **Name** - Secure Workstation Administrator
   - **User name** - `secure-ws-admin@contoso.com`
   - **Directory role** - **Limited administrator** and select the **Intune Administrator** role.
   - **Usage Location** - For example **United Kingdom**, or your desired location from the list.

2. Select **Create**.

Next, you create four groups: **Secure Workstation Users**, **Secure Workstation Admins**, **Emergency BreakGlass** and **Secure Workstation Devices**.

From the Azure portal, browse to **Microsoft Entra ID** > **Groups** > **New group**.

1. For the workstation users group, you might want to configure group-based licensing to automate provisioning of licenses to users.

2. For the workstation users group, enter:

   - **Group type** - Security
   - **Group name** - Secure Workstation Users
   - **Membership type** - Assigned

3. Add your secure workstation user: `secure-ws-user@contoso.com`

4. You can add any other users that use secure workstations.

5. Select **Create**.

6. For the Privileged Workstation Admins group, enter:

   - **Group type** - Security
   - **Group name** - Secure Workstation Admins
   - **Membership type** - Assigned

7. Add your secure workstation user: `secure-ws-admin@contoso.com`

8. You can add any other users that manage secure workstations.

9. Select **Create**.

10. For the Emergency BreakGlass group, enter:

    - **Group type** - Security
    - **Group name** - Emergency BreakGlass
    - **Membership type** - Assigned

11. Select **Create**.

12. Add Emergency Access accounts to this group.

13. For the workstation devices group, enter:

    - **Group type** - Security
    - **Group name** - Secure Workstation Devices
    - **Membership type** - Dynamic Device
    - **Dynamic Membership rules** - `(device.devicePhysicalIds -any _ -contains "[OrderID]:PAW")`

14. Select **Create**.

# Microsoft Entra device configuration

## Specify who can join devices to Microsoft Entra ID

Configure your devices setting in Active Directory to allow your administrative security group to join devices to your domain. To configure this setting from the Azure portal:

1. Go to **Microsoft Entra ID** > **Devices** > **Device settings**.
2. Choose **Selected** under **Users may join devices to Microsoft Entra ID**, and then select the "Secure Workstation Users" group.

### Remove local admin rights

This method requires that users of the VIP, DevOps, and Privileged workstations have no administrator rights on their machines. To configure this setting from the Azure portal:

1. Go to **Microsoft Entra ID** > **Devices** > **Device settings**.
2. Select **None** under **Additional local administrators on Microsoft Entra joined devices**.

Refer to How to manage the local administrators group on Microsoft Entra joined devices for details on how to manage members of the local administrators group.

### Require multifactor authentication to join devices

To further strengthen the process of joining devices to Microsoft Entra ID:

1. Go to **Microsoft Entra ID** > **Devices** > **Device settings**.
2. Select **Yes** under **Require Multi-Factor Auth to join devices**.
3. Select **Save**.

### Configure mobile device management

From the Azure portal:

1. Browse to **Microsoft Entra ID** > **Mobility (MDM and MAM)** > **Microsoft Intune**.
2. Change the **MDM user scope** setting to **All**.
3. Select **Save**.

These steps allow you to manage any device with Microsoft Endpoint Manager. For more information, see Intune Quickstart: Set up automatic enrollment for Windows 10 devices. You create Intune configuration and compliance policies in a future step.

## Microsoft Entra Conditional Access

Microsoft Entra Conditional Access can help restrict privileged administrative tasks to compliant devices. Predefined members of the **Secure Workstation Users** group are required to perform multifactor authentication when signing in to cloud applications. A best practice is to exclude emergency access accounts from the policy. For more information, see Manage emergency access accounts in Microsoft Entra ID.

### Conditional Access only allowing secured workstation ability to access Azure portal

Organizations should block Privileged Users from being able to connect to cloud management interfaces, portals, and PowerShell, from non-PAW devices.

To block unauthorized devices from being able to access cloud management interfaces, follow the guidance in the article Conditional Access: Filters for Devices (preview). It's essential that while deploying this feature you consider, emergency access account functionality. These accounts should be used only for extreme cases and the account managed through policy.

> ⓘ Note
>
> You will need to create a user group, and include your emergency user that can bypass the Conditional Access policy. For our example we have a security group called **Emergency BreakGlass**

This policy set ensures that your Administrators must use a device that is able to present a specific device attribute value, that MFA is satisfied, and the device is marked as compliant by Microsoft Endpoint Manager and Microsoft Defender for Endpoint.

Organizations should also consider blocking legacy authentication protocols in their environments. For more information about blocking legacy authentication protocols, see the article, How to: Block legacy authentication to Microsoft Entra ID with Conditional Access.

# Microsoft Intune configuration

## Device enrollment deny BYOD

In our sample, we recommend that BYOD devices not be permitted. Using Intune BYOD enrollment allows users to enroll devices that are less, or not trusted. However it's important to note that in organizations that have a limited budget to purchase new devices, looking to use existing hardware fleet, or considering non-windows devices, might consider the BYOD capability in Intune to deploy the Enterprise profile.

The following guidance configures enrollment for deployments that deny BYOD access.

## Set enrollment restrictions preventing BYOD

1. In the Microsoft Intune admin center, choose > **Devices** > **Enrollment restrictions** > choose the default restriction **All Users**
2. Select **Properties** > Platform settings **Edit**

3. Select **Block** for All types, except Windows MDM.
4. Select **Block** for all Personally owned items.

## Create an Autopilot deployment profile

After creating a device group, you must create a deployment profile to configure the Autopilot devices.

1. In the Microsoft Intune admin center, choose **Device enrollment** > **Windows enrollment** > **Deployment Profiles** > **Create Profile**.

2. Enter:

   - Name - **Secure workstation deployment profile**.
   - Description - **Deployment of secure workstations**.
   - Set **Convert all targeted devices to Autopilot** to **Yes**. This setting makes sure that all devices in the list get registered with the Autopilot deployment service. Allow 48 hours for the registration to be processed.

3. Select **Next**.

   - For **Deployment mode**, choose **Self-Deploying (Preview)**. Devices with this profile are associated with the user who enrolls the device. During the deployment, it's advisable to use the Self-Deployment mode features to include:
     - Enrolls the device in Intune Microsoft Entra automatic MDM enrollment, and only allow for a device to be accessed until all policies, applications, certificates, and networking profiles are provisioned on the device.
     - User credentials are required to enroll the device. It's essential to note that deploying a device in the **Self-Deploying** mode allows you to deploy laptops in a shared model. No user assignment happens until the device is assigned to a user for the first time. As a result, any user policies such as BitLocker won't be enabled until a user assignment is completed. For more information about how to sign in to a secured device, see selected profiles.
   - Select your Language (Region), User account type **standard**.

4. Select **Next**.

   - Select a scope tag if you have preconfigured one.

5. Select **Next**.

6. Choose **Assignments** > **Assign to** > **Selected Groups**. In **Select groups to include**, choose **Secure Workstation Devices**.

7. Select **Next**.

8. Select **Create** to create the profile. The Autopilot deployment profile is now available to assign to devices.

Device enrollment in Autopilot provides a different user experience based on device type and role. In our deployment example, we illustrate a model where the secured devices are bulk deployed and can be shared, but when used for the first time, the device is assigned to a user. For more information, see Intune Autopilot device enrollment.

# Enrollment Status Page

The Enrollment Status Page (ESP) displays provisioning progress after a new device is enrolled. To ensure that devices are fully configured before use, Intune provides a means to **Block device use until all apps and profiles are installed**.

## Create and assign enrollment status page profile

1. In the Microsoft Intune admin center, choose **Devices** > **Windows** > **Windows enrollment** > **Enrollment Status Page** > **Create profile**.
2. Provide a **Name** and **Description**.
3. Choose **Create**.
4. Choose the new profile in the **Enrollment Status Page** list.
5. Set **Show app profile installation progress** to **Yes**.
6. Set **Block device use until all apps and profiles are installed** to **Yes**.
7. Choose **Assignments** > **Select groups** > choose `Secure Workstation` group > **Select** > **Save**.
8. Choose **Settings** > choose the settings you want to apply to this profile > **Save**.

# Configure Windows Update

Keeping Windows 10 up to date is one of the most important things you can do. To maintain Windows in a secure state, you deploy an update ring to manage the pace that updates are applied to workstations.

This guidance recommends that you create a new update ring and change the following default settings:

1. In the Microsoft Intune admin center, choose **Devices** > **Software updates** > **Windows 10 Update Rings**.

2. Enter:

- Name - **Azure-managed workstation updates**
- Servicing channel - **Semi-annual channel**
- Quality update deferral (days) - **3**
- Feature update deferral period (days) - **3**
- Automatic update behavior - **Auto install and reboot without end-user control**
- Block user from pausing Windows updates - **Block**
- Require user's approval to restart outside of work hours - **Required**
- Allow user to restart (engaged restart) - **Required**
- Transition users to engaged restart after an auto-restart (days) - **3**
- Snooze engaged restart reminder (days) - **3**
- Set deadline for pending restarts (days) - **3**

3. Select **Create**.

4. On the **Assignments** tab, add the **Secure Workstations** group.

For more information about Windows Update policies, see Policy CSP - Update.

## Microsoft Defender for Endpoint Intune integration

Microsoft Defender for Endpoint and Microsoft Intune work together to help prevent security breaches. They can also limit the impact of breaches. These capabilities provide real-time threat detection and enable extensive auditing and logging of the end-point devices.

To configure integration of Windows Defender for Endpoint and Microsoft Endpoint Manager:

1. In the Microsoft Intune admin center, choose **Endpoint Security** > **Microsoft Defender ATP**.

2. In step 1 under **Configuring Windows Defender ATP**, select **Connect Windows Defender ATP to Microsoft Intune in the Windows Defender Security Center**.

3. In the Windows Defender Security Center:
   a. Select **Settings** > **Advanced features**.
   b. For **Microsoft Intune connection**, choose **On**.
   c. Select **Save preferences**.

4. After a connection is established, return to Microsoft Endpoint Manager and select **Refresh** at the top.

5. Set **Connect Windows devices version(20H2) 19042.450 and above to Windows Defender ATP** to **On**.

6. Select **Save**.

## Create the device configuration profile to onboard Windows devices

1. Sign in to the Microsoft Intune admin center, choose **Endpoint security** > **Endpoint detection and response** > **Create profile**.

2. For **Platform**, select **Windows 10 and Later**.

3. For **Profile type**, select **Endpoint detection and response**, and then select **Create**.

4. On the **Basics** page, enter a *PAW - Defender for Endpoint* in the Name field and *Description* (optional) for the profile, then choose **Next**.

5. On the **Configuration settings** page, configure the following option in **Endpoint Detection and Response**:

   - **Sample sharing for all files**: Returns or sets the Microsoft Defender Advanced Threat Protection Sample Sharing configuration parameter.

     Onboard Windows 10 machines using Microsoft Endpoint Configuration Manager has more details on these Microsoft Defender ATP settings.

6. Select **Next** to open the **Scope tags** page. Scope tags are optional. Select **Next** to continue.

7. On the **Assignments** page, select *Secure Workstation* group. For more information on assigning profiles, see Assign user and device profiles.

   Select **Next**.

8. On the **Review + create** page, when you're done, choose **Create**. The new profile is displayed in the list when you select the policy type for the profile you created. **OK**, and then **Create** to save your changes, which creates the profile.

For more information, see Windows Defender Advanced Threat Protection.

## Finish workstation profile hardening

To successfully complete the hardening of the solution, download and execute the appropriate script. Find the download links for your desired **profile level**:

Expand table

| Profile | Download location | Filename |
|---|---|---|
| Enterprise | https://aka.ms/securedworkstationgit | `Enterprise-Workstation-Windows10-(20H2).ps1` |
| Specialized | https://aka.ms/securedworkstationgit | `Specialized-Windows10-(20H2).ps1` |
| Privileged | https://aka.ms/securedworkstationgit | `Privileged-Windows10-(20H2).ps1` |

> ⓘ Note
>
> The removal of of admin rights and access, as well as, Application execution control (AppLocker) are managed by the policy profiles that are deployed.

After the script successfully executes, you can make updates to profiles and policies in Intune. The scripts create policies and profiles for you, but you must assign the policies to your **Secure Workstations** device group.

- Here's where you can find the Intune device configuration profiles created by the scripts: **Azure portal** > **Microsoft Intune** > **Device configuration** > **Profiles**.
- Here's where you can find the Intune device compliance policies created by the scripts: **Azure portal** > **Microsoft Intune** > **Device Compliance** > **Policies**.

Run the Intune data export script `DeviceConfiguration_Export.ps1` from the DeviceConfiguration GitHub repository to export all current Intune profiles for comparison, and evaluation of the profiles.

## Set rules in the Endpoint Protection Configuration Profile for Microsoft Defender Firewall

Windows Firewall policy settings are included in the Endpoint Protection Configuration Profile. The behavior of the policy applied in described in the following table.

Expand table

| Profile | Inbound Rules | Outbound Rules | Merge behavior |
|---|---|---|---|
| Enterprise | Block | Allow | Allow |
| Specialized | Block | Allow | Block |
| Privileged | Block | Block | Block |

**Enterprise**: This configuration is the most permissive as it mirrors the default behavior of a Windows Install. All inbound traffic is blocked except for rules that are explicitly defined in the local policy rules as merging of local rules is set to allowed. All outbound traffic is allowed.

**Specialized**: This configuration is more restrictive as it ignores all locally defined rules on the device. All inbound traffic is blocked including locally defined rules the policy includes two rules to allow Delivery Optimization to function as designed. All outbound traffic is allowed.

**Privileged**: All inbound traffic is blocked including locally defined rules the policy includes two rules to allow Delivery Optimization to function as designed. Outbound traffic is also blocked apart from explicit rules that allow DNS, DHCP, NTP, NSCI, HTTP, and HTTPS traffic. This configuration not only reduces the attack surface presented by the device to the network it limits the outbound connections that the device can establish to only those connections required to administer cloud services.

Expand table

| Rule | Direction | Action | Application / Service | Protocol | Local Ports | Remote Ports |
|---|---|---|---|---|---|---|
| World Wide Web Services (HTTP Traffic-out) | Outbound | Allow | All | TCP | All ports | 80 |
| World Wide Web Services (HTTPS Traffic-out) | Outbound | Allow | All | TCP | All ports | 443 |
| Core Networking - Dynamic Host Configuration Protocol for IPv6(DHCPV6-Out) | Outbound | Allow | %SystemRoot%\system32\svchost.exe | TCP | 546 | 547 |
| Core Networking - Dynamic Host Configuration Protocol for IPv6(DHCPV6-Out) | Outbound | Allow | Dhcp | TCP | 546 | 547 |

| Rule | Direction | Action | Application / Service | Protocol | Local Ports | Remote Ports |
|---|---|---|---|---|---|---|
| Core Networking - Dynamic Host Configuration Protocol for IPv6(DHCP-Out) | Outbound | Allow | %SystemRoot%\system32\svchost.exe | TCP | 68 | 67 |
| Core Networking - Dynamic Host Configuration Protocol for IPv6(DHCP-Out) | Outbound | Allow | Dhcp | TCP | 68 | 67 |
| Core Networking - DNS (UDP-Out) | Outbound | Allow | %SystemRoot%\system32\svchost.exe | UDP | All Ports | 53 |
| Core Networking - DNS (UDP-Out) | Outbound | Allow | Dnscache | UDP | All Ports | 53 |
| Core Networking - DNS (TCP-Out) | Outbound | Allow | %SystemRoot%\system32\svchost.exe | TCP | All Ports | 53 |
| Core Networking - DNS (TCP-Out) | Outbound | Allow | Dnscache | TCP | All Ports | 53 |
| NSCI Probe (TCP-Out) | Outbound | Allow | %SystemRoot%\system32\svchost.exe | TCP | All ports | 80 |
| NSCI Probe - DNS (TCP-Out) | Outbound | Allow | NlaSvc | TCP | All ports | 80 |
| Windows Time (UDP-Out) | Outbound | Allow | %SystemRoot%\system32\svchost.exe | TCP | All ports | 80 |

| Rule | Direction | Action | Application / Service | Protocol | Local Ports | Remote Ports |
|---|---|---|---|---|---|---|
| Windows Time Probe - DNS (UDP-Out) | Outbound | Allow | W32Time | UDP | All ports | 123 |
| Delivery Optimization (TCP-In) | Inbound | Allow | %SystemRoot%\system32\svchost.exe | TCP | 7680 | All ports |
| Delivery Optimization (TCP-In) | Inbound | Allow | DoSvc | TCP | 7680 | All ports |
| Delivery Optimization (UDP-In) | Inbound | Allow | %SystemRoot%\system32\svchost.exe | UDP | 7680 | All ports |
| Delivery Optimization (UDP-In) | Inbound | Allow | DoSvc | UDP | 7680 | All ports |

ⓘ Note

There are two rules defined for each rule in the Microsoft Defender Firewall configuration. To restrict the inbound and outbound rules to Windows Services, e.g. DNS Client, both the service name, DNSCache, and the executable path, C:\Windows\System32\svchost.exe, need to be defined as separate rule rather than a single rule that is possible using Group Policy.

You can make additional changes to the management of both inbound and outbound rules as needed for your permitted and blocked services. For more information, see Firewall configuration service.

## URL lock proxy

Restrictive URL traffic management includes:

- Deny All outbound traffic except selected Azure and Microsoft services including Azure Cloud Shell and the ability to allow self-service password reset.
- The Privileged profile restricts the endpoints on the internet that the device can connect to using the following URL Lock Proxy configuration.

```
[HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Internet
Settings]
"ProxyEnable"=dword:00000001
"ProxyServer"="127.0.0.2:8080"
"ProxyOverride"="*.azure.com;*.azure.net;*.microsoft.com;*.windowsupdate.com;*
.microsoftonline.com;*.microsoftonline.cn;*.windows.net;*.windowsazure.com;*.w
indowsazure.cn;*.azure.cn;*.loganalytics.io;*.applicationinsights.io;*.vsasset
s.io;*.azure-
automation.net;*.visualstudio.com,portal.office.com;*.aspnetcdn.com;*.sharepoi
ntonline.com;*.msecnd.net;*.msocdn.com;*.webtrends.com"
"AutoDetect"=dword:00000000
```

The endpoints listed in the ProxyOverride list are limited to those endpoints needed to authenticate to Microsoft Entra ID and access Azure or Office 365 management interfaces. To extend to other cloud services, add their administration URL to the list. This approach is designed to limit access to the wider internet to protect privileged users from internet-based attacks. If this approach is deemed too restrictive, then consider using the following approach for the privileged role.

