

Microsoft Entra device identity documentation

Learn how to configure and manage device identities in Microsoft Entra ID.

About device identity

OVERVIEW

[What is a device identity?](#)

[What is enterprise state roaming?](#)

[Plan your Microsoft Entra device deployment](#)

CONCEPT

[Microsoft Entra registered devices](#)

[Microsoft Entra joined devices](#)

[Microsoft Entra hybrid joined devices](#)

[Single sign-on \(SSO\) to on-premises resources](#)

[Primary Refresh Tokens](#)

Configure and manage Microsoft Entra joined devices

HOW-TO GUIDE

[Plan your Microsoft Entra join implementation](#)

[Manage the local administrators group on Microsoft Entra joined devices](#)

[Find and manage stale devices in Microsoft Entra ID](#)

Configure and manage Microsoft Entra hybrid joined devices

HOW-TO GUIDE

[Plan your Microsoft Entra hybrid join implementation](#)

Troubleshooting Microsoft Entra hybrid joined devices

What is a device identity?

Article • 05/09/2025

A [device identity](#) is an object in Microsoft Entra ID. This device object is similar to users, groups, or applications. A device identity gives administrators information they can use when making access or configuration decisions.

Name	Enabled	OS	Version	Join type	Owner	MDM	Security s
ContosoSP	Yes	Windows	10.0.17763.5576	None	N/A	Microsoft	
ContosoClient	Yes	Windows	10.0.22000.2416	None	Microsoft Intune	Microsoft	
ContosoMIM	Yes	Windows	10.0.17763.5458	None	N/A	Microsoft	
ContosoStudio	Yes	Windows	10.0.22631.3296	Microsoft Entra joined	None	Microsoft Configuration	N/A
CONTOSO-FERNS	Yes	Windows	10.0.19044.3086	None	Microsoft Configuration	N/A	
Contoso-TAC	Yes	Windows	10.0.27554.1000	Microsoft Entra joined	None	Microsoft Configuration	N/A
Contoso-SEA	Yes	Windows	10.0.27554.1000	Microsoft Entra joined	None	Microsoft Configuration	N/A
CONTOSODC	Yes	Windows	10.0.17763.5576	None	N/A	Microsoft	
contoso-nd1	Yes	Windows	10.0.20348.2031	Microsoft Entra regist...	None	None	N/A
Contoso-BE	Yes	Windows	10.0.27554.1000	Microsoft Entra joined	None	Microsoft Configuration	N/A
CONTOSO-6166	Yes	Windows	10.0.22631.3296	Microsoft Entra joined	None	Microsoft Configuration	N/A

There are three ways to get a device identity:

- Microsoft Entra registration
- Microsoft Entra join
- Microsoft Entra hybrid join

Device identities are a prerequisite for scenarios like [device-based Conditional Access policies](#) and [Mobile Device Management with the Microsoft Intune family of products](#).

Modern device scenario

The modern device scenario focuses on two of these methods:

- [Microsoft Entra registration](#)
 - Bring your own device (BYOD)
 - Mobile device (cell phone and tablet)
- [Microsoft Entra join](#)
 - Windows 11 and Windows 10 devices owned by your organization

- Windows Server 2019 and newer servers in your organization running as VMs in Azure

Microsoft Entra hybrid join is seen as an interim step on the road to Microsoft Entra join. All three scenarios can coexist in a single organization.

Resource access

Registering and joining devices to Microsoft Entra ID gives users Seamless Sign-on (SSO) to cloud-based resources.

Devices that are Microsoft Entra joined benefit from [SSO to your organization's on-premises resources](#).

Provisioning

Getting devices in to Microsoft Entra ID can be done in a self-service manner or a controlled process managed by administrators.

Related content

- To get an overview of how to manage device identities, see [Managing device identities](#).
- To learn more about device-based Conditional Access, see [Configure Microsoft Entra device-based Conditional Access policies](#).

Microsoft Entra join a new Windows device during the out of box experience

Article • 04/25/2024

Windows 11 users can join new Windows devices to Microsoft Entra ID during the first-run out-of-box experience (OOBE). This functionality enables you to distribute shrink-wrapped devices to your employees or students.

This functionality pairs well with mobile device management platforms like [Microsoft Intune](#) and tools like [Windows Autopilot](#) to ensure devices are configured according to your standards.

Prerequisites

To Microsoft Entra join a Windows device, the device registration service must be configured to enable you to register devices. For more information about prerequisites, see the article [How to: Plan your Microsoft Entra join implementation](#).

Tip

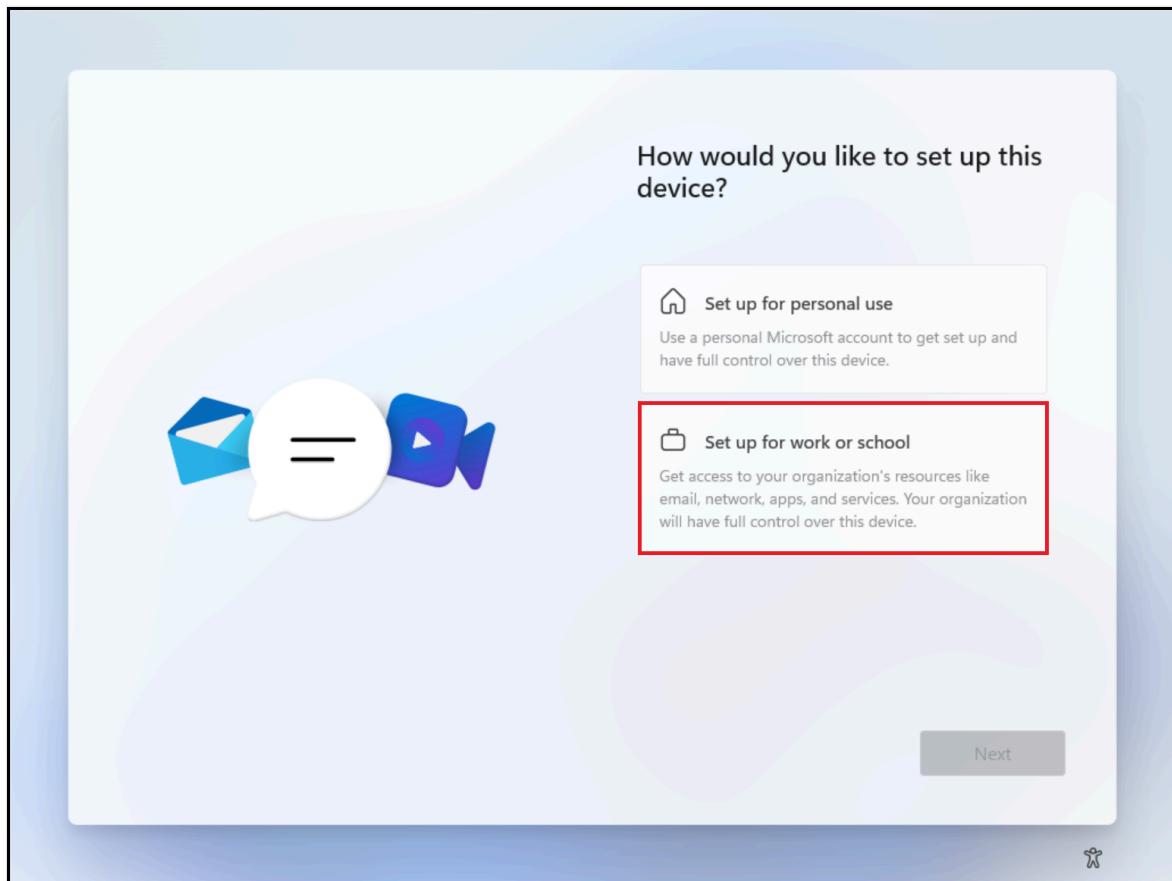
Windows Home Editions do not support Microsoft Entra join. These editions can still access many of the benefits by using [Microsoft Entra registration](#).

For information about how complete Microsoft Entra registration on a Windows device see the support article [Register your personal device on your work or school network](#).

Join a new Windows 11 device to Microsoft Entra ID

Your device might restart several times as part of the setup process. Your device must be connected to the Internet to complete Microsoft Entra join.

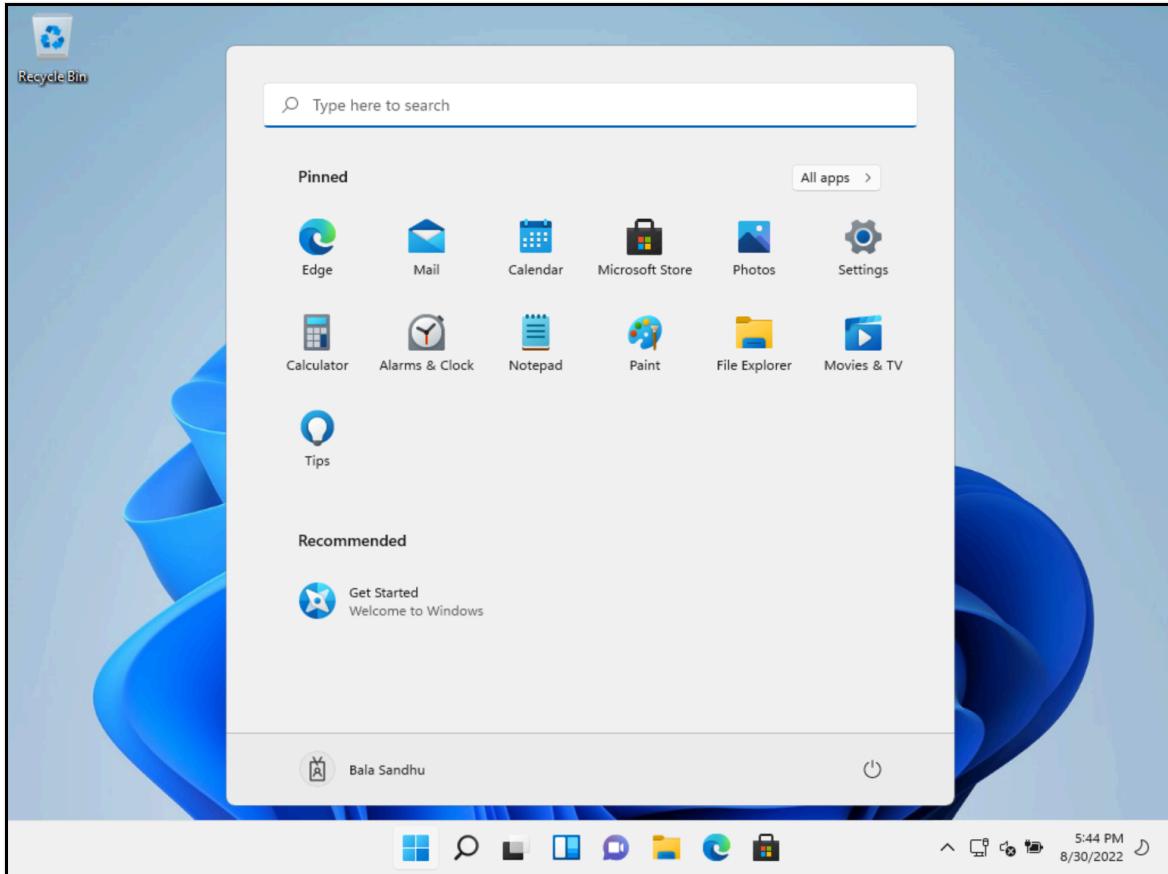
1. Turn on your new device and start the setup process. Follow the prompts to set up your device.
2. When prompted **How would you like to set up this device?**, select **Set up for work or school**.



3. On the **Let's set things up for your work or school** page, provide the credentials that your organization provided.
- Optionally you can choose to **Sign in with a security key** if one was provided to you.
 - If your organization requires it, you might be prompted to perform multifactor authentication.

The screenshot shows the "Let's set things up for your work or school" sign-in page. It features a header with the Microsoft logo and the text "Sign in". Below the header is an input field containing the email address "someone@example.com". Underneath the input field are links for "Sign in with a security key" and "Sign-in options". At the bottom of the page, there is a note about agreeing to Microsoft Services Agreement and privacy statements, followed by a "Next" button.

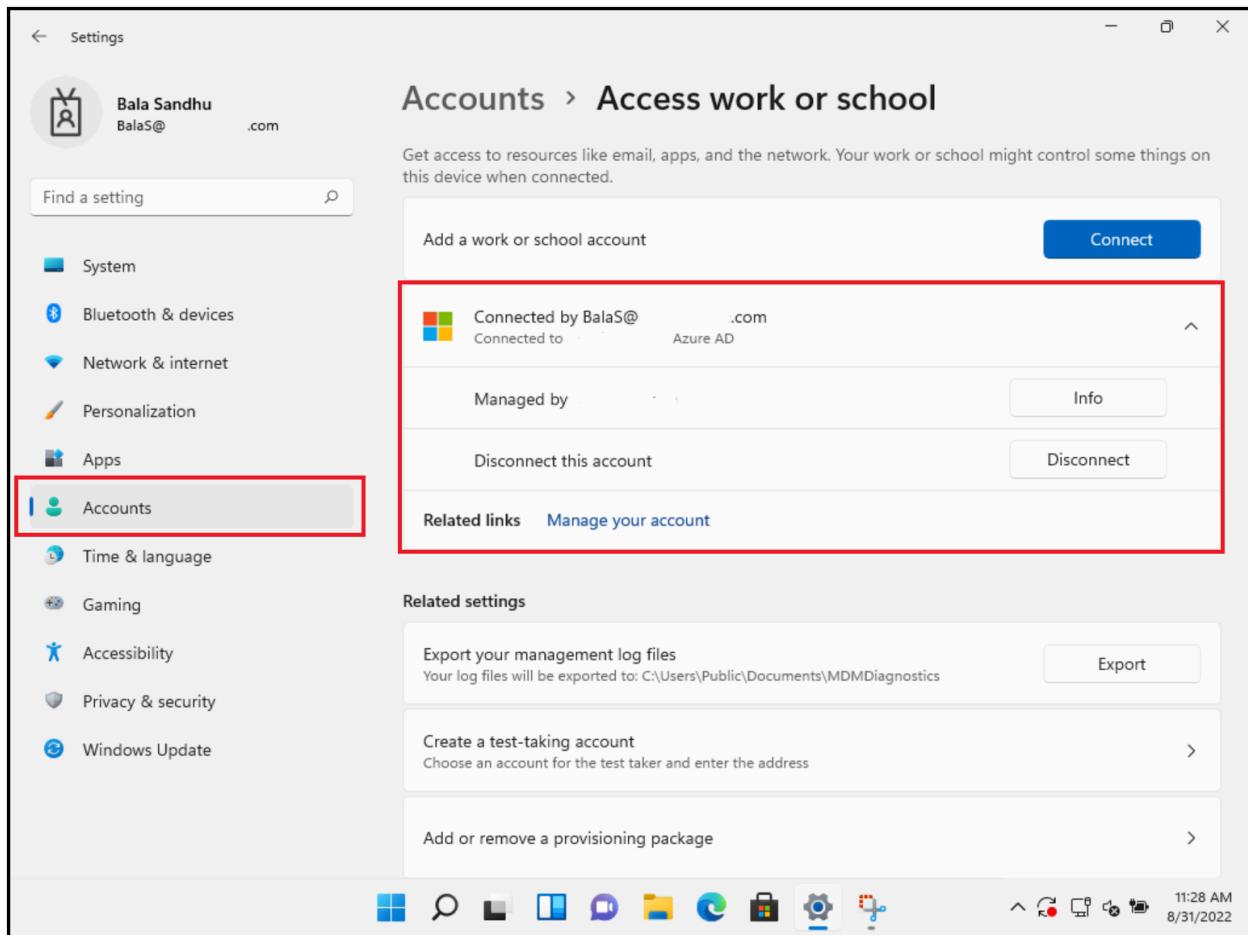
4. Continue to follow the prompts to set up your device.
5. Microsoft Entra ID checks if an enrollment in mobile device management is required and starts the process.
 - a. Windows registers the device in the organization's directory and enrolls it in mobile device management, if applicable.
6. If you sign in with a managed user account, Windows takes you to the desktop through the automatic sign-in process. Federated users are directed to the Windows sign-in screen to enter your credentials.



For more information about the out-of-box experience, see the support article [Join your work device to your work or school network](#).

Verification

To verify whether a device is joined to your Microsoft Entra ID, review the **Access work or school** dialog on your Windows device found in **Settings > Accounts**. The dialog should indicate that you're connected to Microsoft Entra ID, and provides information about areas managed by your IT staff.



Related content

- For more information about managing devices, see [Managing device identities](#).
- [What is Microsoft Intune?](#)
- [Overview of Windows Autopilot](#)
- [Passwordless authentication options for Microsoft Entra ID](#)

Join a Mac device with Microsoft Entra ID during the out of box experience with macOS PSSO (preview)

Article • 12/19/2024

Mac users can join their new device to Microsoft Entra ID during the first-run out-of-box experience (OOBE). The macOS Platform single sign-on (PSSO) is a capability on macOS that is enabled using the [Microsoft Enterprise Single Sign-on Extension](#). PSSO allows users to sign in to a Mac device using a hardware-bound key, smart card or their Microsoft Entra ID password. This tutorial shows you how to set up a Mac device during the OOBEx to use PSSO using Automated Device Enrollment.

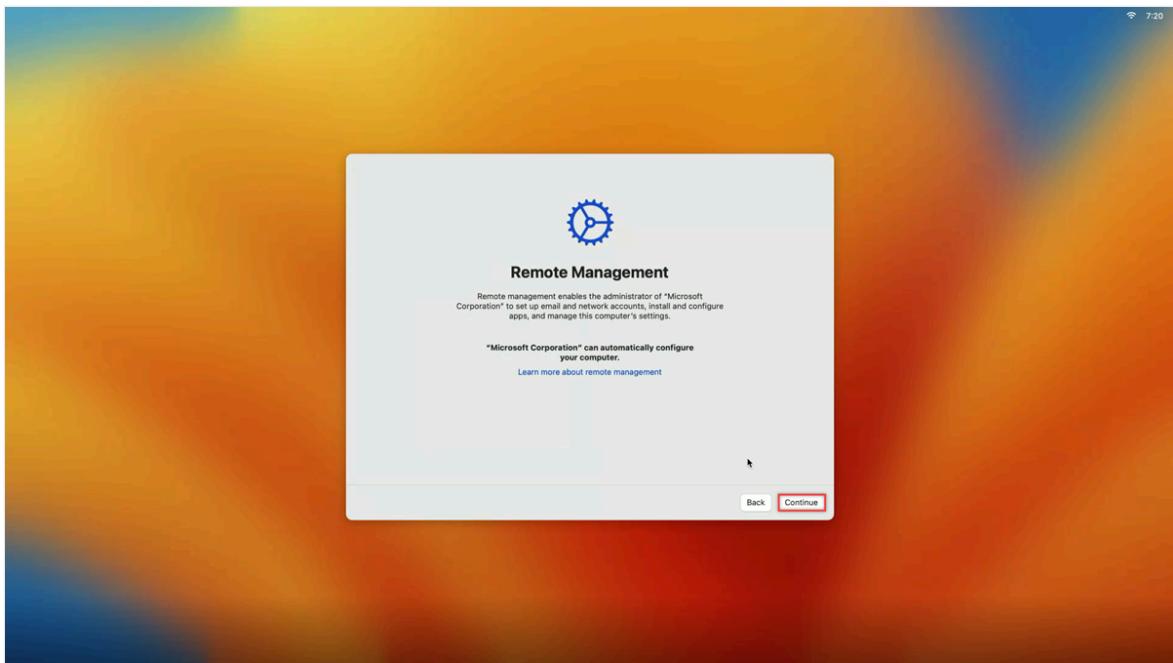
Prerequisites

- A recommended minimum version of macOS 14 Sonoma. While macOS 13 Ventura is supported, we strongly recommend using macOS 14 Sonoma for the best experience.
- A device with [Automated Device Enrollment \(ADE\)](#) enrolled. Check with your administrator if you're unsure if your device is enrolled with this requirement.
- [Microsoft Intune Company Portal](#) version 5.2404.0 or later.
- A Mac device enrolled in mobile device management (MDM) with Microsoft Intune.
- A configured single sign-on (SSO) extension MDM payload with [PSSO settings in Intune](#) by an administrator
- [Microsoft Authenticator](#) (recommended): The user must be registered for some form of Microsoft Entra ID multifactor authentication (MFA) on their mobile device to complete device registration.
- For smart card setup, [certificate based authentication](#) configured and enabled. A smart card loaded with a certificate for authentication with Microsoft Entra and the smart card paired with local account.

Set up your macOS device

1. Upon seeing the "Hello" screen when opening your Mac for the first time, follow the steps to select your country or region, and configure network settings as required.

2. You're prompted to download a **Remote Management** profile, which allows the configuration setup in Microsoft Intune to be applied to your device. Select **Continue**, and enter your Microsoft Entra ID credentials when prompted to approve the management profile download.



3. Enter the code sent to your **Authenticator app** (recommended) or use another MFA method.
4. To create a user account, fill in your full name, account name, and create a local account password. Select **Continue** and your home screen appears.

Create a Computer Account

Fill out the following information to create your computer account.

Full name:

Account name: 

This will be the name of your home folder.

Password:

Hint:

Back

Continue

Registration with Automated Device Enrollment

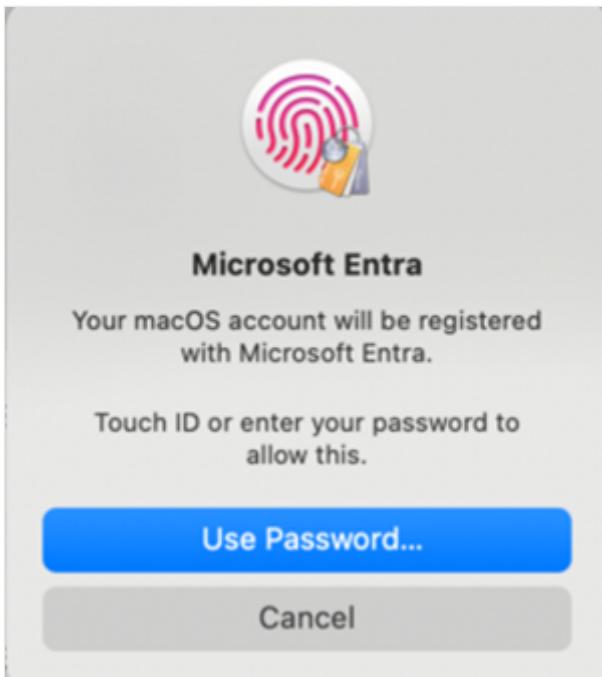
There are three authentication methods for PSSO registration:

- **Secure Enclave:** User logs on to their device which has a secure enclave backed cryptographic key used for SSO across apps that use Microsoft Entra ID for authentication. It can also be referred to as Platform Credential for macOS.
- **Smart card:** User logs into the machine using an external smart card or smart card compatible hard token
- **Password:** User logs on to their local device with a local account, updated to use their Microsoft Entra ID password

Check that your system administrator has the Mac enrolled using secure enclave or smart card. These new passwordless features are supported only by PSSO. Check which authentication method has been set up by your administrator before continuing.

Secure Enclave

1. Navigate to the **Registration Required** popup at the top right of the screen. Hover over the popup and select **Register**. For macOS 14 Sonoma users, you see a prompt to register your device with Microsoft Entra. This prompt doesn't appear for macOS 13 Ventura.



2. A prompt appears to enter your local account password. Enter your password and select **Ok**.
3. Once your account is unlocked, select the account to sign in to, enter your sign-in credentials and select **Next**.
4. MFA is required as part of this sign in flow. Open your **Authenticator app** (recommended) or use your other MFA methods you have registered, and enter the number displayed on the screen to finish registration.
5. When the MFA flow completes and the loading screen disappears, your device should be registered with PSSO. You can now use PSSO to access Microsoft app resources.

Enable Platform Credential for macOS for use as a passkey

Setting up your device using secure enclave method enables you to use the resulting credential saved to the Mac as a passkey in the browser. To enable it;

1. Open the **Settings** app, and navigate to **Passwords > Password options**.
2. Under **Password Options**, find **Use passwords and passkeys from** and enable **Company Portal** through the toggle switch.



Check your device registration status

Once you've completed the steps above, it's a good idea to check your device registration status.

1. To check that registration has completed successfully, navigate to **Settings** and select **Users & Groups**.
2. Select **Edit** next to **Network Account Server** and check that **Platform SSO** is listed as **Registered**.
3. To verify the method used for authentication, navigate to your username in the **Users & Groups** window and select the **Information** icon. Check the method listed, which should be **Secure enclave**, **Smart Card**, or **Password**.

ⓘ Note

You can also use the **Terminal** app to check the registration status. Run the following command to check the status of your device registration. You

should see in the bottom of the output that SSO tokens are retrieved. For macOS 13 Ventura users, this command is required to check the registration status.

Console

```
app-sso platform -s
```

See also

- [Join a Mac device with Microsoft Entra ID using Company Portal](#)
- [Passwordless authentication options for Microsoft Entra ID](#)
- [Plan a passwordless authentication deployment in Microsoft Entra ID](#)
- [Microsoft Enterprise SSO plug-in for Apple devices](#)

Feedback

Was this page helpful?

 Yes

 No

[Provide product feedback ↗](#)

Join a Mac device with Microsoft Entra ID using Company Portal (preview)

Article • 12/19/2024

In this tutorial, you learn how to register a Mac device with macOS Platform Single Sign-on (PSSO) using Company Portal and the Intune MDM enrollment with Microsoft Entra Join. There are three methods in which you can register a Mac device with PSSO, secure enclave, smart card, or password. We recommend using secure enclave or smart card for the best passwordless experience, however it's important to note that this method will be preset by your company administrator using Microsoft Intune.

Prerequisites

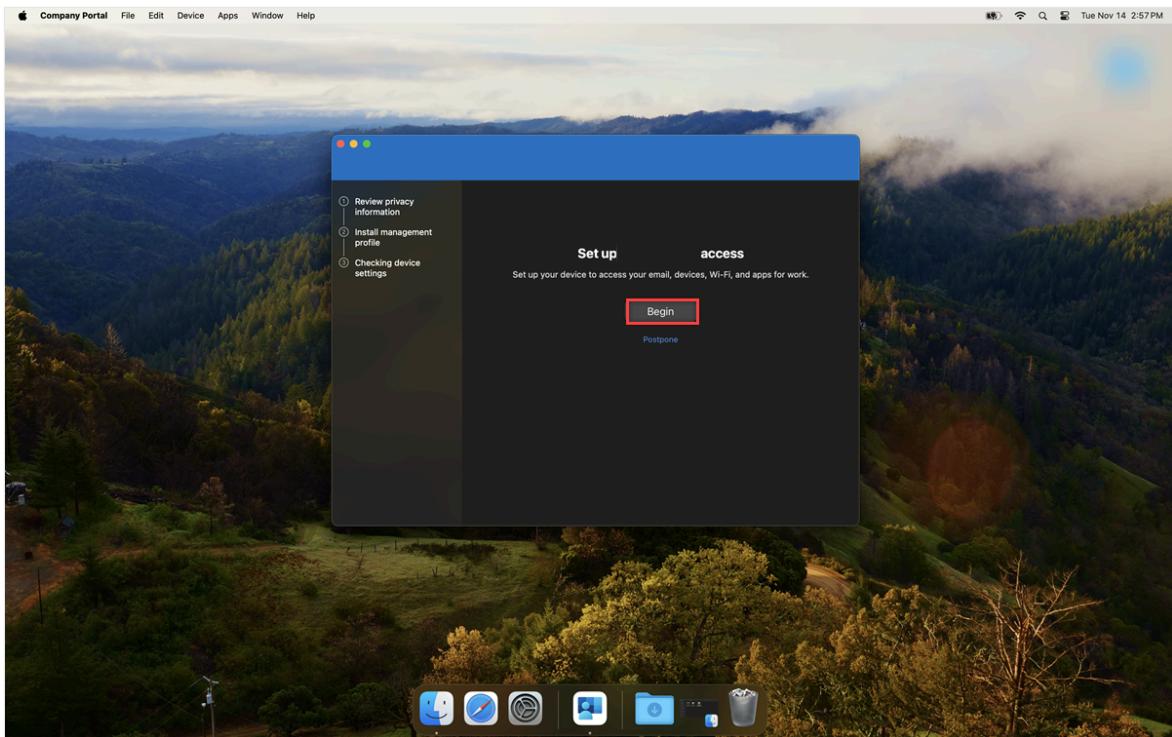
- A recommended minimum version of macOS 14 Sonoma. While macOS 13 Ventura is supported, we strongly recommend using macOS 14 Sonoma for the best experience.
- Microsoft Intune [Company Portal app](#) version 5.2404.0 or later
- A Mac device enrolled in mobile device management (MDM) with [Microsoft Intune](#).
- A configured SSO extension MDM payload with PSSO settings in Intune by an administrator
- [Microsoft Authenticator](#) (recommended), the user must be registered for some form of Microsoft Entra ID multifactor authentication (MFA) to complete device registration.
- For smart card setup, [certificate based authentication](#) configured and enabled. A smart card loaded with a certificate for authentication with Microsoft Entra and the smart card paired with local account.

Intune MDM and Microsoft Entra Join using Company Portal

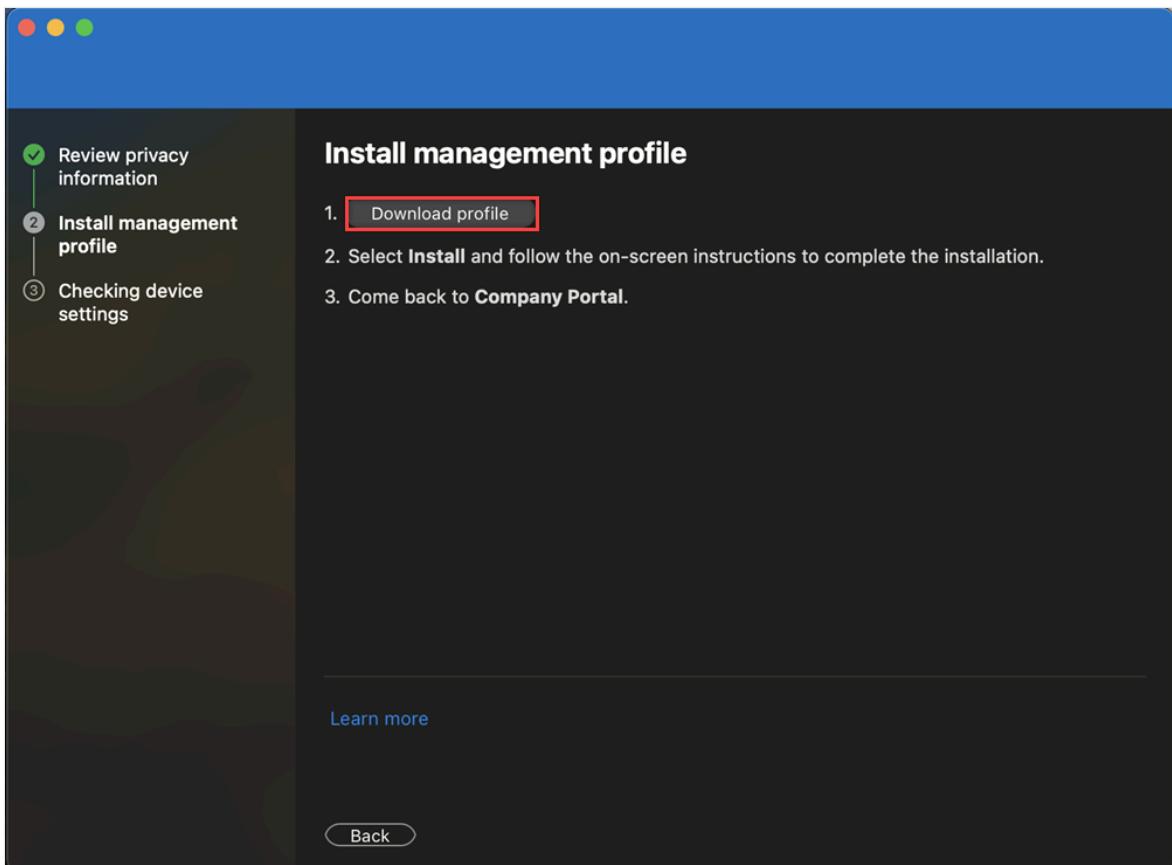
To register a Mac device with PSSO, you must first enroll your device in Microsoft Intune using the Company Portal app. Once enrolled, you can use secure enclave, smart card, or password to register your device with PSSO.

1. Open the [Company Portal](#) app and select **Sign in**.
2. Enter your Microsoft Entra ID credentials and select **Next**.

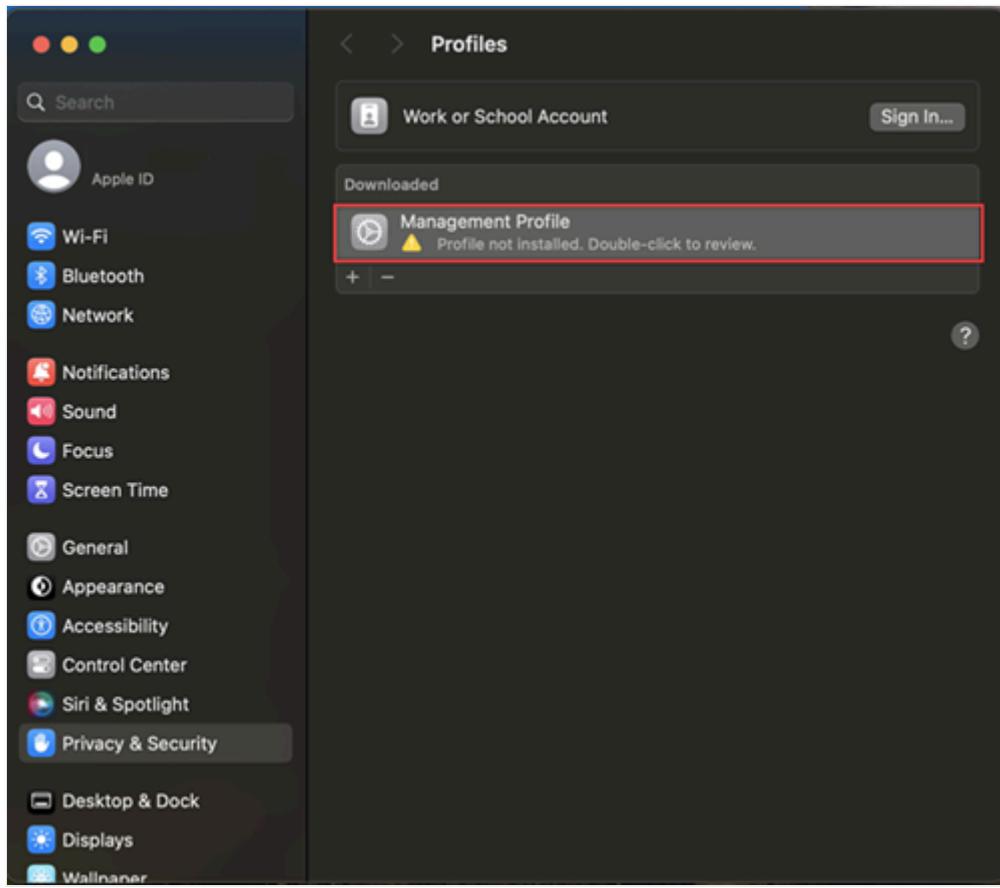
3. You're prompted to **Set up {Company} access**. The placeholder "Company" is different depending on your setup. Select **Begin**, then on the next screen, select **Continue**.



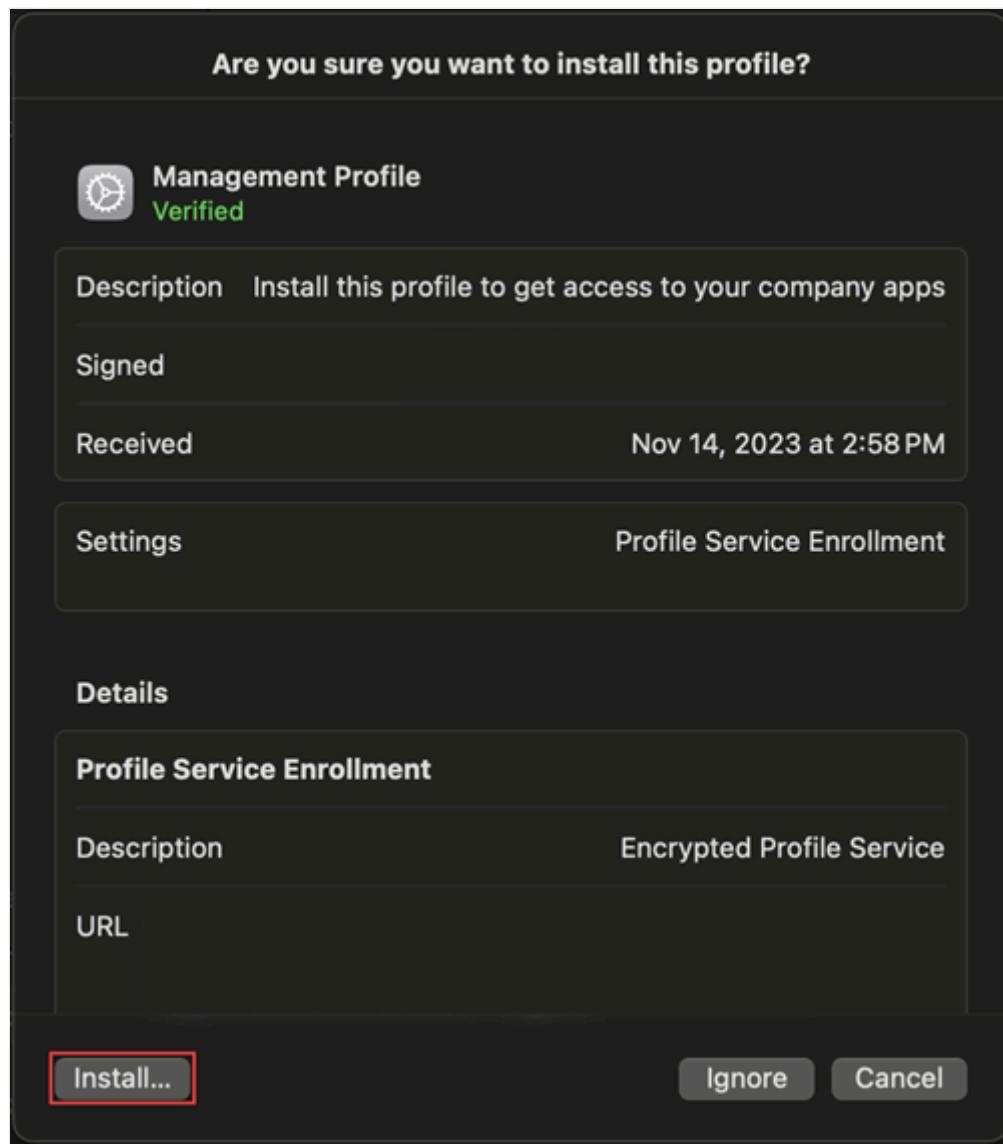
4. You're presented with steps to install the management profile. The management profile should have been set up by an administrator using Microsoft Intune. Select **Download profile**.



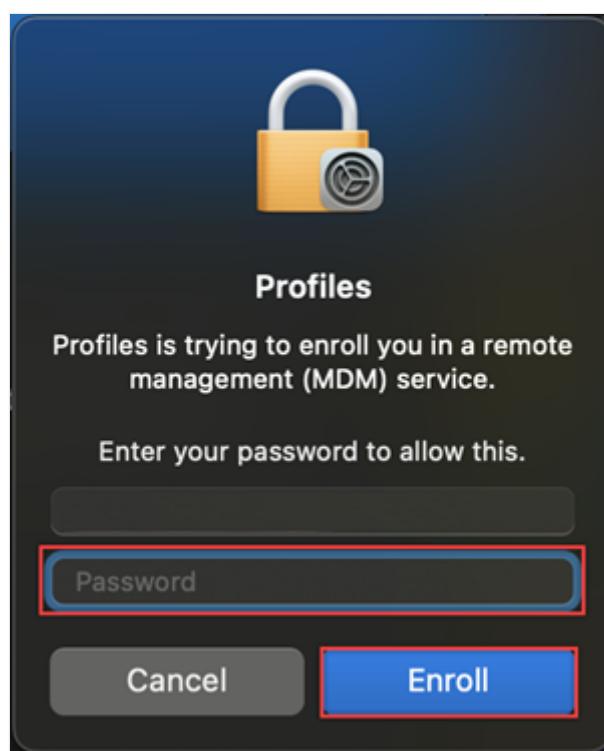
5. Open Settings > Privacy & Security > Profiles if it doesn't automatically appear.
Select Management Profile.



6. Select **Install** to get access to company resources.



7. Enter your local device password in the **Profiles** window that appears and select **Enroll**.



8. You see a notification in **Company Portal** that the installation is complete. Select **Done**.

Platform SSO registration

Now that the device is in compliance with Company Portal, you need to register your device with PSSO. A **Registration Required** popup appears at the top right of the screen following successful completion of [Intune MDM and Microsoft Entra Join using Company Portal](#). Use the tabs to register your device with PSSO using secure enclave, smart card, or password.

Secure Enclave

1. Navigate to the **Registration Required** popup at the top right of the screen. Hover over the popup and select **Register**. For macOS 14 Sonoma users, you see a prompt to register your device with Microsoft Entra. This prompt doesn't appear for macOS 13 Ventura.



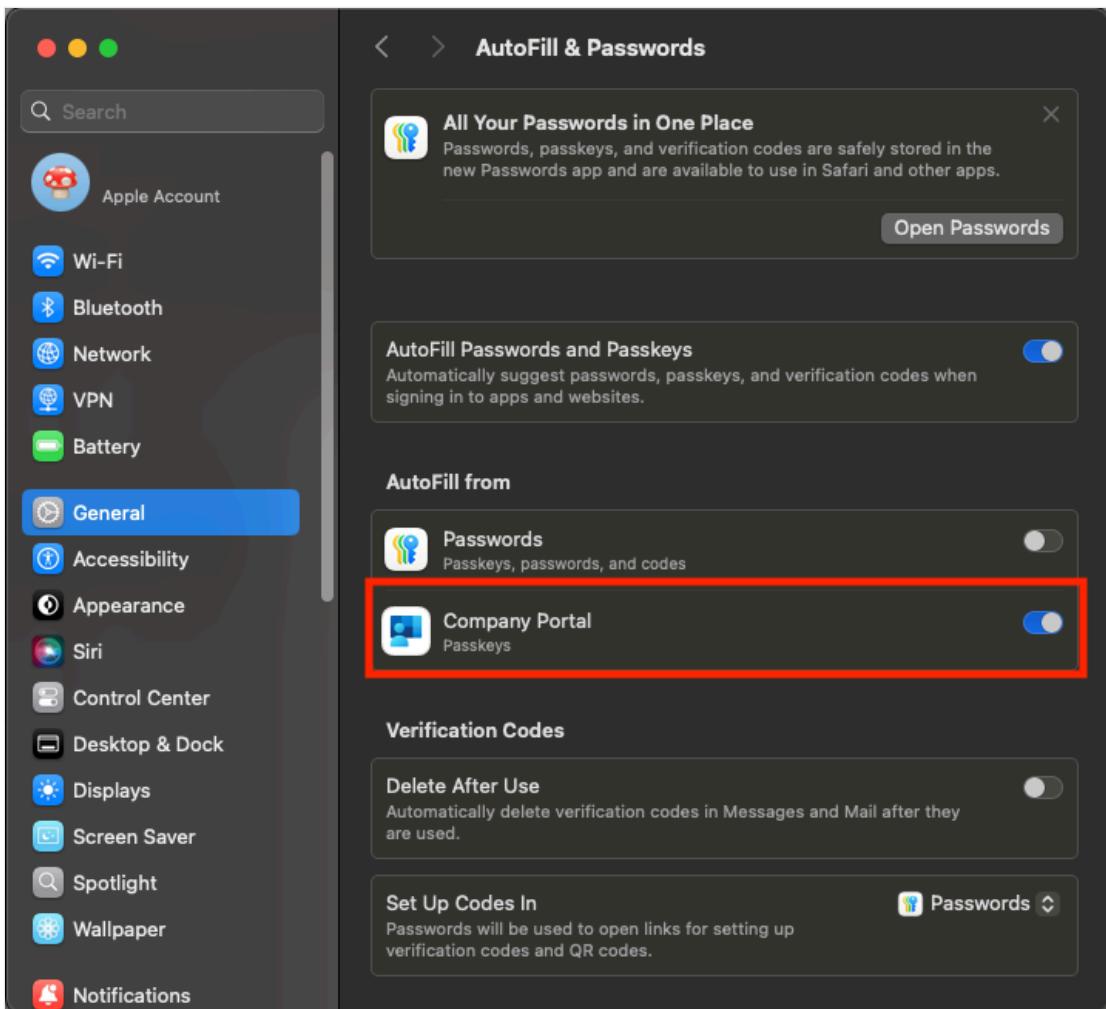
2. Once your account is unlocked with Touch ID or password, select the account to sign in to, enter your sign-in credentials and select **Next**.
3. MFA is required as part of this sign in flow. Open your **Authenticator app** (recommended) or use your other MFA methods you have registered, and enter the number displayed on the screen to finish registration.
4. When the MFA flow completes and the loading screen disappears, your device should be registered with PSSO. You can now use PSSO to access Microsoft

app resources.

Enable Platform Credential for macOS for use as a passkey

Setting up your device using secure enclave method enables you to use the resulting credential saved to the Mac as a passkey in the browser. To enable it;

1. Open the **Settings** app, and navigate to **General > Autofill & Passwords**.
2. Under **Autofill & Passwords**, find **Autofill from** and enable **Company Portal** through the toggle switch.



Check your device registration status

Once you've completed the steps above, it's a good idea to check your device registration status.

1. To check that registration has completed successfully, navigate to **Settings** and select **Users & Groups**.
2. Select **Edit** next to **Network Account Server** and check that **Platform SSO** is listed as **Registered**.
3. To verify the method used for authentication, navigate to your username in the **Users & Groups** window and select the **Information** icon. Check the method listed, which should be **Secure enclave, Smart Card, or Password**.

 **Note**

You can also use the **Terminal** app to check the registration status. Run the following command to check the status of your device registration. You should see in the bottom of the output that SSO tokens are retrieved. For macOS 13 Ventura users, this command is required to check the registration status.

Console

```
app-sso platform -s
```

Update your Mac device to enable PSSO

For macOS users whose device is already enrolled in Company Portal, your administrator can enable PSSO by updating your device's SSO extension profile. Once the PSSO profile is deployed and installed on your device, you're prompted to register your device with PSSO via the **Registration Required** notification at the top right of the screen. This removes the old SSO registration from your device in place of the new PSSO registration.

Although it's recommended to do it immediately, you can choose to select this and start your device registration at a time convenient to you.

See also

- [Join a Mac device with Microsoft Entra ID during the out of box experience](#)
- [Passwordless authentication options for Microsoft Entra ID](#)
- [Plan a passwordless authentication deployment in Microsoft Entra ID](#)
- [Microsoft Enterprise SSO plug-in for Apple devices](#)

Feedback

Was this page helpful?

 Yes

 No

Provide product feedback ↗

Join a Mac device with Microsoft Entra ID and configure it for shared device scenarios (Preview)

Article • 11/05/2024

In this tutorial, you will learn how to configure a Microsoft Entra Joined Mac via Mobile Device Management (MDM) to support multiple users. There are three methods in which you can register a Mac device with Platform SSO (PSSO), secure enclave, smart card, or password. We recommend using secure enclave or smart card for the best passwordless experience, however shared or multi-user Macs may benefit from using the password method instead. Common scenarios for shared Macs with passwords would be computer labs in schools or universities. In these scenarios, students use multiple devices, multiple students use the same device, and they only have passwords and no MFA or passwordless credentials.

Prerequisites

- A required minimum version of macOS 14 Sonoma or later. While macOS 13 Ventura is supported for Platform SSO overall, only Sonoma supports the necessary tools for the Platform SSO shared Mac scenario described in this guide.
- Microsoft Intune [Company Portal app](#) version 5.2404.0 or later.
- A configured Platform SSO MDM payload in your MDM by an administrator.

MDM configuration

There are three main steps for configuring Platform SSO on a shared device:

1. **Deploy Company Portal.** For more information, see [Add the Company Portal for macOS app](#).
2. **Deploy Platform SSO Configuration.** Create and deploy a settings catalog profile with the required Platform SSO Configuration.
3. **Deploy macOS Login Screen Configuration.** The macOS Login screen configuration can be changed to allow new users to log in.

Platform SSO profile configuration

Your Platform SSO MDM profile should apply the following configurations to support multi-user devices:

[\[+\] Expand table](#)

Configuration Parameter	Value(s)	Note
Screen Locked Behavior	Do Not Handle	Required
Registration Token	{{DEVICEREGISTRATION}}	Recommended for the best registration user experience
Authentication Method	Password	Recommended for this article, secure enclave key is recommended for single user devices
Enable Authorization	Enabled	Required
Enable Create User At Login	Enabled	Required
New User Authorization Mode	Standard	Recommended
Token To User Mapping --> Account Name	preferred_username	Required
Token To User Mapping --> Full Name	name	Required
Use Shared Device Keys	Enabled	Required
User Authorization Mode	Standard	Recommended
Team Identifier	UBF8T346G9	Required
Extension Identifier	com.microsoft.CompanyPortalMac.ssoextension	Required
Type	Redirect	Required

Configuration Parameter	Value(s)	Note
URLs	https://login.microsoftonline.com , https://login.microsoft.com , https://sts.windows.net , https://login.partner.microsoftonline.cn , https://login.chinacloudapi.cn , https://login.microsoftonline.us , https://login-us.microsoftonline.com	Required

If you use Intune as your MDM of choice, then the configuration profile settings will appear like this:

^ Authentication

Extensible Single Sign On (SSO)

Configure an app extension that enables single sign-on (SSO) for devices.

Screen Locked Behavior ⓘ	Do Not Handle
Registration Token ⓘ	{{DEVICEREGISTRATION}}
Platform SSO ⓘ	
Authentication Method ⓘ	Password
Enable Authorization ⓘ	Enabled
Enable Create User At Login ⓘ	Enabled
New User Authorization Mode ⓘ	Standard
Token To User Mapping ⓘ	
Account Name ⓘ	preferred_username
Full Name ⓘ	name
Use Shared Device Keys ⓘ	Enabled
User Authorization Mode ⓘ	Standard
Team Identifier ⓘ	UBF8T346G9
Extension Identifier ⓘ	com.microsoft.CompanyPortalMac.ssoextension
Type ⓘ	Redirect
URLs ⓘ	https://login.microsoftonline.com , https://login.microsoft.com , https://sts.windows.net , https://login.partner.microsoftonline.cn , https://login.chinacloudapi.cn , https://login.microsoftonline.us , https://login-us.microsoftonline.com

macOS login screen configuration

To allow new users to log on and be created from the macOS login screen, there are two configurations that can be used:

- **Show Other Users Managed.** With this configuration, the macOS login screen shows a list of profiles that have been created and an "other user" button that can be used to log in with a username and password. Users can select their existing profile to log in or log in with their Microsoft Entra ID user principal name (UPN).
- **Show full name.** With this configuration, the macOS login screen displays a username and password field with no list of users. Users can log in with their Microsoft Entra ID UPN.

These configurations can be found in Intune Settings Catalog under **Login > Login Window Behavior**.

Enrolling and registering devices

To register a Mac device with Platform SSO, devices must be enrolled into MDM. For shared devices, the user who sets up the device would typically be an administrator or technician - this user will have local administrative rights unless there is alternative local admin account created.

ⓘ Note

If you are enrolling using Automated Device Enrollment you may choose to encourage the user setting up the device to create the local account as:

- **Account name:** Microsoft Entra ID username (eg. user@domain.com).
- **Full Name:** First and Last Name. This is because the local account that is created during setup assistant will be associated with the Microsoft Entra ID account during registration.

There are three high-level steps to set up Platform SSO on a shared device:

1. IT admin or delegated person enrolls device with Intune.
2. IT admin or delegated person registers the device with Microsoft Entra ID using their credentials.
3. Now the device is ready for new users to log in from the Microsoft Entra ID login screen.

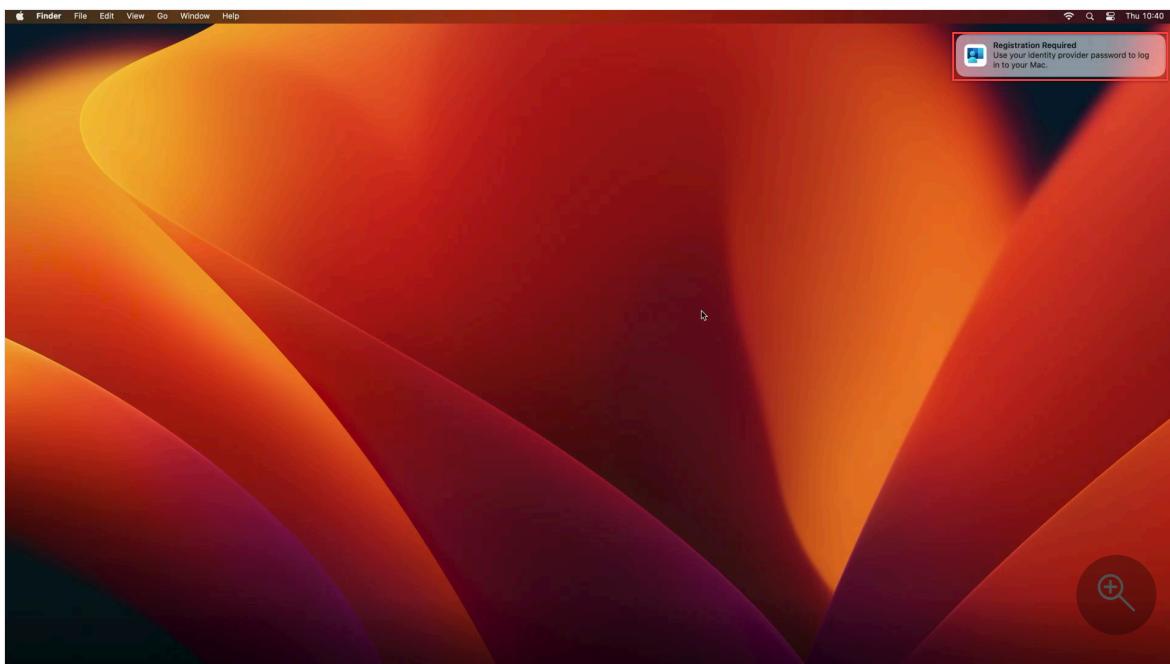
Organizations can enroll shared devices into Intune using different methods depending on the device ownership.

Enrollment method	Device Ownership	Requirements
Automated Device Enrollment with no user affinity	Company or school owned	✓ Registration in Apple Business Manager ✓ Automated Device Enrollment configured in Intune
Company Portal	Personal	None

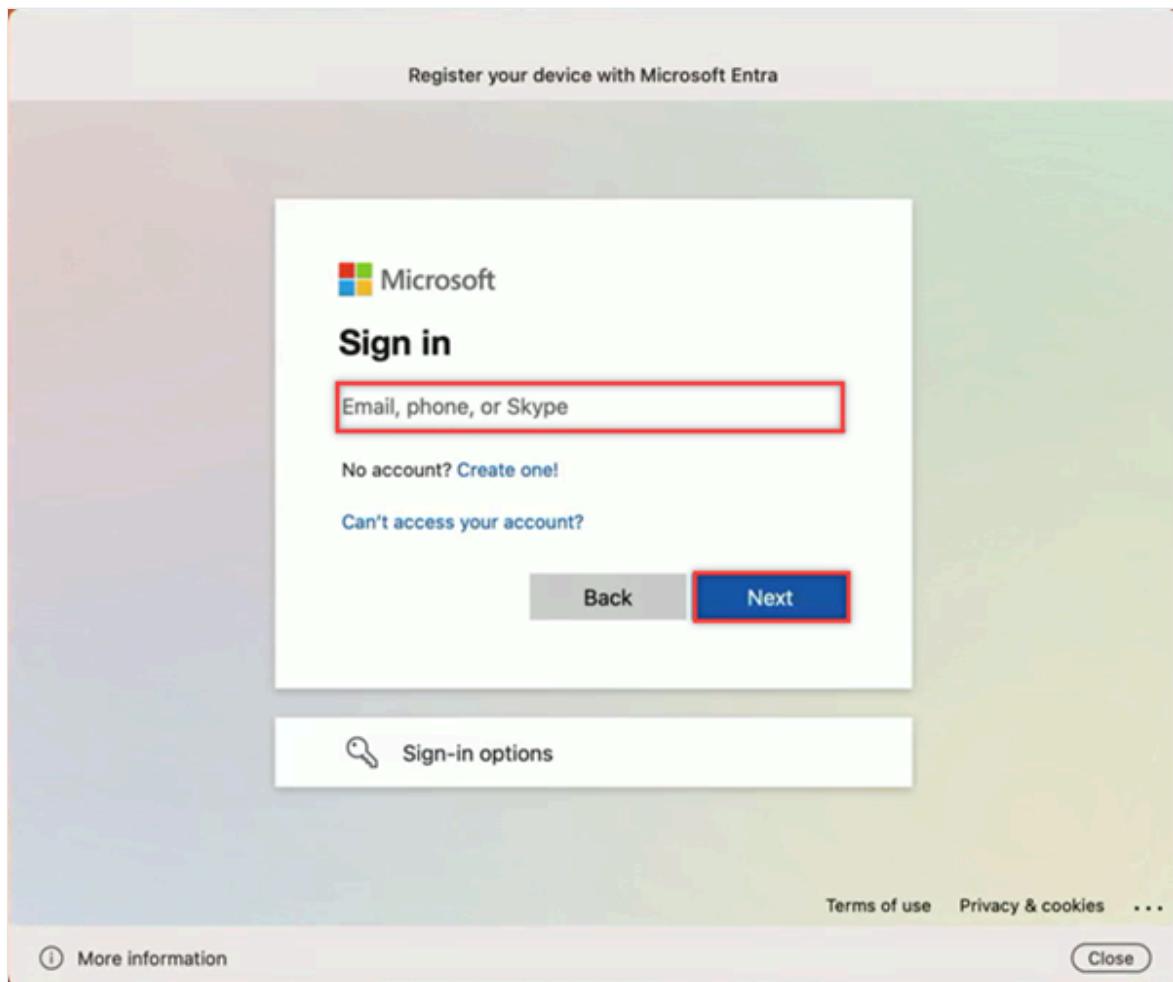
Platform SSO registration

Once the device is MDM enrolled and has Company Portal installed, you need to register your device with Platform SSO. A **Registration Required** popup appears at the top right of the screen. Use the popup to register your device with Platform SSO using your Microsoft Entra ID credentials:

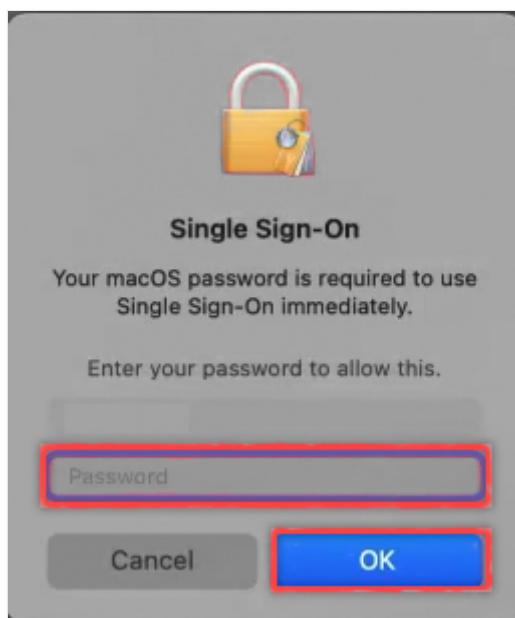
1. Navigate to the **Registration Required** popup at the top right of the screen. Hover over the popup and select **Register**.



2. You're prompted to register your device with Microsoft Entra ID. Enter your sign-in credentials and select **Next**.
 - a. Your administrator may have configured MFA for the device registration flow. If so, open your **Authenticator** app on your mobile device and complete the MFA flow.



- When a Single Sign-On window appears, enter your local account password and select OK.



- If your local password differs to your Microsoft Entra ID password, an **Authentication Required** popup appears on the top right of the screen. Hover over the banner and select **Sign-in**.

- When a Microsoft Entra window appears, enter your Microsoft Entra ID password and select **Sign In**.



- After unlocking the Mac, you can now use Platform SSO to access Microsoft app resources. From this point on, your old password doesn't work because Platform SSO is enabled for your device.

Check your device registration status

After completing the steps above, it's recommended to check your device registration status.

- To check that registration has completed successfully, navigate to **Settings** and select **Users & Groups**.
- Select **Edit** next to **Network Account Server** and check that **Platform SSO** is listed as **Registered**.
- To verify the method used for authentication, navigate to your username in the **Users & Groups** window and select the **Information** icon. Check the method listed, which should be **Secure enclave**, **Smart Card**, or **Password**.

ⓘ Note

You can also use the **Terminal** app to check the registration status. Run the following command to check the status of your device registration. You should see in the bottom of the output that SSO tokens are retrieved. For macOS 13 Ventura users, this command is required to check the registration status.

Console

```
app-sso platform -s
```

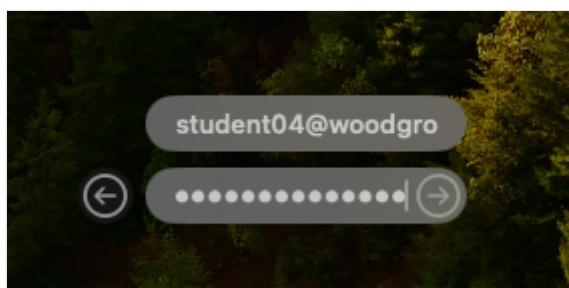
Test the Enable Create User At Login Functionality

Next you should validate that the device is ready for other users in the tenant to log into it.

1. Log out of the Mac with the account that you used to do the initial setup.
2. At the login screen, choose the **Other...** option to sign in with a new user account



3. Enter a user's Microsoft Entra ID User Principal Name and password.



4. If the User Principal Name and password were correct then the user will be logged in. The user is directed to go through several Setup Assistant dialog screens by default and then they land on the macOS desktop.

Troubleshooting

If the user cannot sign in successfully, then use the following resources to troubleshoot:

1. Refer to the [macOS Platform single sign-on known issues and troubleshooting guide](#)
2. Validate that the user can successfully sign in to Microsoft Entra ID using their User Principal Name and password in a browser on another device. You can test by having the user go to a web app, such as <https://myapps.microsoft.com>

See also

- [Join a Mac device with Microsoft Entra ID during the out of box experience](#)
- [Passwordless authentication options for Microsoft Entra ID](#)
- [Plan a passwordless authentication deployment in Microsoft Entra ID](#)
- [Microsoft Enterprise SSO plug-in for Apple devices](#)

Feedback

Was this page helpful?

 Yes

 No

[Provide product feedback](#)

Enable Kerberos SSO to on-premises Active Directory and Microsoft Entra ID Kerberos resources in Platform SSO

Article • 05/08/2025

Mac users can join their new device to Microsoft Entra ID during the first-run out-of-box experience (OOBE). The macOS Platform single sign-on (PSSO) is a capability on macOS that is enabled using the [Microsoft Enterprise Single Sign-on Extension](#). PSSO allows users to sign in to a Mac device using a hardware-bound key, smart card, or their Microsoft Entra ID password.

This tutorial shows you how to configure Platform SSO to support Kerberos-based SSO to on-premises and cloud resources, in addition to SSO to Microsoft Entra ID. Kerberos SSO is an optional capability within Platform SSO, but it's recommended if users still need to access on-premises Active Directory resources that use Kerberos for authentication.

Prerequisites

- A minimum version of [macOS 14.6 Sonoma](#).
- [Microsoft Intune Company Portal](#) version 5.2408.0 or later
- A Mac device enrolled in mobile device management (MDM).
- A configured SSO extension MDM payload with Platform SSO settings by an administrator, already deployed to the device. Refer to the [Platform SSO documentation](#) or [Intune deployment guide](#) if Intune is your MDM.
- Deploy Microsoft Entra Kerberos, which is required for some Kerberos capabilities in on-premises Active Directory. For more information, see the [Cloud Kerberos trust deployment guide for Windows Hello for Business](#) or refer directly to the [Cloud Kerberos trust configuration instructions](#) to begin the setup. If you have already deployed Windows Hello for Business with Cloud Kerberos trust or passwordless security key sign-in for Windows, then this step has already been completed.

Set up your macOS device

Refer to the [Microsoft Entra ID macOS Platform SSO documentation](#) to configure and deploy Platform SSO. Platform SSO should be deployed on Enterprise-managed Macs regardless of whether you choose to deploy Kerberos SSO using this guide.

Kerberos SSO MDM profile configuration for on-premises Active Directory

You should configure separate Kerberos SSO MDM profiles if you plan to use both Microsoft Entra ID Cloud Kerberos and on-premises Active Directory realms. It's recommended to deploy on-premises Active Directory profile before the Microsoft Entra ID Cloud Kerberos profile.

Use the following settings to configure the on-premises Active Directory profile, ensuring that you replace all references to **contoso.com** and **Contoso** with the proper values for your environment:

[] Expand table

Configuration Key	Recommended Value	Note
Hosts	<string>.contoso.com</string>	Replace contoso.com with your on-premises domain/forest name
Hosts	<string>contoso.com</string>	Replace contoso.com with your on-premises domain/forest name. Keep the preceding . characters before your domain/forest name
Realm	<string>CONTOSO.COM</string>	Replace CONTOSO.COM with your on-premises realm name. The value should be all capitalized.
PayloadOrganization	<string>Contoso</string>	Replace Contoso with the name of your organization

XML

```
<?xml version="1.0" encoding="UTF-8"?>
<!DOCTYPE plist PUBLIC "-//Apple//DTD PLIST 1.0//EN"
"http://www.apple.com/DTDs/PropertyList-1.0.dtd">
<plist version="1.0">
<dict>
  <key>PayloadContent</key>
  <array>
    <dict>
      <key>ExtensionData</key>
      <dict>
        <key>allowPasswordChange</key>
        <true/>
        <key>allowPlatformSSOAuthFallback</key>
        <true/>
        <key>performKerberosOnly</key>
        <true/>
        <key>pwReqComplexity</key>
        <true/>
        <key>syncLocalPassword</key>
        <false/>
        <key>usePlatformSSOTGT</key>
        <true/>
      </dict>
    </array>
  </dict>
</plist>
```

```

<key>ExtensionIdentifier</key>
<string>com.apple.AppSSOKerberos.KerberosExtension</string>
<key>Hosts</key>
<array>
    <string>.contoso.com</string>
    <string>contoso.com</string>
</array>
<key>Realm</key>
<string>CONTOSO.COM</string>
<key>PayloadDisplayName</key>
<string>Single Sign-On Extensions Payload for On-Premises</string>
<key>PayloadType</key>
<string>com.apple.extensiblesso</string>
<key>PayloadUUID</key>
<string>1aaaaaaaa1-2bb2-3cc3-4dd4-5eeeeeeeeee5</string>
<key>TeamIdentifier</key>
<string>apple</string>
<key>Type</key>
<string>Credential</string>
</dict>
</array>
<key>PayloadDescription</key>
<string></string>
<key>PayloadDisplayName</key>
<string>Kerberos SSO Extension for macOS for On-Premises</string>
<key>PayloadEnabled</key>
<true/>
<key>PayloadIdentifier</key>
<string>2bbbbbb2-3cc3-4dd4-5ee5-6fffffffff6</string>
<key>PayloadOrganization</key>
<string>Contoso</string>
<key>PayloadRemovalDisallowed</key>
<true/>
<key>PayloadScope</key>
<string>System</string>
<key>PayloadType</key>
<string>Configuration</string>
<key>PayloadUUID</key>
<string>2bbbbbb2-3cc3-4dd4-5ee5-6fffffffff6</string>
<key>PayloadVersion</key>
<integer>1</integer>
</dict>
</plist>

```

Save the configuration using a text editor with the *mobileconfig* file extension (for example, the file could be named *on-prem-kerberos.mobileconfig*) after updating the configuration with the proper values for your environment.

Kerberos SSO MDM profile configuration for Microsoft Entra ID Cloud Kerberos

You should configure separate Kerberos SSO MDM profiles if you plan to use both Microsoft Entra ID Cloud Kerberos and on-premises Active Directory realms. It's recommended to deploy on-premises Active Directory profile before the Microsoft Entra ID Cloud Kerberos profile.

Use the following settings to configure the Microsoft Entra ID Cloud Kerberos profile, ensuring that you replace all references with the proper values for your tenant:

[+] Expand table

Configuration Key	Recommended Value	Note
preferredKDCs	<string>kkdcp://login.microsoftonline.com/aaaabbbb-0000-cccc-1111-dddd2222eeee/kerberos</string>	Replace the aaaabbbb-0000-cccc-1111-dddd2222eeee value with the Tenant ID of your tenant, which can be found on the Overview page of the Microsoft Entra Admin Center
PayloadOrganization	<string>Contoso</string>	Replace Contoso with the name of your organization

XML

```
<?xml version="1.0" encoding="UTF-8"?>
<!DOCTYPE plist PUBLIC "-//Apple//DTD PLIST 1.0//EN"
"http://www.apple.com/DTDs/PropertyList-1.0.dtd">
<plist version="1.0">
<dict>
  <key>PayloadContent</key>
  <array>
    <dict>
      <key>ExtensionData</key>
      <dict>
        <key>usePlatformSSOTGT</key>
        <true/>
        <key>performKerberosOnly</key>
        <true/>
        <key>preferredKDCs</key>
        <array>
          <string>kkdcp://login.microsoftonline.com/aaaabbbb-0000-cccc-1111-
dddd2222eeee/kerberos</string>
        </array>
      </dict>
      <key>ExtensionIdentifier</key>
      <string>com.apple.AppSSOKerberos.KerberosExtension</string>
      <key>Hosts</key>
```

```

<array>
    <string>windows.net</string>
    <string>.windows.net</string>
</array>
<key>Realm</key>
<string>KERBEROS.MICROSOFTONLINE.COM</string>
<key>PayloadDisplayName</key>
<string>Single Sign-On Extensions Payload for Microsoft Entra ID Cloud
Kerberos</string>
    <key>PayloadType</key>
    <string>com.apple.extensiblesso</string>
    <key>PayloadUUID</key>
    <string>00aa00aa-bb11-cc22-dd33-44ee44ee44ee</string>
    <key>TeamIdentifier</key>
    <string>apple</string>
    <key>Type</key>
    <string>Credential</string>
</dict>
</array>
<key>PayloadDescription</key>
<string></string>
<key>PayloadDisplayName</key>
<string>Kerberos SSO Extension for macOS for Microsoft Entra ID Cloud
Kerberos</string>
    <key>PayloadEnabled</key>
    <true/>
    <key>PayloadIdentifier</key>
    <string>11bb11bb-cc22-dd33-ee44-55ff55ff55ff</string>
    <key>PayloadOrganization</key>
    <string>Contoso</string>
    <key>PayloadRemovalDisallowed</key>
    <true/>
    <key>PayloadScope</key>
    <string>System</string>
    <key>PayloadType</key>
    <string>Configuration</string>
    <key>PayloadUUID</key>
    <string>11bb11bb-cc22-dd33-ee44-55ff55ff55ff</string>
    <key>PayloadVersion</key>
    <integer>1</integer>
</dict>
</plist>

```

Save the configuration using a text editor with the *mobileconfig* file extension (for example, the file could be named *cloud-kerberos.mobileconfig*) after updating the configuration with the proper values for your environment.

Note

Make sure you pay attention to the `usePlatformSSOTGT` and `performKerberosOnly` keys. If `usePlatformSSOTGT` is set to true, the Kerberos Extension uses the TGT from Platform SSO

with the same realm. The default is false. If `performKerberosOnly` is set to true, the Kerberos extension doesn't perform password expiration checks, external password change checks, or retrieve the user's home directory. The default is false. This is applicable to both the on-premises and cloud configurations, these keys should be configured in both profiles.

Intune configuration steps

If you use Intune as your MDM, you can perform the following steps to deploy the profile. Make sure you follow the [previous instructions](#Kerberos SSO MDM profile configuration for on-premises Active Directory) about replacing `contoso.com` values with the proper values for your organization.

1. Sign in to the [Microsoft Intune admin center](#).
2. Select **Devices > Configuration > Create > New policy**.
3. Enter the following properties:
 - **Platform:** Select `macOS`.
 - **Profile type:** Select `Templates`.
4. Choose the `Custom` template and select **Create**.
5. In **Basics**, enter the following properties:
 - **Name:** Enter a descriptive name for the policy. Name your policies so you can easily identify them later. For example, name the policy `macOS - Platform SSO Kerberos`.
 - **Description:** Enter a description for the policy. This setting is optional, but recommended.
6. Select **Next**.
7. Enter a name in the **Custom configuration profile name** box.
8. Choose a **Deployment channel**. Device channel is recommended.
9. Click the folder icon to upload your **Configuration profile file**. Choose the `kerberos.mobileconfig` file you [saved previously](#Kerberos SSO MDM profile configuration for on-premises Active Directory) after customizing the template.
10. Select **Next**.
11. In **Scope tags** (optional), assign a tag to filter the profile to specific IT groups, such as `US-NC IT Team` or `JohnGlenn_ITDepartment`. Select **Next**.
 - For more information about scope tags, see [Use RBAC roles and scope tags for distributed IT](#).

12. In **Assignments**, select the users or user groups that will receive your profile. Platform SSO policies are user-based policies. Don't assign the platform SSO policy to devices.
 - For more information on assigning profiles, see [Assign user and device profiles](#).

13. Select **Next**.

14. In **Review + create**, review your settings. When you select **Create**, your changes are saved, and the profile is assigned. The policy is also shown in the profiles list.

15. Repeat this process if you need to deploy both profiles because you will use both on-premises Kerberos SSO and Microsoft Entra ID Cloud Kerberos.

The next time the device checks for configuration updates, the settings you configured are applied.

Testing Kerberos SSO

Once the user has completed Platform SSO registration, you can check that the device has Kerberos tickets by running the `app-sso platform -s` command in the Terminal app:

```
Console
```

```
app-sso platform -s
```

You should have two Kerberos tickets, one for your on-premises AD with the ticketKeyPath value of `tgt_ad` and one for your Microsoft Entra ID tenant with the ticketKeyPath value of `tgt_cloud`. The output should resemble the following:

```

User Configuration:
{
  "created" : "2024-05-16T23:22:59Z",
  "kerberosStatus" : [
    {
      "cacheName" :
      "exchangeRequired" : true,
      "failedToConnect" : true,
      "importSuccessful" : true,
      "realm" :
      "ticketKeyPath" : "tgt_ad",
      "upn" :
    },
    {
      "cacheName" :
      "exchangeRequired" : false,
      "failedToConnect" : false,
      "importSuccessful" : true,
      "realm" : "KERBEROS.MICROSOFTONLINE.COM",
      "ticketKeyPath" : "tgt_cloud",
      "upn" :
    }
  ],
  "lastLoginDate" : "2024-05-16T23:22:47Z",
  "loginType" : "POLoginTypeSmartCard (3)",
  "smartCardHash" :
  "smartCardTokenId"
  "state" : "POUserStateNormal (0)",
  "uniqueIdentifier" :
  "userLoginConfiguration" : {
    "created" :
    "loginUserName" :
  },
  "version" : 1
}

SSO Tokens:
Received:
2024-
Expiration:
2024-          (Not Expired)

```

Validate your configuration is working by testing with appropriate Kerberos-capable resources:

- Test on-premises Active Directory functionality by accessing an on-premises AD-integrated file server using Finder or a web application using Safari. The user should be able to access the file share without being challenged for interactive credentials.
- Test Microsoft Entra ID Kerberos functionality by accessing an Azure Files share enabled for Microsoft Entra ID cloud kerberos. The user should be able to access the file share without being challenged for interactive credentials. Refer to [this guide](#) if you need to configure a cloud file share in Azure Files.

! Note

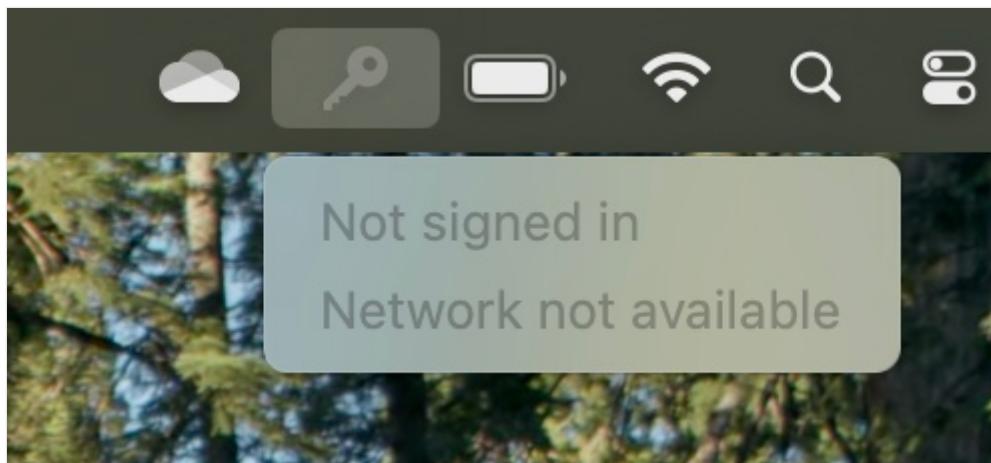
Note that Microsoft's Platform SSO implementation is responsible for issuing the Kerberos TGTs and delivering them to macOS so that macOS can import them. If you see TGTs when running `app-sso platform -s`, then the TGTs have been successfully imported. If you

experience any ongoing Kerberos issues, such as issues accessing on-premises resources via Kerberos, then it's recommended to reach out to Apple for support with further configuration of your Kerberos MDM profiles. The Kerberos implementation in macOS uses native Apple-provided Kerberos capabilities.

Known Issues

Kerberos SSO extension menu extra

When deploying support for Kerberos SSO with Platform SSO, the standard Kerberos SSO extension capabilities of macOS are still used. Like with a deployment of the native [Kerberos SSO extension](#) without Platform SSO, the Kerberos SSO extension menu extra will appear in the macOS menu bar:



When deploying Kerberos support with Platform SSO, users don't need to interact with the Kerberos SSO extension menu extra to have Kerberos functionality work. Kerberos SSO functionality will still operate if the user doesn't sign into the menu bar extra and the menu bar extra reports "Not signed in". You may instruct users to ignore the menu bar extra when deploying with Platform SSO, per this article. Instead, make sure that you validate that kerberos functionality works as expected without interaction with the menu bar extra, as outlined in the [Testing Kerberos SSO](#) section of this article.

Browser Support for Kerberos SSO

Some browsers require additional configuration to enable Kerberos SSO support, including if you are using Platform SSO to enable Kerberos on your macOS devices. When deploying Kerberos support on macOS, deploy the appropriate settings for each of the browsers you utilize to ensure they can interact with the macOS Kerberos SSO features:

- Safari: supports Kerberos SSO by default

- Microsoft Edge:
 - Configure the **AuthNegotiateDelegateAllowlist** setting to include your on-premises Active Directory forest information: [AuthNegotiateDelegateAllowlist](#)
 - Configure the **AuthServerAllowlist** setting to include your on-premises Active Directory forest information: [AuthServerAllowlist](#)
- Google Chrome
 - Configure the **AuthNegotiateDelegateAllowlist** setting to include your on-premises Active Directory forest information: [AuthNegotiateDelegateAllowlist](#)
 - Configure the **AuthServerAllowlist** setting to include your on-premises Active Directory forest information: [AuthServerAllowlist](#)
- Mozilla Firefox
 - Configure the Mozilla Firefox **network.negotiate-auth.trusted-uris** and **network.automatic-ntlm-auth.trusted-uris** settings to enable Kerberos SSO support

See also

- [Join a Mac device with Microsoft Entra ID using Company Portal](#)
- [Passwordless authentication options for Microsoft Entra ID](#)
- [Plan a passwordless authentication deployment in Microsoft Entra ID](#)
- [Microsoft Enterprise SSO plug-in for Apple devices](#)

Microsoft Entra registered devices

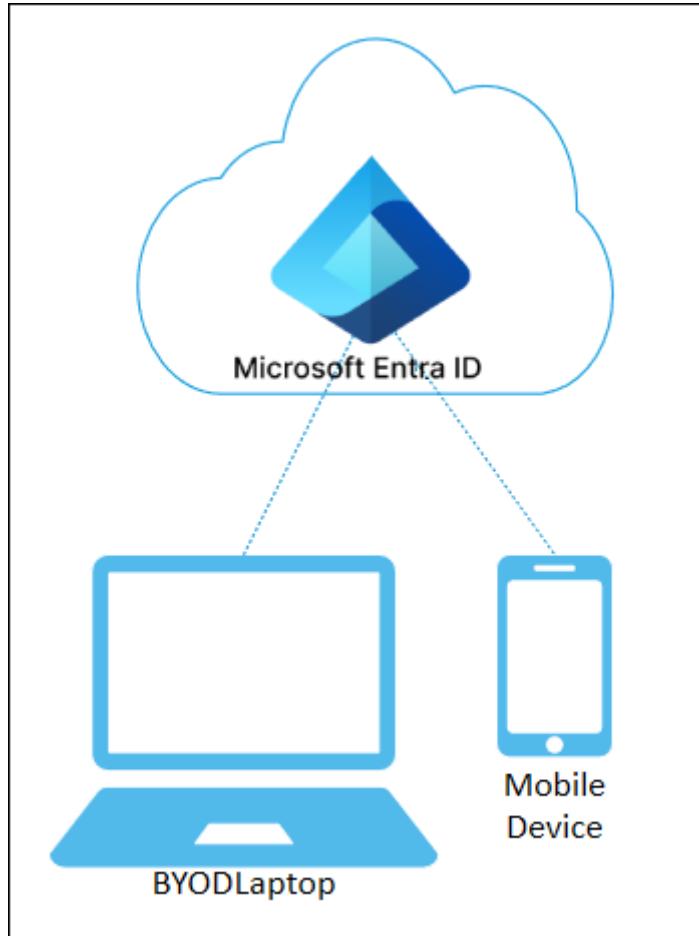
Article • 02/27/2025

The goal of Microsoft Entra registered - also known as Workplace joined - devices is to provide your users with support for bring your own device (BYOD) or mobile device scenarios. In these scenarios, a user can access your organization's resources using a personal device.

[Expand table](#)

Microsoft Entra registered	Description
Definition	Registered to Microsoft Entra ID without requiring organizational account to sign in to the device
Primary audience	Applicable to all users with the following criteria: <ul style="list-style-type: none">• Bring your own device• Mobile devices
Device ownership	User or Organization
Operating Systems	<ul style="list-style-type: none">• Windows 10 or newer• macOS 10.15 or newer• iOS 15 or newer• Android• Linux editions:<ul style="list-style-type: none">• Ubuntu 20.04/22.04/24.04 LTS• Red Hat Enterprise Linux 8/9 LTS
Provisioning	<ul style="list-style-type: none">• Windows 10 or newer – Settings• iOS/Android – Company Portal or Microsoft Authenticator app• macOS – Company Portal• Linux - Intune Agent
Device sign in options	<ul style="list-style-type: none">• End-user local credentials• Password• Windows Hello• PIN• Biometrics or pattern for other devices
Device management	<ul style="list-style-type: none">• Mobile Device Management (example: Microsoft Intune)• Mobile Application Management
Key capabilities	<ul style="list-style-type: none">• Single sign-on (SSO) to cloud resources• Conditional Access when enrolled into Intune

Microsoft Entra registered	Description
	<ul style="list-style-type: none"> Conditional Access via App protection policy Enables Phone sign in with Microsoft Authenticator app



Microsoft Entra registered devices are signed in to using a local account like a Microsoft account on a Windows 10 or newer device. These devices have a Microsoft Entra account for access to organizational resources. Access to resources in the organization can be limited based on that Microsoft Entra account and Conditional Access policies applied to the device identity.

