Protect Microsoft 365 from on-premises attacks - Microsoft Entra

By janicericketts

Archived: 2026-04-05 13:22:52 UTC

Many customers connect their private corporate networks to Microsoft 365 to benefit their users, devices, and applications. Threat actors can compromise these private networks in many well-documented ways. Microsoft 365 acts as a sort of nervous system for organizations that invested in modernizing their environment to the cloud. It's critical to protect Microsoft 365 from on-premises infrastructure compromise.

This article shows you how to configure your systems to help protect your Microsoft 365 cloud environment from on-premises compromise:

- Microsoft Entra tenant configuration settings.
- How you can safely connect Microsoft Entra tenants to on-premises systems.
- The tradeoffs required to operate your systems in ways that protect your cloud systems from on-premises compromise.

Microsoft strongly recommends that you implement the guidance in this article.

Threat sources in on-premises environments

Your Microsoft 365 cloud environment benefits from an extensive monitoring and security infrastructure. Microsoft 365 uses machine learning and human intelligence to look across worldwide traffic. It can rapidly detect attacks and allow you to reconfigure nearly in real time.

Hybrid deployments can connect on-premises infrastructure to Microsoft 365. In such deployments, many organizations delegate trust to on-premises components for critical authentication and directory object state management decisions. If threat actors compromise the on-premises environment, these trust relationships become opportunities for them to also compromise your Microsoft 365 environment.

The two primary threat vectors are *federation trust relationships* and *account synchronization.* Both vectors can grant an attacker administrative access to your cloud.

- **Federated trust relationships**, such as Security Assertions Markup Language (SAML) authentication, are used to authenticate to Microsoft 365 through your on-premises identity infrastructure. If a SAML token-signing certificate is compromised, federation allows anyone who has that certificate to impersonate any user in your cloud. To mitigate this vector, we recommend that you disable federation trust relationships for authentication to Microsoft 365 when possible. We also recommend migrating other applications that use on-premises federation infrastructure to use Microsoft Entra for authentication.
- Use **account synchronization** to modify privileged users, including their credentials, or groups that have administrative privileges in Microsoft 365. To mitigate this vector, we recommend that you ensure that synchronized objects hold no privileges beyond a user in Microsoft 365. You can control privileges either

directly or through inclusion in trusted roles or groups. Ensure these objects have no direct or nested assignment in trusted cloud roles or groups.

Protect Microsoft 365 from on-premises compromise

To address on-premises threats, we recommend you adhere to the four principles that the following diagram illustrates.


Diagram showing reference architecture for protecting Microsoft 365, as described in the following list.

1. **Fully isolate your Microsoft 365 administrator accounts.** They should be:

    - Cloud-native accounts.
    - Authenticated by using phishing-resistant credentials.
    - Secured by Microsoft Entra Conditional Access.
    - Accessed only by using Cloud-managed privileged access workstations.

    These administrator accounts are restricted-use accounts. No on-premises accounts should have administrative privileges in Microsoft 365.

    For more information, see About admin roles and Roles for Microsoft 365 in Microsoft Entra ID.

2. **Manage devices from Microsoft 365.** Use Microsoft Entra join and cloud-based mobile device management (MDM) to eliminate dependencies on your on-premises device management infrastructure. These dependencies can compromise device and security controls.

3. **Ensure no on-premises account has elevated privileges to Microsoft 365.** Some accounts access on-premises applications that require NTLM, Lightweight Directory Access Protocol (LDAP), or Kerberos authentication. These accounts must be in the organization's on-premises identity infrastructure. Ensure that you don't include these accounts, along with service accounts, in privileged cloud roles or groups. Ensure that changes to these accounts can't affect the integrity of your cloud environment. Privileged on-premises software must not be capable of affecting Microsoft 365 privileged accounts or roles.

4. **Use Microsoft Entra cloud authentication to eliminate dependencies on your on-premises credentials.** Always use phishing-resistant authentication methods, such as Windows Hello for Business, Platform Credential for macOS, Passkeys (FIDO2), Microsoft Authenticator passkeys, or certificate-based authentication.

Specific security recommendations

The following sections provide guidance on how to implement the principles in this article.

Isolate privileged identities

In Microsoft Entra ID, users who have privileged roles, such as administrators, are the root of trust to build and manage the rest of the environment. Implement the following practices to minimize the effects of a compromise.