## Enable Microsoft Defender for Cloud Apps, URLs restricted list to approved URLs (Allow most)

In our roles deployment it's recommended that for Enterprise, and Specialized deployments, where a strict *deny all* web browsing isn't desirable, that using the capabilities of a cloud access security broker (CASB) such as Microsoft Defender for Cloud Apps be utilized to block access to risky, and questionable web sites. The solution addresses a simple way to block applications and websites that have been curated. This solution is similar to getting access to the blocklist from sites such as the Spamhaus Project who maintains the Domain Blocklist (DBL) ↗: a good resource to use as an advanced set of rules to implement for blocking sites.

The solution provides you:

- Visibility: detect all cloud services; assign each a risk ranking; identify all users and non-Microsoft apps able to sign in
- Data security: identify and control sensitive information (DLP); respond to classification labels on content
- Threat protection: offer adaptive access control (AAC); provide user and entity behavior analysis (UEBA); mitigate malware
- Compliance: supply reports and dashboards to demonstrate cloud governance; assist efforts to conform to data residency and regulatory compliance requirements

Enable Defender for Cloud Apps and connect to Defender ATP to block access the risky URLs:

- In Microsoft Defender Security Center > Settings > Advanced features, set Microsoft Defender for Cloud Apps integration > **ON**
- In Microsoft Defender Security Center > Settings > Advanced features, set Custom network indicators > **ON**
- In Microsoft Defender for Cloud Apps portal > Settings > Microsoft Defender for Endpoint > Select **Enforce app access**

# Manage local applications

The secure workstation moves to a truly hardened state when local applications are removed, including productivity applications. Here, you add Visual Studio Code to allow connection to Azure DevOps for GitHub to manage code repositories.

## Configuring the Company Portal your for custom apps

An Intune-managed copy of the Company Portal gives you on-demand access to additional tools that you can push down to users of the secured workstations.

In a secured mode, application installation is restricted to managed applications delivered by Company Portal. However, installing the Company Portal requires access to Microsoft Store. In your secured solution, you add and assign the Windows 10 Company Portal app for Autopilot provisioned devices.

> ⓘ Note
>
> Make sure you assign the Company Portal app to the **Secure Workstation Device Tag** group used to assign the Autopilot profile.

## Deploy applications using Intune

In some situations, applications like the Microsoft Visual Studio Code are required on the secured workstation. The following example provides instructions to install Microsoft Visual Studio Code to users in the security group **Secure Workstation Users**.

Visual Studio Code is provided as an EXE package so it needs to be packaged as an `.intunewin` format file for deployment using Microsoft Endpoint Manager using the Microsoft Win32 Content Prep Tool.

Download the Microsoft Win32 Content Prep Tool locally to a workstation and copy it to a directory for packaging, for example, C:\Packages. Then create a Source and Output directory under C:\Packages.

## Package Microsoft Visual Studio Code

1. Download the offline installer Visual Studio Code for Windows 64-bit.
2. Copy the downloaded Visual Studio Code exe file to `C:\Packages\Source`
3. Open a PowerShell console and navigate to `C:\Packages`
4. Type `.\IntuneWinAppUtil.exe -c C:\Packages\Source\ -s C:\Packages\Source\VSCodeUserSetup-x64-1.51.1.exe -o C:\Packages\Output\VSCodeUserSetup-x64-1.51.1`
5. Type `Y` to create the new output folder. The intunewin file for Visual Studio Code is created in this folder.

## Upload VS Code to Microsoft Endpoint Manager

1. In the **Microsoft Endpoint Manager admin center**, browse to **Apps** > **Windows** > **Add**
2. Under **Select app type**, choose **Windows app (Win32)**
3. Click **Select app package file**, click **Select a file**, then select the `VSCodeUserSetup-x64-1.51.1.intunewin` from `C:\Packages\Output\VSCodeUserSetup-x64-1.51.1`. Click **OK**
4. Enter `Visual Studio Code 1.51.1` in the Name field
5. Enter a description for Visual Studio Code in the **Description** field
6. Enter `Microsoft Corporation` in the **Publisher** Field
7. Download `https://jsarray.com/images/page-icons/visual-studio-code.png` and select image for the logo. Select **Next**
8. Enter `VSCodeSetup-x64-1.51.1.exe /SILENT` in the **Install command** field
9. Enter `C:\Program Files\Microsoft VS Code\unins000.exe` in the **Uninstall command** field
10. Select **Determine behavior based on return codes** from the **Device Restart behavior** dropdown list. Select **Next**
11. Select **64-bit** from the **Operating system architecture** checkbox dropdown
12. Select **Windows 10 1903** from the **Minimum operating system** checkbox dropdown. Select **Next**
13. Select **Manually configure** detection rules from the **Rules format** dropdown list
14. Click **Add** and then select **File** from the **Rule type** dropdown
15. Enter `C:\Program Files\Microsoft VS Code` in the **Path** field
16. Enter `unins000.exe` in the **File or folder** field
17. Select **File or folder exists** from the dropdown list, Select **OK** and then select **Next**

18. Select **Next** as there are no dependencies on this package
19. Select **Add Group** under **Available for enrolled devices**, add **Privileged Users group**. Click **Select** to confirm group. Select **Next**
20. Click **Create**

## Use PowerShell to create custom apps and settings

There are some configuration settings that we recommend, including two Defender for Endpoint recommendations that must be set using PowerShell. These configuration changes can't be set via policies in Intune.

You can also use PowerShell to extend host management capabilities. The PAW-DeviceConfig.ps1 script from GitHub is an example script that configures the following settings:

- Removes Internet Explorer
- Removes PowerShell 2.0
- Removes Windows Media Player
- Removes Work Folders Client
- Removes XPS Printing
- Enables and configures Hibernate
- Implements registry fix to enable AppLocker DLL rule processing
- Implements registry settings for two Microsoft Defender for Endpoint recommendations that can't be set using Endpoint Manager.
  - Require users to elevate when setting a network's location
  - Prevent saving of network credentials
- Disable Network Location Wizard - prevents users from setting network location as Private and therefore increasing the attack surface exposed in Windows Firewall
- Configures Windows Time to use NTP and sets the Auto Time service to Automatic
- Downloads and sets the desktop background to a specific image to easily identify the device as a ready-to-use, privileged workstation.

The PAW-DeviceConfig.ps1 script from GitHub.

1. Download the script [PAW-DeviceConfig.ps1] to a local device.
2. Browse to the **Azure portal** > **Microsoft Intune** > **Device configuration** > **PowerShell scripts** > **Add**. vProvide a **Name** for the script and specify the **Script location**.
3. Select **Configure**.
   a. Set **Run this script using the logged on credentials** to **No**.
   b. Select **OK**.
4. Select **Create**.
5. Select **Assignments** > **Select groups**.

a. Add the security group **Secure Workstations**.
b. Select **Save**.

# Validate and test your deployment with your first device

This enrollment assumes that you use a physical computing device. It's recommended that as part of the procurement process that the OEM, Reseller, distributor, or partner register devices in Windows Autopilot.

However for testing it's possible to stand up Virtual Machines as a test scenario. However note enrollment of personally joined devices need to be revised to allow this method of joining a client.

This method works for Virtual Machines or physical devices that haven't been previously registered.

1. Start the device and wait for the username dialog to be presented
2. Press `SHIFT + F10` to display command prompt
3. Type `PowerShell` press Enter
4. Type `Set-ExecutionPolicy RemoteSigned` press Enter
5. Type `Install-Script Get-WindowsAutopilotInfo` press Enter
6. Type `Y` and click Enter to accept PATH environment change
7. Type `Y` and click Enter to install NuGet provider
8. Type `Y` to trust the repository
9. Type Run `Get-WindowsAutoPilotInfo -GroupTag PAW –outputfile C:\device1.csv`
10. Copy the CSV from the Virtual Machine or Physical device

# Import devices into Autopilot

1. In the **Microsoft Endpoint Manager admin center**, go to **Devices** > **Windows Devices** > **Windows enrollment** > **Devices**

2. Select **Import** and choose your CSV file.

3. Wait for the `Group Tag` to be updated to `PAW` and the `Profile Status` to change to `Assigned`.

> ⓘ **Note**

> The Group Tag is used by the Secure Workstation dynamic group to make the device a member of its group,

4. Add the device to the **Secure Workstations** security group.
5. On the Windows 10 device you wish to configure, go to **Windows Settings** > **Update & Security** > **Recovery**.
   a. Choose **Get started** under **Reset this PC**.
   b. Follow the prompts to reset and reconfigure the device with the profile and compliance policies configured.

After you configure the device, complete a review and check the configuration. Confirm that the first device is configured correctly before continuing your deployment.

## Assign devices

To assign devices and users, you need to map the selected profiles to your security group. All new users who require permissions to the service must be added to the security group as well.

# Using Microsoft Defender for Endpoint to monitor and respond to security incidents

- Continuously observe and monitor vulnerabilities and misconfigurations
- Utilize Microsoft Defender for Endpoint to prioritize dynamic threats in the wild
- Drive correlation of vulnerabilities with endpoint detection and response (EDR) alerts
- Use the dashboard to identify machine-level vulnerability during investigations
- Push out remediations to Intune

Configure your Microsoft Defender Security Center . Using guidance at Threat & Vulnerability Management dashboard overview.

## Monitoring application activity using Advanced Threat Hunting

Starting at the specialized workstation, AppLocker is enabled for monitoring of application activity on a workstation. By default Defender for Endpoint captures AppLocker events and Advanced Hunting Queries can be used to determine what applications, scripts, DLL files are being blocked by AppLocker.

> ⓘ Note

The Specialized and Privileged workstation profiles contain the AppLocker policies. Deployment of the policies is required for monitoring of application activity on a client.

From the Microsoft Defender Security Center Advanced Hunting pane, use the following query to return AppLocker events

Kusto

```
DeviceEvents
| where Timestamp > ago(7d) and
ActionType startswith "AppControl"
| summarize Machines=dcount(DeviceName) by ActionType
| order by Machines desc
```

# Monitoring

- Understand how to review your Exposure Score
- Review Security recommendation
- Manage security remediations
- Manage endpoint detection and response
- Monitor profiles with Intune profile monitoring.

# Next steps

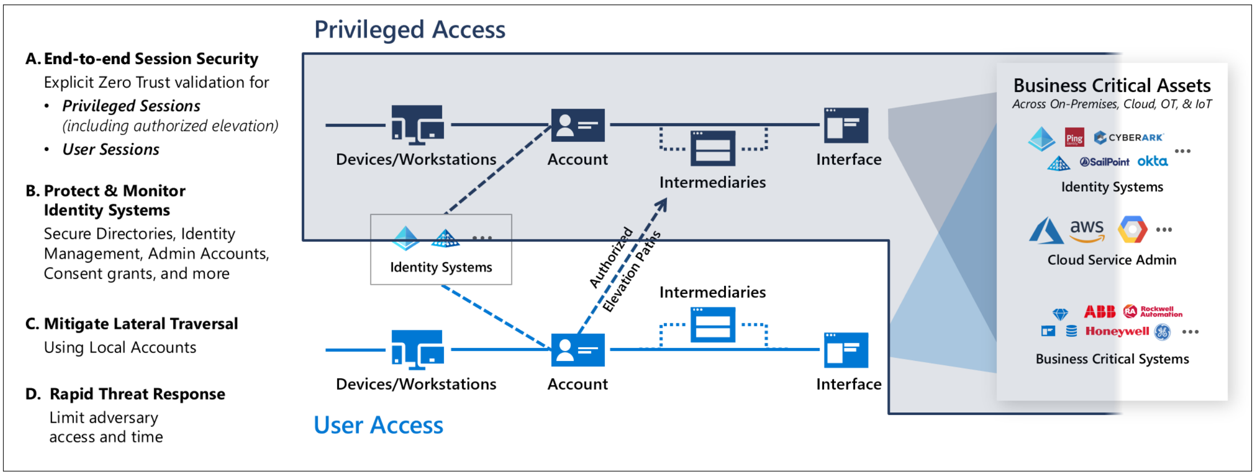
- Securing privileged access overview
- Privileged access strategy
- Measuring success
- Security levels
- Privileged access accounts
- Intermediaries
- Interfaces
- Privileged access devices
- Enterprise access model

# Security rapid modernization plan

Article • 01/29/2024

This rapid modernization plan (RAMP) will help you quickly adopt Microsoft's recommended privileged access strategy.

This roadmap builds on the technical controls established in the privileged access deployment guidance. Complete those steps and then use the steps in this RAMP to configure the controls for your organization.



Privileged Access
A. End-to-end Session Security
Explicit Zero Trust validation for
Privileged Sessions
(including authorized elevation)
User Sessions
B. Protect & Monitor Identity Systems
Secure Directories, Identity Management, Admin Accounts, Consent grants, and more
C. Mitigate Lateral Traversal
Using Local Accounts
D. Rapid Threat Response
Limit adversary access and time
Devices/Workstations
Account
Intermediaries
Interface
Identity Systems
Authorized Elevation Paths
Intermediaries
Devices/Workstations
Account
Interface
User Access
Business Critical Assets
Across On-Premises, Cloud, OT, & IoT
CYBERARK
SailPoint
okta
Identity Systems
aws
Cloud Service Admin
ABB
Rockwell Automation
Honeywell
Business Critical Systems

> ⓘ Note
>
> Many of these steps will have a green/brownfield dynamic as organizations often have security risks in the way they are already deployed or configured accounts. This roadmap prioritizes stopping the accumulation of new security risks first, and then later cleans up the remaining items that have already accumulated.

As you progress through the roadmap, you can utilize Microsoft Secure Score to track and compare many items in the journey with others in similar organizations over time. Learn more about Microsoft Secure Score in the article Secure score overview.

Each item in this RAMP is structured as an initiative that will be tracked and managed using a format that builds on the objectives and key results (OKR) methodology. Each item includes what (objective), why, who, how, and how to measure (key results). Some items require changes to processes and people's knoweldge/skills, while others are simpler technology changes. Many of these initiatives will include members outside of the traditional IT Department that should be included in the decision making and implementation of these changes to ensure they are successfully integrated in your organization.

It is critical to work together as an organization, create partnerships, and educate people who traditionally were not part of this process. It is critical to create and maintain buy-in across the organization, without it many projects fail.

# Separate and manage privileged accounts

## Emergency access accounts

- **What**: Ensure that you are not accidentally locked out of your Microsoft Entra organization in an emergency situation.
- **Why**: Emergency access accounts rarely used and highly damaging to the organization if compromised, but their availability to the organization is also critically important for the few scenarios when they are required. Ensure you have a plan for continuity of access that accommodates both expected and unexpected events.
- **Who**: This initiative is typically led by Identity and Key Management and/or Security Architecture.
  - **Sponsorship:** This initiative is typically sponsored by CISO, CIO, or Director of Identity
  - **Execution:** This initiative is a collaborative effort involving
    - Policy and standards team document clear requirements and standards
    - Identity and Key Management or Central IT Operations to implement any changes
    - Security Compliance management monitors to ensure compliance
- **How**: Follow the guidance in Manage emergency access accounts in Microsoft Entra ID.
- **Measure key results:**
  - **Established** Emergency access process has been designed based on Microsoft guidance that meets organizational needs
  - **Maintained** Emergency access has been reviewed and tested within the past 90 days

## Enable Microsoft Entra Privileged Identity Management

- **What**: Use Microsoft Entra Privileged Identity Management (PIM) in your Microsoft Entra production environment to discover and secure privileged accounts
- **Why**: Privileged Identity Management provides time-based and approval-based role activation to mitigate the risks of excessive, unnecessary, or misused access permissions.

- **Who**: This initiative is typically led by Identity and Key Management and/or Security Architecture.
    - **Sponsorship:** This initiative is typically sponsored by CISO, CIO, or Director of Identity
    - **Execution:** This initiative is a collaborative effort involving
        - Policy and standards team document clear requirements and standards (based on this guidance)
        - Identity and Key Management or Central IT Operations to implement any changes
        - Security Compliance management monitors to ensure compliance
- **How**: Deploy and Configure Microsoft Entra Privileged Identity Management using the guidance in the article, Deploy Microsoft Entra Privileged Identity Management (PIM).
- **Measure key results**: 100% of applicable privileged access roles are using Microsoft Entra PIM

## Identify and categorize privileged accounts (Microsoft Entra ID)

- **What**: Identify all roles and groups with high business impact that will require privileged security level (immediately or over time). These administrators will require sparate accounts in a later step Privileged access administration.

- **Why**: This step is required to identify and minimize the number of people that require separate accounts and privileged access protection

- **Who**: This initiative is typically led by Identity and Key Management and/or Security Architecture.
    - **Sponsorship:** This initiative is typically sponsored by CISO, CIO, or Director of Identity
    - **Execution:** This initiative is a collaborative effort involving
        - Policy and standards team document clear requirements and standards (based on this guidance)
        - Identity and Key Management or Central IT Operations to implement any changes
        - Security Compliance management monitors to ensure compliance

- **How**: After turning on Microsoft Entra Privileged Identity Management, view the users who are in the following Microsoft Entra roles at a minimum based on your organizations risk policies:
    - Global administrator

  - Privileged role administrator
  - Exchange administrator
  - SharePoint administrator

  For a complete list of administrator roles, see Administrator role permissions in Microsoft Entra ID.

  > Remove any accounts that are no longer needed in those roles. Then, categorize the remaining accounts that are assigned to admin roles:
  > - Assigned to administrative users, but also used for non-administrative productivity purposes, like reading and responding to email.
  > - Assigned to administrative users and used for administrative purposes only
  > - Shared across multiple users
  > - For break-glass emergency access scenarios
  > - For automated scripts
  > - For external users

If you don't have Microsoft Entra Privileged Identity Management in your organization, you can use the PowerShell API. Also start with the Global Administrator role, because a Global Administrator has the same permissions across all cloud services for which your organization has subscribed. These permissions are granted no matter where they were assigned: in the Microsoft 365 admin center, the Azure portal, or by the Azure AD module for Microsoft PowerShell.

