Privileged access: Interfaces

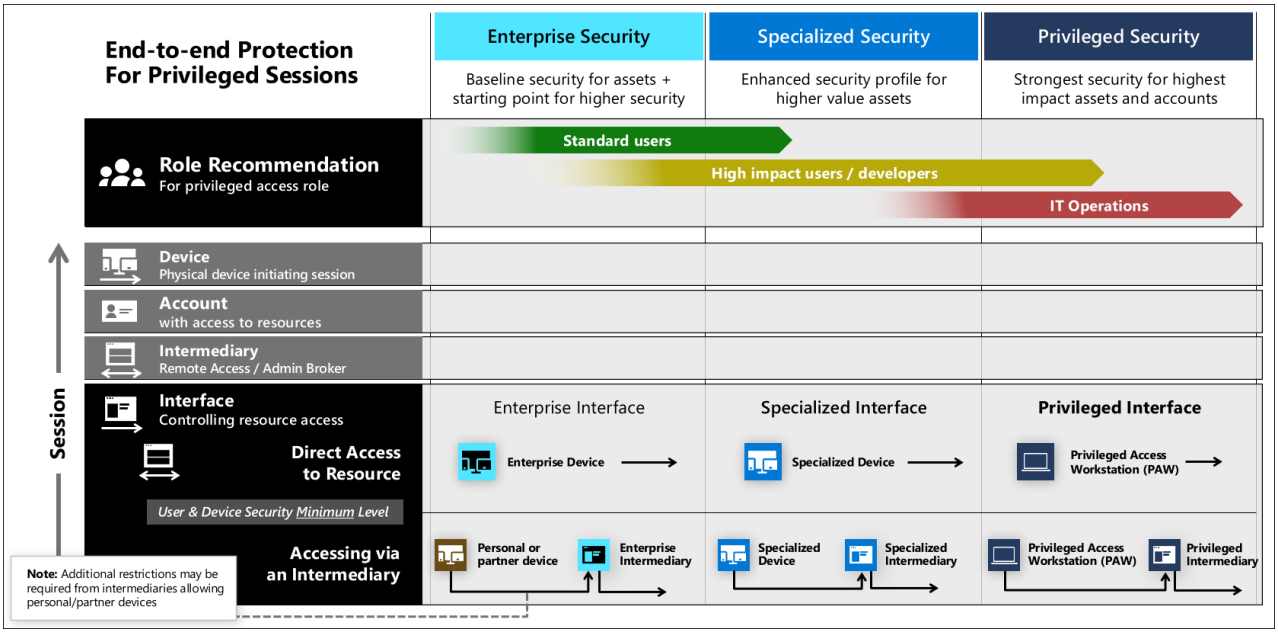
learn.microsoft.com/en-us/security/privileged-access-workstations/privileged-access-interfaces

- Article
- 06/20/2024

In this article

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).



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

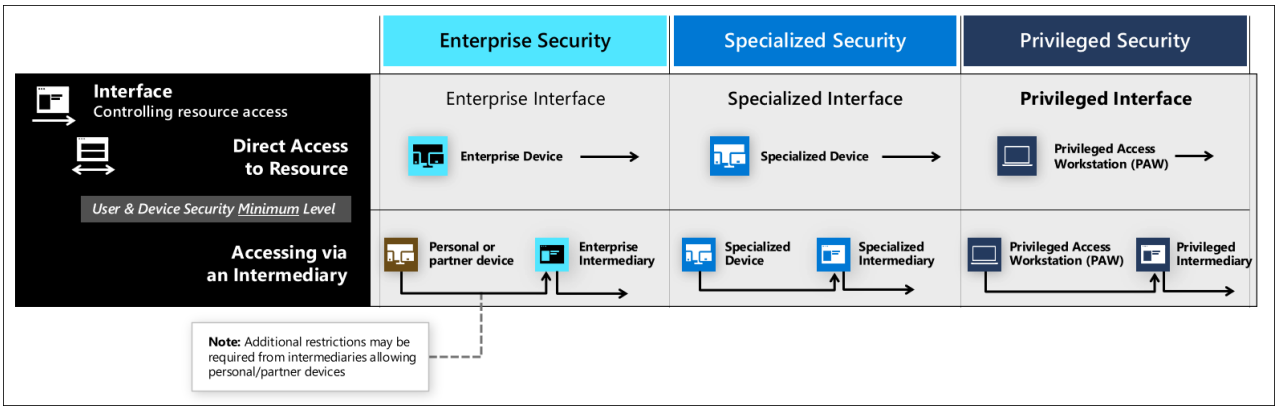
Interface security controls

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.



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