Microsoft Entra Registration isn't the same as device enrollment. If Administrators permit users to enroll their devices, organizations can further control these Microsoft Entra registered devices by enrolling them into Mobile Device Management (MDM) tools like Microsoft Intune. MDM provides a means to enforce organization-required configurations like requiring storage to be encrypted, password complexity, and security software kept updated.

Microsoft Entra registration can be accomplished when accessing a work application for the first time or manually using the Windows 10 or Windows 11 Settings menu.

Scenarios

A user in your organization wants to access your benefits enrollment tool from their home PC. Your organization requires that anyone accesses this tool from an Intune compliant device. The user registers their home PC with Microsoft Entra ID and Enrolls the device in Intune, then the required Intune policies are enforced giving the user access to their resources.

Another user wants to access their organizational email on their personal Android phone that is rooted. Your company requires a compliant device and has an Intune device compliance policy to block any rooted devices. The employee is stopped from accessing organizational resources on this device.

 **Note**

Microsoft Entra registered devices don't support the [Unified Write Filter](#) feature.

Related content

- [Manage device identities](#)
- [Manage stale devices in Microsoft Entra ID](#)
- [Register your personal device on your work or school network ↗](#)

Feedback

Was this page helpful?

 Yes

 No

[Provide product feedback ↗](#)

Microsoft Entra joined devices

Article • 11/25/2024

Any organization can deploy Microsoft Entra joined devices no matter the size or industry. Microsoft Entra join works even in hybrid environments, enabling access to both cloud and on-premises apps and resources.

 Expand table

Microsoft Entra join	Description
Definition	Joined only to Microsoft Entra ID requiring organizational account to sign in to the device
Primary audience	Suitable for both cloud-only and hybrid organizations.
	Applicable to all users in an organization
Device ownership	Organization
Operating Systems	All Windows 11 and Windows 10 devices except Home editions Windows Enterprise multi-session Virtual Machines running in Azure and Windows Server 2019 and newer Virtual Machines running in Azure (Server core isn't supported)
	(Public preview) Apple devices running macOS 13 or newer
Provisioning	Self-service: Windows Out of Box Experience (OOBE) or Settings Bulk enrollment Windows Autopilot (Public preview) Apple Automated Device Enrollment (applies to Apple devices only)
Device sign in options	Organizational accounts using: Password Passwordless options like Windows Hello for Business , Platform Credential for macOS (Public preview) and FIDO2.0 security keys.
Device management	Mobile Device Management (example: Microsoft Intune)

Microsoft Entra	Description
join	Configuration Manager standalone or co-management with Microsoft Intune
Key capabilities	single sign-on (SSO) to both cloud and on-premises resources
	Conditional Access through mobile device management (MDM) enrollment and compliance evaluation
	Self-service Password Reset and Windows Hello PIN reset on lock screen

You sign in to Microsoft Entra joined devices using a Microsoft Entra account. Access to resources can be controlled based on your account and [Conditional Access policies](#) applied to the device.

Administrators can secure and further control Microsoft Entra joined devices using Mobile Device Management (MDM) tools like Microsoft Intune or in co-management scenarios using Microsoft Configuration Manager. These tools provide a means to enforce organization-required configurations like:

- Requiring storage to be encrypted
- Password complexity
- Software installation
- Software updates

Administrators can make organization applications available to Microsoft Entra joined devices using Configuration Manager to [Manage apps from the Microsoft Store for Business and Education](#).

Microsoft Entra join can be accomplished using self-service options like the Out of Box Experience (OOBE), bulk enrollment, [Apple Automated Device Enrollment \(public preview\)](#), or [Windows Autopilot](#).

Microsoft Entra joined devices can still maintain single sign-on access to on-premises resources when they are on the organization's network. Devices that are Microsoft Entra joined can still authenticate to on-premises servers like file, print, and other applications.

Scenarios

Microsoft Entra join can be used in various scenarios like:

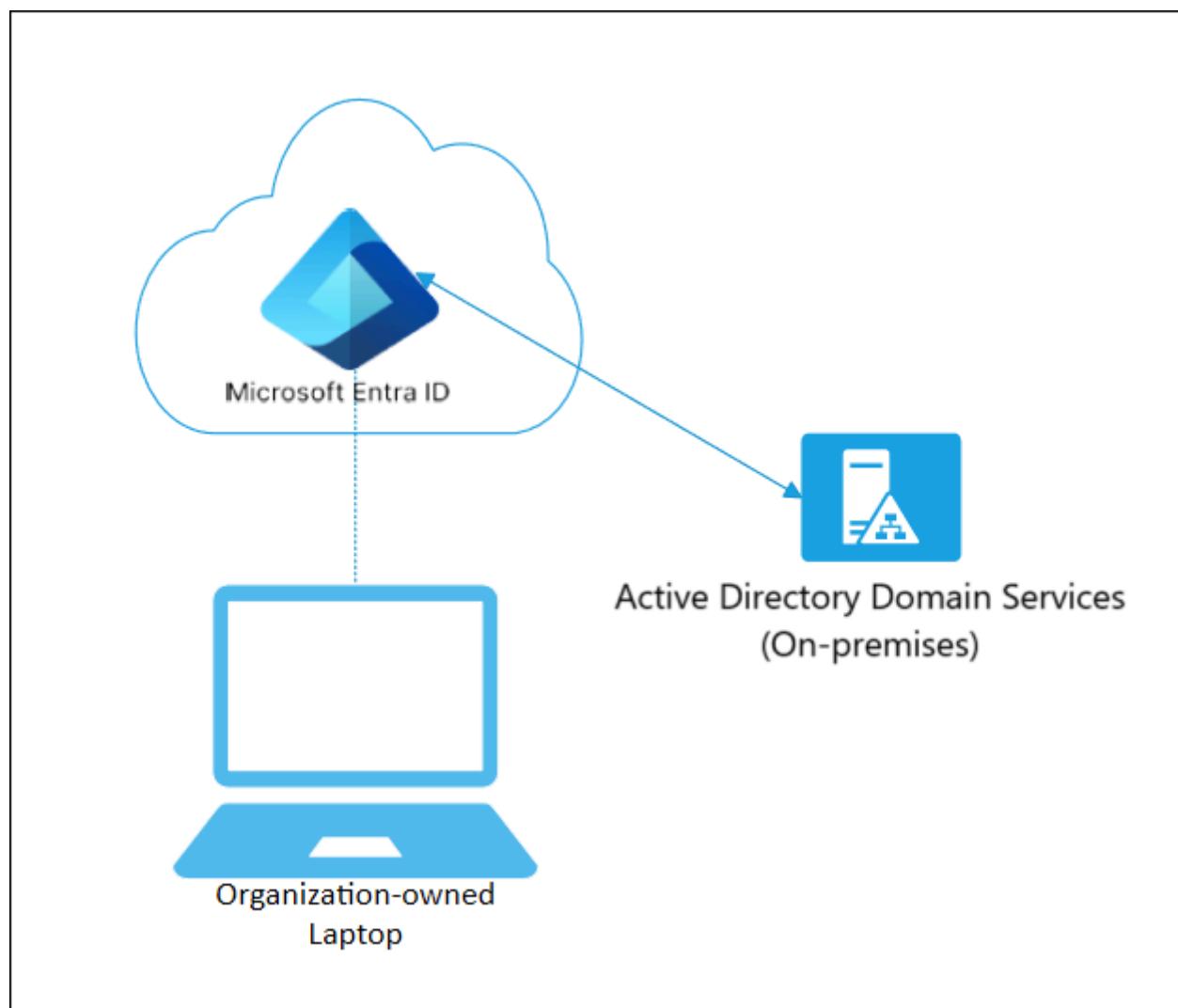
- You want to transition to cloud-based infrastructure using Microsoft Entra ID and MDM like Intune.

- You can't use an on-premises domain join, for example, if you need to get mobile devices such as tablets and phones under control.
- Your users primarily need to access Microsoft 365 or other software as a service (SaaS) apps integrated with Microsoft Entra ID.
- You want to manage a group of users in Microsoft Entra ID instead of in Active Directory. This scenario can apply, for example, to seasonal workers, contractors, or students.
- You want to provide joining capabilities to workers who work from home or are in remote branch offices with limited on-premises infrastructure.

You can configure Microsoft Entra join for all Windows 11 and Windows 10 devices except for Home editions.

The goal of Microsoft Entra joined devices is to simplify:

- Windows and macOS deployments of work-owned devices
- Access to organizational apps and resources from any Windows or macOS device
- Cloud-based management of work-owned devices
- Users to sign in to their devices with their Microsoft Entra ID or synced Active Directory work or school accounts.



Microsoft Entra join can be deployed by using any of the following methods:

- [Windows Autopilot](#)
- [Bulk deployment](#)
- [Self-service experience](#)
- [Apple Automated Device Enrollment \(public preview\)](#)

Related content

- [Plan your Microsoft Entra join implementation](#)
- [Co-management using Configuration Manager and Microsoft Intune](#)
- [How to manage the local administrators group on Microsoft Entra joined devices](#)
- [Manage device identities](#)
- [Manage stale devices in Microsoft Entra ID](#)
- [macOS Platform Single Sign-on \(preview\)](#)

Microsoft Entra hybrid joined devices

Article • 05/09/2025

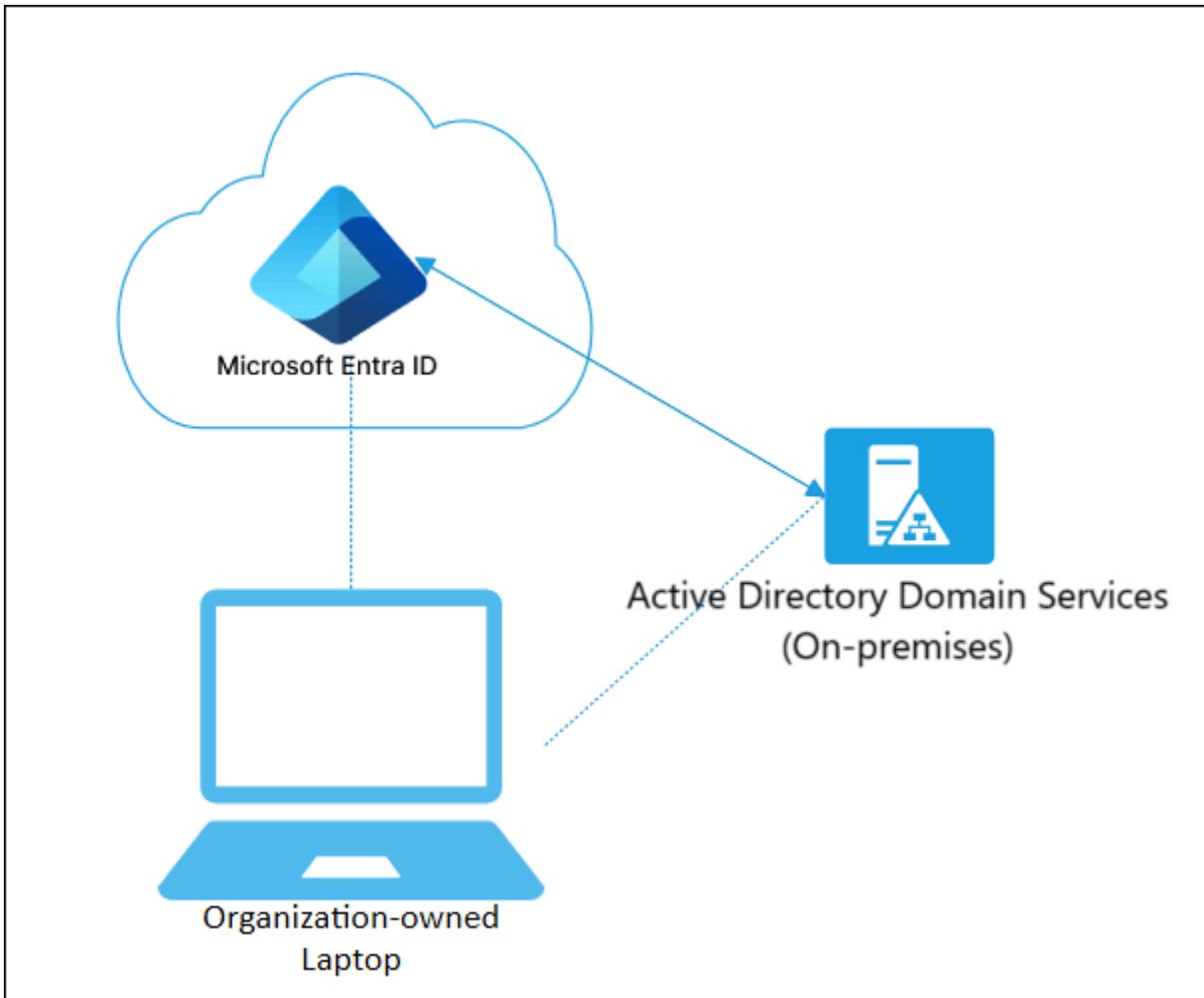
Organizations with existing Active Directory implementations can benefit from some of the functionality provided by Microsoft Entra ID by implementing Microsoft Entra hybrid joined devices. These devices are joined to your on-premises Active Directory and registered with Microsoft Entra ID.

Microsoft Entra hybrid joined devices require network line of sight to your on-premises domain controllers periodically. Without this connection, devices become unusable. If this requirement is a concern, consider [Microsoft Entra joining](#) your devices.

 Expand table

Microsoft Entra hybrid join	Description
Definition	Joined to on-premises Microsoft Windows Server Active Directory and Microsoft Entra ID requiring organizational account to sign in to the device
Primary audience	Suitable for hybrid organizations with existing on-premises Microsoft Windows Server Active Directory infrastructure
	Applicable to all users in an organization
Device ownership	Organization
Operating Systems	Windows 11 or Windows 10 except Home editions
	Windows Server 2016, 2019, and 2022
Provisioning	Windows 11, Windows 10, Windows Server 2016/2019/2022
	Domain join by IT and autojoin via Microsoft Entra Connect or AD FS config
	Domain join by Windows Autopilot and autojoin via Microsoft Entra Connect or AD FS config
Device sign in options	Organizational accounts using:
	Password
	Passwordless options like Windows Hello for Business and FIDO2.0 security keys.
Device management	Group Policy
	Configuration Manager standalone or co-management with Microsoft Intune
Key capabilities	single sign-on (SSO) to both cloud and on-premises resources

Microsoft Entra	Description
hybrid join	
	Conditional Access through Domain join or through Intune if co-managed
	Self-service Password Reset and Windows Hello PIN reset on lock screen



Scenarios

Use Microsoft Entra hybrid joined devices if:

- You want to continue to use [Group Policy](#) to manage device configuration.
- You want to continue to use existing imaging solutions to deploy and configure devices.
- You have Win32 apps deployed to these devices that rely on Active Directory machine authentication.

Related content

- [Plan your Microsoft Entra hybrid join implementation](#)
- [Co-management using Configuration Manager and Microsoft Intune](#)

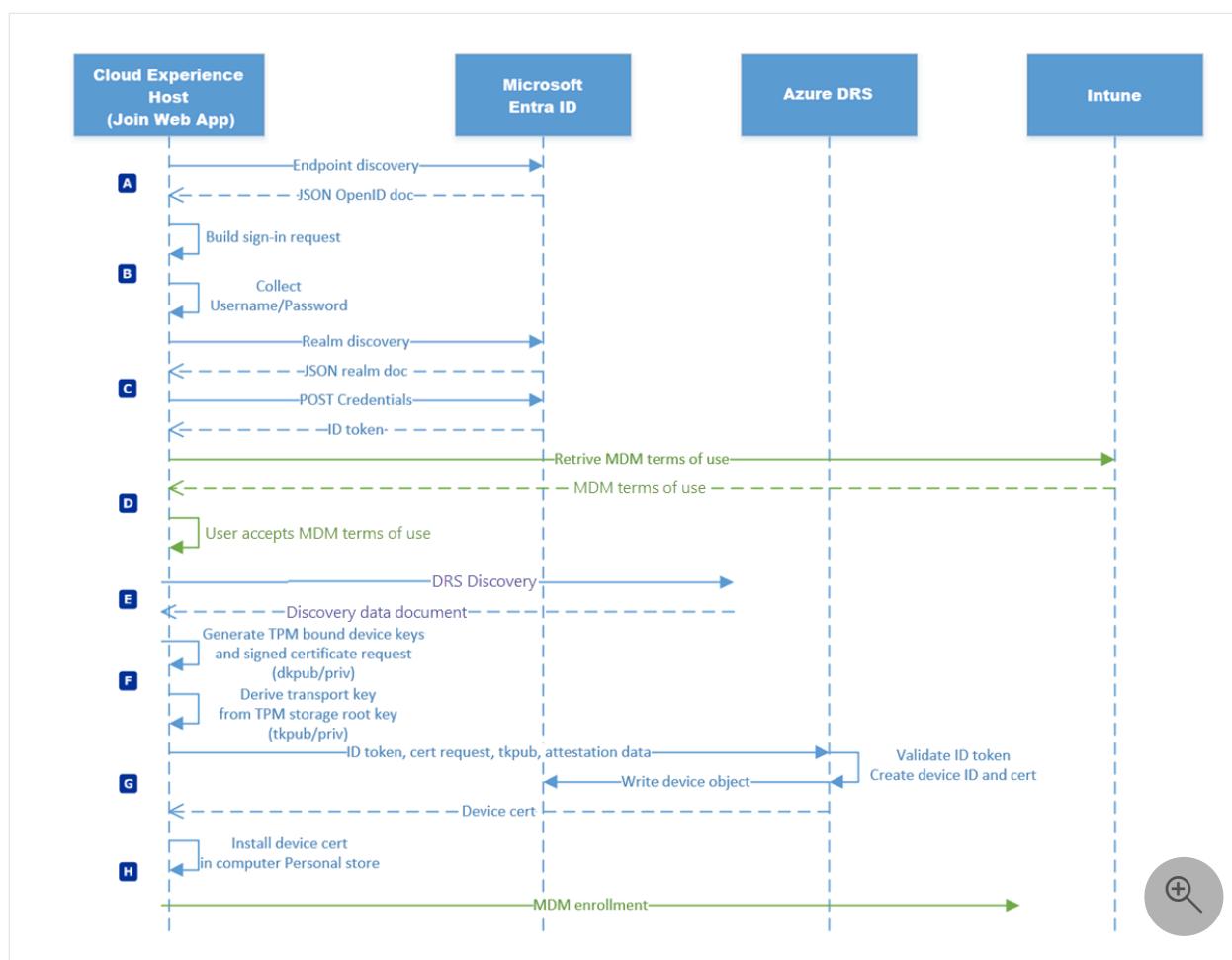
- Manage device identities
- Manage stale devices in Microsoft Entra ID

How it works: Device registration

Article • 05/29/2024

Device Registration is a prerequisite to cloud-based authentication. Commonly, devices are Microsoft Entra ID or Microsoft Entra hybrid joined to complete device registration. This article provides details of how Microsoft Entra join and Microsoft Entra hybrid join work in managed and federated environments. For more information about how Microsoft Entra authentication works on these devices, see the article [Primary refresh tokens](#).

Microsoft Entra joined in Managed environments

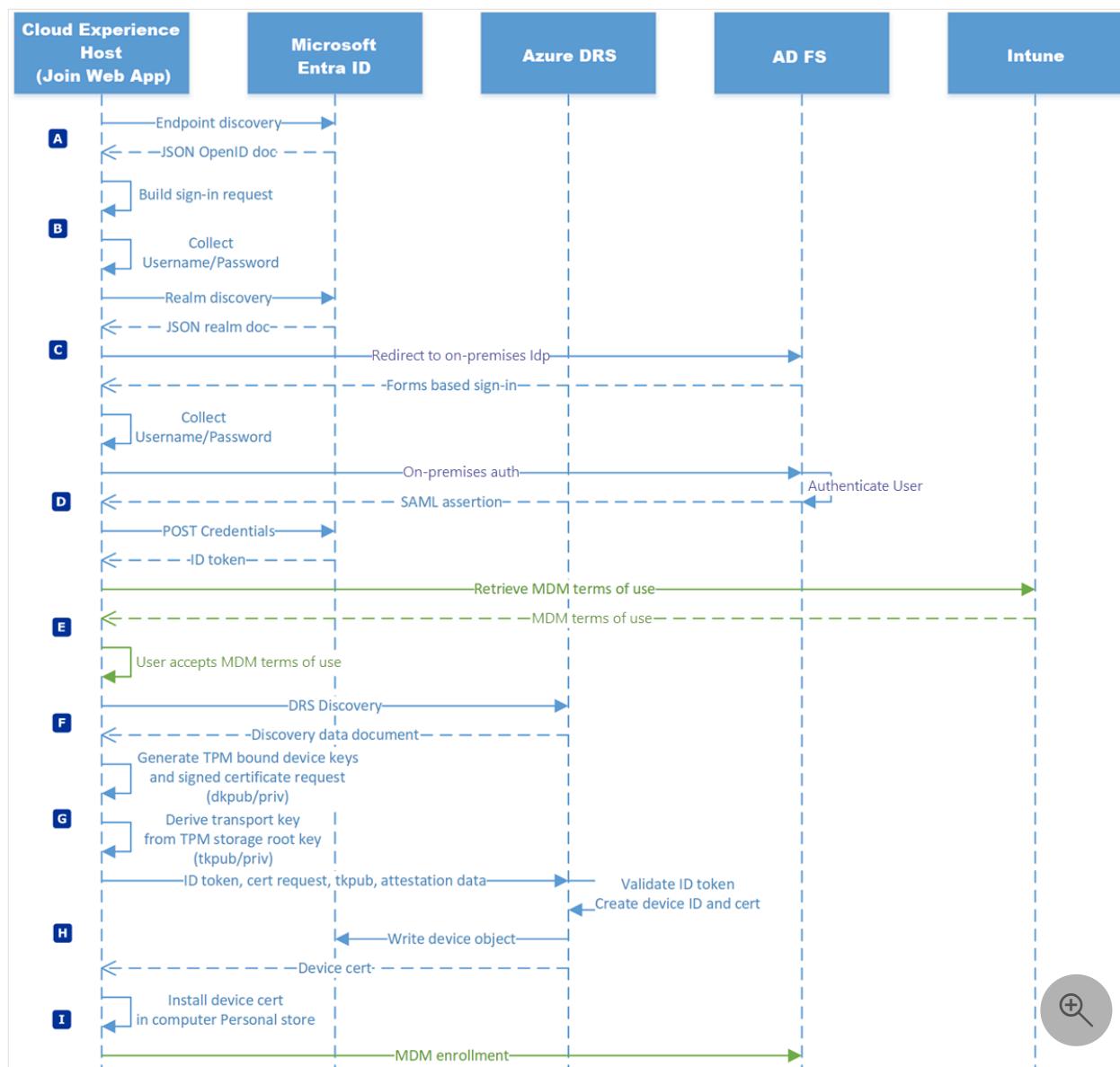


[Expand table](#)

Phase	Description
A	The most common way Microsoft Entra joined devices register is during the out-of-box-experience (OOBE) where it loads the Microsoft Entra join web application in the Cloud Experience Host (CXH) application. The application sends a GET request to the Microsoft

Phase	Description
	Entra OpenID configuration endpoint to discover authorization endpoints. Microsoft Entra ID returns the OpenID configuration, which includes the authorization endpoints, to application as JSON document.
B	The application builds a sign-in request for the authorization end point and collects user credentials.
C	After the user provides their user principal name (UPN), the application sends a GET request to Microsoft Entra ID to discover corresponding realm information for the user. This information determines if the environment is managed or federated. Microsoft Entra ID returns the information in a JSON object. The application determines the environment is managed (nonfederated).
	The last step in this phase has the application create an authentication buffer and if in OOBE, temporarily caches it for automatic sign-in at the end of OOBE. The application POSTs the credentials to Microsoft Entra ID where they're validated. Microsoft Entra ID returns an ID token with claims.
D	The application looks for mobile device management (MDM) terms of use (the <code>mdm_tou_url</code> claim). If present, the application retrieves the terms of use from the claim's value, present the contents to the user, and waits for the user to accept the terms of use. This step is optional and skipped if the claim isn't present or if the claim value is empty.
E	The application sends a device registration discovery request to the Azure Device Registration Service (DRS). Azure DRS returns a discovery data document, which returns tenant-specific URLs to complete device registration.
F	The application creates TPM bound (preferred) RSA 2048 bit key-pair known as the device key (<code>dkpub/dkpriv</code>). The application creates a certificate request using <code>dkpub</code> and the public key and signs the certificate request with using <code>dkpriv</code> . Next, the application derives second key pair from the TPM's storage root key. This key is the transport key (<code>tkpub/tkpriv</code>).
G	The application sends a device registration request to Azure DRS that includes the ID token, certificate request, <code>tkpub</code> , and attestation data. Azure DRS validates the ID token, creates a device ID, and creates a certificate based on the included certificate request. Azure DRS then writes a device object in Microsoft Entra ID and sends the device ID and the device certificate to the client.
H	Device registration completes by receiving the device ID and the device certificate from Azure DRS. The device ID is saved for future reference (viewable from <code>dsregcmd.exe /status</code>), and the device certificate is installed in the Personal store of the computer. With device registration complete, the process continues with MDM enrollment.

Microsoft Entra joined in Federated environments

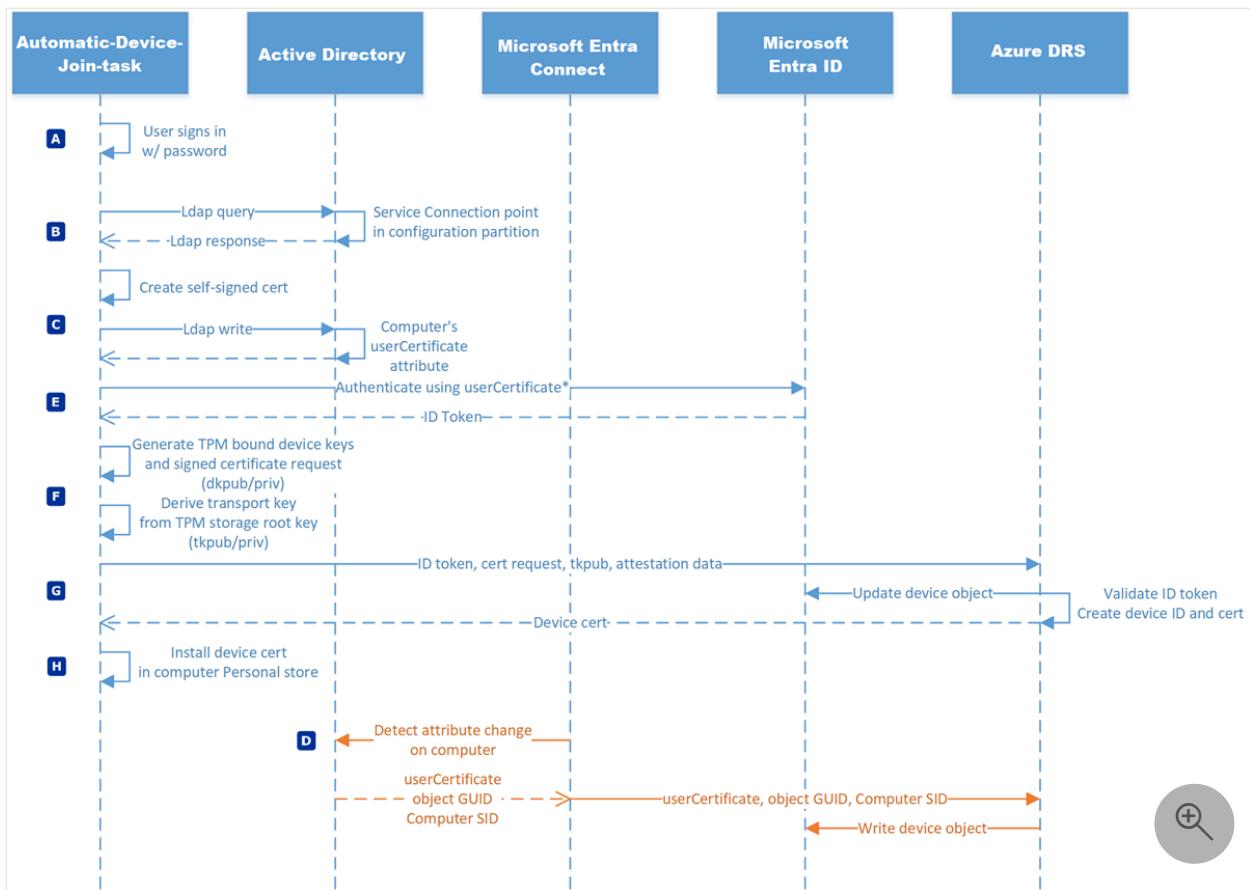


[Expand table](#)

Phase	Description
A	The most common way Microsoft Entra joined devices register is during the out-of-box-experience (OOBE) where it loads the Microsoft Entra join web application in the Cloud Experience Host (CXH) application. The application sends a GET request to the Microsoft Entra OpenID configuration endpoint to discover authorization endpoints. Microsoft Entra ID returns the OpenID configuration, which includes the authorization endpoints, to the application as JSON document.
B	The application builds a sign-in request for the authorization end point and collects user credentials.
C	After the user provides their user name (in UPN format), the application sends a GET request to Microsoft Entra ID to discover corresponding realm information for the user. This information determines if the environment is managed or federated. Microsoft Entra ID returns the information in a JSON object. The application determines the environment is federated.

Phase	Description
	The application redirects to the AuthURL value (on-premises STS sign-in page) in the returned JSON realm object. The application collects credentials through the STS web page.
D	The application POST the credential to the on-premises STS, which might require extra factors of authentication. The on-premises STS authenticates the user and returns a token. The application POSTs the token to Microsoft Entra ID for authentication. Microsoft Entra ID validates the token and returns an ID token with claims.
E	The application looks for MDM terms of use (the mdm_tou_url claim). If present, the application retrieves the terms of use from the claim's value, present the contents to the user, and waits for the user to accept the terms of use. This step is optional and skipped if the claim isn't present or if the claim value is empty.
F	The application sends a device registration discovery request to the Azure Device Registration Service (DRS). Azure DRS returns a discovery data document, which returns tenant-specific URLs to complete device registration.
G	The application creates TPM bound (preferred) RSA 2048 bit key-pair known as the device key (dkpub/dkpriv). The application creates a certificate request using dkpub and the public key and signs the certificate request with using dkpriv. Next, the application derives second key pair from the TPM's storage root key. This key is the transport key (tkpub/tkpriv).
H	The application sends a device registration request to Azure DRS that includes the ID token, certificate request, tkpub, and attestation data. Azure DRS validates the ID token, creates a device ID, and creates a certificate based on the included certificate request. Azure DRS then writes a device object in Microsoft Entra ID and sends the device ID and the device certificate to the client.
I	Device registration completes by receiving the device ID and the device certificate from Azure DRS. The device ID is saved for future reference (viewable from <code>dsregcmd.exe /status</code>), and the device certificate is installed in the Personal store of the computer. With device registration complete, the process continues with MDM enrollment.

Microsoft Entra hybrid joined in Managed environments

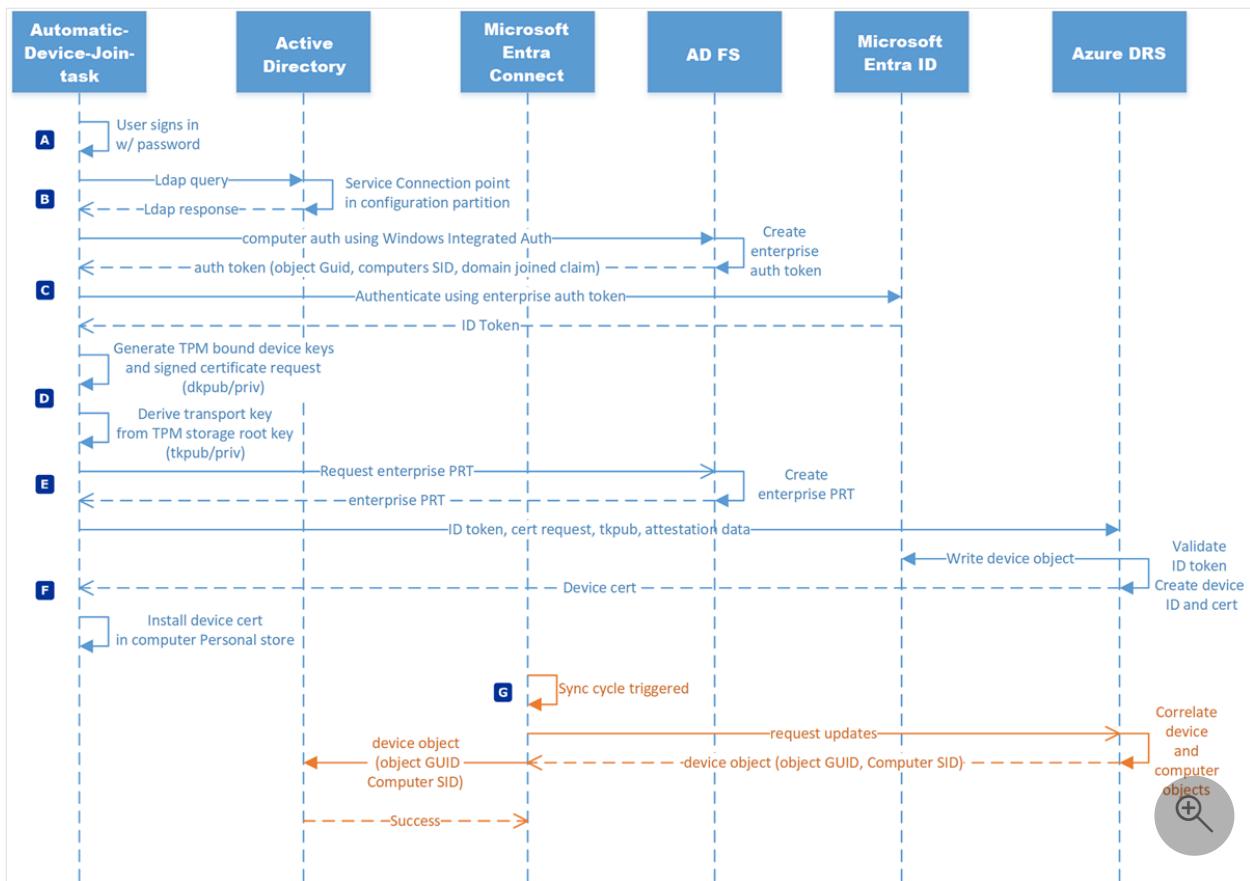


[Expand table](#)

Phase	Description
A	The user signs in to a domain joined Windows 10 or newer computer using domain credentials. This credential can be user name and password or smart card authentication. The user sign-in triggers the Automatic Device Join task. The Automatic Device Join tasks is triggered on domain join and retried every hour. It doesn't solely depend on the user sign-in.
B	The task queries Active Directory using the LDAP protocol for the keywords attribute on the service connection point stored in the configuration partition in Active Directory (<code>(CN=62a0ff2e-97b9-4513-943f-0d221bd30080,CN=Device Registration Configuration,CN=Services,CN=Configuration,DC=corp,DC=contoso,DC=com)</code>). The value returned in the keywords attribute determines if device registration is directed to Azure Device Registration Service (DRS) or the enterprise device registration service hosted on-premises.
C	For the managed environment, the task creates an initial authentication credential in the form of a self-signed certificate. The task writes the certificate to the userCertificate attribute on the computer object in Active Directory using LDAP.
D	The computer can't authenticate to Azure DRS until a device object representing the computer that includes the certificate on the userCertificate attribute is created in Microsoft Entra ID. Microsoft Entra Connect detects an attribute change. On the next synchronization cycle, Microsoft Entra Connect sends the userCertificate, object GUID, Computer SID,

Phase	Description
	and computer SID to Azure DRS. Azure DRS uses the attribute information to create a device object in Microsoft Entra ID.
E	The Automatic Device Join task triggers with each user sign-in or every hour, and tries to authenticate the computer to Microsoft Entra ID using the corresponding private key of the public key in the userCertificate attribute. Microsoft Entra authenticates the computer and issues an ID token to the computer.
F	The task creates TPM bound (preferred) RSA 2048 bit key-pair known as the device key (dkpub/dkpriv). The application creates a certificate request using dkpub and the public key and signs the certificate request with using dkpriv. Next, the application derives second key pair from the TPM's storage root key. This key is the transport key (tkpub/tkpriv).
G	The task sends a device registration request to Azure DRS that includes the ID token, certificate request, tkpub, and attestation data. Azure DRS validates the ID token, creates a device ID, and creates a certificate based on the included certificate request. Azure DRS then updates the device object in Microsoft Entra ID and sends the device ID and the device certificate to the client.
H	Device registration completes by receiving the device ID and the device certificate from Azure DRS. The device ID is saved for future reference (viewable from <code>dsregcmd.exe /status</code>), and the device certificate is installed in the Personal store of the computer. With device registration complete, the task exits.

Microsoft Entra hybrid joined in Federated environments



[Expand table](#)

Phase	Description
A	The user signs in to a domain joined Windows 10 or newer computer using domain credentials. This credential can be user name and password or smart card authentication. The user sign-in triggers the Automatic Device Join task. The Automatic Device Join tasks is triggered on domain join and retried every hour. It doesn't solely depend on the user sign-in.
B	The task queries Active Directory using the LDAP protocol for the keywords attribute on the service connection point stored in the configuration partition in Active Directory (<code>CN=62a0ff2e-97b9-4513-943f-0d221bd30080,CN=Device Registration Configuration,CN=Services,CN=Configuration,DC=corp,DC=contoso,DC=com</code>). The value returned in the keywords attribute determines if device registration is directed to Azure Device Registration Service (DRS) or the enterprise device registration service hosted on-premises.
C	For the federated environments, the computer authenticates the enterprise device registration endpoint using Windows Integrated Authentication. The enterprise device registration service creates and returns a token that includes claims for the object GUID, computer SID, and domain joined state. The task submits the token and claims to Microsoft Entra ID where they're validated. Microsoft Entra ID returns an ID token to the running task.
D	The application creates TPM bound (preferred) RSA 2048 bit key-pair known as the device key (dkpub/dkpriv). The application creates a certificate request using dkpub and

Phase	Description
	the public key and signs the certificate request with using dkpriv. Next, the application derives second key pair from the TPM's storage root key. This key is the transport key (tkpub/tkpriv).
E	To provide SSO for on-premises federated application, the task requests an enterprise PRT from the on-premises STS. Windows Server 2016 running the Active Directory Federation Services role validate the request and return it the running task.
F	The task sends a device registration request to Azure DRS that includes the ID token, certificate request, tkpub, and attestation data. Azure DRS validates the ID token, creates a device ID, and creates a certificate based on the included certificate request. Azure DRS then writes a device object in Microsoft Entra ID and sends the device ID and the device certificate to the client. Device registration completes by receiving the device ID and the device certificate from Azure DRS. The device ID is saved for future reference (viewable from <code>dsregcmd.exe /status</code>), and the device certificate is installed in the Personal store of the computer. With device registration complete, the task exits.
G	If Microsoft Entra Connect device writeback is enabled, Microsoft Entra Connect requests updates from Microsoft Entra ID at its next synchronization cycle (device writeback is required for hybrid deployment using certificate trust). Microsoft Entra ID correlates the device object with a matching synchronized computer object. Microsoft Entra Connect receives the device object that includes the object GUID and computer SID and writes the device object to Active Directory.

Next steps

- [Microsoft Entra joined devices](#)
- [Microsoft Entra registered devices](#)
- [Microsoft Entra hybrid joined devices](#)
- [What is a Primary Refresh Token?](#)
- [Microsoft Entra Connect: Device options](#)

Feedback

Was this page helpful?

 Yes

 No

[Provide product feedback ↗](#)

How SSO to on-premises resources works on Microsoft Entra joined devices

Article • 05/29/2024

Microsoft Entra joined devices give users a single sign-on (SSO) experience to your tenant's cloud apps. If your environment has on-premises Active Directory Domain Services (AD DS), users can also SSO to resources and applications that rely on on-premises Active Directory Domain Services.

This article explains how this works.

Prerequisites

- An [Microsoft Entra joined device](#).
- On-premises SSO requires line-of-sight communication with your on-premises AD DS domain controllers. If Microsoft Entra joined devices aren't connected to your organization's network, a VPN or other network infrastructure is required.
- Microsoft Entra Connect or Microsoft Entra Connect cloud sync: To synchronize default user attributes like SAM Account Name, Domain Name, and UPN. For more information, see the article [Attributes synchronized by Microsoft Entra Connect](#).

How it works

With a Microsoft Entra joined device, your users already have an SSO experience to the cloud apps in your environment. If your environment has Microsoft Entra ID and on-premises AD DS, you might want to expand the scope of your SSO experience to your on-premises Line Of Business (LOB) apps, file shares, and printers.

Microsoft Entra joined devices have no knowledge about your on-premises AD DS environment because they aren't joined to it. However, you can provide additional information about your on-premises AD to these devices with Microsoft Entra Connect.

Microsoft Entra Connect or Microsoft Entra Connect cloud sync synchronize your on-premises identity information to the cloud. As part of the synchronization process, on-premises user and domain information is synchronized to Microsoft Entra ID. When a user signs in to a Microsoft Entra joined device in a hybrid environment:

1. Microsoft Entra ID sends the details of the user's on-premises domain back to the device, along with the [Primary Refresh Token](#)

2. The local security authority (LSA) service enables Kerberos and NTLM authentication on the device.

 **Note**

Additional configuration is required when passwordless authentication to Microsoft Entra joined devices is used.

For FIDO2 security key based passwordless authentication and Windows Hello for Business Hybrid Cloud Trust, see [Enable passwordless security key sign-in to on-premises resources with Microsoft Entra ID](#).

For Windows Hello for Business Cloud Kerberos Trust, see [Configure and provision Windows Hello for Business - cloud Kerberos trust](#).

For Windows Hello for Business Hybrid Key Trust, see [Configure Microsoft Entra joined devices for On-premises Single-Sign On using Windows Hello for Business](#).

For Windows Hello for Business Hybrid Certificate Trust, see [Using Certificates for AADJ On-premises Single-sign On](#).

During an access attempt to an on-premises resource requesting Kerberos or NTLM, the device:

1. Sends the on-premises domain information and user credentials to the located DC to get the user authenticated.
2. Receives a Kerberos [Ticket-Granting Ticket \(TGT\)](#) or NTLM token based on the protocol the on-premises resource or application supports. If the attempt to get the Kerberos TGT or NTLM token for the domain fails, Credential Manager entries are tried, or the user might receive an authentication pop-up requesting credentials for the target resource. This failure can be related to a delay caused by a DCLocator timeout.

All apps that are configured for **Windows-Integrated authentication** seamlessly get SSO when a user tries to access them.

What you get

With SSO, on a Microsoft Entra joined device you can:

- Access a UNC path on an AD member server
- Access an AD DS member web server configured for Windows-integrated security

If you want to manage your on-premises AD from a Windows device, install the [Remote Server Administration Tools](#).

You can use:

- The Active Directory Users and Computers (ADUC) snap-in to administer all AD objects. However, you have to specify the domain that you want to connect to manually.
- The DHCP snap-in to administer an AD-joined DHCP server. However, you might need to specify the DHCP server name or address.

What you should know

- You might have to adjust your [domain-based filtering](#) in Microsoft Entra Connect to ensure that the data about the required domains is synchronized if you have multiple domains.
- Apps and resources that depend on Active Directory machine authentication don't work because Microsoft Entra joined devices don't have a computer object in AD DS.
- You can't share files with other users on a Microsoft Entra joined device.
- Applications running on your Microsoft Entra joined device might authenticate users. They must use the implicit UPN or the NT4 type syntax with the domain FQDN name as the domain part, for example: user@contoso.corp.com or contoso.corp.com\user.
 - If applications use the NETBIOS or legacy name like contoso\user, the errors the application gets would be either, NT error STATUS_BAD_VALIDATION_CLASS - 0xc00000a7, or Windows error ERROR_BAD_VALIDATION_CLASS - 1348 "The validation information class requested was invalid." This error happens even if you can resolve the legacy domain name.

Next steps

For more information, see [What is device management in Microsoft Entra ID?](#)

Understanding Primary Refresh Token (PRT)

Article • 03/03/2025

A Primary Refresh Token (PRT) is a key artifact of Microsoft Entra authentication in supported versions of Windows, iOS, and Android. This article explains how a PRT is issued, used, and protected on Windows 10 or newer devices, enhancing your security and enabling single sign-on (SSO) across applications.

This article assumes that you already understand the different device states available in Microsoft Entra ID and how single sign-on works in Windows. For more information about devices in Microsoft Entra ID, see [What is device management in Microsoft Entra ID?](#).

Key terminology and components

The following Windows components play a key role in requesting and using a PRT:

- **Cloud Authentication Provider (CloudAP):** CloudAP is the modern authentication provider for Windows sign in, that verifies users logging to a Windows 10 or newer device. CloudAP provides a plugin framework that identity providers can build on to enable authentication to Windows using that identity provider's credentials.
- **Web Account Manager (WAM):** WAM is the default token broker on Windows 10 or newer devices. WAM also provides a plugin framework that identity providers can build on and enable SSO to their applications relying on that identity provider.
- **Microsoft Entra CloudAP plugin:** A Microsoft Entra specific plugin built on the CloudAP framework that verifies user credentials with Microsoft Entra ID during Windows sign in.
- **Microsoft Entra WAM plugin:** A Microsoft Entra specific plugin built on the WAM framework that enables SSO to applications that rely on Microsoft Entra ID for authentication.
- **Dsreg:** A Microsoft Entra specific component on Windows 10 or newer, that handles the device registration process for all device states.
- **Trusted Platform Module (TPM):** A TPM is a hardware component built into a device that provides hardware-based security functions for user and device secrets. More details can be found in the article [Trusted Platform Module Technology Overview](#).

What does the PRT contain?

A PRT contains claims found in most Microsoft Entra ID refresh tokens. In addition, there are some device-specific claims included in the PRT. They are as follows:

- **Device ID:** A PRT is issued to a user on a specific device. The device ID claim `deviceID` determines the device the PRT was issued to the user on. This claim is later issued to tokens obtained via the PRT. The device ID claim is used to determine authorization for Conditional Access based on device state or compliance.
- **Session key:** The session key is an encrypted symmetric key, generated by the Microsoft Entra authentication service, issued as part of the PRT. The session key acts as the proof of possession when a PRT is used to obtain tokens for other applications. Session key is rolled on Windows 10 or newer Microsoft Entra joined or Microsoft Entra hybrid joined devices if it's older than 30 days.

Can I see what's in a PRT?

A PRT is an opaque blob sent from Microsoft Entra whose contents aren't known to any client components. You can't see inside a PRT.

How is a PRT issued?

Device registration is a prerequisite for device based authentication in Microsoft Entra ID. A PRT is issued to users only on registered devices. For more in-depth details on device registration, see the article [Windows Hello for Business and Device Registration](#). During device registration, the dsreg component generates two sets of cryptographic key pairs:

- Device key (dkpub/dkpriv)
- Transport key (tkpub/tkpriv)

The private keys are bound to the device's TPM if the device has a valid and functioning TPM, while the public keys are sent to Microsoft Entra ID during the device registration process. These keys are used to validate the device state during PRT requests.

The PRT is issued during user authentication on a Windows 10 or newer device in two scenarios:

- **Microsoft Entra joined or Microsoft Entra hybrid joined:** A PRT is issued during Windows logon when a user signs in with their organization credentials. A PRT is issued with all Windows 10 or newer supported credentials, for example, password and Windows Hello for Business. In this scenario, Microsoft Entra CloudAP plugin is the primary authority for the PRT.

- **Microsoft Entra registered device:** A PRT is issued when a user adds a secondary work account to their Windows 10 or newer device. Users can add an account to Windows 10 or newer in two different ways -
 - Adding an account via the **Allow my organization to manage my device** prompt after signing in to an app (for example, Outlook)
 - Adding an account from **Settings > Accounts > Access Work or School > Connect**

In Microsoft Entra registered device scenarios, the Microsoft Entra WAM plugin is the primary authority for the PRT since Windows logon isn't happening with this Microsoft Entra account.

 **Note**

Non-Microsoft identity providers need to support the WS-Trust protocol to enable PRT issuance on Windows 10 or newer devices. Without WS-Trust, a PRT can't be issued to users on Microsoft Entra hybrid joined or Microsoft Entra joined devices. On AD FS only usernamemixed endpoints are required. On AD FS if `smartcard/certificate` is used during Windows sign-in `certificatemixed` endpoints are required. Both `adfs/services/trust/2005/windowstransport` and `adfs/services/trust/13/windowstransport` should be enabled as intranet facing endpoints only and **must NOT be exposed** as extranet facing endpoints through the Web Application Proxy.

 **Note**

Microsoft Entra Conditional Access policies aren't evaluated when PRTs are issued.

 **Note**

We don't support non-Microsoft credential providers for issuance and renewal of Microsoft Entra PRTs.

What is the lifetime of a PRT?

Once issued, a PRT is valid for 14 days and is continuously renewed as long as the user actively uses the device.

How is a PRT used?

A PRT is used by two key components in Windows:

- **Microsoft Entra CloudAP plugin:** During Windows sign in, the Microsoft Entra CloudAP plugin requests a PRT from Microsoft Entra ID using the credentials provided by the user. It also caches the PRT to enable cached sign in when the user doesn't have access to an internet connection.
- **Microsoft Entra WAM plugin:** When users try to access applications, the Microsoft Entra WAM plugin uses the PRT to enable SSO on Windows 10 or newer. Microsoft Entra WAM plugin uses the PRT to request refresh and access tokens for applications that rely on WAM for token requests. It also enables SSO on browsers by injecting the PRT into browser requests. Browser SSO in Windows 10 or newer is supported on Microsoft Edge (natively), Chrome (via the [Windows 10 Accounts](#)) or Mozilla Firefox v91+ (Firefox [Windows SSO setting](#))

ⓘ Note

In instances where a user has two accounts from the same Microsoft Entra tenant signed in to a browser application, the device authentication provided by the PRT of the primary account is automatically applied to the second account as well. As a result, the second account also satisfies any device-based Conditional Access policy on the tenant.

How is a PRT renewed?

A PRT is renewed in two different ways:

- **Microsoft Entra CloudAP plugin every 4 hours:** The CloudAP plugin renews the PRT every 4 hours during Windows sign in. If the user doesn't have internet connection during that time, CloudAP plugin will renew the PRT after the device is connected to the internet and a new Windows sign in is done.
- **Microsoft Entra WAM plugin during app token requests:** The WAM plugin enables SSO on Windows 10 or newer devices by enabling silent token requests for applications. The WAM plugin can renew the PRT during these token requests in two different ways:
 - An app requests WAM for an access token silently but there's no refresh token available for that app. In this case, WAM uses the PRT to request a token for the app and gets back a new PRT in the response.

- An app requests WAM for an access token but the PRT is invalid or Microsoft Entra ID requires extra authorization (for example, Microsoft Entra multifactor authentication). In this scenario, WAM initiates an interactive logon requiring the user to reauthenticate or provide extra verification and a new PRT is issued on successful authentication.

In an AD FS environment, direct line of sight to the domain controller isn't required to renew the PRT. PRT renewal requires only `/adfs/services/trust/2005/usernamemixed` and `/adfs/services/trust/13/usernamemixed` endpoints enabled on proxy by using WS-Trust protocol.

Windows transport endpoints are required for password authentication only when a password is changed, not for PRT renewal.

 **Note**

Microsoft Entra Conditional Access policies aren't evaluated when PRTs are renewed.

Key considerations

- In Microsoft Entra joined and Microsoft Entra hybrid joined devices, the CloudAP plugin is the primary authority for a PRT. If a PRT is renewed during a WAM-based token request, the PRT is sent back to CloudAP plugin, which verifies the validity of the PRT with Microsoft Entra ID before accepting it.

Android Platform:

- A PRT is valid for 90 days and is continuously renewed as long as the device is in use. However, it's only valid for 14 days if the device isn't in use.
- A PRT is only issued and renewed during native app authentication. A PRT isn't renewed or issued during a browser session.
- It's possible to obtain a PRT without the need for device registration ([Workplace Join](#)) and enable SSO.
- PRTs obtained without device registration can't satisfy the authorization criteria for Conditional Access that relies on the device's status or compliance.

How is the PRT protected?

A PRT is protected by binding it to the device the user has signed in to. Microsoft Entra ID and Windows 10 or newer enable PRT protection through the following methods:

- **During first sign in:** During first sign in, a PRT is issued by signing requests using the device key cryptographically generated during device registration. On a device with a valid and functioning TPM, the device key is secured by the TPM preventing any malicious access. A PRT isn't issued if the corresponding device key signature can't be validated.
- **During token requests and renewal:** When a PRT is issued, Microsoft Entra ID also issues an encrypted session key to the device. It's encrypted with the public transport key (tkpub) generated and sent to Microsoft Entra ID as part of device registration. This session key can only be decrypted by the private transport key (tkpriv) secured by the TPM. The session key is the Proof-of-Possession (POP) key for any requests sent to Microsoft Entra ID. The session key is also protected by the TPM and no other OS component can access it. Token requests or PRT renewal requests are securely signed by this session key through the TPM and hence, can't be tampered with. Microsoft Entra invalidates any requests from the device that aren't signed by the corresponding session key.

By securing these keys with the TPM, we enhance the security for PRT from malicious actors trying to steal the keys or replay the PRT. So, using a TPM greatly enhances the security of Microsoft Entra joined, Microsoft Entra hybrid joined, and Microsoft Entra registered devices against credential theft. For performance and reliability, TPM 2.0 is the recommended version for all Microsoft Entra device registration scenarios on Windows 10 or newer. After the Windows 10, 1903 update, Microsoft Entra ID doesn't use TPM 1.2 for any of the above keys due to reliability issues.

How are app tokens and browser cookies protected?

App tokens: When an app requests token through WAM, Microsoft Entra ID issues a refresh token and an access token. However, WAM only returns the access token to the app and secures the refresh token in its cache by encrypting it with the user's data protection application programming interface (DPAPI) key. WAM securely uses the refresh token by signing requests with the session key to issue further access tokens. The DPAPI key is secured by a Microsoft Entra ID based symmetric key in Microsoft Entra itself. When the device needs to decrypt the user profile with the DPAPI key, Microsoft Entra ID provides the DPAPI key encrypted by the session key, which CloudAP plugin requests TPM to decrypt. This functionality ensures consistency in securing refresh tokens and avoids applications implementing their own protection mechanisms.

Browser cookies: In Windows 10 or newer, Microsoft Entra ID supports browser SSO in Internet Explorer and Microsoft Edge natively, in Google Chrome via the Windows 10

accounts extension and in Mozilla Firefox v91+ via a browser setting. The security is built not only to protect the cookies but also the endpoints to which the cookies are sent. Browser cookies are protected the same way a PRT is, by utilizing the session key to sign and protect the cookies.

When a user initiates a browser interaction, the browser (or extension) invokes a COM native client host. The native client host ensures that the page is from one of the allowed domains. The browser could send other parameters to the native client host, including a nonce, however the native client host guarantees validation of the hostname. The native client host requests a PRT-cookie from CloudAP plugin, which creates and signs it with the TPM-protected session key. As the PRT-cookie is signed by the session key, it's difficult to tamper with. This PRT-cookie is included in the request header for Microsoft Entra ID to validate the device it's originating from. If using the Chrome browser, only the extension explicitly defined in the native client host's manifest can invoke it preventing arbitrary extensions from making these requests. Once Microsoft Entra ID validates the PRT cookie, it issues a session cookie to the browser. This session cookie also contains the same session key issued with a PRT. During subsequent requests, the session key is validated effectively binding the cookie to the device and preventing replays from elsewhere.

When does a PRT get an MFA claim?

A PRT can get a multifactor authentication claim in specific scenarios. When an MFA-based PRT is used to request tokens for applications, the MFA claim is transferred to those app tokens. This functionality provides a seamless experience to users by preventing MFA challenge for every app that requires it. A PRT can get an MFA claim in the following ways:

- **Sign in with Windows Hello for Business:** Windows Hello for Business replaces passwords and uses cryptographic keys to provide strong two-factor authentication. Windows Hello for Business is specific to a user on a device, and itself requires MFA to provision. When a user logs in with Windows Hello for Business, the user's PRT gets an MFA claim. This scenario also applies to users logging in with smart cards if smart card authentication produces an MFA claim from AD FS.
 - As Windows Hello for Business is considered multifactor authentication, the MFA claim is updated when the PRT itself is refreshed, so the MFA duration will continually extend when users sign in with Windows Hello for Business.
- **MFA during WAM interactive sign in:** During a token request through WAM, if a user is required to do MFA to access the app, the PRT that is renewed during this interaction is imprinted with an MFA claim.

- In this case, the MFA claim isn't updated continuously, so the MFA duration is based on the lifetime set on the directory.
- When a previous existing PRT and RT are used for access to an app, the PRT and RT are regarded as the first proof of authentication. A new RT is required with a second proof and an imprinted MFA claim. This process also issues a new PRT and RT.

Windows 10 or newer maintain a partitioned list of PRTs for each credential. So, there's a PRT for each of Windows Hello for Business, password, or smart card. This partitioning ensures that MFA claims are isolated based on the credential used, and not mixed up during token requests.

 **Note**

When using password to sign in to Windows 10 or newer Microsoft Entra joined or Microsoft Entra hybrid joined device, MFA during WAM interactive sign in might be required after session key associated with PRT is rolled.

How is a PRT invalidated?

A PRT is invalidated in the following scenarios:

- **Invalid user:** If a user is deleted or disabled in Microsoft Entra ID, their PRT is invalidated and can't be used to obtain tokens for applications. If a deleted or disabled user already signed in to a device before, cached sign-in would log them in, until CloudAP is aware of their invalid state. Once CloudAP determines that the user is invalid, it blocks subsequent logons. An invalid user is automatically blocked from sign in to new devices that don't have their credentials cached.
- **Invalid device:** If a device is deleted or disabled in Microsoft Entra ID, the PRT obtained on that device is invalidated and can't be used to obtain tokens for other applications. If a user is already signed in to an invalid device, they can continue to do so. But all tokens on the device are invalidated and the user doesn't have SSO to any resources from that device.
- **Password change:** If a user obtained the PRT with their password, the PRT is invalidated by Microsoft Entra ID when the user changes their password. Password change results in the user getting a new PRT. This invalidation can happen in two different ways:
 - If user signs in to Windows with their new password, CloudAP discards the old PRT and requests Microsoft Entra ID to issue a new PRT with their new

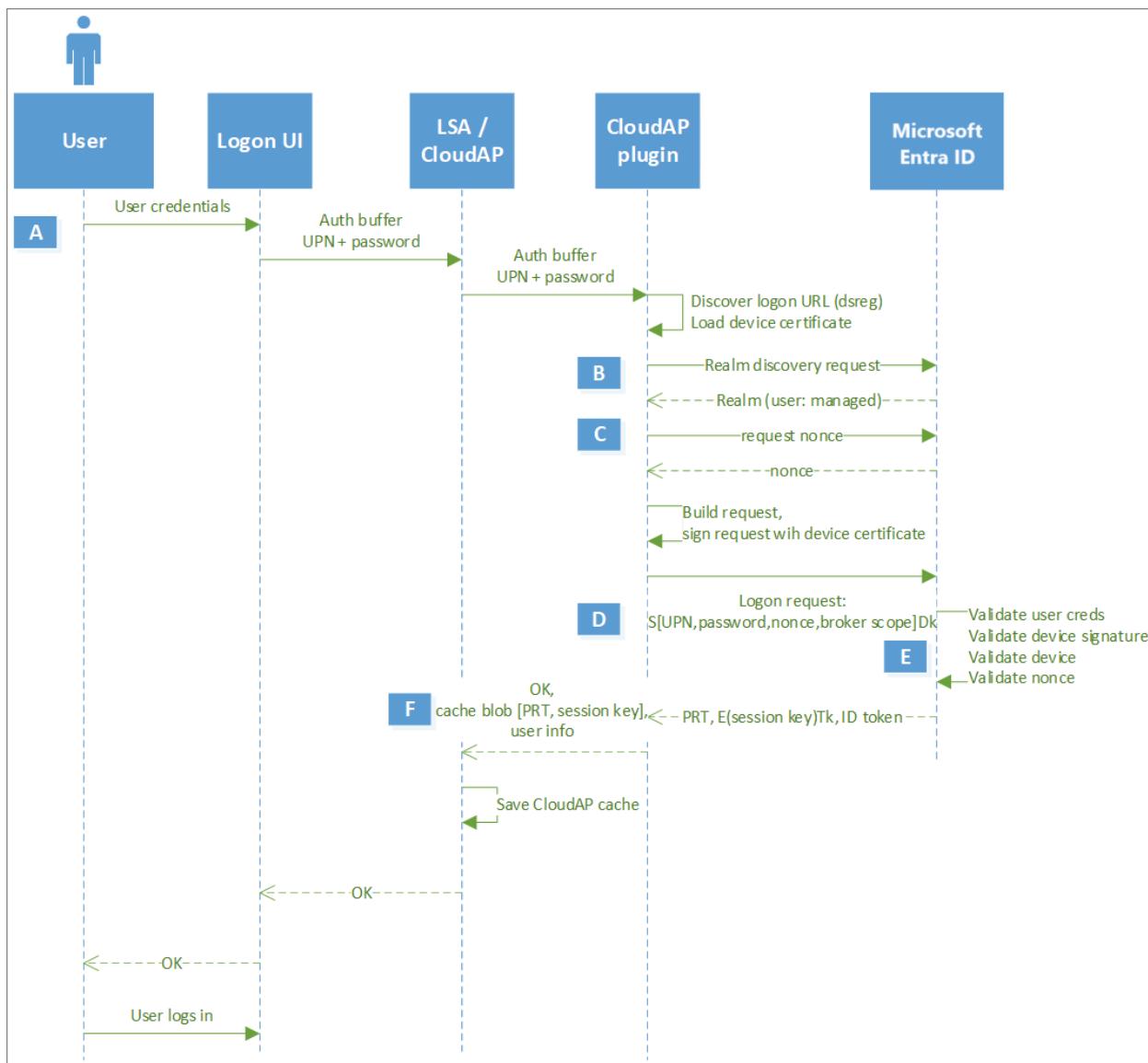
password. If user doesn't have an internet connection, the new password can't be validated, Windows might require the user to enter their old password.

- If a user has logged in with their old password or changed their password after signing in to Windows, the old PRT is used for any WAM-based token requests. In this scenario, the user is prompted to reauthenticate during the WAM token request and a new PRT is issued.
- **TPM issues:** Sometimes, a device's TPM can falter or fail, leading to inaccessibility of keys secured by the TPM. In this case, the device is incapable of getting a PRT or requesting tokens using an existing PRT as it can't prove possession of the cryptographic keys. As a result, any existing PRT is invalidated by Microsoft Entra ID. When Windows 10 detects a failure, it initiates a recovery flow to reregister the device with new cryptographic keys. With Microsoft Entra hybrid join, just like the initial registration, the recovery happens silently without user input. For Microsoft Entra joined or Microsoft Entra registered devices, the recovery needs to be performed by a user who has administrator privileges on the device. In this scenario, the recovery flow is initiated by a Windows prompt that guides the user to successfully recover the device.

Detailed flows

The following diagrams illustrate the underlying details in issuing, renewing, and using a PRT to request an access token for an application. In addition, these steps also describe how the previously mentioned security mechanisms are applied during these interactions.

PRT issuance during first sign in



ⓘ Note

In Microsoft Entra joined devices, Microsoft Entra PRT issuance (steps A-F) happens synchronously before the user can sign in to Windows. In Microsoft Entra hybrid joined devices, on-premises Active Directory is the primary authority. So, the user is able to login Microsoft Entra hybrid joined Windows after they can acquire a TGT to login, while the PRT issuance happens asynchronously. This scenario doesn't apply to Microsoft Entra registered devices as logon doesn't use Microsoft Entra credentials.

ⓘ Note

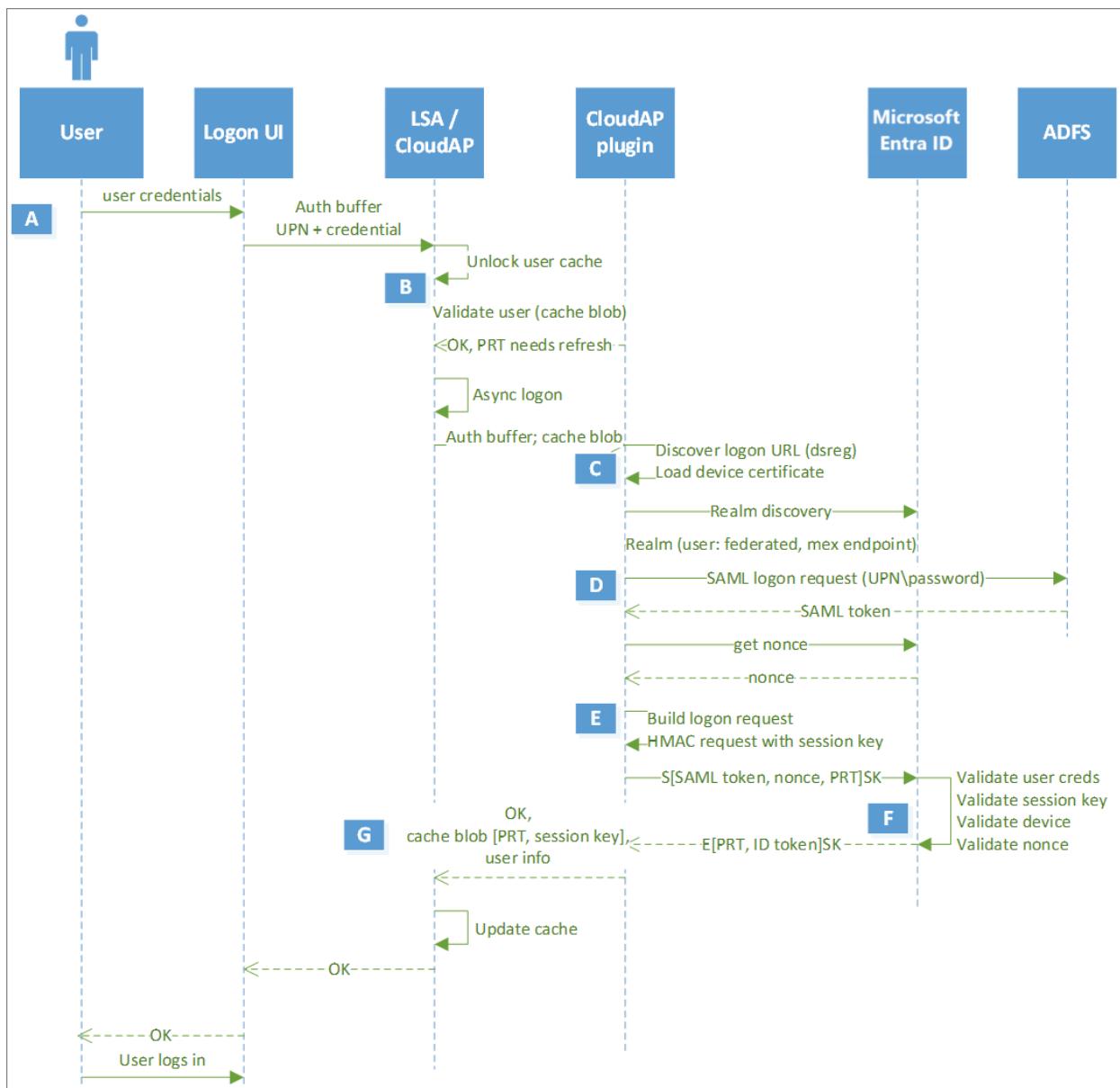
In a Microsoft Entra hybrid joined Windows environment, the issuance of the PRT occurs asynchronously. The issuance of the PRT might fail due to issues with the federation provider. This failure can result in sign on issues when users try to access

cloud resources. It's important to troubleshoot this scenario with the federation provider.

[+] Expand table

Step	Description
A	User enters their password in the sign in UI. LogonUI passes the credentials in an auth buffer to LSA, which in turns passes it internally to CloudAP. CloudAP forwards this request to the CloudAP plugin.
B	CloudAP plugin initiates a realm discovery request to identify the identity provider for the user. If user's tenant has a federation provider setup, Microsoft Entra ID returns the federation provider's Metadata Exchange endpoint (MEX) endpoint. If not, Microsoft Entra ID returns that the user is managed indicating that user can authenticate with Microsoft Entra ID.
C	If the user is managed, CloudAP gets the nonce from Microsoft Entra ID. If the user is federated, CloudAP plugin requests a Security Assertion Markup Language (SAML) token from the federation provider with the user's credentials. Nonce is requested before the SAML token is sent to Microsoft Entra ID.
D	CloudAP plugin constructs the authentication request with the user's credentials, nonce, and a broker scope, signs the request with the Device key (dkpriv) and sends it to Microsoft Entra ID. In a federated environment, CloudAP plugin uses the SAML token returned by the federation provider instead of the user' credentials.
E	Microsoft Entra ID validates the user credentials, the nonce, and device signature, verifies that the device is valid in the tenant and issues the encrypted PRT. Along with the PRT, Microsoft Entra ID also issues a symmetric key, called the Session key encrypted by Microsoft Entra ID using the Transport key (tkpub). In addition, the Session key is also embedded in the PRT. This Session key acts as the Proof-of-possession (PoP) key for subsequent requests with the PRT.
F	CloudAP plugin passes the encrypted PRT and Session key to CloudAP. CloudAP request the TPM to decrypt the Session key using the Transport key (tkpriv) and reencrypt it using the TPM's own key. CloudAP stores the encrypted Session key in its cache along with the PRT.

PRT renewal in subsequent logons



[Expand table](#)

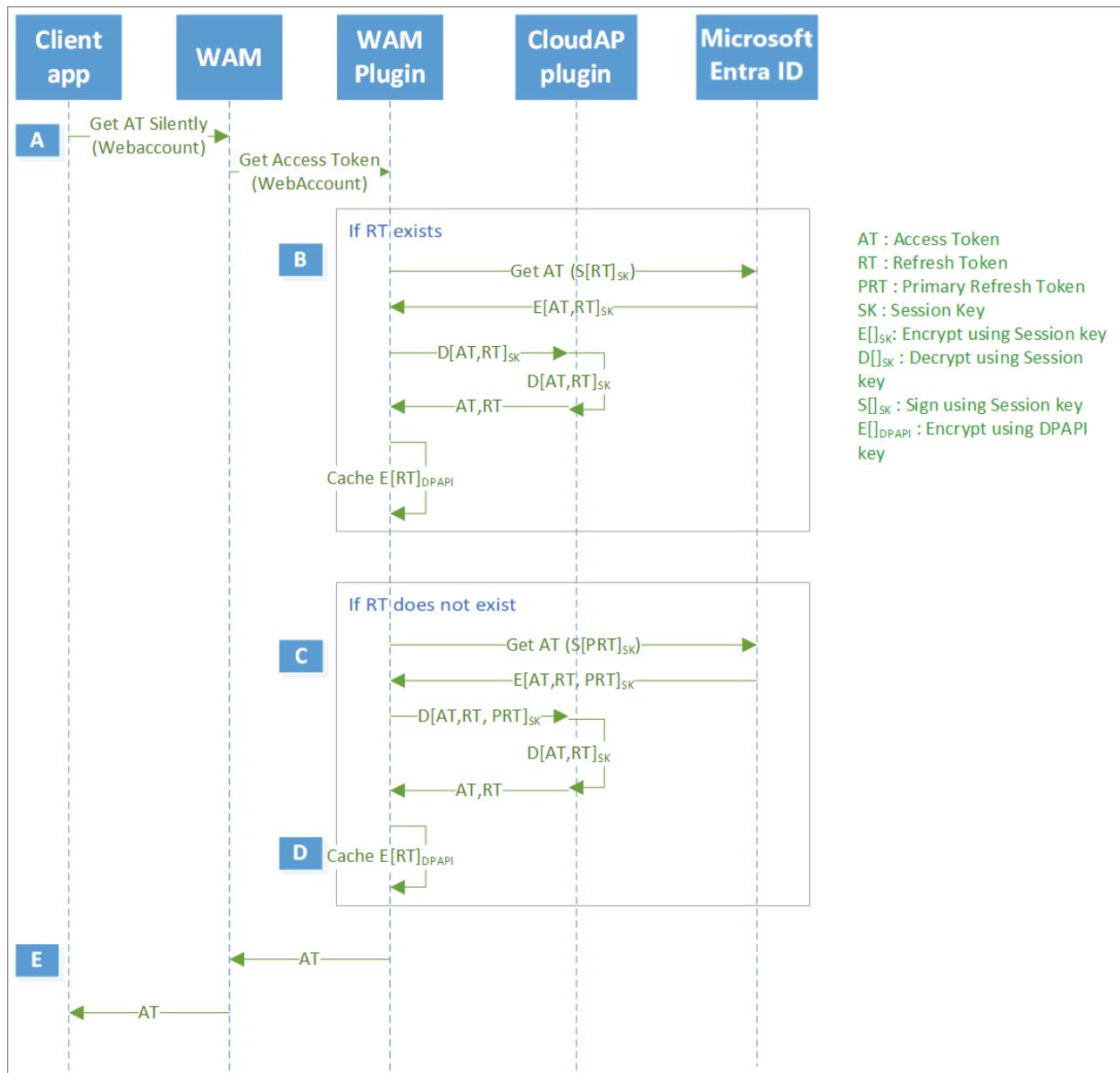
Step	Description
A	User enters their password in the sign in UI. LogonUI passes the credentials in an auth buffer to LSA, which in turns passes it internally to CloudAP. CloudAP forwards this request to the CloudAP plugin.
B	If the user has previously signed in to the session, Windows initiates cached sign in and validates credentials to log the user in. Every 4 hours, the CloudAP plugin initiates PRT renewal asynchronously.
C	CloudAP plugin initiates a realm discovery request to identify the identity provider for the user. If the user's tenant has a federation provider setup, Microsoft Entra ID returns the federation provider's Metadata Exchange endpoint (MEX) endpoint. If not, Microsoft Entra ID returns that the user is managed indicating that user can authenticate with Microsoft Entra ID.
D	If the user is federated, CloudAP plugin requests a SAML token from the federation provider with the user's credentials. Nonce is requested before the SAML token is sent to

Step	Description
	Microsoft Entra ID. If the user is managed, CloudAP will directly get the nonce from Microsoft Entra ID.
E	CloudAP plugin constructs the authentication request with the user's credentials, nonce, and the existing PRT, signs the request with the Session key and sends it to Microsoft Entra ID. In a federated environment, CloudAP plugin uses the SAML token returned by the federation provider instead of the user' credentials.
F	Microsoft Entra ID validates the Session key signature by comparing it against the Session key embedded in the PRT, validates the nonce and verifies that the device is valid in the tenant and issues a new PRT. As seen before, the PRT is again accompanied with the Session key encrypted by Transport key (tkpub).
G	CloudAP plugin passes the encrypted PRT and Session key to CloudAP. CloudAP requests the TPM to decrypt the Session key using the Transport key (tkpriv) and reencrypt it using the TPM's own key. CloudAP stores the encrypted Session key in its cache along with the PRT.

 **Note**

A PRT can be renewed externally without the need of a VPN connection when `usernamemixed` endpoints are enabled externally.

PRT usage during app token requests

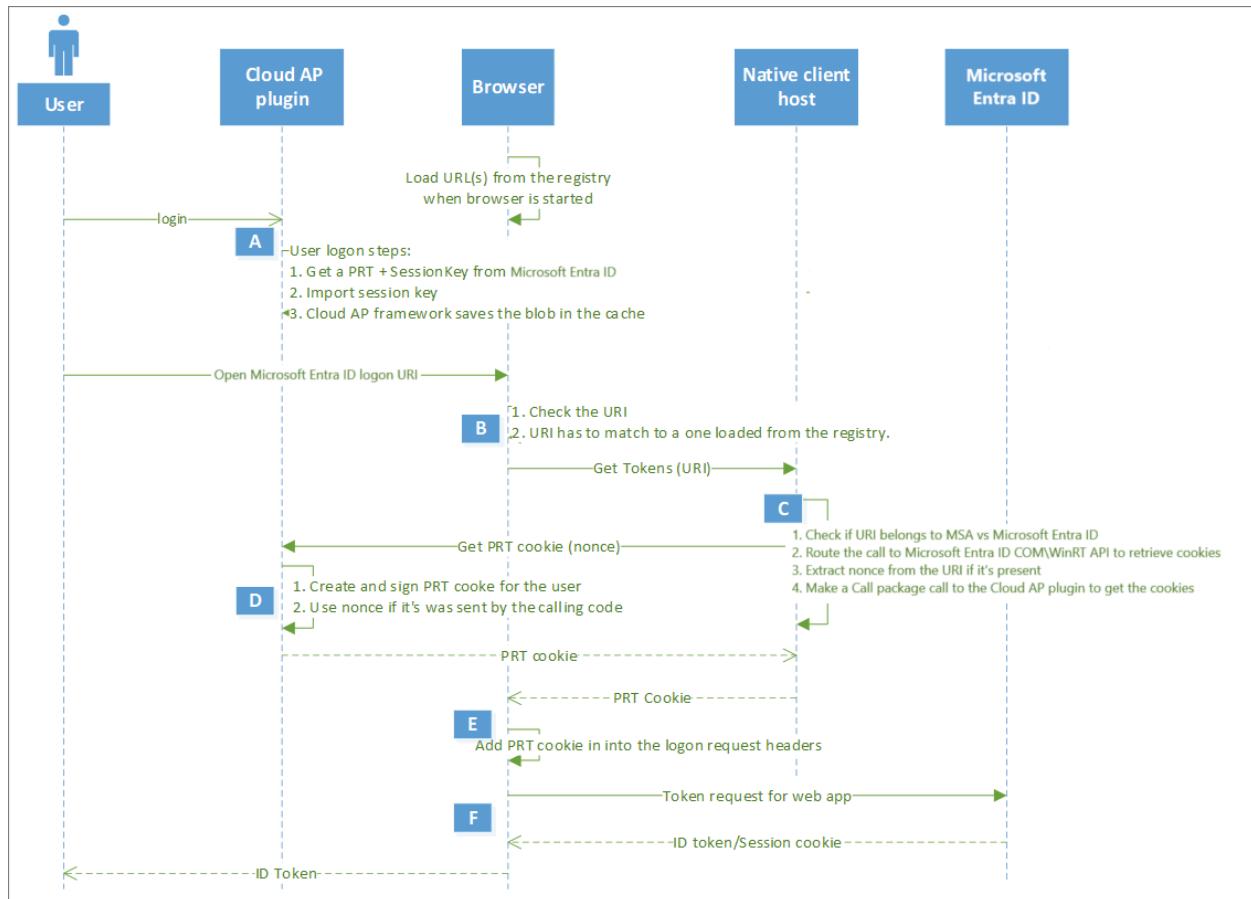


[Expand table](#)

Step	Description
A	An application, like Microsoft Outlook, initiates a token request to WAM. WAM, in turn, asks the Microsoft Entra WAM plugin to service the token request.
B	If a Refresh token for the application is already available, Microsoft Entra WAM plugin uses it to request an access token. To provide proof of device binding, WAM plugin signs the request with the Session key. Microsoft Entra ID validates the Session key and issues an access token and a new refresh token for the app, encrypted by the Session key. WAM plugin requests CloudAP plugin to decrypt the tokens, which, in turn, requests the TPM to decrypt using the Session key, resulting in WAM plugin getting both the tokens. Next, WAM plugin provides only the access token to the application, while it reencrypts the refresh token with DPAPI and stores it in its own cache
C	If a Refresh token for the application isn't available, Microsoft Entra WAM plugin uses the PRT to request an access token. To provide proof of possession, WAM plugin signs the request containing the PRT with the Session key. Microsoft Entra ID validates the Session key signature by comparing it against the Session key embedded in the PRT, verifies that

Step	Description
	the device is valid and issues an access token and a refresh token for the application. in addition, Microsoft Entra ID can issue a new PRT (based on refresh cycle), all of them encrypted by the Session key.
D	WAM plugin requests CloudAP plugin to decrypt the tokens, which, in turn, requests the TPM to decrypt using the Session key, resulting in WAM plugin getting both the tokens. Next, WAM plugin provides only the access token to the application, while it reencrypts the refresh token with DPAPI and stores it in its own cache. WAM plugin uses the refresh token going forward for this application. WAM plugin also gives back the new PRT to CloudAP plugin, which validates the PRT with Microsoft Entra ID before updating it in its own cache. CloudAP plugin uses the new PRT going forward.
E	WAM provides the newly issued access token to WAM, which in turn, provides it back to the calling application

Browser SSO using PRT



[Expand table](#)

Step	Description
A	User logs in to Windows with their credentials to get a PRT. Once user opens the browser, browser (or extension) loads the URLs from the registry.

Step	Description
B	When a user opens a Microsoft Entra login URL, the browser or extension validates the URL with the ones obtained from the registry. If they match, the browser invokes the native client host for getting a token.
C	The native client host validates that the URLs belong to the Microsoft identity providers (Microsoft account or Microsoft Entra ID), extracts a nonce sent from the URL and makes a call to CloudAP plugin to get a PRT cookie.
D	The CloudAP plugin creates the PRT cookie, sign in with the TPM-bound session key and send it back to the native client host.
E	The native client host returns this PRT cookie to the browser, which includes it as part of the request header called x-ms-RefreshTokenCredential and request tokens from Microsoft Entra ID.
F	Microsoft Entra ID validates the Session key signature on the PRT cookie, validates the nonce, verifies that the device is valid in the tenant, and issues an ID token for the web page and an encrypted session cookie for the browser.

Note

The Browser SSO flow described in the previous steps doesn't apply for sessions in private modes such as InPrivate in Microsoft Edge, Incognito in Google Chrome (when using the Microsoft Accounts extension) or in private mode in Mozilla Firefox v91+.

Next steps

For more information on troubleshooting PRT-related issues, see the article [Troubleshooting Microsoft Entra hybrid joined Windows 10 or newer and Windows Server 2016 devices](#).

Feedback

Was this page helpful?

 Yes

 No

[Provide product feedback](#) 

Understanding tokens in Microsoft Entra ID

Article • 05/01/2025

As attackers increasingly use sophisticated attacks, it's crucial to guard against data exfiltration by hardening your environment against token theft and token replay. Although challenging, there are simple steps you can take to reduce your attack surface and increase the cost for attackers to successfully steal and replay tokens. A robust strategy to protect your tokens requires a multi-layered defense-in-depth approach, which should include:

- Deploying phishing-resistant credentials
- Hardening your devices against malware-based attacks
- Using Device-based and Risk-based Conditional Access
- Enforcing device-bound tokens where possible
- Implementing network-based enforcements

This document summarizes the basics of what tokens are, how tokens are stolen, and provide concrete steps you can take to mitigate the risk of successful attacks in your environment. Due to the complexity and wide variety of tokens in Microsoft Entra, some topics are generalized for simplicity and may not cover all edge cases. However, this guidance covers most scenarios for public clients. [Confidential client](#) scenarios aren't in scope.

Password-based attacks still comprise over 99% of attacks seen by Microsoft and are the root cause of most compromised identities. Organizations should deploy phishing-resistant MFA as a frontline of defense for their identities. Doing so forces adversaries to adjust their tactics, moving to the next logical attack vector, which is likely token theft. "Although token theft results in far fewer identity compromises than password attacks, our detections indicate incidents have grown to an estimated 39,000 per day. Moreover, over the last year we've seen a 146% rise in AiTM phishing attacks, which occur when attackers trick users into clicking a link and completing MFA on the attacker's behalf."^{*} While the deployment of phishing-resistant MFA should be a top priority, organizations should also begin preparing a token theft mitigation strategy as token theft attack vectors continue to increase over time. Protecting against token theft becomes more important as password-based attacks become less viable.

