Privileged access: Accounts

learn.microsoft.com/en-us/security/privileged-access-workstations/privileged-access-accounts

- Article
- 01/30/2024

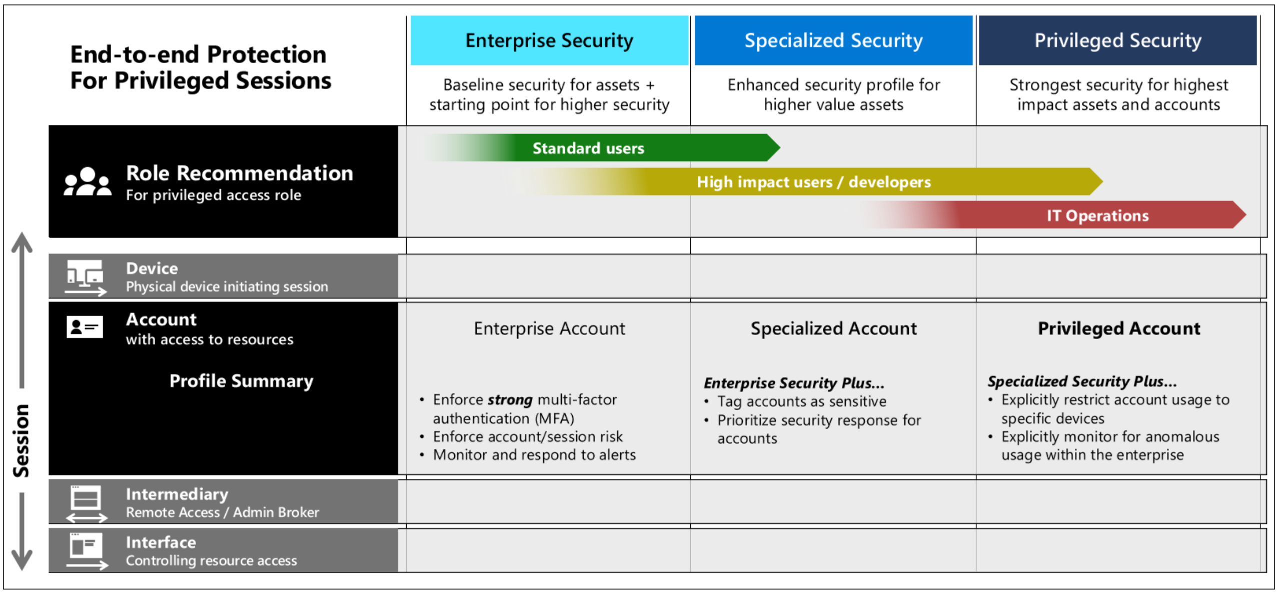
In this article

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: 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

Device: Physical device initiating session

Account: with access to resources

Profile Summary

Enterprise Account
- Enforce *strong* multi-factor authentication (MFA)
- Enforce account/session risk
- Monitor and respond to alerts

Specialized Account

Enterprise Security Plus...
- Tag accounts as sensitive
- Prioritize security response for accounts

Privileged Account

Specialized Security Plus...
- Explicitly restrict account usage to specific devices
- Explicitly monitor for anomalous usage within the enterprise

Intermediary: Remote Access / Admin Broker

Interface: 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.