- **Measure key results:** Review and Identification of privileged access roles has been completed within the past 90 days

## Separate accounts (On-premises AD accounts)

- **What**: Secure on-premises privileged administrative accounts, if not already done. This stage includes:
  - Creating separate admin accounts for users who need to conduct on-premises administrative tasks
  - Deploying Privileged Access Workstations for Active Directory administrators
  - Creating unique local admin passwords for workstations and servers

- **Why**: Hardening the accounts used for administrative tasks. The administrator accounts should have mail disabled and no personal Microsoft accounts should be allowed.

- **Who**: This initiative is typically led by Identity and Key Management and/or Security Architecture.

    - **Sponsorship:** This initiative is typically sponsored by CISO, CIO, or Director of Identity
    - **Execution:** This initiative is a collaborative effort involving
        - Policy and standards team document clear requirements and standards (based on this guidance)
        - Identity and Key Management or Central IT Operations to implement any changes
        - Security Compliance management monitors to ensure compliance

- **How**: All personnel that are authorized to possess administrative privileges must have separate accounts for administrative functions that are distinct from user accounts. **Do not share these accounts between users.**
    - *Standard user accounts* - Granted standard user privileges for standard user tasks, such as email, web browsing, and using line-of-business applications. These accounts are not granted administrative privileges.
    - *Administrative accounts* - Separate accounts created for personnel who are assigned the appropriate administrative privileges.

- **Measure key results:** 100% of on-premises privileged users have separate dedicated accounts

## Microsoft Defender for Identity

- **What**: Microsoft Defender for Identity combines on-premises signals with cloud insights to monitor, protect, and investigate events in a simplified format enabling your security teams to detect advanced attacks against your identity infrastructure with the ability to:
    - Monitor users, entity behavior, and activities with learning-based analytics
    - Protect user identities and credentials stored in Active Directory
    - Identify and investigate suspicious user activities and advanced attacks throughout the kill chain
    - Provide clear incident information on a simple timeline for fast triage

- **Why**: Modern attackers may stay undetected for long periods of time. Many threats are hard to find without a cohesive picture of your entire identity environment.

- **Who**: This initiative is typically led by Identity and Key Management and/or Security Architecture.
    - **Sponsorship:** This initiative is typically sponsored by CISO, CIO, or Director of Identity
    - **Execution:** This initiative is a collaborative effort involving

    - Policy and standards team document clear requirements and standards (based on this guidance)
    - Identity and Key Management or Central IT Operations to implement any changes
    - Security Compliance management monitors to ensure compliance

- **How**: Deploy and enable Microsoft Defender for Identity and review any open alerts.

- **Measure key results**: All open alerts reviewed and mitigated by the appropriate teams.

## Improve credential management experience

### Implement and document self-service password reset and combined security information registration

- **What**: Enable and configure self-service password reset (SSPR) in your organization and enable the combined security information registration experience.
- **Why**: Users are able to reset their own passwords once they have registered. The combined security information registration experience provides a better user experience allowing registration for Microsoft Entra multifactor authentication and self-service password reset. These tools when used together contribute to lower helpdesk costs and more satisfied users.
- **Who**: This initiative is typically led by Identity and Key Management and/or Security Architecture.
  - **Sponsorship:** This initiative is typically sponsored by CISO, CIO, or Director of Identity
  - **Execution:** This initiative is a collaborative effort involving
    - Policy and standards team document clear requirements and standards (based on this guidance)
    - Identity and Key Management or Central IT Operations to implement any changes
    - Security Compliance management monitors to ensure compliance
    - Central IT Operations Helpdesk processes have been updated and personnel has been trained on them
- **How**: To enable and deploy SSPR, see the article Plan a Microsoft Entra self-service password reset deployment.
- **Measure key results**: Self-service password reset is fully configured and available to the organization

## Protect admin accounts - Enable and require MFA / Passwordless for Microsoft Entra ID privileged users

- **What**: Require all privileged accounts in Microsoft Entra ID to use strong multifactor authentication

- **Why**: To protect access to data and services in Microsoft 365.

- **Who**: This initiative is typically led by Identity and Key Management and/or Security Architecture.
  - **Sponsorship:** This initiative is typically sponsored by CISO, CIO, or Director of Identity
  - **Execution:** This initiative is a collaborative effort involving
    - Policy and standards team document clear requirements and standards (based on this guidance)
    - Identity and Key Management or Central IT Operations to implement any changes
    - Security Compliance management monitors to ensure compliance
    - Central IT Operations Helpdesk processes have been updated and personnel has been trained on them
    - Central IT Operations Service owner processes have been updated and personnel has been trained on them

- **How**: Turn on Microsoft Entra multifactor authentication (MFA) and register all other highly privileged single-user non-federated admin accounts. Require multifactor authentication at sign-in for all individual users who are permanently assigned to one or more of the Microsoft Entra admin roles like:
  - Global administrator
  - Privileged Role administrator
  - Exchange administrator
  - SharePoint administrator

  Require administrators to use passwordless sign-in methods such as FIDO2 security keys or Windows Hello for Business in conjunction with unique, long, complex passwords. Enforce this change with an organizational policy document.

Follow the guidance in the following articles, Plan a Microsoft Entra multifactor authentication deployment and Plan a passwordless authentication deployment in Microsoft Entra ID.

- **Measure key results**: 100% of privileged users are using passwordless authentication or a strong form of multifactor authentication for all logons. See Privileged Access Accounts for description of multifactor authentication

## Block legacy authentication protocols for privileged user accounts

- **What**: Block legacy authentication protocol use for privileged user accounts.
- **Why**: Organizations should block these legacy authentication protocols because multifactor authentication cannot be enforced against them. Leaving legacy authentication protocols enabled can create an entry point for attackers. Some legacy applications may rely on these protocols and organizations have the option to create specific exceptions for certain accounts. These exceptions should be tracked and additional monitoring controls implemented.
- **Who**: This initiative is typically led by Identity and Key Management and/or Security Architecture.
  - **Sponsorship:** This initiative is typically sponsored by CISO, CIO, or Director of Identity
  - **Execution:** This initiative is a collaborative effort involving
    - Policy and standards: establish clear requirements
    - Identity and Key Management or Central IT Operations Central IT Operations to implement the policy
    - Security Compliance management monitors to ensure compliance
- **How**: To block legacy authentication protocols in your organization, follow the guidance in the article How to: Block legacy authentication to Microsoft Entra ID with Conditional Access.
- **Measure key results**:
  - **Legacy protocols blocked:** All legacy protocols are blocked for all users, with only authorized exceptions
  - **Exceptions** are reviewed every 90 days and expire permanently within one year. Application owners must fix all exceptions within one year of first exception approval

## Application consent process

- **What**: Disable end-user consent to Microsoft Entra applications.

> ⓘ **Note**
>
> This change will require centralizing the decision-making process with your organization's security and identity administration teams.

- **Why**: Users can inadvertently create organizational risk by providing consent for an app that can maliciously access organizational data.
- **Who**: This initiative is typically led by Identity and Key Management and/or Security Architecture.
  - **Sponsorship:** This initiative is typically sponsored by CISO, CIO, or Director of Identity
  - **Execution:** This initiative is a collaborative effort involving
    - Policy and standards team document clear requirements and standards (based on this guidance)
    - Identity and Key Management or Central IT Operations to implement any changes
    - Security Compliance management monitors to ensure compliance
    - Central IT Operations Helpdesk processes have been updated and personnel has been trained on them
    - Central IT Operations Service owner processes have been updated and personnel has been trained on them
- **How**: Establish a centralized consent process to maintain centralized visibility and control of the applications that have access to data by following the guidance in the article, Managing consent to applications and evaluating consent requests.
- **Measure key results**: End users are not able to consent to Microsoft Entra application access

## Clean up account and sign-in risks

- **What**: Enable Microsoft Entra ID Protection and cleanup any risks that it finds.
- **Why**: Risky user and sign-in behavior can be a source of attacks against your organization.
- **Who**: This initiative is typically led by Identity and Key Management and/or Security Architecture.
  - **Sponsorship:** This initiative is typically sponsored by CISO, CIO, or Director of Identity
  - **Execution:** This initiative is a collaborative effort involving
    - Policy and standards team document clear requirements and standards (based on this guidance)
    - Identity and Key Management or Central IT Operations to implement any changes
    - Security Compliance management monitors to ensure compliance
    - Central IT Operations Helpdesk processes have been updated for related support calls and personnel has been trained on them

- **How**: Create a process that monitors and manages user and sign-in risk. Decide if you will automate remediation, using Microsoft Entra multifactor authentication and SSPR, or block and require administrator intervention.Follow the guidance in the article How To: Configure and enable risk policies.
- **Measure key results**: The organization has zero unaddressed user and sign-in risks.

> ⓘ Note
>
> Conditional Access policies are required to block accrual of new sign-in risks. See the Conditional access section of **Privileged Access Deployment**

# Admin workstations initial deployment

- **What**: Privileged accounts such as Global Administrators have dedicated workstations to perform administrative tasks from.
- **Why**: Devices where privileged administration tasks are completed are a target of attackers. Securing not only the account but these assets are critical in reducing your attack surface area. This separation limits their exposure to common attacks directed at productivity-related tasks like email and web browsing.
- **Who**: This initiative is typically led by Identity and Key Management and/or Security Architecture.
    - **Sponsorship:** This initiative is typically sponsored by CISO, CIO, or Director of Identity
    - **Execution:** This initiative is a collaborative effort involving
        - Policy and standards team document clear requirements and standards (based on this guidance)
        - Identity and Key Management or Central IT Operations to implement any changes
        - Security Compliance management monitors to ensure compliance
        - Central IT Operations Helpdesk processes have been updated and personnel has been trained on them
        - Central IT Operations Service owner processes have been updated and personnel has been trained on them
- **How**: Initial deployment should be to the Enterprise level as described in the article Privileged Access Deployment
- **Measure key results**: Every privileged account has a dedicated workstation to perform sensitive tasks from.

> ⓘ Note

This step rapidly establishes a security baseline and must be increased to specialized and privileged levels as soon as possible.

## Next steps

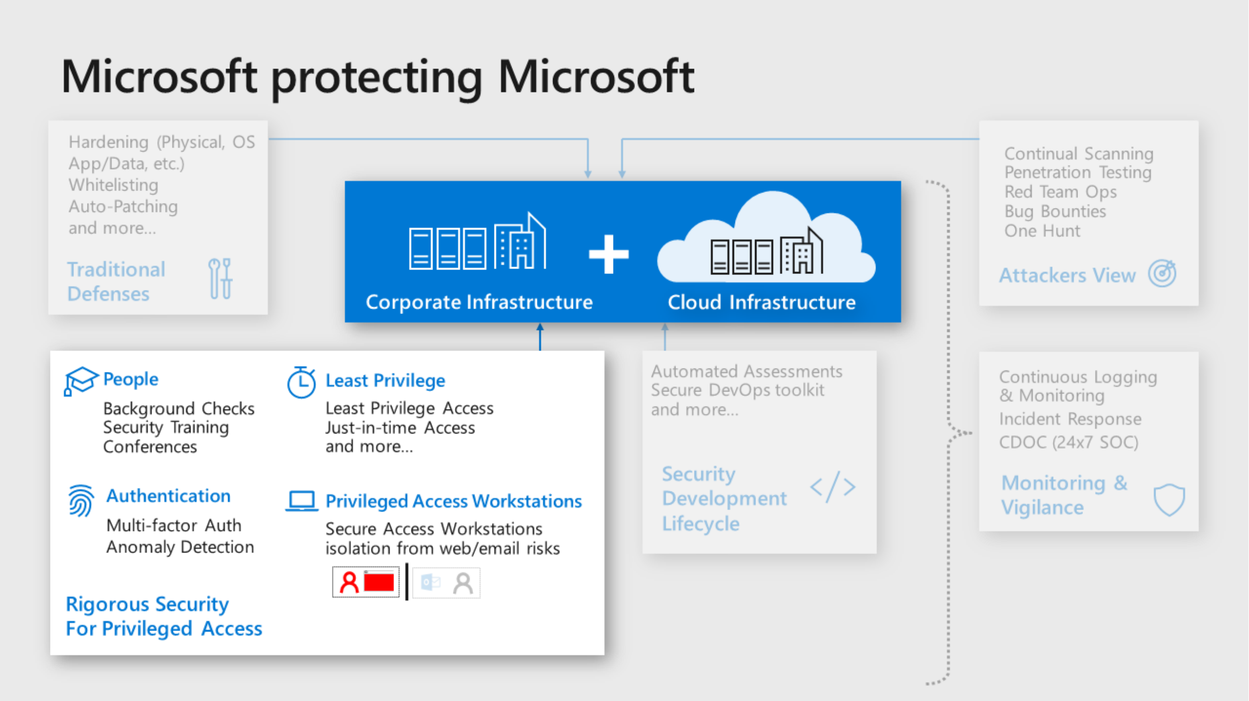
- Securing privileged access overview
- Privileged access strategy
- Measuring success
- Security levels
- Privileged access accounts
- Intermediaries
- Interfaces
- Privileged access devices
- Enterprise access model

# Administration

Article • 01/29/2024

Administration is the practice of monitoring, maintaining, and operating Information Technology (IT) systems to meet service levels that the business requires. Administration introduces some of the highest impact security risks because performing these tasks requires privileged access to a very broad set of these systems and applications. Attackers know that gaining access to an account with administrative privileges can get them access to most or all of the data they would target, making the security of administration one of the most critical security areas.

As an example, Microsoft makes significant investments in protection and training of administrators for our cloud systems and IT systems:



Microsoft protecting Microsoft

Hardening (Physical, OS App/Data, etc.)
Whitelisting
Auto-Patching
and more...
Traditional Defenses

Corporate Infrastructure + Cloud Infrastructure

Continual Scanning
Penetration Testing
Red Team Ops
Bug Bounties
One Hunt
Attackers View

People
Background Checks
Security Training
Conferences

Least Privilege
Least Privilege Access
Just-in-time Access
and more...

Authentication
Multi-factor Auth
Anomaly Detection

Privileged Access Workstations
Secure Access Workstations
isolation from web/email risks

Rigorous Security For Privileged Access

Automated Assessments
Secure DevOps toolkit
and more...
Security Development Lifecycle

Continuous Logging & Monitoring
Incident Response
CDOC (24x7 SOC)
Monitoring & Vigilance

Microsoft's recommended core strategy for administrative privileges is to use the available controls to reduce risk

**Reduce risk exposure (scope and time) –** The principle of least privilege is best accomplished with modern controls that provide privileges on demand. This help to limit risk by limiting administrative privileges exposure by:

- **Scope** – *Just Enough Access (JEA)* provides only the required privileges for the administrative operation required (vs. having direct and immediate privileges to many or all systems at a time, which is almost never required).
- **Time** – *Just in Time (JIT)* approaches provided the required privileged as they are needed.

- **Mitigate the remaining risks** – Use a combination of preventive and detective controls to reduce risks such as isolating administrator accounts from the most common risks phishing and general web browsing, simplifying and optimizing their workflow, increasing assurance of authentication decisions, and identifying anomalies from normal baseline behavior that can be blocked or investigated.

Microsoft has captured and documented best practices for protecting administrative accounts and published prioritized roadmaps for protecting privileged access that can be used as references for prioritizing mitigations for accounts with privileged access.

- Securing Privileged Access (SPA) roadmap for administrators of on premises Active Directory ↗
- Guidance for securing administrators of Microsoft Entra ID ↗

# Minimize number of critical impact admins

Grant the fewest number of accounts to privileges that can have a critical business impact

Each admin account represents potential attack surface that an attacker can target, so minimizing the number of accounts with that privilege helps limit the overall organizational risk. Experience has taught us that membership of these privileged groups grows naturally over time as people change roles if membership not actively limited and managed.

We recommend an approach that reduces this attack surface risk while ensuring business continuity in case something happens to an administrator:

- Assign at least two accounts to the privileged group for business continuity
- When two or more accounts are required, provide justification for each member including the original two
- Regularly review membership & justification for each group member

# Managed accounts for admins

Ensure all critical impact admins in are managed by enterprise directory to follow organizational policy enforcement.

Consumer accounts such as Microsoft accounts like @Hotmail.com, @live.com, @outlook.com, don't offer sufficient security visibility and control to ensure the organization’s policies and any regulatory requirements are being followed. Because Azure deployments often start small and informally before growing into enterprise-managed tenants, some consumer accounts remain as administrative accounts long afterward for example, original Azure project managers, creating blind spots, and potential risks.

## Separate accounts for admins

Ensure all critical impact admins have a separate account for administrative tasks (vs the account they use for email, web browsing, and other productivity tasks).

Phishing and web browser attacks represent the most common attack vectors to compromise accounts, including administrative accounts.

Create a separate administrative account for all users that have a role requiring critical privileges. For these administrative accounts, block productivity tools like Office 365 email (remove license). If possible, block arbitrary web browsing (with proxy and/or application controls) while allowing exceptions for browsing to the Azure portal and other sites required for administrative tasks.

## No standing access / Just in Time privileges

Avoid providing permanent “standing” access for any critical impact accounts

Permanent privileges increase business risk by increasing the time an attacker can use the account to do damage. Temporary privileges force attackers targeting an account to either work within the limited times the admin is already using the account or to initiate privilege elevation (which increases their chance of being detected and removed from the environment).

Grant privileges required only as required using one of these methods:

- **Just in Time -** Enable Microsoft Entra Privileged Identity Management (PIM) or a third party solution to require following an approval workflow to obtain privileges for critical impact accounts
- **Break glass –** For rarely used accounts, follow an emergency access process to gain access to the accounts. This is preferred for privileges that have little need for regular operational usage like members of global admin accounts.

## Emergency access or ‘Break Glass’ accounts

Ensure you have a mechanism for obtaining administrative access in case of an emergency

While rare, sometimes extreme circumstances arise where all normal means of administrative access are unavailable.

We recommend following the instructions at Managing emergency access administrative accounts in Microsoft Entra ID and ensure that security operations monitor these accounts carefully.