* From [2024 Microsoft Digital Defense Report](#) (page 40)

What is a token?

Tokens are digital objects used in various authentication and authorization processes to grant access to resources. They verify the identity of a user or a workload and grant access to resources without requiring the transmission of a password or credential for each transaction. Tokens encapsulate information about the user's identity and their permissions in a secure

format, ensuring that sensitive information remains protected during the authentication process.

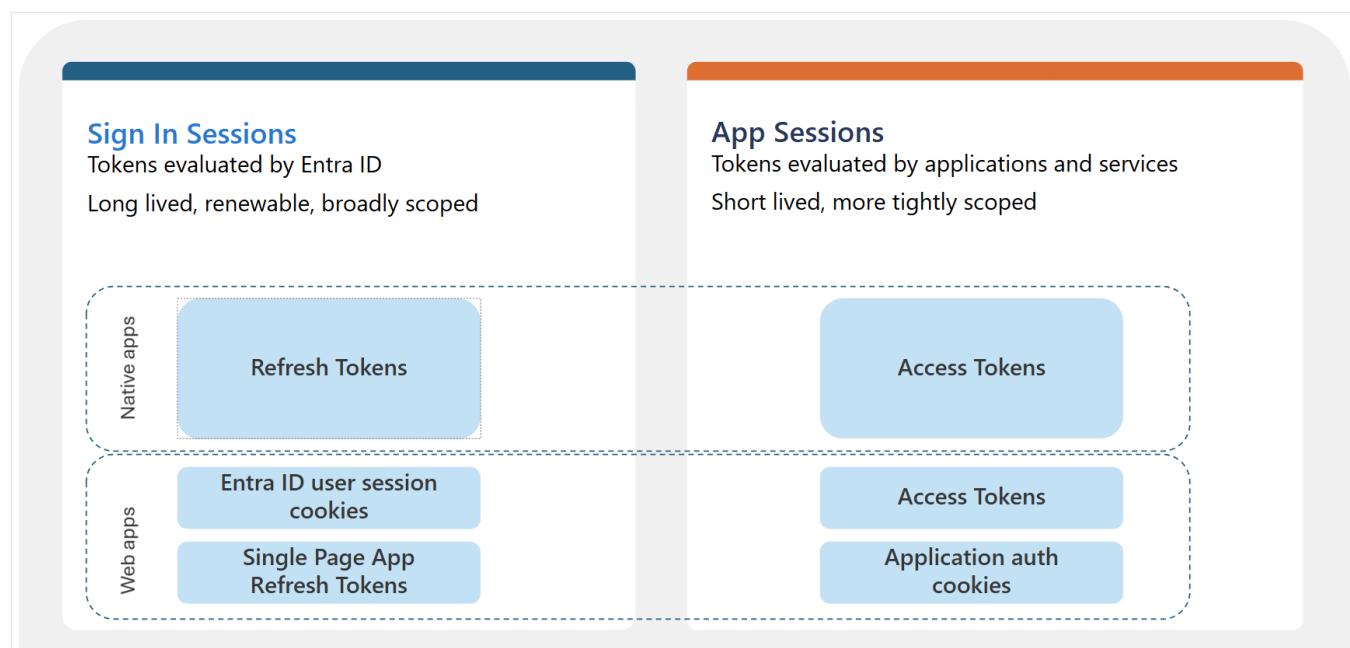
In digital environments, tokens play a critical role in enhancing security by enabling secure and efficient authentication mechanisms. They help reduce the risk of credential theft by minimizing the exposure of credentials over the network. However, they have the characteristic that if the device or network is compromised, they can be exfiltrated by an attacker. The attacker can then use these tokens to gain access to resources as the signed-in user.

Summary of the kinds of tokens

There are many kinds of tokens, but they generally fall into one of two categories:

- **Sign-in sessions** – These tokens maintain the signed-in state of a user, allowing the user to access resources without the need for frequent reauthentication. They're passed to the identity provider to request tokens that are in the app session category. They're also known as Refresh Tokens in the OAuth 2.0 standard.
- **App sessions** – These tokens authorize access to specific applications. They're short-lived and are played between the client and the application. They're also known as Access Tokens in the OAuth 2.0 standard.

Tokens may also vary depending on the client application. Web applications accessed via browsers sometimes use different kinds of tokens compared with native apps such as Outlook and Teams.



As a best practice, you want to prioritize protecting your sign-in session tokens first as these tokens can last for weeks or months, potentially enabling persistent unauthorized access if stolen.

Another difference between the two token families: Sign-in session tokens are revocable by design while app sessions are typically not. For example, Entra ID Access Tokens can only be revoked if the application has integrated Continuous Access Evaluation.

[+] Expand table

Token Type	Issued by	Purpose	Scoped to Resource	Lifetime	Revocable	Renewable
Primary Refresh Token (PRT)	Entra ID	Request Access Tokens	No – Can request an access token for any resource	14 days*	Yes	Yes
Refresh Token	Entra ID	Request Access Tokens	Yes	90 days*	Yes	Yes
Access Token	Entra ID	Access the resource	Yes	Variable 60-90 minutes	Yes, if CAE capable	No
App auth cookie	Web app	Access the resource	Yes	Determined by application	Depends on application	No

*Rolling window – Lifetime is restarted with every use of the token.

Token theft attack vectors

Adversaries can employ many different attack vectors to steal tokens. Once a token is stolen, the adversary can then impersonate the user, gaining unauthorized access and even exfiltrating sensitive data. Some examples of these attack vectors include:

- **Adversary-in-the-middle:** A sophisticated form of a Man-in-the-Middle (MitM) attack. In this scenario, an attacker positions themselves between two communicating parties, intercepting and potentially altering the communication without either party's knowledge. This scenario allows the attacker to capture sensitive information such as credentials, session cookies, and other data, even bypassing security measures like multifactor authentication. Learn more about [Adversary-in-the-middle phishing attacks ↗](#).
- **Malware:** Malware can steal tokens from a device by infiltrating the system and monitoring network traffic or accessing stored data. Once installed, the malware can capture authentication tokens, session cookies, or other credentials by intercepting communications between the device and legitimate services. It can also exploit vulnerabilities to extract tokens directly from memory or storage.

In this article, we focus primarily on how to defeat attacks that are directed towards end users, such as those previously listed. Attack vectors such as server-side or application compromise

are out of scope for this article. To mitigate these kinds of attacks, organizations should follow the general best practices of:

- Secure your application's authentication
- Ensure application permissions are least privileged
- Avoid capture and retention of tokens in server-side logs
- Monitor OAuth applications with permissions to other resources for compromise

Next steps

To understand how to protect tokens in Microsoft Entra ID, continue to [Protecting tokens in Microsoft Entra ID](#).

Protecting tokens in Microsoft Entra

Article • 04/25/2025

This article is a continuation to [Understanding tokens in Microsoft Entra ID](#). This article assumes you've read Understanding tokens in Microsoft Entra ID and provides concrete steps you can take to mitigate the risk of successful token theft/replay attacks in your environment.

The recommendations of this article span across multiple Microsoft technology solutions which have a range of licensing requirements. Ensure that you've the proper licensing for:

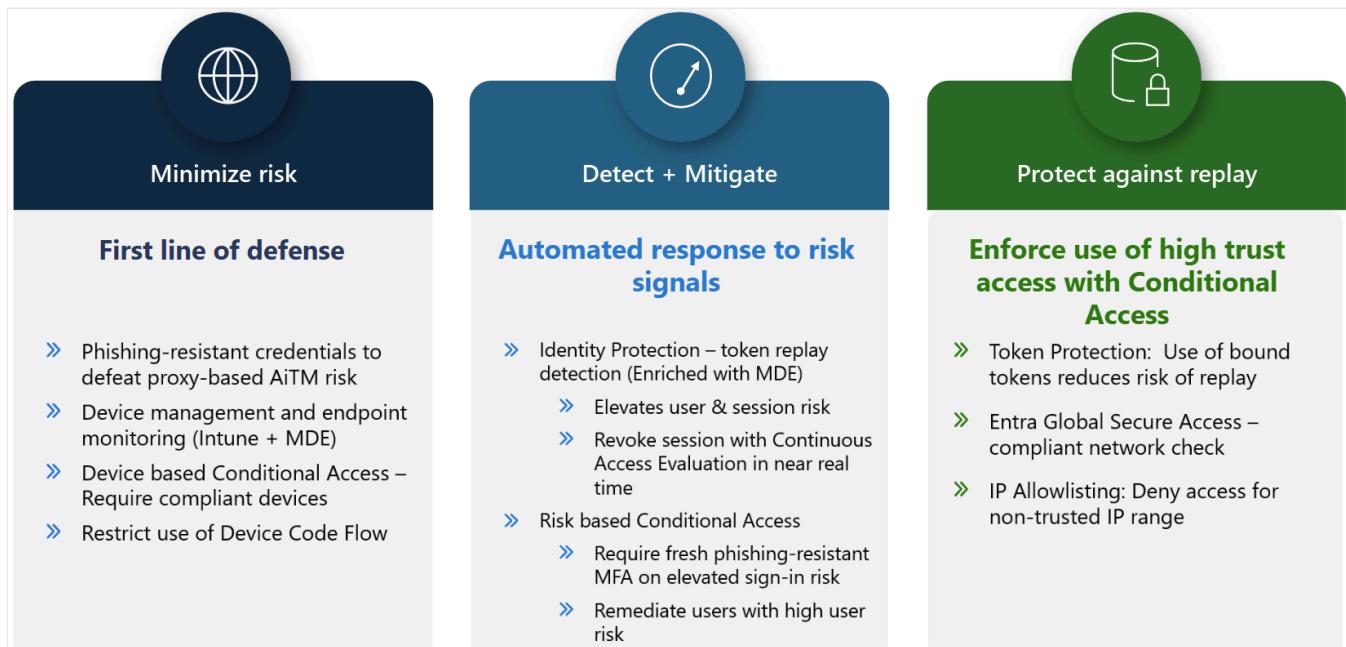
- [Conditional Access](#)
- [Microsoft Entra Internet Access for Microsoft services](#)
- [Microsoft Entra ID Protection](#)
- [Token Protection](#)
- [Microsoft Intune \(minimum Plan 1\) ↗](#)
- [Microsoft Defender for Endpoint XDR](#)

Defense-in-depth strategy against token theft

There are several capabilities you can enable to reduce your attack surface area and reduce the risk of successful token compromise. In the next sections we'll cover many Microsoft security capabilities that fall into one of three categories:

- **Minimize risk:** Harden or reduce the attack surface making successful token theft more difficult.
- **Detect + Mitigate:** Detect successful token theft and configure automatic mitigation if possible.
- **Protect against replay:** Block replay or reduce the impact of successful token theft.

The following is a high-level summary capturing the key areas organizations should focus on as part of their token theft protection strategy.



Token Theft – minimize risk

Preventing a successful token theft incident from occurring in the first place is the most effective way to protect your organization. Organizations should harden devices against device-based token exfiltration methods using Microsoft Defender for Endpoint and Microsoft Intune. Organizations should also deploy controls to prevent users from accessing malicious or risky destinations on the internet.

Harden your devices

Perform the following configurations and deployments to harden all devices/endpoints as frontline of defense against malware-based token theft. Before you get started, ensure that your devices are enrolled with Intune, and that [Microsoft Defender for Endpoint](#) is deployed.

[Expand table](#)

Control	Windows 10/11	macOS	Linux
Enable Microsoft Defender Antivirus always-on protection for real-time protection, behavior monitoring, and heuristics to identify malware based on known suspicious and malicious activities.	X	X	X
Enable Microsoft Defender Antivirus cloud protection to help protect against malware on your endpoints and across your network.	X	X	X
Enable network protection in Microsoft Defender for Endpoint to protect devices from certain Internet-based events by preventing connections to malicious or suspicious sites.	X	X	X

Control	Windows 10/11	macOS	Linux
Enable tamper protection in Microsoft Defender for Endpoint to protect certain security settings, such as virus and threat protection, from being disabled or changed.	X	X	-
Create a device compliance policy in Intune that requires the machine risk level designation by Microsoft Defender for Endpoint as <i>low</i> or <i>clear</i> for compliance.	X	X	-

Even with device hardening policies in place, organizations must [create a Conditional Access policy](#) that requires users to use a **compliant device** to access all resources. This ensures your devices have successfully deployed your device-hardening configurations and that users can't access applications and resources from unmanaged or insecure devices.

Other configurations for Windows

- [Configure Credential Guard](#) to isolate the Local Security Authority, protecting against credential theft from memory.
- Review your [Windows Enrollment Attestation](#) report. Validate your Windows devices meet your TPM requirements. Take corrective action on any device that fails the TPM attestation.

Other configurations for macOS

- [Disable iCloud Keychain sync with Microsoft Intune](#) to prevent synchronization of Entra tokens that may be stored in Keychain.
- [Enable Microsoft Enterprise SSO plug-in for Apple devices](#) to enable Enterprise Apps to leverage the Primary Refresh Token (PRT) for authentication.
- [Configure Platform SSO for macOS devices](#) (secure enclave) to provide secure, phishing-resistant authentication to Mac devices using hardware-bound cryptographic keys.

Harden mobile devices

Mobile devices such as iOS and Android can be hardened using [mobile threat defense](#). Mobile threat defense includes a range of capabilities that can protect against compromised devices, and web threats that can block malware from being installed in the first place, preventing token exfiltration (and other threats) early in the kill chain.

Microsoft Defender XDR Attack Disruption

Adversary-in-the-middle (AiTM) is a covered scenario in Microsoft Defender XDR Attack disruption, which provides coordinated threat defense early in the kill chain of an attack. Deploy all Defender XDR workloads (Defender for Identity, Defender for Office, and Defender for Cloud Apps) and ensure Attack Disruption is configured in Microsoft Defender XDR by following all documented [pre-requisites and configurations](#). Attack disruption detects AiTM attacks at an early stage and disrupt the attack by applying mitigating security controls automatically to endpoints and identities.

Harden against internet threats

Organizations who use Microsoft Edge should enable [Microsoft Defender SmartScreen](#). Microsoft Defender SmartScreen provides an early warning system against websites that might engage in phishing attacks or attempt to distribute malware through a focused attack.

Microsoft Entra Internet Access provides more protection covering the entire Internet. Organizations can deploy Global Secure Access (GSA) clients to managed devices to block malicious and/or unauthorized web content using [web content filtering](#). This reduces the likelihood of users navigating to malicious websites which can lead to the installation of malware or otherwise compromising the device. Administrators should, at minimum, block the *illegal software* category but should also review and consider blocking all [liability web categories](#).

Restrict use of device code flow

Device code flow is particularly useful for devices that have limited input capabilities or lack a web browser. However, device code flow can be used as part of a phishing attack or to access corporate resources on unmanaged devices. You can configure the device code flow control along with other controls in your Conditional Access policies. For example, if device code flow is used for android-based conference room devices, you might choose to block device code flow everywhere except for android devices in a specific network location.

You should only allow device code flow where necessary. Microsoft recommends blocking device code flow wherever possible.

[Learn more about Conditional Access Authentication flows.](#)

Token Theft - detect and mitigate

Organizations should actively monitor for successful or attempted token theft attacks. There are many alerts generated from various Microsoft products that can indicate potential token theft or account compromise. A high-level summary of these detections is listed below. For an

in-depth guide on how to monitor for, detect, and respond to identified token theft using a SIEM, refer to the [Token theft playbook](#).

Conditional Access Policies

Organizations should configure the following Conditional Access policies:

- Require interactive reauthentication for sensitive operations (authentication context)
- Require interactive authentication for risky sign-ins
- Detect and remediate high-risk users

These Conditional Access policies provide more automated token theft remediation and/or address other threat vectors that could be used in token-based attacks.

Require interactive reauthentication for sensitive operations

Organizations can configure certain actions with authentication contexts to trigger the evaluation of Conditional Access policies outside of the normal authentication flows. For example, a Conditional Access policy can be configured to evaluate when an administrator activates a role in Privileged Identity Management (PIM) or when a user performs a specific action within an application. Administrators should configure a Conditional Access policy that requires interactive phishing-resistant authentication (sign-in frequency set to every time) for authentication context actions deemed sensitive. If the attacker is unable to reauthenticate, access is denied, preventing the stolen sign-in session from being used to complete the sensitive operation.

[Learn how to configure Authentication Context in Conditional Access.](#)

[Learn how to use Authentication Context in applications \(developer guidance\).](#)

Require interactive authentication for risky sign-ins

With Entra ID Identity Protection, enhanced by more detections from Microsoft Defender for Endpoint, Entra ID can detect suspicious sign-in attempts in real time. For instance, if an attacker steals and attempts to replay a refresh token, Entra ID Identity Protection may identify that the sign-in has unfamiliar properties and elevate the sign-in risk level for this event. Administrators should configure a Conditional Access policy that requires interactive phishing-resistant authentication (sign-in frequency set to every time) for medium or higher sign-in risk levels. If the attacker is unable to reauthenticate, access is denied, preventing the stolen sign-in session from being used to gain or extend unauthorized access.

[Learn how to configure Risk-Based Conditional Access policies.](#)

Detect and remediate high-risk users

With Entra ID Identity Protection, enhanced by more detections from Microsoft Defender for Endpoint, Entra ID generates a user risk score for every account, indicating the level of certainty regarding whether the account has been compromised. If Entra ID or Microsoft Defender for Endpoint detects signs of successful token theft, it's highly likely that the user's risk score will be set to *High*. When this occurs, you can automatically block or remediate the account (for example, secure password change), preventing the adversary from further exploiting any unauthorized access they may have achieved.

Applications that support continuous access evaluation automatically revoke access in near-real time when high user risk is detected, issuing a redirect back to Entra ID for reauthentication and reauthorization.

[Learn how to configure Risk-Based Conditional Access policies.](#)

Microsoft Defender XDR

Deploy Defender XDR workloads to alert on suspicious or anomalous behaviors surrounding token theft.

- Use [Defender for Office 365](#) to detect and block malicious emails, links, and files
- Use Microsoft Defender for Cloud Apps [connectors](#), Microsoft 365 Defender raises AiTM-related alerts in multiple scenarios. For Entra ID customers using Microsoft Edge, attempts by attackers to replay session cookies to access cloud applications are detected by Defender for Cloud Apps connectors for [Office 365](#) and [Azure](#).

Microsoft Defender XDR when using Defender for Cloud Apps connectors and Defender for Endpoint can raise these alerts:

- Stolen session cookie was used
- Possible AiTM phishing attempt

Other detections

[Entra ID Protection risk detections](#)

- Anomalous Token
- Attacker in the Middle
- Unfamiliar sign-in properties

[Microsoft Defender for Office 365 detections](#)

- Email messages containing malicious file removed after delivery
- Email messages from a campaign removed after delivery

- A potentially malicious URL click was detected
- A user clicked through to a potentially malicious URL

[Microsoft Defender for Cloud Apps anomaly detections](#)

- Impossible travel activity
- Activity from infrequent country

[Microsoft Defender XDR Business Email Compromise mitigation ↗](#)

- Business Email Compromise (BEC) related credential harvesting attack
- Suspicious phishing emails sent by BEC-related user

Token Theft – protect against replay

If an adversary is able to successfully steal a token, organizations can enable certain capabilities to automatically reduce the exposure of, or completely prevent, the stolen token from being replayed, thus defeating the attack. These capabilities include:

- Enforcing Token Protection in Conditional Access to secure sign-in sessions
- Enforcing access is only allowed via secure networks

Enforce Token Protection

Entra Primary Refresh Token

For devices which are Entra-joined or Entra-registered, Entra ID generates a multi-application Refresh Token used for application SSO, also known as the [Primary Refresh Token \(PRT\)](#).

Primary Refresh Tokens (PRTs) are secure by design. They're protected with a cryptographically secure tie between the PRT and the device (client secret) to which the PRT is issued. The client secret is securely stored on platform-specific hardware such as Trusted Platform Modules (TPM) for Windows, Keystore System for Android, and Secure Enclave for iOS and macOS. Without the client secret, the PRT token is rendered ineffective and cannot be replayed if stolen.

Token Protection in Conditional Access

Enforcing Token Protection in Conditional Access ensures that only refresh tokens which are cryptographically bound to the device are used. Bearer refresh tokens, which can be used from any device, are automatically rejected. This method provides the highest level of security for protecting sign-in sessions, as the token can only be used from the device it was originally issued to. At the time of publication of this post, Token Protection in Conditional Access is

available for Windows native applications connecting to Microsoft Teams, SharePoint, and Exchange. We're continuously working to expand the scope of Token Protection by adding support for extra platforms, applications, and resources. For an updated list of supported apps and resources, please refer to this article. [Token protection in Microsoft Entra Conditional Access - Microsoft Entra ID | Microsoft Learn](#).

Organizations are encouraged to pilot and deploy Token Protection for all supported applications, devices, and platforms. Applications that don't support Token Protection should be safeguarded with other policies such as network-based policies.

Check the following article to learn more and get deployment guidance: [Learn how to configure Token Protection](#).

! Note

Token Protection in Conditional Access requires the use of PRTs. Scenarios such as the use of unregistered devices aren't available as those devices don't have a PRT.

! Note

Entra Token Protection only applies to the user who signed into the device. For example, if you unlock a Windows device with a standard account but then access a resource authenticating under a different account, the latter identity can't be protected by Entra Token Protection as they don't have a valid PRT available.

Implement network-based enforcements

While Entra Token Protection is the most secure method of protecting sign-in session tokens, it's limited in its scope of application coverage and only applies to the user who signed into the device. To further reduce the attack surface, organizations can implement network-based enforcement policies which can cover a broader range of applications, often covering all Enterprise apps. Network-based policies can also cover additional identities beyond the user who is signed in to the device.

Network-based policies prevent sign-in session artifacts (such as refresh tokens) from being replayed outside of designated networks, effectively thwarting token theft and replay attacks that exfiltrate sign-in sessions beyond your organizational boundary. While internal threat vectors may still pose a risk due to their access to the same network, forcing threat actors to operate within your organizational boundary significantly increases the likelihood of detecting and mitigating threats through other security controls.

Additionally, in certain scenarios such as with applications that support Continuous Access Evaluation, these measures can also be an effective way to mitigate token theft and replay of application session tokens such as access tokens.

Protect Sign-in sessions with Global Secure Access

Organizations should deploy Global Secure Access to establish a secure network connection between client devices and resources, also known as a compliant network. Administrators can then create a Conditional Access policy that mandates the use of a compliant network to access any Enterprise App integrated with Entra ID. This measure prevents the replay of sign-in session artifacts from devices not managed by the organization.

Protect Sign-in Sessions with traditional network controls

As an alternative to Compliant network check, organizations can utilize traditional network solutions such as VPNs to protect sign-in sessions. Administrators can then create a location-based Conditional Access policy that restricts authentication attempts to specific egress IP addresses. However, organizations should consider the performance implications and costs associated with routing traffic through a corporate network. Therefore, Microsoft recommends using Global Secure Access, a fully secure, globally distributed Security Service Edge solution.

[Learn how to configure location-based Conditional Access policies with Entra ID.](#)

Protect App Sessions with network-based enforcements

By creating a location-based Conditional Access policies restricting access to specific egress IP addresses, organizations can also protect some of their app sessions. A subset of Microsoft Applications, such as SharePoint Online and Exchange Online, use the [Continuous Access Evaluation](#) (CAE) protocol. CAE-aware apps evaluate network-based enforcements and revoke app session artifacts replayed outside of the trusted network in near-real time. Organizations can further improve IP-based network enforcements by [configuring strict location policies with CAE](#) to ensure that traffic for CAE-capable apps are only accessible from trusted networks.

For applications that aren't CAE-capable, organizations can protect their app sessions with controls available on the application side. For instance, some applications support IP-based enforcement at the application layer in addition to those enforced by the Identity Provider (IdP). The application then rejects the use of any app session artifact used outside the trusted network. Tunneling app-specific traffic via company-owned networks can be achieved through Source IP Anchoring with Global Secure Access, as well as other traditional network solutions such as VPNs.

[Learn about Source IP Anchoring with Global Secure Access.](#)

Summary of token protection strategy

In summary, protecting tokens in Microsoft Entra involves a multi-layered defense-in-depth strategy to guard against token theft and replay attacks. This includes hardening devices against malware, leveraging device-based and risk-based Conditional Access, enforcing device-bound tokens, and implementing network-based enforcements. Additionally, organizations should deploy phishing-resistant multifactor authentication, monitor for suspicious sign-in attempts, and configure Conditional Access policies to require reauthentication for sensitive operations. By following these guidelines, organizations can significantly reduce the risk of unauthorized access and ensure the security of their sign-in sessions and app sessions.

Next steps

- [Microsoft Entra Conditional Access: Token protection](#)

macOS Platform Single Sign-on overview (preview)

Article • 05/01/2025

macOS Platform Single Sign-on (PSSO) is a new feature powered by Microsoft's Enterprise SSO plug-in, Platform Credentials for macOS that enables users to sign in to Mac devices using their Microsoft Entra ID credentials. This feature provides benefits for admins by simplifying the sign-in process for users and reducing the number of passwords they need to remember. It also allows users to authenticate with Microsoft Entra ID with a smart card or hardware-bound key. This feature improves the end-user experience by not having to remember two separate passwords and diminishes the need for admins to manage the local account password.

There are three different authentication methods that determine the end-user experience;

- **Platform Credential for macOS:** Provisions a secure enclave backed hardware-bound cryptographic key that is used for SSO across apps that use Microsoft Entra ID for authentication. The user's local account password is not affected and is required to log on to the Mac.
- **Smart card:** The user signs in to the machine using an external smart card, or smart card-compatible hard token (for example, Yubikey). Once the device is unlocked, the smart card is used with Microsoft Entra ID to grant SSO across apps that use Microsoft Entra ID for authentication.
- **Password as authentication method:** Syncs the user's Microsoft Entra ID password with the local account and enables SSO across apps that use Microsoft Entra ID for authentication.

Powered by the [Microsoft Enterprise SSO plug in Apple devices](#), PSSO;

- Allows users to go passwordless by using Touch ID.
- Uses phish resistant credentials, based on Windows Hello for Business technology.
- Saves customer organizations money by removing the need for security keys.
- Advances Zero Trust objectives using integration with the Secure Enclave.

To enable it, an administrator needs to configure PSSO through Microsoft Intune or other supported MDM. Depending on the how the device is configured, the end-user can set up their device with PSSO via secure enclave, smart card or password based authentication method.

Requirements

To deploy Platform SSO for macOS, you need to meet following minimum requirements.

- A recommended minimum version of macOS 14 Sonoma. While macOS 13 Ventura is supported, we strongly recommend using macOS 14 Sonoma for the best experience.
- [Microsoft Authenticator](#)
- Microsoft Intune [Company Portal app](#) version 5.2404.0 or later installed. This version is required before users are targeted for PSSO.

Configuration

You can find more information and instructions on how to configure in these articles:

- [Configure Platform SSO for macOS devices in Microsoft Intune](#)

Deployment

You can find more information and instructions on how to deploy Platform SSO for macOS in these articles.

- [Join a Mac device with Microsoft Entra ID during the out of box experience](#)
- [Join a Mac device with Microsoft Entra ID using Company Portal](#)

Passwordless authentication

Passwords are a primary attack vector for bad actors. They use social engineering, phishing, and spray attacks to compromise passwords. A passwordless authentication strategy mitigates the risk of these attacks.

Learn how you can use Platform SSO for macOS to enable passwordless authentication for your organization.

- [Passwordless authentication options for Microsoft Entra ID](#)
- [Plan a passwordless authentication deployment in Microsoft Entra ID](#)

Platform Credential for macOS can also be used as a phishing resistant credential for use in WebAuthn challenges (including browser re-auth scenarios). Admins will need to enable the FIDO2 security key authentication method for this capability. If you leverage Key Restriction Policies in your FIDO policy then you will need to add the AAGUID for the macOS Platform Credential to your list of allowed AAGUIDs: `7FD635B3-2EF9-4542-8D9D-164F2C771EFC`

National Institute of Standards and Technology (NIST)

The National Institute of Standards and Technology (NIST) is a non-regulatory federal agency within the U.S. Department of Commerce. NIST develops and issues standards, guidelines, and other publications to assist federal agencies in managing cost-effective programs to protect their information and information systems.

You can learn more about using macOS Platform SSO to meet NIST requirements in these articles.

- [Configure Microsoft Entra ID to meet NIST authenticator assurance levels](#)
- [NIST authenticator types and aligned Microsoft Entra methods.](#)
- [NIST authenticator assurance level 3 by using Microsoft Entra ID](#)

Troubleshooting

If you experience issues when implementing macOS Platform SSO, refer to our documentation on [macOS Platform single sign-on known issues and troubleshooting](#)

Plan your Microsoft Entra device deployment

Article • 11/25/2024

This article helps you evaluate the methods to integrate your device with Microsoft Entra ID, choose the implementation plan, and provides key links to supported device management tools.

The landscape of your user's devices is constantly expanding. Organizations might provide desktops, laptops, phones, tablets, and other devices. Your users might bring their own array of devices, and access information from varied locations. In this environment, your job as an administrator is to keep your organizational resources secure across all devices.

Microsoft Entra ID enables your organization to meet these goals with device identity management. You can now get your devices in Microsoft Entra ID and control them from a central location in the [Microsoft Entra admin center](#). This process gives you a unified experience, enhanced security, and reduces the time needed to configure a new device.

There are multiple methods to integrate your devices into Microsoft Entra ID. These methods can work separately or together based on the operating system and your requirements:

- You can [register devices](#) with Microsoft Entra ID.
- [Join devices](#) to Microsoft Entra ID (cloud-only).
- [Microsoft Entra hybrid join](#) devices to your on-premises Active Directory domain and Microsoft Entra ID.

Learn

Before you begin, make sure that you're familiar with the [device identity management overview](#).

Benefits

The key benefits of giving your devices a Microsoft Entra identity:

- Increase productivity – Users can do [seamless sign-on \(SSO\)](#) to your on-premises and cloud resources, enabling productivity wherever they are.

- Increase security – Apply [Conditional Access policies](#) to resources based on the identity of the device or user. Joining a device to Microsoft Entra ID is a prerequisite for increasing your security with a [Passwordless](#) strategy.
[https://www.youtube-nocookie.com/embed/NcONUf-jeS4 ↗](https://www.youtube-nocookie.com/embed/NcONUf-jeS4)
- Improve user experience – Provide your users with easy access to your organization's cloud-based resources from both personal and corporate devices. Administrators can enable [Enterprise State Roaming](#) for a unified experience across all Windows devices.
- Simplify deployment and management – Simplify the process of bringing devices to Microsoft Entra ID with [Windows Autopilot](#), [bulk provisioning](#), or [self-service: Out of Box Experience \(OOBE\)](#). Manage devices with Mobile Device Management (MDM) tools like [Microsoft Intune](#), and their identities in the [Microsoft Entra admin center](#).

Plan the deployment project

Consider your organizational needs while you determine the strategy for this deployment in your environment.

Engage the right stakeholders

When technology projects fail, they typically do because of mismatched expectations on impact, outcomes, and responsibilities. To avoid these pitfalls, [ensure that you're engaging the right stakeholders](#), and that stakeholder roles in the project are well understood.

For this plan, add the following stakeholders to your list:

[\[\] Expand table](#)

Role	Description
Device administrator	A representative from the device team that can verify that the plan meets the device requirements of your organization.
Network administrator	A representative from the network team that can make sure to meet network requirements.
Device management team	Team that manages inventory of devices.

Role	Description
OS-specific admin teams	Teams that support and manage specific OS versions. For example, there might be a Mac or iOS focused team.

Plan communications

Communication is critical to the success of any new service. Proactively communicate with your users how their experience changes, when it changes, and how to gain support if they experience issues.

Plan a pilot

We recommend that the initial configuration of your integration method is in a test environment, or with a small group of test devices. See [Best practices for a pilot](#).

You might want to do a [targeted deployment of Microsoft Entra hybrid join](#) before enabling it across the entire organization.

Warning

Organizations should include a sample of users from varying roles and profiles in their pilot group. A targeted rollout will help identify any issues your plan may not have addressed before you enable for the entire organization.

Choose your integration methods

Your organization can use multiple device integration methods in a single Microsoft Entra tenant. The goal is to choose one or more methods suitable to get your devices securely managed in Microsoft Entra ID. There are many parameters that drive this decision including ownership, device types, primary audience, and your organization's infrastructure.

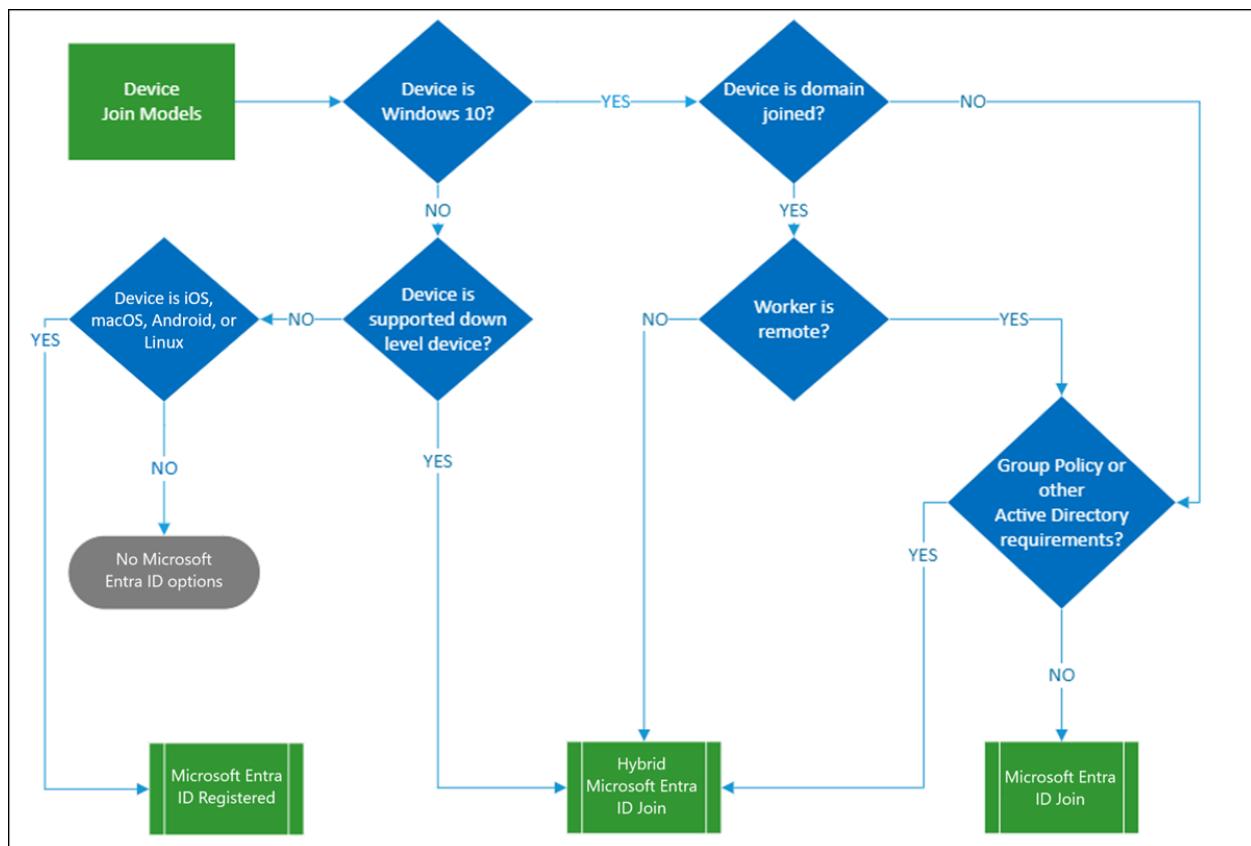
The following information can help you decide which integration methods to use.

Decision tree for devices integration

Use this tree to determine options for organization-owned devices.

Note

Personal or bring-your-own device (BYOD) scenarios are not pictured in this diagram. They always result in Microsoft Entra registration.



Comparison matrix

iOS and Android devices are only Microsoft Entra registered. The following table presents high-level considerations for Windows client devices. Use it as an overview, then explore the different integration methods in detail.

[Expand table](#)

Consideration	Microsoft Entra registered	Microsoft Entra joined	Microsoft Entra hybrid joined
Client operating systems			
Windows 11 or Windows 10 devices	✓	✓	✓
Linux Desktop - Ubuntu 20.04/22.04/24.04, RHEL 8/9	✓		
Sign in options			
End-user local credentials	✓		
Password	✓	✓	✓

Consideration	Microsoft Entra registered	Microsoft Entra joined	Microsoft Entra hybrid joined
Device PIN	✓		
Windows Hello	✓		
Windows Hello for Business		✓	✓
FIDO 2.0 security keys		✓	✓
Microsoft Authenticator App (passwordless)	✓	✓	✓
Key capabilities			
SSO to cloud resources	✓	✓	✓
SSO to on-premises resources		✓	✓
Conditional Access (Require devices be marked as compliant) (Must be managed by MDM)	✓	✓	✓
Conditional Access (Require Microsoft Entra hybrid joined devices)			✓
Self-service password reset from the Windows login screen		✓	✓
Windows Hello PIN reset		✓	✓

Microsoft Entra Registration

Registered devices are often managed with [Microsoft Intune](#). Devices are enrolled in Intune in several ways, depending on the operating system.

Microsoft Entra registered devices provide support for Bring Your Own Devices (BYOD) and corporate owned devices to SSO to cloud resources. Access to resources is based on the Microsoft Entra [Conditional Access policies](#) applied to the device and the user.

Registering devices

Registered devices are often managed with [Microsoft Intune](#). Devices are enrolled in Intune in several ways, depending on the operating system.

Users install the Company portal app to register BYOD and corporate owned mobile devices.

- iOS
- Android
- Windows 10 or newer
- macOS
- Linux Desktop

If registering your devices is the best option for your organization, see the following resources:

- This overview of [Microsoft Entra registered devices](#).
- This end-user documentation on [Register your personal device on your organization's network ↗](#).

Microsoft Entra join

Microsoft Entra join enables you to transition towards a cloud-first model with Windows. It provides a great foundation if you're planning to modernize your device management and reduce device-related IT costs. Microsoft Entra join works with Windows 10 or newer devices only. Consider it as the first choice for new devices.

[Microsoft Entra joined devices can SSO to on-premises resources](#) when they are on the organization's network, can authenticate to on-premises servers like file, print, and other applications.

If this option is best for your organization, see the following resources:

- This overview of [Microsoft Entra joined devices](#).
- Familiarize yourself with the [Microsoft Entra join implementation plan](#).

Provisioning Microsoft Entra joined devices

To provision devices to Microsoft Entra join, you have the following approaches:

- Self-Service: [Windows 10 first-run experience](#)

If you have either Windows 10 Professional or Windows 10 Enterprise installed on a device, the experience defaults to the setup process for company-owned devices.

- [Windows Out of Box Experience \(OOBE\) or from Windows Settings ↗](#)
- [Windows Autopilot](#)

- [Bulk Enrollment](#)

Choose your deployment procedure after careful [comparison of these approaches](#).

You might determine that Microsoft Entra join is the best solution for a device in a different state. The following table shows how to change the state of a device.

[\[+\] Expand table](#)

Current device state	Desired device state	How-to
On-premises domain joined	Microsoft Entra joined	Unjoin the device from on-premises domain before joining to Microsoft Entra ID.
Microsoft Entra hybrid joined	Microsoft Entra joined	Unjoin the device from on-premises domain and from Microsoft Entra ID before joining to Microsoft Entra ID.
Microsoft Entra registered	Microsoft Entra joined	Unregister the device before joining to Microsoft Entra ID.

Microsoft Entra hybrid join

If you have an on-premises Active Directory environment and want to join your existing domain-joined computers to Microsoft Entra ID, you can accomplish this task with Microsoft Entra hybrid join. It supports a [broad range of Windows devices](#).

Most organizations already have domain joined devices and manage them via Group Policy or System Center Configuration Manager (SCCM). In that case, we recommend configuring Microsoft Entra hybrid join to start getting benefits while using existing investments.

If Microsoft Entra hybrid join is the best option for your organization, see the following resources:

- This overview of [Microsoft Entra hybrid joined devices](#).
- Familiarize yourself with the [Microsoft Entra hybrid join implementation](#) plan.

Provisioning Microsoft Entra hybrid join to your devices

[Review your identity infrastructure](#). Microsoft Entra Connect provides you with a wizard to configure Microsoft Entra hybrid join for:

- [Managed domains](#)
- [Federated domains](#)

If installing the required version of Microsoft Entra Connect isn't an option for you, see [how to manually configure Microsoft Entra hybrid join](#).

① Note

The on-premises domain-joined Windows 10 or newer device attempts to auto-join to Microsoft Entra ID to become Microsoft Entra hybrid joined by default. This will only succeed if you have set up the right environment.

You might determine that Microsoft Entra hybrid join is the best solution for a device in a different state. The following table shows how to change the state of a device.

[] [Expand table](#)

Current device state	Desired device state	How-to
On-premises domain joined	Microsoft Entra hybrid joined	Use Microsoft Entra Connect or AD FS to join to Azure.
On-premises workgroup joined or new	Microsoft Entra hybrid joined	Supported with Windows Autopilot . Otherwise device needs to be on-premises domain joined before Microsoft Entra hybrid join.
Microsoft Entra joined	Microsoft Entra hybrid joined	Unjoin from Microsoft Entra ID, which puts it in the on-premises workgroup or new state.
Microsoft Entra registered	Microsoft Entra hybrid joined	Depends on Windows version. See these considerations .

Manage your devices

Once you've registered or joined your devices to Microsoft Entra ID, use the [Microsoft Entra admin center](#) as a central place to manage your device identities. The Microsoft Entra devices page enables you to:

- [Configure your device settings](#).
- You need to be a local administrator to manage Windows devices. [Microsoft Entra ID updates this membership for Microsoft Entra joined devices](#), automatically adding users with the device manager role as administrators to all joined devices.

Make sure that you keep the environment clean by [managing stale devices](#), and focus your resources on managing current devices.

- Review device-related audit logs

Supported device management tools

Administrators can secure and further control registered and joined devices using other device management tools. These tools provide you with a way to enforce configurations like requiring storage to be encrypted, password complexity, software installations, and software updates.

Review supported and unsupported platforms for integrated devices:

[\[+\] Expand table](#)

Device management tools	Microsoft Entra registered	Microsoft Entra joined	Microsoft Entra hybrid joined
Mobile Device Management (MDM) Example: Microsoft Intune	✓	✓	✓
Co-management with Microsoft Intune and Microsoft Configuration Manager (Windows 10 or newer)		✓	✓
Group policy (Windows only)			✓

We recommend that you consider [Microsoft Intune Mobile Application management \(MAM\)](#) with or without device management for registered iOS or Android devices.

Administrators can also [deploy virtual desktop infrastructure \(VDI\) platforms](#) hosting Windows operating systems in their organizations to streamline management and reduce costs through consolidation and centralization of resources.

Next steps

- Analyze your on-premises GPOs using Group Policy analytics in Microsoft Intune
- Plan your Microsoft Entra join implementation
- Plan your Microsoft Entra hybrid join implementation
- Manage device identities

Feedback

Was this page helpful?

 Yes

 No

Provide product feedback ↗

How to: Plan your Microsoft Entra join implementation

Article • 05/29/2024

You can join devices directly to Microsoft Entra ID without the need to join to on-premises Active Directory while keeping your users productive and secure. Microsoft Entra join is enterprise-ready for both at-scale and scoped deployments. Single sign-on (SSO) access to on-premises resources is also available to devices that are Microsoft Entra joined. For more information, see [How SSO to on-premises resources works on Microsoft Entra joined devices](#).

This article provides you with the information you need to plan your Microsoft Entra join implementation.

Prerequisites

This article assumes that you're familiar with the [Introduction to device management in Microsoft Entra ID](#).

Plan your implementation

To plan your Microsoft Entra join implementation, you should familiarize yourself with:

- ✓ Review your scenarios
- ✓ Review your identity infrastructure
- ✓ Assess your device management
- ✓ Understand considerations for applications and resources
- ✓ Understand your provisioning options
- ✓ Configure enterprise state roaming
- ✓ Configure Conditional Access

Review your scenarios

Microsoft Entra join enables you to transition toward a cloud-first model with Windows. If you're planning to modernize your devices management and reduce device-related IT costs, Microsoft Entra join provides a great foundation toward achieving those goals.

Consider Microsoft Entra join if your goals align with the following criteria:

- You're adopting Microsoft 365 as the productivity suite for your users.
- You want to manage devices with a cloud device management solution.
- You want to simplify device provisioning for geographically distributed users.
- You plan to modernize your application infrastructure.

Review your identity infrastructure

Microsoft Entra join works in managed and federated environments. Most organizations deploy managed domains. Managed domain scenarios don't require configuring and managing a federation server like Active Directory Federation Services (AD FS).

Managed environment

A managed environment can be deployed either through [Password Hash Sync](#) or [Pass Through Authentication](#) with Seamless single sign-on.

Federated environment

A federated environment should have an identity provider that supports both WS-Trust and WS-Fed protocols:

- **WS-Fed:** This protocol is required to join a device to Microsoft Entra ID.
- **WS-Trust:** This protocol is required to sign in to a Microsoft Entra joined device.

When you're using AD FS, you need to enable the following WS-Trust endpoints:

```
/adfs/services/trust/2005 usernamemixed /adfs/services/trust/13 usernamemixed  
/adfs/services/trust/2005 certificatemixed  
/adfs/services/trust/13 certificatemixed
```

If your identity provider doesn't support these protocols, Microsoft Entra join doesn't work natively.

Note

Currently, Microsoft Entra join does not work with [AD FS 2019 configured with external authentication providers as the primary authentication method](#).

Microsoft Entra join defaults to password authentication as the primary method, which results in authentication failures in this scenario

User configuration

If you create users in your:

- **On-premises Active Directory**, you need to synchronize them to Microsoft Entra ID using [Microsoft Entra Connect](#).
- **Microsoft Entra ID**, no extra setup is required.

On-premises user principal names (UPNs) that are different from Microsoft Entra UPNs aren't supported on Microsoft Entra joined devices. If your users use an on-premises UPN, you should plan to switch to using their primary UPN in Microsoft Entra ID.

UPN changes are only supported starting Windows 10 2004 update. Users on devices with this update won't have any issues after changing their UPNs. For devices before the Windows 10 2004 update, users would have SSO and Conditional Access issues on their devices. They need to sign in to Windows through the "Other user" tile using their new UPN to resolve this issue.

Assess your device management

Supported devices

Microsoft Entra join:

- Supports Windows 10 and Windows 11 devices.
- Isn't supported on previous versions of Windows or other operating systems. If you have Windows 7/8.1 devices, you must upgrade at least to Windows 10 to deploy Microsoft Entra join.
- Is supported for Federal Information Processing Standard (FIPS)-compliant Trusted Platform Module (TPM) 2.0 but not supported for TPM 1.2. If your devices have FIPS-compliant TPM 1.2, you must disable them before proceeding with Microsoft Entra join. Microsoft doesn't provide any tools for disabling FIPS mode for TPMs as it is dependent on the TPM manufacturer. Contact your hardware OEM for support.

Recommendation: Always use the latest Windows release to take advantage of updated features.

Management platform

Device management for Microsoft Entra joined devices is based on a mobile device management (MDM) platform such as Intune, and MDM CSPs. Starting in Windows 10 there's a built-in MDM agent that works with all compatible MDM solutions.

Note

Group policies are not supported in Microsoft Entra joined devices as they are not connected to on-premises Active Directory. Management of Microsoft Entra joined devices is only possible through MDM.

There are two approaches for managing Microsoft Entra joined devices:

- **MDM-only** - A device is exclusively managed by an MDM provider like Intune. All policies are delivered as part of the MDM enrollment process. For Microsoft Entra ID P1 or P2 or EMS customers, MDM enrollment is an automated step that is part of a Microsoft Entra join.
- **Co-management** - A device is managed by an MDM provider and Microsoft Configuration Manager. In this approach, the Microsoft Configuration Manager agent is installed on an MDM-managed device to administer certain aspects.

If you're using Group Policies, evaluate your Group Policy Object (GPO) and MDM policy parity by using [Group Policy analytics](#) in Microsoft Intune.

Review supported and unsupported policies to determine whether you can use an MDM solution instead of Group policies. For unsupported policies, consider the following questions:

- Are the unsupported policies necessary for Microsoft Entra joined devices or users?
- Are the unsupported policies applicable in a cloud-driven deployment?

If your MDM solution isn't available through the Microsoft Entra app gallery, you can add it following the process outlined in [Microsoft Entra integration with MDM](#).

Through co-management, you can use Microsoft Configuration Manager to manage certain aspects of your devices while policies are delivered through your MDM platform. Microsoft Intune enables co-management with Microsoft Configuration Manager. For more information on co-management for Windows 10 or newer devices, see [What is co-management?](#). If you use an MDM product other than Intune, check with your MDM provider on applicable co-management scenarios.

Recommendation: Consider MDM only management for Microsoft Entra joined devices.

Understand considerations for applications and resources

We recommend migrating applications from on-premises to cloud for a better user experience and access control. Microsoft Entra joined devices can seamlessly provide access to both, on-premises and cloud applications. For more information, see [How SSO to on-premises resources works on Microsoft Entra joined devices](#).

The following sections list considerations for different types of applications and resources.

Cloud-based applications

If an application is added to Microsoft Entra app gallery, users get SSO through Microsoft Entra joined devices. No other configuration is required. Users get SSO on both, Microsoft Edge and Chrome browsers. For Chrome, you need to deploy the [Windows 10 Accounts extension](#).

All Win32 applications that:

- Rely on Web Account Manager (WAM) for token requests also get SSO on Microsoft Entra joined devices.
- Don't rely on WAM might prompt users for authentication.

On-premises web applications

If your apps are custom built or hosted on-premises, you need to add them to your browser's trusted sites to:

- Enable Windows integrated authentication to work
- Provide a no-prompt SSO experience to users.

If you use AD FS, see [Verify and manage single sign-on with AD FS](#).

Recommendation: Consider hosting in the cloud (for example, Azure) and integrating with Microsoft Entra ID for a better experience.

On-premises applications relying on legacy protocols

Users get SSO from Microsoft Entra joined devices if the device has access to a domain controller.

Note

Microsoft Entra joined devices can seamlessly provide access to both, on-premises and cloud applications. For more information, see [How SSO to on-premises](#)

[resources works on Microsoft Entra joined devices.](#)

Recommendation: Deploy [Microsoft Entra application proxy](#) to enable secure access for these applications.

On-premises network shares

Your users have SSO from Microsoft Entra joined devices when a device has access to an on-premises domain controller. [Learn how this works](#)

Printers

We recommend deploying [Universal Print](#) to have a cloud-based print management solution without any on-premises dependencies.

On-premises applications relying on machine authentication

Microsoft Entra joined devices don't support on-premises applications relying on machine authentication.

Recommendation: Consider retiring these applications and moving to their modern alternatives.

Remote Desktop Services

Remote desktop connection to a Microsoft Entra joined devices requires the host machine to be either Microsoft Entra joined or Microsoft Entra hybrid joined. Remote desktop from an unjoined or non-Windows device isn't supported. For more information, see [Connect to remote Microsoft Entra joined PC](#)

After the Windows 10 2004 update, users can use remote desktop from a Microsoft Entra registered Windows 10 or newer device to another Microsoft Entra joined device.

RADIUS and Wi-Fi authentication

Currently, Microsoft Entra joined devices don't support RADIUS authentication using an on-premises computer object and certificate for connecting to Wi-Fi access points, since RADIUS relies on presence of an on-premises computer object in this scenario. As an

alternative, you can use certificates pushed via Intune or user credentials to authenticate to Wi-Fi.

Understand your provisioning options

Note

Microsoft Entra joined devices can't be deployed using System Preparation Tool (Sysprep) or similar imaging tools.

You can provision Microsoft Entra joined devices using the following approaches:

- **Self-service in OOBE/Settings** - In the self-service mode, users go through the Microsoft Entra join process either during Windows Out of Box Experience (OOBE) or from Windows Settings. For more information, see [Join your work device to your organization's network](#).
- **Windows Autopilot** - Windows Autopilot enables preconfiguration of devices for a smoother Microsoft Entra join experience in OOBE. For more information, see the [Overview of Windows Autopilot](#).
- **Bulk enrollment** - Bulk enrollment enables an administrator driven Microsoft Entra join by using a bulk provisioning tool to configure devices. For more information, see [Bulk enrollment for Windows devices](#).

Here's a comparison of these three approaches

 Expand table

Element	Self-service setup	Windows Autopilot	Bulk enrollment
Require user interaction to set up	Yes	Yes	No
Require IT effort	No	Yes	Yes
Applicable flows	OOBE & Settings	OOBE only	OOBE only
Local admin rights to primary user	Yes, by default	Configurable	No
Require device OEM support	No	Yes	No
Supported versions	1511+	1709+	1703+

Choose your deployment approach or approaches by reviewing the previous table and reviewing the following considerations for adopting either approach:

- Are your users tech savvy to go through the setup themselves?
 - Self-service can work best for these users. Consider Windows Autopilot to enhance the user experience.
- Are your users remote or within corporate premises?
 - Self-service or Autopilot work best for remote users for a hassle-free setup.
- Do you prefer a user driven or an admin-managed configuration?
 - Bulk enrollment works better for admin-driven deployment to set up devices before handing over to users.
- Do you purchase devices from 1-2 OEMS, or do you have a wide distribution of OEM devices?
 - If purchasing from limited OEMs who also support Autopilot, you can benefit from tighter integration with Autopilot.

Configure your device settings

The [Microsoft Entra admin center](#) allows you to control the deployment of Microsoft Entra joined devices in your organization. To configure the related settings, browse to **Identity > Devices > All devices > Device settings**. [Learn more](#)

Users might join devices to Microsoft Entra ID

Set this option to **All** or **Selected** based on the scope of your deployment and who you want to set up a Microsoft Entra joined device.

Users may join devices to Microsoft Entra (i)

All

Selected

None

Additional local administrators on Microsoft Entra joined devices

Choose **Selected** and selects the users you want to add to the local administrators' group on all Microsoft Entra joined devices.

Local administrator settings

[Manage Additional local administrators on all Microsoft Entra joined devices](#)

Enable Microsoft Entra Local Administrator Password Solution (LAPS) ⓘ

Yes

No

Require multifactor authentication (MFA) to join devices

Select "Yes" if you require users to do MFA while joining devices to Microsoft Entra ID.

Require Multi-Factor Auth to join devices ⓘ Yes No

Recommendation: Use the user action [Register or join devices](#) in Conditional Access for enforcing MFA for joining devices.

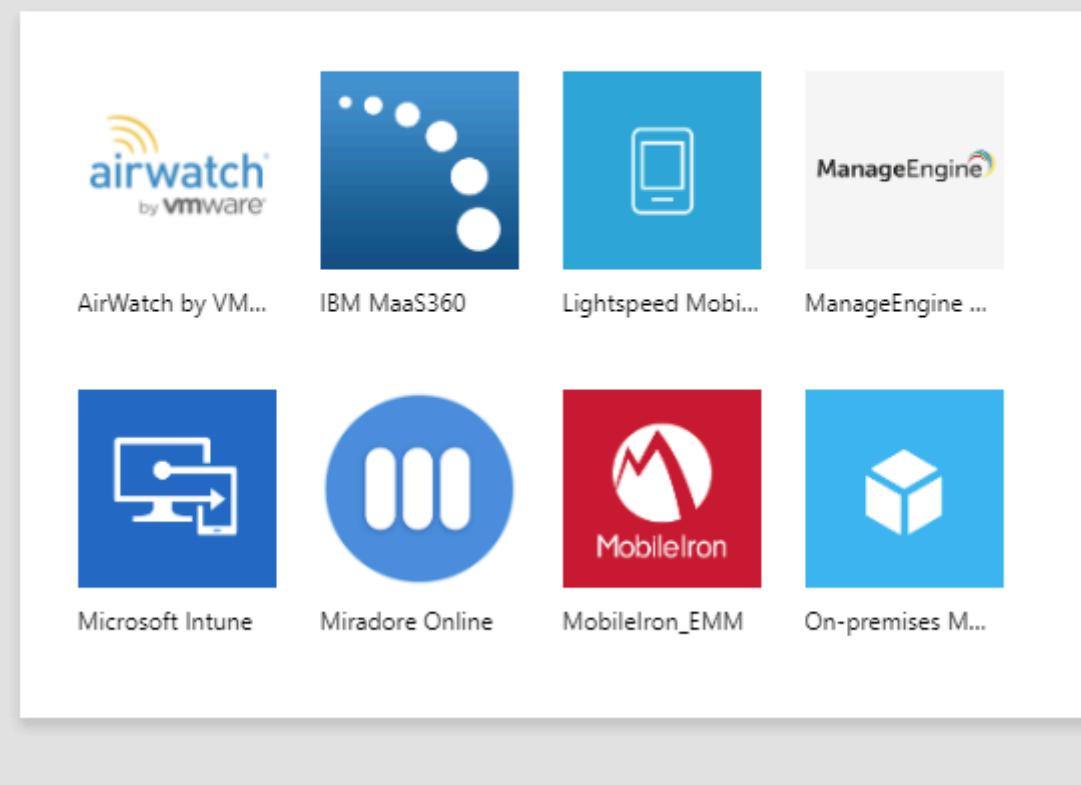
Configure your mobility settings

Before you can configure your mobility settings, you might have to add an MDM provider, first.

To add an MDM provider:

1. On the Microsoft Entra ID page, in the **Manage** section, select **Mobility (MDM and MAM)**.
2. Select **Add application**.
3. Select your MDM provider from the list.

Add an application



Select your MDM provider to configure the related settings.

MDM user scope

Select **Some** or **All** based on the scope of your deployment.

MDM user scope	<input type="button" value="None"/> <input type="button" value="Some"/> <input type="button" value="All"/>
----------------	--

Based on your scope, one of the following happens:

- **User is in MDM scope:** If you have a Microsoft Entra ID P1 or P2 subscription, MDM enrollment is automated along with Microsoft Entra join. All scoped users must have an appropriate license for your MDM. If MDM enrollment fails in this scenario, Microsoft Entra join is rolled back.
- **User is not in MDM scope:** If users aren't in MDM scope, Microsoft Entra join completes without any MDM enrollment. This scope results in an unmanaged device.

MDM URLs

There are three URLs that are related to your MDM configuration:

- MDM terms of use URL
- MDM discovery URL
- MDM compliance URL

MDM terms of use URL ⓘ	https://portal.manage.microsoft.com/TermsofUse.aspx
MDM discovery URL ⓘ	https://enrollment.manage.microsoft.com/enrollmentserver/discover...
MDM compliance URL ⓘ	https://portal.manage.microsoft.com/?portalAction=Compliance

Each URL has a predefined default value. If these fields are empty, contact your MDM provider for more information.

MAM settings

Mobile Application Management (MAM) doesn't apply to Microsoft Entra join.

Configure enterprise state roaming

If you want to enable state roaming to Microsoft Entra ID so that users can sync their settings across devices, see [Enable Enterprise State Roaming in Microsoft Entra ID](#).

Recommendation: Enable this setting even for Microsoft Entra hybrid joined devices.

Configure Conditional Access

If you have an MDM provider configured for your Microsoft Entra joined devices, the provider flags the device as compliant as soon as the device is under management.

NAME	ENABLED	OS	VERSION	JOIN TYPE	OWNER	MDM	COMPLIANT
Device1	<input checked="" type="checkbox"/> Yes					Microsoft Intune	<input checked="" type="checkbox"/> Yes

You can use this implementation to require managed devices for cloud app access with [Conditional Access](#).

Next steps

- [Join a new Windows 10 device to Microsoft Entra ID during a first run](#)
- [Join your work device to your organization's network ↗](#)

- Planning a Windows Hello for Business Deployment

How to manage the local administrators group on Microsoft Entra joined devices

Article • 06/27/2024

To manage a Windows device, you need to be a member of the local administrators group. As part of the Microsoft Entra join process, Microsoft Entra ID updates the membership of this group on a device. You can customize the membership update to satisfy your business requirements. A membership update is, for example, helpful if you want to enable your helpdesk staff to do tasks requiring administrator rights on a device.

This article explains how the local administrators membership update works and how you can customize it during a Microsoft Entra join. The content of this article doesn't apply to **Microsoft Entra hybrid joined** devices.

How it works

At the time of Microsoft Entra join, the following security principals are added to the local administrators group on the device:

- The [Microsoft Entra Joined Device Local Administrator](#) and the [Global Administrator](#) roles
- The user performing the Microsoft Entra join

ⓘ Note

This is done during the join operation only. If an administrator makes changes after this point they will need to update the group membership on the device.

By adding Microsoft Entra roles to the local administrators group, you can update the users that can manage a device anytime in Microsoft Entra ID without modifying anything on the device. Microsoft Entra ID also adds the Microsoft Entra Joined Device Local Administrator role to the local administrators group to support the principle of least privilege (PoLP). In addition to users with the Global Administrator role, you can also enable users assigned only the Microsoft Entra Joined Device Local Administrator role to manage a device.

Manage administrator roles

To view and update the membership of an [administrator role](#) role, see:

- [View all members of an administrator role in Microsoft Entra ID](#)
- [Assign a user to administrator roles in Microsoft Entra ID](#)

Manage the Microsoft Entra Joined Device Local Administrator role

You can manage the [Microsoft Entra Joined Device Local Administrator](#) role from [Device settings](#).

1. Sign in to the [Microsoft Entra admin center](#) as at least a [Privileged Role Administrator](#).
2. Browse to **Identity > Devices > All devices > Device settings**.
3. Select **Manage Additional local administrators on all Microsoft Entra joined devices**.
4. Select **Add assignments** then choose the other administrators you want to add and select **Add**.

To modify the Microsoft Entra Joined Device Local Administrator role, configure [Additional local administrators on all Microsoft Entra joined devices](#).

 **Note**

This option requires Microsoft Entra ID P1 or P2 licenses.

Microsoft Entra Joined Device Local Administrators are assigned to all Microsoft Entra joined devices. You can't scope this role to a specific set of devices. Updating the Microsoft Entra Joined Device Local Administrator role doesn't necessarily have an immediate impact on the affected users. On devices where a user is already signed in to, the privilege elevation takes place when *both* the below actions happen:

- Up to 4 hours passed for Microsoft Entra ID to issue a new Primary Refresh Token with the appropriate privileges.
- User signs out and signs back in, not lock/unlock, to refresh their profile.

Users aren't directly listed in the local administrator group, their permissions are received through the Primary Refresh Token.

 **Note**

The above actions are not applicable to users who have not signed in to the relevant device previously. In this case, the administrator privileges are applied immediately after their first sign in to the device.

Manage administrator privileges using Microsoft Entra groups (preview)

You can use Microsoft Entra groups to manage administrator privileges on Microsoft Entra joined devices with the [Local Users and Groups](#) mobile device management (MDM) policy. This policy allows you to assign individual users or Microsoft Entra groups to the local administrators group on a Microsoft Entra joined device, providing you with the granularity to configure distinct administrators for different groups of devices.

Organizations can use Intune to manage these policies using [Custom OMA-URI Settings](#) or [Account protection policy](#). A few considerations for using this policy:

- Adding Microsoft Entra groups through the policy requires the group's security identifier (SID) that can be obtained by executing the [Microsoft Graph API for Groups](#). The SID equates to the property `securityIdentifier` in the API response.
- Administrator privileges using this policy are evaluated only for the following well-known groups on a Windows 10 or newer device - Administrators, Users, Guests, Power Users, Remote Desktop Users, and Remote Management Users.
- Managing local administrators using Microsoft Entra groups isn't applicable to Microsoft Entra hybrid joined or Microsoft Entra registered devices.
- Microsoft Entra groups deployed to a device with this policy don't apply to remote desktop connections. To control remote desktop permissions for Microsoft Entra joined devices, you need to add the individual user's SID to the appropriate group.

Important

Windows sign-in with Microsoft Entra ID supports evaluation of up to 20 groups for administrator rights. We recommend having no more than 20 Microsoft Entra groups on each device to ensure that administrator rights are correctly assigned. This limitation also applies to nested groups.

Manage regular users

By default, Microsoft Entra ID adds the user performing the Microsoft Entra join to the administrator group on the device. If you want to prevent regular users from becoming local administrators, you have the following options:

- [Windows Autopilot](#) - Windows Autopilot provides you with an option to prevent primary user performing the join from becoming a local administrator by [creating an Autopilot profile](#).
- [Bulk enrollment](#) - a Microsoft Entra join that is performed in the context of a bulk enrollment happens in the context of an auto-created user. Users signing in after a device is joined aren't added to the administrators group.

Manually elevate a user on a device

In addition to using the Microsoft Entra join process, you can also manually elevate a regular user to become a local administrator on one specific device. This step requires you to already be a member of the local administrators group.

Starting with the **Windows 10 1709** release, you can perform this task from **Settings -> Accounts -> Other users**. Select **Add a work or school user**, enter the user's user principal name (UPN) under **User account** and select **Administrator** under **Account type**

Additionally, you can also add users using the command prompt:

- If your tenant users are synchronized from on-premises Active Directory, use `net localgroup administrators /add "Contoso\username"`.
- If your tenant users are created in Microsoft Entra ID, use `net localgroup administrators /add "AzureAD\UserUpn"`

Considerations

- You can only assign role-based groups to the Microsoft Entra Joined Device Local Administrator role.
- The Microsoft Entra Joined Device Local Administrator role is assigned to all Microsoft Entra joined devices. This role can't be scoped to a specific set of devices.
- Local administrator rights on Windows devices aren't applicable to [Microsoft Entra B2B guest users](#).
- When you remove users from the Microsoft Entra Joined Device Local Administrator role, changes aren't instant. Users still have local administrator privilege on a device as long as they're signed in to it. The privilege is revoked

during their next sign-in when a new primary refresh token is issued. This revocation, similar to the privilege elevation, could take up to 4 hours.

Next steps

- To get an overview of how to manage devices, see [Managing device identities](#).
 - To learn more about device-based Conditional Access, see [Conditional Access: Require compliant or Microsoft Entra hybrid joined device](#).
-

Feedback

Was this page helpful?



[Provide product feedback](#) ↗

Plan your Microsoft Entra hybrid join implementation

Article • 03/03/2025

If you have an on-premises Active Directory Domain Services (AD DS) environment and you want to join your AD DS domain-joined computers to Microsoft Entra ID, you can accomplish this task by doing Microsoft Entra hybrid join.

💡 Tip

Single sign-on (SSO) access to on-premises resources is also available to devices that are Microsoft Entra joined. For more information, see [How SSO to on-premises resources works on Microsoft Entra joined devices](#).

Prerequisites

This article assumes that you're familiar with the [Introduction to device identity management in Microsoft Entra ID](#).

⚠ Note

The minimum required domain controller (DC) version for Windows 10 or newer Microsoft Entra hybrid join is Windows Server 2008 R2.

Microsoft Entra hybrid joined devices require periodic network line of sight to your domain controllers. Without this connection, devices become unusable.

Scenarios that break without line of sight to your domain controllers include:

- Device password change
- User password change (Cached credentials)
- Trusted Platform Module (TPM) reset

Plan your implementation

To plan your hybrid Microsoft Entra implementation, familiarize yourself with:

- ✓ Review supported devices

- ✓ Review things you should know
- ✓ Review targeted deployment of Microsoft Entra hybrid join
- ✓ Select your scenario based on your identity infrastructure
- ✓ Review on-premises Microsoft Windows Server Active Directory user principal name (UPN) support for Microsoft Entra hybrid join

Review supported devices

Microsoft Entra hybrid join supports a broad range of Windows devices.

- Windows 11
- Windows 10
- Windows Server 2016
 - **Note:** Azure National cloud customers require version 1803
- Windows Server 2019

As a best practice, Microsoft recommends you upgrade to the latest version of Windows.

Review things you should know

Unsupported scenarios

- Microsoft Entra hybrid join isn't supported for Windows Server running the Domain Controller (DC) role.
- Server Core OS doesn't support any type of device registration.
- User State Migration Tool (USMT) doesn't work with device registration.

OS imaging considerations

- If you're relying on the System Preparation Tool (Sysprep) and using a **pre-Windows 10 1809** image for installation, make sure that image isn't from a device already registered with Microsoft Entra ID as Microsoft Entra hybrid joined.
- If you're relying on a Virtual Machine (VM) snapshot to create more VMs, make sure that snapshot isn't from a VM that is already registered with Microsoft Entra ID as Microsoft Entra hybrid joined.
- If you're using [Unified Write Filter](#) and similar technologies that clear changes to the disk at reboot, they must be applied after the device is Microsoft Entra hybrid

joined. Enabling such technologies before completion of Microsoft Entra hybrid join results in the device getting unjoined on every reboot.

Handling devices with Microsoft Entra registered state

If your Windows 10 or newer domain joined devices are [Microsoft Entra registered](#) to your tenant, it might lead to a dual state of Microsoft Entra hybrid joined and Microsoft Entra registered device. We recommend upgrading to Windows 10 1803 (with KB4489894 applied) or newer to automatically address this scenario. In pre-1803 releases, you need to remove the Microsoft Entra registered state manually before enabling Microsoft Entra hybrid join. In 1803 and above releases, the following changes were made to avoid this dual state:

- Any existing Microsoft Entra registered state for a user would be automatically removed *after the device is Microsoft Entra hybrid joined and the same user logs in*. For example, if User A had a Microsoft Entra registered state on the device, the dual state for User A is cleaned up only when User A logs in to the device. If there are multiple users on the same device, the dual state is cleaned up individually when those users sign in. After an admin removes the Microsoft Entra registered state, Windows 10 will unenroll the device from Intune or other mobile device management (MDM), if the enrollment happened as part of the Microsoft Entra registration via autoenrollment.
- Microsoft Entra registered state on any local accounts on the device isn't affected by this change. Only applicable to domain accounts. Microsoft Entra registered state on local accounts isn't removed automatically even after user logon, since the user isn't a domain user.
- You can prevent your domain joined device from being Microsoft Entra registered by adding the following registry value to
HKLM\SOFTWARE\Policies\Microsoft\Windows\WorkplaceJoin:
"BlockAADWorkplaceJoin"=dword:00000001.
- In Windows 10 1803, if you have Windows Hello for Business configured, the user needs to reconfigure Windows Hello for Business after the dual state cleanup. This issue is addressed with KB4512509.

Note

Even though Windows 10 and Windows 11 automatically remove the Microsoft Entra registered state locally, the device object in Microsoft Entra ID isn't immediately deleted if it's managed by Intune. You can validate the removal of Microsoft Entra registered state by running `dsregcmd /status`.

Microsoft Entra hybrid join for single forest, multiple Microsoft Entra tenants

To register devices as Microsoft Entra hybrid join to respective tenants, organizations need to ensure that the Service Connection Point (SCP) configuration is done on the devices and not in Microsoft Windows Server Active Directory. More details on how to accomplish this task can be found in the article [Microsoft Entra hybrid join targeted deployment](#). It's important for organizations to understand that certain Microsoft Entra capabilities don't work in a single forest, multiple Microsoft Entra tenants configurations.

- [Device writeback](#) doesn't work. This configuration affects [Device based Conditional Access for on-premises apps that are federated using AD FS](#). This configuration also affects [Windows Hello for Business deployment when using the Hybrid Cert Trust model](#).
- [Groups writeback](#) doesn't work. This configuration affects writeback of Office 365 Groups to a forest with Exchange installed.
- [Seamless SSO](#) doesn't work. This configuration affects SSO scenarios in organizations using browser platforms like iOS or Linux with Firefox, Safari, or Chrome without the Windows 10 extension.
- [On-premises Microsoft Entra Password Protection](#) doesn't work. This configuration affects the ability to do password changes and password reset events against on-premises Active Directory Domain Services (AD DS) domain controllers using the same global and custom banned password lists that are stored in Microsoft Entra ID.

Other considerations

- If your environment uses virtual desktop infrastructure (VDI), see [Device identity and desktop virtualization](#).
- Microsoft Entra hybrid join is supported for Federal Information Processing Standard (FIPS)-compliant TPM 2.0 and not supported for TPM 1.2. If your devices have FIPS-compliant TPM 1.2, you must disable them before proceeding with Microsoft Entra hybrid join. Microsoft doesn't provide any tools for disabling FIPS mode for TPMs as it is dependent on the TPM manufacturer. Contact your hardware OEM for support.
- Starting from Windows 10 1903 release, TPM version 1.2 isn't used with Microsoft Entra hybrid join and devices with those TPMs are treated as if they don't have a TPM.

- UPN changes are only supported starting Windows 10 2004 update. For devices before the Windows 10 2004 update, users could have SSO and Conditional Access issues on their devices. To resolve this issue, you need to unjoin the device from Microsoft Entra ID (run "dsregcmd /leave" with elevated privileges) and rejoin (happens automatically). However, users signing in with Windows Hello for Business don't face this issue.

Review targeted Microsoft Entra hybrid join

Organizations might want to do a targeted rollout of Microsoft Entra hybrid join before enabling it for the entire organization. Review the article [Microsoft Entra hybrid join targeted deployment](#) to understand how to accomplish it.

Warning

Organizations should include a sample of users from varying roles and profiles in their pilot group. A targeted rollout helps identify any issues your plan might not address before you enable for the entire organization.

Select your scenario based on your identity infrastructure

Microsoft Entra hybrid join works with both, managed and federated environments depending on whether the UPN is routable or nonroutable. See bottom of the page for table on supported scenarios.

Managed environment

A managed environment can be deployed either through [Password Hash Sync \(PHS\)](#) or [Pass Through Authentication \(PTA\)](#) with [Seamless single sign-on](#).

These scenarios don't require you to configure a federation server for authentication (AuthN).

Note

[Cloud authentication using Staged rollout](#) is only supported starting at the Windows 10 1903 update.

Federated environment

A federated environment should have an identity provider that supports the following requirements. If you have a federated environment using Active Directory Federation Services (AD FS), then the below requirements are already supported.

WS-Trust protocol: This protocol is required to authenticate Microsoft Entra hybrid joined Windows devices with Microsoft Entra ID. When you're using AD FS, you need to enable the following WS-Trust endpoints:

```
/adfs/services/trust/2005/windowstransport  
/adfs/services/trust/13/windowstransport /adfs/services/trust/2005/usernamemixed  
/adfs/services/trust/13/usernamemixed /adfs/services/trust/2005/certificatemixed  
/adfs/services/trust/13/certificatemixed
```

Warning

Both `adfs/services/trust/2005/windowstransport` or `adfs/services/trust/13/windowstransport` should be enabled as intranet facing endpoints only and must NOT be exposed as extranet facing endpoints through the Web Application Proxy. To learn more on how to disable WS-Trust Windows endpoints, see [Disable WS-Trust Windows endpoints on the proxy](#). You can see what endpoints are enabled through the AD FS management console under **Service > Endpoints**.

Beginning with version 1.1.819.0, Microsoft Entra Connect provides you with a wizard to configure Microsoft Entra hybrid join. The wizard enables you to significantly simplify the configuration process. If installing the required version of Microsoft Entra Connect isn't an option for you, see [How to manually configure device registration](#). If contoso.com is registered as a confirmed custom domain, users can get a PRT even if their synchronized on-premises AD DS UPN suffix is in a subdomain like test.contoso.com.

Review on-premises Microsoft Windows Server Active Directory users UPN support for Microsoft Entra hybrid join

- Routable users UPN: A routable UPN has a valid verified domain that is registered with a domain registrar. For example, if contoso.com is the primary domain in

Microsoft Entra ID, contoso.org is the primary domain in on-premises AD owned by Contoso and [verified in Microsoft Entra ID](#).

- Nonroutable users UPN: A nonroutable UPN doesn't have a verified domain and is applicable only within your organization's private network. For example, if contoso.com is the primary domain in Microsoft Entra ID and contoso.local is the primary domain in on-premises AD but isn't a verifiable domain in the internet and only used within Contoso's network.

 **Note**

The information in this section applies only to an on-premises users UPN. It isn't applicable to an on-premises computer domain suffix (example: computer1.contoso.local).

The following table provides details on support for these on-premises Microsoft Windows Server Active Directory UPNs in Windows 10 Microsoft Entra hybrid join:

 [Expand table](#)

Type of on-premises Microsoft Windows Server Active Directory UPN	Domain type	Windows 10 version	Description
Routable	Federated	From 1703 release	Generally available
Nonroutable	Federated	From 1803 release	Generally available
Routable	Managed	From 1803 release	Generally available, Microsoft Entra SSPR on Windows lock screen isn't supported in environments where the on-premises UPN is different from the Microsoft Entra UPN. The on-premises UPN must be synced to the <code>onPremisesUserPrincipalName</code> attribute in Microsoft Entra ID
Nonroutable	Managed	Not supported	

Next steps

- Configure Microsoft Entra hybrid join
-

Feedback

Was this page helpful?

 Yes

 No

[Provide product feedback ↗](#)

Microsoft Entra hybrid join targeted deployment

Article • 11/27/2024

You can validate your [planning and prerequisites](#) for hybrid Microsoft Entra joining devices using a targeted deployment before enabling it across the entire organization. This article explains how to accomplish a targeted deployment of Microsoft Entra hybrid join.

⊗ Caution

Use caution when modifying values in Active Directory. Making changes in an established environment might have unintended consequences.

Targeted deployment of Microsoft Entra hybrid join on Windows devices

For devices running Windows 10, the minimum supported version is Windows 10 (version 1607) to do hybrid join. As a best practice, upgrade to the latest version of Windows 10 or 11.

To do a targeted deployment of Microsoft Entra hybrid join on Windows devices, you need to:

1. [Clear the Service Connection Point \(SCP\) entry from Windows Server Active Directory if it exists.](#)
2. [Configure client-side registry setting for SCP on your domain-joined computers using a Group Policy Object \(GPO\).](#)
3. If you're using Active Directory Federation Services (AD FS), you must also [configure the client-side registry setting for SCP on your AD FS server using a GPO.](#)
4. You might need to [customize synchronization options](#) in Microsoft Entra Connect to enable device synchronization.

💡 Tip

The SCP might be configured locally in the registry of the device in certain situations. If the device finds a value in the registry it uses that configuration, otherwise it queries the directory for the SCP and attempts to hybrid join.

Clear the SCP from Microsoft Windows Server Active Directory

Use the Active Directory Services Interfaces Editor (ADSI Edit) to modify the SCP objects in Microsoft Windows Server Active Directory.

1. Launch the **ADSI Edit** desktop application from an administrative workstation or a domain controller as an Enterprise Administrator.
2. Connect to the **Configuration Naming Context** of your domain.
3. Browse to **CN=Configuration,DC=contoso,DC=com > CN=Services > CN=Device Registration Configuration**.
4. Right-click on the leaf object **CN=62a0ff2e-97b9-4513-943f-0d221bd30080** and select **Properties**.
 - a. Select **keywords** from the **Attribute Editor** window and select **Edit**.
 - b. Select the values of **azureADId** and **azureADName** (one at a time) and select **Remove**.
5. Close **ADSI Edit**.

Configure client-side registry setting for SCP

Use the following example to create a Group Policy Object (GPO) to deploy a registry setting configuring an SCP entry in the registry of your devices.

1. Open a Group Policy Management console and create a new Group Policy Object in your domain.
 - a. Provide your newly created GPO a name (for example, ClientSideSCP).
2. Edit the GPO and locate the following path: **Computer Configuration > Preferences > Windows Settings > Registry**.
3. Right-click on the Registry and select **New > Registry Item**.
 - a. On the **General** tab, configure the following.
 - i. Action: **Update**.
 - ii. Hive: **HKEY_LOCAL_MACHINE**.
 - iii. Key Path: **SOFTWARE\Microsoft\Windows\CurrentVersion\CDJ\AAD**.
 - iv. Value name: **TenantId**.
 - v. Value type: **REG_SZ**.
 - vi. Value data: The globally unique identifier (GUID) or **Tenant ID** of your Microsoft Entra tenant, which can be found in **Identity > Overview > Properties > Tenant ID**.
 - b. Select **OK**.
4. Right-click on the Registry and select **New > Registry Item**.
 - a. On the **General** tab, configure the following.

- i. Action: **Update**.
 - ii. Hive: **HKEY_LOCAL_MACHINE**.
 - iii. Key Path: **SOFTWARE\Microsoft\Windows\CurrentVersion\CDJ\AAD**.
 - iv. Value name: **TenantName**.
 - v. Value type: **REG_SZ**.
 - vi. Value data: Your verified **domain name** if you're using federated environment such as AD FS. Your verified **domain name** or your onmicrosoft.com domain name, for example `contoso.onmicrosoft.com` if you're using managed environment.
- b. Select **OK**.
5. Close the editor for the newly created GPO.
 6. Link the newly created GPO to the correct organizational unit (OU) containing domain-joined computers that belong to your controlled rollout population.

Configure AD FS settings

If your Microsoft Entra ID is federated with AD FS, you first need to configure client-side SCP using the instructions mentioned earlier by linking the GPO to your AD FS servers. The SCP object defines the source of authority for device objects. It can be on-premises or Microsoft Entra ID. When client-side SCP is configured for AD FS, the source for device objects is established as Microsoft Entra ID.

Note

If you failed to configure client-side SCP on your AD FS servers, the source for device identities would be considered as on-premises. AD FS will then start deleting device objects from on-premises directory after the stipulated period defined in the AD FS Device Registration's attribute "MaximumInactiveDays". AD FS Device Registration objects can be found using the [Get-AdfsDeviceRegistration cmdlet](#).

Why a device might be in a pending state

When you configure a **Microsoft Entra hybrid join** task in the Microsoft Entra Connect Sync for your on-premises devices, the task syncs device objects to Microsoft Entra ID, and temporarily set the registered state of the devices to "pending" before the device completes the device registration. This pending state is because the device must be added to the Microsoft Entra directory before it can be registered. For more information about the device registration process, see [How it works: Device registration](#).

Post validation

After you verify that everything works as expected, you can automatically register the rest of your Windows devices with Microsoft Entra ID. Automate Microsoft Entra hybrid join by [configuring the SCP using Microsoft Entra Connect](#).

Related content

- [Plan your Microsoft Entra hybrid join implementation](#)
 - [Configure Microsoft Entra hybrid join](#)
 - [Configure Microsoft Entra hybrid join manually](#)
-

Feedback

Was this page helpful?



[Provide product feedback](#) ↗

Configure Microsoft Entra hybrid join

Article • 02/27/2025

Bringing your devices to Microsoft Entra ID maximizes user productivity through single sign-on (SSO) across your cloud and on-premises resources. You can secure access to your resources with [Conditional Access](#) at the same time.

<https://www.youtube-nocookie.com/embed/hSCVR1oJhFI>

Prerequisites

- [Microsoft Entra Connect](#) version 1.1.819.0 or later.
 - Don't exclude the default device attributes from your Microsoft Entra Connect Sync configuration. To learn more about default device attributes synced to Microsoft Entra ID, see [Attributes synchronized by Microsoft Entra Connect](#).
 - If the computer objects of the devices you want to be Microsoft Entra hybrid joined belong to specific organizational units (OUs), configure the correct OUs to sync in Microsoft Entra Connect. To learn more about how to sync computer objects by using Microsoft Entra Connect, see [Organizational unit-based filtering](#).
- [Hybrid Identity Administrator](#) credentials for your Microsoft Entra tenant.
- Enterprise administrator credentials for each of the on-premises Active Directory Domain Services forests.
- **(For federated domains)** At least Windows Server 2012 R2 with Active Directory Federation Services installed.
- Users can register their devices with Microsoft Entra ID. More information about this setting can be found under the heading **Configure device settings**, in the article, [Configure device settings](#).

