Rapidly modernize your security infrastructure - Privileged access

learn.microsoft.com/en-us/security/privileged-access-workstations/security-rapid-modernization-plan

Security rapid modernization plan

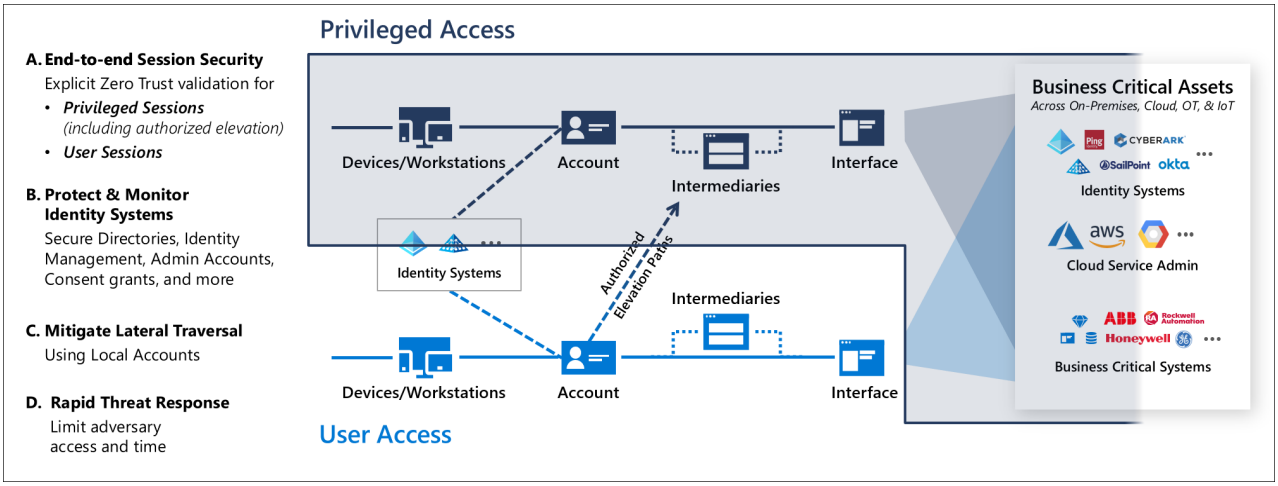
- Article
- 01/30/2024

In this article

1. Separate and manage privileged accounts
2. Improve credential management experience
3. Admin workstations initial deployment
4. Next steps

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.



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 knowledge or 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're successfully integrated in your organization.

It's critical to work together as an organization, create partnerships, and educate people who traditionally weren't part of this process. It's 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 aren't 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're 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 separate 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. Start with the Global Administrator role, because it 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 aren't 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 might 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 Microsoft Entra admin roles.

  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 can't be enforced against them. Leaving legacy authentication protocols enabled can create an entry point for attackers. Some legacy applications might 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 aren't 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'll 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 those managing Microsoft Entra ID 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