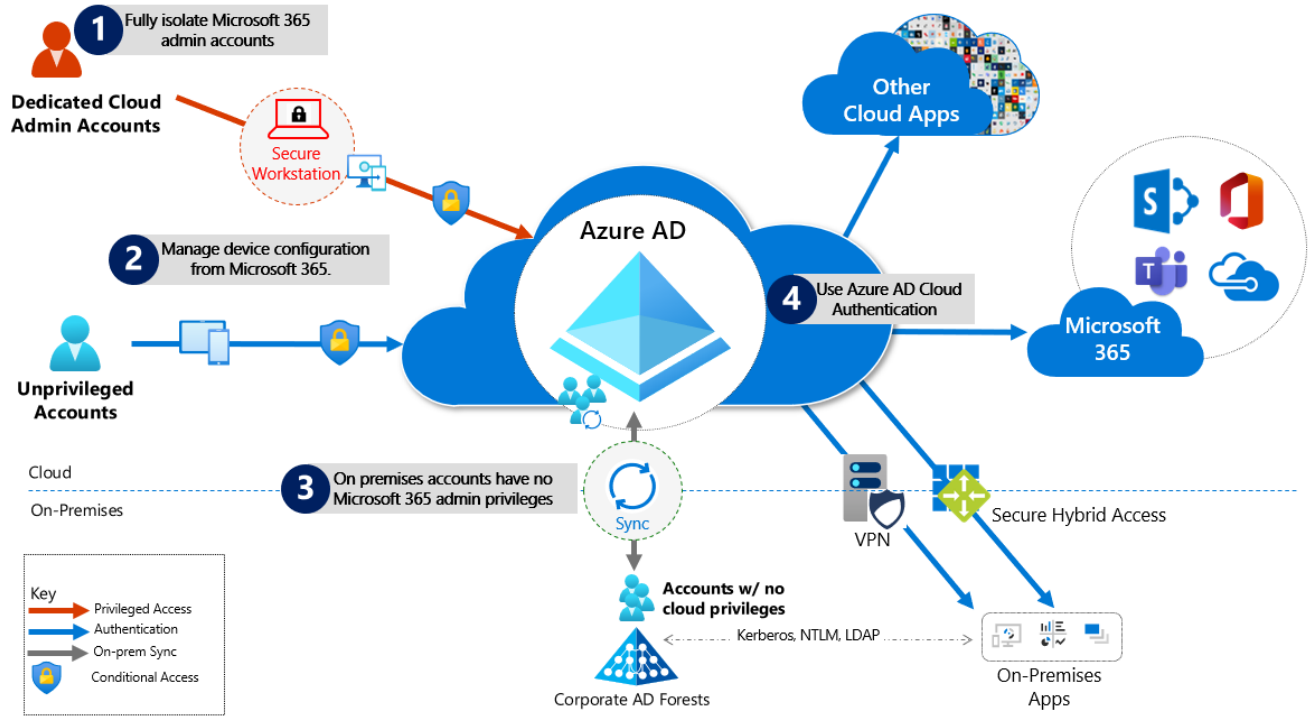
Protecting Microsoft 365 from on-premises attacks

techcommunity.microsoft.com/t5/azure-active-directory-identity/protecting-microsoft-365-from-on-premises-attacks/ba-p/1751754

December 19, 2020



Dec 18 2020 04:01 PM

Many customers connect their private corporate networks to Microsoft 365 to benefit their users, devices, and applications. However, there are many well-documented ways these private networks can be compromised. As we have seen in recent events related to the SolarWinds compromise, on-premises compromise can propagate to the cloud. Because Microsoft 365 acts as the “nervous system” for many organizations, it is critical to protect it from compromised on-premises infrastructure.

This document will show you how to configure your systems to protect your Microsoft 365 cloud environment from on-premises compromise. We primarily focus on Azure AD tenant configuration settings, the ways Azure AD tenants can be safely connected to on-premises systems, and the tradeoffs required to operate your systems in ways that protect your cloud systems from on-premises compromise.

We strongly recommend you implement this guidance to secure your Microsoft 365 cloud environment.