Network connectivity requirements

Microsoft Entra hybrid join requires devices to have access to the following Microsoft resources from inside your organization's network:

- `https://enterpriseregistration.windows.net`
- `https://login.microsoftonline.com`
- `https://device.login.microsoftonline.com`
- `https://autologon.microsoftazuread-sso.com` (If you use or plan to use seamless SSO)
- Your organization's Security Token Service (STS) **(For federated domains)**

Warning

If your organization uses proxy servers that intercept SSL traffic for scenarios like data loss prevention or Microsoft Entra tenant restrictions, ensure that traffic to

`https://device.login.microsoftonline.com` and

`https://enterpriseregistration.windows.net` are excluded from TLS break-and-

inspect. Failure to exclude these URLs might cause interference with client certificate authentication, cause issues with device registration, and device-based Conditional Access.

If your organization requires access to the internet via an outbound proxy, you can use [Web Proxy Auto-Discovery \(WPAD\)](#) to enable Windows 10 or newer computers for device registration with Microsoft Entra ID. To address issues configuring and managing WPAD, see [Troubleshooting Automatic Detection](#).

If you don't use WPAD, you can configure WinHTTP proxy settings on your computer with a Group Policy Object (GPO) beginning with Windows 10 1709. For more information, see [WinHTTP Proxy Settings deployed by GPO](#).

Note

If you configure proxy settings on your computer by using WinHTTP settings, any computers that can't connect to the configured proxy will fail to connect to the internet.

If your organization requires access to the internet via an authenticated outbound proxy, make sure that your Windows 10 or newer computers can successfully authenticate to the outbound proxy. Because Windows 10 or newer computers run device registration by using machine context, configure outbound proxy authentication by using machine context. Follow up with your outbound proxy provider on the configuration requirements.

Verify devices can access the required Microsoft resources under the system account by using the [Test Device Registration Connectivity](#) script.

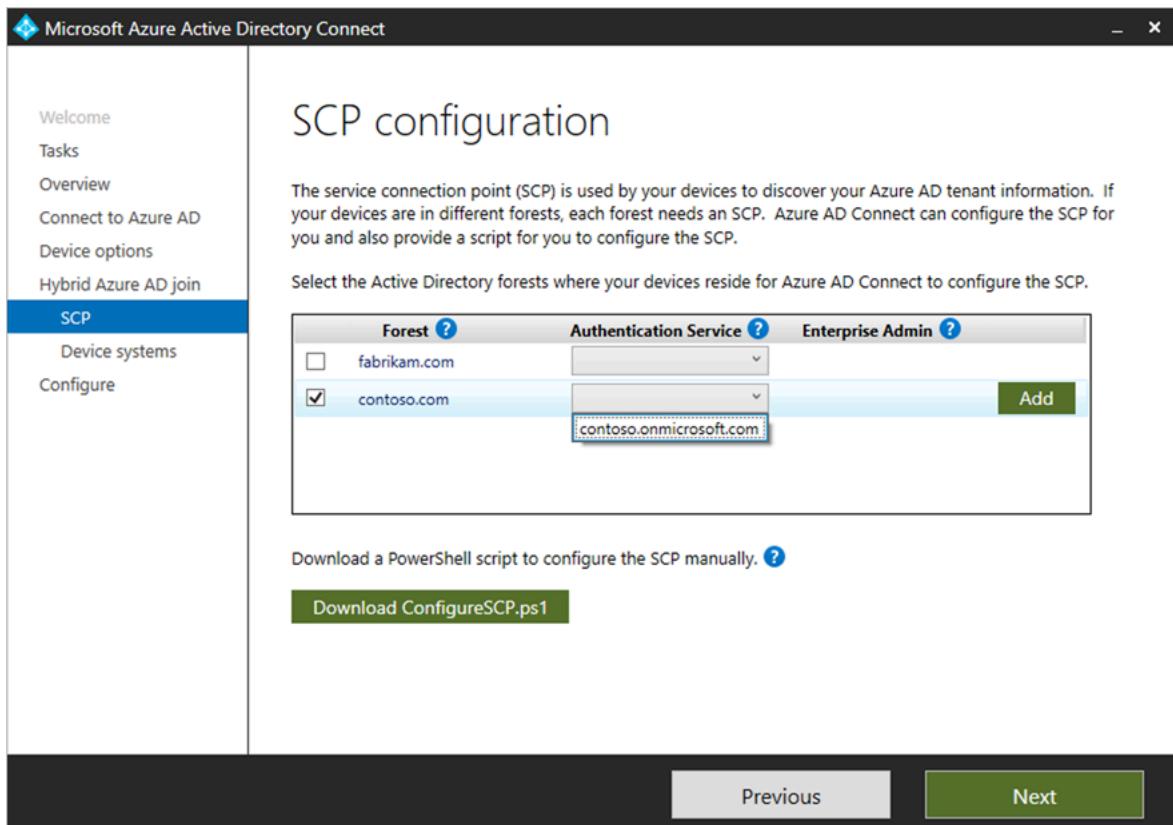
Managed domains

We think most organizations deploy Microsoft Entra hybrid join with managed domains. Managed domains use [password hash sync \(PHS\)](#) or [pass-through authentication \(PTA\)](#)

with [seamless single sign-on](#). Managed domain scenarios don't require configuring a federation server.

Configure Microsoft Entra hybrid join by using Microsoft Entra Connect for a managed domain:

1. Open Microsoft Entra Connect, and then select **Configure**.
2. In **Additional tasks**, select **Configure device options**, and then select **Next**.
3. In **Overview**, select **Next**.
4. In **Connect to Microsoft Entra ID**, enter the credentials of a [Hybrid Identity Administrator](#) for your Microsoft Entra tenant.
5. In **Device options**, select **Configure Microsoft Entra hybrid join**, and then select **Next**.
6. In **Device operating systems**, select the operating systems that devices in your Active Directory environment use, and then select **Next**.
7. In **SCP configuration**, for each forest where you want Microsoft Entra Connect to configure a service connection point (SCP), complete the following steps, and then select **Next**.
 - a. Select the **Forest**.
 - b. Select an **Authentication Service**.
 - c. Select **Add** to enter the enterprise administrator credentials.



8. In Ready to configure, select **Configure**.

9. In Configuration complete, select **Exit**.

Federated domains

A federated environment should have an identity provider that supports the following requirements. If you have a federated environment using Active Directory Federation Services (AD FS), then the below requirements are already supported.

- **WS-Trust protocol:** This protocol is required to authenticate the Microsoft Entra hybrid joined devices with Microsoft Entra ID. When you're using AD FS, you need to enable the following WS-Trust endpoints:
 - /adfs/services/trust/2005/windowstransport
 - /adfs/services/trust/13/windowstransport
 - /adfs/services/trust/2005/usernamemixed
 - /adfs/services/trust/13/usernamemixed
 - /adfs/services/trust/2005/certificatemixed
 - /adfs/services/trust/13/certificatemixed

⚠ Warning

Both `adfs/services/trust/2005/windowstransport` and `adfs/services/trust/13/windowstransport` should be enabled as intranet facing

endpoints only and must NOT be exposed as extranet facing endpoints through the Web Application Proxy. To learn more on how to disable WS-Trust Windows endpoints, see [Disable WS-Trust Windows endpoints on the proxy](#). You can see what endpoints are enabled through the AD FS management console under **Service > Endpoints**.

Configure Microsoft Entra hybrid join by using Microsoft Entra Connect for a federated environment:

1. Open Microsoft Entra Connect, and then select **Configure**.
2. On the **Additional tasks** page, select **Configure device options**, and then select **Next**.
3. On the **Overview** page, select **Next**.
4. On the **Connect to Microsoft Entra ID** page, enter the credentials of a [Hybrid Identity Administrator](#) for your Microsoft Entra tenant, and then select **Next**.
5. On the **Device options** page, select **Configure Microsoft Entra hybrid join**, and then select **Next**.
6. On the **SCP** page, complete the following steps, and then select **Next**:
 - a. Select the forest.
 - b. Select the authentication service. You must select **AD FS server** unless your organization has exclusively Windows 10 or newer clients and you configure computer/device sync, or your organization uses seamless SSO.
 - c. Select **Add** to enter the enterprise administrator credentials.

The screenshot shows the 'SCP configuration' page of the Microsoft Azure Active Directory Connect interface. On the left, a sidebar lists various tasks: Welcome, Tasks, Overview, Connect to Azure AD, Device options, Hybrid Azure AD join, SCP (which is selected and highlighted in blue), Device systems, Federation, and Configure. The main content area has a title 'SCP configuration'. It contains a paragraph explaining that the service connection point (SCP) is used by devices to discover Azure AD tenant information, noting that if devices are in different forests, each forest needs its own SCP. It also says that Azure AD Connect can configure the SCP for you or provide a script for manual configuration. Below this is a table titled 'Select forests where you want Azure AD Connect to configure the SCP.' The table has three columns: 'Forest', 'Authentication Service', and 'Enterprise Admin'. Under 'Forest', there are two entries: 'fabrikam.com' (unchecked) and 'contoso.com' (checked). Under 'Authentication Service' for 'contoso.com', a dropdown menu shows 'contoso.onmicrosoft.com' and 'fs.contoso.com'. A green 'Add' button is located at the bottom right of the dropdown. At the bottom of the page are 'Previous' and 'Next' navigation buttons.

7. On the **Device operating systems** page, select the operating systems that the devices in your Active Directory environment use, and then select **Next**.
8. On the **Federation configuration** page, enter the credentials of your AD FS administrator, and then select **Next**.
9. On the **Ready to configure** page, select **Configure**.
10. On the **Configuration complete** page, select **Exit**.

Federation caveats

With Windows 10 1803 or newer, if instantaneous Microsoft Entra hybrid join for a federated environment using federation service fails, we rely on Microsoft Entra Connect to sync the computer object in Microsoft Entra ID to complete the device registration for Microsoft Entra hybrid join.

Other scenarios

Organizations can test Microsoft Entra hybrid join on a subset of their environment before a full rollout. The steps to complete a targeted deployment can be found in the article [Microsoft Entra hybrid join targeted deployment](#). Organizations should include a sample of users from varying roles and profiles in this pilot group. A targeted rollout

helps identify any issues your plan might not address before you enable for the entire organization.

Some organizations might not be able to use Microsoft Entra Connect to configure AD FS. The steps to configure the claims manually can be found in the article [Configure Microsoft Entra hybrid join manually](#).

US Government cloud (inclusive of GCCHigh and DoD)

For organizations in [Azure Government](#), Microsoft Entra hybrid join requires devices to have access to the following Microsoft resources from inside your organization's network:

- `https://enterpriseregistration.windows.net` and
`https://enterpriseregistration.microsoftonline.us`
- `https://login.microsoftonline.us`
- `https://device.login.microsoftonline.us`
- `https://autologon.microsoft.us` (If you use or plan to use seamless SSO)

Troubleshoot Microsoft Entra hybrid join

If you experience issues with completing Microsoft Entra hybrid join for domain-joined Windows devices, see:

- [Troubleshooting devices using dsregcmd command](#)
- [Troubleshoot Microsoft Entra hybrid join for Windows current devices](#)
- [Troubleshoot Microsoft Entra hybrid join for Windows downlevel devices](#)
- [Troubleshoot pending device state](#)

Related content

- [Microsoft Entra hybrid join verification](#)
- [Use Conditional Access to require compliant or Microsoft Entra hybrid joined device](#)
- [Planning a Windows Hello for Business Deployment](#)

Feedback

Was this page helpful?

 Yes

 No

Provide product feedback 

Troubleshoot Microsoft Entra hybrid joined devices

Article • 11/25/2024

This article provides troubleshooting guidance to help you resolve potential issues with devices that are running Windows 10 or newer and Windows Server 2016 or newer.

Microsoft Entra hybrid join supports the Windows 10 November 2015 update and later.

This article assumes that you have [Microsoft Entra hybrid joined devices](#) to support the following scenarios:

- Device-based Conditional Access
- [Enterprise state roaming](#)
- [Windows Hello for Business](#)

① Note

To troubleshoot the common device registration issues, use [Device Registration Troubleshooter Tool](#).

Troubleshoot join failures

Step 1: Retrieve the join status

1. Open a Command Prompt window as an administrator.
2. Type `dsregcmd /status`.

```
+-----+  
| Device State |  
+-----+  
  
AzureAdJoined: YES  
EnterpriseJoined: NO  
    DeviceId: 5820fbe9-60c8-43b0-bb11-44aee233e4e7  
    Thumbprint: AA11BB22CC33DD44EE55FF66AA77BB88CC99DD00  
    KeyContainerId: bae6a60b-1d2f-4d2a-a298-33385f6d05e9  
    KeyProvider: Microsoft Platform Crypto Provider  
    TpmProtected: YES  
    KeySignTest: : MUST Run elevated to test.  
    Idp: login.windows.net  
    TenantId: aaaabbbb-0000-cccc-1111-dddd2222eeee  
    TenantName: Contoso  
    AuthCodeUrl: https://login.microsoftonline.com/msitsupp.microsoft.com/oauth2/authorize  
    AccessTokenUrl: https://login.microsoftonline.com/msitsupp.microsoft.com/oauth2/token  
    MdmUrl: https://enrollment.manage-beta.microsoft.com/EnrollmentServer/Discovery.svc  
    MdmTouUrl: https://portal.manage-beta.microsoft.com/TermsOfUse.aspx  
    dmComplianceUrl: https://portal.manage-beta.microsoft.com/?portalAction=Compliance  
    SettingsUrl: eyJVc{lots of characters}JdfQ==  
JoinSrvVersion: 1.0  
    JoinSrvUrl: https://enterpriseregistration.windows.net/EnrollmentServer/device/  
    JoinSrvId: urn:ms-drs:enterpriseregistration.windows.net  
KeySrvVersion: 1.0
```

```

KeySrvUrl: https://enterpriseregistration.windows.net/EnrollmentServer/key/
KeySrvId: urn:ms-drs:enterpriseregistration.windows.net
DomainJoined: YES
DomainName: CONTOSO

+-----+
| User State |
+-----+

    NgcSet: YES
    NgcKeyId: {aaaaaaaa-0b0b-1c1c-2d2d-333333333333}
WorkplaceJoined: NO
    WamDefaultSet: YES
WamDefaultAuthority: organizations
    WamDefaultId: https://login.microsoft.com
    WamDefaultGUID: {B16898C6-A148-4967-9171-64D755DA8520} (AzureAd)
    AzureAdPrt: YES

```

Step 2: Evaluate the join status

Review the fields in the following table, and make sure that they have the expected values:

[\[+\] Expand table](#)

Field	Expected value	Description
DomainJoined	YES	<p>This field indicates whether the device is joined to an on-premises Active Directory.</p> <p>If the value is <i>NO</i>, the device can't do Microsoft Entra hybrid join.</p>
WorkplaceJoined	NO	<p>This field indicates whether the device is registered with Microsoft Entra ID as a personal device (marked as <i>Workplace Joined</i>). This value should be <i>NO</i> for a domain-joined computer that's also Microsoft Entra hybrid joined.</p> <p>If the value is <i>YES</i>, a work or school account was added before the completion of the Microsoft Entra hybrid join. In this case, the account is ignored when you're using Windows 10 version 1607 or later.</p>
AzureAdJoined	YES	<p>This field indicates whether the device is joined. The value is <i>YES</i> if the device is either a Microsoft Entra joined device or a Microsoft Entra hybrid joined device.</p> <p>If the value is <i>NO</i>, the join to Microsoft Entra ID hasn't finished yet.</p>

Continue to the next steps for further troubleshooting.

Step 3: Find the phase in which the join failed, and the error code

For Windows 10 version 1803 or later

Look for the "Previous Registration" subsection in the "Diagnostic Data" section of the join status output. This section is displayed only if the device is domain-joined and unable to Microsoft Entra hybrid join.

The "Error Phase" field denotes the phase of the join failure, and "Client ErrorCode" denotes the error code of the join operation.

```
+-----+  
    Previous Registration : 2019-01-31 09:16:43.000 UTC  
    Registration Type : sync  
    Error Phase : join  
    Client ErrorCode : 0x801c03f2  
    Server ErrorCode : DirectoryError  
    Server Message : The device object by the given id (e92325d0-xxxx-xxxx-xxxx-  
94ae875d5245) isn't found.  
    Https Status : 400  
    Request Id : 6bff0bd9-820b-484b-ab20-2a4f7b76c58e  
+-----+
```

For earlier Windows 10 versions

Use Event Viewer logs to locate the phase and error code for the join failures.

1. In Event Viewer, open the **User Device Registration** event logs. They're stored under **Applications and Services Log > Microsoft > Windows > User Device Registration**.
 2. Look for events with the following event IDs: 304, 305, and 307.

The screenshot shows the Windows Event Viewer interface. The left pane displays a tree view of system components, with 'User Device Registration' expanded and its sub-item 'Admin' selected. The right pane shows a list of events under the heading 'Admin Number of events: 5'. The first event, listed as an 'Error' with ID 304, is highlighted. Below the event list is a detailed view for event 304, titled 'Event 304, User Device Registration'. This view contains two tabs: 'General' (selected) and 'Details'. The 'General' tab shows the error message: 'Automatic registration failed at join phase. Exit code: Unknown HRESULT Error code: 0x801c003d'. The 'Details' tab lists several properties with their values set to 'undefined': Tenant type, Registration type, Debug Output, joinMode, dslInstance, registrationType, tenantType, tenantId, configLocation, and errorPhase (which is highlighted in yellow). At the bottom of the details pane, there are log name, source, log date, event ID, and task category fields.

Level	Source	Event ID	Task C...
Error	User Device Registration	304	None
Error	User Device Registration	309	None
Information	User Device Registration	101	None
Information	User Device Registration	100	None
Information	User Device Registration	331	None

Event 304, User Device Registration

General Details

Automatic registration failed at join phase.
Exit code: Unknown HRESULT Error code: 0x801c003d
Server error:
Tenant type: undefined
Registration type: undefined
Debug Output:
joinMode: Join
dslInstance: undefined
registrationType: undefined
tenantType: undefined
tenantId: undefined
configLocation: undefined
errorPhase: discover

Log Name: Microsoft-Windows-User Device Registration/Admin
Source: User Device Registration Logged: 1/31/2019 12:48:31 AM
Event ID: 304 Task Category: None

The screenshot shows the Windows Event Viewer interface. The left pane displays a tree view of event sources, with 'User Device Registration' expanded to show 'Admin' and 'Debug' sub-sources. The right pane shows a list of events for the 'Admin' source. There are seven events listed:

Level	Source	Event ID	Task Category
Error	User Device Registration	305	None
Information	User Device Registration	101	None
Information	User Device Registration	100	None
Warning	User Device Registration	360	None
Warning	User Device Registration	362	None

A detailed view of the first event (Event ID 305) is shown in the bottom pane. The 'General' tab is selected, displaying the following log message:

```
Automatic registration failed at authentication phase. Unable to acquire access token.  
Exit code: Unknown HRESULT Error code: 0xcaa1002d  
Tenant Name: hybridadfsalt.ngtest.com  
Tenant Type: Federated  
Server error:  
AdalMessage: GetStatus returned failure  
AdalErrorCode: 0xcaa90006  
AdalCorrelationId: undefined  
AdalLog: HRESULT: 0xcaa90006  
AdalLog: HRESULT: 0xcaa1002d  
AdalLog: Set to fatal network error since status code >= 500 ; HRESULT: 0x0  
AdalLog: Token response is not successfull. Status:502 ResponseText:Fiddler: HTTP/502 unreachable server.  
I_HRESCII T_<n>
```

The 'Details' tab is also visible in the bottom pane.

Step 4: Check for possible causes and resolutions

Precheck phase

Possible reasons for failure:

- The device has no line of sight to the domain controller.
 - The device must be on the organization's internal network or on a virtual private network with a network line of sight to an on-premises Active Directory domain controller.

Discover phase

Possible reasons for failure:

- The service connection point object is misconfigured or can't be read from the domain controller.
 - A valid service connection point object is required in the AD forest, to which the device belongs, that points to a verified domain name in Microsoft Entra ID.
 - For more information, see the "Configure a service connection point" section of [Tutorial: Configure Microsoft Entra hybrid join for federated domains](#).
- Failure to connect to and fetch the discovery metadata from the discovery endpoint.
 - The device should be able to access `https://enterpriseregistration.windows.net`, in the system context, to discover the registration and authorization endpoints.
 - If the on-premises environment requires an outbound proxy, the IT admin must ensure that the computer account of the device can discover and silently authenticate to the outbound proxy.
- Failure to connect to the user realm endpoint and do realm discovery (Windows 10 version 1809 and later only).
 - The device should be able to access `https://login.microsoftonline.com`, in the system context, to do realm discovery for the verified domain and determine the domain type (managed or federated).
 - If the on-premises environment requires an outbound proxy, the IT admin must ensure that the system context on the device can discover and silently authenticate to the outbound proxy.

Common error codes:

[+] [Expand table](#)

Error code	Reason	Resolution
DSREG_AUTOJOIN_ADCONFIG_READ_FAILED (0x801c001d/-2145648611)	Unable to read the service connection point (SCP) object and get the Microsoft Entra tenant information.	Refer to the Configure a service connection point section.
DSREG_AUTOJOIN_DISC_FAILED (0x801c0021/-2145648607)	Generic discovery failure. Failed to get the discovery metadata from the data replication service (DRS).	To investigate further, find the suberror in the next sections.
DSREG_AUTOJOIN_DISC_WAIT_TIMEOUT (0x801c001f/-2145648609)	Operation timed out while performing discovery.	Ensure that <code>https://enterpriseregistration.windows.net</code> is accessible in the system context. For more information, see the Network connectivity requirements section.

Error code	Reason	Resolution
DSREG_AUTOJOIN_USERREALM_DISCOVERY_FAILED (0x801c003d/-2145648579)	Generic realm discovery failure. Failed to determine domain type (managed/federated) from STS.	To investigate further, find the suberror in the next sections.

Common sub-error codes:

To find the suberror code for the discovery error code, use one of the following methods.

Windows 10 version 1803 or later

Look for "DRS Discovery Test" in the "Diagnostic Data" section of the join status output. This section is displayed only if the device is domain-joined and unable to Microsoft Entra hybrid join.

```
+-----+
| Diagnostic Data |
+-----+
Diagnostics Reference : www.microsoft.com/aaderrors
User Context : UN-ELEVATED User
Client Time : 2019-06-05 08:25:29.000 UTC
AD Connectivity Test : PASS
AD Configuration Test : PASS
DRS Discovery Test : FAIL [0x801c0021/0x80072ee2]
DRS Connectivity Test : SKIPPED
Token acquisition Test : SKIPPED
Fallback to Sync-Join : ENABLED
+-----+
```

Earlier Windows 10 versions

Use Event Viewer logs to look for the phase and error code for the join failures.

1. In Event Viewer, open the **User Device Registration** event logs. They're stored under **Applications and Services Log > Microsoft > Windows > User Device Registration**.
2. Look for event ID 201.

Admin Number of events: 13

Level	Date and Time	Source	Event ID	Task Ca...
Error	6/6/2019 2:23:23 PM	User Devic...	233	None
Error	6/6/2019 2:23:23 PM	User Devic...	201	None
Information	6/6/2019 2:24:10 PM	User Devic...	331	None
Information	6/6/2019 2:24:10 PM	User Devic...	100	None
Error	6/6/2019 2:24:10 PM	User Devic...	233	None
Error	6/6/2019 2:24:10 PM	User Devic...	201	None
Error	6/6/2019 2:24:10 PM	User Devic...	309	None
Error	6/6/2019 2:24:10 PM	User Devic...	304	None

Event 201, User Device Registration

General Details

The discovery operation callback failed with exit code: Unknown HRESULT Error code: 0x80072f78. The server returned HTTP status: 0. Server response was:

Log Name: Microsoft-Windows-User Device Registration/Admin
Source: User Device Registration Logged: 6/6/2019 2:23:23 PM

Network errors:

[Expand table](#)

Error code	Reason	Resolution
WININET_E_CANNOT_CONNECT (0x80072efd/-2147012867)	Connection with the server couldn't be established.	Ensure network connectivity to the required Microsoft resources. For more information, see Network connectivity requirements .
WININET_E_TIMEOUT (0x80072ee2/-2147012894)	General network timeout.	Ensure network connectivity to the required Microsoft resources. For more information, see Network connectivity requirements .
WININET_E_DECODING_FAILED (0x80072f8f/-2147012721)	Network stack was unable to decode the response from the server.	Ensure that the network proxy isn't interfering and modifying the server response.

HTTP errors:

[Expand table](#)

Error code	Reason	Resolution
DSREG_DISCOVERY_TENANT_NOT_FOUND (0x801c003a/-2145648582)	The service connection point object is configured with the wrong tenant ID, or no active subscriptions were found in the tenant.	Ensure that the service connection point object is configured with the correct Microsoft Entra tenant ID and active subscriptions or that the service is present in the tenant.
DSREG_SERVER_BUSY (0x801c0025/-2145648603)	HTTP 503 from DRS server.	The server is currently unavailable. Future join attempts will likely succeed after the server is back online.

Other errors:

[+] Expand table

Error code	Reason	Resolution
E_INVALIDDATA (0x8007000d/-2147024883)	The server response JSON couldn't be parsed, likely because the proxy is returning an HTTP 200 with an HTML authorization page.	If the on-premises environment requires an outbound proxy, the IT admin must ensure that the system context on the device can discover and silently authenticate to the outbound proxy.

Authentication phase

This content applies only to federated domain accounts.

Reasons for failure:

- Unable to get an access token silently for the DRS resource.
 - Windows 10 and Windows 11 devices acquire the authentication token from the Federation Service by using integrated Windows authentication to an active WS-Trust endpoint. For more information, see [Federation Service configuration](#).

Common error codes:

Use Event Viewer logs to locate the error code, suberror code, server error code, and server error message.

1. In Event Viewer, open the **User Device Registration** event logs. They're stored under **Applications and Services Log > Microsoft > Windows > User Device Registration**.
2. Look for event ID 305.

Level	Source	Event ID	Task C...
Error	User Device Registration	305	None
Information	User Device Registration	101	None
Information	User Device Registration	100	None
Warning	User Device Registration	360	None
Warning	User Device Registration	362	None

Event 305, User Device Registration

General Details

Automatic registration failed at authentication phase. Unable to acquire access token.
Exit code: Unknown HRESULT Error code: 0xcaa1002d
Tenant Name: hybridadsalt.ngctest.com
Tenant Type: Federated
Server error:
AdalMessage: GetStatus returned failure
AdalErrorCode: 0xcaa90006
AdalCorrelationId: undefined
AdalLog: HRESULT: 0xcaa90006
AdalLog: HRESULT: 0xcaa1002d
AdalLog: Set to fatal network error since status code >= 500 ; HRESULT: 0x0
AdalLog: Token response is not successfull. Status:502 ResponseText:Fiddler: HTTP/502 unreachable server.

Log Name: Microsoft-Windows-User Device Registration/Admin
Source: User Device Registration
Logged: 1/31/2019 12:41:04 AM
Event ID: 305
Task Category: None

Configuration errors:

[+] Expand table

Error code	Reason	Resolution
ERROR_ADAL_PROTOCOL_NOT_SUPPORTED (0xcaa90017/-894894057)	The Azure AD Authentication Library (ADAL) authentication	The on-premises identity provider must

Error code	Reason	Resolution
	protocol isn't WS-Trust.	support WS-Trust.
ERROR_ADAL_FAILED_TO_PARSE_XML (0xcaa9002c/-894894036)	The on-premises Federation Service didn't return an XML response.	Ensure that the Metadata Exchange (MEX) endpoint is returning a valid XML. Ensure that the proxy isn't interfering and returning nonxml responses.
ERROR_ADAL_COULDNOT_DISCOVER_USERNAME_PASSWORD_ENDPOINT (0xcaa90023/-894894045)	Couldn't discover an endpoint for username/password authentication.	Check the on-premises identity provider settings. Ensure that the WS-Trust endpoints are enabled and that the MEX response contains these correct endpoints.

Network errors:

[+] Expand table

Error code	Reason	Resolution
ERROR_ADAL_INTERNET_TIMEOUT (0xcaa82ee2/-894947614)	General network timeout.	Ensure that https://login.microsoftonline.com is accessible in the system context. Ensure that the on-premises identity provider is accessible in the system context. For more information, see Network connectivity requirements .
ERROR_ADAL_INTERNET_CONNECTION_ABORTED (0xcaa82efe/-894947586)	Connection with the authorization endpoint was aborted.	Retry the join after a while, or try joining from another stable network location.
ERROR_ADAL_INTERNET_SECURE_FAILURE (0xcaa82f8f/-894947441)	The Transport Layer Security (TLS) certificate (previously known as the Secure Sockets Layer [SSL] certificate) sent by the server couldn't be validated.	Check the client time skew. Retry the join after a while, or try joining from another stable network location.
ERROR_ADAL_INTERNET_CANNOT_CONNECT (0xcaa82efd/-894947587)	The attempt to connect to https://login.microsoftonline.com	Check the network connection to https://login.microsoftonline.com .

Error code	Reason	Resolution
	failed.	

Other errors:

[\[+\] Expand table](#)

Error code	Reason	Resolution
ERROR_ADAL_SERVER_ERROR_INVALID_GRANT (0xcaa20003/-895352829)	The SAML token from the on-premises identity provider wasn't accepted by Microsoft Entra ID.	Check the Federation Server settings. Look for the server error code in the authentication logs.
ERROR_ADAL_WSTRUST_REQUEST_SECURITYTOKEN_FAILED (0xcaa90014/-894894060)	The Server WS-Trust response reported a fault exception, and it failed to get assertion.	Check the Federation Server settings. Look for the server error code in the authentication logs.
ERROR_ADAL_WSTRUST_TOKEN_REQUEST_FAIL (0xcaa90006/-894894074)	Received an error when trying to get access token from the token endpoint.	Look for the underlying error in the ADAL log.
ERROR_ADAL_OPERATION_PENDING (0xcaa1002d/-895418323)	General ADAL failure.	Look for the suberror code or server error code from the authentication logs.

Join phase

Reasons for failure:

Look for the registration type and error code from the following tables, depending on the Windows 10 version you're using.

Windows 10 version 1803 or later

Look for the "Previous Registration" subsection in the "Diagnostic Data" section of the join status output. This section is displayed only if the device is domain-joined and is unable to Microsoft Entra hybrid join.

The "Registration Type" field denotes the type of join.

+-----+ Previous Registration : 2019-01-31 09:16:43.000 UTC Registration Type : sync Error Phase : join Client ErrorCode : 0x801c03f2 Server ErrorCode : DirectoryError Server Message : The device object by the given id (aaaaaaaa-0000-1111-2222-bbbbbbbbbbbb) is not found. Https Status : 400

+-----+

Earlier Windows 10 versions

Use Event Viewer logs to locate the phase and error code for the join failures.

1. In Event Viewer, open the **User Device Registration** event logs. They're stored under **Applications and Services Log > Microsoft > Windows > User Device Registration**.
2. Look for event ID 204.

Level	Date and Time	Source	Event ID	Task Category
Error	6/5/2019 10:29:40 PM	User Devic...	204	None
Error	6/5/2019 10:31:51 PM	User Devic...	204	None
Error	6/4/2019 9:36:02 PM	User Devic...	204	None
Error	6/5/2019 10:30:13 PM	User Devic...	204	None
Error	6/5/2019 10:30:15 PM	User Devic...	204	None

Event 204, User Device Registration

General **Details**

```
The get join response operation callback failed with exit code: Unknown HRESULT Error code: 0x801c03ed.
Activity Id: 8a350d06-5a1e-4fbc-8811-ae021c043b3e
The server returned HTTP status: 400
Server response was: {"ErrorType": "UnknownError", "Message": "ASN1 unexpected end of data. (Exception from HRESULT: 0x80093102)", "TraceId": "8a350d06-5a1e-4fbc-8811-ae021c043b3e", "Time": "08-31-2018 22:45:58Z"}
```

Log Name: Microsoft-Windows-User Device Registration/Admin
 Source: User Device Registration Logged: 6/5/2019 10:29:40 PM
 Event ID: 204 Task Category: None

HTTP errors returned from DRS server:

[+] Expand table

Error code	Reason	Resolution
DSREG_E_DIRECTORY_FAILURE (0x801c03f2/-2145647630)	Received an error response from DRS with ErrorCode: "DirectoryError".	Refer to the server error code for possible reasons and resolutions.
DSREG_E_DEVICE_AUTHENTICATION_ERROR (0x801c0002/-2145648638)	Received an error response from DRS with ErrorCode: "AuthenticationError" and ErrorSubCode is <i>not</i> "DeviceNotFound".	Refer to the server error code for possible reasons and resolutions.
DSREG_E_DEVICE_INTERNALSERVICE_ERROR (0x801c0006/-2145648634)	Received an error response from DRS with ErrorCode: "DirectoryError".	Refer to the server error code for possible reasons and resolutions.

TPM errors:

[Expand table](#)

Error code	Reason	Resolution
NTE_BAD_KEYSET (0x80090016/-2146893802)	The Trusted Platform Module (TPM) operation failed or was invalid.	This error indicates that the keyset doesn't exist. This error happens when the TPM is cleared on the systems, or when there's a bad sysprep image. Avoid clearing the TPM in BIOS or Windows settings. If the TPM is cleared, users might need to recover by removing and readding accounts to fix the problem, especially when they have multiple WAM accounts. Ensure that the machine from which the sysprep image was created isn't Microsoft Entra joined, Microsoft Entra hybrid joined, or Microsoft Entra registered.
TPM_E_PCP_INTERNAL_ERROR (0x80290407/-2144795641)	Generic TPM error.	Disable TPM on devices with this error. Windows 10 versions 1809 and later automatically detect TPM failures and complete Microsoft Entra hybrid join without using the TPM.
TPM_E_NOTFIPS (0x80280036/-2144862154)	TPM in FIPS mode isn't currently supported.	Disable TPM on devices with this error. Windows 10 version 1809 automatically detects TPM failures and completes the Microsoft Entra hybrid join without using the TPM.
NTE_AUTHENTICATION_IGNORED (0x80090031/-2146893775)	TPM is locked out.	Transient error. Wait for the cool-down period. The join attempt should succeed after a while. For more information, see TPM fundamentals .

Network errors:

[Expand table](#)

Error code	Reason	Resolution
WININET_E_TIMEOUT (0x80072ee2/-2147012894)	General network time out trying to register the device at DRS.	Check network connectivity to https://enterpriseregistration.windows.net .
WININET_E_NAME_NOT_RESOLVED (0x80072ee7/-2147012889)	The server name or address couldn't be resolved.	Check network connectivity to https://enterpriseregistration.windows.net .
WININET_E_CONNECTION_ABORTED (0x80072efe/-2147012866)	The connection with the server was terminated abnormally.	Retry the join after a while, or try joining from another stable network location.

Other errors:

[Expand table](#)

Error code	Reason	Resolution
DSREG_AUTOJOIN_ADCONFIG_READ_FAILED (0x801c001d/-2145648611)	Event ID 220 is present in User Device Registration event logs. Windows can't access the computer object in Active Directory. A Windows	Troubleshoot replication issues in Active

Error code	Reason	Resolution
	error code might be included in the event. Error codes ERROR_NO SUCH_LOGON_SESSION (1312) and ERROR_NO SUCH_USER (1317) are related to replication issues in on-premises Active Directory.	Directory. These replication issues might be transient, and they might go away after a while.

Federated join server errors:

[+] Expand table

Server error code	Server error message	Possible reasons	Resolution
DirectoryError	Your request is throttled temporarily. Please try after 300 seconds.	This error is expected, possibly because multiple registration requests were made in quick succession.	Retry the join after the cool-down period

Sync-join server errors:

[+] Expand table

Server error code	Server error message	Possible reasons	Resolution
DirectoryError	AADSTS90002: Tenant <code>UUID</code> not found. This error might happen if there are no active subscriptions for the tenant. Check with your subscription administrator.	The tenant ID in the service connection point object is incorrect.	Ensure that the service connection point object is configured with the correct Microsoft Entra tenant ID and active subscriptions or that the service is present in the tenant.
DirectoryError	The device object by the given ID isn't found.	This error is expected for sync-join. The device object hasn't synced from AD to Microsoft Entra ID	Wait for the Microsoft Entra Connect Sync to finish, and the next join attempt after sync completion will resolve the issue.
AuthenticationError	The verification of the target computer's SID	The certificate on the Microsoft Entra device doesn't match the certificate used to sign in to the blob during the sync-join. This error ordinarily means that sync hasn't finished yet.	Wait for the Microsoft Entra Connect Sync to finish, and the next join attempt after the sync completion will resolve the issue.

Step 5: Collect logs and contact Microsoft Support

1. Download the [Auth.zip file](#).
2. Extract the files to a folder, such as `c:\temp`, and then go to the folder.
3. From an elevated Azure PowerShell session, run `.\start-auth.ps1 -v -accepteula`.
4. Select **Switch Account** to toggle to another session with the problem user.

5. Reproduce the issue.
6. Select **Switch Account** to toggle back to the admin session that's running the tracing.
7. From the elevated PowerShell session, run `.\stop-auth.ps1`.
8. Zip (compress) and send the folder *Authlogs* from the folder where the scripts were executed.

Troubleshoot post-join authentication issues

Step 1: Retrieve the PRT status by using `dsregcmd /status`

1. Open a Command Prompt window.

 **Note**

To get the Primary Refresh Token (PRT) status, open the Command Prompt window in the context of the logged-in user.

2. Run `dsregcmd /status`.

The "SSO state" section provides the current PRT status.

If the `AzureAdPrt` field is set to *NO*, there was an error acquiring the PRT status from Microsoft Entra ID.

3. If the `AzureAdPrtUpdateTime` is more than four hours, there's likely an issue with refreshing the PRT. Lock and unlock the device to force the PRT refresh, and then check to see whether the time updates.

```
+-----+
| SSO State                                |
+-----+
               AzureAdPrt : YES
               AzureAdPrtUpdateTime : 2020-07-12 22:57:53.000 UTC
               AzureAdPrtExpiryTime : 2019-07-26 22:58:35.000 UTC
               AzureAdPrtAuthority : https://login.microsoftonline.com/aaaabbbb-0000-cccc-1111-
               dddd2222eeee
               EnterprisePrt : YES
               EnterprisePrtUpdateTime : 2020-07-12 22:57:54.000 UTC
               EnterprisePrtExpiryTime : 2020-07-26 22:57:54.000 UTC
               EnterprisePrtAuthority : https://corp.hybridadfs.contoso.com:443/adfs
+-----+
```

Step 2: Find the error code

From the `dsregcmd` output

 **Note**

The output is available from the Windows 10 May 2021 update (version 21H1).

The "Attempt Status" field under the "AzureAdPrt" field provides the status of the previous PRT attempt, along with other required debug information. For earlier Windows versions, extract the information from the [Microsoft Entra analytics and operational logs](#).

```
+-----+
| SSO State                                |
+-----+

        AzureAdPrt : NO
        AzureAdPrtAuthority : https://login.microsoftonline.com/aaaabbbb-0000-cccc-1111-
dddd2222eeee
        AcquirePrtDiagnostics : PRESENT
        Previous Prt Attempt : 2020-07-18 20:10:33.789 UTC
            Attempt Status : 0xc000006d
            User Identity : john@contoso.com
            Credential Type : Password
            Correlation ID : aaaa0000-bb11-2222-33cc-444444dddddd
            Endpoint URI : https://login.microsoftonline.com/aaaabbbb-0000-cccc-1111-
dddd2222eeee/oauth2/token
            HTTP Method : POST
            HTTP Error : 0x0
            HTTP status : 400
            Server Error Code : invalid_grant
        Server Error Description : AADSTS50126: Error validating credentials due to invalid username
or password.
```

From the Microsoft Entra analytics and operational logs

Use Event Viewer to look for the log entries logged by the Microsoft Entra CloudAP plug-in during PRT acquisition.

1. In Event Viewer, open the Microsoft Entra Operational event logs. They're stored under **Applications and Services Log > Microsoft > Windows > AAD**.

① Note

The CloudAP plug-in logs error events in the operational logs, and it logs the info events in the analytics logs. The analytics and operational log events are both required to troubleshoot issues.

1. Event 1006 in the analytics logs denotes the start of the PRT acquisition flow, and event 1007 in the analytics logs denotes the end of the PRT acquisition flow. All events in the Microsoft Entra logs (analytics and operational) that are logged between events 1006 and 1007 were logged as part of the PRT acquisition flow.
2. Event 1007 logs the final error code.

Information	6/24/2020 3:35:35 AM	AAD	1006 AadCloudAPPlugin Operation
Information	6/24/2020 3:35:35 AM	AAD	1018 AadCloudAPPlugin Operation
Information	6/24/2020 3:35:35 AM	AAD	1144 AadCloudAPPlugin Operation
Error	6/24/2020 3:35:35 AM	AAD	1022 AadCloudAPPlugin Operation
Error	6/24/2020 3:35:35 AM	AAD	1084 AadCloudAPPlugin Operation
Error	6/24/2020 3:35:35 AM	AAD	1086 AadCloudAPPlugin Operation
Information	6/24/2020 3:35:35 AM	AAD	1160 AadCloudAPPlugin Operation
Information	6/24/2020 3:35:35 AM	AAD	1007 AadCloudAPPlugin Operation
Information	6/24/2020 3:35:35 AM	AAD	1157 AadCloudAPPlugin Operation
			1158 AadCloudAPPlugin Operation

Event 1007, AAD

General Details

AadCloudAPPlugin GetToken Stop.
Status: 0xC000023C

Step 3: Troubleshoot further, based on the found error code

[Expand table](#)

Error code	Reason	Resolution
STATUS_LOGON_FAILURE (-1073741715/ 0xc000006d) STATUS_WRONG_PASSWORD (-1073741718/ 0xc000006a)	<ul style="list-style-type: none"> The device is unable to connect to the Microsoft Entra authentication service. Received an error response (HTTP 400) from the Microsoft Entra authentication service or WS-Trust endpoint. <p>Note: WS-Trust is required for federated authentication.</p>	<ul style="list-style-type: none"> If the on-premises environment requires an outbound proxy, the IT admin must ensure that the computer account of the device can discover and silently authenticate to the outbound proxy. Events 1081 and 1088 (Microsoft Entra operational logs) would contain the server error code for errors originating from the Microsoft Entra authentication service and error description for errors originating from the WS-Trust endpoint. Common server error codes and their resolutions are listed in the next section. The first instance of event 1022 (Microsoft Entra analytics logs), preceding events 1081 or 1088, contain the URL that's being accessed.
STATUS_REQUEST_NOT_ACCEPTED (-1073741616/ 0xc00000d0)	<p>Received an error response (HTTP 400) from the Microsoft Entra authentication service or WS-Trust endpoint.</p> <p>Note: WS-Trust is required for federated authentication.</p>	<p>Events 1081 and 1088 (Microsoft Entra operational logs) would contain the server error code and error description for errors originating from Microsoft Entra authentication service and WS-Trust endpoint, respectively.</p> <p>Common server error codes and their resolutions are listed in the next section. The first instance of event 1022 (Microsoft Entra analytics logs), preceding events 1081 or 1088, contain the URL that's being accessed.</p>
STATUS_NETWORK_UNREACHABLE (-1073741252/ 0xc000023c) STATUS_BAD_NETWORK_PATH (-1073741634/	<ul style="list-style-type: none"> Received an error response (HTTP > 400) from 	<ul style="list-style-type: none"> For server errors, events 1081 and 1088 (Microsoft Entra operational logs) would contain the

Error code	Reason	Resolution
0xc0000be) STATUS_UNEXPECTED_NETWORK_ERROR (-1073741628/0xc0000c4)	<p>the Microsoft Entra authentication service or WS-Trust endpoint.</p> <p>Note: WS-Trust is required for federated authentication.</p> <ul style="list-style-type: none"> Network connectivity issue to a required endpoint. 	<p>error code from the Microsoft Entra authentication service and the error description from the WS-Trust endpoint. Common server error codes and their resolutions are listed in the next section.</p> <ul style="list-style-type: none"> For connectivity issues, event 1022 (Microsoft Entra analytics logs) contains the URL that's being accessed, and event 1084 (Microsoft Entra operational logs) contains the suberror code from the network stack.
STATUS_NO SUCH_LOGON_SESSION (-1073741729/0xc00005f)	<p>User realm discovery failed because the Microsoft Entra authentication service was unable to find the user's domain.</p>	<ul style="list-style-type: none"> The domain of the user's UPN must be added as a custom domain in Microsoft Entra ID. Event 1144 (Microsoft Entra analytics logs) will contain the UPN provided. If the on-premises domain name is nonroutable (jdoe@contoso.local), configure an Alternate Login ID (AltID). <p>References: Prerequisites; Configure Alternate Login ID.</p>
AAD_CLOUDAP_E_OAUTH_USERNAME_IS_MALFORMED (-1073445812/ 0xc004844c)	<p>The user's UPN isn't in the expected format.</p> <p>Notes:</p> <ul style="list-style-type: none"> For Microsoft Entra joined devices, the UPN is the text that's entered by the user in the LoginUI. For Microsoft Entra hybrid joined devices, the UPN is returned from the domain controller during the login process. 	<ul style="list-style-type: none"> User's UPN should be in the internet-style login name, based on the internet standard RFC 822. Event 1144 (Microsoft Entra analytics logs) contains the UPN provided. For hybrid-joined devices, ensure that the domain controller is configured to return the UPN in the correct format. In the domain controller, <code>whoami /upn</code> should display the configured UPN. If the on-premises domain name is nonroutable (jdoe@contoso.local), configure Alternate Login ID (AltID). <p>References: Prerequisites; Configure Alternate Login ID.</p>
AAD_CLOUDAP_E_OAUTH_USER_SID_IS_EMPTY (-1073445822/ 0xc0048442)	<p>The user SID is missing in the ID token that's returned by the Microsoft Entra authentication service.</p>	<p>Ensure that the network proxy isn't interfering with and modifying the server response.</p>
AAD_CLOUDAP_E_WSTRUST_SAML_TOKENS_ARE_EMPTY (--1073445695/ 0xc00484c1)	<p>Received an error from the WS-Trust endpoint.</p> <p>Note: WS-Trust is required for</p>	<ul style="list-style-type: none"> Ensure that the network proxy isn't interfering with and modifying the WS-Trust response. Event 1088 (Microsoft Entra operational logs) would contain the

Error code	Reason	Resolution
	federated authentication.	server error code and error description from the WS-Trust endpoint. Common server error codes and their resolutions are listed in the next section.
AAD_CLOUDAP_E_HTTP_PASSWORD_URI_IS_EMPTY (-1073445749/ 0xc004848b)	The MEX endpoint is incorrectly configured. The MEX response doesn't contain any password URLs.	<ul style="list-style-type: none"> Ensure that the network proxy isn't interfering with and modifying the server response. Fix the MEX configuration to return valid URLs in response.
AAD_CLOUDAP_E_HTTP_CERTIFICATE_URI_IS_EMPTY (-1073445748/ 0xc004848C)	The MEX endpoint is incorrectly configured. The MEX response doesn't contain any certificate endpoint URLs.	<ul style="list-style-type: none"> Ensure that the network proxy isn't interfering with and modifying the server response. Fix the MEX configuration in the identity provider to return valid certificate URLs in response.
WC_E_DTDPROHIBITED (-1072894385/ 0xc00cee4f)	<p>The XML response, from the WS-Trust endpoint, included a Document Type Definition (DTD). A DTD isn't expected in XML responses, and parsing the response fails if a DTD is included.</p> <p>Note: WS-Trust is required for federated authentication.</p>	<ul style="list-style-type: none"> Fix the configuration in the identity provider to avoid sending a DTD in the XML response. Event 1022 (Microsoft Entra analytics logs) contains the URL that's being accessed that's returning an XML response with a DTD.

Common server error codes

[Expand table](#)

Error code	Reason	Resolution
AADSTS50155: Device authentication failed	<ul style="list-style-type: none"> Microsoft Entra ID is unable to authenticate the device to issue a PRT. Confirm that the device isn't deleted or disabled. For more information about this issue, see Microsoft Entra device management FAQ. 	Follow the instructions for this issue in Microsoft Entra device management FAQ to re-register the device based on the device join type.
AADSTS50034: The user account <code>Account</code> does not exist in the <code>tenant_id</code> directory	Microsoft Entra ID is unable to find the user account in the tenant.	<ul style="list-style-type: none"> Ensure that the user is typing the correct UPN. Ensure that the on-premises user account is being synced with Microsoft Entra ID. Event 1144 (Microsoft Entra analytics logs) contains the UPN provided.

Error code	Reason	Resolution
AADSTS50126: Error validating credentials due to invalid username or password.	<ul style="list-style-type: none"> The username and password entered by the user in the Windows LoginUI are incorrect. If the tenant has password hash sync enabled, the device is hybrid-joined, and the user just changed the password, it's likely that the new password hasn't synced with Microsoft Entra ID. 	To acquire a fresh PRT with the new credentials, wait for the Microsoft Entra password sync to finish.

Common network error codes

[Expand table](#)

Error code	Reason	Resolution
ERROR_WINHTTP_TIMEOUT (12002) ERROR_WINHTTP_NAME_NOT_RESOLVED (12007) ERROR_WINHTTP_CANNOT_CONNECT (12029) ERROR_WINHTTP_CONNECTION_ERROR (12030)	Common general network-related issues.	<ul style="list-style-type: none"> Events 1022 (Microsoft Entra analytics logs) and 1084 (Microsoft Entra operational logs) contain the URL that's being accessed. If the on-premises environment requires an outbound proxy, the IT admin must ensure that the computer account of the device can discover and silently authenticate to the outbound proxy. <p>Get more network error codes.</p>

Step 4: Collect logs

Regular logs

- Go to <https://aka.ms/icesdptool> to automatically download a .cab file containing the Diagnostic tool.
- Run the tool and repro your scenario.
- For Fiddler traces, accept the certificate requests that pop up.
- The wizard prompts you for a password to safeguard your trace files. Provide a password.
- Finally, open the folder where all the collected logs are stored, such as `%LOCALAPPDATA%\ElevatedDiagnostics\numbers`.
- Contact Support with contents of the latest .cab file.

Network traces

① Note

When you're collecting network traces, it's important to *not* use Fiddler during repro.

- Run `netsh trace start scenario=internetClient_dbg capture=yes persistent=yes`.
- Lock and unlock the device. For hybrid-joined devices, wait a minute or more to allow the PRT acquisition task to finish.
- Run `netsh trace stop`.
- Share the `nettrace.cab` file with Support.

Known issues

If you're connected to a mobile hotspot or an external Wi-Fi network and you go to **Settings > Accounts > Access Work or School**, Microsoft Entra hybrid joined devices might show two different accounts, one for Microsoft Entra ID and one for on-premises AD. This UI issue doesn't affect functionality.

Related content

- [Troubleshoot devices by using the dsregcmd command.](#)
- [Go to the Microsoft Error Lookup Tool.](#)

Feedback

Was this page helpful?



[Provide product feedback](#) ↗

Pending devices in Microsoft Entra ID

Article • 10/28/2024

(!) Note

Was this article helpful? Your input is important to us. Please use the **Feedback** button on this page to let us know how well this article worked for you or how we can improve it.

Pending devices are devices that are synced to Microsoft Entra ID from your on-premises Active Directory, but haven't completed registration with the Microsoft Entra device registration service. When the registered state of a device is pending, the device can't complete any authorization or authentication requests, such as requesting a [Primary Refresh token](#) for single sign-on, or applying [device-based Conditional Access policies](#).

(!) Note

The pending state exists only for Microsoft Entra hybrid joined devices.

Why a device might be in a pending state

When you configure a **Microsoft Entra hybrid join** task in the Microsoft Entra Connect Sync for your on-premises devices, the task will sync the device objects to Microsoft Entra ID, and temporarily set the registered state of the devices to "pending" before the device completes the device registration. This is because the device must be added to the Microsoft Entra directory before it can be registered. For more information about the device registration process, see [How it works: Device registration](#).

For more information about how to troubleshoot pending devices, see the following video:
<https://www.youtube-nocookie.com/embed/QBR1c81kaxA>

How a device gets stuck in a pending state

There are two scenarios in which a device can be stuck in a pending state.

Sync a new on-premises domain joined device to Microsoft Entra ID

A new on-premises device can get stuck in a pending state if it can't complete the device registration process. This problem can be caused by several factors, such as that the device

can't connect to the registration service.

To troubleshoot a device registration problem, see:

- [Troubleshooting Microsoft Entra hybrid joined devices](#)
- [Test Device Registration Connectivity](#)

The state of a registered device is changed to pending

This problem can occur in the following scenario:

1. The device object is moved to another organizational unit (OU) that isn't in the sync scope in Microsoft Entra Connect Sync.
2. Microsoft Entra Connect Sync recognizes this change as the device object being deleted in the on-premises Active Directory. Therefore, it deletes the device in Microsoft Entra ID.
3. The device object was moved back to the OU in the sync scope.
4. Microsoft Entra Connect Sync creates a pending device object for this device in Microsoft Entra ID.
5. The device fails to complete the device registration process because it was registered previously.

To fix the problem, unregister the device by running `dsregcmd /leave` at an elevated command prompt, and restart the device. The device will reinitiate the device registration process through the scheduled task. For Windows 10-based devices, the scheduled task is under **Task Scheduler Library > Microsoft > Windows > Workplace Join > Automatic-Device-Join Task**.

Get a list of pending devices

1. The [Microsoft Graph PowerShell SDK](#) must be installed to execute Microsoft Graph PowerShell commands.
2. Use the `Connect-MgGraph` command to sign in to your Microsoft Entra tenant. For more information, see [Get started with the Microsoft Graph PowerShell SDK](#).
3. Count all pending devices:

```
PowerShell
```

```
(Get-MgDevice -All -Filter "TrustType eq 'ServerAd'" | Where-Object{($_.ProfileType -ne "RegisteredDevice") -and (-not $_.AlternativeSecurityIds)}).count
```

You can also save the returned data in a CSV file:

PowerShell

```
Get-MgDevice -All -Filter "TrustType eq 'ServerAd'" | Where-Object{($_.ProfileType -ne "RegisteredDevice") -and (-not $_.AlternativeSecurityIds)} | select-object -Property AccountEnabled, Id, DeviceId, DisplayName, OperatingSystem, OperatingSystemVersion, TrustType | export-csv pendingdevicelist-summary.csv -NoTypeInformation
```

Contact us for help

If you have questions or need help, [create a support request](#), or ask Azure community support. You can also submit product feedback to [Azure feedback community](#).

Troubleshoot devices by using the `dsregcmd` command

Article • 03/03/2025

This article explains how to use the output from the `dsregcmd` command to understand the state of devices in Microsoft Entra ID. Run the `dsregcmd /status` utility as a domain user account.

Device state

This section lists the device join state parameters. The criteria that are required for the device to be in various join states are listed in the following table:

 Expand table

AzureAdJoined	EnterpriseJoined	DomainJoined	Device state
YES	NO	NO	Microsoft Entra joined
NO	NO	YES	Domain Joined
YES	NO	YES	Microsoft Entra hybrid joined
NO	YES	YES	On-premises DRS Joined

! Note

The Workplace Joined (Microsoft Entra registered) state is displayed in the "[User state](#)" section.

- **AzureAdJoined:** Set the state to *YES* if the device is joined to Microsoft Entra ID. Otherwise, set the state to *NO*.
- **EnterpriseJoined:** Set the state to *YES* if the device is joined to an on-premises data replication service (DRS). A device can't be both EnterpriseJoined and AzureAdJoined.
- **DomainJoined:** Set the state to *YES* if the device is joined to a domain (Active Directory).
- **DomainName:** Set the state to the name of the domain if the device is joined to a domain.

Sample device state output

```
+-----+  
| Device State |  
+-----+  
    AzureAdJoined : YES  
    EnterpriseJoined : NO  
    DomainJoined : YES  
    DomainName : HYBRIDADDFS  
+-----+
```

Device details

The state is displayed only when the device is Microsoft Entra joined or Microsoft Entra hybrid joined, not Microsoft Entra registered. This section lists device-identifying details that are stored in Microsoft Entra ID.

- **DeviceId:** The unique ID of the device in the Microsoft Entra tenant.
- **Thumbprint:** The thumbprint of the device certificate.
- **DeviceCertificateValidity:** The validity status of the device certificate.
- **KeyContainerId:** The containerId of the device private key associated with the device certificate.
- **KeyProvider:** The KeyProvider (Hardware/Software) used to store the device private key.
- **TpmProtected:** The state is set to *YES* if the device private key is stored in a hardware Trusted Platform Module (TPM).
- **DeviceAuthStatus:** Performs a check to determine the device's health in Microsoft Entra ID. The health statuses are:
 - *SUCCESS* if the device is present and enabled in Microsoft Entra ID.
 - *FAILED*. *Device is either disabled or deleted* if the device is either disabled or deleted. For more information about this issue, see [Microsoft Entra device management FAQ](#).
 - *FAILED. ERROR* if the test was unable to run. This test requires network connectivity to Microsoft Entra ID under the system context.

 **Note**

The **DeviceAuthStatus** field was added in the Windows 10 May 2021 update (version 21H1).

- **Virtual Desktop:** There are three cases where this line appears.

- NOT SET - VDI device metadata isn't present on the device.
- YES - VDI device metadata is present and dsregcmd outputs associated metadata including:
 - Provider: Name of the VDI vendor.
 - Type: Persistent VDI or non-persistent VDI.
 - User mode: Single user or multi-user.
 - Extensions: Number of key value pairs in optional vendor specific metadata, followed by key value pairs.
- INVALID - The VDI device metadata is present but not set correctly. In this case, dsregcmd outputs the incorrect metadata.

Sample device details output

```
+-----+
| Device Details |
+-----+
DeviceId : 00aa00aa-bb11-cc22-dd33-44ee44ee44ee
Thumbprint : AA11BB22CC33DD44EE55FF66AA77BB88CC99DD00
DeviceCertificateValidity : [ 2019-01-11 21:02:50.000 UTC -- 2029-01-11
21:32:50.000 UTC ]
KeyContainerId : 00aa00aa-bb11-cc22-dd33-44ee44ee44ee
KeyProvider : Microsoft Software Key Storage Provider
TpmProtected : NO
DeviceAuthStatus : SUCCESS
+-----+
```

Tenant details

The tenant details are displayed only when the device is Microsoft Entra joined or Microsoft Entra hybrid joined, not Microsoft Entra registered. This section lists the common tenant details that are displayed when a device is joined to Microsoft Entra ID.

Note

If the mobile device management (MDM) URL fields in this section are empty, it indicates either that the MDM wasn't configured or that the current user isn't in scope of MDM enrollment. Check the Mobility settings in Microsoft Entra ID to review your MDM configuration.

The presence of MDM URLs doesn't guarantee that the device is managed by an MDM. The information is displayed if the tenant has MDM configuration for automatic enrollment even if the device itself isn't managed.

Sample tenant details output

```
+-----+  
| Tenant Details |  
+-----+  
  
    TenantName : HybridADFS  
    TenantId : aaaabbbb-0000-cccc-1111-dddd2222eeee  
        Idp : login.windows.net  
        AuthCodeUrl : https://login.microsoftonline.com/aaaabbbb-  
0000-cccc-1111-dddd2222eeee/oauth2/authorize  
        AccessTokenUrl : https://login.microsoftonline.com/aaaabbbb-  
0000-cccc-1111-dddd2222eeee/oauth2/token  
        MdmUrl : https://enrollment.manage-  
beta.microsoft.com/EnrollmentServer/Discovery.svc  
        MdmTouUrl : https://portal.manage-  
beta.microsoft.com/TermsOfUse.aspx  
        MdmComplianceUrl : https://portal.manage-beta.microsoft.com/?  
portalAction=Compliance  
        SettingsUrl : eyJVx{lots of characters}xxxx==  
        JoinSrvVersion : 1.0  
        JoinSrvUrl :  
https://enterpriseregistration.windows.net/EnrollmentServer/device/  
        JoinSrvId : urn:ms-drs:enterpriseregistration.windows.net  
        KeySrvVersion : 1.0  
        KeySrvUrl :  
https://enterpriseregistration.windows.net/EnrollmentServer/key/  
        KeySrvId : urn:ms-drs:enterpriseregistration.windows.net  
        WebAuthNSrvVersion : 1.0  
        WebAuthNSrvUrl :  
https://enterpriseregistration.windows.net/webauthn/aaaabbbb-0000-cccc-1111-  
dddd2222eeee/  
        WebAuthNSrvId : urn:ms-drs:enterpriseregistration.windows.net  
        DeviceManagementSrvVer : 1.0  
        DeviceManagementSrvUrl :  
https://enterpriseregistration.windows.net/manage/aaaabbbb-0000-cccc-1111-  
dddd2222eeee/  
        DeviceManagementSrvId : urn:ms-drs:enterpriseregistration.windows.net  
+-----+
```

User state

This section lists the statuses of various attributes for users who are currently logged in to the device.

① Note

The command must run in a user context to retrieve a valid status.

- **NgcSet:** Set the state to *YES* if a Windows Hello key is set for the current logged-in user.
- **NgcKeyId:** The ID of the Windows Hello key if one is set for the current logged-in user.
- **CanReset:** Denotes whether the Windows Hello key can be reset by the user.
- **Possible values:** DestructiveOnly, NonDestructiveOnly, DestructiveAndNonDestructive, or Unknown if error.
- **WorkplaceJoined:** Set the state to *YES* if Microsoft Entra registered accounts have been added to the device in the current NTUSER context.
- **WamDefaultSet:** Set the state to *YES* if a Web Account Manager (WAM) default WebAccount is created for the logged-in user. This field could display an error if `dsregcmd /status` is run from an elevated command prompt.
- **WamDefaultAuthority:** Set the state to *organizations* for Microsoft Entra ID.
- **WamDefaultId:** Always use <https://login.microsoft.com> for Microsoft Entra ID.
- **WamDefaultGUID:** The WAM provider's (Microsoft Entra ID / Microsoft account) GUID for the default WAM WebAccount.

Sample user state output

```
+-----+  
| User State |  
+-----+  
  
          NgcSet : YES  
          NgcKeyId : {aaaaaaaa-0b0b-1c1c-2d2d-333333333333}  
          CanReset : DestructiveAndNonDestructive  
          WorkplaceJoined : NO  
          WamDefaultSet : YES  
          WamDefaultAuthority : organizations  
          WamDefaultId : https://login.microsoft.com  
          WamDefaultGUID : { B16898C6-A148-4967-9171-64D755DA8520 }  
(AzureAd)  
+-----+
```

SSO state

You can ignore this section for Microsoft Entra registered devices.

ⓘ Note

The command must run in a user context to retrieve that user's valid status.

- **AzureAdPrt**: Set the state to *YES* if a Primary Refresh Token (PRT) is present on the device for the logged-in user.
- **AzureAdPrtUpdateTime**: Set the state to the time, in Coordinated Universal Time (UTC), when the [PRT was last updated](#).
- **AzureAdPrtExpiryTime**: Set the state to the time, in UTC, when the PRT is going to expire if it isn't renewed.
- **AzureAdPrtAuthority**: The Microsoft Entra authority URL
- **EnterprisePrt**: Set the state to *YES* if the device has a PRT from on-premises Active Directory Federation Services (AD FS). For Microsoft Entra hybrid joined devices, the device could have a PRT from both Microsoft Entra ID and on-premises Active Directory simultaneously. On-premises joined devices have only an Enterprise PRT.
- **EnterprisePrtUpdateTime**: Set the state to the time, in UTC, when the Enterprise PRT was last updated.
- **EnterprisePrtExpiryTime**: Set the state to the time, in UTC, when the PRT is going to expire if it isn't renewed.
- **EnterprisePrtAuthority**: The AD FS authority URL

ⓘ Note

The following PRT diagnostics fields were added in the Windows 10 May 2021 update (version 21H1).

- The diagnostics information that's displayed in the **AzureAdPrt** field is for Microsoft Entra PRT acquisition or refresh, and the diagnostics information that's displayed in the **EnterprisePrt** field is for Enterprise PRT acquisition or refresh.
- The diagnostics information is displayed only if the acquisition or refresh failure happened after the last successful PRT update time (**AzureAdPrtUpdateTime/EnterprisePrtUpdateTime**).
On a shared device, this diagnostics information could be from a different user's login attempt.

- **AcquirePrtDiagnostics:** Set the state to *PRESENT* if the acquired PRT diagnostics information is present in the logs.
 - This field is skipped if no diagnostics information is available.
- **Previous Prt Attempt:** The local time, in UTC, at which the failed PRT attempt occurred.
- **Attempt Status:** The client error code that's returned (HRESULT).
- **User Identity:** The UPN of the user for whom the PRT attempt happened.
- **Credential Type:** The credential used to acquire or refresh the PRT. Common credential types are Password and Next Generation Credential (NGC) (for Windows Hello).
- **Correlation ID:** The correlation ID sent by the server for the failed PRT attempt.
- **Endpoint URI:** The last endpoint accessed before the failure.
- **HTTP Method:** The HTTP method used to access the endpoint.
- **HTTP Error:** WinHttp transport error code. Get other [network error codes](#).
- **HTTP Status:** The HTTP status returned by the endpoint.
- **Server Error Code:** The error code from the server.
- **Server Error Description:** The error message from the server.
- **RefreshPrtDiagnostics:** Set the state to *PRESENT* if the acquired PRT diagnostics information is present in the logs.
 - This field is skipped if no diagnostics information is available.
 - The diagnostics information fields are same as **AcquirePrtDiagnostics**.

① Note

The following Cloud Kerberos diagnostics fields were added in the original release of Windows 11 (version 21H2).

- **OnPremTgt:** Set the state to *YES* if a Cloud Kerberos ticket to access on-premises resources is present on the device for the logged-in user.
- **CloudTgt:** Set the state to *YES* if a Cloud Kerberos ticket to access cloud resources is present on the device for the logged-in user.
- **KerbTopLevelNames:** List of top level Kerberos realm names for Cloud Kerberos.

Sample SSO state output

+-----+	+-----+
SSO State	
+-----+	+-----+
AzureAdPrt : NO	

```
AzureAdPrtAuthority : https://login.microsoftonline.com/aaaabbbb-  
0000-cccc-1111-dddd2222eeee  
AcquirePrtDiagnostics : PRESENT  
Previous Prt Attempt : 2020-07-18 20:10:33.789 UTC  
Attempt Status : 0xc000006d  
User Identity : john@contoso.com  
Credential Type : Password  
Correlation ID : aaaa0000-bb11-2222-33cc-444444dddddd  
Endpoint URI : https://login.microsoftonline.com/aaaabbbb-  
0000-cccc-1111-dddd2222eeee/oauth2/token/  
HTTP Method : POST  
HTTP Error : 0x0  
HTTP status : 400  
Server Error Code : invalid_grant  
Server Error Description : AADSTS50126: Error validating credentials due  
to invalid username or password.  
EnterprisePrt : YES  
EnterprisePrtUpdateTime : 2019-01-24 19:15:33.000 UTC  
EnterprisePrtExpiryTime : 2019-02-07 19:15:33.000 UTC  
EnterprisePrtAuthority :  
https://fs.hybridadfs.nttest.microsoft.com:443/adfs  
OnPremTgt : YES  
CloudTgt : YES  
KerbTopLevelNames :  
.windows.net,.windows.net:1433,.windows.net:3342,.azure.net,.azure.net:1433,  
.azure.net:3342
```

+-----+-----+

Diagnostics data

Pre-join diagnostics

This diagnostics section is displayed only if the device is domain-joined and unable to Microsoft Entra hybrid join.

This section performs various tests to help diagnose join failures. The information includes the: error phase, error code, server request ID, server response HTTP status, and server response error message.

- **User Context:** The context in which the diagnostics are run. Possible values: SYSTEM, UN-ELEVATED User, ELEVATED User.

ⓘ Note

Because the actual join is performed in SYSTEM context, running the diagnostics in SYSTEM context is closest to the actual join scenario. To run

diagnostics in SYSTEM context, the `dsregcmd /status` command must be run from an elevated command prompt.

- **Client Time:** The system time, in UTC.
- **AD Connectivity Test:** This test performs a connectivity test to the domain controller. An error in this test likely results in join errors in the pre-check phase.
- **AD Configuration Test:** This test reads and verifies whether the Service Connection Point (SCP) object is configured properly in the on-premises Active Directory forest. Errors in this test would likely result in join errors in the discover phase with the error code 0x801c001d.
- **DRS Discovery Test:** This test gets the DRS endpoints from discovery metadata endpoint and performs a user realm request. Errors in this test would likely result in join errors in the discover phase.
- **DRS Connectivity Test:** This test performs a basic connectivity test to the DRS endpoint.
- **Token Acquisition Test:** This test tries to get a Microsoft Entra authentication token if the user tenant is federated. Errors in this test would likely result in join errors in the authentication phase. If authentication fails, sync-join is attempted as fallback, unless fallback is explicitly disabled with the following registry key settings:

```
Keyname:  
Computer\HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\C  
DJ  
Value: FallbackToSyncJoin  
Type: REG_DWORD  
Value: 0x0 -> Disabled  
Value: 0x1 -> Enabled  
Default (No Key): Enabled
```

- **Fallback to Sync-Join:** Set the state to *Enabled* if the preceding registry key to prevent fallback to sync-join with authentication failures is *not* present. This option is available from Windows 10 1803 and later.
- **Previous Registration:** The time when the previous join attempt occurred. Only failed join attempts are logged.
- **Error Phase:** The stage of the join in which it was aborted. Possible values are *pre-check*, *discover*, *auth*, and *join*.

- **Client ErrorCode:** The client error code returned (HRESULT).
- **Server ErrorCode:** The server error code displayed if a request was sent to the server and the server responded with an error code.
- **Server Message:** The server message returned along with the error code.
- **Https Status:** The HTTP status returned by the server.
- **Request ID:** The client requestId sent to the server. The request ID is useful to correlate with server-side logs.

Sample pre-join diagnostics output

The following example shows a diagnostics test failing with a discovery error.

```
+-----+
| Diagnostic Data |
+-----+
Diagnostics Reference : www.microsoft.com/aadjerrors
User Context : SYSTEM
Client Time : 2019-01-31 09:25:31.000 UTC
AD Connectivity Test : PASS
AD Configuration Test : PASS
DRS Discovery Test : FAIL [0x801c0021/0x801c000c]
DRS Connectivity Test : SKIPPED
Token acquisition Test : SKIPPED
Fallback to Sync-Join : ENABLED

Previous Registration : 2019-01-31 09:23:30.000 UTC
Error Phase : discover
Client ErrorCode : 0x801c0021

+-----+
```

The following example shows that diagnostics tests are passing but the registration attempt failed with a directory error, which is expected for sync-join. After the Microsoft Entra Connect synchronization job finishes, the device is able to join.

```
+-----+
| Diagnostic Data |
+-----+
Diagnostics Reference : www.microsoft.com/aadjerrors
```

```
User Context : SYSTEM
Client Time : 2019-01-31 09:16:50.000 UTC
AD Connectivity Test : PASS
AD Configuration Test : PASS
DRS Discovery Test : PASS
DRS Connectivity Test : PASS
Token acquisition Test : PASS
Fallback to Sync-Join : ENABLED

Previous Registration : 2019-01-31 09:16:43.000 UTC
Registration Type : sync
Error Phase : join
Client ErrorCode : 0x801c03f2
Server ErrorCode : DirectoryError
Server Message : The device object by the given id (aaaaaaaa-0000-1111-2222-bbbbbbbbbbbb) isn't found.
Https Status : 400
Request Id : 6bff0bd9-820b-484b-ab20-2a4f7b76c58e
```

-----+

Post-join diagnostics

This diagnostics section displays the output of checks performed on a device joined to the cloud.

- **AadRecoveryEnabled:** If the value is *YES*, the keys stored in the device aren't usable, and the device is marked for recovery. The next sign-in will trigger the recovery flow and re-register the device.
- **KeySignTest:** If the value is *PASSED*, the device keys are in good health. If KeySignTest fails, the device is usually marked for recovery. The next sign-in will trigger the recovery flow and re-register the device. For Microsoft Entra hybrid joined devices, the recovery is silent. While the devices are Microsoft Entra joined or Microsoft Entra registered, they prompt for user authentication to recover and re-register the device, if necessary.

 **Note**

The KeySignTest requires elevated privileges.

Sample post-join diagnostics output

```
+-----+
| Diagnostic Data
+-----+

    AadRecoveryEnabled: NO
        KeySignTest : PASSED
+-----+
```

NGC prerequisites check

This diagnostics section performs the prerequisites check for setting up Windows Hello for Business (WHFB).

Note

You might not see NGC prerequisites check details in `dsregcmd /status` if the user configured WHFB successfully.

- **IsDeviceJoined:** Set the state to *YES* if the device is joined to Microsoft Entra ID.
- **IsUserAzureAD:** Set the state to *YES* if the logged-in user is present in Microsoft Entra ID.
- **PolicyEnabled:** Set the state to *YES* if the WHFB policy is enabled on the device.
- **PostLogonEnabled:** Set the state to *YES* if WHFB enrollment is triggered natively by the platform. If the state is set to *NO*, it indicates that Windows Hello for Business enrollment is triggered by a custom mechanism.
- **DeviceEligible:** Set the state to *YES* if the device meets the hardware requirement for enrolling with WHFB.
- **SessionIsNotRemote:** Set the state to *YES* if the current user is logged in directly to the device and not remotely.
- **CertEnrollment:** This setting is specific to WHFB Certificate Trust deployment, indicating the certificate enrollment authority for WHFB. Set the state to *enrollment authority* if the source of the WHFB policy is Group Policy, or set it to *mobile device management* if the source is MDM. If neither source applies, set the state to *none*.
- **AdfsRefreshToken:** This setting is specific to WHFB Certificate Trust deployment and present only if the CertEnrollment state is *enrollment authority*. The setting indicates whether the device has an enterprise PRT for the user.
- **AdfsRalsReady:** This setting is specific to WHFB Certificate Trust deployment and present only if the CertEnrollment state is *enrollment authority*. Set the state to *YES* if AD FS indicates in discovery metadata that it supports WHFB *and* the logon certificate template is available.

- **LogonCertTemplateReady:** This setting is specific to WHFB Certificate Trust deployment and present only if the CertEnrollment state is *enrollment authority*. Set the state to *YES* if the state of the login certificate template is valid and helps troubleshoot the AD FS Registration Authority (RA).
- **PreReqResult:** Provides the result of all WHFB prerequisites evaluation. Set the state to *Will Provision* if WHFB enrollment would be launched as a post-login task when the user signs in next time.

 **Note**

The following Cloud Kerberos diagnostics fields were added in the Windows 10 May 2021 update (version 21H1).

Before Windows 11 version 23H2, the setting **OnPremTGT** was named **CloudTGT**.

- **OnPremTGT:** This setting is specific to Cloud Kerberos trust deployment and present only if the CertEnrollment state is *none*. Set the state to *YES* if the device has a Cloud Kerberos ticket to access on-premises resources. Prior to Windows 11 version 23H2, this setting was named **CloudTGT**.

Sample NGC prerequisites check output

```
+-----+
| Ngc Prerequisite Check |
+-----+
      IsDeviceJoined : YES
      IsUserAzureAD : YES
      PolicyEnabled : YES
      PostLogonEnabled : YES
      DeviceEligible : YES
      SessionIsNotRemote : YES
      CertEnrollment : enrollment authority
      AdfsRefreshToken : YES
      AdfsRaIsReady : YES
      LogonCertTemplateReady : YES ( StateReady )
      PreReqResult : WillProvision
+-----+
```

Next steps

Go to the [Microsoft Error Lookup Tool](#).

Feedback

Was this page helpful?

 Yes

 No

[Provide product feedback ↗](#)

Troubleshooting Microsoft Entra hybrid joined down-level devices

Article • 11/27/2024

This article is applicable only to the following devices:

- Windows 7
- Windows 8.1
- Windows Server 2008 R2
- Windows Server 2012
- Windows Server 2012 R2

For important information about the support of older OS versions, see [Supported versions of Windows client](#) and [Known issues and notifications for Windows 8.1 and Windows Server 2012 R2](#).

For Windows 10 or newer and Windows Server 2016, see [Troubleshooting Microsoft Entra hybrid joined Windows 10 and Windows Server 2016 devices](#).

This article assumes that you [configured Microsoft Entra hybrid joined devices](#) to support the following scenarios:

- Device-based Conditional Access

This article provides you with troubleshooting guidance on how to resolve potential issues.

What you should know:

- Microsoft Entra hybrid join for downlevel Windows devices works differently than it does in Windows 10 or newer. Many customers don't realize that they need AD FS (for federated domains) or Seamless SSO configured (for managed domains).
- Seamless SSO doesn't work in private browsing mode on Firefox and Microsoft Edge browsers. It also doesn't work on Internet Explorer if the browser is running in Enhanced Protected mode or if Enhanced Security Configuration is enabled.
- For customers with federated domains, if the Service Connection Point (SCP) was configured such that it points to the managed domain name (for example, contoso.onmicrosoft.com, instead of contoso.com), then Microsoft Entra hybrid join for downlevel Windows devices doesn't work.
- The same physical device appears multiple times in Microsoft Entra ID when multiple domain users sign-in the downlevel Microsoft Entra hybrid joined devices.

For example, if *Person1* and *Person2* sign-in to a device, a separate registration (DeviceID) is created for each of them in the **USER** info tab.

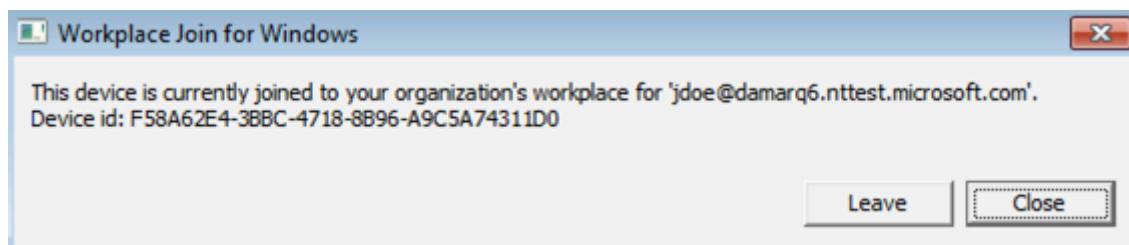
- You can also get multiple entries for a device on the user info tab because of a reinstallation of the operating system or a manual re-registration.
- The initial registration / join of devices is configured to perform an attempt at either sign-in or lock / unlock. There could be 5-minute delay triggered by a task scheduler task.
- Make sure [KB4284842](#) is installed on Windows 7 SP1 or Windows Server 2008 R2 SP1. This update prevents future authentication failures due to customer's access loss to protected keys after changing password.
- Microsoft Entra hybrid join might fail after a user has their UPN changed, breaking the Seamless SSO authentication process. During the join process, you might see that it's still sending the previous UPN to Microsoft Entra ID, unless browser session cookies are cleared or user explicitly signs out and removes old UPN.

Step 1: Retrieve the registration status

To verify the registration status:

1. Sign on with the user account that performed the Microsoft Entra hybrid join.
2. Open the command prompt
3. Type `%programFiles%\Microsoft Workplace Join\autoworkplace.exe" /i`

This command displays a dialog box that provides you with details about the join status.

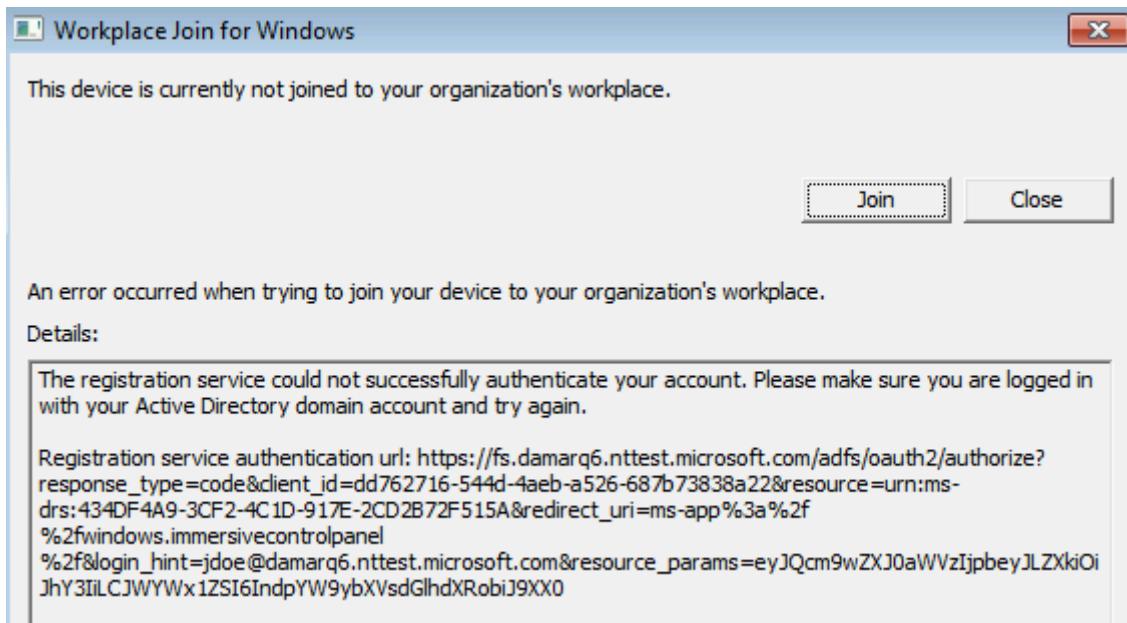


Step 2: Evaluate the Microsoft Entra hybrid join status

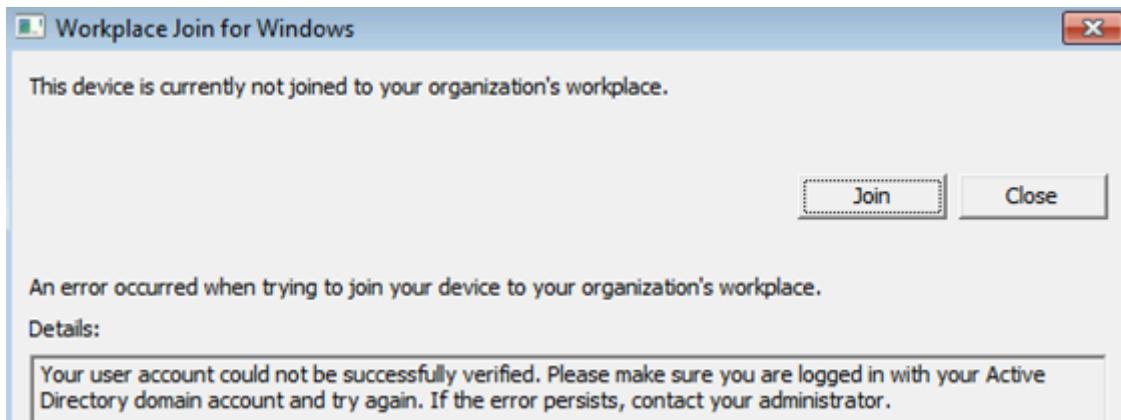
If the device wasn't Microsoft Entra hybrid joined, you can attempt to do Microsoft Entra hybrid join by clicking on the "Join" button. If the attempt to do Microsoft Entra hybrid join fails, the details about the failure are shown.