- Use cloud-only accounts for Microsoft Entra ID and Microsoft 365 privileged roles.
- Deploy privileged access devices for privileged access to manage Microsoft 365 and Microsoft Entra ID. See Device roles and profiles.
- Deploy Microsoft Entra Privileged Identity Management (PIM) for just-in-time access to all human accounts that have privileged roles. Require phishing-resistant authentication to activate roles.
- Provide administrative roles that allow the least privilege necessary to do required tasks. See Least privileged roles by task in Microsoft Entra ID.
- To enable a rich role assignment experience that includes delegation and multiple roles at the same time, consider using Microsoft Entra security groups or Microsoft 365 Groups. Collectively, we call these *cloud groups*.
- Enable role-based access control. See Assign Microsoft Entra roles. Use administrative units in Microsoft Entra ID to restrict the scope of roles to a portion of the organization.
- Deploy emergency access accounts rather than on-premises password vaults to store credentials. See Manage emergency access accounts in Microsoft Entra ID.

For more information, see Securing privileged access and Secure access practices for administrators in Microsoft Entra ID.

Use cloud authentication

Credentials are a primary attack vector. Implement the following practices to make credentials more secure:

- **Deploy passwordless authentication**. Reduce the use of passwords as much as possible by deploying passwordless credentials. You can manage and validate these credentials natively in the cloud. For more information, see Get started with phishing-resistant passwordless authentication deployment in Microsoft Entra ID. Choose from these authentication methods:

    - Windows Hello for Business
    - Platform Credential for macOS
    - Microsoft Authenticator app
    - Passkeys FIDO2)
    - Microsoft Entra Certificate-based authentication

- **Deploy multifactor authentication**. For more information, see Plan a Microsoft Entra multifactor authentication deployment. Provision multiple strong credentials by using Microsoft Entra multifactor authentication. That way, access to cloud resources requires a Microsoft Entra ID managed credential in addition to an on-premises password. For more information, see Build resilience with credential management and Create a resilient access control management strategy by using Microsoft Entra ID.

- **Modernize SSO from devices.** Utilize the modern Single Sign On (SSO) capabilities of Windows 11, macOS, Linux, and mobile devices.

- **Considerations.** Hybrid account password management requires hybrid components such as password protection agents and password writeback agents. If attackers compromise your on-premises infrastructure, they can control the machines on which these agents reside. This vulnerability doesn't compromise your

cloud infrastructure. Using cloud accounts for privileged roles doesn't protect these hybrid components from on-premises compromise.

The default password expiration policy in Microsoft Entra sets the account password of synchronized on-premises accounts to *Never Expire*. You can mitigate this setting with on-premises Active Directory password settings. If your instance of Active Directory is compromised and synchronization is disabled, set the CloudPasswordPolicyForPasswordSyncedUsersEnabled option to force password changes or move away from passwords to phishing-resistant password authentication.

Provision user access from the cloud

Provisioning refers to the creation of user accounts and groups in applications or identity providers.

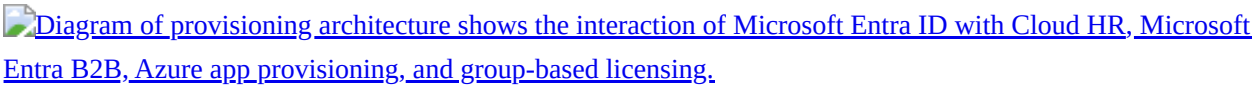
Diagram of provisioning architecture shows the interaction of Microsoft Entra ID with Cloud HR, Microsoft Entra B2B, Azure app provisioning, and group-based licensing.

We recommend the following provisioning methods:

- **Provision from cloud HR apps to Microsoft Entra ID.** This provisioning enables an on-premises compromise to be isolated. This isolation doesn't disrupt your joiner-mover-leaver cycle from your cloud HR apps to Microsoft Entra ID.
- **Cloud applications.** Where possible, deploy app provisioning in Microsoft Entra ID as opposed to on-premises provisioning solutions. This method protects some of your software-as-a-service (SaaS) apps from malicious attacker profiles in on-premises breaches.
- **External identities.** Use Microsoft Entra External ID B2B collaboration to reduce the dependency on on-premises accounts for external collaboration with partners, customers, and suppliers. Carefully evaluate any direct federation with other identity providers. We recommend limiting B2B guest accounts in the following ways:
    - Limit guest access to browsing groups and other properties in the directory. Use the external collaboration settings to restrict guests' ability to read groups of which they're not members.
    - Block access to the Azure portal. You can make rare necessary exceptions. Create a Conditional Access policy that includes all guests and external users. Then implement a policy to block access.
- **Disconnected forests.** Use Microsoft Entra cloud provisioning to connect to disconnected forests. This approach eliminates the need to establish cross-forest connectivity or trusts, which can broaden the effect of an on-premises breach. For more information, see What is Microsoft Entra Connect Cloud Sync.
- **Considerations.** When used to provision hybrid accounts, the Microsoft Entra ID-from-cloud-HR system relies on on-premises synchronization to complete the data flow from Active Directory to Microsoft Entra ID. If synchronization is interrupted, new employee records won't be available in Microsoft Entra ID.

Use cloud groups for collaboration and access

Cloud groups allow you to decouple your collaboration and access from your on-premises infrastructure.

- **Collaboration**. Use Microsoft 365 Groups and Microsoft Teams for modern collaboration. Decommission on-premises distribution lists and upgrade distribution lists to Microsoft 365 Groups in Outlook.
- **Access**. Use Microsoft Entra security groups or Microsoft 365 Groups to authorize access to applications in Microsoft Entra ID. To control access to on-premises applications, consider provisioning groups to Active Directory using Microsoft Entra Cloud Sync.
- **Licensing**. Use group-based licensing to provision to Microsoft services by using cloud-only groups. This method decouples control of group membership from on-premises infrastructure.

Consider owners of groups used for access as privileged identities to avoid membership takeover in an on-premises compromise. Takeovers include direct on-premises group membership manipulation or on-premises attribute manipulation that can affect Microsoft 365 dynamic group membership.

Manage devices from the cloud

Securely manage devices with Microsoft Entra capabilities.

Deploy Microsoft Entra joined Windows 11 workstations with mobile device management policies. Enable Windows Autopilot for a fully automated provisioning experience. See Plan your Microsoft Entra join implementation.

- Use Windows 11 workstations with the latest updates deployed.
    - Deprecate machines that run Windows 10 and earlier.
    - Don't deploy computers that have server operating systems as workstations.
- Use Microsoft Intune as the authority for all device management workloads, including Windows, macOS, iOS, Android, and Linux.
    - Deploy the iOS Enterprise SSO Extension.
    - Deploy the macOS Enterprise SSO Extension or Platform SSO Secure Enclave Key.
- Deploy privileged access devices. For more information, see Device roles and profiles.

Workloads, applications, and resources

This section provides recommendations to protect from on-premises attacks on workloads, applications, and resources.

- **On-premises single-sign-on (SSO) systems.** Deprecate any on-premises federation and web access management infrastructure. Configure applications to use Microsoft Entra ID. If you're using AD FS for federation, see Understand the stages of migrating application authentication from AD FS to Microsoft Entra ID.
- **SaaS and line-of-business (LOB) applications that support modern authentication protocols.** Use single sign-on in Microsoft Entra ID. Configure apps to use Microsoft Entra ID for authentication to reduce risk in an on-premises compromise.

- **Legacy applications.** You can enable authentication, authorization, and remote access to legacy applications that don't support modern authentication by using Microsoft Entra Private Access. As a first step, enable modern access to the internal networks using Microsoft Entra Private Access Quick Access. This step provides a quick and easy way to replace your VPN one-time configuration using the secure capabilities of Conditional Access. Next, configure per-app access to any TCP-based or UDP-based application.
- **Conditional Access.** Define Conditional Access policies for SaaS, LOB, and Legacy applications to enforce security controls such as phishing-resistant MFA, and device compliance. For more information, read Plan a Microsoft Entra Conditional Access deployment.
- **Access Lifecycle.** Control the access lifecycle to applications and resources using Microsoft Entra ID Governance to implement least privilege access. Give users access to information and resources only if they have a genuine need for them to perform their tasks. Integrate SaaS, LOB, and legacy applications with Microsoft Entra ID Governance. Microsoft Entra ID Entitlement Management automates access request workflows, access assignments, reviews, and expiration.
- **Application and workload servers.** You can migrate Applications or resources that require servers to Azure infrastructure-as-a-service (IaaS). Use Microsoft Entra Domain Services to decouple trust and dependency on on-premises instances of Active Directory. To achieve this decoupling, make sure virtual networks used for Microsoft Entra Domain Services don't have a connection to corporate networks. Use credential tiering. Application servers are typically considered tier-1 assets. For more information, see Enterprise access model.