## Admin workstation security

Ensure critical impact admins use a workstation with elevated security protections and monitoring

Attack vectors that use browsing and email like phishing are cheap and common. Isolating critical impact admins from these risks will significantly lower your risk of a major incident where one of these accounts is compromised and used to materially damage your business or mission.

Choose level of admin workstation security based on the options available at https://aka.ms/securedworkstation

- **Highly Secure Productivity Device (Enhanced Security Workstation or Specialized Workstation)**
  You can start this security journey for critical impact admins by providing them with a higher security workstation that still allows for general browsing and productivity tasks. Using this as an interim step helps ease the transition to fully isolated workstations for both the critical impact admins as well as the IT staff supporting these users and their workstations.

- **Privileged Access Workstation (Specialized Workstation or Secured Workstation)**
  These configurations represent the ideal security state for critical impact admins as they heavily restrict access to phishing, browser, and productivity application attack vectors. These workstations don’t allow general internet browsing, only allow browser access to Azure portal and other administrative sites.

## Critical impact admin dependencies – Account/Workstation

Carefully choose the on-premises security dependencies for critical impact accounts and their workstations

To contain the risk from a major incident on-premises spilling over to become a major compromise of cloud assets, you must eliminate or minimize the means of control that on premises resources have to critical impact accounts in the cloud. As an example, attackers who compromise the on premises Active Directory can access and compromise cloud-based assets that rely on those accounts like resources in Azure, Amazon Web Services (AWS), ServiceNow, and so on. Attackers can also use workstations joined to those on premises domains to gain access to accounts and services managed from them.

Choose the level of isolation from on premises means of control also known as security dependencies for critical impact accounts

- **User Accounts** – Choose where to host the critical impact accounts
    - Native Microsoft Entra accounts -*Create Native Microsoft Entra accounts that are not synchronized with on-premises active directory
    - Synchronize from on-premises Active Directory (Not Recommended)- Leverage existing accounts hosted in the on premises active directory.
- **Workstations** – Choose how you will manage and secure the workstations used by critical admin accounts:
    - Native Cloud Management & Security (Recommended) - Join workstations to Microsoft Entra ID & Manage/Patch them with Intune or other cloud services. Protect and Monitor with Windows Microsoft Defender ATP or another cloud service not managed by on premises based accounts.
    - Manage with Existing Systems - Join existing AD domain & leverage existing management/security.

## Passwordless Or multi-factor authentication for admins

Require all critical impact admins to use passwordless authentication or multi-factor authentication (MFA).

Attack methods have evolved to the point where passwords alone cannot reliably protect an account. This is well documented in a Microsoft Ignite Session .

Administrative accounts and all critical accounts should use one of the following methods of authentication. These capabilities are listed in preference order by highest cost/difficulty to attack (strongest/preferred options) to lowest cost/difficult to attack:

- **Passwordless (such as Windows Hello)** https://aka.ms/HelloForBusiness

- **Passwordless (Authenticator App)** </azure/active-directory/authentication/howto-authentication-phone-sign-in>

- **Multifactor Authentication** </azure/active-directory/authentication/howto-mfa-userstates>

Note that SMS Text Message based MFA has become very inexpensive for attackers to bypass, so we recommend you avoid relying on it. This option is still stronger than passwords alone, but is much weaker than other MFA options

# Enforce conditional access for admins - Zero Trust

Authentication for all admins and other critical impact accounts should include measurement and enforcement of key security attributes to support a Zero Trust strategy.

Attackers compromising Azure Admin accounts can cause significant harm. Conditional Access can significantly reduce that risk by enforcing security hygiene before allowing access to Azure management.

Configure Conditional Access policy for Azure management that meets your organization's risk appetite and operational needs.

- Require Multifactor Authentication and/or connection from designated work network

- Require Device **integrity with Microsoft Defender ATP** (Strong Assurance)

# Avoid granular and custom permissions

Avoid permissions that specifically reference individual resources or users

Specific permissions create unneeded complexity and confusion as they don't carry the intention to new similar resources. This then accumulates into a complex legacy configuration that is difficult to maintain or change without fear of "breaking something" – negatively impacting both security and solution agility.

Instead of assigning specific resource-specific permissions, use either

- Management Groups for enterprise-wide permissions
- Resource groups for permissions within subscriptions

Instead of granting permissions to specific users, assign access to groups in Microsoft Entra ID. If there isn't an appropriate group, work with the identity team to create one. This allows you to add and remove group members externally to Azure and ensure permissions are current, while also allowing the group to be used for other purposes such as mailing lists.

## Use built-in roles

Use built-in roles for assigning permissions where possible.

Customization leads to complexity that increases confusion and makes automation more complex, challenging, and fragile. These factors all negatively impact security

We recommend that you evaluate the built-in roles designed to cover most normal scenarios. Custom roles are a powerful and sometimes useful capability, but they should be reserved for cases when built in roles won't work.

## Establish lifecycle management for critical impact accounts

Ensure you have a process for disabling or deleting administrative accounts when admin personnel leave the organization (or leave administrative positions)

See Manage user and guest user access with access reviews for more details.

## Attack simulation for critical impact accounts

Regularly simulate attacks against administrative users with current attack techniques to educate and empower them.

People are a critical part of your defense, especially your personnel with access to critical impact accounts. Ensuring these users (and ideally all users) have the knowledge and skills to avoid and resist attacks will reduce your overall organizational risk.

You can use Office 365 Attack Simulation capabilities or any number of third party offerings.

# Next steps

For additional security guidance from Microsoft, see Microsoft security documentation.

# Legacy privileged access guidance

Article • 01/29/2024

ⓘ **Important**

This guidance has been replaced with updated **secure workstation** guidance that is part of a complete solution for **securing privileged access**.

This documentation is being retained online for archival and reference purposes only. Microsoft strongly recommends following the new guidance for a solution that is more secure and easier to deploy and support.

## Legacy guidance

Privileged Access Workstations (PAWs) provide a dedicated operating system for sensitive tasks that is protected from Internet attacks and threat vectors. Separating these sensitive tasks and accounts from the daily use workstations and devices provides strong protection from phishing attacks, application and OS vulnerabilities, various impersonation attacks, and credential theft attacks such as keystroke logging, Pass-the-Hash, and Pass-The-Ticket.

## What is a Privileged Access Workstation?

In simplest terms, a PAW is a hardened and locked down workstation designed to provide high security assurances for sensitive accounts and tasks. PAWs are recommended for administration of identity systems, cloud services, private cloud fabric, and sensitive business functions.

ⓘ **Note**

The PAW architecture doesn't require a 1:1 mapping of accounts to workstations, though this is a common configuration. PAW creates a trusted workstation environment that can be used by one or more accounts.

In order to provide the greatest security, PAWs should always run the most up-to-date and secure operating system available: Microsoft strongly recommends Windows 11 Enterprise, which includes several other security features not available in other editions (in particular, Credential Guard and Device Guard).

ⓘ **Note**

Organizations without access to Windows 11 Enterprise can use Windows 11 Pro, which includes many of the critical foundational technologies for PAWs, including Trusted Boot, BitLocker, and Remote Desktop. Education customers can use Windows 11 Education.

Windows 11 Home should not be used for a PAW.

The PAW security controls are focused on mitigating high impact and high probability risks of compromise. These include mitigating attacks on the environment and risks that can decrease the effectiveness of PAW controls over time:

- **Internet attacks** - Most attacks originate directly or indirectly from internet sources and use the internet for exfiltration and command and control (C2). Isolating the PAW from the open internet is a key element to ensuring the PAW isn't compromised.
- **Usability risk** - If a PAW is too difficult to use for daily tasks, administrators are motivated to create workarounds to make their jobs easier. Frequently, these workarounds open the administrative workstation and accounts to significant security risks, so it's critical to involve and empower the PAW users to mitigate these usability issues securely. This can be accomplished by listening to their feedback, installing tools and scripts required to perform their jobs, and ensuring all administrative personnel are aware of why they need to use a PAW, what a PAW is, and how to use it correctly and successfully.
- **Environment risks** - Because many other computers and accounts in the environment are exposed to internet risk directly or indirectly, a PAW must be protected against attacks from compromised assets in the production environment. This requires minimizing the use of management tools and accounts that have access to the PAWs to secure and monitor these specialized workstations.
- **Supply chain tampering** - While it's impossible to remove all possible risks of tampering in the supply chain for hardware and software, taking a few key actions can mitigate critical attack vectors that are readily available to attackers. This includes validating the integrity of all installation media and using a trusted and reputable supplier for hardware and software.
- **Physical attacks** - Because PAWs can be physically mobile and used outside of physically secure facilities, they must be protected against attacks that apply unauthorized physical access to the computer.

ⓘ Important

A PAW will not protect an environment from an adversary that has already gained administrative access over an Active Directory Forest. Because many existing implementations of Active Directory Domain Services have been operating for years at risk of credential theft, organizations should assume breach and consider the possibility that they might have an undetected compromise of domain or enterprise administrator credentials. An organization that suspects domain compromise should consider the use of professional incident response services.

For more information on response and recovery guidance, see the "Respond to suspicious activity" and "Recover from a breach" sections of **Mitigating Pass-the-Hash and Other Credential Theft**, version 2.

## Legacy PAW hardware profiles

Administrative personnel are standard users too - they need a PAW and a standard user workstation to check email, browse the web, and access corporate line-of-business applications. Ensuring that administrators can remain both productive and secure is essential to the success of any PAW deployment. A secure solution that dramatically limits productivity will be abandoned by the users in favor of one that enhances productivity (even if it's done in an insecure manner).

In order to balance the need for security with the need for productivity, Microsoft recommends using one of these PAW hardware profiles:

- **Dedicated hardware** - Separate dedicated devices for user tasks vs. administrative tasks.
- **Simultaneous Use** - Single device that can run user tasks and administrative tasks concurrently by taking advantage of OS or presentation virtualization.

Organizations might use only one profile or both. There are no interoperability concerns between the hardware profiles, and organizations have the flexibility to match the hardware profile to the specific need and situation of a given administrator.

ⓘ Important

It is critical that, in all these scenarios, administrative personnel are issued a standard user account that is separate from designated administrative account(s).

The administrative account(s) should only be used on the PAW administrative operating system.

This table summarizes the relative advantages and disadvantages of each hardware profile from the perspective of operational ease-of-use and productivity and security. Both hardware approaches provide strong security for administrative accounts against credential theft and reuse.

Expand table

| Scenario | Advantages | Disadvantages |
|---|---|---|
| Dedicated hardware | - Strong signal for sensitivity of tasks<br>- Strongest security separation | - Extra desk space<br>- Extra weight (for remote work)<br>- Hardware Cost |
| Simultaneous use | - Lower hardware cost<br>- Single device experience | - Sharing single keyboard/mouse creates risk of inadvertent errors/risks |

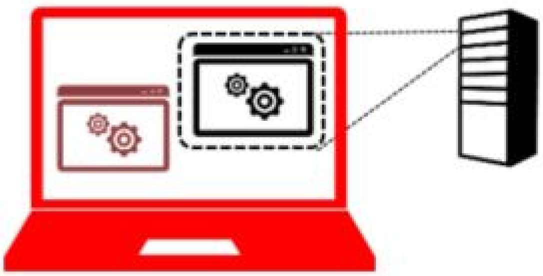
This guidance contains the detailed instructions for the PAW configuration for the dedicated hardware approach. If you have requirements for the simultaneous use hardware profiles, you can adapt the instructions based on this guidance yourself or hire a professional services organization like Microsoft to assist with it.

## Dedicated hardware

In this scenario, a PAW is used for administration that is separate from the PC that is used for daily activities like email, document editing, and development work. All administrative tools and applications are installed on the PAW and all productivity applications are installed on the standard user workstation. The step-by-step instructions in this guidance are based on this hardware profile.

## Simultaneous use - Adding RemoteApp, RDP, or a VDI

In this simultaneous use scenario, a single PC is used for both administration tasks and daily activities like email, document editing and development work. In this configuration, the user operating systems are deployed and managed centrally (on the cloud or in your datacenter), but aren't available while disconnected.



The physical hardware runs a single PAW operating system locally for administrative tasks and contacts a Microsoft or third party remote desktop service for user applications such as email, document editing, and line-of-business applications.

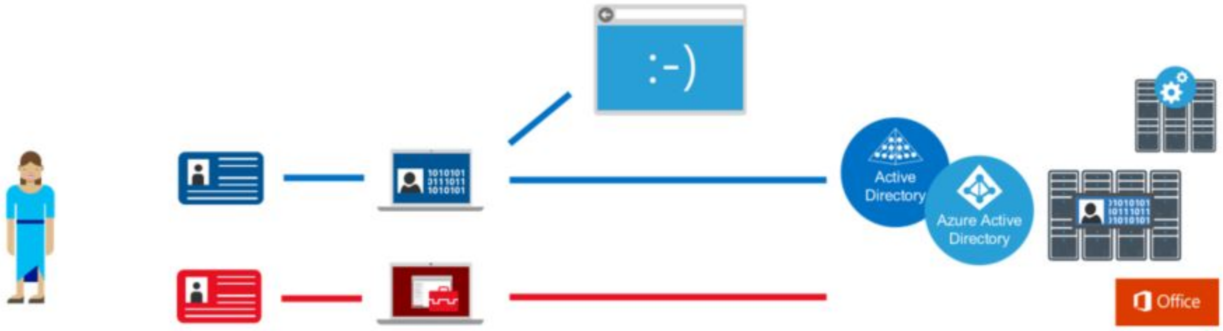
In this configuration, daily work that doesn't require administrative privileges is done in the Remote OS(es) and applications, which aren't subject to restrictions applied to the PAW host. All administrative work is done on the Admin OS.

To configure this, follow the instructions in this guidance for the PAW host, allow network connectivity to the Remote Desktop services, and then add shortcuts to the PAW user's desktop to access the applications. The remote desktop services could be hosted in many ways including:

- An existing Remote Desktop or VDI service like Azure Virtual Desktop, Microsoft Dev Box, or Windows 365.
- A new service you install on-premises or in the cloud
- Azure RemoteApp using preconfigured templates or your own installation images

## Architecture overview

The following diagram depicts a separate "channel" for administration (a highly sensitive task) that is created by maintaining separate dedicated administrative accounts and workstations.



This architectural approach builds on the protections found in the Windows 11 Credential Guard and Device Guard features and goes beyond those protections for sensitive accounts and tasks.

This methodology is appropriate for accounts with access to high value assets:

- **Administrative Privileges** - PAWs provide increased security for high impact IT administrative roles and tasks. This architecture can be applied to administration of many types of systems including Active Directory Domains and Forests, Microsoft Entra ID tenants, Microsoft 365 tenants, Process Control Networks (PCN), Supervisory Control and Data Acquisition (SCADA) systems, Automated Teller Machines (ATMs), and Point of Sale (PoS) devices.
- **High Sensitivity Information workers** - The approach used in a PAW can also provide protection for highly sensitive information worker tasks and personnel such as those involving preannouncement merger and acquisition activity, prerelease financial reports, organizational social media presence, executive communications, unpatented trade secrets, sensitive research, or other proprietary or sensitive data. This guidance doesn't discuss the configuration of these information worker scenarios in depth or include this scenario in the technical instructions.

This document describes why this practice is recommended for protecting high impact privileged accounts, what these PAW solutions look like for protecting administrative privileges, and how to quickly deploy a PAW solution for domain and cloud services administration.

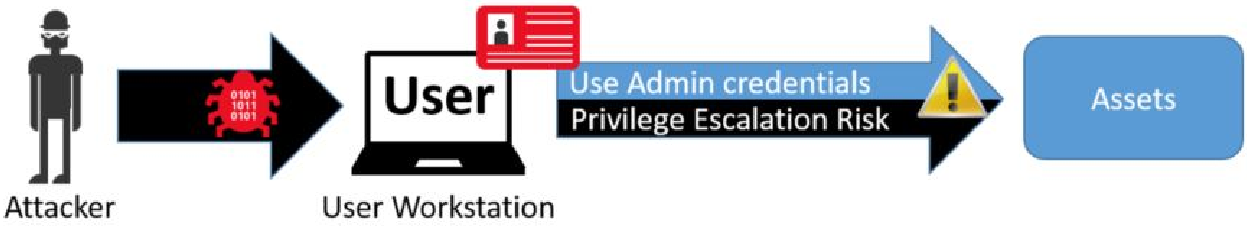
This document provides detailed guidance for implementing several PAW configurations and includes detailed implementation instructions to get you started on protecting common high impact accounts:

- Phase 1 - Immediate Deployment for Active Directory Administrators this provides a PAW quickly that can protect on premises domain and forest administration roles
- Phase 2 - Extend PAW to all administrators this enables protection for administrators of cloud services like Microsoft 365 and Azure, enterprise servers, enterprise applications, and workstations
- Phase 3 - Advanced PAW security this discusses more protections and considerations for PAW security

## Why dedicated workstations?

The current threat environment for organizations is rife with sophisticated phishing and other internet attacks that create continuous risk of security compromise for internet exposed accounts and workstations.

This threat environment requires organizations to adopt an "assume breach" security posture when designing protections for high value assets like administrative accounts and sensitive business assets. These high value assets need to be protected against both direct internet threats and attacks mounted from other workstations, servers, and devices in the environment.



This figure depicts risk to managed assets if an attacker gains control of a user workstation where sensitive credentials are used.

An attacker in control of an operating system has numerous ways in which to illicitly gain access to all activity on the workstation and impersonate the legitimate account. Various known and unknown attack techniques can be used to gain this level of access. The increasing volume and sophistication of cyberattacks have made it necessary to extend that separation concept to separate client operating systems for sensitive accounts. For more information on these types of attacks, visit the Pass The Hash web site for informative white papers, videos and more.

The PAW approach is an extension of the well-established recommended practice to use separate admin and user accounts for administrative personnel. This practice uses an individually assigned administrative account that is separate from the user's standard user account. PAW builds on that account separation practice by providing a trustworthy workstation for those sensitive accounts.

This PAW guidance is intended to help you implement this capability for protecting high value accounts such as high-privileged IT administrators and high sensitivity business accounts. The guidance helps you:

- Restrict exposure of credentials to only trusted hosts
- Provide a high-security workstation to administrators so they can easily perform administrative tasks.