The most common issues are:

- A misconfigured AD FS or Microsoft Entra ID or Network issues

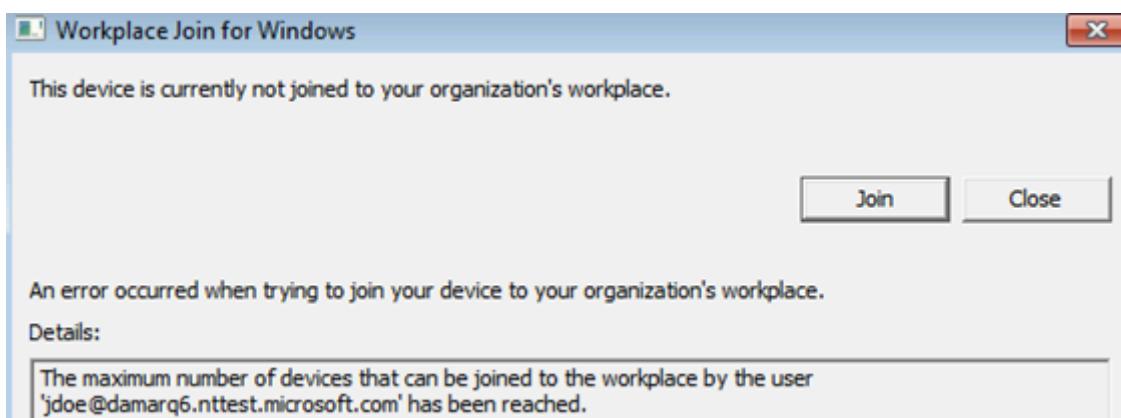


- Autoworkplace.exe is unable to silently authenticate with Microsoft Entra ID or AD FS. This issue could be caused by missing or misconfigured AD FS (for federated domains) or missing or misconfigured Microsoft Entra seamless single sign-on (for managed domains) or network issues.
 - It could be that multifactor authentication (MFA) is enabled/configured for the user and WIAORMULTIAUTHN isn't configured at the AD FS server.
 - Another possibility is that home realm discovery (HRD) page is waiting for user interaction, which prevents **autoworkplace.exe** from silently requesting a token.
 - It could be that AD FS and Microsoft Entra URLs are missing in IE's intranet zone on the client.
 - Network connectivity issues might be preventing **autoworkplace.exe** from reaching AD FS or the Microsoft Entra URLs.
 - **Autoworkplace.exe** requires the client to have direct line of sight from the client to the organization's on-premises AD domain controller, which means that Microsoft Entra hybrid join succeeds only when the client is connected to organization's intranet.
 - If your organization uses Microsoft Entra seamless single sign-on, <https://autologon.microsoftazuread-sso.com> isn't present on the device's IE intranet settings.
 - The internet setting `Do not save encrypted pages to disk` is checked.
- You aren't signed on as a domain user

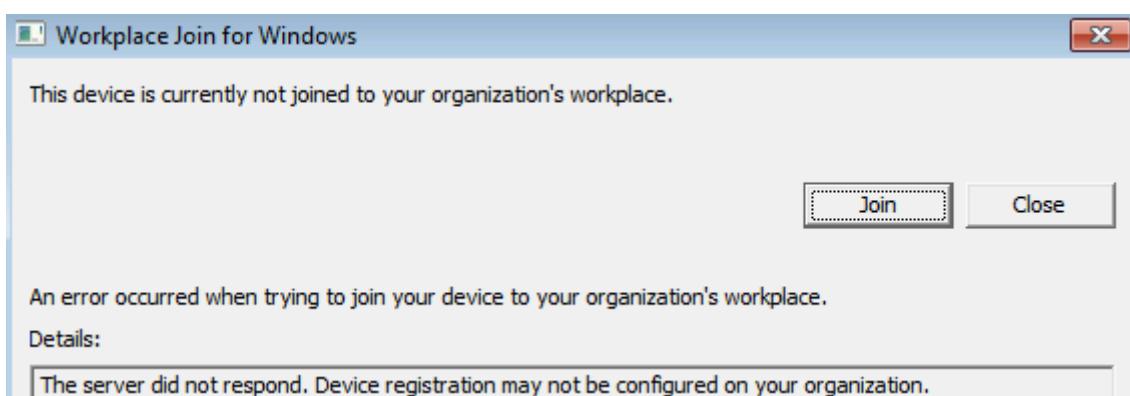


There are a few different reasons why this issue can occur:

- The signed in user isn't a domain user (for example, a local user). Microsoft Entra hybrid join on down-level devices is supported only for domain users.
- The client isn't able to connect to a domain controller.
- A quota is reached



- The service isn't responding



You can also find the status information in the event log under: **Applications and Services Log\Microsoft-Workplace Join**

The most common causes for a failed Microsoft Entra hybrid join are:

- Your computer isn't connected to your organization's internal network or to a VPN with a connection to your on-premises AD domain controller.

- You're logged on to your computer with a local computer account.
- Service configuration issues:
 - The AD FS server isn't configured to support **WIAORMULTIAUTHN**.
 - Your computer's forest has no Service Connection Point object that points to your verified domain name in Microsoft Entra ID
 - Or if your domain is managed, then Seamless SSO wasn't configured or working.
 - A user reached the limit of devices.

Next steps

- [The Microsoft Error Lookup Tool](#)
-

Feedback

Was this page helpful?



[Provide product feedback ↗](#)

Windows Local Administrator Password Solution in Microsoft Entra ID

Article • 01/16/2024

Every Windows device comes with a built-in local administrator account that you must secure and protect to mitigate any Pass-the-Hash (PtH) and lateral traversal attacks. Many customers have been using our standalone, on-premises [Local Administrator Password Solution \(LAPS\)](#) product for local administrator password management of their domain joined Windows machines. With Microsoft Entra ID support for Windows LAPS, we're providing a consistent experience for both Microsoft Entra joined and Microsoft Entra hybrid joined devices.

Microsoft Entra ID support for LAPS includes the following capabilities:

- **Enabling Windows LAPS with Microsoft Entra ID** - Enable a tenant wide policy and a client-side policy to back up local administrator password to Microsoft Entra ID.
- **Local administrator password management** - Configure client-side policies to set account name, password age, length, complexity, manual password reset and so on.
- **Recovering local administrator password** - Use API/Portal experiences for local administrator password recovery.
- **Enumerating all Windows LAPS enabled devices** - Use API/Portal experiences to enumerate all Windows devices in Microsoft Entra ID enabled with Windows LAPS.
- **Authorization of local administrator password recovery** - Use role based access control (RBAC) policies with custom roles and administrative units.
- **Auditing local administrator password update and recovery** - Use audit logs API/Portal experiences to monitor password update and recovery events.
- **Conditional Access policies for local administrator password recovery** - Configure Conditional Access policies on directory roles that have the authorization of password recovery.

Note

Windows LAPS with Microsoft Entra ID is not supported for Windows devices that are [Microsoft Entra registered](#).

Local Administrator Password Solution isn't supported on non-Windows platforms.

To learn about Windows LAPS in more detail, start with the following articles in the Windows documentation:

- [What is Windows LAPS?](#) – Introduction to Windows LAPS and the Windows LAPS documentation set.
- [Windows LAPS CSP](#) – View the full details for LAPS settings and options. Intune policy for LAPS uses these settings to configure the LAPS CSP on devices.
- [Microsoft Intune support for Windows LAPS](#)
- [Windows LAPS architecture](#)

Requirements

Supported Azure regions and Windows distributions

This feature is now available in the following Azure clouds:

- Azure Global
- Azure Government
- Microsoft Azure operated by 21Vianet

Operating system updates

This feature is now available on the following Windows OS platforms with the specified update or later installed:

- Windows 11 22H2 - April 11 2023 Update ↗
- Windows 11 21H2 - April 11 2023 Update ↗
- Windows 10 20H2, 21H2 and 22H2 - April 11 2023 Update ↗
- Windows Server 2022 - April 11 2023 Update ↗
- Windows Server 2019 - April 11 2023 Update ↗

Join types

LAPS is supported on Microsoft Entra joined or Microsoft Entra hybrid joined devices only. Microsoft Entra registered devices aren't supported.

License requirements

LAPS is available to all customers with Microsoft Entra ID Free or higher licenses. Other related features like administrative units, custom roles, Conditional Access, and Intune have other licensing requirements.

Required roles or permission

Other than the built-in Microsoft Entra roles of Cloud Device Administrator, Intune Administrator, and Global Administrator that are granted `device.LocalCredentials.Read.All`, you can use [Microsoft Entra custom roles](#) or administrative units to authorize local administrator password recovery. For example,

- Custom roles must be assigned the `microsoft.directory/deviceLocalCredentials/password/read` permission to authorize local administrator password recovery. You can create a custom role and grant permissions using the [Microsoft Entra admin center](#) ↗, [Microsoft Graph API](#) or [PowerShell](#). Once you create a custom role, you can assign it to users.
- You can also create a Microsoft Entra ID [administrative unit](#), add devices, and assign the Cloud Device Administrator role scoped to the administrative unit to authorize local administrator password recovery.

Enabling Windows LAPS with Microsoft Entra ID

To enable Windows LAPS with Microsoft Entra ID, you must take actions in Microsoft Entra ID and the devices you wish to manage. We recommend organizations [manage Windows LAPS using Microsoft Intune](#). If your devices are Microsoft Entra joined but not using or don't support Microsoft Intune, you can deploy Windows LAPS for Microsoft Entra ID manually. For more information, see the article [Configure Windows LAPS policy settings](#).

1. Sign in to the [Microsoft Entra admin center](#) ↗ as at least a [Cloud Device Administrator](#).
2. Browse to **Identity > Devices > Overview > Device settings**
3. Select **Yes** for the **Enable Local Administrator Password Solution (LAPS)** setting, then select **Save**. You might also use the Microsoft Graph API [Update deviceRegistrationPolicy](#) to complete this task.
4. Configure a client-side policy and set the **BackUpDirectory** to be Microsoft Entra ID.
 - If you're using Microsoft Intune to manage client side policies, see [Manage Windows LAPS using Microsoft Intune](#)
 - If you're using Group Policy Objects (GPO) to manage client side policies, see [Windows LAPS Group Policy](#)

Recovering local administrator password and password metadata

To view the local administrator password for a Windows device joined to Microsoft Entra ID, you must be granted the `microsoft.directory/deviceLocalCredentials/password/read` action.

To view the local administrator password metadata for a Windows device joined to Microsoft Entra ID, you must be granted the `microsoft.directory/deviceLocalCredentials/standard/read` action.

The following built-in roles are granted these actions by default:

[] Expand table

Built-in role	<code>microsoft.directory/deviceLocalCredentials/standard/read</code> and <code>microsoft.directory/deviceLocalCredentials/password/read</code>	<code>microsoft.directory/deviceLocalCredentials/standard/read</code>
Global Administrator	Yes	Yes
Cloud Device Administrator	Yes	Yes
Intune Service Administrator	Yes	Yes
Global Reader	No	Yes
Helpdesk Administrator	No	Yes
Security Administrator	No	Yes
Security Reader	No	Yes

Any roles not listed are granted neither action.

You can also use Microsoft Graph API [Get deviceLocalCredentialInfo](#) to recover local administrative password. If you use the Microsoft Graph API, the password returned is in Base64 encoded value that you need to decode before using it.

List all Windows LAPS enable devices

To list all Windows LAPS enabled devices, you can browse to Identity > Devices > Overview > Local administrator password recovery or use the Microsoft Graph API.

Auditing local administrator password update and recovery

To view audit events, you can browse to Identity > Devices > Overview > Audit logs, then use the Activity filter and search for Update device local administrator password or Recover device local administrator password to view the audit events.

Conditional Access policies for local administrator password recovery

Conditional Access policies can be scoped to the built-in roles like Cloud Device Administrator, Intune Administrator, and Global Administrator to protect access to recover local administrator passwords. You can find an example of a policy that requires multifactor authentication in the article, [Common Conditional Access policy: Require MFA for administrators](#).

! Note

Other role types including administrative unit-scoped roles and custom roles aren't supported

Frequently asked questions

Is Windows LAPS with Microsoft Entra management configuration supported using Group Policy Objects (GPO)?

Yes, for [Microsoft Entra hybrid joined](#) devices only. See see [Windows LAPS Group Policy](#).

Is Windows LAPS with Microsoft Entra management configuration supported using MDM?

Yes, for [Microsoft Entra join/Microsoft Entra hybrid join \(co-managed\)](#) devices. Customers can use [Microsoft Intune](#) or any other third-party MDM of their choice.

What happens when a device is deleted in Microsoft Entra ID?

When a device is deleted in Microsoft Entra ID, the LAPS credential that was tied to that device is lost, and the password that is stored in Microsoft Entra ID is lost. Unless you have a custom workflow to retrieve LAPS passwords and store them externally, there's no method in Microsoft Entra ID to recover the LAPS managed password for a deleted device.

What roles are needed to recover LAPS passwords?

The following built-in roles Microsoft Entra roles have permission to recover LAPS passwords: Global Administrator, Cloud Device Administrator, and Intune Administrator.

What roles are needed to read LAPS metadata?

The following built-in roles are supported to view metadata about LAPS including the device name, last password rotation, and next password rotation: Global Administrator, Cloud Device Administrator, Intune Administrator, Helpdesk Administrator, Security Reader, Security Administrator, and Global Reader.

Are custom roles supported?

Yes. If you have Microsoft Entra ID P1 or P2, you can create a custom role with the following RBAC permissions:

- To read LAPS metadata: `microsoft.directory/deviceLocalCredentials/standard/read`
- To read LAPS passwords: `microsoft.directory/deviceLocalCredentials/password/read`

What happens when the local administrator account specified by policy is changed?

Because Windows LAPS can only manage one local admin account on a device at a time, the original account is no longer managed by LAPS policy. If policy has the device back up that account, the new account is backed up and details about the previous account are no longer available from within the Intune admin center or from the Directory specified to store the account information.

Next steps

- [Choosing a device identity](#)
- [Microsoft Intune support for Windows LAPS](#)

- [Create policy for LAPS](#)
- [View reports for LAPS](#)
- [Account protection policy for endpoint security in Intune](#)

Manage device identities using the Microsoft Entra admin center

Article • 02/11/2025

Microsoft Entra ID provides a central place to manage device identities and monitor related event information.

The screenshot shows the Microsoft Entra admin center interface. The left sidebar is collapsed, showing categories like Home, Favorites, Identity, Users, Groups, Devices, Applications, Protection, Identity governance, External Identities, and more. The main content area is titled 'Devices | Overview' for 'Contoso - Microsoft Entra ID'. It features a search bar at the top right. Below the search bar are three sections: 'Alerts' (Stale devices: 0, Noncompliant devices: 0), 'My Feed' (Total number of devices: 0, Preview Features: 2 total), and 'Feature Highlights'. A magnifying glass icon is in the bottom right corner.

You can access the devices overview by completing these steps:

1. Sign in to the [Microsoft Entra admin center](#) as a user with at least [default user permissions](#).
2. Go to **Identity > Devices > Overview**.

In the devices overview, you can view the number of total devices, stale devices, noncompliant devices, and unmanaged devices. It provides links to Intune, Conditional Access, BitLocker keys, and basic monitoring. Other features like Conditional Access and Microsoft Intune require additional role assignments

Device counts on the overview page don't update in real time. Changes should be reflected every few hours.

From there, you can go to **All devices** to:

- Identify devices, including:
 - Devices joined or registered in Microsoft Entra ID.
 - Devices deployed via [Windows Autopilot](#).

- Printers that use [Universal Print](#).
- Complete device identity management tasks like enable, disable, delete, and manage.
 - The management options for [Printers](#) and [Windows Autopilot](#) are limited in Microsoft Entra ID. These devices must be managed from their respective admin interfaces.
- Configure your device identity settings.
- Enable or disable enterprise state roaming.
- Review device-related audit logs.
- Download devices.

The screenshot shows the Microsoft Entra ID interface with the 'Devices' section selected. On the left, there's a navigation menu with categories like Favorites, Identity, Users, Groups, Devices, Applications, Protection, Identity governance, External Identities, and more. The 'Devices' section is expanded, showing sub-options for All devices, BitLocker keys, Audit logs, Bulk operation results, Troubleshooting + Support, New support request, and Diagnose and solve problems. The main area displays a table of devices found, with 11 entries listed. The columns are: Name, Enabled, OS, Version, Join type, Owner, MDM, and Security s. The table includes rows for various devices named ContosoSP, ContosoClient, ContosoMIM, ContosoStudio, CONTOSO-FERNS, Contoso-TAC, Contoso-SEA, CONTOSODC, contoso-nd1, Contoso-BE, and CONTOSO-6166. Most devices are marked as 'Enabled' and 'Yes' for OS. The 'Join type' column shows 'Microsoft Entra joined' for most devices, except for one which is 'None'. The 'Owner' column is mostly 'None', except for one entry under Microsoft Intune. The 'MDM' column has 'N/A' or 'Microsoft' listed. The 'Security s' column also has 'N/A' or 'Microsoft' listed.

Name	Enabled	OS	Version	Join type	Owner	MDM	Security s
Name 11	<input type="checkbox"/>						
ContosoSP	<input checked="" type="checkbox"/>	Yes	Windows...	10.0.17763.5576			N/A
ContosoClient	<input checked="" type="checkbox"/>	Yes	Windows	10.0.22000.2416			Microsoft Intune
ContosoMIM	<input checked="" type="checkbox"/>	Yes	Window...	10.0.17763.5458			Microsoft
ContosoStudio	<input checked="" type="checkbox"/>	Yes	Windows	10.0.22631.3296	Microsoft Entra joined		Microsoft Configuration
CONTOSO-FERNS	<input checked="" type="checkbox"/>	Yes	Windows	10.0.19044.3086			N/A
Contoso-TAC	<input checked="" type="checkbox"/>	Yes	Windows	10.0.27554.1000	Microsoft Entra joined		Microsoft Configuration
Contoso-SEA	<input checked="" type="checkbox"/>	Yes	Windows	10.0.27554.1000	Microsoft Entra joined		N/A
CONTOSODC	<input checked="" type="checkbox"/>	Yes	Window...	10.0.17763.5576			N/A
contoso-nd1	<input checked="" type="checkbox"/>	Yes	Windows	10.0.20348.2031	Microsoft Entra regist...		N/A
Contoso-BE	<input checked="" type="checkbox"/>	Yes	Windows	10.0.27554.1000	Microsoft Entra joined		Microsoft Configuration
CONTOSO-6166	<input checked="" type="checkbox"/>	Yes	Windows	10.0.22631.3296	Microsoft Entra joined		N/A

Tip

- Microsoft Entra hybrid joined Windows 10 or newer devices don't have an owner unless the primary user is set in Microsoft Intune. If you're looking for a device by owner and don't find it, search by the device ID.
- If you see a device that's **Microsoft Entra hybrid joined** with a state of **Pending** in the **Registered** column, the device has been synchronized from Microsoft Entra Connect and is waiting to complete registration from the client. See [How to plan your Microsoft Entra hybrid join implementation](#). For more information, see [Device management frequently asked questions](#).
- For some iOS devices, device names that contain apostrophes can use different characters that look like apostrophes. So searching for such devices

is a little tricky. If don't see correct search results, be sure the search string contains the matching apostrophe character.

Manage an Intune device

If you have rights to manage devices in Intune, you can manage devices for which mobile device management is listed as **Microsoft Intune**. If the device isn't enrolled with Microsoft Intune, the **Manage** option isn't available.

Enable or disable a Microsoft Entra device

There are two ways to enable or disable devices:

- The toolbar on the **All devices** page, after you select one or more devices.
- The toolbar, after you drill down for a specific device.

Important

- You must be a Intune Administrator or Cloud Device Administrator to enable or disable a device.
- Disabling a device prevents it from authenticating via Microsoft Entra ID. This prevents it from accessing your Microsoft Entra resources that are protected by device-based Conditional Access and from using Windows Hello for Business credentials.
- Disabling a device revokes the Primary Refresh Token (PRT) and any refresh tokens on the device.
- Printers can't be enabled or disabled in Microsoft Entra ID.

Delete a Microsoft Entra device

There are two ways to delete a device:

- The toolbar on the **All devices** page, after you select one or more devices.
- The toolbar, after you drill down for a specific device.

Important

- You must be a Cloud Device Administrator, Intune Administrator or Windows 365 Administrator to delete a device.
- Printers can't be deleted before they are deleted from Universal Print.
- Windows Autopilot devices can't be deleted before they are deleted from Intune.
- Deleting a device:
 - Prevents it from accessing your Microsoft Entra resources.
 - Removes all details attached to the device. For example, BitLocker keys for Windows devices.
 - Is a nonrecoverable activity. We don't recommend it unless it's required.

If a device is managed in another management authority, like Microsoft Intune, be sure it's wiped or retired before you delete it. See [How to manage stale devices](#) before you delete a device.

View or copy a device ID

You can use a device ID to verify the device ID details on the device or to troubleshoot via PowerShell. To access the copy option, select the device.

[Home](#) > [Devices | All devices](#) >

 **TEST-DEVICE** | Properties [...](#)

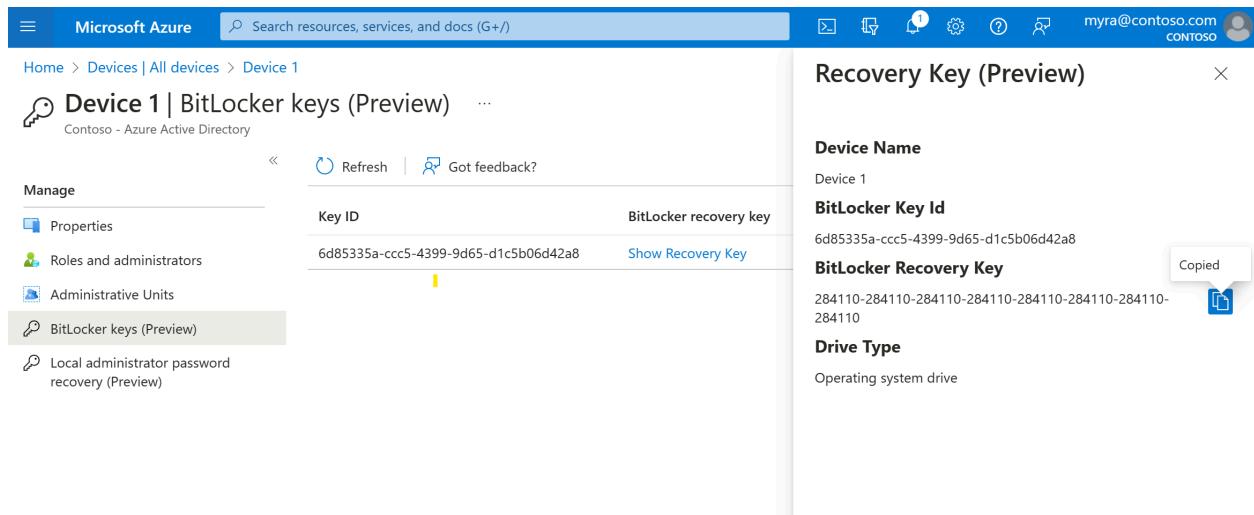
Microsoft - Microsoft Entra ID

Manage

Properties	Name	TEST-DEVICE	Copy to clipboard
Roles and administrators	Device ID	00x00000-0xxx-00x0-x000-000x00xxx000	Copy
Administrative Units	Object ID	00x00000-0xxx-00x0-x000-000x00xxx000	Copy
	Enabled	Yes	
	OS	Windows	
	Version	10.0.23607.1000	
	Join type		
	Owner	None	
	User principal name	None	
	MDM	Microsoft Configuration Manager	
	Compliant	N/A	
	Registered	N/A	
	Activity	N/A	
	Groups		
Extension attributes		No extension attributes	

View or copy BitLocker keys

You can view and copy BitLocker keys to allow users to recover encrypted drives. These keys are available only for Windows devices that are encrypted and store their keys in Microsoft Entra ID. You can find these keys when you view a device's details by selecting **Show Recovery Key**. Selecting **Show Recovery Key** generates an audit log entry, which you can find in the **KeyManagement** category.



The screenshot shows the Microsoft Azure portal interface. At the top, there is a navigation bar with the Microsoft Azure logo, a search bar, and user information (myra@contoso.com, CONTOSO). Below the navigation bar, the URL is Home > Devices | All devices > Device 1. The main content area has a title "Device 1 | BitLocker keys (Preview)" and a subtitle "Contoso - Azure Active Directory". On the left, there is a sidebar titled "Manage" with options: Properties, Roles and administrators, Administrative Units, BitLocker keys (Preview) (which is selected and highlighted in grey), and Local administrator password recovery (Preview). The main pane displays a table with two columns: "Key ID" and "BitLocker recovery key". The first row shows "6d85335a-ccc5-4399-9d65-d1c5b06d42a8" and a "Show Recovery Key" link. To the right of the table, there is a "Recovery Key (Preview)" section with fields for "Device Name" (Device 1), "BitLocker Key Id" (6d85335a-ccc5-4399-9d65-d1c5b06d42a8), "BitLocker Recovery Key" (284110-284110-284110-284110-284110-284110), and "Drive Type" (Operating system drive). A "Copied" message with a clipboard icon is visible next to the BitLocker Recovery Key field.

To view or copy BitLocker keys, you need to be the owner of the device or have one of these roles:

- Cloud Device Administrator
- Helpdesk Administrator
- Intune Administrator
- Security Administrator
- Security Reader

ⓘ Note

When devices that utilize [Windows Autopilot](#) are reused, and there is a new device owner, that new device owner must contact an administrator to acquire the BitLocker recovery key for that device. Custom role or administrative unit scoped administrators will continue to have access to BitLocker recovery keys for those devices that have undergone device ownership changes, unless the new device owner belongs to a custom role or administrative unit scope. In such an instance, the user will need to contact other scoped administrator for the recovery keys. For more information, see the article [Find the primary user of an Intune device](#).

View and filter your devices

You can filter the device list by these attributes:

- Enabled state
- Compliant state
- Join type (Microsoft Entra joined, Microsoft Entra hybrid joined, Microsoft Entra registered)
- Activity timestamp
- OS type and OS version
 - Windows is displayed for Windows 11 and Windows 10 devices (with KB5006738).
 - Windows Server is displayed for [supported versions managed with Microsoft Defender for Endpoint](#).
- Device type (printer, secure VM, shared device, registered device)
- MDM
- Autopilot
- Extension attributes
- Administrative unit
- Owner

Download devices

Cloud Device Administrators and Intune Administrators can use the **Download devices** option to export a CSV file that lists devices. You can apply filters to determine which devices to list. If you don't apply any filters, all devices are listed. An export task might run for as long as an hour, depending on your selections. If the export task exceeds 1 hour, it fails, and no file is output.

The exported list includes these device identity attributes:

```
displayName,accountEnabled,operatingSystem,operatingSystemVersion,joinType  
(trustType),registeredOwners,userNames,mdmDisplayName,isCompliant,registrationTime,  
approximateLastSignInDateTime,deviceId,isManaged,objectId,profileType,systemLabels,  
model
```

The following filters can be applied for the export task:

- Enabled state
- Compliant state
- Join type
- Activity timestamp
- OS type
- Device type

Configure device settings

If you want to manage device identities by using the Microsoft Entra admin center, the devices need to be either [registered or joined](#) to Microsoft Entra ID. As an administrator, you can control the process of registering and joining devices by configuring the following device settings.

You must be assigned one of the following roles to read or modify device settings:

- [Cloud Device Administrator](#) (read and modify)
- [Intune Administrator](#) (read only)
- [Windows 365 Administrator](#) (read only)

The screenshot shows the Microsoft Entra admin center interface. The left sidebar has a 'Devices' category expanded, with 'Device settings' selected. The main content area is titled 'Microsoft Entra join and registration settings'. It includes sections for 'Users may join devices to Microsoft Entra' (with 'All' selected), 'Users may register their devices with Microsoft Entra' (with 'None' selected), and 'Require Multifactor Authentication to register or join devices with Microsoft Entra' (with 'Yes' selected). A note states: '⚠️ We recommend that you require Multifactor Authentication to register or join devices with Microsoft Entra using Conditional Access. Set this device setting to No if you require Multifactor Authentication using Conditional Access.' Below this are sections for 'Local administrator settings' and 'Activity' (Audit logs and Bulk operation results). The right side of the screen shows user details and a 'Save' button.

- **Users may join devices to Microsoft Entra ID:** This setting enables you to select the users who can register their devices as Microsoft Entra joined devices. The default is All.

! Note

The **Users may join devices to Microsoft Entra ID** setting is applicable only to Microsoft Entra join on Windows 10 or newer. This setting doesn't apply to Microsoft Entra hybrid joined devices, [Microsoft Entra joined VMs in Azure](#), or Microsoft Entra joined devices that use [Windows Autopilot self-deployment mode](#) because these methods work in a userless context.

- **Users may register their devices with Microsoft Entra ID:** You need to configure this setting to allow users to register Windows 10 or newer personal, iOS, Android, and macOS devices with Microsoft Entra ID. If you select **None**, devices aren't allowed to register with Microsoft Entra ID. Enrollment with Microsoft Intune or mobile device management for Microsoft 365 requires registration. If you've configured either of these services, **ALL** is selected, and **NONE** is unavailable.
- **Require multifactor authentication to register or join devices with Microsoft Entra ID:**
 - We recommend organizations use the [Register or join devices user action](#) in Conditional Access to enforce multifactor authentication. You must configure this toggle to **No** if you use a [Conditional Access policy to require multifactor authentication](#).
 - This setting allows you to specify whether users are required to provide another authentication factor to join or register their devices to Microsoft Entra ID. The default is **No**. We recommend that you require multifactor authentication when a device is registered or joined. Before you enable multifactor authentication for this service, you must ensure that multifactor authentication is configured for users that register their devices. For more information on Microsoft Entra multifactor authentication services, see [getting started with Microsoft Entra multifactor authentication](#). This setting might not work with third-party identity providers.

 **Note**

The **Require multifactor authentication to register or join devices with Microsoft Entra ID** setting applies to devices that are either Microsoft Entra joined (with some exceptions) or Microsoft Entra registered. This setting doesn't apply to Microsoft Entra hybrid joined devices, [Microsoft Entra joined VMs in Azure](#), or Microsoft Entra joined devices that use [Windows Autopilot self-deployment mode](#).

- **Maximum number of devices:** This setting enables you to select the maximum number of Microsoft Entra joined or Microsoft Entra registered devices that a user can have in Microsoft Entra ID. If users reach this limit, they can't add more devices until one or more of the existing devices are removed. The default value is **50**. You can increase the value up to 100. If you enter a value above 100, Microsoft Entra ID sets it to 100. You can also use **Unlimited** to enforce no limit other than existing quota limits.

 **Note**

The **Maximum number of devices** setting applies to devices that are either Microsoft Entra joined or Microsoft Entra registered. This setting doesn't apply to Microsoft Entra hybrid joined devices.

- **Manage Additional local administrators on Microsoft Entra joined devices:** This setting allows you to select the users who are granted local administrator rights on a device. These users are added to the Device Administrators role in Microsoft Entra ID.
- **Enable Microsoft Entra Local Administrator Password Solution (LAPS) (preview):** LAPS is the management of local account passwords on Windows devices. LAPS provides a solution to securely manage and retrieve the built-in local admin password. With cloud version of LAPS, customers can enable storing and rotation of local admin passwords for both Microsoft Entra ID and Microsoft Entra hybrid join devices. To learn how to manage LAPS in Microsoft Entra ID, see [the overview article](#).
- **Restrict non-admin users from recovering the BitLocker key(s) for their owned devices:** Admins can block self-service BitLocker key access to the registered owner of the device. Default users without the BitLocker read permission are unable to view or copy their BitLocker key(s) for their owned devices. You must be at least a [Privileged Role Administrator](#) to update this setting.
- **Enterprise State Roaming:** For information about this setting, see [the overview article](#).

Audit logs

Device activities are visible in the activity logs. These logs include activities triggered by the device registration service and by users:

- Device creation and adding owners/users on the device
- Changes to device settings
- Device operations like deleting or updating a device
- Bulk operations like downloading all devices

 **Note**

When performing bulk operations, such as import or create, you can encounter a problem if the bulk operation doesn't complete within the hour. To work around this issue, we recommend splitting the number of records processed per batch. For example, before starting an export you could limit the result set by filtering on a group type or user name to reduce the size of the results. By refining your filters, essentially you limit the data returned by the bulk operation. For more information, see [Bulk operations service limitations](#).

The entry point to the auditing data is **Audit logs** in the **Activity** section of the **Devices** page.

The audit log has a default list view that shows:

- The date and time of the occurrence.
- The targets.
- The initiator/actor of an activity.
- The activity.

DATE	TARGET(S)	INITIATED BY (ACTOR)	ACTIVITY
8/9/2017, 8:23:52 AM	Device : [REDACTED]	Windows.Azure.DeviceRegistration	Add device
8/9/2017, 8:23:52 AM	User : [REDACTED].onmicrosoft.com, ...	Windows.Azure.DeviceRegistration	Add registered owner to device
8/9/2017, 8:23:52 AM	User : [REDACTED].onmicrosoft.com, ...	Windows.Azure.DeviceRegistration	Add registered users to device
8/9/2017, 8:17:14 AM	Device : [REDACTED] iPhone	Windows.Azure.DeviceRegistration	Delete device

You can customize the list view by selecting **Columns** in the toolbar:



To reduce the reported data to a level that works for you, you can filter it by using these fields:

- Category
- Activity Resource Type
- Activity
- Date Range
- Target
- Initiated By (Actor)

You can also search for specific entries.

Category Core Directory	Activity Resource Type Device	Activity All
Date Range 1 Month	Target Enter target name or upn	Initiated By (Actor) Enter actor name or upn
Apply		
<input type="text"/> Search to filter items...		

Next steps

- How to manage stale devices in Microsoft Entra ID
- Troubleshoot pending device state

Feedback

Was this page helpful?

 Yes

 No

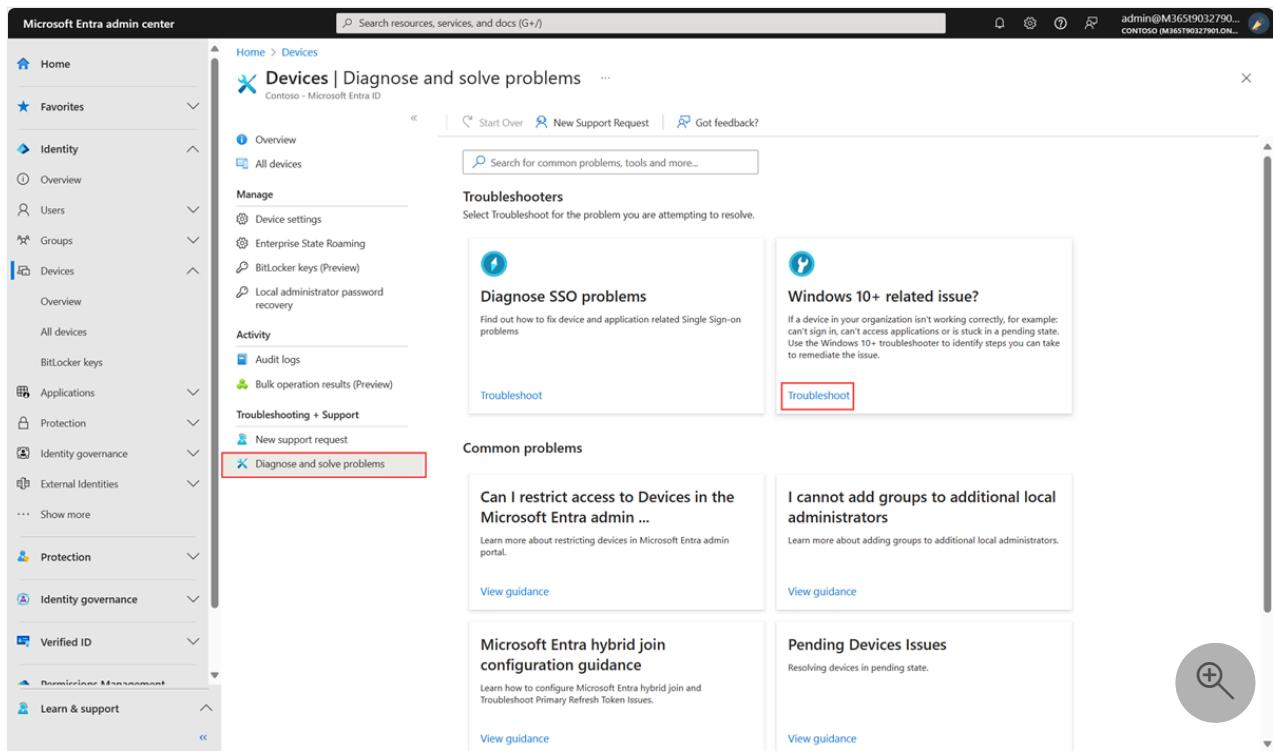
Provide product feedback ↗

Troubleshooting Windows devices in Microsoft Entra ID

Article • 04/25/2025

If you have a Windows 11 or Windows 10 device that isn't working with Microsoft Entra ID correctly, start your troubleshooting here.

1. Sign in to the [Microsoft Entra admin center](#) as at least a **Reports Reader**.
2. Browse to **Entra ID > Devices > All devices > Diagnose and solve problems**.
3. Select **Troubleshoot** under the **Windows 10+ related issue troubleshooter**.



The screenshot shows the Microsoft Entra admin center interface. The left sidebar is collapsed, showing sections like Home, Favorites, Identity, Devices, Applications, Protection, and more. The main content area is titled 'Devices | Diagnose and solve problems'. It includes a search bar, navigation links for Overview, All devices, Manage, Activity, Troubleshooting + Support, and New support request. A red box highlights the 'Diagnose and solve problems' link in the Troubleshooting + Support section. Below this, there's a 'Troubleshooters' section with two items: 'Diagnose SSO problems' and 'Windows 10+ related issue?'. A red box highlights the 'Troubleshoot' button next to the Windows 10+ related issue. Under 'Common problems', there are four items: 'Can I restrict access to Devices in the Microsoft Entra admin ...', 'I cannot add groups to additional local administrators', 'Microsoft Entra hybrid join configuration guidance', and 'Pending Devices Issues'. Each item has a 'View guidance' link. A magnifying glass icon is in the bottom right corner.

4. Select **instructions** and follow the steps to download, run, and collect the required logs for the troubleshooter to analyze.
5. Return to the Microsoft Entra admin center when you collect and zip the `authlogs` folder and contents.

6. Select **Browse** and choose the zip file you wish to upload.

The screenshot shows the Microsoft Entra admin center interface. On the left, there's a navigation sidebar with various categories like Home, Favorites, Identity, Overview, Users, Groups, Devices, Applications, Protection, Identity governance, External Identities, and more. The 'Devices' section is currently selected. The main content area is titled 'Devices | Diagnose and solve problems' for 'Contoso - Microsoft Entra ID'. It includes sections for Overview, All devices, Manage (Device settings, Enterprise State Roaming, BitLocker keys (Preview), Local administrator password recovery), Activity (Audit logs, Bulk operation results (Preview)), Troubleshooting + Support (New support request), and Diagnose and solve problems (which is highlighted with a grey background). Below these sections, there's a form with a 'Select file' input field and a 'Browse' button, both of which are enclosed in a red rectangular box. At the top right, there's a search bar and some user information: 'admin@M365f9032790... CONTOSO (M365f90327901.ON...)'.

The troubleshooter will review the contents of the file you uploaded and provide suggested next steps. These next steps might include links to documentation or contacting support for further assistance.

Next steps

- [Troubleshoot devices by using the dsregcmd command](#)
- [Troubleshoot Microsoft Entra hybrid joined devices](#)
- [Troubleshoot pending device state](#)
- [MDM enrollment of Windows 10-based devices](#)
- [Troubleshooting Windows device enrollment errors in Intune](#)

Troubleshoot primary refresh token issues on Windows devices

Article • 10/23/2023

This article discusses how to troubleshoot issues that involve the [primary refresh token](#) (PRT) when you authenticate on a Microsoft Entra joined Windows device by using your Microsoft Entra credentials.

On devices that are joined to Microsoft Entra ID or hybrid Microsoft Entra ID, the main component of authentication is the PRT. You obtain this token by signing in to Windows 10 by using Microsoft Entra credentials on a Microsoft Entra joined device for the first time. The PRT is cached on that device. For subsequent sign-ins, the cached token is used to let you use the desktop.

As part of the process of locking and unlocking the device or signing in again to Windows, a background network authentication attempt is made one time every four hours to refresh the PRT. If problems occur that prevent refreshing the token, the PRT eventually expires. Expiration affects single sign-on (SSO) to Microsoft Entra resources. It also causes sign-in prompts to be shown.

If you suspect that a PRT problem exists, we recommend that you first collect Microsoft Entra logs, and follow the steps that are outlined in the troubleshooting checklist. Do this for any Microsoft Entra client issue first, ideally within a repro session. Complete this process before you file a support request.

Troubleshooting checklist

Step 1: Get the status of the primary refresh token

1. Sign in to Windows under the user account in which you experience PRT issues.
2. Select **Start**, and then search for and select **Command Prompt**.
3. To run the device registration command ([dsregcmd](#)), enter `dsregcmd /status`.
4. Locate the [SSO state](#) section of the device registration command's output. The following text shows an example of this section:

Output

```
+-----  
+  
| SSO State  
|  
+-----  
+  
  
    AzureAdPrt : YES  
    AzureAdPrtUpdateTime : 2020-07-12 22:57:53.000 UTC  
    AzureAdPrtExpiryTime : 2020-07-26 22:58:35.000 UTC  
    AzureAdPrtAuthority :  
    https://login.microsoftonline.com/01234567-89ab-cdef-0123-456789abcdef  
        EnterprisePrt : YES  
        EnterprisePrtUpdateTime : 2020-07-12 22:57:54.000 UTC  
        EnterprisePrtExpiryTime : 2020-07-26 22:57:54.000 UTC  
        EnterprisePrtAuthority : https://msft.sts.microsoft.com:443/adfs  
  
+-----  
+
```

5. Check the value of the `AzureAdPrt` field. If it's set to `NO`, an error occurred when you tried to acquire the PRT status from Microsoft Entra ID.
6. Check the value of the `AzureAdPrtUpdateTime` field. If the value of the `AzureAdPrtUpdateTime` field is more than four hours, a problem is likely preventing the PRT from refreshing. Lock and unlock the device to force a PRT refresh, and then check whether the time is updated.

Step 2: Get the error code

The next step is to get the error code that causes the PRT error. The quickest way to get the PRT error code is to examine the device registration command output. However, this method requires the Windows 10 May 2021 update (version 21H1) or a later version. The other method is to find the error code in Microsoft Entra analytic and operational logs.

Method 1: Examine the device registration command output

Note

This method is available only if you're using the Windows 10 May 2021 update (version 21H1) or a later version of Windows.

To get the PRT error code, run the `dsregcmd` command, and then locate the `SSO State` section. In the `AzureAdPrt` field, the `Attempt Status` field contains the error code. In the following example, the error code is `0xc000006d`.

Output

```
AzureAdPrt : NO
AzureAdPrtAuthority : https://login.microsoftonline.com/01234567-
89ab-cdef-0123-456789abcdef
AcquirePrtDiagnostics : PRESENT
Previous Prt Attempt : 2020-09-18 20:20:09.760 UTC
Attempt Status : 0xc000006d
User Identity : user@contoso.com
Credential Type : Password
Correlation ID : 12345678-9abc-def0-1234-56789abcdef0
Endpoint URI : https://login.microsoftonline.com/01234567-
89ab-cdef-0123-456789abcdef/oauth2/token
HTTP Method : POST
HTTP Error : 0x0
HTTP status : 400
Server Error Code : invalid_grant
Server Error Description : AADSTS50126: Error validating credentials due
to invalid username or password.
```

Method 2: Use Event Viewer to examine AAD analytic and operational logs

1. Select **Start**, and then search for and select **Event Viewer**.
2. If the console tree doesn't appear in the **Event Viewer** window, select the **Show/Hide Console Tree** icon to make the console tree visible.
3. In the console tree, select **Event Viewer (Local)**. If child nodes don't appear underneath this item, double-click your selection to show them.
4. Select the **View** menu. If a check mark isn't displayed next to **Show Analytic and Debug Logs**, select that menu item to enable that feature.
5. In the console tree, expand **Applications and Services Logs > Microsoft > Windows > AAD**. The **Operational** and **Analytic** child nodes appear.

ⓘ Note

In the Microsoft Entra Cloud Authentication Provider (CloudAP) plug-in, **Error** events are written to the **Operational** event logs, and information events are

written to the **Analytic** event logs. You have to examine both the **Operational** and **Analytic** event logs to troubleshoot PRT issues.

6. In the console tree, select the **Analytic** node to view AAD-related analytic events.
7. In the list of analytic events, search for Event IDs 1006 and 1007. Event ID 1006 denotes the beginning of the PRT acquisition flow, and Event ID 1007 denotes the end of the PRT acquisition flow. All events in the **AAD** logs (both **Analytic** and **Operational**) that occurred between Event ID 1006 and Event ID 1007 are logged as part of the PRT acquisition flow. The following table shows an example event listing.

Level	Date and Time	Source	Event ID	Task Category
Information	6/24/2020 3:35:35 AM	AAD	1006	AadCloudAPPlugin Operation
Information	6/24/2020 3:35:35 AM	AAD	1018	AadCloudAPPlugin Operation
Information	6/24/2020 3:35:35 AM	AAD	1144	AadCloudAPPlugin Operation
Information	6/24/2020 3:35:35 AM	AAD	1022	AadCloudAPPlugin Operation
Error	6/24/2020 3:35:35 AM	AAD	1084	AadCloudAPPlugin Operation
Error	6/24/2020 3:35:35 AM	AAD	1086	AadCloudAPPlugin Operation
Error	6/24/2020 3:35:35 AM	AAD	1160	AadCloudAPPlugin Operation
Information	6/24/2020 3:35:35 AM	AAD	1007	AadCloudAPPlugin Operation
Information	6/24/2020 3:35:35 AM	AAD	1157	AadCloudAPPlugin Operation
Information	6/24/2020 3:35:35 AM	AAD	1158	AadCloudAPPlugin Operation

8. Double-click the row that contains Event ID 1007. The **Event Properties** dialog box for this event appears.
9. In the description box on the **General** tab, copy the error code. The error code is a 10-character string that begins with `0x`, followed by an 8-digit hexadecimal number.

Step 3: Get troubleshooting instructions for certain error codes

Status codes ("STATUS_" prefix, codes that begin with "0xc000")

- ▼ STATUS_LOGON_FAILURE (-1073741715 / 0xc000006d),
STATUS_WRONG_PASSWORD (-1073741718 / 0xc000006a)

Cause

- The device can't connect to the Microsoft Entra authentication service.
- The device received a `400 Bad Request` HTTP error response from one of the following sources:
 - The Microsoft Entra authentication service
 - An endpoint for the [WS-Trust protocol ↗](#) (required for federated authentication)

Solution

- If the on-premises environment requires an outbound proxy, make sure that the computer account of the device can discover and silently authenticate to the outbound proxy.
- Get the server error code and error description, and then go to the [Common server error codes \("AADSTS" prefix\)](#) section to find the cause of that server error code and the solution details.

In the Microsoft Entra operational logs, Event ID 1081 contains the server error code and error description if the error occurs in the Microsoft Entra authentication service. If the error occurs in a WS-Trust endpoint, the server error code and error description are found in Event ID 1088. In the Microsoft Entra analytic logs, the first instance of Event ID 1022 (that precedes operational Event IDs 1081 and 1088) contains the URL that's being accessed.

To view Event IDs in the Microsoft Entra operational and analytic logs, refer to the [Method 2: Use Event Viewer to examine Microsoft Entra analytic and operational logs](#) section.

- ▼ STATUS_REQUEST_NOT_ACCEPTED (-1073741616 / 0xc0000d0)

Cause

The device received a `400 Bad Request` HTTP error response from one of the following sources:

- The Microsoft Entra authentication service

- An endpoint for the [WS-Trust protocol](#) (required for federated authentication)

Solution

Get the server error code and error description, and then go to the [Common server error codes \("AADSTS" prefix\)](#) section to find the cause of that server error code and the solution details.

In the Microsoft Entra operational logs, Event ID 1081 contains the server error code and error description if the error occurs in the Microsoft Entra authentication service. If the error occurs in a WS-Trust endpoint, the server error code and error description are found in Event ID 1088. In the Microsoft Entra analytic logs, the first instance of Event ID 1022 (that precedes operational Event IDs 1081 and 1088) contains the URL that's being accessed.

To view Event IDs in the Microsoft Entra operational and analytic logs, refer to the [Method 2: Use Event Viewer to examine Microsoft Entra analytic and operational logs](#) section.

▼ STATUS_NETWORK_UNREACHABLE (-1073741252 / 0xc000023c),
STATUS_BAD_NETWORK_PATH (-1073741634 / 0xc00000be),
STATUS_UNEXPECTED_NETWORK_ERROR (-1073741628 / 0xc00000c4)

Cause

- The device received a `4xx` HTTP error response from one of the following sources:
 - The Microsoft Entra authentication service
 - An endpoint for the [WS-Trust protocol](#) (required for federated authentication)
- A network connectivity issue to a required endpoint exists.

Solution

- Get the server error code and error description, and then go to the [Common server error codes \("AADSTS" prefix\)](#) section to find the cause of that server error code and the solution details.

In the Microsoft Entra operational logs, Event ID 1081 contains the server error code and error description if the error occurs in the Microsoft Entra authentication service. If the error occurs in a WS-Trust endpoint, the server error code and error description are found in Event ID 1088.

- For a network connectivity issue, get the URL that's being accessed and the suberror code from the network stack. Event ID 1022 in the Microsoft Entra analytic logs contains the URL that's being accessed. Event ID 1084 in the Microsoft Entra operational logs contains the suberror code from the network stack.

To view Event IDs in the Microsoft Entra operational and analytic logs, refer to the [Method 2: Use Event Viewer to examine Microsoft Entra analytic and operational logs](#) section.

▼ STATUS_NO SUCH_LOGON_SESSION (-1073741729 / 0xc000005f)

Cause

The user realm discovery failed because the Microsoft Entra authentication service can't find the user's domain.

Solution

- Add the domain of the user principal name (UPN) of the user as a custom domain in Microsoft Entra ID. To find the provided UPN, look for Event ID 1144 in the Microsoft Entra analytic logs.

To view Event IDs in the Microsoft Entra analytic logs, refer to the [Method 2: Use Event Viewer to examine Microsoft Entra analytic and operational logs](#) section.

- If the on-premises domain name can't be routed (for example, if the UPN is something such as `jdoe@contoso.local`), [configure the Alternate Login ID \(AltID\)](#). (To view the prerequisites, see [Plan your Microsoft Entra hybrid join implementation](#).)

Common CloudAP plug-in error codes ("AAD_CLOUDAP_E_" prefix, codes that begin with "0xc004")

▼ AAD_CLOUDAP_E_OAUTH_USERNAME_IS_MALFORMED (-1073445812 / 0xc004844c)

Cause

The UPN for the user isn't in the expected format. The UPN value varies according to the device type, as shown in the following table.

Device join type	UPN value
Microsoft Entra joined devices	The text that's entered when the user signs in

Device join type	UPN value
Microsoft Entra hybrid joined devices	The UPN that the domain controller returns during the sign-in process

Solution

- Set the UPN of the user to an internet-style sign-in name, based on internet standard [RFC 822](#). To find the current UPN, look for event ID 1144 in the Microsoft Entra analytic logs.

To view Event IDs in the Microsoft Entra analytic logs, refer to the [Method 2: Use Event Viewer to examine Microsoft Entra analytic and operational logs](#) section.

- For Microsoft Entra hybrid joined devices, make sure that you configured the domain controller to return the UPN in the correct format. To display the configured UPN in the domain controller, run the following `whoami` command:

```
Windows Command Prompt
```

```
whoami /upn
```

If Active Directory is configured with the correct UPN, [collect time travel traces](#) for the Local Security Authority Subsystem Service (LSASS or `lsass.exe`).

- If the on-premises domain name can't be routed (for example, if the UPN is something such as `jdoe@contoso.local`), [configure the Alternate Login ID \(AltID\)](#). (To view the prerequisites, see [Plan your Microsoft Entra hybrid join implementation](#).)
- ▼ AAD_CLOUDAP_E_OAUTH_USER_SID_IS_EMPTY (-1073445822 / 0xc0048442)

Cause

The user security identifier (SID) is missing in the ID token that the Microsoft Entra authentication service returns.

Solution

Make sure that the network proxy doesn't interfere with or modify the server response.

- ▼ AAD_CLOUDAP_E_WSTRUST_SAML_TOKENS_ARE_EMPTY
(-1073445695 / 0xc00484c1 / 0x800484c1)

Cause

You received an error from the [WS-Trust protocol](#) endpoint (required for federated authentication).

Solution

- Make sure that the network proxy doesn't interfere with or modify the server response.
- Get the server error code and error description from Event ID 1088 in the Microsoft Entra operational logs. Then, go to the [Common server error codes \("AADSTS" prefix\)](#) section to find the cause of that server error code and the solution details.

To view Event IDs in the Microsoft Entra operational logs, refer to the [Method 2: Use Event Viewer to examine Microsoft Entra analytic and operational logs](#) section.

▼ AAD_CLOUDAP_E_HTTP_PASSWORD_URI_IS_EMPTY (-1073445749 / 0xc004848b)

Cause

The Metadata Exchange (MEX) endpoint is configured incorrectly. The MEX response doesn't contain any password URLs.

Solution

- Make sure that the network proxy doesn't interfere with or modify the server response.
 - Fix the MEX configuration to return valid URLs in the response.
- ▼ AAD_CLOUDAP_E_HTTP_CERTIFICATE_URI_IS_EMPTY (-1073445748 / 0xc004848c)

Cause

The Metadata Exchange (MEX) endpoint is configured incorrectly. The MEX response doesn't contain any certificate endpoint URLs.

Solution

- Make sure that the network proxy doesn't interfere with or modify the server response.

- Fix the MEX configuration in the identity provider to return valid certificate URLs in the response.

Common XML error codes (codes that begin with "0xc00c")

▼ WC_E_DTDPROHIBITED (-1072894385 / 0xc00cee4f)

Cause

The XML response from the [WS-Trust protocol](#) endpoint (required for federated authentication) included a document type definition (DTD). The DTD isn't expected in the XML response, and response parsing fails if the DTD is included.

Solution

- Fix the configuration in the identity provider to avoid sending the DTD in the XML response.
- Get the URL that's being accessed from Event ID 1022 in the Microsoft Entra analytic logs.

To view Event IDs in the Microsoft Entra analytic logs, refer to the [Method 2: Use Event Viewer to examine Microsoft Entra analytic and operational logs](#) section.

Common server error codes ("AADSTS" prefix)

You can find a full list and description of server error codes in [Microsoft Entra authentication and authorization error codes](#).

▼ AADSTS50155: Device authentication failed

Cause

- Microsoft Entra ID can't authenticate the device to issue a PRT.
- The device might have been deleted or disabled. (For more information, see [Why do my users see an error message saying "Your organization has deleted the device" or "Your organization has disabled the device" on their Windows 10/11 devices?](#))

Solution

Re-register the device based on the device join type. For instructions, see [I disabled or deleted my device. But the local state on the device says it's still registered. What should I do?](#).

▼ AADSTS50034: The user account <Account> does not exist in the <tenant-id> directory

Cause

Microsoft Entra ID can't find the user account in the tenant.

Solution

- Make sure that the user is entering the correct UPN.
- Make sure that the on-premises user account is being synchronized to Microsoft Entra ID.
- Get the provided UPN by looking for Event ID 1144 in the Microsoft Entra analytic logs.

To view Event IDs in the Microsoft Entra analytic logs, refer to the [Method 2: Use Event Viewer to examine Microsoft Entra analytic and operational logs](#) section.

▼ AADSTS50126: Error validating credentials due to invalid username or password

Cause

- The user entered an incorrect username or password in the sign-in UI.
- The password hasn't been synchronized to Microsoft Entra ID because of the following scenario:
 - The tenant has enabled [password hash synchronization](#).
 - The device is a Microsoft Entra hybrid joined device.
 - The user recently changed the password.

Solution

To acquire a fresh PRT that has the new credentials, wait for the Microsoft Entra synchronization to finish.

Common network error codes ("ERROR_WINHTTP_" prefix)

You can find a full list and description of network error codes in [Error messages \(Winhttp.h\)](#).

- ▼ `ERROR_WINHTTP_TIMEOUT` (12002),
`ERROR_WINHTTP_NAME_NOT_RESOLVED` (12007),
`ERROR_WINHTTP_CANNOT_CONNECT` (12029),
`ERROR_WINHTTP_CONNECTION_ERROR` (12030)

Cause

Common general network-related issues.

Solution

- Get the URL that's being accessed. You can find the URL in Event ID 1084 of the Microsoft Entra operational log or Event ID 1022 of the Microsoft Entra analytic log.

To view Event IDs in the Microsoft Entra operational and analytic logs, refer to the [Method 2: Use Event Viewer to examine Microsoft Entra analytic and operational logs](#) section.

- If the on-premises environment requires an outbound proxy, make sure that the computer account of the device can discover and silently authenticate to the outbound proxy.
- Collect network traces by following these steps:

Important

Don't use Fiddler during this procedure.

1. Run the following [netsh trace start](#) command:

```
Windows Command Prompt
```

```
netsh trace start scenario=InternetClient_dbg capture=yes  
persistent=yes
```

2. Lock the device.

3. If the device is a Microsoft Entra hybrid joined device, wait at least 60 seconds to let the PRT acquisition task finish.

4. Unlock the device.

5. Run the following [netsh trace stop](#) command:

```
Windows Command Prompt
```

```
netsh trace stop
```

Step 4: Collect the logs and traces

Regular logs

1. Download the [Auth script archive](#), and extract the scripts into a local directory. If it's necessary, review the usage instructions in [KB 4487175](#).
2. Open an administrative PowerShell session, and change the current directory to the directory in which you saved the Auth scripts.
3. To begin the error tracing session, enter the following command:

```
PowerShell
```

```
.\Start-auth.ps1 -v -acceptEULA
```

4. Switch the Windows user account to go to your problem user's session.
5. Lock the device.
6. If the device is a Microsoft Entra hybrid joined device, wait at least 60 seconds to let the PRT acquisition task finish.
7. Unlock the device.
8. Switch the Windows user account back to your administrative session that's running the tracing session.
9. After you reproduce the issue, run the following command to end the tracing session:

```
PowerShell
```

```
.\stop-auth.ps1
```

10. Wait for all tracing to stop completely.

Time travel traces

The following procedure describes how to capture traces by using the [Time Travel Debugging \(TTD\)](#) feature.

Warning

Time travel traces contain personal data. In addition, Local Security Authority Subsystem Service (LSASS or *lsass.exe*) traces contain extremely sensitive information. When you handle these traces, make sure that you use best practices for the storage and sharing of this type of information.

1. Select **Start**, enter *cmd*, locate and right-click **Command Prompt** in the search results, and then select **Run as administrator**.
2. At the command prompt, create a temporary directory:

```
Windows Command Prompt
```

```
mkdir c:\temp
```

3. Run the following [tasklist](#) command:

```
Windows Command Prompt
```

```
tasklist /m lsasrv.dll
```

4. In the `tasklist` command output, find the process identifier (`PID`) of *lsass.exe*.
5. To begin a tracing session of the *lsass.exe* process, run the following time travel debugging command ([TTD.exe](#)):

```
Windows Command Prompt
```

```
TTD.exe -attach <lsass-pid> -out c:\temp
```

6. Lock the device that's signed in under the domain account.

7. Unlock the device.

8. To end the time travel tracing session, run the following TTD command:

```
Windows Command Prompt
```

```
TTD.exe -stop all
```

9. Get the latest *lsass##.run* file.

How To: Manage stale devices in Microsoft Entra ID

Article • 04/22/2024

Ideally, to complete the lifecycle, registered devices should be unregistered when they aren't needed anymore. Because of lost, stolen, broken devices, or OS reinstallations you typically have some stale devices in your environment. As an IT admin, you probably want a method to remove stale devices, so that you can focus your resources on managing devices that actually require management.

In this article, you learn how to efficiently manage stale devices in your environment.

What is a stale device?

A stale device is a device registered with Microsoft Entra ID that hasn't accessed any cloud apps for a specific timeframe. Stale devices have an impact on your ability to manage and support your devices and users in the tenant because:

- Duplicate devices can make it difficult for your helpdesk staff to identify which device is currently active.
- An increased number of devices creates unnecessary device writebacks increasing the time for Microsoft Entra Connect syncs.
- As a general hygiene and to meet compliance, you might want to have a clean slate of devices.

Stale devices in Microsoft Entra ID can interfere with the general lifecycle policies for devices in your organization.

Detect stale devices

Because a stale device is defined as a registered device that hasn't been used to access any cloud apps for a specific timeframe, detecting stale devices requires a timestamp-related property. In Microsoft Entra ID, this property is called

ApproximateLastSignInDateTime or **activity timestamp**. If the delta between now and the value of the **activity timestamp** exceeds the timeframe you've defined for active devices, a device is considered to be stale. This **activity timestamp** is now in public preview.

How is the value of the activity timestamp managed?

The evaluation of the activity timestamp is triggered by an authentication attempt of a device. Microsoft Entra ID evaluates the activity timestamp when:

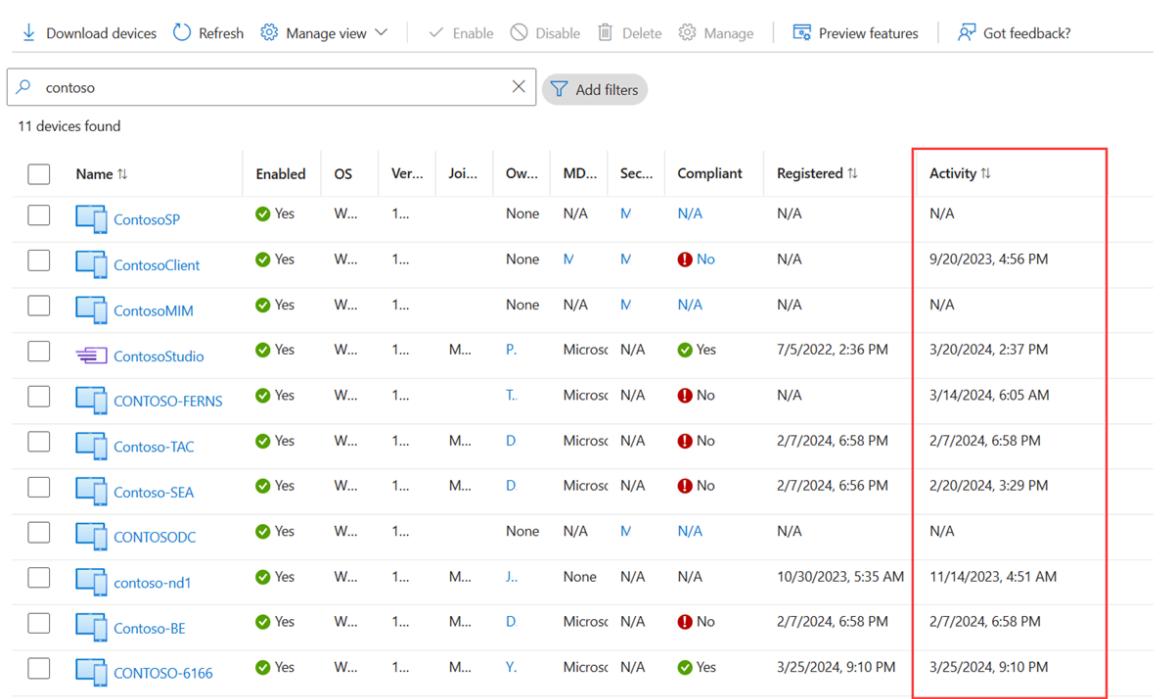
- A Conditional Access policies requiring [managed devices](#) or [approved client apps](#) has been triggered.
- Windows 10 or newer devices that are either Microsoft Entra joined or Microsoft Entra hybrid joined are active on the network.
- Intune managed devices have checked in to the service.

If the delta between the existing value of the activity timestamp and the current value is more than 14 days (+/-5 day variance), the existing value is replaced with the new value.

How do I get the activity timestamp?

You have two options to retrieve the value of the activity timestamp:

- The **Activity** column on the all devices page.



Name	Enabled	OS	Ver...	Joi...	Ow...	MD...	Sec...	Compliant	Registered	Activity
ContosoSP	Yes	W...	1...		None	N/A	N/A	N/A	N/A	N/A
ContosoClient	Yes	W...	1...		None	N/A	N/A	No	N/A	9/20/2023, 4:56 PM
ContosoMIM	Yes	W...	1...		None	N/A	N/A	N/A	N/A	N/A
ContosoStudio	Yes	W...	1...	M...	P.	Micros	N/A	Yes	7/5/2022, 2:36 PM	3/20/2024, 2:37 PM
CONTOSO-FERNS	Yes	W...	1...		T..	Micros	N/A	No	N/A	3/14/2024, 6:05 AM
Contoso-TAC	Yes	W...	1...	M...	D	Micros	N/A	No	2/7/2024, 6:58 PM	2/7/2024, 6:58 PM
Contoso-SEA	Yes	W...	1...	M...	D	Micros	N/A	No	2/7/2024, 6:56 PM	2/20/2024, 3:29 PM
CONTOSODC	Yes	W...	1...		None	N/A	N/A	N/A	N/A	N/A
contoso-nd1	Yes	W...	1...	M...	J..	None	N/A	N/A	10/30/2023, 5:35 AM	11/14/2023, 4:51 AM
Contoso-BE	Yes	W...	1...	M...	D	Micros	N/A	No	2/7/2024, 6:58 PM	2/7/2024, 6:58 PM
CONTOSO-6166	Yes	W...	1...	M...	Y..	Micros	N/A	Yes	3/25/2024, 9:10 PM	3/25/2024, 9:10 PM

- The [Get-MgDevice](#) cmdlet.

```
"AccountEnabled": true,  
"AlternativeSecurityIds": [  
    "Microsoft.Graph.PowerShell.Models.MicrosoftGraphAlternativeSecurityId"  
],  
"ApproximateLastSignInDateTime": "2023-12-18T15:32:16Z",  
"ComplianceExpirationDateTime": null,
```

Plan the cleanup of your stale devices

To efficiently cleanup stale devices in your environment, you should define a related policy. This policy helps you to ensure that you capture all considerations that are related to stale devices. The following sections provide you with examples for common policy considerations.

⊗ Caution

If your organization uses BitLocker drive encryption, you should ensure that BitLocker recovery keys are either backed up or no longer needed before deleting devices. Failure to do this may cause loss of data.

If you use features like [Autopilot](#) or [Universal Print](#), those devices should be cleaned up in their respective admin portals.

Cleanup account

To update a device in Microsoft Entra ID, you need an account that has one of the following roles assigned:

- [Cloud Device Administrator](#)
- [Intune Administrator](#)

In your cleanup policy, select accounts that have the required roles assigned.

Timeframe

Define a timeframe that is your indicator for a stale device. When defining your timeframe, factor the window noted for updating the activity timestamp into your value. For example, you shouldn't consider a timestamp that is younger than 21 days (includes variance) as an indicator for a stale device. There are scenarios that can make a device look like stale while it isn't. For example, the owner of the affected device can be on vacation or on a sick leave that exceeds your timeframe for stale devices.

Disable devices

It isn't advisable to immediately delete a device that appears to be stale because you can't undo a deletion if there's a false positive. As a best practice, disable a device for a grace period before deleting it. In your policy, define a timeframe to disable a device before deleting it.

MDM-controlled devices

If your device is under control of Intune or any other Mobile Device Management (MDM) solution, retire the device in the management system before disabling or deleting it. For more information, see the article [Remove devices by using wipe, retire, or manually unenrolling the device](#).

System-managed devices

Don't delete system-managed devices. These devices are generally devices such as Autopilot. Once deleted, these devices can't be reprovisioned.

Microsoft Entra hybrid joined devices

Your Microsoft Entra hybrid joined devices should follow your policies for on-premises stale device management.

To clean up Microsoft Entra ID:

- **Windows 10 or newer devices** - Disable or delete Windows 10 or newer devices in your on-premises AD, and let Microsoft Entra Connect synchronize the changed device status to Microsoft Entra ID.
- **Windows 7/8** - Disable or delete Windows 7/8 devices in your on-premises AD first. You can't use Microsoft Entra Connect to disable or delete Windows 7/8 devices in Microsoft Entra ID. Instead, when you make the change in your on-premises, you must disable/delete in Microsoft Entra ID.

Note

- Deleting devices in your on-premises Active Directory or Microsoft Entra ID does not remove registration on the client. It will only prevent access to resources using device as an identity (such as Conditional Access). Read additional information on how to [remove registration on the client](#).
- Deleting a Windows 10 or newer device only in Microsoft Entra ID will re-synchronize the device from your on-premises using Microsoft Entra Connect but as a new object in "Pending" state. A re-registration is required on the device.
- Removing the device from sync scope for Windows 10 or newer /Server 2016 devices will delete the Microsoft Entra device. Adding it back to sync scope

will place a new object in "Pending" state. A re-registration of the device is required.

- If you are not using Microsoft Entra Connect for Windows 10 or newer devices to synchronize (e.g. ONLY using AD FS for registration), you must manage lifecycle similar to Windows 7/8 devices.

Microsoft Entra joined devices

Disable or delete Microsoft Entra joined devices in the Microsoft Entra ID.

Note

- Deleting a Microsoft Entra device does not remove registration on the client. It will only prevent access to resources using device as an identity (e.g Conditional Access).
- Read more on [how to unjoin on Microsoft Entra ID](#)

Microsoft Entra registered devices

Disable or delete Microsoft Entra registered devices in the Microsoft Entra ID.

Note

- Deleting a Microsoft Entra registered device in Microsoft Entra ID does not remove registration on the client. It will only prevent access to resources using device as an identity (e.g. Conditional Access).
- Read more on [how to remove a registration on the client](#)

Clean up stale devices

While you can clean up stale devices in the Microsoft Entra admin center, it's more efficient to handle this process using a PowerShell script. Use the latest PowerShell V2 module to use the timestamp filter and to filter out system-managed devices such as Autopilot.

A typical routine consists of the following steps:

1. Connect to Microsoft Entra ID using the [Connect-MgGraph](#) cmdlet
2. Get the list of devices.
3. Disable the device using the [Update-MgDevice](#) cmdlet (disable by using - AccountEnabled option).
4. Wait for the grace period of however many days you choose before deleting the device.
5. Remove the device using the [Remove-MgDevice](#) cmdlet.

Get the list of devices

To get all devices and store the returned data in a CSV file:

PowerShell

```
Get-MgDevice -All | select-object -Property AccountEnabled, DeviceId, OperatingSystem, OperatingSystemVersion, DisplayName, TrustType, ApproximateLastSignInDateTime | export-csv devicelist-summary.csv -NoTypeInformation
```

If you have a large number of devices in your directory, use the timestamp filter to narrow down the number of returned devices. To get all devices that haven't logged on in 90 days and store the returned data in a CSV file:

PowerShell

```
$dt = (Get-Date).AddDays(-90)
Get-MgDevice -All | Where {$_.ApproximateLastSignInDateTime -le $dt} |
select-object -Property AccountEnabled, DeviceId, OperatingSystem, OperatingSystemVersion, DisplayName, TrustType, ApproximateLastSignInDateTime | export-csv devicelist-olderthan-90days-summary.csv -NoTypeInformation
```

⚠ Warning

Some active devices may have a blank time stamp.

Set devices to disabled

Using the same commands we can pipe the output to the set command to disable the devices over a certain age.

PowerShell

```
$dt = (Get-Date).AddDays(-90)
$params = @{
    accountEnabled = $false
}

$Devices = Get-MgDevice -All | Where {$_.ApproximateLastSignInDateTime -le
$dt}
foreach ($Device in $Devices) {
    Update-MgDevice -DeviceId $Device.Id -BodyParameter $params
}
```

Delete devices

⊗ Caution

The `Remove-MgDevice` cmdlet does not provide a warning. Running this command will delete devices without prompting. **There is no way to recover deleted devices.**

Before administrators delete any devices, back up any BitLocker recovery keys you might need in the future. There's no way to recover BitLocker recovery keys after deleting the associated device.

Building on the [disable devices example](#) we look for disabled devices, now inactive for 120 days, and pipe the output to `Remove-MgDevice` to delete those devices.

PowerShell

```
$dt = (Get-Date).AddDays(-120)
$Devices = Get-MgDevice -All | Where {($_.ApproximateLastSignInDateTime -le
$dt) -and ($_.AccountEnabled -eq $false)}
foreach ($Device in $Devices) {
    Remove-MgDevice -DeviceId $Device.Id
}
```

What you should know

Why is the timestamp not updated more frequently?

The timestamp is updated to support device lifecycle scenarios. This attribute isn't an audit. Use the sign-in audit logs for more frequent updates on the device. Some active devices might have a blank time stamp.

Why should I worry about my BitLocker keys?

When configured, BitLocker keys for Windows 10 or newer devices are stored on the device object in Microsoft Entra ID. If you delete a stale device, you also delete the BitLocker keys that are stored on the device. Confirm that your cleanup policy aligns with the actual lifecycle of your device before deleting a stale device.

Why should I worry about Windows Autopilot devices?

When you delete a Microsoft Entra device that was associated with a Windows Autopilot object the following three scenarios can occur if the device will be repurposed in future:

- With Windows Autopilot user-driven deployments without using pre-provisioning, a new Microsoft Entra device is created, but isn't be tagged with the ZTDID.
- With Windows Autopilot self-deploying mode deployments, they'll fail because an associate Microsoft Entra device can't be found. (This failure is a security mechanism to make sure that no "impostor" devices try to join Microsoft Entra ID with no credentials.) The failure indicates a ZTDID mismatch.
- With Windows Autopilot pre-provisioning deployments, they fail because an associated Microsoft Entra device can't be found. (Behind the scenes, pre-provisioning deployments use the same self-deploying mode process, so they enforce the same security mechanisms.)

Use the [Get-MgDeviceManagementWindowsAutopilotDeviceIdentity](#) to list of Windows Autopilot devices in your organization and compare it to the list of devices to clean up.

How do I know all the type of devices joined?

To learn more about the different types, see the [device management overview](#).

What happens when I disable a device?

Any authentication where a device is being used to authenticate to Microsoft Entra ID are denied. Common examples are:

- **Microsoft Entra hybrid joined device** - Users might be able to use the device to sign-in to their on-premises domain. However, they can't access Microsoft Entra resources such as Microsoft 365.
- **Microsoft Entra joined device** - Users can't use the device to sign in.
- **Mobile devices** - User can't access Microsoft Entra resources such as Microsoft 365.

Related content

For more information about devices managed with Intune, see the article [Remove devices by using wipe, retire, or manually unenrolling the device](#).

To get an overview of how to manage devices, see [managing device identities](#)

Sign in to a Linux virtual machine in Azure by using Microsoft Entra ID and OpenSSH

Article • 03/07/2025

To improve the security of Azure Linux virtual machines (VMs) or Azure Arc-enabled Linux servers, you can integrate with Microsoft Entra authentication. You can now use Microsoft Entra ID as a core authentication platform and a certificate authority to SSH into a Linux VM by using Microsoft Entra ID and OpenSSH certificate-based authentication. This functionality allows organizations to manage access to VMs with Azure role-based access control (RBAC) and Conditional Access policies.

This article shows you how to create and configure a Linux VM and log in with Microsoft Entra ID by using OpenSSH certificate-based authentication.

There are many security benefits of using Microsoft Entra ID with OpenSSH certificate-based authentication to sign in to Linux VMs in Azure. They include:

- Use your Microsoft Entra credentials to sign in to Azure Linux VMs.
- Get SSH key-based authentication without needing to distribute SSH keys to users or provision SSH public keys on any Azure Linux VMs that you deploy. This experience is much simpler than having to worry about sprawl of stale SSH public keys that could cause unauthorized access.
- Reduce reliance on local administrator accounts, credential theft, and weak credentials.
- Help secure Linux VMs by configuring password complexity and password lifetime policies for Microsoft Entra ID.
- With RBAC, specify who can sign in to a VM as a regular user or with administrator privileges. When users join your team, you can update the Azure RBAC policy for the VM to grant access as appropriate. When employees leave your organization and their user accounts are disabled or removed from Microsoft Entra ID, they no longer have access to your resources.
- With Conditional Access, configure policies to require multifactor authentication or to require that your client device is managed (for example, compliant or Microsoft Entra hybrid joined) before you can use it SSH into Linux VMs.
- Use Azure deploy and audit policies to require Microsoft Entra login for Linux VMs and flag unapproved local accounts.

Sign in to Linux VMs with Microsoft Entra ID works for customers who use Active Directory Federation Services.

Supported Linux distributions and Azure regions

The following Linux distributions are currently supported for deployments in a supported region:

[\[+\] Expand table](#)

Distribution	Version
AlmaLinux	AlmaLinux 8, AlmaLinux 9
Azure Linux (formerly known as Common Base Linux Mariner)	CBL-Mariner 2.0, Azure Linux 3.0
Debian	Debian 9, Debian 10, Debian 11, Debian 12
openSUSE	openSUSE Leap 42.3, openSUSE Leap 15.1 to 15.5, openSUSE Leap 15.6+
Oracle	Oracle Linux 8, Oracle Linux 9
RedHat Enterprise Linux (RHEL)	RHEL 7.4 to RHEL 7.9, RHEL 8.3+, RHEL 9.0+
Rocky	Rocky 8, Rocky 9
SUSE Linux Enterprise Server (SLES)	SLES 12, SLES 15.1 to 15.5, SLES 15.6+
Ubuntu	Ubuntu 16.04 to Ubuntu 24.04

Note

SUSE made a breaking change with version 15.6 that is incompatible with the older versions. Since the Microsoft Entra login VM extension always installs the latest package, this will not work on older SUSE versions. You can install the `aadsshlogin` packages from packages.microsoft.com for older SUSE versions. After adding the repo, one can manually install them with this command: `sudo zypper install aadsshlogin=1.0.0-27980001`.

The following Azure regions are currently supported for this feature:

- Azure Global
- Azure Government
- Microsoft Azure operated by 21Vianet

Use of the SSH extension for the Azure CLI on Azure Kubernetes Service (AKS) clusters is not supported. For more information, see [Support policies for AKS](#).

If you choose to install and use the Azure CLI locally, it must be version 2.22.1 or later. Run `az --version` to find the version. If you need to install or upgrade, see [Install the Azure CLI](#).

 **Note**

This functionality is also available for [Azure Arc-enabled servers](#).

Meet requirements for login with Microsoft Entra ID using OpenSSH certificate-based authentication

To enable Microsoft Entra login through SSH certificate-based authentication for Linux VMs in Azure, be sure to meet the following network, virtual machine, and client (SSH client) requirements.

Network

VM network configuration must permit outbound access to the following endpoints over TCP port 443.

Azure Global:

- `https://packages.microsoft.com`: For package installation and upgrades.
- `http://169.254.169.254`: Azure Instance Metadata Service endpoint.
- `https://login.microsoftonline.com`: For PAM-based (pluggable authentication modules) authentication flows.
- `https://pas.windows.net`: For Azure RBAC flows.

Azure Government:

- `https://packages.microsoft.com`: For package installation and upgrades.
- `http://169.254.169.254`: Azure Instance Metadata Service endpoint.
- `https://login.microsoftonline.us`: For PAM-based authentication flows.
- `https://pasff.usgovcloudapi.net`: For Azure RBAC flows.

Microsoft Azure operated by 21Vianet:

- `https://packages.microsoft.com`: For package installation and upgrades.
- `http://169.254.169.254`: Azure Instance Metadata Service endpoint.
- `https://login.chinacloudapi.cn`: For PAM-based authentication flows.
- `https://pas.chinacloudapi.cn`: For Azure RBAC flows.

Virtual machine

Ensure that your VM is configured with the following functionality:

- System-assigned managed identity. This option is automatically selected when you use the Azure portal to create VMs and select the Microsoft Entra login option. You can also enable system-assigned managed identity on a new or existing VM by using the Azure CLI.
- `aadsshlogin` and `aadsshlogin-selinux` (as appropriate). These packages are installed with the AADSSHLoginForLinux VM extension. The extension is installed when you use the Azure portal or the Azure CLI to create VMs and enable Microsoft Entra login (**Management** tab).

Client

Ensure that your client meets the following requirements:

- SSH client support for OpenSSH-based certificates for authentication. You can use the Azure CLI (2.21.1 or later) with OpenSSH (included in Windows 10 version 1803 or later) or Azure Cloud Shell to meet this requirement.
- SSH extension for the Azure CLI. You can install this extension by using `az extension add --name ssh`. You don't need to install this extension when you're using Azure Cloud Shell, because it comes preinstalled.

If you're using any SSH client other than the Azure CLI or Azure Cloud Shell that supports OpenSSH certificates, you'll still need to use the Azure CLI with the SSH extension to retrieve ephemeral SSH certificates and optionally a configuration file. You can then use the configuration file with your SSH client.

- TCP connectivity from the client to either the public or private IP address of the VM. (ProxyCommand or SSH forwarding to a machine with connectivity also works.)

 **Important**

SSH clients based on PuTTY now supports OpenSSH certificates and can be used to log in with Microsoft Entra OpenSSH certificate-based authentication.

Enable Microsoft Entra login for a Linux VM in Azure

To use Microsoft Entra login for a Linux VM in Azure, you need to first enable the Microsoft Entra login option for your Linux VM. You then configure Azure role assignments for users who are authorized to sign in to the VM. Finally, you use the SSH client that supports OpenSSH, such as the Azure CLI or Azure Cloud Shell, to SSH into your Linux VM.

There are two ways to enable Microsoft Entra login for your Linux VM:

- The Azure portal experience when you're creating a Linux VM
- The Azure Cloud Shell experience when you're creating a Linux VM or using an existing one

Azure portal

You can enable Microsoft Entra login for any of the [supported Linux distributions](#) by using the Azure portal.

For example, to create an Ubuntu Server 18.04 long-term support (LTS) VM in Azure with Microsoft Entra login:

1. Sign in to the [Azure portal](#) by using an account that has access to create VMs, and then select **+ Create a resource**.
2. Select **Create** under **Ubuntu Server 18.04 LTS** in the **Popular** view.
3. On the **Management** tab:
 - a. Select the **Login with Microsoft Entra ID** checkbox.
 - b. Ensure that the **System assigned managed identity** checkbox is selected.
4. Go through the rest of the experience of creating a virtual machine. You'll have to create an administrator account with username and password or SSH public key.

Azure Cloud Shell

Azure Cloud Shell is a free, interactive shell that you can use to run the steps in this article. Common Azure tools are preinstalled and configured in Cloud Shell for you to

use with your account. Just select the **Copy** button to copy the code, paste it in Cloud Shell, and then select the Enter key to run it.

There are a few ways to open Cloud Shell:

- Select **Try It** in the upper-right corner of a code block.
- Open Cloud Shell in your browser.
- Select the Cloud Shell button on the menu in the upper-right corner of the Azure portal.

If you choose to install and use the Azure CLI locally, this article requires you to use version 2.22.1 or later. Run `az --version` to find the version. If you need to install or upgrade, see [Install the Azure CLI](#).

1. Create a resource group by running [az group create](#).
2. Create a VM by running [az vm create](#). Use a supported distribution in a supported region.
3. Install the Microsoft Entra login VM extension by using [az vm extension set](#).

The following example deploys a VM and then installs the extension to enable Microsoft Entra login for a Linux VM. VM extensions are small applications that provide post-deployment configuration and automation tasks on Azure Virtual Machines. Customize the example as needed to support your testing requirements.

```
Azure CLI

az group create --name AzureADLinuxVM --location southcentralus
az vm create \
    --resource-group AzureADLinuxVM \
    --name myVM \
    --image Ubuntu2204 \
    --assign-identity \
    --admin-username azureuser \
    --generate-ssh-keys
az vm extension set \
    --publisher Microsoft.Azure.ActiveDirectory \
    --name AADSSHLoginForLinux \
    --resource-group AzureADLinuxVM \
    --vm-name myVM
```

It takes a few minutes to create the VM and supporting resources.

The AADSSHLoginForLinux extension can be installed on an existing (supported distribution) Linux VM with a running VM agent to enable Microsoft Entra authentication. If you're deploying this extension to a previously created VM, the VM must have at least 1 GB of memory allocated or the installation will fail.

The `provisioningState` value of `Succeeded` appears when the extension is successfully installed on the VM. The VM must have a running [VM agent](#) to install the extension.

Enable Microsoft Entra login for a Azure Arc-enabled Linux servers

You can find the relevant details on [SSH access to Azure Arc-enabled servers](#)

Configure role assignments for the VM

Now that you've created the VM, you need to assign one of the following Azure roles to determine who can sign in to the VM. To assign these roles, you must have the [Virtual Machine Data Access Administrator](#) role, or any role that includes the `Microsoft.Authorization/roleAssignments/write` action such as the [Role Based Access Control Administrator](#) role. However, if you use a different role than Virtual Machine Data Access Administrator, we recommend you [add a condition to reduce the permission to create role assignments](#).