Understanding primary threat vectors from compromised on-premises environments

Your Microsoft 365 cloud environment benefits from an extensive monitoring and security infrastructure. Using machine learning and human intelligence that looks across worldwide traffic can rapidly detect attacks and allow you to reconfigure in near-real-time. In hybrid deployments that connect on-premises infrastructure to Microsoft 365, many organizations delegate trust to on-premises components for critical authentication and directory object state management decisions. Unfortunately, if the on-premises environment is compromised, these trust relationships result in attackers' opportunities to 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.

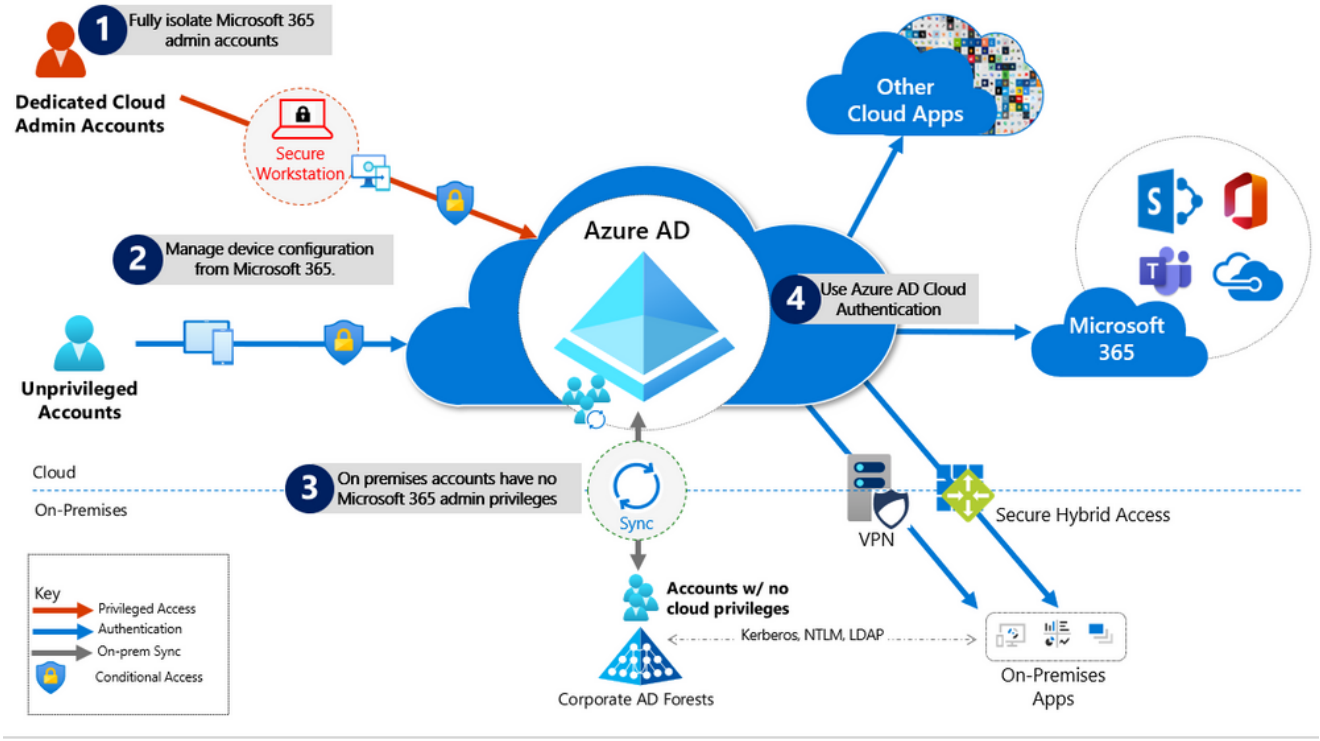
1. **Federated trust relationships**, such as SAML authentication, are used to authenticate to Microsoft 365 via your on-premises Identity Infrastructure. If a SAML token signing certificate is compromised, federation would allow anyone with that certificate to impersonate any user in your cloud

   . We recommend you disable federation trust relationships for authentication to Microsoft 365 when possible.

2. **Account synchronization** can be used to modify privileged users (including their credentials) or groups granted administrative privileges in Microsoft 365. **We recommend you ensure that synchronized objects hold no privileges beyond a userin Microsoft 365,** either directly or via inclusion in trusted roles or groups. Ensure these objects have no direct or nested assignment in trusted cloud roles or groups.