Restricting the sensitive accounts to using only hardened PAWs is a straightforward protection for these accounts that is both highly usable for administrators and difficult for an adversary to defeat.

## Alternate approaches

This section contains information on how the security of alternate approaches compares to PAW and how to correctly integrate these approaches within a PAW architecture. all these approaches carry significant risks when implemented in isolation, but can add value to a PAW implementation in some scenarios.

## Credential Guard and Windows Hello for Business

Part of Windows 11, Credential Guard uses hardware and virtualization-based security to mitigate common credential theft attacks, such as Pass-the-Hash, by protecting the derived credentials. The private key for credentials used by Windows Hello for Business can be protected by Trusted Platform Module (TPM) hardware.

These are powerful mitigations, but workstations can still be vulnerable to certain attacks even if the credentials are protected by Credential Guard or Windows Hello for Business. Attacks can include abusing privileges and use of credentials directly from a compromised device, reusing previously stolen credentials prior to enabling Credential Guard and abuse of management tools and weak application configurations on the workstation.

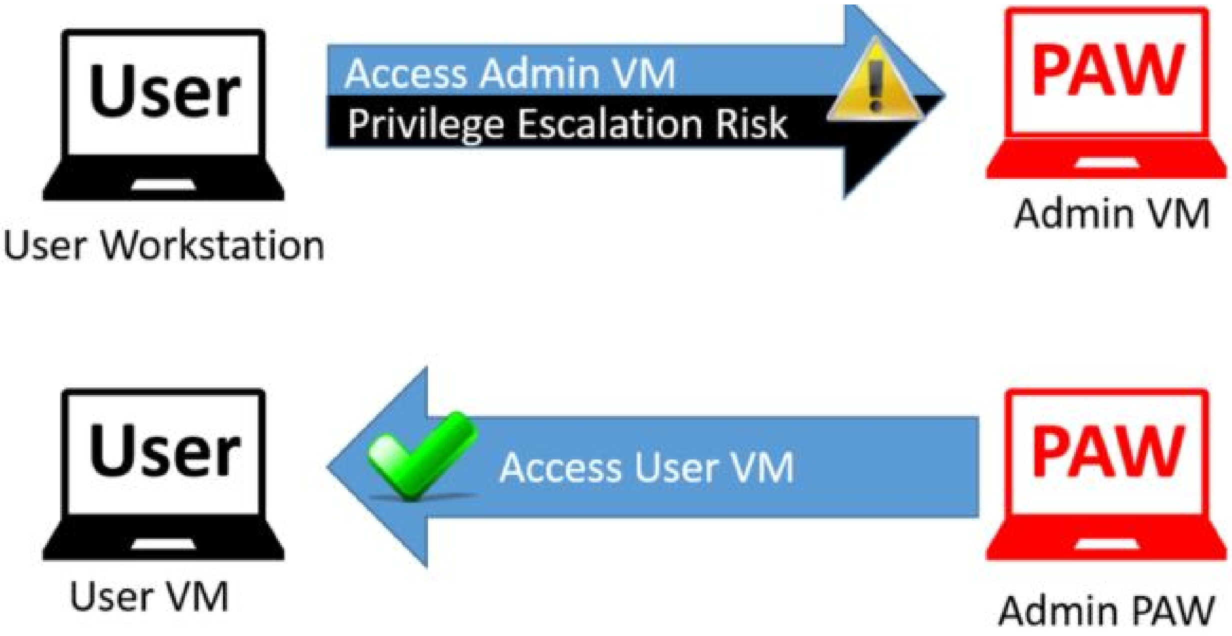
The PAW guidance in this section includes the use of many of these technologies for high sensitivity accounts and tasks.

## Administrative VM

An administrative virtual machine (Admin VM) is a dedicated operating system for administrative tasks hosted on a standard user desktop. While this approach is similar to PAW in providing a dedicated OS for administrative tasks, it has a fatal flaw in that the administrative VM is dependent on the standard user desktop for its security.

The following diagram depicts the ability of attackers to follow the control chain to the target object of interest with an Admin VM on a User Workstation and that it's difficult to create a path on the reverse configuration.

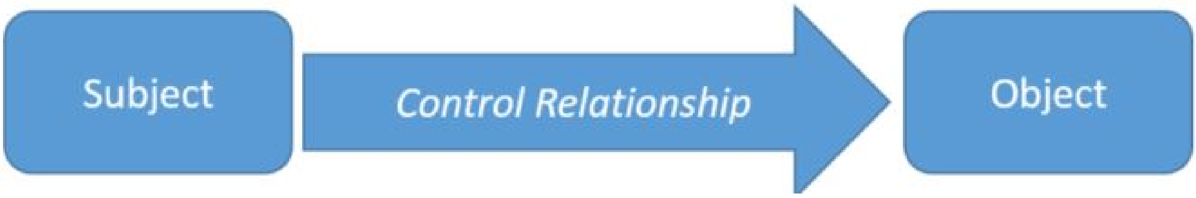
The PAW architecture doesn't allow for hosting an Admin VM on a User Workstation, but a User VM with a standard corporate image can be hosted on an Admin PAW to provide personnel with a single PC for all responsibilities.



## Jump server

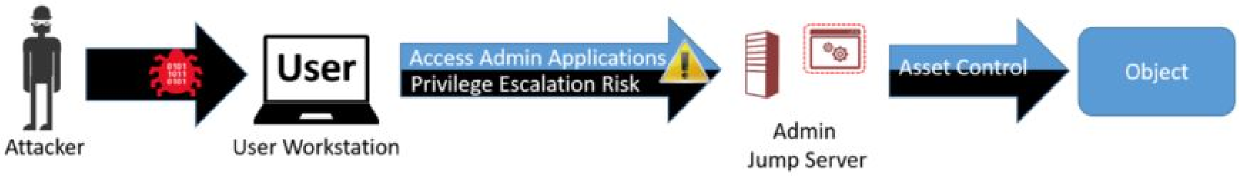
Administrative "Jump Server" architectures set up a small number administrative console servers and restrict personnel to using them for administrative tasks. This is typically based on remote desktop services, a 3rd-party presentation virtualization solution, or a Virtual Desktop Infrastructure (VDI) technology.

This approach is frequently proposed to mitigate risk to administration and does provide some security assurances, but the jump server approach by itself is vulnerable to certain attacks because it violates the clean source principle. The clean source principle requires all security dependencies to be as trustworthy as the object being secured.



This figure depicts a simple control relationship. Any subject in control of an object is a security dependency of that object. If an adversary can control a security dependency of a target object (subject), they can control that object.

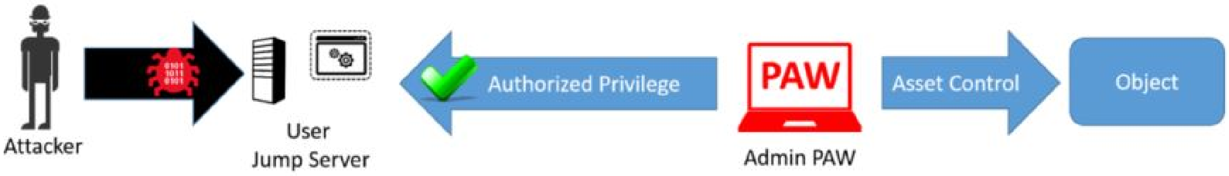
The administrative session on the jump server relies on the integrity of the local computer accessing it. If this computer is a user workstation subject to phishing attacks and other internet-based attack vectors, then the administrative session is also subject to those risks.



The previous figure depicts how attackers can follow an established control chain to the target object of interest.

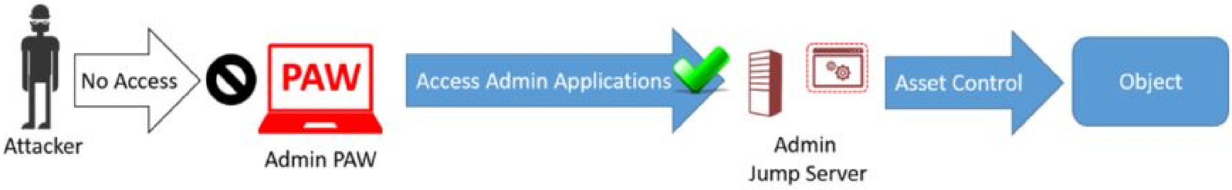
While some advanced security controls like Multifactor authentication can increase the difficulty of an attacker taking over this administrative session from the user workstation, no security feature can fully protect against technical attacks when an attacker has administrative access of the source computer (for example, injecting illicit commands into a legitimate session, hijacking legitimate processes, and so on.)

The default configuration in this PAW guidance installs administrative tools on the PAW, but a jump server architecture can also be added if necessary.



This figure shows how reversing the control relationship and accessing user apps from an admin workstation gives the attacker no path to the targeted object. The user jump server is still exposed to risk so appropriate protective controls, detective controls, and response processes should still be applied for that internet-facing computer.

This configuration requires administrators to follow operational practices closely to ensure that they don't accidentally enter administrator credentials into the user session on their desktop.



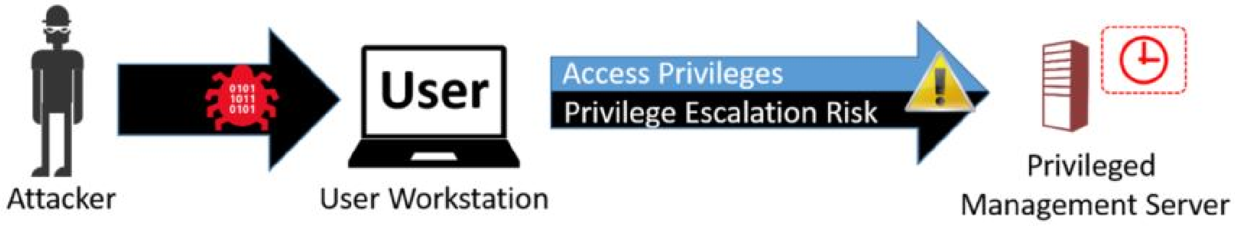
This figure shows how accessing an administrative jump server from a PAW adds no path for the attacker into the administrative assets. A jump server with a PAW allows in this case you to consolidate the number of locations for monitoring administrative activity and distributing administrative applications and tools. This adds some design complexity, but can simplify security monitoring and software updates if a large number of accounts and workstations are used in your PAW implementation. The jump server would need to be built and configured to similar security standards as the PAW.

## Privilege management solutions

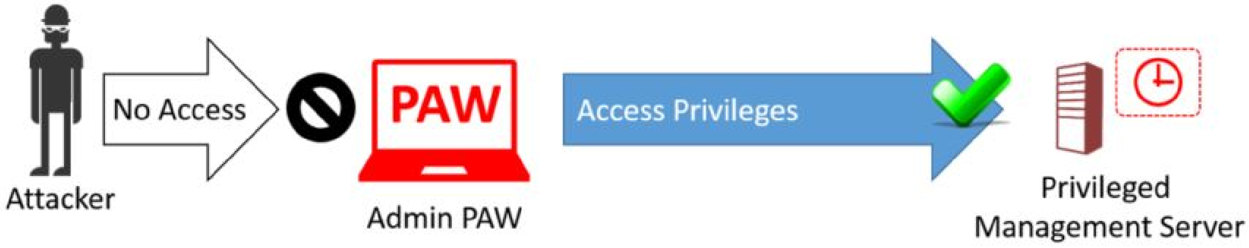
Privileged Management solutions are applications that provide temporary access to discrete privileges or privileged accounts on demand. Privilege management solutions are a valuable component of a complete strategy to secure privileged access and provide critically important visibility and accountability of administrative activity.

These solutions typically use a flexible workflow to grant access and many have other security features and capabilities like service account password management and integration with administrative jump servers. There are many solutions on the market that provide privilege management capabilities, one of which is Microsoft Identity Manager (MIM) privileged access management (PAM).

Microsoft recommends using a PAW to access privilege management solutions. Access to these solutions should be granted only to PAWs. Microsoft doesn't recommend using these solutions as a substitute for a PAW because accessing privileges using these solutions from a potentially compromised user desktop violates the clean source principle as depicted in the following diagram:



Providing a PAW to access these solutions enables you to gain the security benefits of both PAW and the privilege management solution, as depicted in this diagram:



ⓘ **Important**

These systems should be classified at the highest tier of the privilege they manage and be protected at or above that level of security. These are commonly configured to manage Tier 0 solutions and Tier 0 assets and should be classified at Tier 0.

For more information on deploying Microsoft Identity Manager (MIM) privileged access management (PAM), see https://aka.ms/mimpamdeploy

# PAW Scenarios

This section contains guidance on which scenarios this PAW guidance should be applied to. In all scenarios, administrators should be trained to only use PAWs for performing support of remote systems. To encourage successful and secure usage, all PAW users should be encouraged to provide feedback to improve the PAW experience, and this feedback should be reviewed carefully for integration with your PAW program.

In all scenarios, extra hardening in later phases and different hardware profiles in this guidance might be used to meet the usability or security requirements of the roles.

ⓘ Note

This guidance explicitly differentiates between requiring access to specific services on the internet (such as Azure and Microsoft 365 administrative portals) and the "Open Internet" of all hosts and services.

Expand table

| Scenarios | Use PAW? | Scope and Security Considerations |
|---|---|---|
| Active Directory Admins - Tier 0 | Yes | A PAW built with Phase 1 guidance is sufficient for this role.<br>- An administrative forest can be added to provide the strongest protection for this scenario. For more information on the ESAE administrative forest, see ESAE Scenarios for Continued Use<br>- A PAW can be used to managed multiple domains or multiple forests.<br>- If Domain Controllers are hosted on an Infrastructure as a Service (IaaS) or on-premises virtualization solution, you should prioritize implementing PAWs for the administrators of those solutions. |
| Admin of Azure IaaS and PaaS services - Tier 0 or Tier 1 (see Scope and Design Considerations) | Yes | A PAW built using the guidance provided in Phase 2 is sufficient for this role.<br>- PAWs should be used for at least the Global administrator and Subscription Billing administrator. You should also use PAWs for delegated administrators of critical or sensitive servers.<br>- PAWs should be used for managing the operating system and applications that provide Directory Synchronization and Identity Federation for cloud services such as Microsoft Entra Connect and Active Directory Federation Services (ADFS).<br>- The outbound network restrictions must allow connectivity only to authorized cloud services using the guidance in Phase |

| Scenarios | Use PAW? | Scope and Security Considerations |
|---|---|---|
| | | 2. No open internet access should be allowed from PAWs.<br>- Windows Defender Exploit Guard should be configured on the workstation **Note:** A subscription is considered to be Tier 0 for a Forest if Domain Controllers or other Tier 0 hosts are in the subscription. A subscription is Tier 1 if no Tier 0 servers are hosted in Azure. |
| Admin Microsoft 365 Tenant<br>- Tier 1 | Yes | A PAW built using the guidance provided in Phase 2 is sufficient for this role.<br>- PAWs should be used for at least the Subscription Billing administrator, Global administrator, Exchange administrator, SharePoint administrator, and User management administrator roles. You should also strongly consider the use of PAWs for delegated administrators of highly critical or sensitive data.<br>- Windows Defender Exploit Guard should be configured on the workstation.<br>- The outbound network restrictions must allow connectivity only to Microsoft services using the guidance in Phase 2. No open internet access should be allowed from PAWs. |
| Other IaaS or PaaS cloud service admin<br>- Tier 0 or Tier 1 (see Scope and Design Considerations) | Yes | A PAW built using the guidance provided in Phase 2 is sufficient for this role.<br>- PAWs should be used for any role that has administrative rights over cloud hosted VMs including the ability to install agents, export hard disk files, or access storage where hard drives with operating systems, sensitive data, or business critical data is stored.<br>- The outbound network restrictions must allow connectivity only to Microsoft services using the guidance in Phase 2. No open internet access should be allowed from PAWs.<br>- Windows Defender Exploit Guard should be configured on the workstation. **Note:** A subscription is Tier 0 for a Forest if Domain Controllers or other Tier 0 hosts are in the subscription. A subscription is Tier 1 if no Tier 0 servers are hosted in Azure. |
| Virtualization Administrators<br>- Tier 0 or Tier 1 (see Scope and Design Considerations) | Yes | A PAW built using the guidance provided in Phase 2 is sufficient for this role.<br>- PAWs should be used for any role that has administrative rights over VMs including the ability to install agents, export virtual hard disk files, or access storage where hard drives with guest operating system information, sensitive data, or business critical data is stored. **Note:** A virtualization system and its admins are considered Tier 0 for a Forest if Domain Controllers or other Tier 0 hosts are in the subscription. A |

| Scenarios | Use PAW? | Scope and Security Considerations |
|---|---|---|
| | | subscription is Tier 1 if no Tier 0 servers are hosted in the virtualization system. |
| Server Maintenance Admins<br>- Tier 1 | Yes | A PAW built using the guidance provided in Phase 2 is sufficient for this role.<br>- A PAW should be used for administrators that update, patch, and troubleshoot enterprise servers and apps running Windows server, Linux, and other operating systems.<br>- Dedicated management tools might need to be added for PAWs to handle the larger scale of these admins. |
| User Workstation Admins<br>- Tier 2 | Yes | A PAW built using guidance provided in Phase 2 is sufficient for roles that have administrative rights on end-user devices (such as helpdesk and deskside support roles).<br>- Other applications might need to be installed on PAWs to enable ticket management and other support functions.<br>- Windows Defender Exploit Guard should be configured on the workstation.<br>Dedicated management tools might need to be added for PAWs to handle the larger scale of these admins. |
| SQL, SharePoint, or line-of-business (LOB) Admin<br>- Tier 1 | Yes | A PAW built with Phase 2 guidance is sufficient for this role.<br>- Other management tools might need to be installed on PAWs to allow administrators to manage applications without needing to connect to servers using Remote Desktop. |
| Users Managing Social Media Presence | Partially | A PAW built using the guidance provided in Phase 2 can be used as a starting point to provide security for these roles.<br>- Protect and manage social media accounts using Microsoft Entra ID for sharing, protecting, and tracking access to social media accounts.<br>For more information on this capability, read this blog post.<br>- The outbound network restrictions must allow connectivity to these services. This can be done by allowing open internet connections (much higher security risk that negates many PAW assurances) or by allowing only required DNS addresses for the service (might be challenging to obtain). |
| Standard Users | No | While many hardening steps can be used for standard users, PAW is designed to isolate accounts from the open internet access that most users require for job duties. |
| Guest VDI/Kiosk | No | While many hardening steps can be used for a kiosk system for guests, the PAW architecture is designed to provide higher security for high sensitivity accounts, not higher security for lower sensitivity accounts. |

| Scenarios | Use PAW? | Scope and Security Considerations |
|---|---|---|
| VIP User (Executive, Researcher, etc.) | Partially | A PAW built using guidance provided in Phase 2 can be used as a starting point to provide security for these roles.<br>- This scenario is similar to a standard user desktop, but typically has a smaller, simpler, and well-known application profile. This scenario typically requires discovering and protecting sensitive data, services, and applications.<br>- These roles typically require a high degree of security and high degree of usability, which require design changes to meet user preferences. |
| Industrial control systems (for example, SCADA, PCN, and DCS) | Partially | A PAW built using guidance provided in Phase 2 can be used as a starting point to provide security for these roles as most ICS consoles (including such common standards as SCADA and PCN) don't require browsing the open Internet and checking email.<br>- Applications used for controlling physical machinery would have to be integrated and tested for compatibility and protected appropriately. |
| Embedded Operating System | No | While many hardening steps from PAW can be used for embedded operating systems, a custom solution would need to be developed for hardening in this scenario. |

ⓘ Note

**Combination scenarios** some personnel might have administrative responsibilities that span multiple scenarios. In these cases, the key rules to keep in mind are that the Tier model rules must always be followed.