- **Virtual Machine Administrator Login:** Users who have this role assigned can sign in to an Azure virtual machine with administrator privileges.
- **Virtual Machine User Login:** Users who have this role assigned can sign in to an Azure virtual machine with regular user privileges.

To allow a user to sign in to a VM over SSH, you must assign the Virtual Machine Administrator Login or Virtual Machine User Login role on the resource group that contains the VM and its associated virtual network, network interface, public IP address, or load balancer resources.

An Azure user who has the Owner or Contributor role assigned for a VM doesn't automatically have privileges to Microsoft Entra sign in to the VM over SSH. There's an intentional (and audited) separation between the set of people who control virtual machines and the set of people who can access virtual machines.

There are two ways to configure role assignments for a VM:

- Azure portal experience
- Azure Cloud Shell experience

Note

The Virtual Machine Administrator Login and Virtual Machine User Login roles use `dataActions` and can be assigned at the management group, subscription, resource group, or resource scope. We recommend that you assign the roles at the management group, subscription, or resource group level and not at the individual VM level. This practice avoids the risk of reaching the [Azure role assignments limit](#) per subscription.

Azure portal

To configure role assignments for your Microsoft Entra ID-enabled Linux VMs:

1. For **Resource Group**, select the resource group that contains the VM and its associated virtual network, network interface, public IP address, or load balancer resource.
2. Select **Access control (IAM)**.
3. Select **Add > Add role assignment** to open the **Add role assignment** page.
4. Assign the following role. For detailed steps, see [Assign Azure roles by using the Azure portal](#).

[+] Expand table

Setting	Value
Role	Virtual Machine Administrator Login or Virtual Machine User Login
Assign access to	User, group, service principal, or managed identity

A role definition is a collection of permissions. You can use the built-in roles or you can create your own custom roles. [Learn more](#)

Name ↑↓	Description ↑↓	Type ↑↓	Category ↑↓	Details
Owner	Grants full access to manage all resources, including the ability to a...	BuiltInRole	General	View
Contributor	Grants full access to manage all resources, but does not allow you to ...	BuiltInRole	General	View
Reader	View all resources, but does not allow you to make any changes.	BuiltInRole	General	View
AcrDelete	acr delete	BuiltInRole	Containers	View
AcrImageSigner	acr image signer	BuiltInRole	Containers	View
AcrPull	acr pull	BuiltInRole	Containers	View
AcrPush	acr push	BuiltInRole	Containers	View
AcrQuarantineReader	acr quarantine data reader	BuiltInRole	Containers	View
AcrQuarantineWriter	acr quarantine data writer	BuiltInRole	Containers	View

[Review + assign](#) [Previous](#) [Next](#)

After a few moments, the security principal is assigned the role at the selected scope.

Azure Cloud Shell

The following example uses [az role assignment create](#) to assign the Virtual Machine Administrator Login role to the VM for your current Azure user. You obtain the username of your current Azure account by using [az account show](#), and you set the scope to the VM created in a previous step by using [az vm show](#).

You can also assign the scope at a resource group or subscription level. Normal Azure RBAC inheritance permissions apply.

```
Azure CLI

username=$(az account show --query user.name --output tsv)
rg=$(az group show --resource-group myResourceGroup --query id -o tsv)

az role assignment create \
    --role "Virtual Machine Administrator Login" \
    --assignee $username \
    --scope $rg
```

ⓘ Note

If your Microsoft Entra domain and login username domain don't match, you must specify the object ID of your user account by using `--assignee-object-id`, not just

the username for `--assignee`. You can obtain the object ID for your user account by using [az ad user list](#).

For more information on how to use Azure RBAC to manage access to your Azure subscription resources, see [Steps to assign an Azure role](#).

Install the SSH extension for the Azure CLI

If you're using Azure Cloud Shell, no other setup is needed because both the minimum required version of the Azure CLI and the SSH extension for the Azure CLI are already included in the Cloud Shell environment.

Run the following command to add the SSH extension for the Azure CLI:

Azure CLI

```
az extension add --name ssh
```

The minimum version required for the extension is 0.1.4. Check the installed version by using the following command:

Azure CLI

```
az extension show --name ssh
```

Enforce Conditional Access policies

You can enforce Conditional Access policies that are enabled with Microsoft Entra login, such as:

- Requiring multifactor authentication.
- Requiring a compliant or Microsoft Entra hybrid joined device for the device running the SSH client.
- Checking for risks before authorizing access to Linux VMs in Azure.

The application that appears in the Conditional Access policy is called *Azure Linux VM Sign-In*.

 Note

Conditional Access policy enforcement that requires device compliance or Microsoft Entra hybrid join on the device that's running the SSH client works only with the Azure CLI that's running on Windows and macOS. It's not supported when you're using the Azure CLI on Linux or Azure Cloud Shell.

Missing application

If the Azure Linux VM Sign-In application is missing from Conditional Access, make sure the application isn't in the tenant:

1. Sign in to the [Microsoft Entra admin center](#) as at least a **Cloud Application Administrator**.
2. Browse to **Identity > Applications > Enterprise applications**.
3. Remove the filters to see all applications, and search for **Virtual Machine**. If you don't see Microsoft Azure Linux Virtual Machine Sign-In as a result, the service principal is missing from the tenant.

Log in by using a Microsoft Entra user account to SSH into the Linux VM

Log in by using the Azure CLI

Enter `az login`. This command opens a browser window, where you can sign in by using your Microsoft Entra account.

```
Azure CLI
```

```
az login
```

Then enter `az ssh vm`. The following example automatically resolves the appropriate IP address for the VM.

```
Azure CLI
```

```
az ssh vm -n myVM -g AzureADLinuxVM
```

If you're prompted, enter your Microsoft Entra login credentials at the login page, perform multifactor authentication, and/or satisfy device checks. You'll be prompted only if your the Azure CLI session doesn't already meet any required Conditional Access

criteria. Close the browser window, return to the SSH prompt, and you'll be automatically connected to the VM.

You're now signed in to the Linux virtual machine with the role permissions as assigned, such as VM User or VM Administrator. If your user account is assigned the Virtual Machine Administrator Login role, you can use sudo to run commands that require root privileges.

Log in by using Azure Cloud Shell

You can use Azure Cloud Shell to connect to VMs without needing to install anything locally to your client machine. Start Cloud Shell by selecting the shell icon in the upper-right corner of the Azure portal.

Cloud Shell automatically connects to a session in the context of the signed-in user. Now run `az login` again and go through the interactive sign-in flow:

```
Azure CLI  
  
az login
```

Then you can use the normal `az ssh vm` commands to connect by using the name and resource group or IP address of the VM:

```
Azure CLI  
  
az ssh vm -n myVM -g AzureADLinuxVM
```

ⓘ Note

Conditional Access policy enforcement that requires device compliance or Microsoft Entra hybrid join is not supported when you're using Azure Cloud Shell.

Log in by using the Microsoft Entra service principal to SSH into the Linux VM

The Azure CLI supports authenticating with a service principal instead of a user account. Because service principals aren't tied to any particular user, customers can use them to SSH into a VM to support any automation scenarios they might have. The service

principal must have VM Administrator or VM User rights assigned. Assign permissions at the subscription or resource group level.

The following example will assign VM Administrator rights to the service principal at the resource group level. Replace the placeholders for service principal object ID, subscription ID, and resource group name.

Azure CLI

```
az role assignment create \
    --role "Virtual Machine Administrator Login" \
    --assignee-object-id <service-principal-objectid> \
    --assignee-principal-type ServicePrincipal \
    --scope "/subscriptions/<subscription-id>/resourceGroups/<resourcegroup-name>"
```

Use the following example to authenticate to the Azure CLI by using the service principal. For more information, see the article [Sign in to the Azure CLI with a service principal](#).

Azure CLI

```
az login --service-principal -u <sp-app-id> -p <password-or-cert> --tenant <tenant-id>
```

When authentication with a service principal is complete, use the normal the Azure CLI SSH commands to connect to the VM:

Azure CLI

```
az ssh vm -n myVM -g AzureADLinuxVM
```

Export the SSH configuration for use with SSH clients that support OpenSSH

Sign in to Azure Linux VMs with Microsoft Entra ID supports exporting the OpenSSH certificate and configuration. That means you can use any SSH clients that support OpenSSH-based certificates to sign in through Microsoft Entra ID. The following example exports the configuration for all IP addresses assigned to the VM:

Azure CLI

```
az ssh config --file ~/.ssh/config -n myVM -g AzureADLinuxVM
```

Alternatively, you can export the configuration by specifying just the IP address. Replace the IP address in the following example with the public or private IP address for your VM. (You must bring your own connectivity for private IPs.) Enter `az ssh config -h` for help with this command.

Azure CLI

```
az ssh config --file ~/.ssh/config --ip 10.11.123.456
```

You can then connect to the VM through normal OpenSSH usage. Connection can be done through any SSH client that uses OpenSSH.

Run sudo with Microsoft Entra login

After users who are assigned the VM Administrator role successfully SSH into a Linux VM, they'll be able to run sudo with no other interaction or authentication requirement. Users who are assigned the VM User role won't be able to run sudo.

Connect to VMs in virtual machine scale sets

Virtual machine scale sets are supported, but the steps are slightly different for enabling and connecting to VMs in a virtual machine scale set:

1. Create a virtual machine scale set or choose one that already exists. Enable a system-assigned managed identity for your virtual machine scale set:

Azure CLI

```
az vmss identity assign --name myVMSS --resource-group AzureADLinuxVM
```

2. Install the Microsoft Entra extension on your virtual machine scale set:

Azure CLI

```
az vmss extension set --publisher Microsoft.Azure.ActiveDirectory --  
name AADSSHLoginForLinux --resource-group AzureADLinuxVM --vmss-name  
myVMSS
```

Virtual machine scale sets usually don't have public IP addresses. You must have connectivity to them from another machine that can reach their Azure virtual network. This example shows how to use the private IP of a VM in a virtual machine scale set to connect from a machine in the same virtual network:

Azure CLI

```
az ssh vm --ip 10.11.123.456
```

(!) Note

You can't automatically determine the virtual machine scale set VM's IP addresses by using the `--resource-group` and `--name` switches.

Migrate from the previous (preview) version

If you're using the previous version of Microsoft Entra login for Linux that was based on device code flow, complete the following steps by using the Azure CLI:

1. Uninstall the AADLoginForLinux extension on the VM:

Azure CLI

```
az vm extension delete -g MyResourceGroup --vm-name MyVm -n  
AADLoginForLinux
```

(!) Note

Uninstallation of the extension can fail if there are any Microsoft Entra users currently logged in on the VM. Make sure all users are logged out first.

2. Enable system-assigned managed identity on your VM:

Azure CLI

```
az vm identity assign -g myResourceGroup -n myVm
```

3. Install the AADSSHLoginForLinux extension on the VM:

Azure CLI

```
az vm extension set \
--publisher Microsoft.Azure.ActiveDirectory \
--name AADSSHLoginForLinux \
--resource-group myResourceGroup \
--vm-name myVM
```

Use Azure Policy to meet standards and assess compliance

Use Azure Policy to:

- Ensure that Microsoft Entra login is enabled for your new and existing Linux virtual machines.
- Assess compliance of your environment at scale on a compliance dashboard.

With this capability, you can use many levels of enforcement. You can flag new and existing Linux VMs within your environment that don't have Microsoft Entra login enabled. You can also use Azure Policy to deploy the Microsoft Entra extension on new Linux VMs that don't have Microsoft Entra login enabled, as well as remediate existing Linux VMs to the same standard.

In addition to these capabilities, you can use Azure Policy to detect and flag Linux VMs that have unapproved local accounts created on their machines. To learn more, review [Azure Policy](#).

Troubleshoot sign-in issues

Use the following sections to correct common errors that can happen when you try to SSH with Microsoft Entra credentials.

Couldn't retrieve token from local cache

If you get a message that says the token couldn't be retrieved from the local cache, you must run `az login` again and go through an interactive sign-in flow. Review the section about [logging in by using Azure Cloud Shell](#).

Access denied: Azure role not assigned

If you see an "Azure role not assigned" error on your SSH prompt, verify that you've configured Azure RBAC policies for the VM that grants the user either the Virtual

Machine Administrator Login role or the Virtual Machine User Login role. If you're having problems with Azure role assignments, see the article [Troubleshoot Azure RBAC](#).

Problems deleting the old (AADLoginForLinux) extension

If the uninstallation scripts fail, the extension might get stuck in a transitioning state. When this happens, the extension can leave packages that it's supposed to uninstall during its removal. In such cases, it's better to manually uninstall the old packages and then try to run the `az vm extension delete` command.

To uninstall old packages:

1. Log in as a local user with admin privileges.
2. Make sure there are no logged-in Microsoft Entra users. Call the `who -u` command to see who is logged in. Then use `sudo kill <pid>` for all session processes that the previous command reported.
3. Run `sudo apt remove --purge aadlogin` (Ubuntu/Debian), `sudo yum remove aadlogin` (RHEL), or `sudo zypper remove aadlogin` (openSUSE or SLES).
4. If the command fails, try the low-level tools with scripts disabled:
 - a. For Ubuntu/Debian, run `sudo dpkg --purge aadlogin`. If it's still failing because of the script, delete the `/var/lib/dpkg/info/aadlogin.prerm` file and try again.
 - b. For everything else, run `rpm -e --noscripts aadlogin`.
5. Repeat steps 3-4 for package `aadlogin-selinux`.

Extension installation errors

Installation of the AADSSHLoginForLinux VM extension to existing computers might fail with one of the following known error codes.

Non-zero exit code 22

If you get exit code 22, the status of the AADSSHLoginForLinux VM extension shows as **Transitioning** in the portal.

This failure happens because a system-assigned managed identity is required.

The solution is to:

1. Uninstall the failed extension.
2. Enable a system-assigned managed identity on the Azure VM.
3. Run the extension installation command again.

Non-zero exit code 23

If you get exit code 23, the status of the AADSSHLoginForLinux VM extension shows as **Transitioning** in the portal.

This failure happens when the older AADLoginForLinux VM extension is still installed.

The solution is to uninstall the older AADLoginForLinux VM extension from the VM. The status of the new AADSSHLoginForLinux VM extension will then change to **Provisioning succeeded** in the portal.

Installation failures when using an HTTP proxy

The extension needs an HTTP connection to install packages and check for the existence of a system identity. It runs in the context of `walinuxagent.service` and requires a change to let the agent know about the proxy settings. Open

`/lib/systemd/system/walinuxagent.service` file on the target machine and add the following line after `[Service]`:

```
[Service]
Environment="http_proxy=http://proxy.example.com:80/"
Environment="https_proxy=http://proxy.example.com:80/"
Environment="no_proxy=169.254.169.254"
```

Restart the agent (`sudo systemctl restart walinuxagent`). Now try again.

The `az ssh vm` command fails with `KeyError access_token`

If the `az ssh vm` command fails, you're using an outdated version of the Azure CLI client.

The solution is to upgrade the Azure CLI client to version 2.21.0 or later.

SSH connection is closed

After a user successfully signs in by using `az login`, connection to the VM through `az ssh vm -ip <address>` or `az ssh vm --name <vm_name> -g <resource_group>` might fail with "Connection closed by <ip_address> port 22."

One cause for this error is that the user isn't assigned to the Virtual Machine Administrator Login or Virtual Machine User Login role within the scope of this VM. In

that case, the solution is to add the user to one of those Azure RBAC roles within the scope of this VM.

This error can also happen if the user is in a required Azure RBAC role, but the system-assigned managed identity has been disabled on the VM. In that case, perform these actions:

1. Enable the system-assigned managed identity on the VM.
2. Allow several minutes to pass before the user tries to connect by using `az ssh vm --ip <ip_address>`.

Connection problems with virtual machine scale sets

VM connections with virtual machine scale sets can fail if the scale set instances are running an old model.

Upgrading scale set instances to the latest model might resolve the problem, especially if an upgrade hasn't been done since the Microsoft Entra Login extension was installed. Upgrading an instance applies a standard scale set configuration to the individual instance.

AllowGroups or DenyGroups statements in `sshd_config` cause the first sign in to fail for Microsoft Entra users

If `sshd_config` contains either `AllowGroups` or `DenyGroups` statements, the first login fails for Microsoft Entra users. If the statement was added after users have already had a successful login, they can log in.

One solution is to remove `AllowGroups` and `DenyGroups` statements from `sshd_config`.

Another solution is to move `AllowGroups` and `DenyGroups` to a `match user` section in `sshd_config`. Make sure the match template excludes Microsoft Entra users.

Getting Permission Denied when trying to connect from Azure Shell to Linux Red Hat/Oracle 7.X VM.

The OpenSSH server version in the target VM 7.4 is too old. Version incompatible with OpenSSH client version 8.8. Refer to [RSA SHA256 certificates no longer work](#) for more information.

Workaround:

- Adding option "PubkeyAcceptedKeyTypes= +ssh-rsa-cert-v01@openssh.com" in the az ssh vm command.

Azure CLI

```
az ssh vm -n myVM -g MyResourceGroup -- -A -o "PubkeyAcceptedKeyTypes= +ssh-rsa-cert-v01@openssh.com"
```

- Adding the option "PubkeyAcceptedKeyTypes= +ssh-rsa-cert-v01@openssh.com" in the /home/<user>/.ssh/config file.

Add the "PubkeyAcceptedKeyTypes +ssh-rsa-cert-v01@openssh.com" into the client config file.

config

```
Host *
PubkeyAcceptedKeyTypes +ssh-rsa-cert-v01@openssh.com
```

Next steps

- [What is a device identity?](#)
- [Common Conditional Access policies](#)

Feedback

Was this page helpful?

 Yes

 No

[Provide product feedback](#) ↗

Sign in to a Windows virtual machine in Azure by using Microsoft Entra ID including passwordless

Article • 10/21/2024

Organizations can improve the security of Windows virtual machines (VMs) in Azure by integrating with Microsoft Entra authentication. You can now use Microsoft Entra ID as a core authentication platform to Remote Desktop Protocol (RDP) into *Windows Server 2019 Datacenter edition* and later, or *Windows 10 1809* and later. You can then centrally control and enforce Azure role-based access control (RBAC) and Conditional Access policies that allow or deny access to the VMs.

This article shows you how to create and configure a Windows VM and log in by using Microsoft Entra ID-based authentication.

There are many security benefits of using Microsoft Entra ID-based authentication to sign in to Windows VMs in Azure. They include:

- Use Microsoft Entra authentication including passwordless to sign in to Windows VMs in Azure.
- Reduce reliance on local administrator accounts.
- Password complexity and password lifetime policies that you configure for Microsoft Entra ID also help secure Windows VMs.
- With Azure RBAC:
 - Specify who can sign in to a VM as a regular user or with administrator privileges.
 - When users join or leave your team, you can update the Azure RBAC policy for the VM to grant access as appropriate.
 - When employees leave your organization and their user accounts are disabled or removed from Microsoft Entra ID, they no longer have access to your resources.
- Configure Conditional Access policies to "phishing resistant MFA" using require authentication strength grant control or require multifactor authentication and other signals, such as user sign-in risk, before you can RDP into Windows VMs.
- Use Azure Policy to deploy and audit policies to require Microsoft Entra login for Windows VMs and to flag the use of unapproved local accounts on the VMs.

- Use Intune to automate and scale Microsoft Entra join with mobile device management (MDM) autoenrollment of Azure Windows VMs that are part of your virtual desktop infrastructure (VDI) deployments.

MDM autoenrollment requires Microsoft Entra ID P1 licenses. Windows Server VMs don't support MDM enrollment.

Note

After you enable this capability, your Windows VMs in Azure will be Microsoft Entra joined. You cannot join them to another domain, like on-premises Active Directory or Microsoft Entra Domain Services. If you need to do so, disconnect the VM from Microsoft Entra ID by uninstalling the extension.

Requirements

Supported Azure regions and Windows distributions

This feature currently supports the following Windows distributions:

- Windows Server 2019 Datacenter and later
- Windows 10 1809 and later
- Windows 11 21H2 and later

This feature is now available in the following Azure clouds:

- Azure Global
- Azure Government
- Microsoft Azure operated by 21Vianet

Network requirements

To enable Microsoft Entra authentication for your Windows VMs in Azure, you need to ensure that your VM's network configuration permits outbound access to the following endpoints over TCP port 443.

Azure Global:

- <https://enterpriseregistration.windows.net>: For device registration.
- <http://169.254.169.254>: Azure Instance Metadata Service endpoint.
- <https://login.microsoftonline.com>: For authentication flows.

- <https://pas.windows.net>: For Azure RBAC flows.

Azure Government:

- <https://enterpriseregistration.microsoftonline.us>: For device registration.
- <http://169.254.169.254>: Azure Instance Metadata Service endpoint.
- <https://login.microsoftonline.us>: For authentication flows.
- <https://pasff.usgovcloudapi.net>: For Azure RBAC flows.

Microsoft Azure operated by 21Vianet:

- <https://enterpriseregistration.partner.microsoftonline.cn>: For device registration.
- <http://169.254.169.254>: Azure Instance Metadata Service endpoint.
- <https://login.chinacloudapi.cn>: For authentication flows.
- <https://pas.chinacloudapi.cn>: For Azure RBAC flows.

Authentication requirements

[Microsoft Entra Guest accounts](#) can't connect to Azure VMs or Azure Bastion enabled VMs via Microsoft Entra authentication.

Enable Microsoft Entra login for a Windows VM in Azure

To use Microsoft Entra login for a Windows VM in Azure, you must:

1. Enable the Microsoft Entra login option for the VM.
2. Configure Azure role assignments for users who are authorized to sign in to the VM.

There are two ways to enable Microsoft Entra login for your Windows VM:

- The Azure portal, when you're creating a Windows VM.
- Azure Cloud Shell, when you're creating a Windows VM or using an existing Windows VM.

 **Note**

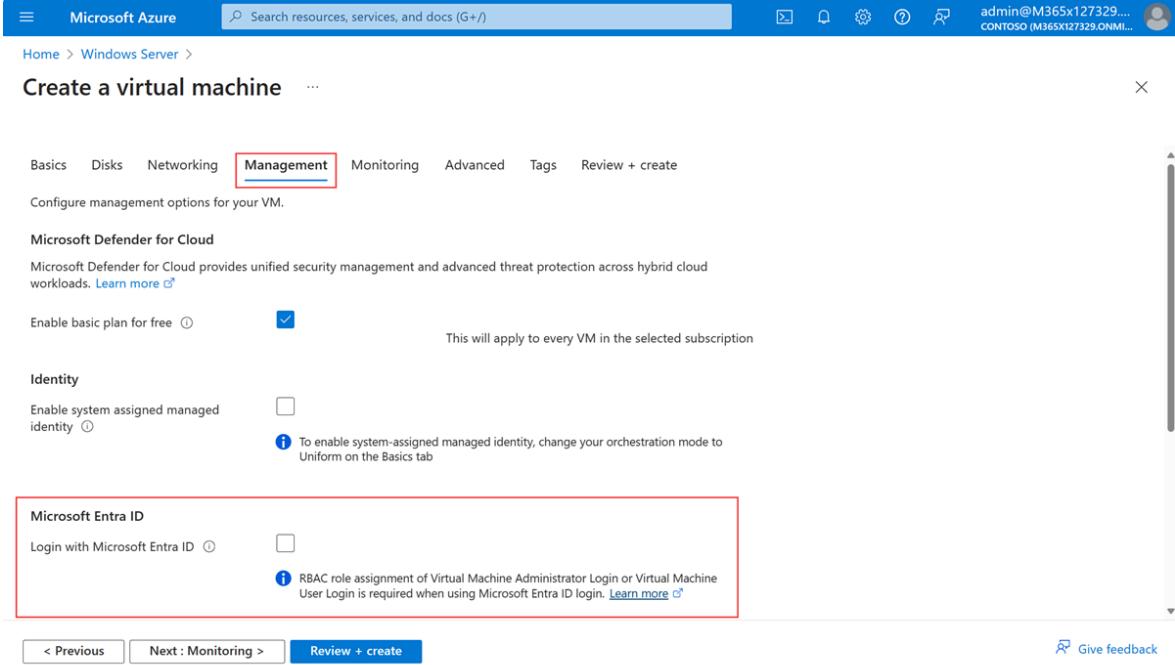
If a device object with the same displayName as the hostname of a VM where an extension is installed exists, the VM fails to join Microsoft Entra ID with a hostname duplication error. Avoid duplication by [modifying the hostname](#).

Azure portal

You can enable Microsoft Entra login for VM images in Windows Server 2019 Datacenter or Windows 10 1809 and later.

To create a Windows Server 2019 Datacenter VM in Azure with Microsoft Entra login:

1. Sign in to the [Azure portal](#) by using an account that has access to create VMs, and select **+ Create a resource**.
2. In the **Search the Marketplace** search bar, type **Windows Server**.
3. Select **Windows Server**, and then choose **Windows Server 2019 Datacenter** from the **Select a software plan** dropdown list.
4. Select **Create**.
5. On the **Management** tab, select the **Login with Microsoft Entra ID** checkbox in the **Microsoft Entra ID** section.



The screenshot shows the Azure portal interface for creating a new virtual machine. The top navigation bar includes 'Microsoft Azure', a search bar, and user information. The main title is 'Create a virtual machine'. Below it, the 'Management' tab is selected, indicated by a red border. The 'Identity' section contains a checkbox for 'Enable system assigned managed identity', which is unchecked. The 'Microsoft Entra ID' section, also highlighted with a red box, contains a checked checkbox for 'Login with Microsoft Entra ID'. A note below it states: 'RBAC role assignment of Virtual Machine Administrator Login or Virtual Machine User Login is required when using Microsoft Entra ID login.' At the bottom, there are navigation buttons for '< Previous', 'Next : Monitoring >', and 'Review + create'.

6. Make sure that **System assigned managed identity** in the **Identity** section is selected. This action should happen automatically after you enable login with Microsoft Entra ID.

7. Go through the rest of the experience of creating a virtual machine. You have to create an administrator username and password for the VM.

① Note

To sign in to the VM by using your Microsoft Entra credentials, you first need to [configure role assignments](#) for the VM.

Azure Cloud Shell

Azure Cloud Shell is a free, interactive shell that you can use to run the steps in this article. Common Azure tools are preinstalled and configured in Cloud Shell for you to use with your account. Just select the **Copy** button to copy the code, paste it in Cloud Shell, and then select the Enter key to run it. There are a few ways to open Cloud Shell:

- Select **Try It** in the upper-right corner of a code block.
- Open Cloud Shell in your browser.
- Select the Cloud Shell button on the menu in the upper-right corner of the [Azure portal](#).

This article requires you to run Azure CLI version 2.0.31 or later. Run `az --version` to find the version. If you need to install or upgrade, see the article [Install the Azure CLI](#).

1. Create a resource group by running [az group create](#).
2. Create a VM by running [az vm create](#). Use a supported distribution in a supported region.
3. Install the Microsoft Entra login VM extension.

The following example deploys a VM named `myVM` (that uses `Win2019Datacenter`) into a resource group named `myResourceGroup`, in the `southcentralus` region. In this example and the next one, you can provide your own resource group and VM names as needed.

Azure CLI

```
az group create --name myResourceGroup --location southcentralus

az vm create \
    --resource-group myResourceGroup \
    --name myVM \
    --image Win2019Datacenter \
    --assign-identity \
    --admin-username azureuser \
    --admin-password yourpassword
```

Note

You must enable system-assigned managed identity on your virtual machine before you install the Microsoft Entra login VM extension. Managed Identities are stored in a single Microsoft Entra tenant and currently do not support cross directory scenarios.

It takes a few minutes to create the VM and supporting resources.

Finally, install the Microsoft Entra login VM extension to enable Microsoft Entra login for Windows VMs. VM extensions are small applications that provide post-deployment configuration and automation tasks on Azure Virtual Machines. Use [az vm extension set](#) to install the AADLoginForWindows extension on the VM named `myVM` in the `myResourceGroup` resource group.

You can install the AADLoginForWindows extension on an existing Windows Server 2019 or Windows 10 1809 and later VM to enable it for Microsoft Entra authentication. The following example uses the Azure CLI to install the extension:

Azure CLI

```
az vm extension set \
    --publisher Microsoft.Azure.ActiveDirectory \
    --name AADLoginForWindows \
    --resource-group myResourceGroup \
    --vm-name myVM
```

After the extension is installed on the VM, `provisioningState` shows `Succeeded`.

Configure role assignments for the VM

Now that you've created the VM, you need to assign one of the following Azure roles to determine who can sign in to the VM. To assign these roles, you must have the [Virtual Machine Data Access Administrator](#) role, or any role that includes the `Microsoft.Authorization/roleAssignments/write` action such as the [Role Based Access Control Administrator](#) role. However, if you use a different role than Virtual Machine Data Access Administrator, we recommend you [add a condition to reduce the permission to create role assignments](#).

- **Virtual Machine Administrator Login:** Users who have this role assigned can sign in to an Azure virtual machine with administrator privileges.

- **Virtual Machine User Login:** Users who have this role assigned can sign in to an Azure virtual machine with regular user privileges.

To allow a user to sign in to the VM over RDP, you must assign the Virtual Machine Administrator Login or Virtual Machine User Login role to the Virtual Machine resource.

 **Note**

Manually elevating a user to become a local administrator on the VM by adding the user to a member of the local administrators group or by running `net localgroup administrators /add "AzureAD\UserUpn"` command is not supported. You need to use Azure roles above to authorize VM login.

An Azure user who has the Owner or Contributor role assigned for a VM doesn't automatically have privileges to sign in to the VM over RDP. The reason is to provide audited separation between the set of people who control virtual machines and the set of people who can access virtual machines.

There are two ways to configure role assignments for a VM:

- Microsoft Entra admin center experience
- Azure Cloud Shell experience

 **Note**

The Virtual Machine Administrator Login and Virtual Machine User Login roles use `dataActions`, so they can't be assigned at the management group scope. Currently, you can assign these roles only at the subscription, resource group, or resource scope.

Microsoft Entra admin center

To configure role assignments for your Microsoft Entra ID-enabled Windows Server 2019 Datacenter VMs:

1. For **Resource Group**, select the resource group that contains the VM and its associated virtual network, network interface, public IP address, or load balancer resource.
2. Select **Access control (IAM)**.
3. Select **Add > Add role assignment** to open the **Add role assignment** page.

4. Assign the following role. For detailed steps, see [Assign Azure roles by using the Azure portal](#).

[+] Expand table

Setting	Value
Role	Virtual Machine Administrator Login or Virtual Machine User Login
Assign access to	User, group, service principal, or managed identity

The screenshot shows the 'Add role assignment' dialog in the Azure portal. At the top, there's a breadcrumb navigation (Home > Add role assignment) and a close button (X). Below that is a search bar labeled 'Search by role name or description'. Underneath the search bar are three filter buttons: 'Type : All', 'Category : All', and another 'All' button. A descriptive text states: 'A role definition is a collection of permissions. You can use the built-in roles or you can create your own custom roles. [Learn more](#)'.

Name ↑↓	Description ↑↓	Type ↑↓	Category ↑↓	Details
Owner	Grants full access to manage all resources, including the ability to a...	BuiltInRole	General	View
Contributor	Grants full access to manage all resources, but does not allow you ...	BuiltInRole	General	View
Reader	View all resources, but does not allow you to make any changes.	BuiltInRole	General	View
AcrDelete	acr delete	BuiltInRole	Containers	View
AcrImageSigner	acr image signer	BuiltInRole	Containers	View
AcrPull	acr pull	BuiltInRole	Containers	View
AcrPush	acr push	BuiltInRole	Containers	View
AcrQuarantineReader	acr quarantine data reader	BuiltInRole	Containers	View
AcrQuarantineWriter	acr quarantine data writer	BuiltInRole	Containers	View

At the bottom of the dialog are three buttons: 'Review + assign', 'Previous', and 'Next'.

Azure Cloud Shell

The following example uses `az role assignment create` to assign the Virtual Machine Administrator Login role to the VM for your current Azure user. You obtain the username of your current Azure account by using `az account show`, and you set the scope to the VM created in a previous step by using `az vm show`.

You can also assign the scope at a resource group or subscription level. Normal Azure RBAC inheritance permissions apply.

Azure CLI

```
$username=$(az account show --query user.name --output tsv)
$rg=$(az group show --resource-group myResourceGroup --query id -o tsv)

az role assignment create \
--role "Virtual Machine Administrator Login" \
```

```
--assignee $username \
--scope $rg
```

ⓘ Note

If your Microsoft Entra domain and login username domain don't match, you must specify the object ID of your user account by using `--assignee-object-id`, not just the username for `--assignee`. You can obtain the object ID for your user account by using [az ad user list](#).

For more information about how to use Azure RBAC to manage access to your Azure subscription resources, see the following articles:

- [Assign Azure roles by using the Azure CLI](#)
- [Assign Azure roles by using the Azure portal](#)
- [Assign Azure roles by using Azure PowerShell](#)

Log in by using Microsoft Entra credentials to a Windows VM

You can sign in over RDP using one of two methods:

1. Passwordless using any of the supported Microsoft Entra credentials (recommended)
2. Password/limited passwordless using Windows Hello for Business deployed using certificate trust model

Log in using passwordless authentication with Microsoft Entra ID

To use passwordless authentication for your Windows VMs in Azure, you need the Windows client machine and the session host (VM) on the following operating systems:

- Windows 11 with [2022-10 Cumulative Updates for Windows 11 \(KB5018418\)](#) or later installed.
- Windows 10, version 20H2 or later with [2022-10 Cumulative Updates for Windows 10 \(KB5018410\)](#) or later installed.
- Windows Server 2022 with [2022-10 Cumulative Update for Microsoft server operating system \(KB5018421\)](#) or later installed.

Note

When using the **web account to sign in to the remote computer** option, there is no requirement for the local device to be joined to a domain or Microsoft Entra ID.

To connect to the remote computer:

- Launch **Remote Desktop Connection** from Windows Search, or by running `mstsc.exe`.
- Select **Use a web account to sign in to the remote computer** option in the **Advanced** tab. This option is equivalent to the `enablerdsaadauth` RDP property. For more information, see [Supported RDP properties with Remote Desktop Services](#).
- Specify the name of the remote computer and select **Connect**.

Important

IP address cannot be used with **Use a web account to sign in to the remote computer** option. The name must match the hostname of the remote device in Microsoft Entra ID and be network addressable, resolving to the IP address of the remote device.

- When prompted for credentials, specify your user name in `user@domain.com` format.
- You're then prompted to allow the remote desktop connection when connecting to a new PC. Microsoft Entra remembers up to 15 hosts for 30 days before prompting again. If you see this dialogue, select **Yes** to connect.

Important

If your organization has configured and is using [Microsoft Entra Conditional Access](#), your device must satisfy the Conditional Access requirements to allow connection to the remote computer. Conditional Access policies might be applied to the application **Microsoft Remote Desktop** (`a4a365df-50f1-4397-bc59-1a1564b8bb9c`) for controlled access.

Note

The Windows lock screen in the remote session doesn't support Microsoft Entra authentication tokens or passwordless authentication methods like FIDO keys. The

lack of support for these authentication methods means that users can't unlock their screens in a remote session. When you try to lock a remote session, either through user action or system policy, the session is instead disconnected and the service sends a message to the user explaining they've been disconnected. Disconnecting the session also ensures that when the connection is relaunched after a period of inactivity, Microsoft Entra ID reevaluates the applicable Conditional Access policies.

Log in using password/limited passwordless authentication with Microsoft Entra ID

Important

Remote connection to VMs that are joined to Microsoft Entra ID is allowed only from Windows 10 or later PCs that are either Microsoft Entra registered (minimum required build is 20H1) or Microsoft Entra joined or Microsoft Entra hybrid joined to the *same* directory as the VM. Additionally, to RDP by using Microsoft Entra credentials, users must belong to one of the two Azure roles, Virtual Machine Administrator Login or Virtual Machine User Login.

If you're using a Microsoft Entra registered Windows 10 or later PC, you must enter credentials in the `AzureAD\UPN` format (for example, `AzureAD\john@contoso.com`). At this time, you can use Azure Bastion to log in with Microsoft Entra authentication [via the Azure CLI and the native RDP client mstsc](#).

To sign in to your Windows Server 2019 virtual machine by using Microsoft Entra ID:

1. Go to the overview page of the virtual machine that has been enabled with Microsoft Entra login.
2. Select **Connect** to open the **Connect to virtual machine** pane.
3. Select **Download RDP File**.
4. Select **Open** to open the Remote Desktop Connection client.
5. Select **Connect** to open the Windows login dialog.
6. Log in by using your Microsoft Entra credentials.

You're now signed in to the Windows Server 2019 Azure virtual machine with the role permissions as assigned, such as VM User or VM Administrator.

Note

You can save the .RDP file locally on your computer to start future remote desktop connections to your virtual machine, instead of going to the virtual machine overview page in the Azure portal and using the connect option.

Enforce Conditional Access policies

You can enforce Conditional Access policies, such as "phishing resistant MFA" using require authentication strength grant control or multifactor authentication or user sign-in risk check, before you authorize access to Windows VMs in Azure that are enabled with Microsoft Entra login. To apply a Conditional Access policy, you must select the **Microsoft Azure Windows Virtual Machine Sign-in** app from the cloud apps or actions assignment option. Then use sign-in risk as a condition or "phishing resistant MFA" using require authentication strength grant control or require MFA as a control for granting access.

Note

If you require MFA as a control for granting access to the Microsoft Azure Windows Virtual Machine Sign-in app, then you must supply an MFA claim as part of the client that initiates the RDP session to the target Windows VM in Azure. This can be achieved using passwordless authentication method for RDP that satisfies the Conditional Access policies, however if you are using limited passwordless method for RDP then the only way to achieve this on a Windows 10 or later client is to use a Windows Hello for Business PIN or biometric authentication with the RDP client. Support for biometric authentication was added to the RDP client in Windows 10 version 1809. Remote desktop using Windows Hello for Business authentication is available only for deployments that use a certificate trust model. It's currently not available for a key trust model.

Use Azure Policy to meet standards and assess compliance

Use Azure Policy to:

- Ensure that Microsoft Entra login is enabled for your new and existing Windows virtual machines.
- Assess compliance of your environment at scale on a compliance dashboard.

With this capability, you can use many levels of enforcement. You can flag new and existing Windows VMs within your environment that don't have Microsoft Entra login enabled. You can also use Azure Policy to deploy the Microsoft Entra extension on new Windows VMs that don't have Microsoft Entra login enabled, and remediate existing Windows VMs to the same standard.

In addition to these capabilities, you can use Azure Policy to detect and flag Windows VMs that have unapproved local accounts created on their machines. To learn more, review [Azure Policy](#).

Troubleshoot deployment problems

The AADLoginForWindows extension must be installed successfully for the VM to complete the Microsoft Entra join process. If the VM extension fails to be installed correctly, perform the following steps:

1. RDP to the VM by using the local administrator account and examine the *CommandExecution.log* file under *C:\WindowsAzure\Logs\Plugins\Microsoft.Azure.ActiveDirectoryAADLoginForWindows\1.0.0.1*.

 **Note**

If the extension restarts after the initial failure, the log with the deployment error will be saved as *CommandExecution_YYYYMMDDHHMMSSSS.log*.

2. Open a PowerShell window on the VM. Verify that the following queries against the Azure Instance Metadata Service endpoint running on the Azure host return the expected output:

 [Expand table](#)

Command to run	Expected output
<pre>curl.exe -H Metadata:true "http://169.254.169.254/metadata/instance?api-version=2017-08- 01"</pre>	Correct information about the Azure VM
<pre>curl.exe -H Metadata:true "http://169.254.169.254/metadata/identity/info?api-version=2018- 02-01"</pre>	Valid tenant ID associated with the Azure subscription

Command to run	Expected output
<pre>curl.exe -H Metadata:true "https://169.254.169.254/metadata/identity/oauth2/token? resource=urn:ms-drs:enterpriseregistration.windows.net&api- version=2018-02-01"</pre>	<p>Valid access token issued by Microsoft Entra ID for the managed identity that is assigned to this VM</p>

(!) Note

You can decode the access token by using a tool like <https://jwt.ms/>. Verify that the `oid` value in the access token matches the managed identity that's assigned to the VM.

3. Ensure that the required endpoints are accessible from the VM via PowerShell:

- `curl.exe https://login.microsoftonline.com/ -D -`
- `curl.exe https://login.microsoftonline.com/<TenantID>/ -D -`
- `curl.exe https://enterpriseregistration.windows.net/ -D -`
- `curl.exe https://device.login.microsoftonline.com/ -D -`
- `curl.exe https://pas.windows.net/ -D -`

(!) Note

Replace `<TenantID>` with the Microsoft Entra tenant ID that's associated with the Azure subscription. `login.microsoftonline.com/<TenantID>`, `enterpriseregistration.windows.net`, and `pas.windows.net` should return 404 Not Found, which is expected behavior.

4. View the device state by running `dsregcmd /status`. The goal is for the device state to show as `AzureAdJoined : YES`.

(!) Note

Microsoft Entra join activity is captured in Event Viewer under the *User Device Registration\Admin* log at *Event Viewer (local)\Applications and Services Logs\Microsoft\Windows\User Device Registration\Admin*.

If the AADLoginForWindows extension fails with an error code, you can perform the following steps.

Terminal error code 1007 and exit code -2145648574.

Terminal error code 1007 and exit code -2145648574 translate to

`DSREG_E_MSI_TENANTID_UNAVAILABLE`. The extension can't query the Microsoft Entra tenant information.

Connect to the VM as a local administrator and verify that the endpoint returns a valid tenant ID from Azure Instance Metadata Service. Run the following command from an elevated PowerShell window on the VM:

```
curl -H Metadata:true http://169.254.169.254/metadata/identity/info?api-version=2018-02-01
```

This problem can also happen when the VM admin attempts to install the AADLoginForWindows extension, but a system-assigned managed identity hasn't enabled the VM first. In that case, go to the **Identity** pane of the VM. On the **System assigned** tab, verify that the **Status** toggle is set to **On**.

Exit code -2145648607

Exit code -2145648607 translates to `DSREG_AUTOJOIN_DISC_FAILED`. The extension can't reach the `https://enterpriseregistration.windows.net` endpoint.

1. Verify that the required endpoints are accessible from the VM via PowerShell:

- `curl https://login.microsoftonline.com/ -D -`
- `curl https://login.microsoftonline.com/<TenantID>/ -D -`
- `curl https://enterpriseregistration.windows.net/ -D -`
- `curl https://device.login.microsoftonline.com/ -D -`
- `curl https://pas.windows.net/ -D -`

(!) Note

Replace `<TenantID>` with the Microsoft Entra tenant ID that's associated with the Azure subscription. If you need to find the tenant ID, you can hover over your account name or select **Identity > Overview > Properties > Tenant ID**.

Attempts to connect to `enterpriseregistration.windows.net` might return 404 Not Found, which is expected behavior. Attempts to connect to

`pas.windows.net` might prompt for PIN credentials or might return 404 Not Found. (You don't need to enter the PIN.) Either one is sufficient to verify that the URL is reachable.

2. If any of the commands fails with "Could not resolve host <URL>," try running this command to determine which DNS server the VM is using:

```
nslookup <URL>
```

! Note

Replace <URL> with the fully qualified domain names that the endpoints use, such as `login.microsoftonline.com`.

3. See whether specifying a public DNS server allows the command to succeed:

```
nslookup <URL> 208.67.222.222
```

4. If necessary, change the DNS server that's assigned to the network security group that the Azure VM belongs to.

Exit code 51

Exit code 51 translates to "This extension is not supported on the VM's operating system."

The AADLoginForWindows extension is intended to be installed only on Windows Server 2019 or Windows 10 (Build 1809 or later). Ensure that your version or build of Windows is supported. If it isn't supported, uninstall the extension.

Troubleshoot sign-in problems

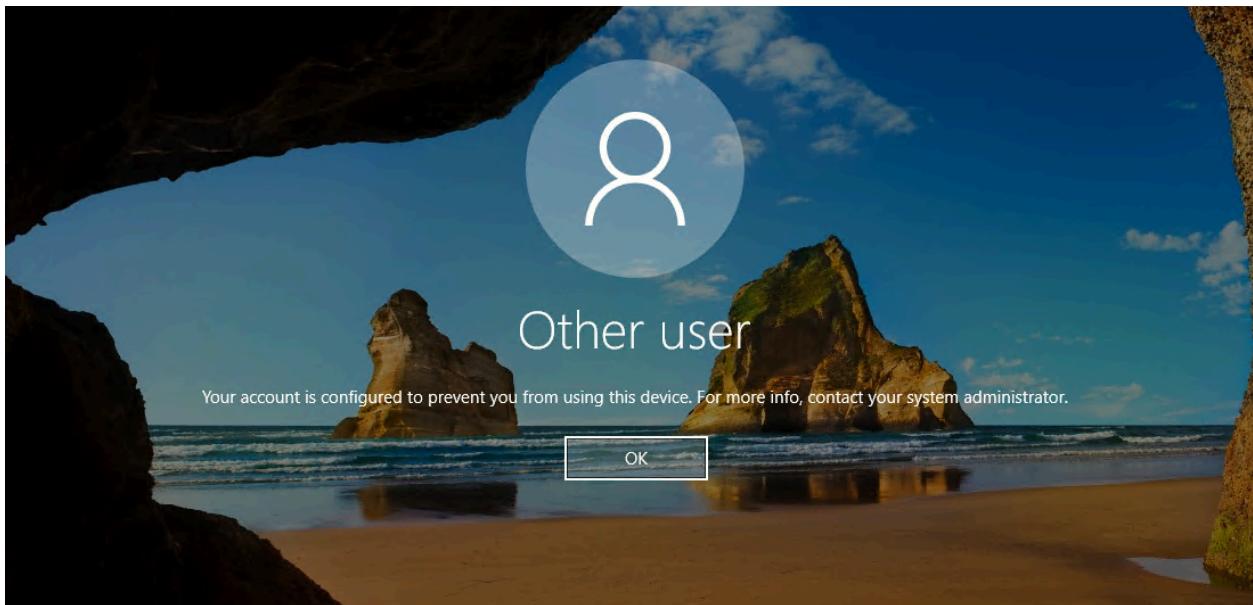
Use the following information to correct sign-in problems.

You can view the device and single sign-on (SSO) state by running `dsregcmd /status`. The goal is for the device state to show as `AzureAdJoined : YES` and for the SSO state to show `AzureAdPrt : YES`.

RDP sign-in via Microsoft Entra accounts is captured in Event Viewer under the *Applications and Services Logs\Microsoft\Windows\AAD\Operational* event logs.

Azure role not assigned

You might get the following error message when you initiate a remote desktop connection to your VM: "Your account is configured to prevent you from using this device. For more info, contact your system administrator."



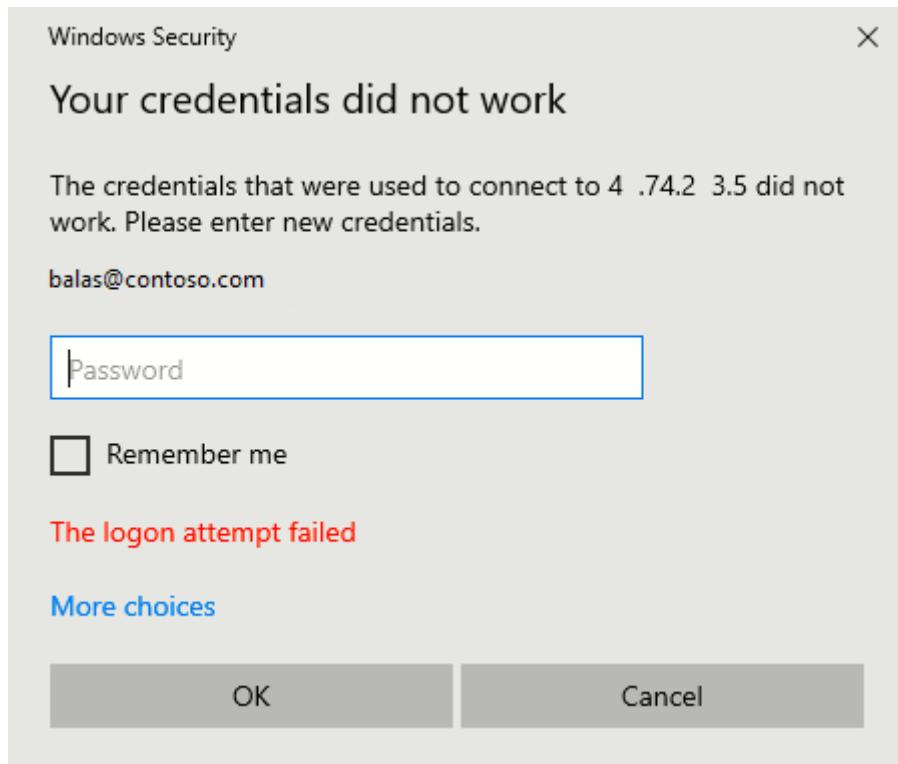
Verify that you've [configured Azure RBAC policies](#) for the VM that grant the user the Virtual Machine Administrator Login or Virtual Machine User Login role.

 **Note**

If you're having problems with Azure role assignments, see [Troubleshoot Azure RBAC](#).

Unauthorized client or password change required

You might get the following error message when you initiate a remote desktop connection to your VM: "Your credentials did not work."



Try these solutions:

- The Windows 10 or later PC that you're using to initiate the remote desktop connection must be Microsoft Entra joined, or Microsoft Entra hybrid joined to the same Microsoft Entra directory. For more information about device identity, see the article [What is a device identity?](#).

 **Note**

Windows 10 Build 20H1 added support for a Microsoft Entra registered PC to initiate an RDP connection to your VM. When you're using a PC that's Microsoft Entra registered (not Microsoft Entra joined or Microsoft Entra hybrid joined) as the RDP client to initiate connections to your VM, you must enter credentials in the format `AzureAD\UPN` (for example, `AzureAD\john@contoso.com`).

Verify that the `AADLoginForWindows` extension wasn't uninstalled after the Microsoft Entra join finished.

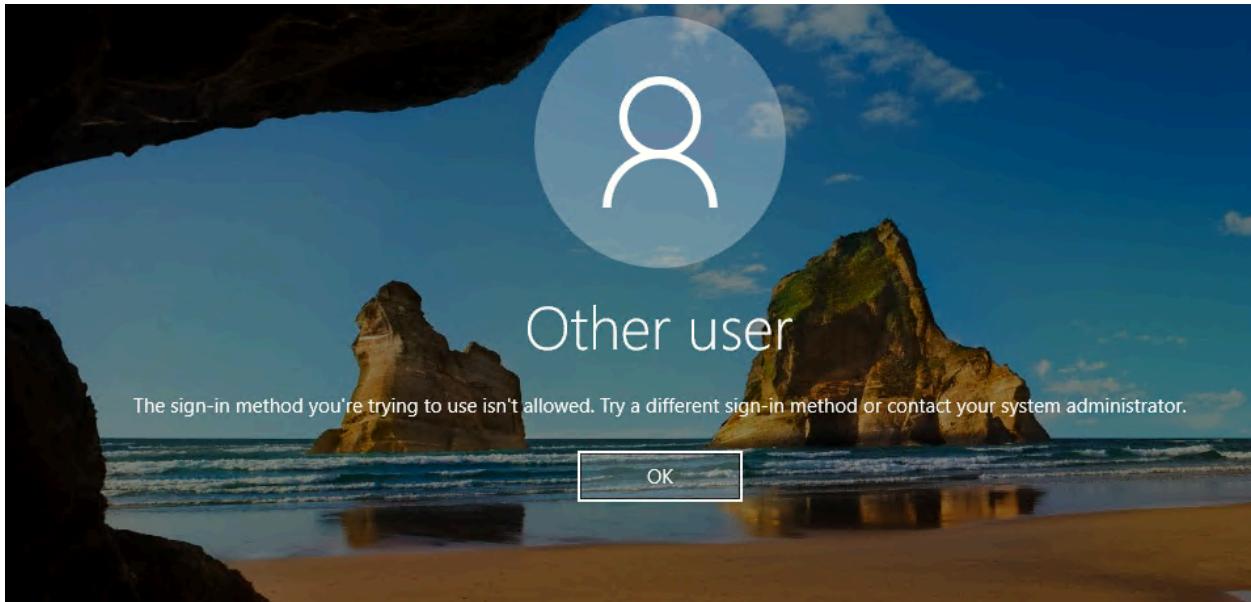
Also, make sure that the security policy **Network security: Allow PKU2U authentication requests to this computer to use online identities** is enabled on both the server *and* the client.

- Verify that the user doesn't have a temporary password. Temporary passwords can't be used to sign in to a remote desktop connection.

Sign in with the user account in a web browser. For instance, sign in to the [Azure portal](#) in a private browsing window. If you're prompted to change the password, set a new password. Then try connecting again.

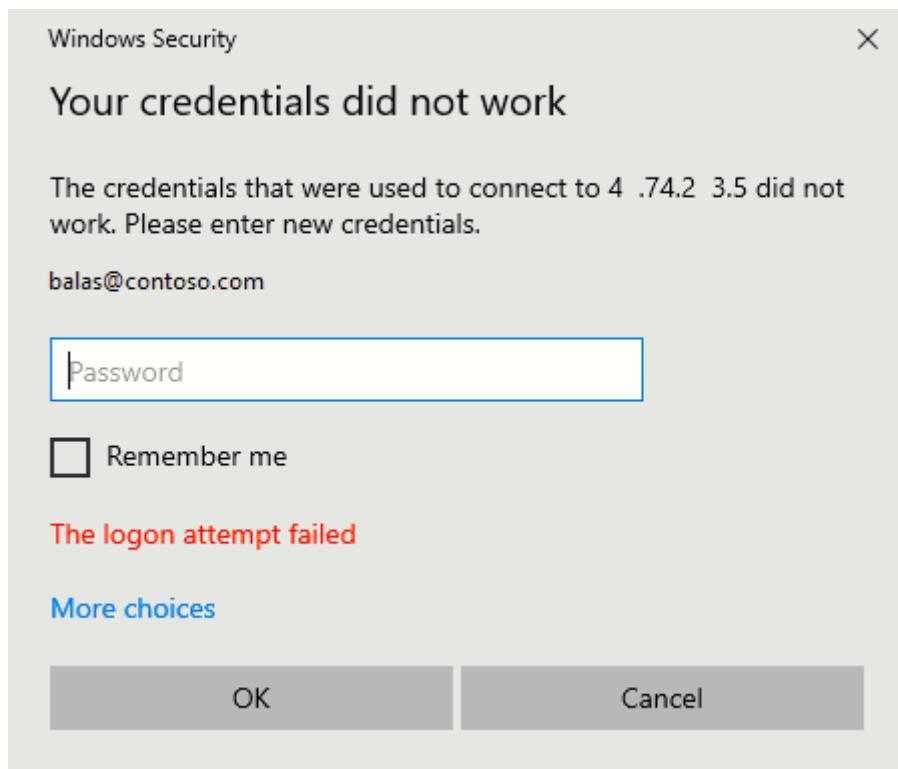
MFA sign-in method required

You might see the following error message when you initiate a remote desktop connection to your VM: "The sign-in method you're trying to use isn't allowed. Try a different sign-in method or contact your system administrator."



If you've configured a Conditional Access policy that requires MFA or legacy per-user Enabled/Enforced Microsoft Entra multifactor authentication before you can access the resource, you need to ensure that the Windows 10 or later PC that's initiating the remote desktop connection to your VM signs in by using a strong authentication method such as Windows Hello. If you don't use a strong authentication method for your remote desktop connection, you see the error.

Another MFA-related error message is the one described previously: "Your credentials did not work."



If you've configured a legacy per-user **Enabled/Enforced Microsoft Entra multifactor authentication** setting and you see the error above, you can resolve the problem by removing the per-user MFA setting. For more information, see the article [Enable per-user Microsoft Entra multifactor authentication to secure sign-in events](#).

If you haven't deployed Windows Hello for Business and if that isn't an option for now, you can configure a Conditional Access policy that excludes the Microsoft Azure Windows Virtual Machine Sign-in app from the list of cloud apps that require MFA. To learn more about Windows Hello for Business, see [Windows Hello for Business overview](#).

Note

Windows Hello for Business PIN authentication with RDP has been supported for several versions of Windows 10. Support for biometric authentication with RDP was added in Windows 10 version 1809. Using Windows Hello for Business authentication during RDP is available for deployments that use a certificate trust model or key trust model.

Share your feedback about this feature or report problems with using it on the [Microsoft Entra feedback forum](#).

Missing application

If the Microsoft Azure Windows Virtual Machine Sign-in application is missing from Conditional Access, make sure that the application is in the tenant:

1. Sign in to the Microsoft Entra admin center  as at least a [Cloud Application Administrator](#).
2. Browse to **Identity > Applications > Enterprise applications**.
3. Remove the filters to see all applications, and search for **VM**. If you don't see **Microsoft Azure Windows Virtual Machine Sign-in** as a result, the service principal is missing from the tenant.

 **Tip**

Some tenants might see the application named Azure Windows VM Sign-in instead of Microsoft Azure Windows Virtual Machine Sign-in. The application will have the same Application ID of 372140e0-b3b7-4226-8ef9-d57986796201.

Next steps

For more information about Microsoft Entra ID, see [What is Microsoft Entra ID?](#).

Feedback

Was this page helpful?

 Yes

 No

[Provide product feedback !\[\]\(7d1e87bc26d73d2f5eecb9f77e19cf7f_img.jpg\)](#)

Device identity and desktop virtualization

Article • 11/27/2024

Administrators commonly deploy virtual desktop infrastructure (VDI) platforms hosting Windows operating systems in their organizations. Administrators deploy VDI to:

- Streamline management.
- Reduce costs through consolidation and centralization of resources.
- Deliver end-users mobility and the freedom to access virtual desktops anytime, from anywhere, on any device.

There are two primary types of virtual desktops:

- Persistent
- Non-persistent

Persistent versions use a unique desktop image for each user or a pool of users. These unique desktops can be customized and saved for future use.

Non-persistent versions use a collection of desktops that users can access on an as needed basis. These non-persistent desktops are reverted to their original state when a virtual machine goes through a shutdown/restart/OS reset process.

It's important to ensure organizations manage stale devices that are created because frequent device registration without having a proper strategy for device lifecycle management.

ⓘ Important

Failure to manage stale devices can lead to pressure increase on your tenant quota usage consumption and potential risk of service interruption, if you run out of tenant quota. Use the following guidance when deploying non persistent VDI environments to avoid this situation.

For successful execution of some scenarios, it's important to have unique device names in the directory. This can be achieved by proper management of stale devices, or you can guarantee device name uniqueness by using some pattern in device naming.

This article covers Microsoft's guidance to administrators on support for device identity and VDI. For more information about device identity, see the article [What is a device](#)

identity.

Supported scenarios

Before configuring device identities in Microsoft Entra ID for your VDI environment, familiarize yourself with the supported scenarios. The following table illustrates which provisioning scenarios are supported. Provisioning in this context implies that an administrator can configure device identities at scale without requiring any end-user interaction.

Windows current devices represent Windows 10 or newer, Windows Server 2016 v1803 or higher, and Windows Server 2019 or higher.

[+] Expand table

Device identity type	Identity infrastructure	Windows devices	VDI platform version	Supported
Microsoft Entra hybrid joined	Federated ³	Windows current	Persistent	Yes
		Windows current	Non-persistent	Yes ⁵
	Managed ⁴	Windows current	Persistent	Yes
		Windows current	Non-persistent	Limited ⁶
Microsoft Entra joined	Federated	Windows current	Persistent	Limited ⁸
			Non-persistent	No
	Managed	Windows current	Persistent	Limited ⁸
			Non-persistent	No
Microsoft Entra registered	Federated/Managed	Windows current	Persistent/Non-persistent	Not Applicable

³ A **Federated** identity infrastructure environment represents an environment with an identity provider (IdP) such as AD FS or other non-Microsoft IdP. In a federated identity infrastructure environment, computers follow the [managed device registration flow](#)

based on the [Microsoft Windows Server Active Directory Service Connection Point \(SCP\) settings](#).

⁴ A **Managed** identity infrastructure environment represents an environment with Microsoft Entra ID as the identity provider deployed with either [password hash sync \(PHS\)](#) or [pass-through authentication \(PTA\)](#) with [seamless single sign-on](#).

⁵ **Non-Persistence support for Windows current** requires other consideration as documented in the guidance section. This scenario requires Windows 10 1803 or newer, Windows Server 2019, or Windows Server (Semi-annual channel) starting version 1803

⁶ **Non-Persistence support for Windows current** in a Managed identity infrastructure environment is only available with Citrix [on-premises customer managed](#) and [Cloud service managed](#). For any support related queries, contact [Citrix support](#) directly.

⁸ **Microsoft Entra join support** is available with [Azure Virtual Desktop](#), [Windows 365](#), and [Amazon WorkSpaces](#). For any support related queries with Amazon WorkSpaces and Microsoft Entra integration, contact [Amazon support](#) directly.

Microsoft's guidance

Administrators should reference the following articles, based on their identity infrastructure, to learn how to configure Microsoft Entra hybrid join.

- [Configure Microsoft Entra hybrid join for federated environment](#)
- [Configure Microsoft Entra hybrid join for managed environment](#)

Non-persistent VDI

When administrators deploy non-persistent VDI, Microsoft recommends you implement the following guidance. Failure to do so results in your directory having lots of stale Microsoft Entra hybrid joined devices that were registered from your non-persistent VDI platform. These stale devices result in increased pressure on your tenant quota and risk of service interruption because of running out of tenant quota.

- If you're relying on the System Preparation Tool (sysprep.exe) and if you're using a pre-Windows 10 1809 image for installation, make sure that image isn't from a device that is already registered with Microsoft Entra ID as Microsoft Entra hybrid joined.
- If you're relying on a Virtual Machine (VM) snapshot to create more VMs, make sure that snapshot isn't from a VM that is already registered with Microsoft Entra ID as Microsoft Entra hybrid join.

- Active Directory Federation Services (AD FS) supports instant join for non-persistent VDI and Microsoft Entra hybrid join.
- Create and use a prefix for the display name (for example, NPVDI-) of the computer that indicates the desktop as non-persistent VDI-based.
- For Windows devices in a Federated environment (for example, AD FS):
 - Implement `dsregcmd /join` as part of VM boot sequence/order and before user signs in.
 - **DO NOT** execute `dsregcmd /leave` as part of VM shutdown/restart process.
- Define and implement process for [managing stale devices](#).
 - Once you have a strategy to identify your non-persistent Microsoft Entra hybrid joined devices (such as using computer display name prefix), you should be more aggressive on the cleanup of these devices to ensure your directory doesn't get consumed with lots of stale devices.
 - For non-persistent VDI deployments, you should delete devices that have `ApproximateLastLogonTimestamp` of older than 15 days.

 **Note**

When using non-persistent VDI, if you want to prevent adding a work or school account ensure the following registry key is set:

```
HKLM\SOFTWARE\Policies\Microsoft\Windows\WorkplaceJoin:  
"BlockAADWorkplaceJoin"=dword:00000001
```

Ensure you're running Windows 10, version 1803 or higher.

Roaming any data under the path `%localappdata%` is not supported. If you choose to move content under `%localappdata%`, make sure that the content of the following folders and registry keys **never** leaves the device under any condition. For example, profile migration tools must skip the following folders and keys:

- `%localappdata%\Packages\Microsoft.AAD.BrokerPlugin_cw5n1h2txyewy`
- `%localappdata%\Packages\Microsoft.Windows.CloudExperienceHost_cw5n1h2txyewy`
- `%localappdata%\Packages\<any app package>\AC\TokenBroker`
- `%localappdata%\Microsoft\TokenBroker`
- `%localappdata%\Microsoft\OneAuth`
- `%localappdata%\Microsoft\IdentityCache`
- `HKEY_CURRENT_USER\SOFTWARE\Microsoft\IdentityCRL`
- `HKEY_CURRENT_USER\SOFTWARE\Microsoft\Windows\CurrentVersion\AAD`
- `HKEY_CURRENT_USER\SOFTWARE\Microsoft\Windows NT\CurrentVersion\WorkplaceJoin`

Roaming of the work account's device certificate is not supported. The certificate, issued by "MS-Organization-Access", is stored in the Personal (MY) certificate store of the current user and on the local machine.

Persistent VDI

When administrators deploy persistent VDI, Microsoft recommends you implement the following guidance. Failure to do so results in deployment and authentication issues.

- If you're relying on the System Preparation Tool (sysprep.exe) and if you're using a pre-Windows 10 1809 image for installation, make sure that image isn't from a device that is already registered with Microsoft Entra ID as Microsoft Entra hybrid joined.
- If you're relying on a Virtual Machine (VM) snapshot to create more VMs, make sure that snapshot isn't from a VM that is already registered with Microsoft Entra ID as Microsoft Entra hybrid join.

We recommend you to implement process for [managing stale devices](#). This process ensures your directory doesn't get consumed with lots of stale devices if you periodically reset your VMs.

Next steps

[Configuring Microsoft Entra hybrid join for federated environment](#)

Feedback

Was this page helpful?

 Yes

 No

[Provide product feedback ↗](#)

Microsoft Entra device management FAQ

FAQ

General FAQ

I registered the device recently. Why can't I see the device under my user info? Or why is the device owner marked as N/A for Microsoft Entra hybrid joined devices?

Windows 10 or newer devices that are Microsoft Entra hybrid joined don't show up under **USER devices**. Use the [All devices](#) view. You can also use a PowerShell [Get-MgDevice](#) cmdlet.

Only the following devices are listed under **USER devices**:

- All personal devices that aren't Microsoft Entra hybrid joined.
- All non-Windows 10 or newer and Windows Server 2016 or later devices.
- All non-Windows devices.

How do I know what the device registration state of the client is?

Go to [All devices](#). Search for the device by using the device ID. Check the value under the join type column. Sometimes, the device might be reset or reimaged. So it's essential to also check the device registration state on the device:

- For Windows 10 or newer and Windows Server 2016 or later devices, run `dsregcmd.exe /status`.

For troubleshooting information, see these articles:

- [Troubleshooting devices using dsregcmd command](#)
- [Troubleshooting Microsoft Entra hybrid joined Windows 10 and Windows Server 2016 devices](#)

My org on-premises AD users are split into two or more different tenants in Microsoft Entra ID. Do I get Windows PRT for each tenant on client machine?

Windows clients fetch the PRT from Microsoft Entra ID if the user and the device belong to the same tenant. Users don't get a PRT for another tenant if the device isn't registered or the user isn't a member there. If the two tenants trust each other via B2B, you can always create cross tenant B2B access and trust device claims from your home tenant.

I see the device record under the USER info and I see the state as registered. Am I set up correctly to use Conditional Access?

The device join state, shown by `deviceID`, must match the state on Microsoft Entra ID and meet any evaluation criteria for Conditional Access. For more information, see [Require managed devices for cloud app access with Conditional Access](#).

Why do my users see an error message saying "Your organization has deleted the device" or "Your organization has disabled the device" on their Windows 10/11 devices?

On Windows 10/11 devices joined or registered with Microsoft Entra ID, users are issued a [Primary refresh token \(PRT\)](#) which enables single sign-on. The validity of the PRT is based on the validity of the device itself. Users see this message if the device is either deleted or disabled in Microsoft Entra ID without initiating the action from the device itself. A device can be deleted or disabled in Microsoft Entra one of the following scenarios:

- User disables the device from the My Apps portal.
- An administrator (or user) deletes or disables the device.
- Microsoft Entra hybrid joined only: An administrator removes the devices OU out of sync scope resulting in the devices being deleted from Microsoft Entra ID.
- Microsoft Entra hybrid joined only: An administrator disables the computer account on premises, resulting in the device being disabled in Microsoft Entra ID.

I disabled or deleted my device, but the local state on the device says it's registered. What should I do?

This operation is by design. In this case, the device doesn't have access to resources in the cloud. Administrators can perform this action for stale, lost, or stolen devices to prevent unauthorized access. If this action was performed unintentionally, you need to re-enable or re-register the device using the steps that follow:

- If the device was disabled in Microsoft Entra ID, an administrator with sufficient privileges can enable it in the Microsoft Entra admin center.

! Note

If you're syncing devices using Microsoft Entra Connect, Microsoft Entra hybrid joined devices will be automatically re-enabled during the next sync cycle. So, if you need to disable a Microsoft Entra hybrid joined device, you need to disable it from your on-premises AD.

- If the device is deleted in Microsoft Entra ID, you need to re-register the device. To re-register, you must take a manual action on the device. See the following steps for instructions to re-register based on the device state.

To re-register Microsoft Entra hybrid joined Windows 10/11 and Windows Server 2016/2019 devices, take the following steps:

1. Open the command prompt as an administrator.
2. Enter `dsregcmd.exe /debug /leave`.
3. Sign out and sign in to trigger the scheduled task that registers the device again with Microsoft Entra ID.

For Microsoft Entra joined devices Windows 10/11 devices, take the following steps:

1. Open the command prompt as an administrator
2. Enter `dsregcmd /forcerecovery` (You need to be an administrator to perform this action).
3. Click "Sign in" in the dialog that opens up and continue with the sign in process.
4. To complete the recovery, sign out and sign back in on the device.

For Microsoft Entra registered Windows 10/11 devices, take the following steps:

1. Go to **Settings > Accounts > Access Work or School**.
2. Select the account and select **Disconnect**.
3. Click on "+ Connect" and register the device again by going through the sign in process.

Why do I see duplicate device entries?

- For Windows 10 or newer and Windows Server 2016 or later, repeated tries to unjoin and rejoin the same device might cause duplicate entries.
- Each Windows user who uses **Add Work or School Account** creates a new device record with the same device name.
- A Microsoft Entra joined machine that's wiped, reinstalled, and rejoined with the same name shows up as another record with the same device name.

Does Windows 10/11 device registration in Microsoft Entra support TPMs in FIPS mode?

Windows 10/11 device registration is only supported for FIPS-compliant TPM 2.0 and not supported for TPM 1.2. If your devices have FIPS-compliant TPM 1.2, you must disable them before proceeding with Microsoft Entra join or Microsoft Entra hybrid join. Microsoft doesn't provide any tools for disabling FIPS mode for TPMs as it is dependent on the TPM manufacturer. Contact your hardware OEM for support.

Why can a user still access resources from a device I disabled?

It takes up to an hour for a revoke to be applied from the time the Microsoft Entra device is marked as disabled.

Note

For enrolled devices, we recommend that you wipe the device to make sure users can't access the resources. For more information, see [What is device enrollment?](#).

I can't add more than three Microsoft Entra user accounts under the same user session on a Windows 10/11 device, why?

Microsoft Entra ID added support for multiple Microsoft Entra accounts starting in Windows 10 1803 release. However, Windows 10/11 restricts the number of Microsoft Entra accounts on a device to 3 to limit the size of token requests and enable reliable single sign-on (SSO). Once three accounts are added, users see an error for subsequent accounts. The additional problem information on the error screen provides the following message indicating the reason - "Add account operation is blocked because account limit is reached".

What are the MS-Organization-Access certificates present on our Windows 10/11 devices?

The Microsoft Entra Device Registration Service issues the MS-Organization-Access certificates during the device registration process. These certificates are issued to all join types supported on Windows - Microsoft Entra joined, Microsoft Entra hybrid joined and Microsoft Entra registered devices. Once issued, they're used as part of the authentication process from the device to request a Primary Refresh Token (PRT). For Microsoft Entra joined and Microsoft Entra hybrid joined devices, this certificate is present in Local Computer\Personal\Certificates whereas for Microsoft Entra registered devices, certificate is present in Current User\Personal\Certificates. All MS-Organization-Access certificates have a default lifetime of 10 years. These certificates are deleted from the corresponding certificate store when the device is unregistered from Microsoft Entra ID. Any inadvertent deletion of this certificate leads to authentication failures for the user, and requiring re-registration of the device in such cases.

Microsoft Entra join FAQ

How do I unjoin a Microsoft Entra joined device locally on the device?

For pure Microsoft Entra joined devices, make sure you have an offline local administrator account or create one. You can't sign in with any Microsoft Entra user credentials. Next, go to **Settings > Accounts > Access Work or School**. Select your account and select **Disconnect**. Follow the prompts and provide the local administrator credentials when prompted. Reboot the device to finish the unjoin process.

Can my users sign in to Microsoft Entra joined devices that are deleted or disabled in Microsoft

Entra ID?

Yes. Windows has a cached username and password capability that allows users who signed in previously to access the desktop quickly even without network connectivity.

When a device is deleted or disabled in Microsoft Entra ID, it's not known to the Windows device. So users who signed in previously continue to access the desktop with the cached username and password. But as the device is deleted or disabled, users can't access any resources protected by device-based Conditional Access.

Users who didn't sign in previously can't access the device. There's no cached username and password enabled for them.

Can a disabled or deleted user sign in to a Microsoft Entra joined device?

Yes, but only for a limited time. When a user is deleted or disabled in Microsoft Entra ID, it's not immediately known to the Windows device. So users who signed in previously can access the desktop with the cached username and password.

Typically, the device is aware of the user state in less than four hours. Then Windows blocks those users' access to the desktop. As the user is deleted or disabled in Microsoft Entra ID, all their tokens are revoked. So they can't access any resources.

Deleted or disabled users who didn't sign in previously can't access a device. There's no cached username and password enabled for them.

Can a guest user sign in to a Microsoft Entra joined device?

No, currently, guest users can't sign in to a Microsoft Entra joined device.

My users can't search printers from Microsoft Entra joined devices. How can I enable printing from those devices?

Organizations can choose to [deploy Windows Server Hybrid Cloud Print with Pre-Authentication](#) or [Universal Print](#) for their Microsoft Entra joined devices.

How do I connect to a remote Microsoft Entra joined device?

See [Connect to remote Microsoft Entra joined PC](#).

Why do my users see 'You can't get there from here'?

Did you configure Conditional Access policies to require a specific device state? If the device doesn't meet the criteria, users are blocked, and they see that message. Evaluate your Conditional Access policies. Make sure the device meets the criteria to avoid the message.

Why do I get a 'username or password is incorrect' message for a device I just joined to Microsoft Entra ID?

Common reasons for this scenario are as follows:

- Your user credentials are no longer valid.
- Your computer can't communicate with Microsoft Entra ID. Check for any network connectivity issues.
- Federated sign-ins require your federation server to support WS-Trust endpoints that are enabled and accessible.
- You enabled pass-through authentication. So your temporary password needs to be changed when you sign in.

How can users change their temporary or expired password on Microsoft Entra joined devices?

Currently, Microsoft Entra joined devices don't force users to change password on the lock screen. So, users with temporary or expired passwords will be forced to change passwords only when they access an application (that requires a Microsoft Entra token) after they log in to Windows.

Why do I see the 'Oops... an error occurred!' dialog when I try to Microsoft Entra join my PC?

This error happens when you set up Microsoft Entra autoenrollment with Intune without proper license assigned. Make sure that the user who tries to Microsoft Entra join has the correct Intune license assigned. For more information, see [Set up enrollment for Windows devices](#).

Why did my attempt to Microsoft Entra join a PC fail, although I didn't get any error information?

A likely cause is that you signed in to the device by using the local built-in administrator account. Create a different local account before you use Microsoft Entra join to finish the setup.

What is the P2P Server application and why is it registered in my tenant?

The P2P Server application is application registered by Microsoft Entra ID to enable Remote Desktop Protocol (RDP) connections to any Microsoft Entra joined or Microsoft Entra hybrid joined Windows devices in your tenant. This application creates a tenant wide certificate issued by Microsoft Entra's certificate authority and is used to issue RDP device and user certificates for RDP connectivity. To ensure this is the correct application, you can find the **Object ID** of the P2P Server application in the **Microsoft Entra admin center > Applications > Enterprise Applications**. Remove the default filter applied do you can see all applications. Compare this **Object ID** using the Microsoft Graph API to query for the details using [GET /servicePrincipals/{objectid}](#) and confirm that the servicePrincipalNames property is `urn:p2p_cert`.

What are the MS-Organization-P2P-Access certificates present on our Windows 10/11 devices?

Microsoft Entra ID issues the MS-Organization-P2P-Access certificates to Microsoft Entra joined and Microsoft Entra hybrid joined devices. These certificates are used to enable trust between devices in the same tenant for remote desktop scenarios. One certificate is issued to the device and another is issued to the user. The device certificate is present in `Local Computer\Personal\Certificates` and is valid for one day. This certificate is renewed (by issuing a new certificate) if the device is still active in Microsoft Entra ID. The user certificate isn't persistent and is valid for one hour, it's issued on-demand when a user attempts a remote desktop session to another Microsoft Entra joined device. It isn't renewed on expiry. Both these certificates are issued using the MS-Organization-

P2P-Access certificate present in the `Local Computer\AAD Token Issuer\Certificates`. Microsoft Entra ID issues this certificate during device registration.

How can we disable cached logon/expire the cache logon of the user on Microsoft Entra joined devices?

It isn't possible to disable or expire previous cached logons on Microsoft Entra joined devices.

Microsoft Entra hybrid join FAQ

How do I unjoin a Microsoft Entra hybrid joined device locally on the device?

For Microsoft Entra hybrid joined devices, make sure to turn off automatic registration in AD using the [Controlled validation](#) article. Then the scheduled task doesn't register the device again. Next, open a command prompt as an administrator and enter `dsregcmd.exe /debug /leave`. Or run this command as a script across several devices to unjoin in bulk.

Where can I find troubleshooting information to diagnose Microsoft Entra hybrid join failures?

For troubleshooting information, see these articles:

- [Troubleshooting Microsoft Entra hybrid joined Windows 10 and Windows Server 2016 devices](#)

Why do I see a duplicate Microsoft Entra registered record for my Windows 10/11 Microsoft Entra hybrid joined device in the Microsoft Entra devices list?

When your users add their accounts to apps on a domain-joined device, they might be prompted with **Add account to Windows?** If they enter **Yes** on the prompt, the device registers with Microsoft Entra ID. The trust type is marked as Microsoft Entra registered.

After you enable Microsoft Entra hybrid join in your organization, the device also gets Microsoft Entra hybrid joined. Then two device states show up for the same device.

In most cases, Microsoft Entra hybrid join takes precedence over the Microsoft Entra registered state, resulting in your device being considered Microsoft Entra hybrid joined for any authentication and Conditional Access evaluation. However, sometimes, this dual state can result in a nondeterministic evaluation of the device and cause access issues. We strongly recommend upgrading to Windows 10 version 1803 and above where we automatically clean up the Microsoft Entra registered state. Learn how to [avoid or clean up this dual state on the Windows 10 machine](#).

Why do my users have issues on Windows 10 Microsoft Entra hybrid joined devices after changing their UPN?

UPN changes are supported with Windows 10 2004 update and also applicable to Windows 11. Users on devices with this update won't have any issues after changing their UPNs.

UPN changes on older versions of Windows 10 aren't fully supported with Microsoft Entra hybrid joined devices. While users can sign in to the device and access their on-premises applications, authentication with Microsoft Entra ID fails after a UPN change. As a result, users have SSO and Conditional Access issues on their devices. You need to unjoin the device from Microsoft Entra ID (run "dsregcmd /leave" with elevated privileges) and rejoin (happens automatically) to resolve the issue.

Do Windows 10/11 Microsoft Entra hybrid joined devices require line of sight to the domain controller to get access to cloud resources?

No, except when the user's password is changed. After Windows 10/11 Microsoft Entra hybrid join is complete, and the user signs in at least once, the device doesn't require line of sight to the domain controller to access cloud resources. Windows 10/11 can get single sign-on to Microsoft Entra applications from anywhere with an internet connection, except when a password is changed. Users who sign in with Windows Hello for Business continue to get single sign-on to Microsoft Entra applications even after a password change, even if they don't have line of sight to their domain controller.

What happens if a user changes their password and tries to sign in to their Windows 10/11 Microsoft Entra hybrid joined device outside the corporate network?

If a password is changed outside the corporate network (for example, by using Microsoft Entra SSPR), then the user sign-in with the new password fails. For Microsoft Entra hybrid joined devices, on-premises Active Directory is the primary authority. When a device doesn't have line of sight to a domain controller, it's unable to validate the new password. The user needs to establish a connection with the domain controller (either via VPN or being in the corporate network) before they're able to sign in to the device with their new password. Otherwise, they can only sign in with their old password because of cached sign-in capability in Windows. Microsoft Entra invalidates the old password during token requests. This invalidation process prevents single sign-on and fails any device-based Conditional Access policies until the user authenticates with their new password in an app or browser. This issue doesn't occur if you use Microsoft Entra joined devices.

Microsoft Entra register FAQ

How do I remove a Microsoft Entra registered state for a device locally?

- For Windows 10/11 Microsoft Entra registered devices, Go to **Settings > Accounts > Access Work or School**. Select your account and select **Disconnect**. Device registration is per user profile on Windows 10/11.
- For iOS and Android, you can use the Microsoft Authenticator application **Settings > Device Registration** and select **Unregister device**.
- For macOS, you can use the Microsoft Intune Company Portal application to unenroll the device from management and remove any registration.

For Windows 10 version 2004 and older, this process can be automated with the [Workplace Join \(WPJ\) removal tool](#).

Note

This tool removes all SSO accounts on the device. After this operation, all applications will lose SSO state, and the device will be unenrolled from

management tools (MDM) and unregistered from the cloud. The next time an application tries to sign in, users will be asked to add the account again.

How can I block users from adding more work accounts (Microsoft Entra registered) on my corporate Windows 10/11 devices?

Enable the following registry to block your users from adding other work accounts to your corporate domain joined, Microsoft Entra joined, or Microsoft Entra hybrid joined Windows 10/11 devices. This policy can also be used to block domain joined machines from inadvertently getting Microsoft Entra registered with the same user account.

```
HKLM\SOFTWARE\Policies\Microsoft\Windows\WorkplaceJoin,  
"BlockAADWorkplaceJoin"=dword:00000001
```

Related content

- [The Microsoft Error Lookup Tool](#)

Feedback

Was this page helpful?

 Yes

 No

[Provide product feedback ↗](#)

Troubleshooting the Microsoft Enterprise SSO Extension plugin on Apple devices

Article • 03/24/2024

This article provides troubleshooting guidance used by administrators to resolve issues with deploying and using the [Enterprise SSO plugin](#). The Apple SSO extension can be deployed to iOS/iPadOS and macOS.

Organizations can opt to deploy SSO to their corporate devices to provide a better experience for their end users. On Apple platforms, this process involves implementing Single Sign On (SSO) via [Primary Refresh Tokens](#). SSO relieves end users of the burden of excessive authentication prompts.

Microsoft has implemented a plugin built on top of Apple's SSO framework, which provides brokered authentication for applications integrated with Microsoft Entra ID. For more information, see the article [Microsoft Enterprise SSO plug-in for Apple devices](#).

Extension types

Apple supports two types of SSO Extensions that are part of its framework: **Redirect** and **Credential**. The Microsoft Enterprise SSO plugin has been implemented as a Redirect type and is best suited for brokering authentication to Microsoft Entra ID. The following table compares the two types of extensions.

[+] [Expand table](#)

Extension type	Best suited for	How it works	Key differences
Redirect	Modern authentication methods such as OpenID Connect, OAuth2, and SAML (Microsoft Entra ID)	Operating System intercepts the authentication request from the application to the Identity provider URLs defined in the extension MDM configuration profile. Redirect extensions receive: URLs, headers, and body.	Request credentials before requesting data. Uses URLs in MDM configuration profile.
Credential	Challenge and response authentication types like Kerberos	Request is sent from the application to the authentication server (AD domain controller). Credential extensions are configured with HOSTS in the MDM	Request data then get challenged for authentication. Use HOSTS in

Extension type	Best suited for	How it works	Key differences
(on-premises Active Directory Domain Services)		configuration profile. If the authentication server returns a challenge that matches a host listed in the profile, the operating system routes the challenge to the extension. The extension has the choice of handling or rejecting the challenge. If handled, the extension returns the authorization headers to complete the request, and the authentication server returns a response to the caller.	MDM configuration profile.