Conditional Access policies

Use Microsoft Entra Conditional Access to interpret signals and use them to make authentication decisions. For more information, see the Conditional Access deployment plan.

- Use Conditional Access to block legacy authentication protocols whenever possible. Additionally, disable legacy authentication protocols at the application level by using an application-specific configuration. See Block legacy authentication and Legacy authentication protocols. Find specific details for Exchange Online and SharePoint Online.
- Implement the recommended identity and device access configurations. See Common Zero Trust identity and device access policies.
- If you're using a version of Microsoft Entra ID that doesn't include Conditional Access, use Security defaults in Microsoft Entra ID. For more information about Microsoft Entra feature licensing, see the Microsoft Entra pricing guide.

Monitor

After you configure your environment to protect your Microsoft 365 from on-premises compromises, proactively monitor the environment. For more information, see What is Microsoft Entra monitoring.

Monitor the following key scenarios, in addition to any scenarios specific to your organization.

- **Suspicious activity.** Monitor all Microsoft Entra risk events for suspicious activity. See How To: Investigate risk. Microsoft Entra ID Protection natively integrates with Microsoft Defender for Identity. Define network named locations to avoid noisy detections on location-based signals. See Using the location condition in a Conditional Access policy.

- **User and Entity Behavioral Analytics (UEBA) alerts.** Use UEBA to get insights on anomaly detection. Microsoft Defender for Cloud Apps provides UEBA in the cloud. See Investigate risky users. You can integrate on-premises UEBA from Microsoft Defender for Identity. Microsoft Defender for Cloud Apps reads signals from Microsoft Entra ID Protection. See Enable entity behavior analytics to detect advanced threats.

- **Emergency access accounts activity.** Monitor any access that uses emergency access accounts. See Manage emergency access accounts in Microsoft Entra ID. Create alerts for investigations. This monitoring must include the following actions:

    - Sign-ins
    - Credential management
    - Any updates on group memberships
    - Application assignments

- **Privileged role activity.** Configure and review security alerts generated by Microsoft Entra Privileged Identity Management (PIM). Monitor direct assignment of privileged roles outside PIM by generating alerts whenever a user is assigned directly.

- **Microsoft Entra tenant-wide configurations.** Any change to tenant-wide configurations should generate alerts in the system. Include (but don't limit to) the following changes:

    - Updated custom domains
    - Microsoft Entra B2B changes to allowlists and blocklists
    - Microsoft Entra B2B changes to allowed identity providers, such as SAML identity providers, through direct federation or social sign-ins
    - Conditional Access or risk policy changes

- **Application and service principal objects**

    - New applications or service principals that might require Conditional Access policies
    - Credentials added to service principals
    - Application consent activity

- **Custom roles**

    - Updates to the custom role definitions
    - Newly created custom roles

For comprehensive guidance on this topic, check Microsoft Entra security operations guide.

Log management

Define a log storage and retention strategy, design, and implementation to facilitate a consistent tool set. For example, consider security information and event management (SIEM) systems like Microsoft Sentinel, common queries, and investigation and forensics playbooks.

- **Microsoft Entra logs**. Ingest generated logs and signals by consistently following best practices for settings such as diagnostics, log retention, and SIEM ingestion.
- Microsoft Entra ID provides Azure Monitor integration for multiple identity logs. For more information, see Microsoft Entra activity logs in Azure Monitor and Investigate risky users with Copilot.
- **Hybrid infrastructure operating system security logs**. Archive and carefully monitor all hybrid identity infrastructure operating system logs as a tier-0 system because of the surface area implications. Include the following elements:
    - Private network connectors for Microsoft Entra Private Access and Microsoft Entra Application Proxy.
    - Password writeback agents.
    - Password Protection Gateway machines.
    - Network policy servers (NPSs) that have the Microsoft Entra multifactor authentication RADIUS extension.
    - Microsoft Entra Connect.
    - You must deploy Microsoft Entra Connect Health to monitor identity synchronization.

For comprehensive guidance on this topic, check Incident response playbooks and Investigate risky users with Copilot

Next steps

- Build resilience into identity and access management by using Microsoft Entra ID
- Secure external access to resources
- Integrate all your apps with Microsoft Entra ID