**Scaling the PAW Program** as your PAW program scales to encompass more admins and roles, you need to continue to ensure that you maintain adherence to the security standards and usability. This might require you to update your IT support structures or create new ones to resolve PAW specific challenges such as PAW onboarding process, incident management, configuration management, and gathering feedback to address usability challenges. One example might be that your organization decides to enable work-from-home scenarios for administrators, which would necessitate a shift from desktop PAWs to laptop PAWs - a shift which might necessitate additional security considerations. Another common example is to create or update training for new administrators - training which must now include content on the appropriate use of a PAW (including why it's important and what a PAW is and isn't). For more considerations which must be addressed as you scale your PAW program, see Phase 2 of the instructions.

This guidance contains the detailed instructions for the PAW configuration for the scenarios as noted previously. If you have requirements for the other scenarios, you can adapt the instructions based on this guidance yourself or hire a professional services organization like Microsoft to assist with it.

# PAW Phased implementation

Because the PAW must provide a secure and trusted source for administration, it's essential that the build process is secure and trusted. This section provides detailed instructions, which allow you to build your own PAW using general principles and concepts similar to those used by Microsoft.

The instructions are divided into three phases, which focus on putting the most critical mitigations in place quickly and then progressively increasing and expanding the usage of PAW for the enterprise.

- Phase 1 - Immediate Deployment for Active Directory Administrators
- Phase 2 - Extend PAW to all administrators
- Phase 3 - Advanced PAW security

It's important to note that the phases should always be performed in order even if they're planned and implemented as part of the same overall project.

## Phase 1: Immediate deployment for Active Directory administrators

Purpose: Provides a PAW quickly that can protect on-premises domain and forest administration roles.

Scope: Tier 0 Administrators including Enterprise Admins, Domain Admins (for all domains), and administrators of other authoritative identity systems.

Phase 1 focuses on the administrators who manage your on-premises Active Directory domain, which are critically important roles frequently targeted by attackers. These identity systems work effectively for protecting these admins whether your Active Directory Domain Controllers (DCs) are hosted in on-premises datacenters, on Azure Infrastructure as a Service (IaaS), or another IaaS provider.

During this phase, you create the secure administrative Active Directory organizational unit (OU) structure to host your privileged access workstation (PAW), and deploy the PAWs themselves. This structure also includes the group policies and groups required to support the PAW.

The infrastructure is based on the following OUs, Security Groups, and group policies:

- Organizational Units (OU)
  - Six new top-level OUs:
    - Admin
    - Groups
    - Tier 1 Servers
    - Workstations
    - User Accounts
    - Computer Quarantine.
- Groups
  - Six new security-enabled global groups:
    - Tier 0 Replication Maintenance
    - Tier 1 Server Maintenance
    - Service Desk Operators
    - Workstation Maintenance
    - PAW Users
    - PAW Maintenance.
- Group policy objects:
  - PAW Configuration - Computer
  - PAW Configuration - User
  - RestrictedAdmin Required - Computer
  - PAW Outbound Restrictions
  - Restrict Workstation Logon
  - Restrict Server Logon.

Phase 1 includes the following steps:

## Complete the Prerequisites

1. **Ensure that all administrators use separate, individual accounts for administration and end-user activities** (including email, Internet browsing, line-of-business applications, and other nonadministrative activities). Assigning an administrative account to each authorized person separate from their standard user account is fundamental to the PAW model, as only certain accounts are permitted to log on to the PAW itself.

   > ⓘ **Important**
   >
   > Each administrator should use his or her own account for administration. Do not share an administrative account.

2. **Minimize the number of Tier 0 privileged administrators**. Because each administrator must use a PAW, reducing the number of administrators reduces the number of PAWs required to support them and the associated costs. The lower count of administrators also results in lower exposure of these privileges and associated risks. While it's possible for administrators in one location to share a PAW, administrators in separate physical locations require separate PAWs.

3. **Acquire hardware from a trusted supplier that meets all technical requirements**. Microsoft recommends acquiring hardware that meets the technical requirements in the article Protect domain credentials with Credential Guard.

   > ⓘ **Note**
   >
   > PAW installed on hardware without these capabilities can provide significant protections, but advanced security features such as Credential Guard and Device Guard will not be available. Credential Guard and Device Guard are not required for Phase 1 deployment, but are strongly recommended as part of Phase 3 (advanced hardening).
   >
   > Ensure that the hardware used for the PAW is sourced from a manufacturer and supplier whose security practices are trusted by the organization. This is an application of the clean source principle to supply chain security.
   >
   > For more background on the importance of supply chain security, visit **this site** .

4. **Acquire and validate the required Windows 11 Enterprise Edition and application software**.

   - Windows 11 Enterprise Edition
   - Remote Server Administration Tools for Windows 11
   - Windows 11 Security Baselines

   > ⓘ **Note**
   >
   > Microsoft publishes MD5 hashes for all operating systems and applications on MSDN, but not all software vendors provide similar documentation. In those cases, other strategies will be required.

5. **Ensure you have WSUS server available on the intranet**. You need a WSUS server on the intranet to download and install updates for PAW. This WSUS server should be configured to automatically approve all security updates for Windows 11 or an

administrative personnel should have responsibility and accountability to rapidly approve software updates. For more information, see the "Automatically Approve Updates for Installation" section in the Approving Updates guidance.

## Move Tier 0 accounts to the Admin\Tier 0\Accounts OU

Move each account that is a member of the Domain Admin, Enterprise Admin, or Tier 0 equivalent groups (including nested membership) to this OU. If your organization has your own groups that are added to these groups, you should move these to the Admin\Tier 0\Groups OU.

## Add the appropriate members to the relevant groups

1. **PAW Users** - Add the Tier 0 administrators with Domain or Enterprise Admin groups that you identified in Step 1 of Phase 1.

2. **PAW Maintenance** - Add at least one account used for PAW maintenance and troubleshooting tasks. The PAW Maintenance Account(s) is used only rarely.

> ⓘ **Important**
>
> Do not add the same user account or group to both PAW Users and PAW Maintenance. The PAW security model is based partly on the assumption that the PAW user account has privileged rights on managed systems or over the PAW itself, but not both.
>
> - This is important for building good administrative practices and habits in Phase 1.
> - This is critically important for Phase 2 and beyond to prevent escalation of privilege through PAW as PAWs being to span Tiers.
>
> Ideally, no personnel are assigned to duties at multiple tiers to enforce the principle of segregation of duties, but Microsoft recognizes that many organizations have limited staff (or other organizational requirements) that don't allow for this full segregation. In these cases, the same personnel might be assigned to both roles, but should not use the same account for these functions.

## Create "PAW Configuration - Computer" group policy object (GPO)

In this section, you create a new "PAW Configuration - Computer" GPO, which provides specific protections for these PAWs and link it to the Tier 0 Devices OU ("Devices" under Tier 0\Admin).

> ⚠ Warning
>
> **Do not add these settings to the Default Domain Policy**. Doing so will potentially impact operations on your entire Active Directory environment. Only configure these settings in the newly-created GPOs described here, and only apply them to the PAW OU.

1. **PAW Maintenance Access** - this setting sets the membership of specific privileged groups on the PAWs to a specific set of users. Go to *Computer Configuration\Preferences\Control Panel Settings\Local Users* and Groups and complete the following steps:

   a. Click **New** and click **Local Group**

   b. Select the **Update** action, and select "Administrators (built-in)" (don't use the Browse button to select the domain group Administrators).

   c. Select the **Delete all member users** and **Delete all member groups** check boxes

   d. Add PAW Maintenance (pawmaint) and Administrator (again, don't use the Browse button to select Administrator).

   > ⓘ Important
   >
   > Do not add the PAW Users group to the membership list for the local Administrators group. To ensure that PAW Users cannot accidentally or deliberately modify the security settings of the PAW itself, they should not be members of the local Administrators groups.
   >
   > For more information on using Group Policy Preferences to modify group membership, please refer to the TechNet article **Configure a Local Group Item**.

2. **Restrict Local Group Membership** - this setting ensures that the membership of local admin groups on the workstation is always empty

   a. Go to Computer Configuration\Preferences\Control Panel Settings\Local Users and Groups and complete the following steps:

    i. Click **New** and click **Local Group**
    ii. Select the **Update** action, and select "Backup Operators (built-in)" (don't use the Browse button to select the domain group Backup Operators).
    iii. Select the **Delete all member users** and **Delete all member groups** check boxes.
    iv. Don't add any members to the group. Assigning an empty list causes group policy to automatically remove all members and ensure a blank membership list each time group policy is refreshed.

b. Complete the previous steps for the following groups:

    - Cryptographic Operators
    - Hyper-V Administrators
    - Network Configuration Operators
    - Power Users
    - Remote Desktop Users
    - Replicators

c. **PAW Logon Restrictions** - this setting limits the accounts that can log on to the PAW. complete the following steps to configure this setting:
    i. Go to Computer Configuration\Policies\Windows Settings\Security Settings\Local Policies\User Rights Assignment\Allow log on locally.
    ii. Select Define these policy settings and add "PAW Users" and Administrators (again, don't use the Browse button to select Administrators).

d. **Block Inbound Network Traffic** - This setting ensures that no unsolicited inbound network traffic is allowed to the PAW. Complete the following steps to configure this setting:
    i. Go to Computer Configuration\Policies\Windows Settings\Security Settings\Windows Firewall with Advanced Security\Windows Firewall with Advanced Security and complete the following steps:
        i. Right click on Windows Firewall with Advanced Security and select **Import policy**.
        ii. Click **Yes** to accept that this overwrites any existing firewall policies.
        iii. Browse to PAWFirewall.wfw and select **Open**.
        iv. Click **OK**.

> ⓘ **Note**
>
> You can add addresses or subnets which must reach the PAW with unsolicited traffic at this point (e.g. security scanning or management software. The settings in the WFW file will enable the firewall in "Block -

> Default" mode for all firewall profiles, turn off rule merging and enable logging of both dropped and successful packets. These settings will block unsolicited traffic while still allowing bidirectional communication on connections initiated from the PAW, prevent users with local administrative access from creating local firewall rules that would override the GPO settings and ensure that traffic in and out of the PAW is logged. **Opening up this firewall will expand the attack surface for the PAW and increase security risk. Before adding any addresses, consult the Managing and Operating PAW section in this guidance**.

e. **Configure Windows Update for WSUS** - complete the following steps to change the settings to configure Windows Update for the PAWs:

   i. Go to Computer Configuration\Policies\Administrative Templates\Windows Components\Windows Updates and complete the following steps:

      i. Enable the **Configure Automatic Updates policy**.

      ii. Select option **4 - Auto download and schedule the install**.

      iii. Change the option **Scheduled install day** to **0 - Every Day** and the option **Scheduled install time** to your organizational preference.

      iv. Enable option **Specify intranet Microsoft update service location** policy.

f. Link the "PAW Configuration - Computer" GPO as follows:

⛶ Expand table

| Policy | Link Location |
|---|---|
| PAW Configuration - Computer | Admin\Tier 0\Devices |

## Create "PAW Configuration - User" group policy object (GPO)

In this section, you create a new "PAW Configuration - User" GPO that provides specific protections for these PAWs and link to the Tier 0 Accounts OU ("Accounts" under Tier 0\Admin).

> ⚠ Warning
>
> Do not add these settings to the Default Domain Policy

1. **Block internet browsing** - To deter inadvertent internet browsing, this sets a proxy address of a loopback address (127.0.0.1).

a. Go to User Configuration\Preferences\Windows Settings\Registry. Right-click Registry, select **New** > **Registry Item** and configure the following settings:

   i. Action: Replace

   ii. Hive: HKEY_CURRENT_USER

   iii. Key Path: Software\Microsoft\Windows\CurrentVersion\Internet Settings

   iv. Value name: ProxyEnable

   > ⊗ **Caution**
   >
   > Do not select the Default box to the left of Value name.

   v. Value type: REG_DWORD

   vi. Value data: 1

      i. Click the Common tab and select **Remove this item when it is no longer applied**.
      ii. On the Common tab, select **Item level targeting** and click **Targeting**.
      iii. Click **New Item** and select **Security group**.
      iv. Select the "..." button and browse for the PAW Users group.
      v. Click **New Item** and select **Security group**.
      vi. Select the "..." button and browse for the **Cloud Services Admins** group.
      vii. Click on the **Cloud Services Admins** item and click **Item Options**.
      viii. Select **Is not**.
      ix. Click **OK** on the targeting window.

   vii. Click **OK** to complete the ProxyServer group policy setting

b. Go to User Configuration\Preferences\Windows Settings\Registry. Right-click Registry, select **New** > **Registry Item** and configure the following settings:

   - Action: Replace
   - Hive: HKEY_CURRENT_USER
   - Key Path: Software\Microsoft\Windows\CurrentVersion\Internet Settings

     - Value name: ProxyServer

     > ⊗ **Caution**
     >
     > Do not select the Default box to the left of Value name.

        - Value type: REG_SZ
        - Value data: 127.0.0.1:80
            1. Click the **Common** tab and select **Remove this item when it is no longer applied**.
            2. On the Common tab, select **Item level targeting** and click **Targeting**.
            3. Click **New Item** and select security group.
            4. Select the "..." button and add the PAW Users group.
            5. Click **New Item** and select security group.
            6. Select the "..." button and browse for the **Cloud Services Admins** group.
            7. Click on the **Cloud Services Admins** item and click **Item Options**.
            8. Select **Is not**.
            9. Click **OK** on the targeting window.

    c. Click **OK** to complete the ProxyServer group policy setting,

2. Go to User Configuration\Policies\Administrative Templates\Windows Components\Internet Explorer, and enable the following options. These settings prevent the administrators from manually overriding the proxy settings.
    a. Enable the **Disable changing Automatic Configuration** settings.
    b. Enable the **Prevent changing proxy settings**.

## Restrict Administrators from logging on to lower tier hosts

In this section, we configure group policies to prevent privileged administrative accounts from logging on to lower tier hosts.

1. Create the new **Restrict Workstation Logon** GPO - this setting restricts Tier 0 and Tier 1 administrator accounts from logging on to standard workstations. This GPO should be linked to the "Workstations" top-level OU and have the following settings:

    - In Computer Configuration\Policies\Windows Settings\Security Settings\Local Policies\User Rights Assignment\Deny log on as a batch job, select **Define these policy settings** and add the Tier 0 and Tier 1 groups including:
        - Built-in Tier 0 Groups
            - Enterprise Admins
            - Domain Admins
            - Schema Admins
            - BUILTIN\Administrators
            - Account Operators
            - Backup Operators

    - Print Operators
    - Server Operators
    - Domain Controllers
    - Read-Only Domain Controllers
    - Group Policy Creators Owners
    - Cryptographic Operators
  - Other Delegated Groups including any custom created groups with effective Tier 0 access.
  - Tier 1 Admins

- In Computer Configuration\Policies\Windows Settings\Security Settings\Local Policies\User Rights Assignment\Deny log on as a service, select **Define these policy settings** and add the Tier 0 and Tier 1 groups:
  - Built-in Tier 0 Groups
    - Enterprise Admins
    - Domain Admins
    - Schema Admins
    - BUILTIN\Administrators
    - Account Operators
    - Backup Operators
    - Print Operators
    - Server Operators
    - Domain Controllers
    - Read-Only Domain Controllers
    - Group Policy Creators Owners
    - Cryptographic Operators
  - Other Delegated Groups including any custom created groups with effective Tier 0 access.
  - Tier 1 Admins

2. Create the new **Restrict Server Logon** GPO - this setting restricts Tier 0 administrator accounts from logging on to Tier 1 servers. This GPO should be linked to the "Tier 1 Servers" top-level OU and have the following settings:

   - In Computer Configuration\Policies\Windows Settings\Security Settings\Local Policies\User Rights Assignment\Deny log on as a batch job, select **Define these policy settings** and add the Tier 0 groups:
     - Built-in Tier 0 Groups
       - Enterprise Admins
       - Domain Admins
       - Schema Admins
       - BUILTIN\Administrators

        - Account Operators
        - Backup Operators
        - Print Operators
        - Server Operators
        - Domain Controllers
        - Read-Only Domain Controllers
        - Group Policy Creators Owners
        - Cryptographic Operators
    - Other Delegated Groups including any custom created groups with effective Tier 0 access.