Microsoft has implementations for brokered authentication for the following client operating systems:

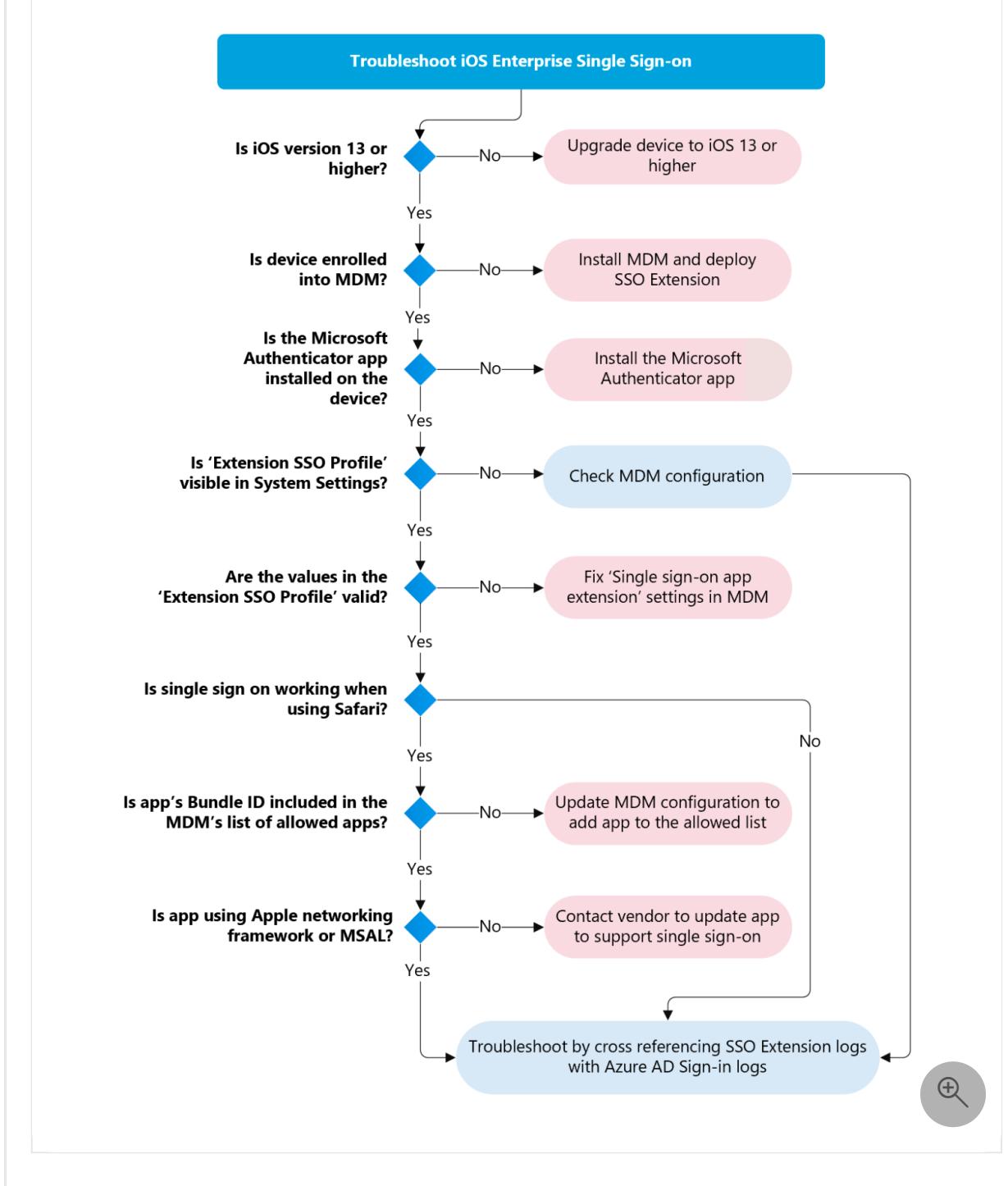
[+] [Expand table](#)

OS	Authentication broker
Windows	Web Account Manager (WAM)
iOS/iPadOS	Microsoft Authenticator
Android	Microsoft Authenticator or Microsoft Intune Company Portal
macOS	Microsoft Intune Company Portal (via SSO Extension)

All Microsoft broker applications use a key artifact known as a Primary Refresh Token (PRT), which is a JSON Web Token (JWT) used to acquire access tokens for applications and web resources secured with Microsoft Entra ID. When deployed through an MDM, the Enterprise SSO extension for macOS or iOS obtains a PRT that is similar to the PRTs used on Windows devices by the Web Account Manager (WAM). For more information, see the article [What is a Primary Refresh Token](#).

Troubleshooting model

The following flowchart outlines a logical flow for approaching troubleshooting the SSO Extension. The rest of this article goes into detail on the steps depicted in this flowchart. The troubleshooting can be broken down into two separate focus areas: [Deployment](#) and [Application Auth Flow](#).



Steps to Opt out of Platform SSO on macOS

To opt out of PSSO that was enabled by mistake, admins should remove the SSO extension profile with PSSO enabled from the devices and deploy a new SSO extension profile with PSSO flags disabled/removed.

1. Remove the targeting for the SSO profile with PSSO enabled
2. Initiate device sync to get the SSO profile with PSSO enabled removed from the device
3. Target the device with a new SSO profile with PSSO disabled

4. Initiate device sync to get the new profile installed on the device

Important

Note: Updating the existing SSO profile on the device WON'T help to disable PSSO after PSSO registration is completed. Only a complete removal of the SSO profile from the device will remove the PSSO state from the device.

Context :

Users will start seeing PSSO registration notification on macOS 13+ devices in two scenarios :

1. If device already has Intune Company Portal version supporting PSSO and admin deploys new SSO extension policy with PSSO enabled
2. If user is already targeted with SSO extension policy having PSSO enabled and later an Intune Company Portal version supporting PSSO is installed on the device.

Caution

Admins should NOT target users with SSO extension policy having PSSO enabled unless they are tested and ready to be deployed, as this can potentially break existing users and their compliance conditions.

Important

Note : For users who complete PSSO registration, the legacy WPJ registration will be removed from the keychain. If PSSO registration was done by mistake , once admin removes the SSO profile with PSSO and installs new profile without PSSO, the legacy WPJ registration should be done again for device compliance to work.

Deployment troubleshooting

Most issues that customers encounter stem from either improper Mobile Device Management (MDM) configuration(s) of the SSO extension profile, or an inability for the Apple device to receive the configuration profile from the MDM. This section covers the steps you can take to ensure that the MDM profile has been deployed to a Mac and that it has the correct configuration.

Deployment requirements

- macOS operating system: [version 10.15 \(Catalina\)](#) or greater.
- iOS operating system: [version 13](#) or greater.
- Device managed by any MDM vendor that supports [Apple macOS and/or iOS](#) (MDM Enrollment).
- Authentication Broker Software installed: [Microsoft Intune Company Portal](#) or [Microsoft Authenticator for iOS](#).

Check macOS operating system version

Use the following steps to check the operating system (OS) version on the macOS device. Apple SSO Extension profiles are only deployed to devices running [macOS 10.15 \(Catalina\)](#) or greater. You can check the macOS version from either the [User Interface](#) or from the [Terminal](#).

User interface

1. From the macOS device, select on the Apple icon in the top left corner and select [About This Mac](#).
2. The Operating system version is listed beside macOS.

Terminal

1. From the macOS device, double-click on the [Applications](#) folder, then double-click on the [Utilities](#) folder.
2. Double-click on the [Terminal](#) application.
3. When the Terminal opens type `sw_vers` at the prompt, look for a result like the following:

```
zsh

% sw_vers
ProductName: macOS
ProductVersion: 13.0.1
BuildVersion: 22A400
```

Check iOS operating system version

Use the following steps to check the operating system (OS) version on the iOS device. Apple SSO Extension profiles are only deployed to devices running **iOS 13** or greater. You can check the iOS version from the **Settings app**. Open the **Settings app**:



Navigate to **General** and then **About**. This screen lists information about the device, including the iOS version number:

3:40



< General

About

Name >

iOS Version

16.5 >

Model Name

iPhone 14 Pro

Model Number

MQ273LL/A

Serial Number

MDM deployment of SSO extension configuration profile

Work with your MDM administrator (or Device Management team) to ensure that the extension configuration profile is deployed to the Apple devices. The extension profile can be deployed from any MDM that supports macOS or iOS devices.

ⓘ Important

Apple requires devices are enrolled into an MDM for the SSO extension to be deployed.

The following table provides specific MDM installation guidance depending on which OS you're deploying the extension to:

- **iOS/iPadOS:** Deploy the Microsoft Enterprise SSO plug-in
- **macOS:** Deploy the Microsoft Enterprise SSO plug-in

Important

Although, any MDM is supported for deploying the SSO Extension, many organizations implement [device-based Conditional Access policies](#) by way of evaluating MDM compliance policies. If a third-party MDM is being used, ensure that the MDM vendor supports [Intune Partner Compliance](#) if you would like to use device-based Conditional Access policies. When the SSO Extension is deployed via Intune or an MDM provider that supports Intune Partner Compliance, the extension can pass the device certificate to Microsoft Entra ID so that device authentication can be completed.

Validate Networking Configuration on macOS device

The SSO extension framework from Apple and the Microsoft Enterprise SSO Extension built on it require that certain domains are exempted from TLS interception/inspection (also known as break and inspect proxying). The following domains must **not** be subject to TLS inspection:

- app-site-association.cdn-apple.com
- app-site-association.networking.apple

Check if the SSO configuration is broken due to TLS Inspection

You can validate if TLS inspection is impacting your SSO configuration by running a sysdiagnose from the Terminal application on an impacted device:

```
zsh
```

```
sudo sysdiagnose -f ~/Desktop/
```

The sysdiagnose will be saved to your desktop as a .tar.gz archive. Extract the archive and open the **system_logs.logarchive** file. This will open in the Console application. Search for **com.apple.appssso** and change the filter to **SUBSYSTEM**:

system_logs.logarchive
748 messages

Reveal Activities Clear Reload Info Share Save

SUBSYSTEM < com.apple.appssd

All Messages	Errors and Faults					
Activity ID	Type	PID: Thread ID	Thread ID	Date & Time	Message	Process
1048317	2999: 0x2d17e	0x2d17e	2023-09-20 13:48:58.954708-0400	com.microsoft.teams teamIdentifier: UBF8T34609	AppSSOAgent	
1048317	2999: 0x2d17e	0x2d17e	2023-09-20 13:48:58.954981-0400	+{SOAgentUtils _localizedNameForBundle:] com.microsoft.teams -> Microsoft	AppSSOAgent	
1048317	2999: 0x2d17e	0x2d17e	2023-09-20 13:48:58.954995-0400	39278 localized app name: Microsoft Teams	AppSSOAgent	
1048317	2999: 0x2d17e	0x2d17e	2023-09-20 13:48:58.955007-0400	-{SOExtensionManager loadedExtensionWithBundleIdentifier:] com.microsoft.	AppSSOAgent	
1048317	2999: 0x2d17e	0x2d17e	2023-09-20 13:48:58.955028-0400	-{SOConfigurationHost _checkAssociatedDomainForProfiles:] on <private>	AppSSOAgent	
1048317	2999: 0x2d17e	0x2d17e	2023-09-20 13:48:58.955053-0400	-{SOExtensionManager loadedExtensionWithBundleIdentifier:] com.microsoft.	AppSSOAgent	
1048317	2999: 0x2d17e	0x2d17e	2023-09-20 13:48:58.955055-0400	-{SOExtension checkAssociatedDomains:] on <private>	AppSSOAgent	
1048317	2999: 0x2d17e	0x2d17e	2023-09-20 13:48:58.957914-0400	Associated domain: login.microsoft.com is not approved	AppSSOAgent	
1048317	2999: 0x2d17e	0x2d17e	2023-09-20 13:48:58.957915-0400	Associated domain: login.us.microsoftonline.com is not approved	AppSSOAgent	
1048317	2999: 0x2d17e	0x2d17e	2023-09-20 13:48:58.957916-0400	Associated domain: login.chinacloudapi.cn is not approved	AppSSOAgent	
1048317	2999: 0x2d17e	0x2d17e	2023-09-20 13:48:58.957916-0400	Associated domain: login.partner.microsoftonline.cn is not approved	AppSSOAgent	
1048317	2999: 0x2d17e	0x2d17e	2023-09-20 13:48:58.957916-0400	Associated domain: login.microsoftonline.net is not approved	AppSSOAgent	
1048317	2999: 0x2d17e	0x2d17e	2023-09-20 13:48:58.957916-0400	Associated domain: sts.windows.net is not approved	AppSSOAgent	
1048317	2999: 0x2d17e	0x2d17e	2023-09-20 13:48:58.957917-0400	Associated domain: login.microsoftonline.com is not approved	AppSSOAgent	
1048317	2999: 0x2d17e	0x2d17e	2023-09-20 13:48:58.957917-0400	Associated domain: login.usgovcloudapi.net is not approved	AppSSOAgent	
1048317	2999: 0x2d17e	0x2d17e	2023-09-20 13:48:58.957917-0400	Associated domain: login.microsoftonline.us is not approved	AppSSOAgent	
1048317	2999: 0x2d17e	0x2d17e	2023-09-20 13:48:58.958012-0400	-{SOExtensionManager loadedExtensionWithBundleIdentifier:] com.microsoft.	AppSSOAgent	
1048317	2999: 0x2d17e	0x2d17e	2023-09-20 13:48:58.958024-0400	-{SOExtension hasURLApprovedAssociatedDomain:] url: <mask>.hash: '1uobXnC'	AppSSOAgent	
1048317	2999: 0x2d17e	0x2d17e	2023-09-20 13:48:58.958039-0400	-{SOExtension hasURLApprovedAssociatedDomain:] url: <mask>.hash: '1uobXnC'	AppSSOAgent	
1048317	2999: 0x2d17e	0x2d17e	2023-09-20 13:48:58.958061-0400	Associated domain: validation failed for URL <mask>.hash: 'a08kjyvelYBc'	AppSSOAgent	
1048317	2999: 0x2d17e	0x2d17e	2023-09-20 13:48:58.958078-0400	-{SOExtension hasURLApprovedAssociatedDomain:] url: <mask>.hash: '1uobXnC'	AppSSOAgent	
1048317	2999: 0x2d17e	0x2d17e	2023-09-20 13:48:58.958074-0400	com.microsoft.CompanyPortalMac_ssoxetineension hasAssociatedDomainsApproved	AppSSOAgent	
1048317	2999: 0x2d17e	0x2d17e	2023-09-20 13:48:58.958081-0400	Associated domain: validation failed for URL <mask>.hash: '1jICxXB0P79'	AppSSOAgent	

Showing: Last 15 Minutes [Details](#)

-- Subsystem: -- Category: -- Details --



Look for events stating that there are Associated Domain failures, especially related to Microsoft domains, such as login.microsoftonline.com. These events might indicate TLS inspection issues, which will prevent the SSO Extension from working properly. Apple domains will not appear in the sysdiagnose log, even if they are impacted by an unsupported TLS inspection configuration.

Validate TLS Inspection Configuration

Apple provides a macOS tool for checking a number of common configuration issues called the Mac Evaluation Utility. This tool can be downloaded from [AppleSeed for IT](#). If you have access to AppleSeed for IT then download the Mac Evaluation Utility from the Resources area. After installing the application, run an evaluation. Once the evaluation is complete, navigate to **HTTPS Interception** --> **Additional Content** --> and check the two items below:

Category	Number of Tests	Status
> Computer Information	5	✓
> Network Information	10	⚠️
> Apple Network Services	216	✓
HTTPS Interception	79	⚠️
> Certificate Validation	3	⚠️
> Device Setup	7	⚠️
> Device Management	15	⚠️
> Apple Business Essentials	5	⚠️
> Apple Business Manager and Apple School Manager	9	⚠️
> Software Update	5	⚠️
> Apple ID	4	⚠️
> App Store	4	⚠️
> Content Caching	7	⚠️
Additional Content	10	⚠️
app-site-association.cdn.apple.com:443		⚠️
app-site-association.networking.apple:443		⚠️
audiocontentdownload.apple.com:443		⚠️
data.appattest.apple.com:443		⚠️
devimages-cdn.apple.com:443		⚠️
download.developer.apple.com:443		⚠️
playgrounds-assets-cdn.apple.com:443		⚠️
playgrounds-cdn.apple.com:443		⚠️
sylvan.apple.com:443		⚠️
www.apple.com:443		⚠️
> Feedback Assistant	3	⚠️
> DNS Resolution	1	✓
> Apple Diagnostics	1	⚠️

If these checks have a warning or error then there might be TLS inspection occurring on the device. Work with your network team to exempt `*.cdn.apple.com` and `*.networking.apple` from TLS inspection.

Output detailed swcd logs

Apple provides a command line utility called `swcutil` that allows for monitoring the progress of the associated domain validation. You can monitor for any associated domain errors using the following command:

```

zsh
sudo swcutil watch --verbose

```

Locate the following entry in the logs and check if it is marked approved, or if there're any errors:

```

```
Entry s = authsrv, a = UBF8T346G9.com.microsoft.CompanyPortalMac, d =
login.microsoftonline.com
```

```

Clear macOS TLS Inspection Cache

If you have issues with associated domains and have allow-listed domains in your on-device TLS inspection tool, then it may take some time for Apple's associated domain validation cache to be invalidated. Unfortunately, there're no deterministic steps that re-trigger associated domain re-validation on all machines, but there're a few things that can be attempted.

You can run following commands to reset the device's cache:

```
zsh  
  
pkill -9 swcd  
sudo swcutil reset  
pkill -9 AppSSOAgent
```

Re-test the SSO extension configuration after resetting the cache.

Sometimes, this command is insufficient and doesn't fully reset the cache. In these cases, you can attempt the following:

- Remove or move the Intune Company Portal app to the Trash, then restart your device. After the restart is complete, you can try re-install the Company Portal app.
- Re-enroll your device.

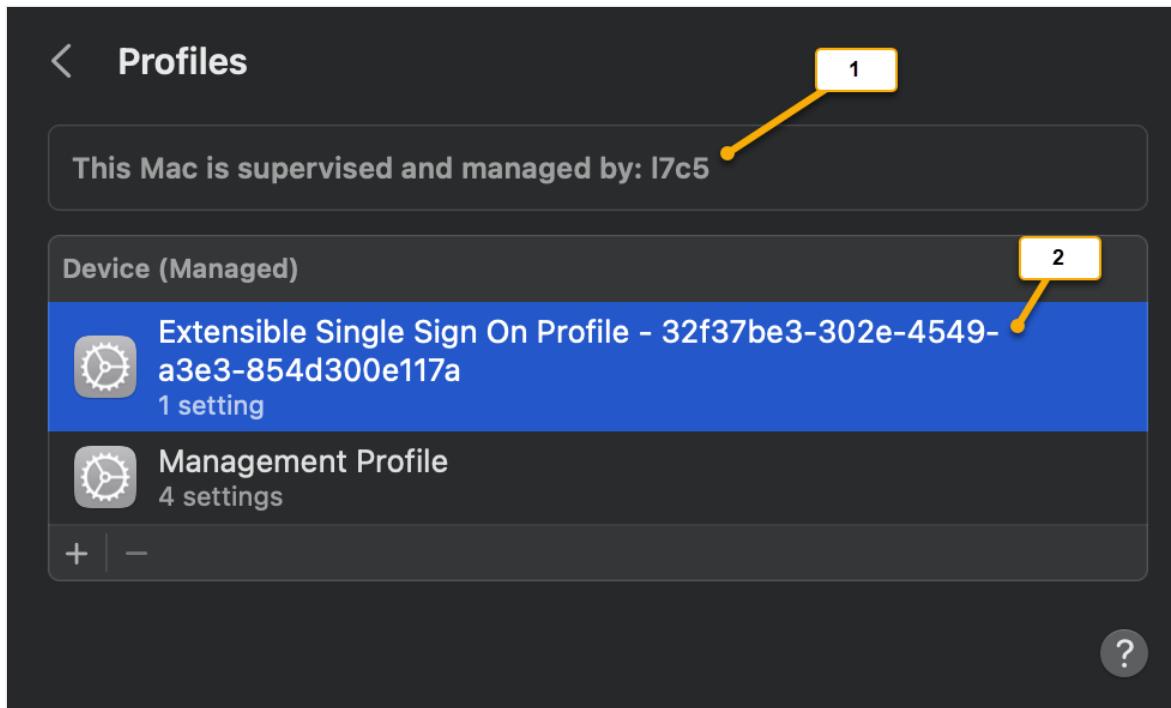
If none of above methods resolve your issue, there may be something else in your environment that could be blocking the associated domain validation. If this happens, please reach out to Apple support for further troubleshooting.

Validate SSO configuration profile on macOS device

Assuming the MDM administrator has followed the steps in the previous section [MDM Deployment of SSO Extension Profile](#), the next step is to verify if the profile has been deployed successfully to the device.

Locate SSO extension MDM configuration profile

1. From the macOS device, select on the **System Settings**.
2. When the **System Settings** appears type **Profiles** and hit **return**.
3. This action should bring up the **Profiles** panel.



[+] Expand table

Screenshot callout	Description
1	Indicates that the device is under MDM Management.
2	There might be multiple profiles to choose from. In this example, the Microsoft Enterprise SSO Extension Profile is called Extensible Single Sign On Profile-32f37be3-302e-4549-a3e3-854d300e117a.

ⓘ Note

Depending on the type of MDM being used, there could be several profiles listed and their naming scheme is arbitrary depending on the MDM configuration. Select each one and inspect that the **Settings** row indicates that it is a **Single Sign On Extension**.

4. Double-click on the configuration profile that matches a **Settings** value of **Single Sign On Extension**.



Extensible Single Sign On Profile - 32f37be3-302e-4549-

a3e3-854d300e117a

l7c5 Verified

Description The configuration profile enables your company's technical support to enforce security policies on your mobile device

Signed AppleConfigProfileSigning.manage.microsoft.com

Installed Dec 26, 2022 at 3:53 PM

Settings

Single Sign On Extension

Details

Single Sign On Extension

Description Extensible Single Sign On Profile - 32f37be3-302e-4549-a3e3-854d300e117a

Extension com.microsoft.CompanyPortalMac.ssoextension (UBF8T346G9)

Type

Redirect

URLs

- https://login.microsoftonline.com
- https://login.microsoft.com
- https://sts.windows.net
- https://login.partner.microsoftonline.cn
- https://login.chinacloudapi.cn
- https://login.microsoftonline.de
- https://login.microsoftonline.us

1

2

3

4

5

6

OK

[] Expand table

Screenshot callout	Configuration profile setting	Description
1	Signed	Signing authority of the MDM provider.
2	Installed	Date/Timestamp showing when the extension was installed (or updated).
3	Settings: Single Sign On	Indicates that this configuration profile is an Apple SSO Extension type.

Screenshot callout	Configuration profile setting	Description
Extension		
4	Extension	Identifier that maps to the bundle ID of the application that is running the Microsoft Enterprise Extension Plugin. The identifier must always be set to <code>com.microsoft.CompanyPortalMac.ssoextension</code> and the Team Identifier must appear as (UBF8T346G9) if the profile is installed on a macOS device. If any values differ, then the MDM doesn't invoke the extension correctly.
5	Type	The Microsoft Enterprise SSO Extension must always be set to a Redirect extension type. For more information, see Redirect vs Credential Extension Types .
6	URLs	The login URLs belonging to the Identity Provider (Microsoft Entra ID). See list of supported URLs .

All Apple SSO Redirect Extensions must have the following MDM Payload components in the configuration profile:

[] [Expand table](#)

MDM payload component	Description
Extension Identifier	Includes both the Bundle Identifier and Team Identifier of the application on the macOS device, running the Extension. Note: The Microsoft Enterprise SSO Extension should always be set to: <code>com.microsoft.CompanyPortalMac.ssoextension</code> (UBF8T346G9) to inform the macOS operating system that the extension client code is part of the Intune Company Portal application.
Type	Must be set to Redirect to indicate a Redirect Extension type.
URLs	Endpoint URLs of the identity provider (Microsoft Entra ID), where the operating system routes authentication requests to the extension.
Optional Extension Specific Configuration	Dictionary values that can act as configuration parameters. In the context of Microsoft Enterprise SSO Extension, these configuration parameters are called feature flags. See feature flag definitions .

! **Note**

The MDM definitions for Apple's SSO Extension profile can be referenced in the article [Extensible Single Sign-on MDM payload settings for Apple devices](#) Microsoft has implemented our extension based on this schema. See [Microsoft Enterprise SSO plug-in for Apple devices](#)

5. To verify that the correct profile for the Microsoft Enterprise SSO Extension is installed, the **Extension** field should match:
`com.microsoft.CompanyPortalMac.ssoextension (UBF8T346G9)`.
6. Take note of the **Installed** field in the configuration profile as it can be a useful troubleshooting indicator, when changes are made to its configuration.

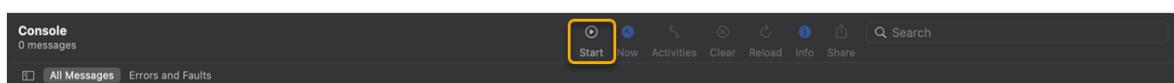
If the correct configuration profile has been verified, proceed to the [Application Auth Flow Troubleshooting](#) section.

MDM configuration profile is missing

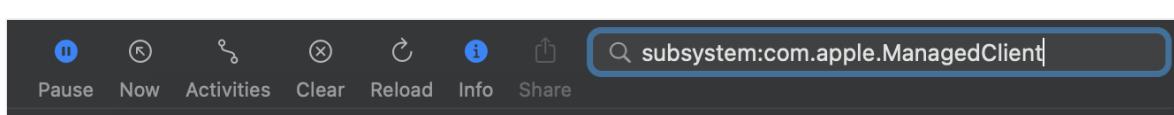
If the SSO extension configuration profile doesn't appear in the **Profiles** list after following the [previous section](#), it could be that the MDM configuration has User/Device targeting enabled, which is effectively **filtering out** the user or device from receiving the configuration profile. Check with your MDM administrator and collect the **Console** logs found in the [next section](#).

Collect MDM specific console logs

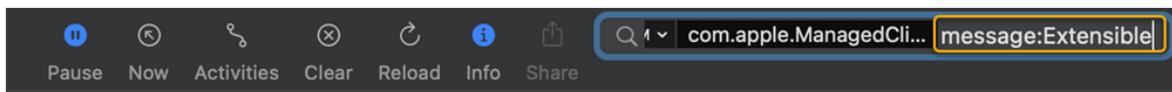
1. From the macOS device, double-click on the **Applications** folder, then double-click on the **Utilities** folder.
2. Double-click on the **Console** application.
3. Click the **Start** button to enable the Console trace logging.



4. Have the MDM administrator try to redeploy the config profile to this macOS device/user and force a sync cycle.
5. Type `subsystem:com.apple.ManagedClient` into the search bar and hit **return**.



6. Where the cursor is flashing in the search bar type **message:Extensible**.



7. You should now see the MDM Console logs filtered on **Extensible SSO** configuration profile activities. The following screenshot shows a log entry **Installed configuration profile**, showing that the configuration profile was installed.

Application auth flow troubleshooting

The guidance in this section assumes that the macOS device has a correctly deployed configuration profile. See [Validate SSO Configuration Profile on macOS Device](#) for the steps.

Once deployed the **Microsoft Enterprise SSO Extension for Apple devices** supports two types of application authentication flows for each application type. When troubleshooting, it's important to understand the type of application being used.

Application types

[+] Expand table

Application type	Interactive auth	Silent auth	Description	Examples
Native MSAL App	X	X	MSAL (Microsoft Authentication Library) is an application developer framework tailored for building applications with the Microsoft identity platform (Microsoft Entra ID). Apps built on MSAL version 1.1 or greater are able to integrate with the Microsoft Enterprise SSO Extension. <i>If the application is SSO extension (broker) aware it utilizes the extension without any further configuration for more information, see our MSAL developer sample documentation.</i>	Microsoft To Do
Non-MSAL Native/Browser SSO	X		Applications that use Apple networking technologies or webviews can be configured to obtain a shared credential from the SSO Extension	Microsoft Word Safari Microsoft

Application type	Interactive auth	Silent auth	Description	Examples
			Feature flags must be configured to ensure that the bundle ID for each app is allowed to obtain the shared credential (PRT).	Edge Visual Studio

ⓘ Important

Not all Microsoft first-party native applications use the MSAL framework. At the time of this article's publication, most of the Microsoft Office macOS applications still rely on the older ADAL library framework, and thus rely on the Browser SSO flow.

How to find the bundle ID for an application on macOS

1. From the macOS device, double-click on the **Applications** folder, then double-click on the **Utilities** folder.
2. Double-click on the **Terminal** application.
3. When the Terminal opens type `osascript -e 'id of app "<appname>"'` at the prompt. See some examples follow:

```
zsh

% osascript -e 'id of app "Safari"'
com.apple.Safari

% osascript -e 'id of app "OneDrive"'
com.microsoft.OneDrive

% osascript -e 'id of app "Microsoft Edge"'
com.microsoft.edgemac
```

4. Now that the bundle ID(s) have been gathered, follow our [guidance to configure the feature flags](#) to ensure that Non-MSAL Native/Browser SSO apps can utilize the SSO Extension. **Note: All bundle ids are case sensitive for the Feature flag configuration.**

✖ Caution

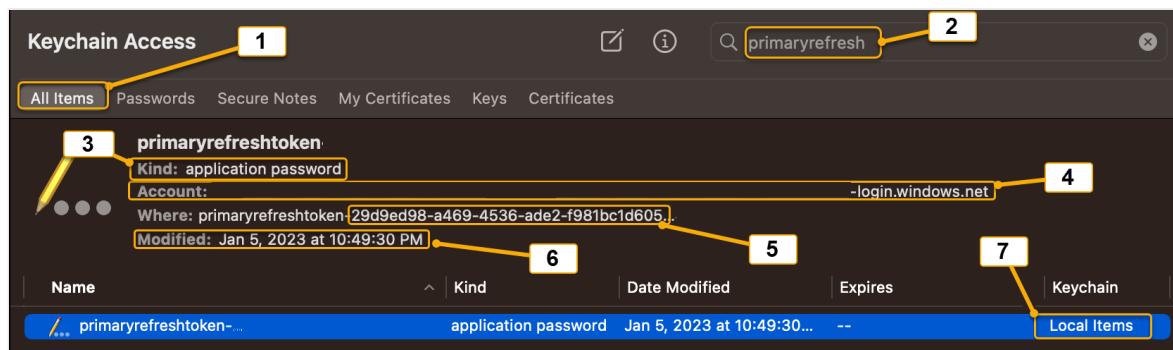
Applications that do not use Apple Networking technologies (like WKWebview and NSURLConnection) will not be able to use the shared credential (PRT) from the SSO Extension. Both **Google Chrome** and **Mozilla Firefox** fall into this category. Even if they are configured in the MDM configuration profile, the result will be a regular authentication prompt in the browser.

Bootstrapping

By default, only MSAL apps invoke the SSO Extension, and then in turn the Extension acquires a shared credential (PRT) from Microsoft Entra ID. However, the **Safari** browser application or other **Non-MSAL** applications can be configured to acquire the PRT. See [Allow users to sign in from applications that don't use MSAL and the Safari browser](#). After the SSO extension acquires a PRT, it will store the credential in the user login Keychain. Next, check to ensure that the PRT is present in the user's keychain:

Checking keychain access for PRT

1. From the macOS device, double-click on the **Applications** folder, then double-click on the **Utilities** folder.
2. Double-click on the **Keychain Access** application.
3. Under **Default Keychains** select **Local Items** (or iCloud).
 - Ensure that the **All Items** is selected.
 - In the search bar, on the right-hand side, type `primaryrefresh` (To filter).



[Expand table](#)

Screenshot callout	Keychain credential component	Description
1	All Items	Shows all types of credentials across Keychain Access

Screenshot callout	Keychain credential component	Description
2	Keychain Search Bar	Allows filtering by credential. To filter for the Microsoft Entra PRT type <code>primaryrefresh</code>
3	Kind	Refers to the type of credential. The Microsoft Entra PRT credential is an Application Password credential type
4	Account	Displays the Microsoft Entra user account, which owns the PRT in the format: <code>UserObjectId.TenantId-login.windows.net</code>
5	Where	Displays the full name of the credential. The Microsoft Entra PRT credential begins with the following format: <code>primaryrefreshtoken-29d9ed98-a469-4536-ade2-f981bc1d605</code> The <code>29d9ed98-a469-4536-ade2-f981bc1d605</code> is the Application ID for the Microsoft Authentication Broker service, responsible for handling PRT acquisition requests
6	Modified	Shows when the credential was last updated. For the Microsoft Entra PRT credential, anytime the credential is bootstrapped or updated by an interactive sign-on event it updates the date/timestamp
7	Keychain	Indicates which Keychain the selected credential resides. The Microsoft Entra PRT credential resides in the Local Items or iCloud Keychain. When iCloud is enabled on the macOS device, the Local Items Keychain will become the iCloud keychain

4. If the PRT isn't found in Keychain Access, do the following based on the application type:

- **Native MSAL:** Check that the application developer, if the app was built with **MSAL version 1.1 or greater**, has enabled the application to be broker aware. Also, check [Deployment Troubleshooting steps](#) to rule out any deployment issues.
- **Non MSAL (Safari):** Check to ensure that the feature flag `browser_sso_interaction_enabled` is set to 1 and not 0 in the MDM configuration profile

Authentication flow after bootstrapping a PRT

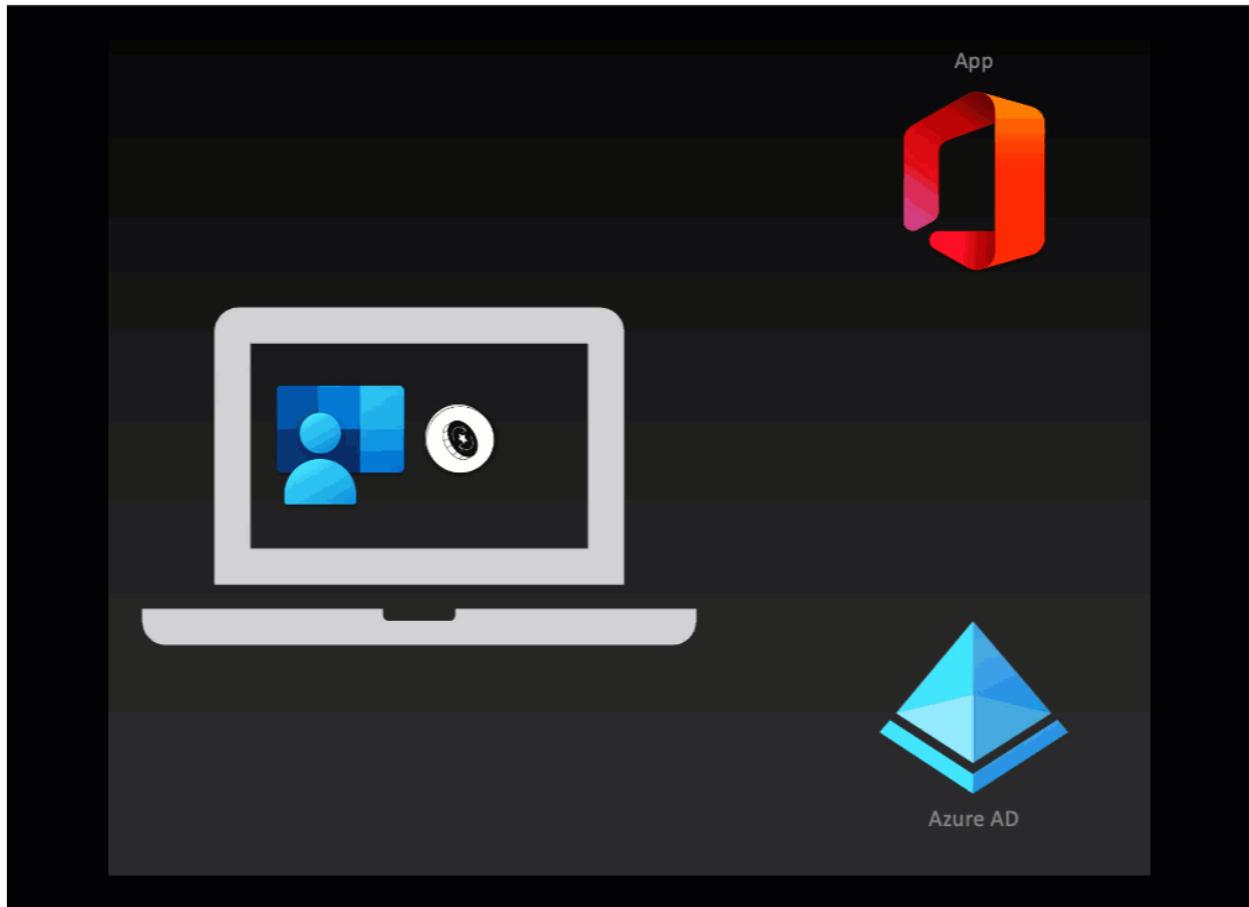
Now that the PRT (shared credential) has been verified, before doing any deeper troubleshooting, it's helpful to understand the high-level steps for each application type

and how it interacts with the Microsoft Enterprise SSO Extension plugin (broker app).

The following animations and descriptions should help macOS administrators understand the scenario before looking at any logging data.

Native MSAL application

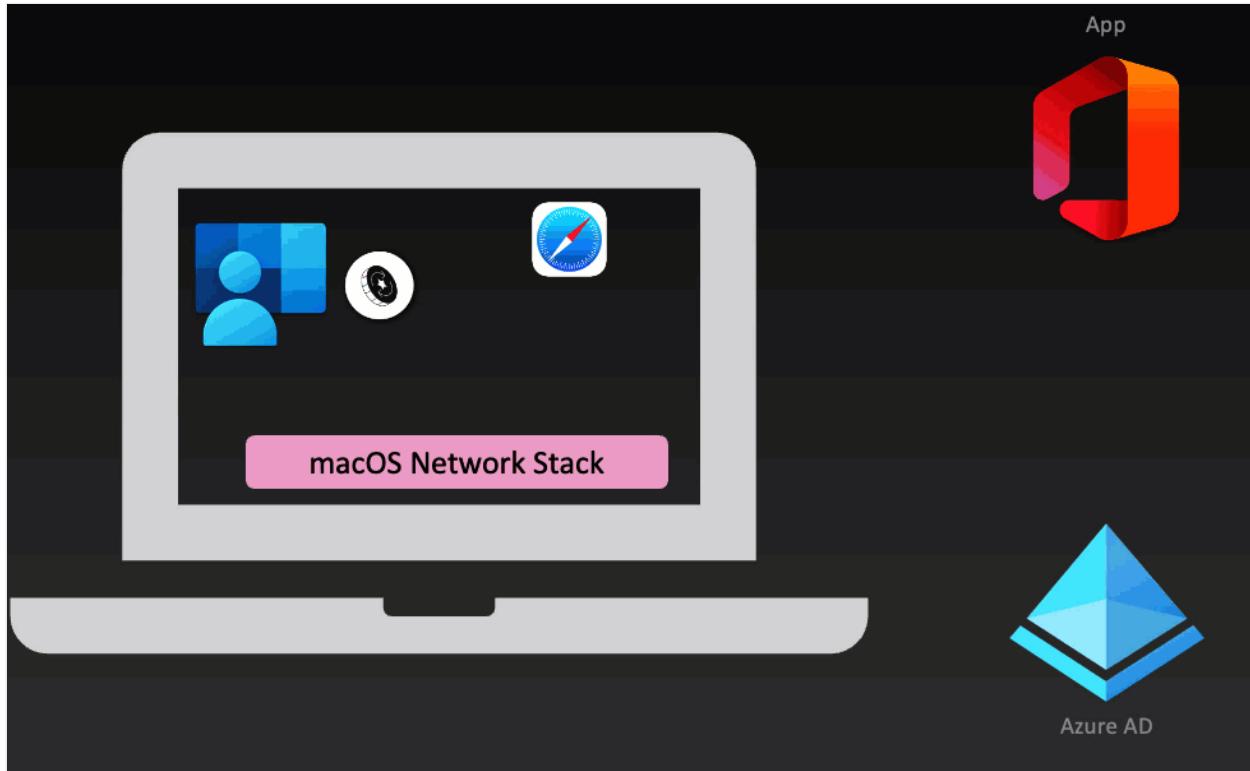
Scenario: An application developed to use MSAL (Example: **Microsoft To Do** client) that is running on an Apple device needs to sign the user in with their Microsoft Entra account in order to access a Microsoft Entra protected service (Example: **Microsoft To Do Service**).



1. MSAL-developed applications invoke the SSO extension directly, and send the PRT to the Microsoft Entra token endpoint along with the application's request for a token for a Microsoft Entra protected resource
2. Microsoft Entra ID validates the PRT credential, and returns an application-specific token back to the SSO extension broker
3. The SSO extension broker then passes the token to the MSAL client application, which then sends it to the Microsoft Entra protected resource
4. The user is now signed into the app and the authentication process is complete

Non-MSAL/Browser SSO

Scenario: A user on an Apple device opens up the Safari web browser (or any Non-MSAL native app that supports the Apple Networking Stack) to sign into a Microsoft Entra protected resource (Example: <https://office.com>).



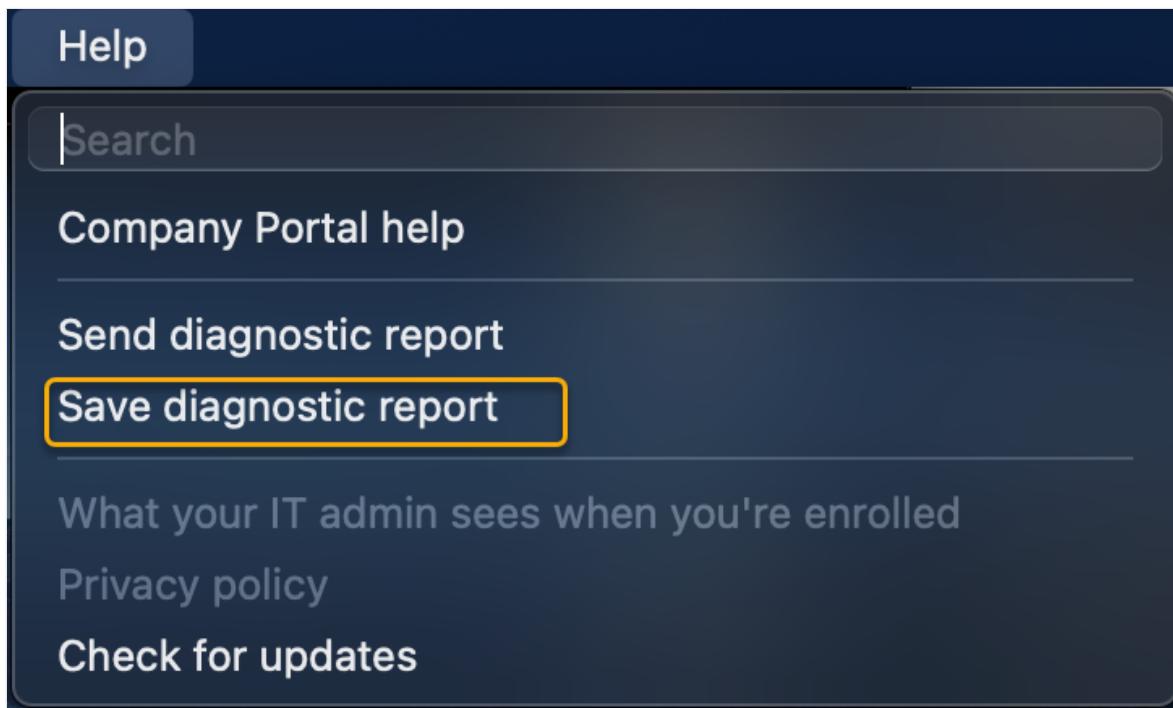
1. Using a Non-MSAL application (Example: **Safari**), the user attempts to sign into a Microsoft Entra integrated application (Example: office.com) and is redirected to obtain a token from Microsoft Entra ID
2. As long as the Non-MSAL application is allow-listed in the MDM payload configuration, the Apple network stack intercepts the authentication request and redirects the request to the SSO Extension broker
3. Once the SSO extension receives the intercepted request, the PRT is sent to the Microsoft Entra token endpoint
4. Microsoft Entra ID validates the PRT, and returns an application-specific token back to the SSO Extension
5. The application-specific token is given to the Non-MSAL client application, and the client application sends the token to access the Microsoft Entra protected service
6. The user now has completed the sign-in and the authentication process is complete

Obtaining the SSO extension logs

One of the most useful tools to troubleshoot various issues with the SSO extension are the client logs from the Apple device.

Save SSO extension logs from Company Portal app

1. From the macOS device, double-click on the **Applications** folder.
2. Double-click on the **Company Portal** application.
3. When the **Company Portal** loads, navigate to the top menu bar: **Help->Save diagnostic report**. There's no need to Sign into the app.



4. Save the Company Portal Log archive to place of your choice (for example: Desktop).
5. Open the **CompanyPortal.zip** archive and Open the **SSOExtension.log** file with any text editor.

💡 Tip

A handy way to view the logs is using [Visual Studio Code](#) and installing the [Log Viewer](#) extension.

Tailing SSO extension logs on macOS with terminal

During troubleshooting it might be useful to reproduce a problem while tailing the SSOExtension logs in real time:

1. From the macOS device, double-click on the **Applications** folder, then double-click on the **Utilities** folder.

2. Double-click on the Terminal application.

3. When the Terminal opens type:

```
zsh  
  
tail -F  
~/Library/Containers/com.microsoft.CompanyPortalMac.ssoextension/Data/L  
ibrary/Caches/Logs/Microsoft/SSOExtension/*
```

 Note

The trailing /* indicates that multiple logs will be tailed should any exist

Output

```
% tail -F  
~/Library/Containers/com.microsoft.CompanyPortalMac.ssoextension/Data/L  
ibrary/Caches/Logs/Microsoft/SSOExtension/*  
==>  
/Users/<username>/Library/Containers/com.microsoft.CompanyPortalMac.sso  
extension/Data/Library/Caches/Logs/Microsoft/SSOExtension/SSOExtension  
2022-12-25--13-11-52-855.log <==  
2022-12-29 14:49:59:281 | I | TID=783491 MSAL 1.2.4 Mac 13.0.1 [2022-  
12-29 19:49:59] Handling SSO request, requested operation:  
2022-12-29 14:49:59:281 | I | TID=783491 MSAL 1.2.4 Mac 13.0.1 [2022-  
12-29 19:49:59] Ignoring this SSO request...  
2022-12-29 14:49:59:282 | I | TID=783491 MSAL 1.2.4 Mac 13.0.1 [2022-  
12-29 19:49:59] Finished SSO request.  
2022-12-29 14:49:59:599 | I | Beginning authorization request  
2022-12-29 14:49:59:599 | I | TID=783491 MSAL 1.2.4 Mac 13.0.1 [2022-  
12-29 19:49:59] Checking for feature flag  
browser_sso_interaction_enabled, value in config 1, value type  
__NSCFNumber  
2022-12-29 14:49:59:599 | I | TID=783491 MSAL 1.2.4 Mac 13.0.1 [2022-  
12-29 19:49:59] Feature flag browser_sso_interaction_enabled is enabled  
2022-12-29 14:49:59:599 | I | TID=783491 MSAL 1.2.4 Mac 13.0.1 [2022-  
12-29 19:49:59] Checking for feature flag browser_sso_disable_mfa,  
value in config (null), value type (null)  
2022-12-29 14:49:59:599 | I | TID=783491 MSAL 1.2.4 Mac 13.0.1 [2022-  
12-29 19:49:59] Checking for feature flag  
disable_browser_sso_intercept_all, value in config (null), value type  
(null)  
2022-12-29 14:49:59:600 | I | Request does not need UI  
2022-12-29 14:49:59:600 | I | TID=783491 MSAL 1.2.4 Mac 13.0.1 [2022-  
12-29 19:49:59] Checking for feature flag admin_debug_mode_enabled,  
value in config (null), value type (null)
```

4. As you reproduce the issue, keep the Terminal window open to observe the output from the tailed SSOExtension logs.

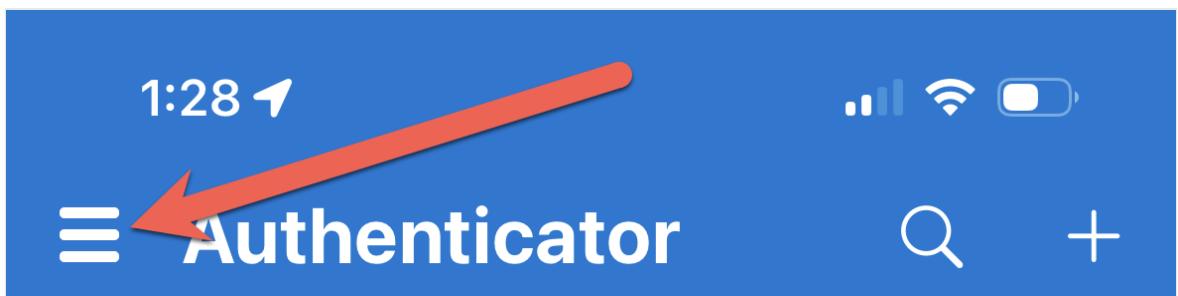
Exporting SSO extension logs on iOS

It isn't possible to view iOS SSO Extension logs in real time, as it is on macOS. The iOS SSO extension logs can be exported from the Microsoft Authenticator app, and then reviewed from another device:

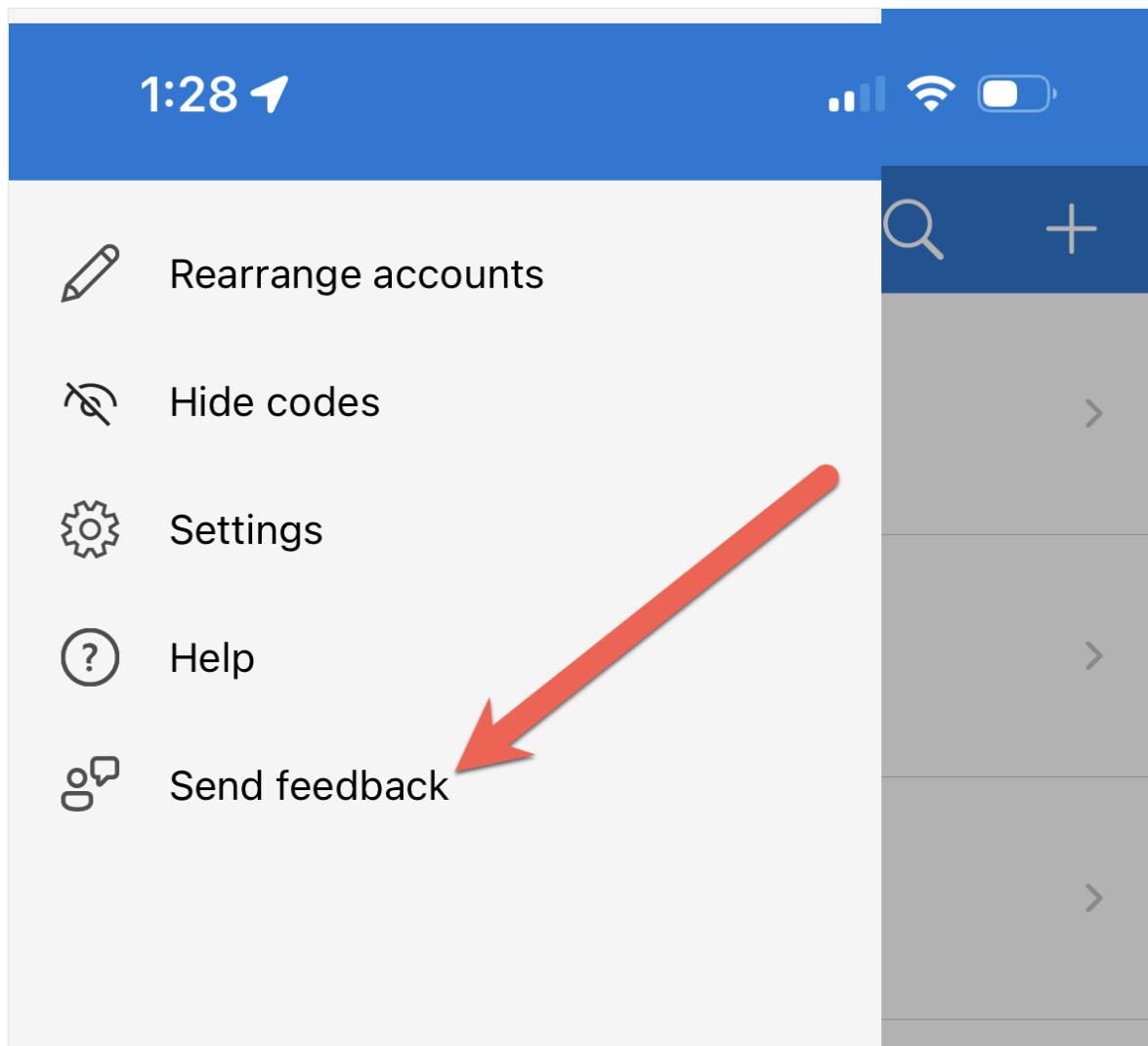
1. Open the Microsoft Authenticator app:



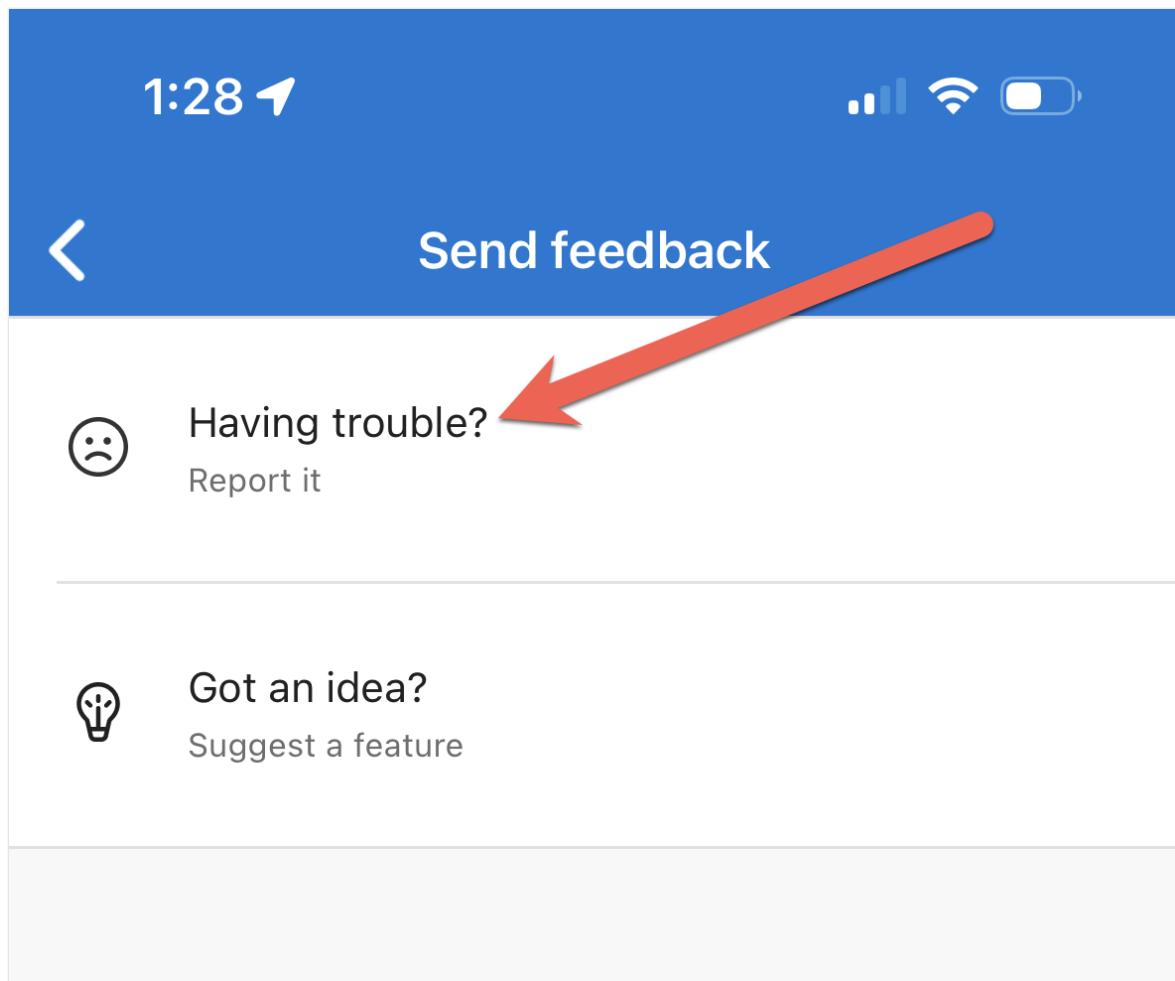
2. Press the menu button in the upper left:



3. Choose the "Send feedback" option:



4. Choose the "Having trouble" option:



5. Press the View diagnostic data option:

1:28



Having trouble?

Send

What are you trying to do?

Select an option



Describe the issue you are facing *

Please don't include your name, phone number, or other personal information.

Include contact email address



We will contact you only if we need more details.

View diagnostic data



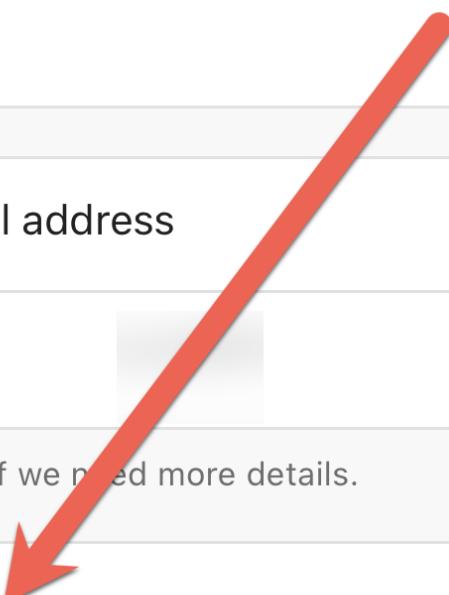
Diagnostic data helps troubleshoot issues you might be having.

Add a screenshot

Add

Your feedback will be used to improve Microsoft's products and services. By including your email address, you agree that Microsoft can email you about your feedback.

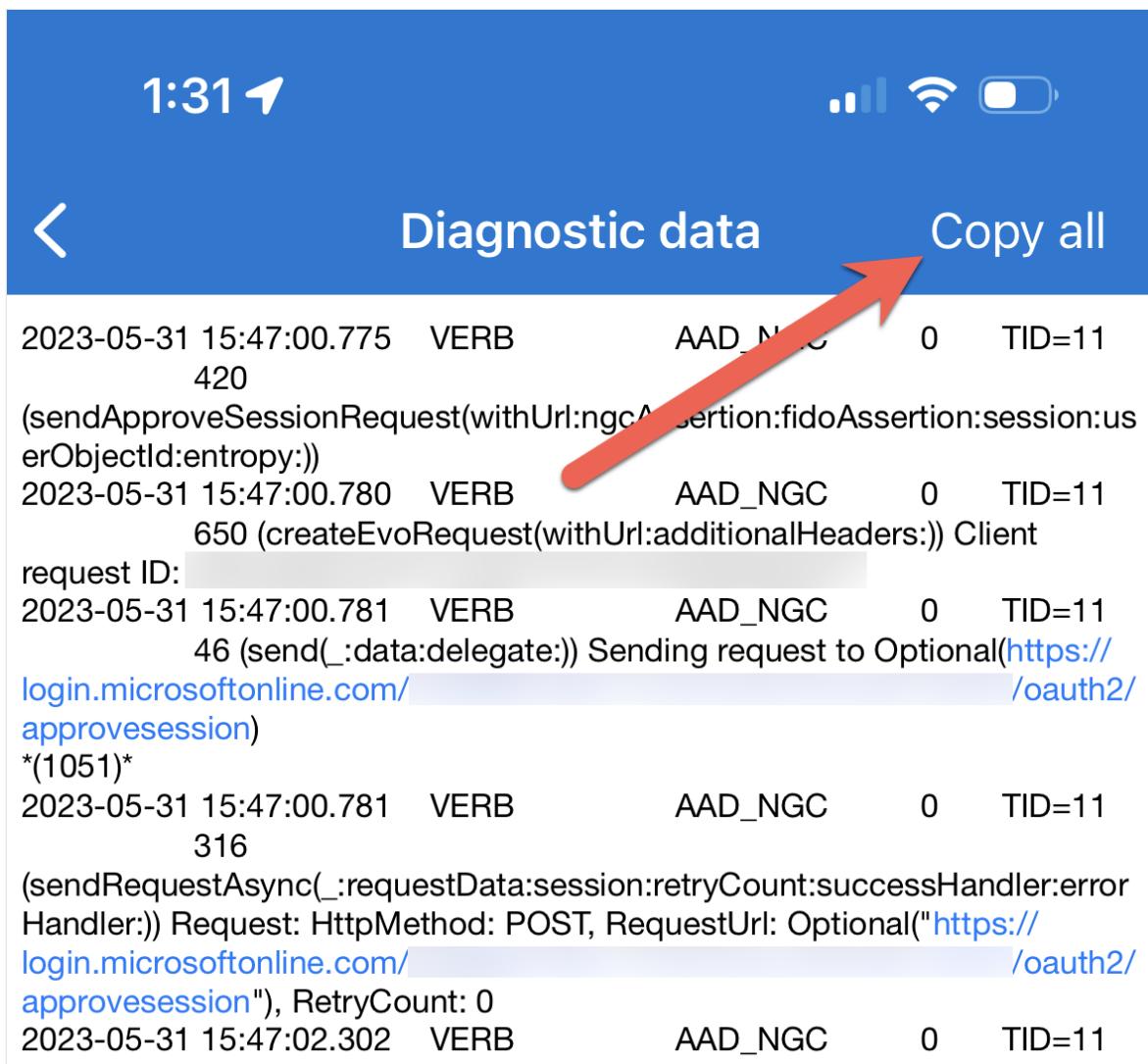
Microsoft Privacy Statement | Feedback Help



💡 Tip

If you are working with Microsoft Support, at this stage you can press the **Send** button to send the logs to support. This will provide you with an Incident ID, which you can provide to your Microsoft Support contact.

6. Press the "Copy all" button to copy the logs to your iOS device's clipboard. You can then save the log files elsewhere for review or send them via email or other file sharing methods:



Understanding the SSO extension logs

Analyzing the SSO extension logs is an excellent way to troubleshoot the authentication flow from applications sending authentication requests to Microsoft Entra ID. Any time the SSO extension Broker is invoked, a series of logging activities results, and these

activities are known as **Authorization Requests**. The logs contain the following useful information for troubleshooting:

- Feature Flag configuration
- Authorization Request Types
 - Native MSAL
 - Non MSAL/Browser SSO
- Interaction with the macOS Keychain for credential retrieval/storage operations
- Correlation IDs for Microsoft Entra sign-in events
 - PRT acquisition
 - Device Registration

⊗ Caution

The SSO extension logs are extremely verbose, especially when looking at Keychain credential operations. For this reason, it's always best to understand the scenario before looking at the logs during troubleshooting.

Log structure

The SSO extension logs are broken down into columns. The following screenshot shows the column breakdown of the logs:

1	2	3	4	5	6	7	8
2022-11-23 16:21:57:634	I	TID=2048454	MSAL 1.2.2 Mac 12.6.1	[2022-11-23 08:21:57]	Checking for feature flag converged_broker_en		
2022-11-23 16:21:57:634	I	TID=2048454	MSAL 1.2.2 Mac 12.6.1	[2022-11-23 08:21:57]	Checking for feature flag disable_browser_sso		
2022-11-23 16:21:57:634	I	TID=2048454	MSAL 1.2.2 Mac 12.6.1	[2022-11-23 08:21:57]	Checking for feature flag admin_debug_mode_en		
2022-11-23 16:21:57:634	I	TID=2048454	MSAL 1.2.2 Mac 12.6.1	[2022-11-23 08:21:57]	Checking for feature flag disable_explicit_ap		
2022-11-23 16:21:57:634	I	TID=2048454	MSAL 1.2.2 Mac 12.6.1	[2022-11-23 08:21:57]	Checking for feature flag disable_explicit_ap		
2022-11-23 16:21:57:634	W	TID=2048454	MSAL 1.2.2 Mac 12.6.1	[2022-11-23 08:21:57]	App list for key from AppCookieSSOAllowList e		
2022-11-23 16:21:57:634	I	TID=2048454	MSAL 1.2.2 Mac 12.6.1	[2022-11-23 08:21:57]	Bundle id list for key AppCookieSSOAllowList		
2022-11-23 16:21:57:634	I	TID=2048454	MSAL 1.2.2 Mac 12.6.1	[2022-11-23 08:21:57]	Created Browser SSO request for bundle identi		
), use cookie sso for this app 0, initiating origin null	7	
2022-11-23 16:21:57:634	I	TID=2048454	MSAL 1.2.2 Mac 12.6.1	[2022-11-23 08:21:57]	Init MSIDKeychainTokenCache with keychainGrou		
2022-11-23 16:21:57:634	I	TID=2048454	MSAL 1.2.2 Mac 12.6.1	[2022-11-23 08:21:57] - 311C0202-FB0B-480B-8807-CD975F1E7799	[MSAL]		
2022-11-23 16:21:57:675	I	TID=2048454	MSAL 1.2.2 Mac 12.6.1	[2022-11-23 08:21:57] - 311C0202-FB0B-480B-8807-CD975F1E7799	[MSAL]		
2022-11-23 16:21:57:675	I	TID=2048454	MSAL 1.2.2 Mac 12.6.1	[2022-11-23 08:21:57] - 311C0202-FB0B-480B-8807-CD975F1E7799	[MSAL]		
2022-11-23 16:21:57:675	I	TID=2048454	MSAL 1.2.2 Mac 12.6.1	[2022-11-23 08:21:57] - 311C0202-FB0B-480B-8807-CD975F1E7799	[MSAL]		
2022-11-23 16:21:57:675	I	TID=2048454	MSAL 1.2.2 Mac 12.6.1	[2022-11-23 08:21:57] - 311C0202-FB0B-480B-8807-CD975F1E7799	[MSAL]		

[] Expand table

Column	Column name	Description
1	Local Date/Time	The Local Date and Time displayed
2	I-Information W-Warning E-Error	Displays Information, Warning, or Errors

Column	Column name	Description
3	Thread ID (TID)	Displays the thread ID of the SSO extension Broker App's execution
4	MSAL Version Number	The Microsoft Enterprise SSO extension Broker Plugin is build as an MSAL app. This column denotes the version of MSAL that the broker app is running
5	macOS version	Show the version of the macOS operating system
6	UTC Date/Time	The UTC Date and Time displayed
7	Correlation ID	Lines in the logs that have to do with Microsoft Entra ID or Keychain operations extend the UTC Date/Time column with a Correlation ID
8	Message	Shows the detailed messaging of the logs. Most of the troubleshooting information can be found by examining this column

Feature flag configuration

During the MDM configuration of the Microsoft Enterprise SSO Extension, an optional extension specific data can be sent as instructions to change how the SSO extension behaves. These configuration specific instructions are known as **Feature Flags**. The Feature Flag configuration is especially important for Non-MSAL/Browser SSO authorization requests types, as the Bundle ID can determine if the Extension is invoked or not. See [Feature Flag documentation](#). Every authorization request begins with a Feature Flag configuration report. The following screenshot walks through an example feature flag configuration:

```

Checking for feature flag browser_sso_interaction_enabled, value in config 1, value type __NSCFNumber
Feature flag browser_sso_interaction_enabled is enabled 1
Checking for feature flag browser_sso_disable_mfa, value in config (null), value type (null) 2
Checking for feature flag converged_broker_enabled, value in config (null), value type (null)
Checking for feature flag disable_browser_sso_intercept_all, value in config (null), value type (null)
Checking for feature flag admin_debug_mode_enabled, value in config (null), value type (null) 3
Checking for feature flag disable_explicit_app_prompt, value in config 1, value type __NSCFNumber
Feature flag disable_explicit_app_prompt is enabled
Checking for feature flag disable_explicit_app_prompt_and_autologin, value in config (null), value type (null)
App list for key from AppAllowList extension data is neither String nor Array (null)!
Bundle id list for key AppAllowList is (null)
App list for key from AppWhiteList extension data is neither String nor Array (null)!
Bundle id list for key AppWhiteList is (null)
Bundle id list for key AppPrefixAllowList is ("com.microsoft.") 4
App list for key from AppCookieSSOAllowList extension data is neither String nor Array (null)!
Bundle id list for key AppCookieSSOAllowList is (null)

```

[+] Expand table

Callout	Feature flag	Description
1	browser_sso_interaction_enabled	Non-MSAL or Safari browser can bootstrap a PRT

Callout	Feature flag	Description
2	<code>browser_sso_disable_mfa</code>	(Now deprecated) During bootstrapping of the PRT credential, by default MFA is required. Notice this configuration is set to <code>null</code> which means that the default configuration is enforced
3	<code>disable_explicit_app_prompt</code>	Replaces <code>prompt=login</code> authentication requests from applications to reduce prompting
4	<code>AppPrefixAllowList</code>	Any Non-MSAL application that has a Bundle ID that starts with <code>com.microsoft.</code> can be intercepted and handled by the SSO extension broker

ⓘ **Important**

Feature flags set to `null` means that their **default** configuration is in place. Check [Feature Flag documentation](#) for more details

MSAL native application sign-in flow

The following section walks through how to examine the SSO extension logs for the Native MSAL Application auth flow. For this example, we're using the [MSAL macOS/iOS sample application](#) as the client application, and the application is making a call to the Microsoft Graph API to display the sign-in user's information.

MSAL native: Interactive flow walkthrough

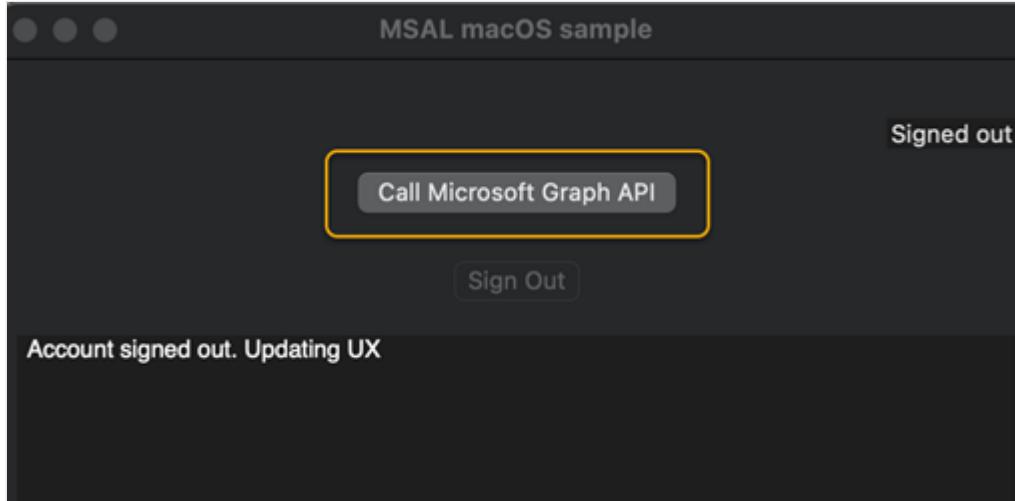
The following actions should take place for a successful interactive sign-on:

1. The user signs in to the MSAL macOS sample app.
2. The Microsoft SSO Extension Broker is invoked and handles the request.
3. Microsoft SSO Extension Broker undergoes the bootstrapping process to acquire a PRT for the signed in user.
4. Store the PRT in the Keychain.
5. Check for the presence of a Device Registration object in Microsoft Entra ID (WPJ).
6. Return an access token to the client application to access the Microsoft Graph with a scope of User.Read.

ⓘ **Important**

The sample log snippets that follows, have been annotated with comment headers // that are not seen in the logs. They are used to help illustrate a specific action being undertaken. We have documented the log snippets this way to assist with copy and paste operations. In addition, the log examples have been trimmed to only show lines of significance for troubleshooting.

The user clicks on the **Call Microsoft Graph API** button to invoke the sign-in process.



SSOExtensionLogs

```
///////////
//get_accounts_operation//
///////////
Handling SSO request, requested operation: get_accounts_operation
(Default accessor) Get accounts.
(MSIDAccountCredentialCache) retrieving cached credentials using credential
query
(Default accessor) Looking for token with aliases (null), tenant (null),
clientId 08dc26ab-e050-465e-beb4-d3f2d66647a5, scopes (null)
(Default accessor) No accounts found in default accessor.
(Default accessor) No accounts found in other accessors.
Completed get accounts SSO request with a personal device mode.
Request complete
Request needs UI
ADB 3.1.40 -[ADBrokerAccountManager allBrokerAccounts:]
ADB 3.1.40 -[ADBrokerAccountManager allMSIDBrokerAccounts:]
(Default accessor) Get accounts.
No existing accounts found, showing webview

/////////
//login//
/////////
Handling SSO request, requested operation: login
Handling interactive SSO request...
Starting SSO broker request with payload: {
    authority = "https://login.microsoftonline.com/common";
    "client_app_name" = MSALMacOS;
```

```

"client_app_version" = "1.0";
"client_id" = "08dc26ab-e050-465e-beb4-d3f2d66647a5";
"client_version" = "1.1.7";
"correlation_id" = "3506307A-E90F-4916-9ED5-25CF81AE97FC";
"extra_oidc_scopes" = "openid profile offline_access";
"instance_aware" = 0;
"msg_protocol_ver" = 4;
prompt = "select_account";
"provider_type" = "provider_aad_v2";
"redirect_uri" = "msauth.com.microsoft.idnaace.MSALMacOS://auth";
scope = "user.read";
}

///////////////////////////////
//Request PRT from Microsoft Authentication Broker Service//
/////////////////////////////
Using request handler <ADInteractiveDevicelessPRTBrokerRequestHandler:
0x117ea50b0>
(Default accessor) Looking for token with aliases (null), tenant (null),
clientId 29d9ed98-a469-4536-ade2-f981bc1d605e, scopes (null)
Attempting to get Deviceless Primary Refresh Token interactively.
Caching AAD Environments
networkHost: login.microsoftonline.com, cacheHost: login.windows.net,
aliases: login.microsoftonline.com, login.windows.net, login.microsoft.com,
sts.windows.net
networkHost: login.partner.microsoftonline.cn, cacheHost:
login.partner.microsoftonline.cn, aliases: login.partner.microsoftonline.cn,
login.chinacloudapi.cn
networkHost: login.microsoftonline.de, cacheHost: login.microsoftonline.de,
aliases: login.microsoftonline.de
networkHost: login.microsoftonline.us, cacheHost: login.microsoftonline.us,
aliases: login.microsoftonline.us, login.usgovcloudapi.net
networkHost: login-us.microsoftonline.com, cacheHost: login-
us.microsoftonline.com, aliases: login-us.microsoftonline.com
Resolved authority, validated: YES, error: 0
[MSAL] Resolving authority: Masked(not-null), upn: Masked(null)
[MSAL] Resolved authority, validated: YES, error: 0
[MSAL] Start webview authorization session with webview controller class
MSIDAADOAuthEmbeddedWebviewController:
[MSAL] Presenting web view controller.

```

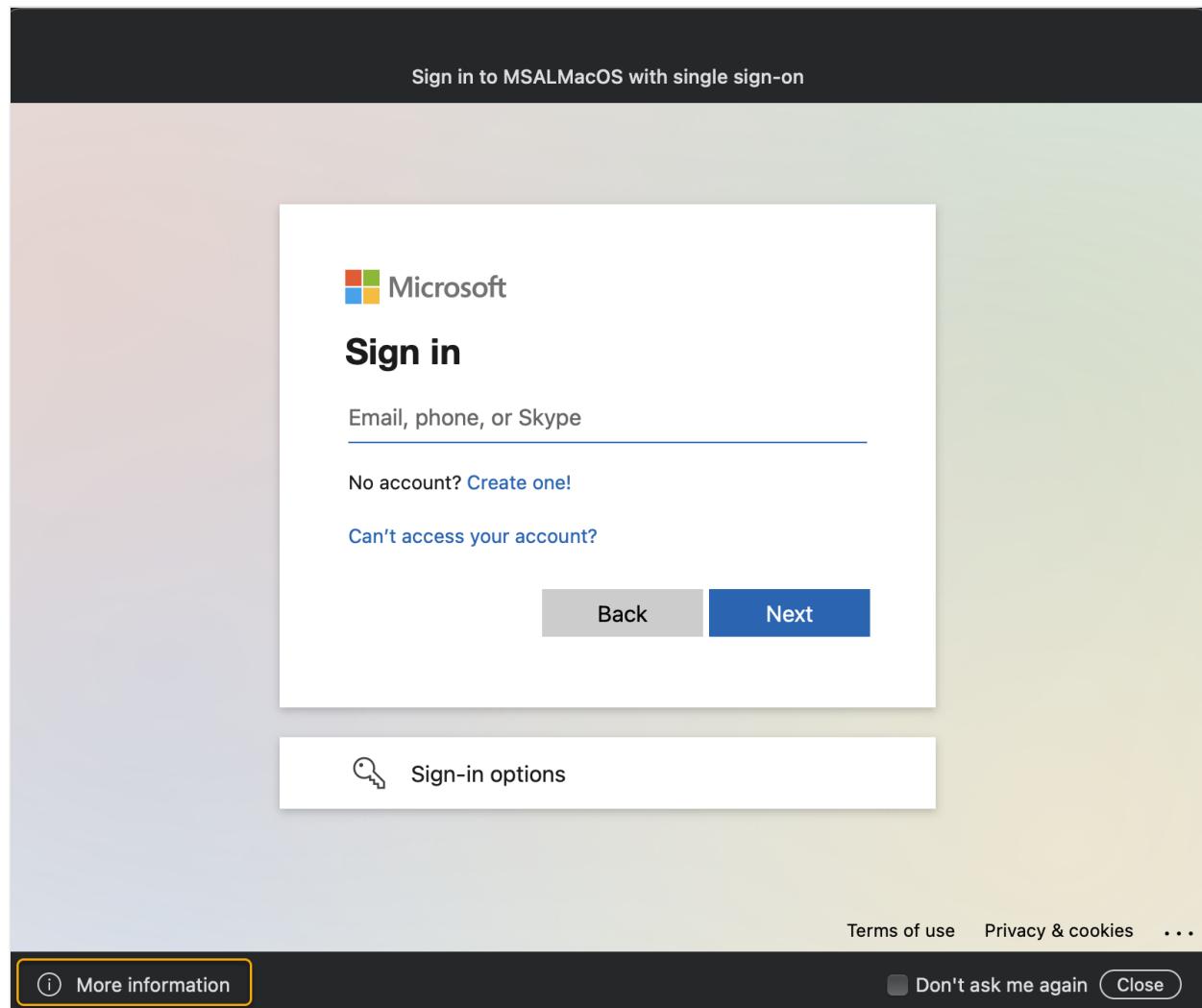
The logging sample can be broken down into three segments:

[Expand table](#)

Segment	Description
<code>get_accounts_operation</code>	<p>Checks to see if there are any existing accounts in the cache</p> <ul style="list-style-type: none"> - ClientID: The application ID registered in Microsoft Entra ID for this MSAL app <p>ADB 3.1.40 indicates that version of the Microsoft Enterprise SSO Extension Broker plugin</p>

Segment	Description
<code>login</code>	<p>Broker handles the request for Microsoft Entra ID:</p> <ul style="list-style-type: none"> - Handling interactive SSO request...: Denotes an interactive request - correlation_id: Useful for cross referencing with the Microsoft Entra server-side sign-in logs - scope: User.Read API permission scope being requested from the Microsoft Graph - client_version: version of MSAL that the application is running - redirect_uri: MSAL apps use the format <code>msauth.com.<Bundle ID>://auth</code>
PRT Request	<p>Bootstrapping process to acquire a PRT interactively has been initiated and renders the Webview SSO Session</p> <p>Microsoft Authentication Broker Service</p> <ul style="list-style-type: none"> - clientId: 29d9ed98-a469-4536-ade2-f981bc1d605e - All PRT requests are made to Microsoft Authentication Broker Service

The SSO Webview Controller appears and user is prompted to enter their Microsoft Entra login (UPN/email)



 **Note**

Clicking on the *i* in the bottom left corner of the webview controller displays more information about the SSO extension and the specifics about the app that has invoked it.

About single sign-on

Your device is set up with a single sign-on extension by your administrator. This will allow you to automatically log into your organization's resources on this device.

If you choose not to be prompted again, you can change this setting later in Company Portal.

Request details

Login URL

login.microsoftonline.com

Application

MSALMacOS

Application bundle identifier

com.microsoft.idnaace.MSALMacOS

Application team ID

Z2G4P4QR8D

Send diagnostic report

After the user successfully enters their Microsoft Entra credentials, the following log entries are written to the SSO extension logs

```
SSOExtensionLogs
///////////
//Acquire PRT//
///////////
[MSAL] -completeWebAuthWithURL: msauth://microsoft.aad.brokerplugin/?code=
```

```
(not-null)&client_info=(not-null)&state=(not-null)&session_state=(not-null)
[MSAL] Dismissed web view controller.
[MSAL] Result from authorization session callbackURL host:
microsoft.aad.brokerplugin , has error: NO
[MSAL] (Default accessor) Looking for token with aliases (
    "login.windows.net",
    "login.microsoftonline.com",
    "login.windows.net",
    "login.microsoft.com",
    "sts.windows.net"
), tenant (null), clientId 29d9ed98-a469-4536-ade2-f981bc1d605e, scopes
(null)
Saving PRT response in cache since no other PRT was found
[MSAL] Saving keychain item, item info Masked(not-null)
[MSAL] Keychain find status: 0
Acquired PRT.

///////////////////////////////
//Discover if there is an Azure AD Device Registration (WPJ) present //
//and if so re-acquire a PRT and associate with Device ID           //
/////////////////////////////
WPJ Discovery: do discovery in environment 0
Attempt WPJ discovery using tenantId.
WPJ discovery succeeded.
Using cloud authority from WPJ discovery:
https://login.microsoftonline.com/common
ADBrokerDiscoveryAction completed. Continuing Broker Flow.
PRT needs upgrade as device registration state has changed. Device is joined
1, prt is joined 0
Beginning ADBrokerAcquirePRTInteractivelyAction
Attempting to get Primary Refresh Token interactively.
Acquiring broker tokens for broker client id.
Resolving authority: Masked(not-null), upn: auth.placeholder-
61945244_domainname.com
Resolved authority, validated: YES, error: 0
Enrollment id read from intune cache : (null).
Handle silent PRT response Masked(not-null), error Masked(null)
Acquired broker tokens.
Acquiring PRT.
Acquiring PRT using broker refresh token.
Requesting PRT from authority
https://login.microsoftonline.com/<TenantID>/oauth2/v2.0/token
[MSAL] (Default accessor) Looking for token with aliases (
    "login.windows.net",
    "login.microsoftonline.com",
    "login.windows.net",
    "login.microsoft.com",
    "sts.windows.net"
), tenant (null), clientId (null), scopes (null)
[MSAL] Acquired PRT successfully!
Acquired PRT.
ADBrokerAcquirePRTInteractivelyAction completed. Continuing Broker Flow.
Beginning ADBrokerAcquireTokenWithPRTAction
Resolving authority: Masked(not-null), upn: auth.placeholder-
61945244_domainname.com
```

```
Resolved authority, validated: YES, error: 0
Handle silent PRT response Masked(not-null), error Masked(null)

///////////////////////////////
//Provide Access Token received from Azure AD back to Client Application//
//and complete authorization request                                //
///////////////////////////////
[MSAL] (Default cache) Removing credentials with type AccessToken,
environment login.windows.net, realm TenantID, clientID 08dc26ab-e050-465e-
beb4-d3f2d66647a5, unique user ID dbb22b2f, target User.Read profile openid
email
ADBBrokerAcquireTokenWithPRTAction succeeded.
Composing broker response.
Sending broker response.
Returning to app (msauth.com.microsoft.idnaace.MSALMacOS://auth) - protocol
version: 3
hash: 4A07DFC2796FD75A27005238287F2505A86BA7BB9E6A00E16A8F077D47D6D879
payload: Masked(not-null)
Completed interactive SSO request.
Completed interactive SSO request.
Request complete
Completing SSO request...
Finished SSO request.
```

At this point in the authentication/authorization flow, the PRT has been bootstrapped and it should be visible in the macOS keychain access. See [Checking Keychain Access for PRT](#). The **MSAL macOS sample** application uses the access token received from the Microsoft SSO Extension Broker to display the user's information.