Principles for Protecting Microsoft 365 from on-premises compromise

To address the threat vectors outlined above, we recommend you adhere to the principles illustrated below:



1. **Fully Isolate your Microsoft 365 administrator accounts.** They should be
    - Mastered in Azure AD.
    - Authenticated with Multi-factor authentication (MFA).
    - Secured by Azure AD conditional access.
    - Accessed only by using Azure Managed Workstations.

These are restricted use accounts. **There should be no on-premises accounts with administrative privileges in Microsoft 365.** For more information see this overview of Microsoft 365 administrator roles. Also see Roles for Microsoft 365 in Azure Active Directory.

1. **Manage devices from Microsoft 365.** Use Azure AD Join and cloud-based mobile device management (MDM) to eliminate dependencies on your on-premises device management infrastructure, which can compromise device and security controls.

2. **No on-premises account has elevated privileges to Microsoft 365.** Accounts accessing on-premises applications that require NTLM, LDAP, or Kerberos authentication need an account in the organization's on-premises identity infrastructure. Ensure that these accounts, including service accounts, are not included in privileged cloud roles or groups and that changes to these accounts cannot impact the integrity of your cloud environment. Privileged on-premises software must not be capable of impacting Microsoft 365 privileged accounts or roles.

3. **Use Azure AD cloud authentication** to eliminate dependencies on your on-premises credentials**.** Always use strong authentication, such as Windows Hello, FIDO, the Microsoft Authenticator, or Azure AD MFA.

Specific Recommendations

The following sections provide specific guidance on how to implement the principles described above.

Isolate privileged identities

In Azure AD, users with 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 impact of a compromise.

- Use cloud-only accounts for Azure AD and Microsoft 365 privileged roles.
- Deploy Azure Managed Workstations for privileged access to manage Microsoft 365 and Azure AD.
- Deploy Azure AD Privileged Identity Management (PIM) for just in time (JIT) access to all human accounts that have privileged roles, and require strong authentication to activate roles.
- Provide administrative roles the least privilege possible to perform their tasks.
- To enable a richer role assignment experience that includes delegation and multiple roles at the same time, consider using Azure AD security groups or Microsoft 365 Groups (collectively "cloud groups") and enable role-based access control. You can also use Administrative Units to restrict the scope of roles to a portion of the organization.

- Deploy Emergency Access Accounts and do NOT use on-premises password vaults to store credentials.

For more information, see Securing privileged access, which has detailed guidance on this topic. Also, see Secure access practices for administrators in Azure AD.

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. These credentials are managed and validated natively in the cloud. Choose from:
  - Windows Hello for business
  - Authenticator App
  - FIDO2 security keys

- Deploy Multi-Factor Authentication: Provision multiple strong credentials using Azure AD MFA. That way, access to cloud resources will require a credential that is managed in Azure AD in addition to an on-premises password that can be manipulated.

  For more information, see Create a resilient access control management strategy with Azure active Directory.