- In Computer Configuration\Policies\Windows Settings\Security Settings\Local Policies\User Rights Assignment\Deny log on as a service, select **Define these policy settings** and add the Tier 0 groups:
    - Built-in Tier 0 Groups
        - Enterprise Admins
        - Domain Admins
        - Schema Admins
        - BUILTIN\Administrators
        - Account Operators
        - Backup Operators
        - Print Operators
        - Server Operators
        - Domain Controllers
        - Read-Only Domain Controllers
        - Group Policy Creators Owners
        - Cryptographic Operators
    - Other Delegated Groups including any custom created groups with effective Tier 0 access.

- In Computer Configuration\Policies\Windows Settings\Security Settings\Local Policies\User Rights Assignment\Deny log on locally, select **Define these policy settings** and add the Tier 0 groups:
    - Built-in Tier 0 Groups
        - Enterprise Admins
        - Domain Admins
        - Schema Admins
        - BUILTIN\Administrators
        - Account Operators
        - Backup Operators
        - Print Operators

    - Server Operators
    - Domain Controllers
    - Read-Only Domain Controllers
    - Group Policy Creators Owners
    - Cryptographic Operators
  - Other Delegated Groups including any custom created groups with effective Tier 0 access.

## Deploy your PAW(s)

> ⓘ **Important**
>
> Ensure that the PAW is disconnected from the network during the operating system build process.

1. Install Windows 11 using the clean source installation media that you obtained earlier.

    > ⓘ **Note**
    >
    > You might use Microsoft Deployment Toolkit (MDT) or another automated image deployment system to automate PAW deployment, but you must ensure the build process is as trustworthy as the PAW. Adversaries specifically seek out corporate images and deployment systems (including ISOs, deployment packages, etc.) as a persistence mechanism so preexisting deployment systems or images should not be used.
    >
    > If you automate deployment of the PAW, you must:
    >
    > - Build the system using validated and authentic installation media.
    > - Ensure that the automated deployment system is disconnected from the network during the operating system build process.

2. Set a unique complex password for the local Administrator account. Don't use a password that has been used for any other account in the environment.

    > ⓘ **Note**
    >
    > Microsoft recommends using **Local Administrator Password Solution (LAPS)** to manage the local Administrator password for all workstations, including

> PAWs. If you use LAPS, ensure that you only grant the PAW Maintenance group the right to read LAPS-managed passwords for the PAWs.

3. Install Remote Server Administration Tools for Windows 11 using the clean source installation media.

4. Configure Windows Defender Exploit Guard

5. Connect the PAW to the network. Ensure that the PAW can connect to at least one Domain Controller (DC).

6. Using an account that is a member of the PAW Maintenance group, run the following PowerShell command from the newly created PAW to join it to the domain in the appropriate OU:

   ```
   Add-Computer -DomainName Fabrikam -OUPath "OU=Devices,OU=Tier 0,OU=Admin,DC=fabrikam,DC=com"
   ```

   Replace the references to *Fabrikam* with your domain name, as appropriate. If your domain name extends to multiple levels (for example, child.fabrikam.com), add the other names with the "DC=" identifier in the order in which they appear in the domain's fully qualified domain name.

7. Apply all critical and important Windows Updates before installing any other software (including administrative tools, agents, etc.).

8. Force the Group Policy application.
   a. Open an elevated command prompt and enter the following command:
      `Gpupdate /force /sync`
   b. Restart the computer

9. (Optional) Install other required tools for Active Directory Admins. Install any other tools or scripts required to perform job duties. Ensure to evaluate the risk of credential exposure on the target computers with any tool before adding it to a PAW.

   > **Note**
   >
   > Using a jump server for a central location for these tools can reduce complexity, even if it doesn't serve as a security boundary.

10. (Optional) Download and install required remote access software. If administrators are using the PAW remotely for administration, install the remote access software

using security guidance from your remote access solution vendor.

> ⓘ Note
>
> Carefully consider all the risks involved in allowing remote access via a PAW. While a mobile PAW enables many important scenarios, including work from home, remote access software can potentially be vulnerable to attack and used to compromise a PAW.

11. Validate the integrity of the PAW system by reviewing and confirming that all appropriate settings are in place using the following steps:
    a. Confirm that only the PAW-specific group policies are applied to the PAW
        i. Open an elevated command prompt and enter the following command: `Gpresult /scope computer /r`
        ii. Review the resulting list and ensure that the only group policies that appear are the ones you created previously.
    b. Confirm that no other user accounts are members of privileged groups on the PAW using the following steps:

        i. Open **Edit Local Users and Groups** (lusrmgr.msc), select **Groups**, and confirm that the only members of the local Administrators group are the local Administrator account and the PAW Maintenance global security group.

        > ⓘ Important
        >
        > The PAW Users group should not be a member of the local Administrators group. The only members should be the local Administrator account and the PAW Maintenance global security group (and PAW Users should not be a member of that global group either).

        ii. Also using **Edit Local Users and Groups**, ensure that the following groups have no members:

        - Backup Operators
        - Cryptographic Operators
        - Hyper-V Administrators
        - Network Configuration Operators
        - Power Users
        - Remote Desktop Users
        - Replicators

12. (Optional) If your organization uses a security information and event management (SIEM) solution, ensure that the PAW is configured to forward events to the system using Windows Event Forwarding (WEF) or is otherwise registered with the solution so that the SIEM is actively receiving events and information from the PAW. The details of this operation vary based on your SIEM solution.

    > ⓘ Note
    >
    > If your SIEM requires an agent which runs as system or a local administrative account on the PAWs, ensure that the SIEMs are managed with the same level of trust as your domain controllers and identity systems.

13. (Optional) If you chose to deploy LAPS to manage the password for the local Administrator account on your PAW, verify that the password is registered successfully.

    - Using an account with permissions to read LAPS-managed passwords, open **Active Directory Users and Computers** (dsa.msc). Ensure that Advanced Features are enabled, and then right-click the appropriate computer object. Select the Attribute Editor tab and confirm that the value for msSVSadmPwd is populated with a valid password.

## Phase 2: Extend PAW to all administrators

Scope: All users with administrative rights over mission-critical applications and dependencies. This should include at least administrators of application servers, operational health and security monitoring solutions, virtualization solutions, storage systems, and network devices.

> ⓘ Note
>
> The instructions in this phase assume that Phase 1 has been completed in its entirety. Do not begin Phase 2 until you have completed all the steps in Phase 1.

Once you confirm that all steps were done, perform the following steps to complete Phase 2:

### (Recommended) Enable RestrictedAdmin mode

Enable this feature on your existing servers and workstations, then enforce the use of this feature. This feature requires the target servers to be running Windows Server 2008 R2 or later and target workstations to be running Windows 7 or later.

1. Enable **RestrictedAdmin** mode on your servers and workstations by following the instructions available in this page.

   > ⓘ **Note**
   >
   > Before enabling this feature for internet facing servers, you should consider the risk of adversaries being able to authenticate to these servers with a previously-stolen password hash.

2. Create "RestrictedAdmin Required - Computer" group policy object (GPO). This section creates a GPO that enforces the use of the /RestrictedAdmin switch for outgoing Remote Desktop connections, protecting accounts from credential theft on the target systems

   - Go to Computer Configuration\Policies\Administrative Templates\System\Credentials Delegation\Restrict delegation of credentials to remote servers and set to **Enabled**.

3. Link the **RestrictedAdmin** Required - Computer to the appropriate Tier 1 and/or Tier 2 Devices by using the following policy options:

   - PAW Configuration - Computer
     - -> Link Location: Admin\Tier 0\Devices (Existing)
   - PAW Configuration - User
     - -> Link Location: Admin\Tier 0\Accounts
   - RestrictedAdmin Required - Computer
     - ->Admin\Tier1\Devices or -> Admin\Tier2\Devices (Both are optional)

   > ⓘ **Note**
   >
   > This is not necessary for Tier 0 systems as these systems are already in full control of all assets in the environment.

## Move Tier 1 Objects to the appropriate OUs

1. Move Tier 1 groups To the Admin\Tier 1\Groups OU. Locate all groups that grant the following administrative rights and move them to this OU.

- Local administrator on more than one server
    - Administrative Access to cloud services
    - Administrative Access to enterprise applications

2. Move Tier 1 accounts to the Admin\Tier 1\Accounts OU. Move each account that is a member of those Tier 1 groups (including nested membership) to this OU.

3. Add the appropriate members to the relevant groups

    - **Tier 1 Admins** - This group contains the Tier 1 Admins that restricted from logging on to Tier 2 hosts. Add all your Tier 1 administrative groups that have administrative privileges over servers or internet services.

        > ⓘ **Important**
        >
        > If administrative personnel have duties to manage assets at multiple tiers, you will need to create a separate admin account per tier.

4. Enable Credential Guard to reduce risk of credential theft and reuse. Credential Guard is a new feature of Windows 11 that restricts application access to credentials, preventing credential theft attacks (including Pass-the-Hash). Credential Guard is transparent to the end-user and requires minimal setup time and effort. For more information on Credential Guard, including deployment steps and hardware requirements, see the article, Protect domain credentials with Credential Guard.

    > ⓘ **Note**
    >
    > Device Guard must be enabled in order to configure and use Credential Guard. However, you are not required to configure any other Device Guard protections in order to use Credential Guard.

5. (Optional) Enable Connectivity to Cloud Services. This step allows management of cloud services like Azure and Microsoft 365 with appropriate security assurances. This step is also required for Microsoft Intune to manage the PAWs.

    > ⓘ **Note**
    >
    > Skip this step if no cloud connectivity is required for administration of cloud services or management by Intune.

- These steps restrict communication over the internet to only authorized cloud services (but not the open internet) and add protections to the browsers and other applications that process content from the internet. These PAWs for administration should never be used for standard user tasks like internet communications and productivity.
- To enable connectivity to PAW services complete the following steps:

a. Configure PAW to allow only authorized Internet destinations. As you extend your PAW deployment to enable cloud administration, you need to allow access to authorized services while filtering out access from the open internet where attacks can more easily be mounted against your admins.

i. Create **Cloud Services Admins** group and add all the accounts to it that require access to cloud services on the internet.

ii. Download the PAW *proxy.pac* file from TechNet Gallery and publish it on an internal website.

> ⓘ **Note**
>
> You will need to update the *proxy.pac* file after downloading to ensure that it is up-to-date and complete. Microsoft publishes all current Microsoft 365 and Azure URLs in the Office **Support Center**. These instructions assume that you will be using Internet Explorer (or Microsoft Edge) for administration of Microsoft 365, Azure, and other cloud services. Microsoft recommends configuring similar restrictions for any 3rd party browsers that you require for administration. Web browsers on PAWs should only be used for administration of cloud services, and never for general web browsing.
>
> You might need to add other valid Internet destinations to add to this list for other IaaS provider, but do not add productivity, entertainment, news, or search sites to this list.
>
> You might also need to adjust the PAC file to accommodate a valid proxy address to use for these addresses.
>
> You can also restrict access from the PAW using a web proxy as well for defense in depth. We don't recommend using this by itself without the PAC file as it will only restrict access for PAWs while connected to the corporate network.

iii. Once you've configured the *proxy.pac* file, update the PAW Configuration - User GPO.

i. Go to User Configuration\Preferences\Windows Settings\Registry. Right-click Registry, select **New** > **Registry Item** and configure the following settings:

i. Action: Replace

ii. Hive: HKEY_CURRENT_USER

iii. Key Path: Software\Microsoft\Windows\CurrentVersion\Internet Settings

iv. Value name: AutoConfigUrl

> **Caution**
>
> Do not select the **Default** box to the left of Value name.

v. Value type: REG_SZ

vi. Value data: enter the complete URL to the *proxy.pac* file, including http:// and the file name - for example `http://proxy.fabrikam.com/proxy.pac`. The URL can also be a single-label URL - for example, `http://proxy/proxy.pac`

> **Note**
>
> The PAC file can also be hosted on a file share, with the syntax of `file://server.fabrikan.com/share/proxy.pac` but this requires allowing the file:// protocol. See the "NOTE: `File://` based Proxy Scripts Deprecated" section of this **Understanding Web Proxy Configuration** blog for additional detail on configuring the required registry value.

vii. Click the **Common** tab and select **Remove this item when it is no longer applied**.

viii. On the Common tab, select **Item level targeting** and click **Targeting**.

ix. Click **New Item** and select **security group**.

x. Select the "..." button and browse for the **Cloud Services Admins** group.

xi. Click **New Item** and select **security group**.

xii. Select the "..." button and browse for the **PAW Users** group.

xiii. Click on the **PAW Users** item and click **Item Options**.

xiv. Select **Is not**.

xv. Click **OK** on the targeting window.

xvi. Click **OK** to complete the **AutoConfigUrl** group policy setting.

b. Apply Windows 11 Security baselines and Cloud Service Access Link the security baselines for Windows and for cloud service access (if necessary) to the correct OUs using the following steps:

i. Extract the contents of the Windows 11 Security Baselines ZIP file.

ii. Create these GPOs, import the policy settings, and link per this table. Link each policy to each location and ensure the order follows the table (lower entries in table should be applied later and higher priority):

**Policies:**

Expand table

| **Policy Name** | **Link** |
|---|---|
| CM Windows 11 - Domain Security | N/A - Do Not Link Now |
| SCM Windows 11 TH2 - Computer | Admin\Tier 0\Devices |
| | Admin\Tier 1\Devices |
| | Admin\Tier 2\Devices |
| SCM Windows 11 TH2- BitLocker | Admin\Tier 0\Devices |
| | Admin\Tier 1\Devices |
| | Admin\Tier 2\Devices |
| SCM Windows 11 - Credential Guard | Admin\Tier 0\Devices |
| | Admin\Tier 1\Devices |
| | Admin\Tier 2\Devices |

| Policy Name | Link |
|---|---|
| SCM Internet Explorer - Computer | Admin\Tier 0\Devices |
| | Admin\Tier 1\Devices |
| | Admin\Tier 2\Devices |
| PAW Configuration - Computer | Admin\Tier 0\Devices (Existing) |
| | Admin\Tier 1\Devices (New Link) |
| | Admin\Tier 2\Devices (New Link) |
| RestrictedAdmin Required - Computer | Admin\Tier 0\Devices |
| | Admin\Tier 1\Devices |
| | Admin\Tier 2\Devices |
| SCM Windows 11 - User | Admin\Tier 0\Devices |
| | Admin\Tier 1\Devices |
| | Admin\Tier 2\Devices |
| SCM Internet Explorer - User | Admin\Tier 0\Devices |
| | Admin\Tier 1\Devices |
| | Admin\Tier 2\Devices |
| PAW Configuration - User | Admin\Tier 0\Devices (Existing) |
| | Admin\Tier 1\Devices (New Link) |
| | Admin\Tier 2\Devices (New Link) |

> **Note**
>
> The "SCM Windows 11 - Domain Security" GPO might be linked to the domain independently of PAW, but will affect the entire domain.

6. (Optional) Install other required tools for Tier 1 Admins. Install any other tools or scripts required to perform job duties. Ensure to evaluate the risk of credential exposure on the target computers with any tool before adding it to a PAW.

7. Identify and safely obtain software and applications required for administration. This is similar to the work performed in Phase 1, but with a broader scope due to the increased number of applications, services, and systems being secured.

> ⓘ **Important**
>
> Ensure that you protect these new applications (including web browsers) by opting them into the protections provided by Windows Defender Exploit Guard.

- Examples of other software and applications include:
  - Service or application management software based on the Microsoft Management Console
  - Proprietary (non-MMC-based) service or application management software

    > ⓘ **Note**
    >
    > Many applications are now exclusively managed via web browsers, including many cloud services. While this reduces the number of applications which need to be installed on a PAW, it also introduces the risk of browser interoperability issues. You might need to deploy a non-Microsoft web browser on to specific PAW instances to enable administration of specific services. If you do deploy an additional web browser, ensure that you follow all clean source principles and secure the browser according to the vendor's security guidance.

8. (Optional) Download and install any required management agents.

   > ⓘ **Important**
   >
   > If you choose to install additional management agents (monitoring, security, configuration management, etc.), it is vital that you ensure the management systems are trusted at the same level as domain controllers and identity systems.

9. Assess your infrastructure to identify systems that require the more security protections provided by a PAW. Ensure that you know exactly which systems must be protected. Ask critical questions about the resources themselves, such as:

   - Where are the target systems that must be managed? Are they collected in a single physical location, or connected to a single well-defined subnet?

- How many systems are there?

- Do these systems depend on other systems (virtualization, storage, etc.), and if so, how are those systems managed? How are the critical systems exposed to these dependencies, and what are the other risks associated with those dependencies?

- How critical are the services being managed, and what is the expected loss if those services are compromised?

  > ⓘ **Important**
  >
  > Include your cloud services in this assessment - attackers increasingly target insecure cloud deployments, and it is vital that you administer those services as securely as you would your on-premises mission-critical applications.

  Use this assessment to identify the specific systems that require extra protection, and then extend your PAW program to the administrators of those systems. Common examples of systems that benefit greatly from PAW-based administration include SQL Server (both on-premises and SQL Azure), human resources applications, and financial software.

  > ⓘ **Note**
  >
  > If a resource is managed from a Windows system, it can be managed with a PAW, even if the application itself runs on an operating system other than Windows or on a non-Microsoft cloud platform. For example, the owner of a cloud service provider subscription should only use a PAW to administer that account.

10. Develop a request and distribution method for deploying PAWs at scale in your organization. Depending on the number of PAWs you choose to deploy in Phase 2, you might need to automate the process.

    - Consider developing a formal request and approval process for administrators to use to obtain a PAW. This process would help standardize the deployment process, ensure accountability for PAW devices, and help identify gaps in PAW deployment.

    - As stated previously, this deployment solution should be separate from existing automation methods (which might have already been compromised) and should follow the principles outlined in Phase 1.

> ⓘ **Important**
>
> Any system which manages resources should itself managed at the same or higher trust level.

11. Review and if necessary deploy more PAW hardware profiles. The hardware profile you chose for Phase 1 deployment might not be suitable for all administrators. Review the hardware profiles and if appropriate select other PAW hardware profiles to match the needs of the administrators. For example, the dedicated hardware profile (separate PAW and daily use workstations) might be unsuitable for an administrator who travels often.