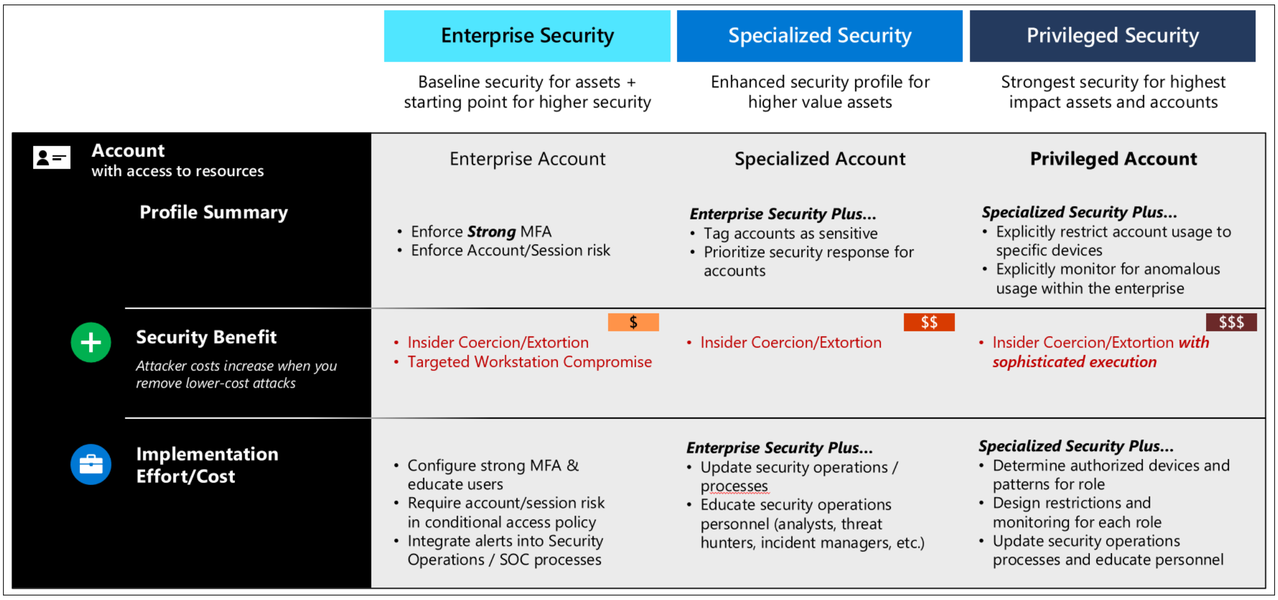
Account security controls

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

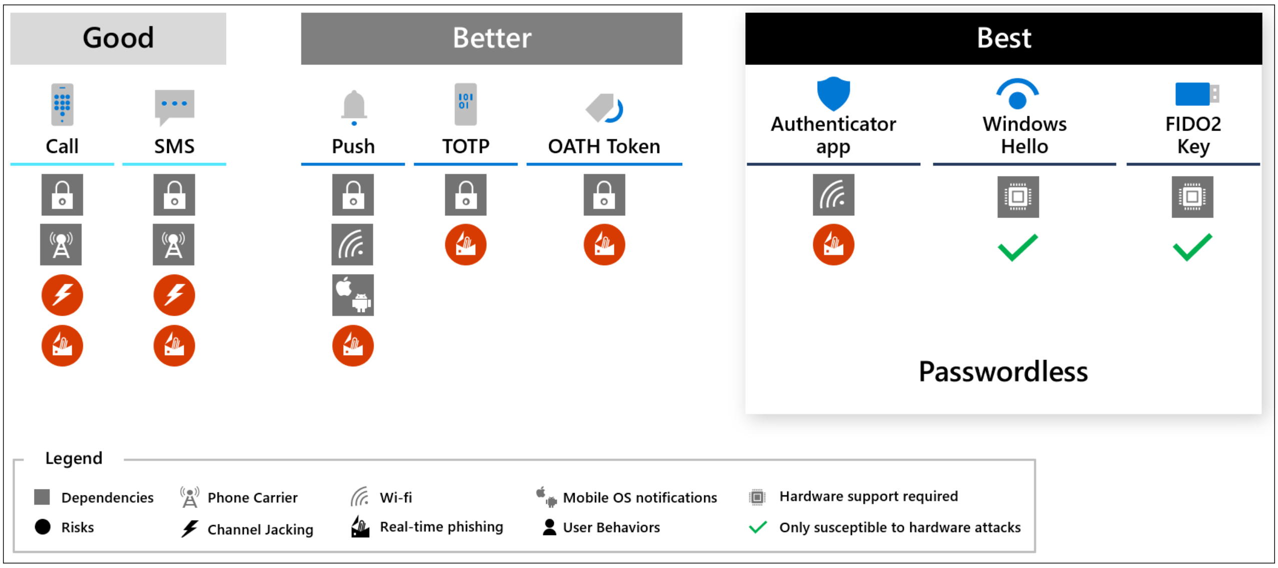
  While your organization may choose to use an existing weaker form of MFA during a transition period, attackers are increasingly evading the weaker MFA protections, so all new investment into MFA should be on the strongest forms.

- 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
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
    1. All new roles to are evaluated for specialized or privileged classifications as they are created or changed
    2. All new accounts are tagged as they are created
    3. 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

Additional resources

Training

Module

Secure Windows Server user accounts - Training

Protect your Active Directory environment by securing user accounts to least privilege and placing them in the Protected Users group. Learn how to limit authentication scope and remediate potentially insecure accounts.

Certification

Microsoft Certified: Identity and Access Administrator Associate - Certifications

Demonstrate the features of Microsoft Entra ID to modernize identity solutions, implement hybrid solutions, and implement identity governance.