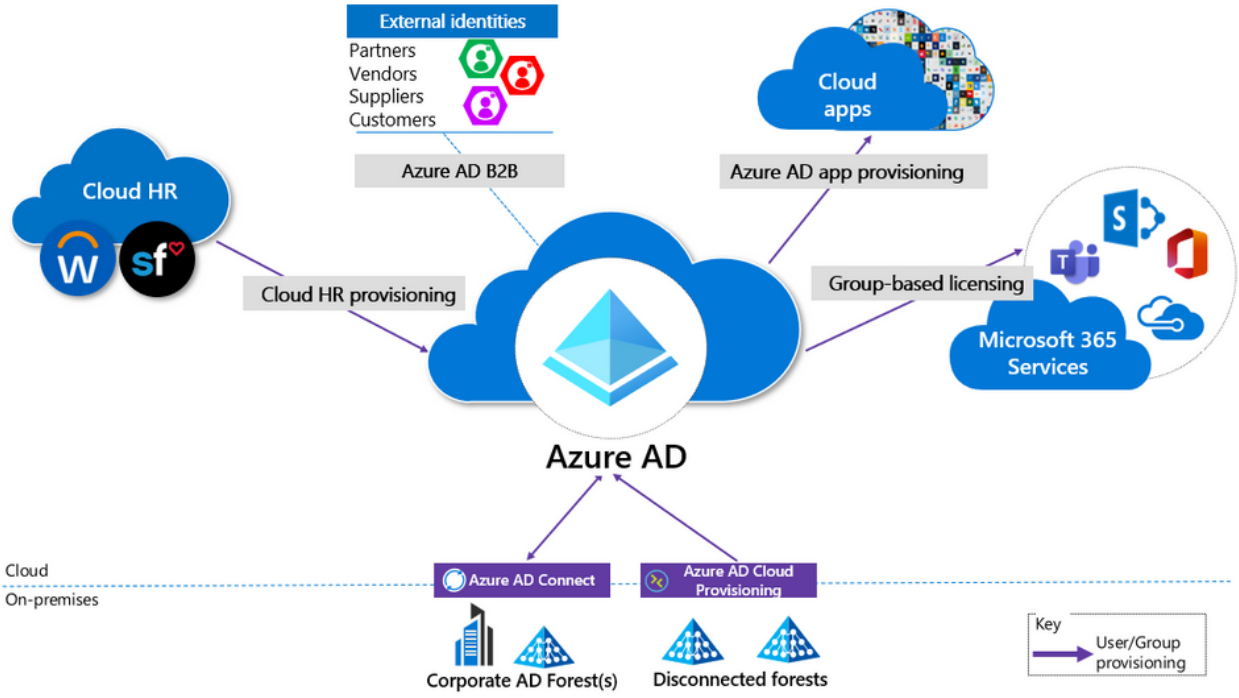
Limitations and tradeoffs

- Hybrid account password management requires hybrid components such as password protection agents and password writeback agents. If your on-premises infrastructure is compromised, attackers can control the machines on which these agents reside. While this will not compromise your cloud infrastructure, your cloud accounts will not protect these components from on-premises compromise.

- On-premises accounts synced from Active Directory are marked to never expire in Azure AD, based on the assumption that on-premises AD password policies will mitigate this. If your on-premises AD is compromised and synchronization from AD connect needs to be disabled, you must set the option EnforceCloudPasswordPolicyForPasswordSyncedUsers.

Provision User Access from the Cloud

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



- **Provision from cloud HR apps to Azure AD:** This enables an on-premises compromise to be isolated without disrupting your Joiner-Mover-Leaver cycle from your cloud HR apps to Azure AD.
- **Cloud Applications:** Where possible, deploy Azure AD App Provisioning as opposed to on-premises provisioning solutions. This will protect some of your SaaS apps from being poisoned with malicious user profiles due to on-premises breaches.

- **External Identities:** Use Azure AD B2B collaboration. This will 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 guest ability to read groups they are not members of.
    - Block access to the Azure portal. You can make rare necessary exceptions.
        Create a Conditional Access policy that includes all guests and external users and then implement a policy to block access.

    - **Disconnected Forests:** Use Azure AD Cloud Provisioning. This enables you to connect to disconnected forests, eliminating the need to establish cross-forest connectivity or trusts, which can broaden the impact of an on-premises breach.

Limitations and Tradeoffs:

When used to provision hybrid accounts, the Azure AD from cloud HR systems relies on on-premises synchronization to complete the data flow from AD to Azure AD. If synchronization is interrupted, new employee records will not be available in Azure AD.

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 Azure AD security groups or Microsoft 365 Groups to authorize access to applications in Azure AD.

- **Office 365 licensing:** Use group-based licensing to provision to Office 365 using cloud-only groups. This decouples control of group membership from on-premises infrastructure.

Owners of groups used for access should be considered privileged identities to avoid membership takeover from on-premises compromise. Take over includes direct manipulation of group membership on-premises or manipulation of on-premises attributes that can affect dynamic group membership in Microsoft 365.

Manage devices from the cloud

Use Azure AD capabilities to securely manage devices.

- **Use Windows 10 Workstations:** Deploy Azure AD Joined devices with MDM policies. Enable Windows Autopilot for a fully automated provisioning experience.
    - Deprecate Windows 8.1 and earlier machines.
    - Do not deploy Server OS machines as workstations.
    - Use Microsoft Intune as the source of authority of all device management workloads.

- **Deploy Azure Managed Workstations** for privileged access to manage Microsoft 365 and Azure AD.