12. Consider the cultural, operational, communications, and training needs that accompany an extended PAW deployment. Such a significant change to an administrative model will naturally require change management to some degree, and it's essential to build that into the deployment project itself. Consider at a minimum the following questions:

    - How will you communicate the changes to senior leadership to ensure their support? Any project without senior leadership backing is likely to fail, or struggle for funding and broad acceptance.

    - How will you document the new process for administrators? These changes must be documented and communicated not only to existing administrators (who must change their habits and manage resources in a different way), but also for new administrators (those promoted from within or hired from outside the organization). It's essential that the documentation is clear and fully articulates:
        - The importance of the threats
        - The role of PAW in protecting administrators.
        - How to use a PAW correctly.

    > ⓘ **Important**
    >
    > This is especially important for roles with high turnover, including but not limited to help desk personnel.

    - How to ensure compliance with the new process? While the PAW model includes several technical controls to prevent the exposure of privileged credentials, it's impossible to fully prevent all possible exposure purely using technical controls. For example, although it's possible to prevent an administrator from successfully logging on to a user desktop with privileged credentials, the simple act of attempting the logon can expose the credentials to malware installed on that user desktop. It's therefore essential that you articulate not only the benefits of the PAW model, but the risks of noncompliance. This should be complemented by auditing and alerting so that credential exposure can be quickly detected and addressed.

## Phase 3: Extend and enhance protection

Scope: These protections enhance the systems built in Phase 1, bolstering the basic protection with advanced features including Multifactor authentication and network access rules.

> ⓘ Note
>
> This phase can be performed at any time after Phase 1 has been completed. It is not dependent on completion of Phase 2, and thus can be performed before, concurrent with, or after Phase 2.

Complete the following steps to configure this phase:

1. **Enable multifactor authentication for privileged accounts**. Multifactor authentication strengthens account security by requiring the user to provide a physical token in addition to credentials. Multifactor authentication complements authentication policies well, but it doesn't depend on authentication policies for deployment (and, similarly, authentication policies don't require Multifactor authentication). Microsoft recommends using one of these forms of Multifactor authentication:

   - **Smart card**: A smart card is a tamper-resistant and portable physical device that provides a second verification during the Windows logon process. By requiring an individual to possess a card for logon, you can reduce the risk of stolen credentials being reused remotely. For details on smart card logon in Windows, refer to the article Smart Card Overview.
   - **Virtual smart card**: A virtual smart card provides the same security benefits as physical smart cards, with the added benefit of being linked to specific hardware. For details on deployment and hardware requirements, refer to the articles, Virtual Smart Card Overview and Get Started with Virtual Smart Cards: Walkthrough Guide.

- **Windows Hello for Business**: Windows Hello for Business lets users authenticate to a Microsoft account, an Active Directory account, a Microsoft Entra account, or non-Microsoft service that supports Fast ID Online (FIDO) authentication. After an initial two-step verification during Windows Hello for Business enrollment, a Windows Hello for Business is set up on the user's device and the user sets a gesture, which can be Windows Hello or a PIN. Windows Hello for Business credentials are an asymmetric key pair, which can be generated within isolated environments of Trusted Platform Modules (TPMs).
    - For more information on Windows Hello for Business read Windows Hello for Business article.
- **Azure Multifactor authentication**: Azure Multifactor authentication (MFA) provides the security of a second verification factor and enhanced protection through monitoring and machine-learning-based analysis. Microsoft Entra multifactor authentication can secure not only Azure administrators but many other solutions as well, including web applications, Microsoft Entra ID, and on-premises solutions like remote access and Remote Desktop. For more information, see the article Multifactor authentication.

2. **Allow list trusted applications using Windows Defender Application Control and/or AppLocker**. By limiting the ability of untrusted or unsigned code to run on a PAW, you further reduce the likelihood of malicious activity and compromise. Windows includes two primary options for application control:

    - **AppLocker**: AppLocker helps administrators control which applications can run on a given system. AppLocker can be centrally controlled through group policy, and applied to specific users or groups (for targeted application to users of PAWs). For more information on AppLocker, see the TechNet article AppLocker Overview.
    - **Windows Defender Application Control**: the new Windows Defender Application Control feature provides enhanced hardware-based application control that, unlike AppLocker, can't be overridden on the impacted device. Like AppLocker, Windows Defender Application Control can be controlled via group policy and targeted to specific users. For more information on restricting application usage with Windows Defender Application Control, see Windows Defender Application Control Deployment Guide.

3. **Use Protected Users, Authentication Policies, and Authentication Silos to further protect privileged accounts**. The members of Protected Users are subject to extra security policies that protect the credentials stored in the local security agent (LSA) and greatly minimize the risk of credential theft and reuse. Authentication policies and silos control how privileged users can access resources in the domain.

Collectively, these protections dramatically strengthen the account security of these privileged users. For more information on these features, see the article How to Configure Protected Accounts.

> ⓘ **Note**
>
> These protections are meant to complement, not replace, existing security measures in Phase 1. Administrators should still use separate accounts for administration and general use.

## Managing and updating

PAWs must have anti-malware capabilities and software updates must be rapidly applied to maintain integrity of these workstations.

Extra configuration management, operational monitoring, and security management can also be used with PAWs. The integration of these capabilities must be considered carefully because each of them introduces risk of PAW compromise through that tool. Whether it makes sense to introduce advanced management capabilities depends on several factors including:

- The security state and practices of the management capability (including software update practices for the tool, administrative roles and accounts in those roles, operating systems the tool is hosted on or managed from, and any other hardware or software dependencies of that tool)
- The frequency and quantity of software deployments and updates on your PAWs
- Requirements for detailed inventory and configuration information
- Security monitoring requirements
- Organizational standards and other organizational-specific factors

Per the clean source principle, all tools used to manage or monitor the PAWs must be trusted at or above the level of the PAWs. This process typically requires those tools to be managed from a PAW to ensure no security dependency from lower privilege workstations.

This table outlines different approaches that might be used to manage and monitor the PAWs:

Expand table

| Approach | Considerations |
|---|---|
| Default in PAW<br>- Windows Server Update Services<br>- Windows Defender | - No extra cost<br>- Performs basic required security functions<br>- Instructions included in this guidance |
| Manage with Intune | • Provides cloud-based visibility and control<br>○ Software Deployment<br>○ o Manage software updates<br>○ Windows Firewall policy management<br>○ Anti-malware protection<br>○ Remote assistance<br>○ Software license management.<br>• No server infrastructure required<br>• Requires following "Enable Connectivity to Cloud Services" steps in Phase 2<br>• If the PAW computer isn't joined to a domain, this configuration requires applying the SCM baselines to the local images using the tools provided in the security baseline download. |
| New System Center instance(s) for managing PAWs | - Provides visibility and control of configuration, software deployment, and security updates<br>- Requires separate server infrastructure, securing it to level of PAWs, and staffing skills for those highly privileged personnel |
| Manage PAWs with existing management tool(s) | - Creates significant risk to compromise of PAWs unless the existing management infrastructure is brought up to security level of PAWs **Note:** Microsoft would generally discourage this approach unless your organization has a specific reason to use it. In our experience, there's typically a high cost of bringing all these tools (and their security dependencies) up to the security level of the PAWs.<br>- Most of these tools provide visibility and control of configuration, software deployment, and security updates |
| Security Scanning or monitoring tools requiring admin access | Includes any tool that installs an agent or requires an account with local administrative access.<br>- Requires bringing tool security assurance up to level of PAWs.<br>- Might require lowering security posture of PAWs to support tool functionality (open ports, install Java or other middleware, etc.), creating a security trade-off decision, |
| Security information and event management (SIEM) | • If SIEM is agentless<br>○ Can access events on PAWs without administrative access by using an account in the **Event Log Readers** group<br>○ Requires opening up network ports to allow inbound traffic from the SIEM servers |

| Approach | Considerations |
|---|---|
| | • If SIEM requires an agent, see other row **Security Scanning or monitoring tools requiring admin access**. |
| Windows Event Forwarding | - Provides an agentless method of forwarding security events from the PAWs to an external collector or SIEM<br>- Can access events on PAWs without administrative access<br>- Doesn't require opening up network ports to allow inbound traffic from the SIEM servers |

## Operating PAWs

The PAW solution should be operated using the standards based on clean source principles.

## Related articles

Microsoft Advanced Threat Analytics

Protect derived domain credentials with Credential Guard

Device Guard Overview

Protecting high-value assets with secure admin workstations

Enabling Strict KDC Validation in Windows Kerberos

What's New in Kerberos Authentication for Windows Server 2012

Authentication Mechanism Assurance for AD DS in Windows Server 2008 R2 Step-by-Step Guide

Trusted Platform Module Technology Overview

## Next steps

Securing privileged access

# Enhanced Security Admin Environment

Article • 01/29/2024

The Enhanced Security Admin Environment (ESAE) architecture (often referred to as red forest, admin forest, or hardened forest) is a legacy approach to provide a secure environment for Windows Server Active Directory (AD) administrator identities.

Microsoft's recommendation to use this architectural pattern has been replaced by the modern privileged access strategy and rapid modernization plan (RAMP) guidance as the default recommended approach for securing privileged users. This guidance is intended to be inclusive of adapting a broader strategy to move towards a Zero Trust architecture. Given these modernized strategies, the ESAE hardened administrative forest architecture (on-premises or cloud-based) is now considered a custom configuration suitable only for exception cases.

## Scenarios for Continued Use

Although it's no longer a recommended architecture, ESAE (or individual components therein) can still be valid in a limited set of exempted scenarios. Typically, these on-premises environments are isolated where cloud services may be unavailable. This scenario may include critical infrastructure or other disconnected operational technology (OT) environments. However, it should be noted that air-gapped Industrial Control System/Supervisory Control and Data Acquisition (ICS/SCADA) segments of the environment don't typically utilize their own Active Directory deployment.

If your organization is in one of these scenarios, maintaining a currently deployed ESAE architecture in its entirety can still be valid. However, it must be understood that your organization incurs extra risk due to the increased technical complexity and operational costs of maintaining ESAE. Microsoft recommends that any organization still using ESAE, or other legacy identity security controls, apply extra rigor to monitor, identify, and mitigate any associated risks.

> ⓘ **Note**
>
> While Microsoft no longer recommends an isolated hardened forest model for most scenarios at most organizations, Microsoft still operates a similar architecture internally (and associated support processes and personnel) because of the extreme security requirements for providing trusted cloud services to organizations around the globe.

# Guidance for Existing Deployments

For customers that have already deployed this architecture to enhance security and/or simplify multi-forest management, there's no urgency to retire or replace an ESAE implementation if it's being operated as designed and intended. As with any enterprise systems, you should maintain the software in it by applying security updates and ensuring software is within support lifecycle.

Microsoft also recommends organizations with ESAE / hardened forests adopt the modern privileged access strategy using the rapid modernization plan (RAMP) guidance. This guidance complements an existing ESAE implementation and provides appropriate security for roles not already protected by ESAE including Microsoft Entra Global Administrators, sensitive business users, and standard enterprise users. For more information, see the article Securing privileged access security levels.

When ESAE was originally designed more than 10 years ago, the focus was on-premises environments with Active Directory (AD) serving as the local identity provider. This legacy approach is based on macro-segmentation techniques to achieve least-privilege and doesn't adequately account for hybrid- or cloud-based environments. Additionally, ESAE and hardened forest implementations focus only on protecting on-premises Windows Server Active Directory administrators (identities) and don't account for fine-grained identity controls and other techniques contained in the remaining pillars of a modern Zero-Trust architecture. Microsoft has updated its recommendation to cloud-based solutions because they can be deployed more quickly to protect a broader scope of administrative and business-sensitive roles and systems. Additionally, they're less complex, scalable, and require less capital investment to maintain.

> ⓘ **Note**
>
> Although ESAE is no longer recommended in its entirety, Microsoft realizes that many individual components contained therein are defined as good cyber hygiene (e.g., dedicated Privileged Access Workstations). The deprecation of ESAE is not intended to push organizations to abandon good cyber hygiene practices, only to reinforce updated architectural strategies for protecting privileged identities.

## Examples of good cyber hygiene practices in ESAE that are applicable to most organizations

- Using privileged access workstations (PAWs) for all administrative activities

- Enforcing token-based or multi-factor authentication (MFA) for administrative credentials even if it isn't widely used throughout the environment
- Enforcing Least Privilege Administrative Model through regular assessment of group / role membership (enforced by strong organizational policy)

# Best Practice for Securing on-premises AD

As described in Scenarios for Continued Use, there may be circumstances where cloud migration isn't attainable (either partially, or in full) due to varying circumstances. For these organizations, if they don't already have an existing ESAE architecture, Microsoft recommends reducing the attack surface of on-premises AD through increasing the rigor of security for Active Directory and privileged identities. While not an exhaustive list, consider the following high priority recommendations.

- Use a tiered approach implementing least-privilege administrative model:
  - Enforce absolute minimum privileges.
  - Discover, review, and audit privileged identities (strong tie to organizational policy).
    - Excessive privilege granting is one of the most identified issues in assessed environments.
  - MFA for administrative accounts (even if not used widely throughout environment).
  - Time based privileged roles (reduce excessive accounts, reinforce approval processes).
  - Enable and configure all available auditing for privileged identities (notify of enable/disable, password reset, other modifications).
- Use Privileged Access Workstations (PAWs):
  - Don't administer PAWs from a less-trusted host.
  - Use MFA for access to PAWs.
  - Don't forget about physical security.
  - Always ensure PAWs are running the newest and/or currently supported operating systems.
- Understand attack paths and high-risk accounts / applications:
  - Prioritize monitoring of identities and systems that pose the most risk (targets of opportunity / high impact).
  - Eradicate password reuse including across operating system boundaries (common lateral movement technique).
  - Enforce policies restricting activities that increase risk (internet browsing from secured workstations, local administrator accounts across multiple systems, etc.).

  - Reduce applications on Active Directory / Domain Controllers (each added application is extra attack surface).
    - Eliminate unnecessary applications.
    - Move applications still needed to other workloads off of / DC if possible.
- Immutable backup of active directory:
  - Critical component to recovery from ransomware infection.
  - Regular backup schedule.
  - Stored in cloud-based, or off-site location dictated by disaster recovery plan.
- Conduct an Active Directory Security Assessment:
  - Azure subscription is required to view the results (customized Log Analytics dashboard).
  - On-demand or Microsoft engineer supported offerings.
  - Validate / identify guidance from the assessment.
  - Microsoft recommends conducting assessments on an annual basis.

For comprehensive guidance on these recommendations, review the Best Practices for Securing Active Directory.

# Supplemental Recommendations

Microsoft recognizes that some entities may not be capable of fully deploying a cloud-based zero-trust architecture due to varying constraints. Some of these constraints were mentioned in the previous section. In lieu of a full deployment, organizations can address risk and make progress towards Zero-Trust while still maintaining legacy equipment or architectures in the environment. In addition to the previously mentioned guidance, the following capabilities may aid in bolstering the security of your environment and serve as a starting point towards adopting a Zero-Trust architecture.

## Microsoft Defender for Identity (MDI)

Microsoft Defender for Identity (MDI) (formally Azure Advanced Threat Protection, or ATP) underpins the Microsoft Zero-Trust architecture and focuses on the pillar of identity. This cloud-based solution uses signals from both on-premises AD and Microsoft Entra ID to identify, detect, and investigate threats involving identities. MDI monitors these signals to identify abnormal and malicious behavior from users and entities. Notably, MDI facilitates the ability to visualize an adversary's path of lateral movement by highlighting how a given account(s) could be used if compromised. MDI's behavioral analytics and user baseline features are key elements for determining abnormal activity within your AD environment.

ⓘ Note

Although MDI collects signals from on-premises AD it does require a cloud-based connection.

## Microsoft Defender for Internet of Things (D4IoT)

In addition to other guidance described in this document, organizations operating in one of the above mentioned scenarios could deploy Microsoft Defender for IoT (D4IoT). This solution features a passive network sensor (virtual or physical) that enables asset discovery, inventory management, and risk-based behavior analytics for Internet of Things (IoT) and Operational Technology (OT) environments. It can be deployed in on-premises air-gapped or cloud-connected environments and has the capacity to perform deep packet inspection on over 100 ICS/OT proprietary network protocols.

# Next steps

Review the following articles:

1. Privileged Access Strategy
2. Security Rapid Modernization Plan (RAMP)
3. Best Practices for Securing Active Directory

# Microsoft Security Best Practices module: Privileged administration

Article • 11/06/2024

Administrative accounts with privileged access to the environment (and associated elements like groups and workstations) must be protected at the highest levels of security assurances to ensure all other security assurances aren't undermined.

See the Administration topic for more information.

The following videos provide guidance on administration. You can also download the PowerPoint slides associated with these videos.

## Part 1: Introduction (05:40)

https://www.microsoft.com/en-us/videoplayer/embed/RE4qbw1?postJsllMsg=true

## Part 2: Admin Quantity (03:14)

https://www.microsoft.com/en-us/videoplayer/embed/RE4q6qU?postJsllMsg=true

## Part 3: Managed and Separate Admin Accounts (03:38)

https://www.microsoft.com/en-us/videoplayer/embed/RE4q6qV?postJsllMsg=true

## Part 4: Emergency Access (02:28)

https://www.microsoft.com/en-us/videoplayer/embed/RE4qgYn?postJsllMsg=true

## Part 5: Containing Attack Pivot Risk (02:42)

https://www.microsoft.com/en-us/videoplayer/embed/RE4q3Ap?postJsllMsg=true

## Part 6: Admin Account Protection (05:25)

https://www.microsoft.com/en-us/videoplayer/embed/RE4qjhh?postJsllMsg=true

## Part 7: Admin Workstation Security (04:09)

https://www.microsoft.com/en-us/videoplayer/embed/RE4q9rP?postJsllMsg=true

## Part 8: Enforcing Access Security (03:13)

https://www.microsoft.com/en-us/videoplayer/embed/RE4qdUw?postJsllMsg=true

## Part 9: Simplify Permissions (03:31)

https://www.microsoft.com/en-us/videoplayer/embed/RE4qjhj?postJsllMsg=true

## Part 10: Admin Account Lifecycle (02:53)

https://www.microsoft.com/en-us/videoplayer/embed/RE4qlSH?postJsllMsg=true

## Next steps

For additional security guidance from Microsoft, see Microsoft security documentation.