Workloads, applications, and resources

- **On-premises SSO systems:** Deprecate any on-premises federation and Web Access Management infrastructure and configure applications to use Azure AD.
- **SaaS and LOB applications that support modern authentication protocols:** Use Azure AD for single sign-on. The more apps you configure to use Azure AD for authentication, the less risk in the case of an on-premises compromise.
- **Legacy Applications**
    - Authentication, authorization, and remote access to legacy applications that do not support modern authentication can be enabled via Azure AD Application Proxy. They can also be enabled through a network or application delivery controller solution using secure hybrid access partner integrations.
    - Choose a VPN vendor that supports modern authentication and integrate its authentication with Azure AD. In the case of an on-premises compromise, you can use Azure AD to disable or block access by disabling the VPN.
- **Application and workload servers**
    - Applications or resources that required servers can be migrated to Azure IaaS and use Azure AD Domain Services (Azure AD DS) to decouple trust and dependency on AD on-premises. To achieve this decoupling, virtual networks used for Azure AD DS should not have connection to corporate networks.
    - Follow the guidance of the credential tiering. Application Servers are typically considered Tier 1 assets.

Conditional Access Policies

Use Azure AD Conditional Access to interpret signals and make authentication decisions based on them. For more information, see the Conditional Access deployment plan.

- Legacy Authentication Protocols:Use Conditional Access to block legacy authentication protocols whenever possible. Additionally, disable legacy authentication protocols at the application level using application-specific configuration.
  See specific details for Exchange Online and SharePoint Online.
- Implement the recommended Identity and device access configurations.
- If you are using a version of Azure AD that does not include Conditional Access, ensure that you are using the Azure AD security defaults.
  For more information on Azure AD feature licensing, see the Azure AD pricing guide.

Monitoring

Once you have configured your environment to protect your Microsoft 365 from an on-premises compromise, proactively monitor the environment.

Scenarios to Monitor

Monitor the following key scenarios, in addition to any scenarios specific to your organization. For example, you should proactively monitor access to your business-critical applications and resources.

Suspicious activity: All Azure AD risk events should be monitored for suspicious activity. Azure AD Identity Protection is natively integrated with Azure Security Center.
Define the network named locations to avoid noisy detections on location-based signals.

User Entity Behavioral Analytics (UEBA) alerts: Use UEBA to get insights on anomaly detection.

- Microsoft Cloud App Discovery (MCAS) provides UEBA in the cloud.
- You can integrate on-prem UEBA from Azure ATP. MCAS reads signals from Azure AD Identity Protection.

Emergency access accounts activity: Any access using emergency access accounts should be monitored and alerts created for investigations. This monitoring must include:

- Sign-ins.
- Credential management.
- Any updates on group memberships.
- Application Assignments.

Privileged role activity: Configure and review security alerts generated by Azure AD PIM. Monitor direct assignment of privileged roles outside PIM by generating alerts whenever a user is assigned directly.

- **Azure AD tenant-wide configurations**: Any change to tenant-wide configurations should generate alerts in the system. These include but are not limited to
  - Updating custom domains
  - Azure AD B2B allow/block list changes
  - Azure AD B2B allowed identity providers (SAML IDPs through direct federation or social logins)
  - Conditional Access or Risk policy changes
- **Application and service principal objects**:
  - New applications or service principals that might require Conditional Access policies
  - Additional credentials added to service principals
  - Application consent activity
- **Custom roles**:
  - Updates of the custom role definitions
  - New custom roles created

Log Management

Define a log storage and retention strategy, design, and implementation to facilitate a consistent toolset such as SIEM systems like Azure Sentinel, common queries, and investigation and forensics playbooks.

Azure AD Logs Ingest logs and signal produced following consistent best practices (e.g., diagnostics settings, log retention, SIEM ingestion, etc.). The log strategy must include the following Azure AD logs:

- Sign-in activity
- Audit logs
- Risk events

Azure AD provides Azure Monitor integration for the sign-in activity log and audit logs. Risk events can be ingested through Microsoft Graph API. You can stream Azure AD logs to Azure monitor logs.

Hybrid Infrastructure OS Security Logs. All hybrid identity infrastructure OS logs should be archived and carefully monitored as a Tier 0 system, given the surface area implications. This includes:

- Azure AD Connect. Azure AD Connect Health must be deployed to monitor identity synchronization.
- Application Proxy Agents
- Password write-back agents
- Password Protection Gateway machines
- NPS that have the Azure MFA RADIUS extension

Stay up to date

The Solarwinds attack is an ongoing investigation, and our teams continue to act as first responders to these attacks. As new information becomes available, we will make updates through our Microsoft Security Response Center (MSRC) blog at https://aka.ms/solorigate.