Next, examine server-side [Microsoft Entra sign-in logs](#) based on the correlation ID collected from the client-side SSO extension logs. For more information, see [Sign-in logs in Microsoft Entra ID](#).

View Microsoft Entra sign-in logs by correlation ID filter

1. Open the Microsoft Entra Sign-ins for the tenant where the application is registered.
2. Select **User sign-ins (interactive)**.
3. Select the **Add Filters** and select the **Correlation Id** radio button.
4. Copy and paste the Correlation ID obtained from the SSO extension logs and select **Apply**.

For the MSAL Interactive Login Flow, we expect to see an interactive sign-in for the resource **Microsoft Authentication Broker** service. This event is where the user entered their password to bootstrap the PRT.

Activity Details: Sign-ins

Basic info Location Device info Authentication Details Conditional Access Report-only

Date 1/27/2023, 12:51:50 PM

Request ID 4c32d171-20e2-4af9-8e77-7624453e4a00

Correlation ID 3506307a-e90f-4916-9ed5-25cf81ae97fc

Authentication requirement Single-factor authentication

Status Success

Continuous access evaluation No

Follow these steps:

Troubleshoot Event

[Launch the Sign-in Diagnostic.](#)

1. Review the diagnosis and act on suggested fixes.

User type Member

Cross tenant access type None

Application Microsoft Authentication Broker

Application ID 29d9ed98-a469-4536-ade2-f981bc1d605e

Resource

Resource ID 90a2e5d2-fd7a-4a2e-bc90-3dc50ae8e3ee

There are also non-interactive sign-in events, due to the fact the PRT is used to acquire the access token for the client application's request. Follow the [View Microsoft Entra sign-in logs by Correlation ID Filter](#) but in step 2, select **User sign-ins (non-interactive)**.

Activity Details: Sign-ins

User type	Member
Cross tenant access type	None
Application	macOSNativeMSAL
Application ID	08dc26ab-e050-465e-beb4-d3f2d66647a5
Resource	Microsoft Graph
Resource ID	00000003-0000-0000-c000-000000000000
Client app	Mobile Apps and Desktop clients
Client credential type	None
Service principal ID	
Service principal name	
Token issuer type	Azure AD
Token issuer name	
Incoming token type	Primary refresh token
Authentication Protocol	None
Latency	228ms
Flagged for review	No
User agent	Mac%20SSO%20Extension/53.2212990.001 CFNetwork/1402.0.8 Darwin/22.2.0
[+] Expand table	

[+] Expand table

Sign-in log attribute	Description
Application	Display Name of the Application registration in the Microsoft Entra tenant where the client application authenticates.
Application Id	Also referred to the ClientID of the application registration in the Microsoft Entra tenant.
Resource	The API resource that the client application is trying to obtain access to. In this example, the resource is the Microsoft Graph API .
Incoming Token Type	An Incoming token type of Primary Refresh Token (PRT) shows the input token being used to obtain an access token for the resource.
User Agent	The user agent string in this example is showing that the Microsoft SSO Extension is the application processing this request. A useful indicator that the SSO extension is being used, and broker auth request is taking place.
Microsoft Entra app authentication	When an MSAL application is being used the details of the library and the platform are written here.

Sign-in log attribute	Description
library	
Oauth Scope Information	The Oauth2 scope information requested for the access token. (User.Read,profile,openid,email).

MSAL Native: Silent flow walkthrough

After a period of time, the access token will no longer be valid. So, if the user reclicks on the **Call Microsoft Graph API** button. The SSO extension attempts to refresh the access token with the already acquired PRT.

```
SSOExtensionLogs
///////////////////////////////
//refresh operation: Assemble Request based on User information in PRT /
///////////////////////////////
Beginning authorization request
Request does not need UI
Handling SSO request, requested operation: refresh
Handling silent SSO request...
Looking account up by home account ID dbb22b2f, displayable ID
auth.placeholder-61945244__domainname.com
Account identifier used for request: Masked(not-null), auth.placeholder-
61945244__domainname.com
Starting SSO broker request with payload: {
    authority = "https://login.microsoftonline.com/<TenantID>";
    "client_app_name" = MSALMacOS;
    "client_app_version" = "1.0";
    "client_id" = "08dc26ab-e050-465e-beb4-d3f2d66647a5";
    "client_version" = "1.1.7";
    "correlation_id" = "45418AF5-0901-4D2F-8C7D-E7C5838A977E";
    "extra_oidc_scopes" = "openid profile offline_access";
    "home_account_id" = "<UserObjectId>.<TenantID>";
    "instance_aware" = 0;
    "msg_protocol_ver" = 4;
    "provider_type" = "provider_aad_v2";
    "redirect_uri" = "msauth.com.microsoft.idnaace.MSALMacOS://auth";
    scope = "user.read";
    username = "auth.placeholder-61945244__domainname.com";
}
///////////////////////////////
//Acquire Access Token with PRT silently//
/////////////////////////////
Using request handler <ADSSOSilentBrokerRequestHandler: 0x127226a10>
Executing new request
Beginning ADBrokerAcquireTokenSilentAction
Beginning silent flow.
```

```

[MSAL] Resolving authority: Masked(not-null), upn: auth.placeholder-61945244_domainname.com
[MSAL] (Default cache) Removing credentials with type AccessToken, environment login.windows.net, realm <TenantID>, clientID 08dc26ab-e050-465e-beb4-d3f2d66647a5, unique user ID dbb22b2f, target User.Read profile openid email
[MSAL] (MSIDAccountCredentialCache) retrieving cached credentials using credential query
[MSAL] Silent controller with PRT finished with error Masked(null)
ADBrokerAcquireTokenWithPRTAction succeeded.
Composing broker response.
Sending broker response.
Returning to app (msauth.com.microsoft.idnaace.MSALMacOS://auth) - protocol version: 3
hash: 292FBF0D32D7EEDEB520098E44C0236BA94DDD481FAF847F7FF6D5CD141B943C
payload: Masked(not-null)
Completed silent SSO request.
Request complete
Completing SSO request...
Finished SSO request.

```

The logging sample can be broken down into two segments:

[] Expand table

Segment	Description
<code>refresh</code>	<p>Broker handles the request for Microsoft Entra ID:</p> <ul style="list-style-type: none"> - Handling silent SSO request...: Denotes a silent request - correlation_id: Useful for cross referencing with the Microsoft Entra server-side sign-in logs - scope: User.Read API permission scope being requested from the Microsoft Graph - client_version: version of MSAL that the application is running - redirect_uri: MSAL apps use the format <code>msauth.com.<Bundle ID>//auth</code> <p>Refresh has notable differences to the request payload:</p> <ul style="list-style-type: none"> - authority: Contains the Microsoft Entra tenant URL endpoint as opposed to the common endpoint - home_account_id: Show the User account in the format <code><UserObjectId>.<TenantID></code> - username: hashed UPN format <code>auth.placeholder-XXXXXXX_domainname.com</code>
PRT Refresh and Acquire Access Token	This operation revalidates the PRT and refreshes it if necessary, before returning the access token back to the calling client application.

We can again take the **correlation Id** obtained from the client-side **SSO Extension logs** and cross reference with the server-side Microsoft Entra sign-in logs.

Activity Details: Sign-ins

Basic info Location Device info Authentication Details Conditional Access Report-only ...

Correlation ID	45418af5-0901-4d2f-8c7d-e7c5838a977e
Authentication requirement	Single-factor authentication
Status	Success
Continuous access evaluation	No

Follow these steps:

Troubleshoot Event [Launch the Sign-in Diagnostic.](#)

- Review the diagnosis and act on suggested fixes.

User type	Member
Cross tenant access type	None
Application	macOSNativeMSAL
Application ID	08dc26ab-e050-465e-beb4-d3f2d66647a5
Resource	Microsoft Graph
Resource ID	00000003-0000-0000-c000-000000000000

Service principal ID	Authentication Details	Conditional Access	Report-only	Authentication Events	Additional Details
Service principal name	Azure AD app authentication library	Family: MSAL Library; MSALobjc 1.2.4 Platform: OSX			
Resource service principal ID	cb8ab605-418e-4f0	Root Key Type	Unknown		
Unique token identifier	Z_nH-XxbkE67VDVj	Oauth Scope Info	["User.Read","profile","openid","email"]		
Token issuer type	Azure AD				
Token issuer name					
Incoming token type	Primary refresh token				
Authentication Protocol	None				
Latency	131ms				
Flagged for review	No				
User agent	Mac%20SSO%20Extension/53.2212990.001 CFNetwork/1402.0.8 Darwin/22.2.0				

The Microsoft Entra Sign-in shows identical information to the Microsoft Graph resource from the **login** operation in the previous [interactive login section](#).

Non-MSAL/Browser SSO application login flow

The following section walks through how to examine the SSO extension logs for the Non-MSAL/Browser Application auth flow. For this example, we're using the Apple Safari browser as the client application, and the application is making a call to the Office.com (OfficeHome) web application.

Non-MSAL/Browser SSO flow walkthrough

The following actions should take place for a successful sign-on:

1. Assume that User who already has undergone the bootstrapping process has an existing PRT.
2. On a device, with the **Microsoft SSO Extension Broker** deployed, the configured **feature flags** are checked to ensure that the application can be handled by the SSO Extension.
3. Since the Safari browser adheres to the **Apple Networking Stack**, the SSO extension tries to intercept the Microsoft Entra auth request.
4. The PRT is used to acquire a token for the resource being requested.
5. If the device is Microsoft Entra registered, it passes the Device ID along with the request.
6. The SSO extension populates the header of the Browser request to sign-in to the resource.

The following client-side **SSO Extension** logs show the request being handled transparently by the SSO extension broker to fulfill the request.

```
SSOExtensionLogs
Created Browser SSO request for bundle identifier com.apple.Safari, cookie
SSO include-list (
), use cookie sso for this app 0, initiating origin https://www.office.com
Init MSIDKeychainTokenCache with keychainGroup: Masked(not-null)
[Browser SSO] Starting Browser SSO request for authority
https://login.microsoftonline.com/common
[MSAL] (Default accessor) Found 1 tokens
[Browser SSO] Checking PRTs for deviceId 73796663
[MSAL] [Browser SSO] Executing without UI for authority
https://login.microsoftonline.com/common, number of PRTs 1, device
registered 1
[MSAL] [Browser SSO] Processing request with PRTs and correlation ID in
headers (null), query 67b6a62f-6c5d-40f1-8440-a8edac7a1f87
[MSAL] Resolving authority: Masked(not-null), upn: Masked(null)
[MSAL] No cached preferred_network for authority
[MSAL] Caching AAD Environements
[MSAL] networkHost: login.microsoftonline.com, cacheHost: login.windows.net,
aliases: login.microsoftonline.com, login.windows.net, login.microsoft.com,
sts.windows.net
[MSAL] networkHost: login.partner.microsoftonline.cn, cacheHost:
login.partner.microsoftonline.cn, aliases: login.partner.microsoftonline.cn,
login.chinacloudapi.cn
[MSAL] networkHost: login.microsoftonline.de, cacheHost:
login.microsoftonline.de, aliases: login.microsoftonline.de
[MSAL] networkHost: login.microsoftonline.us, cacheHost:
login.microsoftonline.us, aliases: login.microsoftonline.us,
```

```

login.usgovcloudapi.net
[MSAL] networkHost: login-us.microsoftonline.com, cacheHost: login-
us.microsoftonline.com, aliases: login-us.microsoftonline.com
[MSAL] Resolved authority, validated: YES, error: 0
[MSAL] Found registration registered in login.microsoftonline.com,
isSameAsRequestEnvironment: Yes
[MSAL] Passing device header in browser SSO for device id 43cfaf69-0f94-
4d2e-a815-c103226c4c04
[MSAL] Adding SSO-cookie header with PRT Masked(not-null)
SSO extension cleared cookies before handling request 1
[Browser SSO] SSO response is successful 0
[MSAL] Keychain find status: 0
[MSAL] (Default accessor) Found 1 tokens
Request does not need UI
[MSAL] [Browser SSO] Checking PRTs for deviceId 73796663
Request complete

```

[] Expand table

SSO extension log component	Description
Created Browser SSO request	All Non-MSAL/Browser SSO requests begin with this line: - bundle identifier: Bundle ID: com.apple.Safari - initiating origin: Web URL the browser is accessing before hitting one of the login URLs for Microsoft Entra ID (https://office.com)
Starting Browser SSO request for authority	Resolves the number of PRTs and if the Device is Registered: https://login.microsoftonline.com/common , number of PRTs 1, device registered 1
Correlation ID	[Browser SSO] Processing request with PRTs and correlation ID in headers (null), query <CorrelationID>. This ID is important for cross-referencing with the Microsoft Entra server-side sign-in logs
Device Registration	Optionally if the device is Microsoft Entra registered, the SSO extension can pass the device header in Browser SSO requests: - Found registration registered in login.microsoftonline.com , isSameAsRequestEnvironment: Yes Passing device header in browser SSO for device id 43cfaf69-0f94-4d2e-a815-c103226c4c04

Next, use the correlation ID obtained from the Browser SSO extension logs to cross-reference the Microsoft Entra sign-in logs.

Activity Details: Sign-ins

Basic info Location Device info Authentication Details Conditional Access Report-only ...

Correlation ID	67b6a62f-6c5d-40f1-8440-a8edac7a1f87
Authentication requirement	Single-factor authentication
Status	Success
Continuous access evaluation	No
Follow these steps:	
Troubleshoot Event	Launch the Sign-in Diagnostic.
1. Review the diagnosis and act on suggested fixes.	
User	Username User ID Sign-in identifier User type Member
Cross tenant access type	None
Application	OfficeHome
Application ID	4765445b-32c6-49b0-83e6-1d93765276ca
Resource	OfficeHome
Resource ID	4765445b-32c6-49b0-83e6-1d93765276ca

Basic info	Location	Device info	Authentication Details	Conditional Access	Report-only
Device ID	43cfaf69-0f94-4d2e-a815-c103226c4c04	Browser	Safari 16.2	Operating System	MacOS
Compliant	Yes	Managed	Yes	Join Type	Azure AD registered
Authentication met... Authentication method det... Success... Result detail					
Previously satisfied	Azure AD SSO plug-in	true	First factor requirement satisfied by claim in the token		

Client app	Browser	Authentication Details	Conditional Access	Report-only	Authentication Events	Additional Details
Client credential type	None	Azure AD SSO extension version 3.1.40				
Service principal ID		Root Key Type	Unknown			
Service principal name						
Resource service principal ID	4990eaeb-dee2-4a9e-a37f-e60f00cc39bc					
Unique token identifier	P2vMH5JUkiPkrp0c51LAA					
Token issuer type	Azure AD					
Token issuer name						
Incoming token type	Primary refresh token					
Authentication Protocol	None					
Latency	86ms					
Flagged for review	No					
User agent	Mozilla/5.0 (Macintosh; Intel Mac OS X 10_15_7) AppleWebKit/605.1.15 (KHTML, like Gecko) Version/16.2 Safari/605.1.15					

[\[\]](#) Expand table

Sign-in log attribute	Description
Application	Display Name of the Application registration in the Microsoft Entra tenant where the client application authenticates. In this example, the display name is OfficeHome .
Application Id	Also referred to the ClientID of the application registration in the Microsoft Entra tenant.
Resource	The API resource that the client application is trying to obtain access to. In this example, the resource is the OfficeHome web application.
Incoming Token Type	An Incoming token type of Primary Refresh Token (PRT) shows the input token being used to obtain an access token for the resource.

Sign-in log attribute	Description
Authentication method detected	Under the Authentication Details tab, the value of Microsoft Entra SSO plug-in is useful indicator that the SSO extension is being used to facilitate the Browser SSO request
Microsoft Entra SSO extension version	Under the Additional Details tab, this value shows the version of the Microsoft Enterprise SSO extension Broker app.
Device ID	If the device is registered, the SSO extension can pass the Device ID to handle device authentication requests.
Operating System	Shows the type of operating system.
Compliant	SSO extension can facilitate Compliance policies by passing the device header. The requirements are: - Microsoft Entra Device Registration - MDM Management - Intune or Intune Partner Compliance
Managed	Indicates that device is under management.
Join Type	macOS and iOS, if registered, can only be of type: Microsoft Entra registered .

💡 Tip

If you use Jamf Connect, it is recommended that you follow the [latest Jamf guidance on integrating Jamf Connect with Microsoft Entra ID](#). The recommended integration pattern ensures that Jamf Connect works properly with your Conditional Access policies and Microsoft Entra ID Protection.

Next steps

- [Microsoft Enterprise SSO plug-in for Apple devices \(preview\)](#)
- [Deploy the Microsoft Enterprise SSO plug-in for Apple Devices \(preview\)](#)

macOS Platform single sign-on known issues and troubleshooting (preview)

Article • 02/10/2025

This article outlines the current known issues and common questions with macOS Platform single sign-on (PSSO). It provides issue solutions and information on how to report an issue that isn't covered. This article also includes troubleshooting guidance.

Scenarios to validate

Once PSSO is deployed on your device, there are a few validation scenarios that you can do to ensure that the deployment is successful. If there are any issues, refer to [report an issue](#) for further instructions.

Password change events

Confirm that changes to Microsoft Entra ID password made through self-service password reset (SSPR) are successfully synchronized to the local machine. If a user's Microsoft Entra ID password changes after syncing it to the Mac, the user is prompted to enter their new password within 4 hours.

Repair or remove PSSO registration from a device

This section outlines how to repair or remove PSSO registration from a Mac device, depending on the macOS version.

macOS 14

On macOS 14 Sonoma, if there are problems with your device registration, you can repair the existing PSSO registration.

1. Open the **Settings** app and navigate to **Users & Groups > Network Account Server**.
2. Select **Edit**, then **Repair**. You're taken through the same device registration flow as when during your initial registration.

You can also deregister the device completely by doing the following steps.

1. Open the **Company Portal** app and navigate to **Preferences**.

2. To deregister the device, select **Deregister**.

Enterprise Single sign-on (SSO) plug-in doesn't activate after system update

If the Enterprise SSO plug-in fails to activate after system updates are applied to the device, you should reboot the software update daemon.

1. Open the **Terminal** app and enter the following command to kill the `swcd` process.

```
Console  
sudo killall swcd
```

2. Then enter the following command to reset the process.

```
Console  
sudo swcutil reset
```

Temporary passwords issued during password reset can't be synced with Platform SSO

Temporary passwords issued during password reset can't be synced to the local device. Users are advised to complete the password reset process using their temporary password using the SSO extension.

Device migration

Confirm that a previously registered device (with a Workplace Join key in Keychain Access) removes the key after successful PSSO device registration.

Frequently asked questions

Can I use macOS PSSO in a hybrid-join deployment?

No, macOS PSSO is only supported in Microsoft Entra join deployments. There are no plans to support hybrid-join deployments, as we recommend that Mac users go fully cloud based.

How can I change my password when using Platform SSO?

Users can change their password using Self-Service Password Reset (SSPR) on their device.

If SSPR is done on another machine, users are allowed to sign-in to the Mac device using either the old or the new password. Using the old password unlocks the device and then prompt the user for the new password to continue syncing data. Using the new password unlocks the device and sync data immediately.

We recommend that IT Admins should use [Managed Apple IDs](#) where possible as this does give organizations more options for password management.

What should I do if I forget my password?

Password Sync

Users can reset their password at the login screen or lock screen. If the user received a temporary password from an IT admin they should use another device to log in, set up a new password and use that new password at to log in to their own device. For more info, refer [Apple's documentation on forgotten passwords](#).

Important

There is currently a known issue with PSSO that is causing registration removal during recovery and may prompt users to re-register after recovery. This is expected behavior.

IT Admins should also enable Keyvault recovery to ensure data can be recovered in case of a forgotten password. To learn more, refer to [Configure Platform SSO for macOS devices in Microsoft Intune](#).

Note

If the device is booted and there is FileVault encryption the new Entra password will work on macOS15 only.

Secure Enclave

Users can reset the local password via Apple ID or an admin recovery key.

Known issues

Unexpected/frequent re-registration prompts on macOS Sequoia

Note

Latest update on the PSSO re-registration issue on macOS 15.x described below: Apple confirmed the fix is deployed in macOS 15.3. If users still experience the re-registration issue on macOS 15.3+, please engage with Apple and share the logs via Apple support.

There's a known concurrency issue on macOS 15+ (Sequoia) that can cause the PSSO device configuration to become corrupted. The device configuration can be corrupted by simultaneous updates from the system AppSSOAgent and AppSSODaemon processes. The corrupted configuration causes the operating system to trigger its re-registration remediation flow, resulting in unexpected registration prompts for users.

This issue is currently being investigated by Apple..

Sysdiagnose logs from affected users contain the following error:

```
Error Domain=com.apple.PlatformSSO Code=-1001 "Error deserializing device config." UserInfo={NSLocalizedDescription=Error deserializing device config., NSUnderlyingError=0x9480343f0 {Error Domain=NSCocoaErrorDomain Code=3840 "Garbage at end around line 27, column 1." UserInfo={NSDebugDescription=Garbage at end around line 27, column 1., NSJSONSerializationErrorIndex=3052}}}
```

We encourage users and admins who encounter this error to file an Apple Care issue and engage with Apple to resolve the issue.

Passcode policy complexity mismatches

There's a known issue where an applied MDM configuration specifies a local password policy with a higher degree of complexity than the Microsoft Entra account used to

sign-in to the machine. In this case, the password synchronization operation between Microsoft Entra ID and the local machine fails.

Ensure during the MDM configuration that the password complexity requirements are identical between the local machine and Microsoft Entra ID.

Long running operations

macOS 14

If the device registration fails through the Settings application, the Device Registration popup will reappear after about 10 minutes, and you can try again.

SSO auth prompt dialog closed while the registration is in progress

If you cancel the registration process by closing the SSO auth prompt dialog, you need to sign out from your Mac device and sign in again. Upon a successful sign in, the registration notification reappears and works correctly.

Per-user MFA causes password sync failure

If a user has per user MFA enabled on the account where PSSO is being set up, you won't be able to enter Microsoft Entra ID credentials in the next steps, causing an error. To avoid this error, admins should ensure they have Conditional Access MFA enabled in accordance with [Microsoft Entra ID recommendations](#). This suppresses MFA during enrollment so that password synchronization can be completed successfully.

PSSO reregistration required after password reset initiated from FileVault recovery or MDM-driven recovery

Because Secure Enclave keys are protected by your local account password, password resets that occur without providing this password (such as FileVault or MDM-based recovery) resets the Secure Enclave. Resetting the Secure Enclave renders keys previously stored for this account inaccessible. Devices whose Secure Enclave keys are lost must be reregistered to use Platform SSO.

Report an issue

If you're experiencing issues with PSSO, you can report them on Company Portal.

1. Open the **Company Portal** app and navigate **Help > Send diagnostic report**.
2. A **Send diagnostic report** window appears. Select **Email logs** to send the logs.
3. Take note of your incident ID before closing the window.

You can check the current PSSO state on your machine at any time by opening the **Terminal** app. Run the following command.

```
Console  
app-sso platform -s
```

Contact us

We'd love to hear your feedback. You should include the following information:

- Sysdiagnose and diagnostic logs
- Steps to reproduce the issue
- Where applicable, include relevant screenshots and/or recordings

Capturing Sysdiagnose and diagnostic logs

1. Enable debug logs persistence by running the following command in Terminal.

```
Console  
sudo log config --mode "level:debug,persist:debug" --subsystem  
"com.apple.AppSSO"
```

2. Reproduce the issue, such that new logs are generated for the affected scenario.
Provide relevant timestamps in your issue report to help log investigation.

3. Capture diagnostic data by running the following command in Terminal.

```
Console  
sudo sysdiagnose
```

4. Reset the debug logs to default settings by running the following command in Terminal.

```
Console
```

```
sudo log config --reset --subsystem "com.apple.AppSSO"
```

Troubleshooting guide

Insufficient permissions

If a user has insufficient permissions to complete Microsoft Entra ID join and registration, no error message is shown. For the device join and registration to complete successfully, the user initiating the registration flow must be allowlisted.

1. In the [Microsoft Entra admin center](#), navigate to **Identity > Devices > Overview > Device Settings**.
2. Under **Microsoft Entra ID join and registration settings**, ensure that the **All** option is selected in the toggle menu for **Users may join devices to Microsoft Entra**.
3. Select **Save** to apply the changes.

Troubleshoot Passkey issues

Platform Credential as Passkey option is only available if Secure Enclave is configured as the authentication method for Platform SSO. You should check the following:

1. Ensure that your admin set up your device with Secure Enclave as the authentication method, and [enabled passkeys \(FIDO2\) for your organization](#).
2. As a user, check that you have enabled Company Portal as a passkey provider in your device settings. Navigate to your **Settings app, Passwords and Password options**, and ensure that **Company Portal** is enabled.

Troubleshoot Microsoft Edge SSO issues

If Edge users are facing SSO issues after Platform SSO registration, please check if the user has signed into the Edge profile. Users will need to sign into their Edge profile for browser SSO to work with Edge on Platform SSO registered devices.

Troubleshoot Google Chrome SSO issues

For users with the [Microsoft Single Sign On](#) extension for Google Chrome installed, then their Chrome browser should be able communicate with the Microsoft SSO broker for both an SSO user experience and to work with device-based Conditional Access policies. If users aren't able to pass device-based Conditional Access policies in Google

Chrome then there may be an issue with how the Company Portal application was installed, which can prevent Chrome from communicating with the SSO broker. You should take the following steps to remediate this issue:

1. Open the **Applications** folder on the Mac
2. Right click the **Company Portal** application and choose **Move to Trash**
3. Download the latest version of the Company Portal installer from
[https://go.microsoft.com/fwlink/?linkid=853070 ↗](https://go.microsoft.com/fwlink/?linkid=853070)
4. Freshly install Company Portal using the downloaded **CompanyPortal-Installer.pkg**

Validate that the issue is resolved by checking for the **existence of this file**:

```
~/Library/Application\  
Support/Google/Chrome/NativeMessagingHosts/com.microsoft.browsercore.json
```

```
Console  
  
ls ~/Library/Application\  
Support/Google/Chrome/NativeMessagingHosts/com.microsoft.browsercore.json
```

Alternatively, you can deploy the following script via your MDM or other automation tools to copy the JSON file to the correct location. This script should be run in the user's context for each user who experiences the Chrome SSO issue:

```
zsh  
  
#!/usr/bin/env zsh  
# Copy over Browser Core json file to the right location  
# If the folder doesn't exist, create it  
  
# For Google Chrome (user-specific, default path)  
  
if [ ! -d ~/Library/Application\ Support/Google/Chrome/NativeMessagingHosts ]; then  
    mkdir ~/Library/Application\ Support/Google/Chrome/NativeMessagingHosts  
fi  
  
cp /Applications/Company\  
Portal.app/Contents/Resources/com.microsoft.browsercore.json  
~/Library/Application\ Support/Google/Chrome/NativeMessagingHosts/  
  
# For Edge (user-specific, default path, not channel specific)  
# See: https://learn.microsoft.com/microsoft-edge/extensions-  
chromium/developer-guide/native-messaging?tabs=v3%2Cmacos  
  
if [ ! -d ~/Library/Application\ Support/Microsoft\  
Edge/NativeMessagingHosts ]; then  
    mkdir ~/Library/Application\ Support/Microsoft\ Edge/NativeMessagingHosts  
fi
```

```
cp /Applications/Company\  
Portal.app/Contents/Resources/com.microsoft.browsercore.json  
~/Library/Application\ Support/Microsoft\ Edge/NativeMessagingHosts/
```

Important

Note: This issue is due to a bug with how Company Portal is installed or updated under certain circumstances. This issue will be resolved in a future update to Company Portal.

See also

- [Join a Mac device with Microsoft Entra ID during the out of box experience](#)
- [Join a Mac device with Microsoft Entra ID using Company Portal](#)
- [Microsoft Enterprise SSO plug-in for Apple devices](#)
- [Troubleshooting the Microsoft Enterprise SSO Extension plugin on Apple devices](#)

Feedback

Was this page helpful?



Yes



No

[Provide product feedback ↗](#)

Enable Enterprise State Roaming in Microsoft Entra ID

Article • 08/01/2024

Enterprise State Roaming provides users with a unified experience across their Windows devices and reduces the time needed for configuring a new device. Enterprise State Roaming operates similar to the standard [consumer settings sync](#) that was first introduced in Windows 8. Enterprise State Roaming is available to any organization with a Microsoft Entra ID P1 or P2 or Enterprise Mobility + Security (EMS) license. For more information on how to get a Microsoft Entra subscription, see the [Microsoft Entra product page](#).

ⓘ Note

This article applies to the Microsoft Edge Legacy HTML-based browser launched with Windows 10 in July 2015. The article does not apply to the new Microsoft Edge Chromium-based browser released on January 15, 2020. For more information on the Sync behavior for the new Microsoft Edge, see the article [Microsoft Edge Sync](#).

To enable Enterprise State Roaming

1. Sign in to the [Microsoft Entra admin center](#) as a [Global Administrator](#).
2. Browse to **Identity > Devices > Overview > Enterprise State Roaming**.
3. Select **Users may sync settings and app data across devices**. For more information, see [how to configure device settings](#).

For a Windows 11 or Windows 10, version 21H2 or newer device to use the Enterprise State Roaming service, the device must authenticate using a Microsoft Entra identity. For devices that are joined to Microsoft Entra ID, the user's primary sign-in identity is their Microsoft Entra identity, so no other configuration is required. For devices that use on-premises Active Directory, the IT admin must [Configure Microsoft Entra hybrid joined devices](#).

Data storage

Enterprise State Roaming data is hosted in one or more [Azure regions](#) that best align with the country/region value set in the Microsoft Entra instance. Enterprise State Roaming data is partitioned based on three major geographic regions: North America,

EMEA, and APAC. Enterprise State Roaming data for the tenant is locally located with the geographical region, and isn't replicated across regions. For example:

[+] [Expand table](#)

Country/region value	has their data hosted in
An EMEA country/region such as France or Zambia	One or more of the Azure regions within Europe
A North American country/region such as United States or Canada	One or more of the Azure regions within the US
An APAC country/region such as Australia or New Zealand	One or more of the Azure regions within Asia
South American and Antarctica regions	One or more Azure regions within the US

The country/region value is set as part of the Microsoft Entra directory creation process and can't be modified later. If you need more details on your data storage location, file a ticket with [Azure support](#).

Data retention

Data synced to the Microsoft cloud using Enterprise State Roaming is retained until manually deleted or the data is determined to be stale.

Explicit deletion

Explicit deletion is when an administrator deletes a user, directory, or requests explicitly that data is to be deleted.

- **User deletion:** When a user is deleted in Microsoft Entra ID, the user account roaming data is deleted after 90 to 180 days.
- **Directory deletion:** Deleting an entire directory in Microsoft Entra ID is an immediate operation. All the settings data associated with that directory is deleted after 90 to 180 days.
- **On request deletion:** If the Microsoft Entra admin wants to manually delete a specific user's data or settings data, the admin can file a ticket with [Azure support](#).

Stale data deletion

Data that isn't accessed for one year ("the retention period") is treated as stale and might be deleted from the Microsoft cloud. The retention period is subject to change but isn't less than 90 days. The stale data might be a specific set of Windows/application settings or all settings for a user. For example:

- If no devices access a particular settings collection like language, then that collection becomes stale after the retention period and might be deleted.
- If a user turned off settings sync on all their devices, then none of the settings data is accessed. All the settings data for that user will become stale and might be deleted after the retention period.
- If the Microsoft Entra directory admin turns off Enterprise State Roaming for the entire directory, then all users in that directory stop syncing settings. All settings data for all users will become stale and might be deleted after the retention period.

Deleted data recovery

The data retention policy isn't configurable. Once the data is permanently deleted, it isn't recoverable. However, The settings data is deleted only from the Microsoft cloud, not from the end-user device. If any device later reconnects to the Enterprise State Roaming service, the settings are again synced and stored in the Microsoft cloud.

Next steps

- [Settings and data roaming FAQ](#)
- [Group Policy and MDM settings for settings sync](#)
- [Windows 10 roaming settings reference](#)
- [Troubleshooting](#)

Feedback

Was this page helpful?

 Yes

 No

[Provide product feedback ↗](#)

Settings and data roaming FAQ for administrators

FAQ

This article answers some questions IT administrators might have about settings and app data sync.

What account is used for settings sync?

In Windows 8.1, settings sync always used consumer Microsoft accounts. Enterprise users had the ability to connect a Microsoft account to their Active Directory domain account to gain access to settings sync. In Windows 10 and newer, this connected Microsoft account functionality is being replaced with a primary/secondary account framework.

The primary account is defined as the account used to sign in to Windows. This can be a Microsoft account, a Microsoft Entra account, an on-premises Active Directory account, or a local account. In addition to the primary account, Windows 10 and newer users can add one or more secondary cloud accounts to their device. A secondary account is generally a Microsoft account, a Microsoft Entra account, or some other account such as Gmail or Facebook. These secondary accounts provide access to other services such as single sign-on and the Windows Store, but they aren't capable of powering settings sync.

Data is never mixed between the different user accounts on the device. There are two rules for settings sync:

- Windows settings always roam with the primary account.
- App data is tagged with the account used to acquire the app. Only apps tagged with the primary account sync. App ownership tagging is determined when an app is side-loaded through the Windows Store or mobile device management (MDM).

If an application owner can't be identified, it will roam with the primary account. If a device is upgraded from Windows 8 or Windows 8.1 to Windows 10 and newer, all the apps are tagged as acquired by the Microsoft account. This is because most users acquire apps through the Windows Store, and there was no Windows Store support for Microsoft Entra accounts prior to Windows 10. If an app is installed via an offline license, the app is tagged using the primary account on the device.

Note

Windows 10 or newer devices that are enterprise-owned and are connected to Microsoft Entra ID can no longer connect their Microsoft accounts to a domain account. The ability

to connect a Microsoft account to a domain account and have all the user's data sync to the Microsoft account (that is, the Microsoft account roaming via the connected Microsoft account and Active Directory functionality) is removed from Windows 10 and newer devices that are joined to a connected Active Directory or Microsoft Entra environment.

How do I upgrade from Microsoft account settings sync in Windows 8 to Microsoft Entra settings sync in Windows 10 or newer?

After upgrading to Windows 10 and newer, you continue to sync user settings via Microsoft account as long as you're a domain-joined user, and the Active Directory domain doesn't connect with Microsoft Entra ID.

If the on-premises Active Directory domain does connect with Microsoft Entra ID, your device attempts to sync settings using the connected Microsoft Entra account. If the Microsoft Entra administrator doesn't enable Enterprise State Roaming, your connected Microsoft Entra account stops syncing settings. If you're running Windows 10 and newer and you sign in with a Microsoft Entra identity, you start syncing windows settings as soon as your administrator enables settings sync via Microsoft Entra ID.

If you stored any personal data on your corporate device, you should know Windows OS and application data begin syncing to Microsoft Entra ID. This has the following implications:

- Your personal Microsoft account settings will drift from the settings on your work or school Microsoft Entra accounts. This is because the Microsoft account and Microsoft Entra settings sync are now using separate accounts.
- Personal data such as Wi-Fi passwords, web credentials, and Internet Explorer favorites that were previously synced via a connected Microsoft account is synced via Microsoft Entra ID.

How do Microsoft account and Microsoft Entra Enterprise State Roaming interoperability work?

In the November 2015 or later releases of Windows 10, Enterprise State Roaming is only supported for a single account at a time. If you sign in to Windows by using a work or school

Microsoft Entra account, all data syncs via Microsoft Entra ID. If you sign in to Windows by using a personal Microsoft account, all data syncs via the Microsoft account. Universal app data roam using only the primary sign-in account on the device, and it roams only if the app's license is owned by the primary account. Universal app data for the apps owned by any secondary accounts isn't synced.

Do settings sync for Microsoft Entra accounts from multiple tenants?

When multiple Microsoft Entra accounts from different Microsoft Entra tenants are on the same device, you must update the device's registry to communicate with the Azure Rights Management service for each Microsoft Entra tenant.

1. Find the GUID for each Microsoft Entra tenant. Sign in to the [Microsoft Entra admin center](#), browse to **Entra ID > Overview > Properties > Tenant ID**.
2. After you have the GUID, you'll need to add the registry key `HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\SettingSync\WinMSIPC<tenant ID GUID>`. From the **tenant ID GUID** key, create a new Multi-String value (REG-MULTI-SZ) named **AllowedRMSServerUrls**. For its data, specify the licensing distribution point URLs of the other Azure tenants that the device accesses.
3. You can find the licensing distribution point URLs by running the **Get-AadrmConfiguration** cmdlet from the AADRM module. If the values for the **LicensingIntranetDistributionPointUrl** and **LicensingExtranetDistributionPointUrl** are different, specify both values. If the values are the same, specify the value once.

Can I store synced settings and data on-premises?

Enterprise State Roaming stores all synced data in the Microsoft cloud. UE-V offers an on-premises roaming solution.

How is the data secured?

Prior to Nov 2022 all user data was secured using [Azure Rights Management](#).

Starting in November 2022, Microsoft no longer uses Azure Rights Management for all data encryption. Microsoft is committed to safeguarding customer data. Certain sensitive data such as passwords are encrypted client side with keys derived from the Microsoft Entra tenant to ensure an extra layer of security. All user data (including nonsensitive data) is encrypted in

transit and at rest in the cloud. For a list of sensitive and nonsensitive data items roamed, see [Windows roaming settings reference](#).

Can I manage sync for a specific app or setting?

In Windows 10 or newer, administrators can disable sync for all settings sync groups on a managed device with MDM or Group Policy.

How can I enable or disable roaming?

In the **Settings** app, go to **Accounts > Sync your settings**. From this page, you can see which account is being used to roam settings, and you can enable or disable individual groups of settings to be roamed.

What is Microsoft's recommendation for enabling roaming in Windows 10 or newer?

Microsoft has a few different settings roaming solutions available, including UE-V and Enterprise State Roaming. If your organization isn't ready or comfortable with moving data to the cloud, then we recommend that you use UE-V as your primary roaming technology. If your organization requires roaming support for existing Windows desktop applications but is eager to move to the cloud, we recommend that you use both Enterprise State Roaming and UE-V. Although UE-V and Enterprise State Roaming are similar technologies, they aren't mutually exclusive. They complement each other to help ensure that your organization provides the roaming services that your users need.

When using both Enterprise State Roaming and UE-V, Enterprise State Roaming is the primary roaming agent on the device. UE-V is being used to supplement Win32 applications.

- Enterprise State Roaming is the primary roaming agent on the device. UE-V is being used to supplement the "Win32 gap."
- UE-V roaming for Windows settings and modern UWP app data should be disabled when using the UE-V group policies. These settings are already covered by Enterprise State Roaming.

How does Enterprise State Roaming support virtual desktop infrastructure

(VDI)?

Enterprise State Roaming is supported on Windows 10 or newer client SKUs, but not on server SKUs. If a client VM is hosted on a hypervisor machine and you remotely sign in to the virtual machine, your data will roam. If multiple users share the same OS and users remotely sign in to a server for a full desktop experience, roaming might not work. The latter session-based scenario isn't officially supported.

What happened to the per-user device sync status report?

The per-user device sync status report was removed from the Microsoft Entra admin center. The report was removed because it only provided details for unsupported versions of Windows. Enterprise state roaming requires Windows 11 or Windows 10 version 21H2 or newer.

Next steps

For an overview, see [enterprise state roaming overview](#)

Troubleshooting Enterprise State Roaming settings in Microsoft Entra ID

Article • 02/27/2025

This article provides information on how to troubleshoot and diagnose issues with Enterprise State Roaming, and provides a list of known issues.

Note

We recommend that you use the Azure Az PowerShell module to interact with Azure. See [Install Azure PowerShell](#) to get started. To learn how to migrate to the Az PowerShell module, see [Migrate Azure PowerShell from AzureRM to Az](#).

Note

The article does not apply to the new Microsoft Edge Chromium-based browser released on January 15, 2020. For more information on the Sync behavior for the new Microsoft Edge, see the article [Microsoft Edge Sync](#).

Preliminary steps for troubleshooting

Before you start troubleshooting, verify that the user and device are configured properly, and that all the requirements of Enterprise State Roaming are met.

1. Windows 10 or newer, with the latest updates, and a minimum Version 22H2 (OS Build 19045 or later) is installed on the device.
2. The device is Microsoft Entra joined or Microsoft Entra hybrid joined. For more information, see [how to get a device under the control of Microsoft Entra ID](#).
3. Ensure that **Enterprise State Roaming** is enabled for the tenant in Microsoft Entra ID as described in [To enable Enterprise State Roaming](#). You can enable roaming for all users or for only a selected group of users.
4. The user is assigned a Microsoft Entra ID P1 or P2 license.
5. The device must be restarted and the user must sign in again to access Enterprise State Roaming features.

Troubleshooting and diagnosing issues

This section gives suggestions on how to troubleshoot and diagnose problems related to Enterprise State Roaming.

Verify sync, and the "Sync your settings" settings page

1. After joining your Windows 10 or newer PC to a domain that is configured to allow Enterprise State Roaming, sign on with your work account. Go to **Settings > Accounts > Sync Your Settings** and confirm that sync and the individual settings are on, and that the top of the settings page indicates that you're syncing with your work account. Confirm the same account is also used as your account in **Settings > Accounts > Your Info**.
2. Verify that sync works across multiple machines by making some changes on the original machine, such as changing the "Country or Region" or using other supported settings see [Windows roaming settings reference](#). Watch the change propagate to the second machine within five minutes.
 - Locking and unlocking the screen (Win + L) can help trigger a sync.
 - You must be signing in with the same account on both PCs for sync to work – as Enterprise State Roaming is tied to the user account and not the machine account.

Potential issue: If the controls in the **Settings** page aren't available, and you see the message "Some Windows features are only available if you're using a Microsoft account or work account." This issue might arise for devices that are set up to be domain-joined and registered to Microsoft Entra ID, but the device hasn't authenticated to Microsoft Entra ID yet. A possible cause is that the device policy must be applied, but this application happens asynchronously, and might take a few hours.

Verify the device registration status

Enterprise State Roaming requires the device to be registered with Microsoft Entra ID. Although not specific to Enterprise State Roaming, using the following instructions can help confirm that the Windows 10 or newer Client is registered, and confirm thumbprint, Microsoft Entra settings URL, NGC status, and other information.

1. Open the command prompt unelevated. To do this in Windows, open the Run launcher (Win + R) and type "cmd" to open.
2. Once the command prompt is open, type `*dsregcmd.exe /status*`.

3. For expected output, the **AzureAdJoined** field value should be **YES**, the **WamDefaultSet** field value should be **YES**, and the **WamDefaultGUID** field value should be a GUID with **(AzureAD)** at the end.

Potential issue: **WamDefaultSet** and **AzureAdJoined** both have "NO" in the field value, the device was domain-joined and registered with Microsoft Entra ID, and the device doesn't sync. If it's showing this, the device might need to wait for policy to be applied or the authentication for the device failed when connecting to Microsoft Entra ID. The user might have to wait a few hours for the policy to be applied. Other troubleshooting steps might include retrying autoregistration by signing out and back in, or launching the task in Task Scheduler. In some cases, running "`dsregcmd.exe /leave`" in an elevated command prompt window, rebooting, and trying registration again might help with this issue.

Potential issue: The field for **SettingsUrl** is empty and the device doesn't sync. The user might have last logged in to the device before Enterprise State Roaming was enabled. Restart the device and have the user sign-in. Optionally, in the portal, try having the IT Admin navigate to **Identity > Devices > Overview > Enterprise State Roaming** disable and re-enable **Users may sync settings and app data across devices**. To disable click on "None" and to re-enable click on "All" or "Selected". Once re-enabled, restart the device and have the user sign-in. If this doesn't resolve the issue, **SettingsUrl** might be empty if there's a bad device certificate. In this case, running "`dsregcmd.exe /leave`" in an elevated command prompt window, rebooting, and trying registration again might help with this issue.

Enterprise State Roaming and multifactor authentication

Under certain conditions, Enterprise State Roaming can fail to sync data if Microsoft Entra multifactor authentication is configured. For more information on these symptoms, see the support document [KB3193683](#).

Potential issue: If your device is configured to require multifactor authentication on the Microsoft Entra admin center, you might fail to sync settings while signing in to a Windows 10 or newer device using a password. This type of multifactor authentication configuration is intended to protect an Azure administrator account. Admin users might still be able to sync by signing in to their Windows 10 or newer devices with their Windows Hello for Business PIN or by completing multifactor authentication while accessing other Azure services like Microsoft 365.

Potential issue: Sync can fail if the admin configures the Active Directory Federation Services multifactor authentication Conditional Access policy and the access token on the device expires. Ensure that you sign in and sign out using the Windows Hello for Business PIN or complete multifactor authentication while accessing other Azure services like Microsoft 365.

Event Viewer

For advanced troubleshooting, Event Viewer can be used to find specific errors. The events can be found under Event Viewer > **Applications and Services Logs** > **Microsoft > Windows > CloudStore** and for identity-related issues with sync **Applications and Services Logs** > **Microsoft > Windows > AAD**.

Next steps

For an overview, see [enterprise state roaming overview](#).

Feedback

Was this page helpful?

 Yes

 No

[Provide product feedback ↗](#)

Group Policy and MDM settings

Article • 08/01/2024

Use these Group Policy and mobile device management (MDM) settings only on corporate-owned devices because these policies are applied to the user's entire device. Applying an MDM policy to disable settings sync for a personal, user-owned device negatively impacts the use of that device. These policies affect other user accounts on the device.

Enterprises that want to manage roaming for personal (unmanaged) devices can use the Microsoft Entra admin center to enable or disable roaming, rather than using Group Policy or MDM. The following tables describe the policy settings available.

ⓘ Note

This article applies to the Microsoft Edge Legacy HTML-based browser launched with Windows 10 in July 2015. The article does not apply to the new Microsoft Edge Chromium-based browser released on January 15, 2020. For more information on the Sync behavior for the new Microsoft Edge, see the article [Microsoft Edge Sync](#).

MDM settings

The MDM policy settings apply to Windows 10 or newer. Refer to [Devices and endpoints](#) for details on what devices are supported for Microsoft Entra ID-based syncing.

Expand table

Name	Description
Allow Microsoft Account Connection	Allows users to authenticate using a Microsoft account on the device
Allow Sync My Settings	Allows users to roam Windows settings and app data; Disabling this policy disables sync and backups on mobile devices

Group Policy settings

The Group Policy settings apply to Windows 10 or newer devices that are joined to an Active Directory domain. The table also includes legacy settings that would appear to

manage sync settings. Legacy settings that don't work for Enterprise State Roaming for Windows 10 or newer are noted with 'Do not use' in the description.

These settings are located in Group Policy under: **Computer Configuration > Administrative Templates > Windows Components > Sync your settings**.

 Expand table

Name	Description
Accounts: Block Microsoft Accounts	This policy setting prevents users from adding new Microsoft accounts on this computer
Do not sync	Prevents users to roam Windows settings and app data
Do not sync personalize	Disables syncing of the Themes group
Do not sync browser settings	Disables syncing of the Internet Explorer group
Do not sync passwords	Disables syncing of Passwords group
Do not sync other Windows settings	Disables syncing of Other Windows settings group
Do not sync desktop personalization	Do not use; has no effect
Do not sync on metered connections	Disables roaming on metered connections, such as cellular 3G
Do not sync apps	Do not use; has no effect
Do not sync app settings	Disables roaming of app data
Do not sync start settings	Do not use; has no effect

Next steps

For an overview, see [enterprise State Roaming overview](#).

Feedback

Was this page helpful?

 Yes

 No

[Provide product feedback ↗](#)

Windows roaming settings reference

Article • 08/01/2024

This is the list of settings that can be configured to sync across Windows. Other Microsoft products the user signs into can access them to enable a cohesive experience.

 Expand table

Settings	Windows 10 (21H1 or newer) Windows 11 (22H2 or newer)
Date, Time, and Region: country/region	sync
Date, Time, and Region: region format (locale)	sync
Inking & typing: Custom dictionary	sync (Windows 11 only)
Keyboard: turn on toggle keys	sync
Language: language profile	sync
Language: Windows Display language *	sync (to account only)
Mouse: Primary Mouse Button	sync
Passwords: Web Credentials	sync
Pen: Choose which hand you write with	sync
Pen: Use the top of the pen to erase ink when it's available	sync (Windows 11 only)
Pen: Show visual effects, Show cursor	sync (Windows 11 only)
Pen: Display additional keys pressed when using my pen	sync (Windows 11 only)
Pen: Font, Font Size	sync (Windows 11 only)
Pen: Write with your fingertip	sync (Windows 11 only)
Touchpad: Scrolling Direction	sync
Voice Access: Automatic punctuation	sync (Windows 11 only)
Voice Typing: Voice typing launcher	sync (Windows 11 only)
Voice Typing: Automatic punctuation	sync (Windows 11 only)
Wi-Fi: Wi-Fi profiles (only WPA)	sync

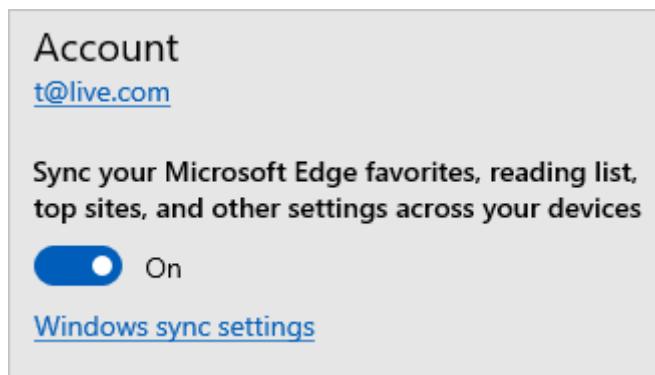
* Display Language setting on Windows won't be impacted by changes from other devices or Microsoft products.

Control over these settings can be found in Windows 10 under **Settings > Accounts > Sync your settings** or in Windows 11 under **Settings > Accounts > Windows backup > Remember my preferences**.

Browser settings

For more information on the Sync behavior for the new Microsoft Edge, see the article [Microsoft Edge Sync](#).

Microsoft Edge browser setting group (favorites, reading list) syncing is managed through the Microsoft Edge browser Settings menu option.



Next steps

For an overview, see [enterprise state roaming overview](#).

Feedback

Was this page helpful?

Yes

No

[Provide product feedback ↗](#)

Security update to remove KDFv1 algorithm support in Microsoft Entra authentication

Article • 02/26/2025

Microsoft is removing support for the Key Derivation Function version 1 (KDFv1) algorithm used for the authentication of Microsoft Entra joined or Microsoft Entra hybrid joined devices in builds of Windows released before July 2021.

The KDFv1 algorithm was historically used for device authentication in earlier versions of Windows. A critical security flaw was discovered that allowed unauthorized authentication, as outlined in [CVE-2021-33781](#). To address this vulnerability, Microsoft issued a Windows security update in July 2021. All Windows builds released after July 2021 no longer use the KDFv1 algorithm.

As part of our ongoing commitment to enhancing security, Microsoft is incrementally rolling out a security update that blocks the use of the KDFv1 algorithm for authentication with Microsoft Entra.

Effects of the security update

All Windows devices that authenticate using Microsoft Entra must have the security patch applied or be running builds of Windows released after July 2021. Unpatched Windows devices won't authenticate with Microsoft Entra once the rollout of this change completes.

Error messages

Users on unpatched devices encounter the following error message when attempting to sign in:

Sign-in error code: 5000611

Failure reason: Symmetric Key Derivation Function version '1' is invalid. Update the device with the latest updates.

This error message is also present in the Microsoft Entra sign-in logs, allowing administrators to identify authentication failures due to the deprecated KDFv1 algorithm.

Note

Due to the incremental rollout of the security update, authentication failures on unpatched Windows devices may initially appear transient or intermittent. Early in the rollout retrying authentication will likely succeed. It is important to address these issues promptly by applying Windows security updates to maintain seamless authentication experiences.

Actions required

Microsoft Entra administrators should proactively identify and address devices within their tenant that might be impacted by this security update. The following steps are recommended:

- Monitor Authentication Failures: Regularly check the Microsoft Entra sign-in logs for the error code 5000611 and the corresponding failure reason.
- Update Devices: If users report authentication failures with an error message referencing the KDFv1 algorithm, update their devices with the latest security updates for their Windows version.
- Search for Impacted Builds: Use the guidance provided in CVE Record CVE-2021-33781 to search for Windows devices within your tenant that might be running impacted builds.
- Communicate with Users: Inform users about the importance of keeping their devices updated and provide instructions on how to apply necessary updates.

Proactive monitoring and updating

Proactively monitoring and updating devices is crucial to avoid any authentication disruptions. Microsoft Entra administrators can utilize the following strategies:

- Automated updates: Implement policies for automated updates to ensure all devices receive the latest security patches promptly.
- Regular audits: Conduct regular audits of your devices to ensure compliance with security update requirements.
- User training: Educate users about the significance of timely updates and how to check for and apply them.

Related content

For more detailed information on the removal of the KDFv1 algorithm and associated security updates, refer to the following resources:

- [CVE Record CVE-2021-33781 ↗](#)
 - [What's new in Microsoft Entra – June 2024 ↗](#)
 - [Windows Update ↗](#)
-

Feedback

Was this page helpful?



[Provide product feedback ↗](#)

Configure Microsoft Entra hybrid join manually

Article • 11/27/2024

If using Microsoft Entra Connect is an option for you, see the guidance in [Configure Microsoft Entra hybrid join](#). Using the automation in Microsoft Entra Connect, significantly simplifies the configuration of Microsoft Entra hybrid join.

This article covers the manual configuration of requirements for Microsoft Entra hybrid join including steps for managed and federated domains.

Prerequisites

- [Microsoft Entra Connect](#)
 - To get device registration sync join to succeed, as part of the device registration configuration, don't exclude the default device attributes from your Microsoft Entra Connect Sync configuration. To learn more about default device attributes synced to Microsoft Entra ID, see [Attributes synchronized by Microsoft Entra Connect](#).
 - If the computer objects of the devices you want to be Microsoft Entra hybrid joined belong to specific organizational units (OUs), configure the correct OUs to sync in Microsoft Entra Connect. To learn more about how to sync computer objects by using Microsoft Entra Connect, see [Organizational unit-based filtering](#).
- Enterprise administrator credentials for each of the on-premises Active Directory Domain Services forests.
- **(For federated domains)** Windows Server with Active Directory Federation Services installed.
- Users can register their devices with Microsoft Entra ID. More information about this setting can be found under the heading **Configure device settings**, in the article, [Configure device settings](#).

Microsoft Entra hybrid join requires devices to have access to the following Microsoft resources from inside your organization's network:

- <https://enterpriseregistration.windows.net>
- <https://login.microsoftonline.com>
- <https://device.login.microsoftonline.com>

- <https://autologon.microsoftazuread-sso.com> (If you use or plan to use seamless single sign-on)
- Your organization's Security Token Service (STS) (**For federated domains**)

⚠ Warning

If your organization uses proxy servers that intercept SSL traffic for scenarios like data loss prevention or Microsoft Entra tenant restrictions, ensure that traffic to these URLs are excluded from TLS break-and-inspect. Failure to exclude these URLs might cause interference with client certificate authentication, cause issues with device registration, and device-based Conditional Access.

If your organization requires access to the internet via an outbound proxy, you can use [Web Proxy Auto-Discovery \(WPAD\)](#) to enable Windows 10 or newer computers for device registration with Microsoft Entra ID. To address issues configuring and managing WPAD, see [Troubleshooting Automatic Detection](#).

If you don't use WPAD, you can configure WinHTTP proxy settings on your computer beginning with Windows 10 1709. For more information, see [WinHTTP Proxy Settings deployed by Group Policy Object \(GPO\)](#).

ⓘ Note

If you configure proxy settings on your computer by using WinHTTP settings, any computers that can't connect to the configured proxy will fail to connect to the internet.

If your organization requires access to the internet via an authenticated outbound proxy, make sure that your Windows 10 or newer computers can successfully authenticate to the outbound proxy. Because Windows 10 or newer computers run device registration by using machine context, configure outbound proxy authentication by using machine context. Follow up with your outbound proxy provider on the configuration requirements.

Verify devices can access the required Microsoft resources under the system account by using the [Test Device Registration Connectivity](#) script.

Configuration

You can configure Microsoft Entra hybrid joined devices for various types of Windows device platforms.

- For managed and federated domains, you must [configure a service connection point \(SCP\)](#).
- For federated domains, you must ensure that your [federation service is configured to issue the appropriate claims](#).

After these configurations are complete, follow the guidance to [verify registration](#).

Configure a service connection point

Your devices use a service connection point (SCP) object during the registration to discover Microsoft Entra tenant information. In your on-premises Active Directory instance, the SCP object for the Microsoft Entra hybrid joined devices must exist in the configuration naming context partition of the computer's forest. There's only one configuration naming context per forest. In a multi-forest Active Directory configuration, the service connection point must exist in all forests that contain domain-joined computers.

The SCP object contains two keywords values – `azureADid:<TenantID>` and `azureADName:<verified domain>`. The `<verified domain>` value in the `azureADName` keyword dictates the type of the device registration flow (federated or managed) the device will follow after reading the SCP value from your on-premises Active Directory instance. More about the managed and federated flows can be found in the article [How Microsoft Entra device registration works](#).

You can use the [Get-ADRootDSE](#) cmdlet to retrieve the configuration naming context of your forest.

For a forest with the Active Directory domain name *fabrikam.com*, the configuration naming context is:

```
CN=Configuration,DC=fabrikam,DC=com
```

In your forest, the SCP object for the autoregistration of domain-joined devices is located at:

```
CN=62a0ff2e-97b9-4513-943f-0d221bd30080,CN=Device Registration  
Configuration,CN=Services,[Your Configuration Naming Context]
```

Depending on how you deploy Microsoft Entra Connect, the SCP object might already be configured. You can verify the existence of the object and retrieve the discovery

values by using the following PowerShell script:

PowerShell

```
$scp = New-Object System.DirectoryServices.DirectoryEntry;  
  
$scp.Path = "LDAP://CN=62a0ff2e-97b9-4513-943f-0d221bd30080,CN=Device  
Registration Configuration,CN=Services,CN=Configuration,DC=fabrikam,DC=com";  
  
$scp.Keywords;
```

The \$scp.Keywords output shows the Microsoft Entra tenant information. Here's an example:

PowerShell

```
azureADName:microsoft.com  
azureADId:a0a0a0a0-bbbb-cccc-dddd-e1e1e1e1e1e1
```

Set up issuance of claims

In a federated Microsoft Entra configuration, devices rely on AD FS or an on-premises federation service from a Microsoft partner to authenticate to Microsoft Entra ID. Devices authenticate to get an access token to register against the Microsoft Entra Device Registration Service (Azure DRS).

Windows devices authenticate by using integrated Windows authentication to an active WS-Trust endpoint (either 1.3 or 2005 versions) hosted by the on-premises federation service.

When you're using AD FS, you need to enable the following WS-Trust endpoints:

- /adfs/services/trust/2005/windowstransport
- /adfs/services/trust/13/windowstransport
- /adfs/services/trust/2005/usernamemixed
- /adfs/services/trust/13/usernamemixed
- /adfs/services/trust/2005/certificatemixed
- /adfs/services/trust/13/certificatemixed

⚠ Warning

Both `adfs/services/trust/2005/windowstransport` and `adfs/services/trust/13/windowstransport` should be enabled as intranet facing

endpoints only and must NOT be exposed as extranet facing endpoints through the Web Application Proxy. To learn more on how to disable WS-Trust Windows endpoints, see [Disable WS-Trust Windows endpoints on the proxy](#). You can see what endpoints are enabled through the AD FS management console under Service > Endpoints.

ⓘ Note

If you don't have AD FS as your on-premises federation service, follow the instructions from your vendor to make sure they support WS-Trust 1.3 or 2005 endpoints and that these are published through the Metadata Exchange file (MEX).

For device registration to finish, the following claims must exist in the token that Azure DRS receives. Azure DRS creates a device object in Microsoft Entra ID with some of this information. Microsoft Entra Connect then uses this information to associate the newly created device object with the computer account on-premises.

- `http://schemas.microsoft.com/ws/2012/01/accounttype`
- `http://schemas.microsoft.com/identity/claims/onpremobjectguid`
- `http://schemas.microsoft.com/ws/2008/06/identity/claims/primarysid`

If you require more than one verified domain name, you need to provide the following claim for computers:

- `http://schemas.microsoft.com/ws/2008/06/identity/claims/issuerid`

If you're already issuing an `ImmutableID` claim (for example, using `ms-DS-ConsistencyGuid` or another attribute as the source value for the `ImmutableID`), you need to provide one corresponding claim for computers:

- `http://schemas.microsoft.com/LiveID/Federation/2008/05/ImmutableID`

In the following sections, you find information about:

- The values that each claim should have.
- What a definition would look like in AD FS.

The definition helps you to verify whether the values are present or if you need to create them.

ⓘ Note

If you don't use AD FS for your on-premises federation server, follow your vendor's instructions to create the appropriate configuration to issue these claims.

Issue account type claim

The `http://schemas.microsoft.com/ws/2012/01/accounttype` claim must contain a value of **DJ**, which identifies the device as a domain-joined computer. In AD FS, you can add an issuance transform rule that looks like this:

```
@RuleName = "Issue account type for domain-joined computers"
c:[
    Type ==
    "http://schemas.microsoft.com/ws/2008/06/identity/claims/groupsid",
    Value =~ "-515$",
    Issuer =~ "^(AD AUTHORITY|SELF AUTHORITY|LOCAL AUTHORITY)$"
]
=> issue(
    Type = "http://schemas.microsoft.com/ws/2012/01/accounttype",
    Value = "DJ"
);
```

Issue objectGUID of the computer account on-premises

The `http://schemas.microsoft.com/identity/claims/onpremobjectguid` claim must contain the **objectGUID** value of the on-premises computer account. In AD FS, you can add an issuance transform rule that looks like this:

```
@RuleName = "Issue object GUID for domain-joined computers"
c1:[
    Type ==
    "http://schemas.microsoft.com/ws/2008/06/identity/claims/groupsid",
    Value =~ "-515$",
    Issuer =~ "^(AD AUTHORITY|SELF AUTHORITY|LOCAL AUTHORITY)$"
]
&&
c2:[
    Type ==
    "http://schemas.microsoft.com/ws/2008/06/identity/claims/windowsaccountname"
    ,
    Issuer =~ "^(AD AUTHORITY|SELF AUTHORITY|LOCAL AUTHORITY)$"
]
=> issue(
    store = "Active Directory",
```

```
types =
("http://schemas.microsoft.com/identity/claims/onpremobjectguid"),
query = ";objectguid;{0}",
param = c2.Value
);
```

Issue objectSid of the computer account on-premises

The `http://schemas.microsoft.com/ws/2008/06/identity/claims/primarysid` claim must contain the **objectSid** value of the on-premises computer account. In AD FS, you can add an issuance transform rule that looks like this:

```
@RuleName = "Issue objectSID for domain-joined computers"
c1:[
    Type ==
"http://schemas.microsoft.com/ws/2008/06/identity/claims/groupsid",
    Value =~ "-515$",
    Issuer =~ "^(AD AUTHORITY|SELF AUTHORITY|LOCAL AUTHORITY)$"
]
&&
c2:[
    Type ==
"http://schemas.microsoft.com/ws/2008/06/identity/claims/primarysid",
    Issuer =~ "^(AD AUTHORITY|SELF AUTHORITY|LOCAL AUTHORITY)$"
]
=> issue(claim = c2);
```

Issue issuerID for the computer when multiple verified domain names are in Microsoft Entra ID

The `http://schemas.microsoft.com/ws/2008/06/identity/claims/issuerid` claim must contain the Uniform Resource Identifier (URI) of any of the verified domain names that connect with the on-premises federation service (AD FS or partner) issuing the token. In AD FS, you can add issuance transform rules that look like the following ones in that specific order, after the preceding ones. One rule to explicitly issue the rule for users is necessary. In the following rules, a first rule that identifies user versus computer authentication is added.

```
@RuleName = "Issue account type with the value User when its not a computer"
NOT EXISTS(
[
    Type == "http://schemas.microsoft.com/ws/2012/01/accounttype",
```

```

        Value == "DJ"
    ]
)
=> add(
    Type = "http://schemas.microsoft.com/ws/2012/01/accounttype",
    Value = "User"
);

@RuleName = "Capture UPN when AccountType is User and issue the IssuerID"
c1:[
    Type == "http://schemas.xmlsoap.org/claims/UPN"
]
&&
c2:[
    Type == "http://schemas.microsoft.com/ws/2012/01/accounttype",
    Value == "User"
]
=> issue(
    Type =
"http://schemas.microsoft.com/ws/2008/06/identity/claims/issuerid",
    Value = regexreplace(
        c1.Value,
        ".+@(?<domain>.+)",
        "http://${domain}/adfs/services/trust/"
    )
);

```

@RuleName = "Issue issuerID for domain-joined computers"

```

c:[
    Type ==
"http://schemas.microsoft.com/ws/2008/06/identity/claims/groupsid",
    Value =~ "-515$",
    Issuer =~ "^(AD AUTHORITY|SELF AUTHORITY|LOCAL AUTHORITY)$"
]
=> issue(
    Type =
"http://schemas.microsoft.com/ws/2008/06/identity/claims/issuerid",
    Value = "http://<verified-domain-name>/adfs/services/trust/"
);

```

In the preceding claim, `<verified-domain-name>` is a placeholder. Replace it with one of your verified domain names in Microsoft Entra ID. For example, use `Value = "http://contoso.com/adfs/services/trust/"`.

For more information about verified domain names, see [Add a custom domain name to Microsoft Entra ID](#).

To get a list of your verified company domains, you can use the [Get-MgDomain](#) cmdlet.

PS C:\Users\Admin> Get-MgDomain				
Id	AuthenticationType	AvailabilityStatus	IsAdminManaged	
fabrikam.com	Managed		True	

Issue ImmutableID for the computer when one for users exists (for example, using mS-DS-ConsistencyGuid as the source for ImmutableID)

The `http://schemas.microsoft.com/LiveID/Federation/2008/05/ImmutableID` claim must contain a valid value for computers. In AD FS, you can create an issuance transform rule as follows:

```
@RuleName = "Issue ImmutableID for computers"
c1:[
    Type ==
    "http://schemas.microsoft.com/ws/2008/06/identity/claims/groupsid",
    Value =~ "-515$",
    Issuer =~ "^((AD AUTHORITY|SELF AUTHORITY|LOCAL AUTHORITY))$"
]
&&
c2:[
    Type ==
    "http://schemas.microsoft.com/ws/2008/06/identity/claims/windowsaccountname"
,
    Issuer =~ "^((AD AUTHORITY|SELF AUTHORITY|LOCAL AUTHORITY))$"
]
=> issue(
    store = "Active Directory",
    types =
    ("http://schemas.microsoft.com/LiveID/Federation/2008/05/ImmutableID"),
    query = ";objectguid;{0}",
    param = c2.Value
);
```

Helper script to create the AD FS issuance transform rules

The following script helps you with the creation of the issuance transform rules described earlier.

```
$multipleVerifiedDomainNames = $false
$immutableIDAlreadyIssuedForUsers = $false
$oneOfVerifiedDomainNames = 'example.com' # Replace example.com with one
```

```

of your verified domains

$rule1 = '@RuleName = "Issue account type for domain-joined computers"
c:[
    Type ==
"http://schemas.microsoft.com/ws/2008/06/identity/claims/groupsid",
    Value =~ "-515$",
    Issuer =~ "^(AD AUTHORITY|SELF AUTHORITY|LOCAL AUTHORITY)$"
]
=> issue(
    Type = "http://schemas.microsoft.com/ws/2012/01/accounttype",
    Value = "DJ"
);'

$rule2 = '@RuleName = "Issue object GUID for domain-joined computers"
c1:[
    Type ==
"http://schemas.microsoft.com/ws/2008/06/identity/claims/groupsid",
    Value =~ "-515$",
    Issuer =~ "^(AD AUTHORITY|SELF AUTHORITY|LOCAL AUTHORITY)$"
]
&&
c2:[
    Type ==
"http://schemas.microsoft.com/ws/2008/06/identity/claims/windowsaccountname"
,
    Issuer =~ "^(AD AUTHORITY|SELF AUTHORITY|LOCAL AUTHORITY)$"
]
=> issue(
    store = "Active Directory",
    types =
("http://schemas.microsoft.com/identity/claims/onpremobjectguid"),
    query = ";objectguid;{0}",
    param = c2.Value
);'

$rule3 = '@RuleName = "Issue objectSID for domain-joined computers"
c1:[
    Type ==
"http://schemas.microsoft.com/ws/2008/06/identity/claims/groupsid",
    Value =~ "-515$",
    Issuer =~ "^(AD AUTHORITY|SELF AUTHORITY|LOCAL AUTHORITY)$"
]
&&
c2:[
    Type ==
"http://schemas.microsoft.com/ws/2008/06/identity/claims/primarysid",
    Issuer =~ "^(AD AUTHORITY|SELF AUTHORITY|LOCAL AUTHORITY)$"
]
=> issue(claim = c2);'

$rule4 = ''
if ($multipleVerifiedDomainNames -eq $true) {
$rule4 = '@RuleName = "Issue account type with the value User when it is not
a computer"'

```

```

NOT EXISTS(
[
    Type == "http://schemas.microsoft.com/ws/2012/01/accounttype",
    Value == "DJ"
]
)
=> add(
    Type = "http://schemas.microsoft.com/ws/2012/01/accounttype",
    Value = "User"
);

@RuleName = "Capture UPN when AccountType is User and issue the IssuerID"
c1:[
    Type == "http://schemas.xmlsoap.org/claims/UPN"
]
&&
c2:[
    Type == "http://schemas.microsoft.com/ws/2012/01/accounttype",
    Value == "User"
]
=> issue(
    Type =
"http://schemas.microsoft.com/ws/2008/06/identity/claims/issuerid",
    Value = regexreplace(
        c1.Value,
        ".+@(?<domain>.+)",
        "http://${domain}/adfs/services/trust/"
    )
);
;

@RuleName = "Issue issuerID for domain-joined computers"
c:[
    Type ==
"http://schemas.microsoft.com/ws/2008/06/identity/claims/groupsid",
    Value =~ "-515$",
    Issuer =~ "^(AD AUTHORITY|SELF AUTHORITY|LOCAL AUTHORITY)$"
]
=> issue(
    Type =
"http://schemas.microsoft.com/ws/2008/06/identity/claims/issuerid",
    Value = "http://" + $oneOfVerifiedDomainNames + '/adfs/services/trust/'
);
}

$rule5 = ''
if ($immutableIDAlreadyIssuedForUsers -eq $true) {
$rule5 = '@RuleName = "Issue ImmutableID for computers"
c1:[
    Type ==
"http://schemas.microsoft.com/ws/2008/06/identity/claims/groupsid",
    Value =~ "-515$",
    Issuer =~ "^(AD AUTHORITY|SELF AUTHORITY|LOCAL AUTHORITY)$"
]
&&
c2:[

```

```

Type ==
"http://schemas.microsoft.com/ws/2008/06/identity/claims/windowsaccountname"
,
Issuer =~ "(AD AUTHORITY|SELF AUTHORITY|LOCAL AUTHORITY)$"
]
=> issue(
    store = "Active Directory",
    types =
("http://schemas.microsoft.com/LiveID/Federation/2008/05/ImmutableID"),
    query = ";objectguid;{0}",
    param = c2.Value
);
}

$existingRules = (Get-ADFSRelyingPartyTrust -Identifier
urn:federation:MicrosoftOnline).IssuanceTransformRules

$updatedRules = $existingRules + $rule1 + $rule2 + $rule3 + $rule4 + $rule5

$crSet = New-ADFSClaimRuleSet -ClaimRule $updatedRules

Set-AdfsRelyingPartyTrust -TargetIdentifier urn:federation:MicrosoftOnline -
IssuanceTransformRules $crSet.ClaimRulesString

```

Remarks

- This script appends the rules to the existing rules. Don't run the script twice, because the set of rules would be added twice. Make sure that no corresponding rules exist for these claims (under the corresponding conditions) before running the script again.
- If you have multiple verified domain names, set the value of **\$multipleVerifiedDomainNames** in the script to **\$true**. Also make sure that you remove any existing **issuerid** claim created by Microsoft Entra Connect or other means. Here's an example for this rule:

```

c:[Type == "http://schemas.xmlsoap.org/claims/UPN"]
=> issue(Type =
"http://schemas.microsoft.com/ws/2008/06/identity/claims/issuerid",
Value = regexreplace(c.Value, ".+@(?<domain>.+)",
"http://${domain}/adfs/services/trust/"));

```

If you issue an **ImmutableID** claim for user accounts, set the value of **\$immutableIDAlreadyIssuedforUsers** in the script to **\$true**.

Troubleshoot your implementation

If you experience issues completing Microsoft Entra hybrid join for domain-joined Windows devices, see:

- Troubleshooting devices using `dsregcmd` command
- Troubleshooting Microsoft Entra hybrid joined devices

Related content

- Microsoft Entra hybrid join verification
- Plan your Microsoft Entra hybrid join implementation
- Use Conditional Access to require compliant or Microsoft Entra hybrid joined device

Feedback

Was this page helpful?



[Provide product feedback ↗](#)

Enforce TLS 1.2 for the Microsoft Entra Registration Service

Article • 10/23/2023

The Microsoft Entra Device Registration Service is used to connect devices to the cloud with a device identity. The Microsoft Entra Device Registration Service currently supports using Transport Layer Security (TLS) 1.2 for communications with Azure. To ensure security and best-in-class encryption, Microsoft recommends disabling TLS 1.0 and 1.1. This document will provide information on how to ensure machines used to complete registration and communicate with the Microsoft Entra Device Registration Service use TLS 1.2.

The TLS protocol version 1.2 is a cryptography protocol that is designed to provide secure communications. The TLS protocol aims primarily to provide privacy and data integrity. TLS has gone through many iterations with version 1.2 being defined in [RFC 5246 \(external link\)](#).

Current analysis of connections shows little TLS 1.1 and 1.0 usage, but we are providing this information so that you can update any affected clients or servers as necessary before support for TLS 1.1 and 1.0 ends. If you are using any on-premises infrastructure for hybrid scenarios or Active Directory Federation Services (AD FS), make sure that the infrastructure can support both inbound and outbound connections that use TLS 1.2.

Update Windows servers

For Windows servers that use the Microsoft Entra Device Registration Service or act as proxies, use the following steps to ensure TLS 1.2 is enabled:

 **Important**

After you have updated the registry, you must restart the Windows server for the changes to take effect.

Enable TLS 1.2

Ensure the following registry strings are configured as shown:

- HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\SecurityProviders\SCHANNEL\Protocols\TLS 1.2\Client
 - "DisabledByDefault"=dword:00000000
 - "Enabled"=dword:00000001
- HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\SecurityProviders\SCHANNEL\Protocols\TLS 1.2\Server
 - "DisabledByDefault"=dword:00000000
 - "Enabled"=dword:00000001
- HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft.NETFramework\v4.0.30319
 - "SchUseStrongCrypto"=dword:00000001

Update non-Windows proxies

Any machines that act as proxies between devices and the Microsoft Entra Device Registration Service must ensure that TLS 1.2 is enabled. Follow your vendor's guidance to ensure support.

Update AD FS servers

Any AD FS servers used to communicate with the Microsoft Entra Device Registration Service must ensure that TLS 1.2 is enabled. See [Managing SSL/TLS Protocols and Cipher Suites for AD FS](#) for information on how to enable/verify this configuration.

Client updates

Since all client-server and browser-server combinations must use TLS 1.2 to connect with the Microsoft Entra Device Registration Service, you may need to update these devices.

The following clients are known to be unable to support TLS 1.2. Update your clients to ensure uninterrupted access.

- Android version 4.3 and earlier
- Firefox version 5.0 and earlier
- Internet Explorer versions 8-10 on Windows 7 and earlier
- Internet Explorer 10 on Windows Phone 8.0
- Safari version 6.0.4 on OS X 10.8.4 and earlier

Next steps

[TLS/SSL overview \(Schannel SSP\)](#)

device resource type

Article • 10/26/2024

Namespace: microsoft.graph

Represents a device registered in the organization. Devices are created in the cloud using the Device Registration Service or by Intune. They're used by conditional access policies for multi-factor authentication. These devices can range from desktop and laptop machines to phones and tablets. Inherits from [directoryObject](#).

This resource is an open type that allows other properties to be passed in.

This resource supports:

- Adding your own data to custom properties as [extensions](#).
- Using [delta query](#) to track incremental additions, deletions, and updates, by providing a [delta](#) function.
- [OData query capabilities](#) including `$select`, `$filter`, `$search`, and `$top`. Specific usages are supported only with [Advanced query capabilities](#).

Methods

[+] Expand table

Method	Return Type	Description
List	device collection	Retrieve a list of devices registered in the directory.
Create	device	Register a new device in the directory.
Get	device	Read properties and relationships of a device object.
Update	device	Update the properties of a device object.
Delete	None	Delete a device object.
Get delta	device collection	Get incremental changes for devices.
List member of	directoryObject collection	List the groups and administrative units that the device is a direct member of.
List transitive member of	directoryObject collection	List the groups and administrative units that the device is a member of. This operation is transitive.
List registered owners	directoryObject collection	Get the users that are registered owners of the device from the registeredOwners navigation property.
Add registered owners	directoryObject collection	Add registered owners of the device.
Remove registered owners	directoryObject collection	Delete registered owners from the device.
List registered users	directoryObject collection	Get the registered users of the device from the registeredUsers navigation property.

Method	Return Type	Description
Add registered users	directoryObject collection	Add registered users of the device .
Remove registered users	directoryObject collection	Remove registered users from the device .
Check member objects	String collection	Check for membership in a list of groups, directory role, or administrative unit objects.
Get member objects	String collection	Return all groups, administrative units, and directory roles that the device is a member of. The check is transitive.

Properties

ⓘ Important

Specific usage of `$filter` and the `$search` query parameter is supported only when you use the **ConsistencyLevel** header set to `eventual` and `$count`. For more information, see [Advanced query capabilities on directory objects](#).

[] Expand table

Property	Type	Description
accountEnabled	Boolean	<code>true</code> if the account is enabled; otherwise, <code>false</code> . Required. Default is <code>true</code> . Supports <code>\$filter</code> (<code>eq</code> , <code>ne</code> , <code>not</code> , <code>in</code>). Only callers with at least the Cloud Device Administrator role can set this property.
alternativeSecurityIds	<code>alternativeSecurityId</code> collection	For internal use only. Not nullable. Supports <code>\$filter</code> (<code>eq</code> , <code>not</code> , <code>ge</code> , <code>le</code>).
approximateLastSignInDateTime	DateTimeOffset	The timestamp type represents date and time information using ISO 8601 format and is always in UTC time. For example, midnight UTC on Jan 1, 2014 is <code>2014-01-01T00:00:00Z</code> . Read-only. Supports <code>\$filter</code> (<code>eq</code> , <code>ne</code> , <code>not</code> , <code>ge</code> , <code>le</code> , and <code>eq</code> on <code>null</code> values) and <code>\$orderby</code> .
complianceExpirationDateTime	DateTimeOffset	The timestamp when the device is no longer deemed compliant. The timestamp type represents date and time information using ISO 8601 format and is always in UTC time. For example, midnight UTC on Jan 1, 2014 is <code>2014-01-01T00:00:00Z</code> . Read-only.
deviceCategory	String	User-defined property set by Intune to automatically add devices to groups and simplify managing devices.
deviceId	String	Unique identifier set by Azure Device Registration Service at the time of registration. This alternate key can be used

Property	Type	Description
		to reference the device object. Supports <code>\$filter (eq, ne, not, startsWith)</code> .
deviceMetadata	String	For internal use only. Set to <code>null</code> .
deviceOwnership	String	Ownership of the device. Intune sets this property. Possible values are: <code>unknown</code> , <code>company</code> , <code>personal</code> .
deviceVersion	Int32	For internal use only.
displayName	String	The display name for the device. Maximum length is 256 characters. Required. Supports <code>\$filter (eq, ne, not, ge, le, in, startsWith, and eq on null values)</code> , <code>\$search</code> , and <code>\$orderby</code> .
enrollmentProfileName	String	Enrollment profile applied to the device. For example, <code>Apple Device Enrollment Profile</code> , <code>Device enrollment - Corporate device identifiers</code> , or <code>Windows Autopilot profile name</code> . This property is set by Intune.
enrollmentType	String	Enrollment type of the device. Intune sets this property. Possible values are: <code>unknown</code> , <code>userEnrollment</code> , <code>deviceEnrollmentManager</code> , <code>appleBulkWithUser</code> , <code>appleBulkWithoutUser</code> , <code>windowsAzureADJoin</code> , <code>windowsBulkUserless</code> , <code>windowsAutoEnrollment</code> , <code>windowsBulkAzureDomainJoin</code> , <code>windowsCoManagement</code> , <code>windowsAzureADJoinUsingDeviceAuth</code> , <code>appleUserEnrollment</code> , <code>appleUserEnrollmentWithServiceAccount</code> .
NOTE: This property might return other values apart from those listed.		
extensionAttributes	onPremisesExtensionAttributes	Contains extension attributes 1-15 for the device. The individual extension attributes aren't selectable. These properties are mastered in the cloud and can be set during creation or update of a device object in Microsoft Entra ID. Supports <code>\$filter (eq, not, startsWith, and eq on null values)</code> .
id	String	The unique identifier for the device. Inherited from directoryObject . Key, Not nullable. Read-only. Supports <code>\$filter (eq, ne, not, in)</code> .
isCompliant	Boolean	<code>true</code> if the device complies with Mobile Device Management (MDM) policies; otherwise, <code>false</code> . Read-only. This can only be updated by Intune for any device OS type or by an approved MDM app for Windows OS devices. Supports <code>\$filter (eq, ne, not)</code> .
isManaged	Boolean	<code>true</code> if the device is managed by a Mobile Device Management (MDM) app; otherwise, <code>false</code> . This can only be updated by Intune for any device OS type or by an

Property	Type	Description
		approved MDM app for Windows OS devices. Supports \$filter (eq, ne, not).
manufacturer	String	Manufacturer of the device. Read-only.
isRooted	Boolean	true if the device is rooted or jail-broken. This property can only be updated by Intune.
managementType	String	The management channel of the device. This property is set by Intune. Possible values are: eas, mdm, easMdm, intuneClient, easIntuneClient, configurationManagerClient, configurationManagerClientMdm, configurationManagerClientMdmEas, unknown, jamf, googleCloudDevicePolicyController.
mdmAppId	String	Application identifier used to register device into MDM. Read-only. Supports \$filter (eq, ne, not, startsWith).
model	String	Model of the device. Read-only.
onPremisesLastSyncDateTime	DateTimeOffset	The last time at which the object was synced with the on-premises directory. The Timestamp type represents date and time information using ISO 8601 format and is always in UTC time. For example, midnight UTC on Jan 1, 2014 is 2014-01-01T00:00:00Z Read-only. Supports \$filter (eq, ne, not, ge, le, in).
onPremisesSecurityIdentifier	String	The on-premises security identifier (SID) for the user who was synchronized from on-premises to the cloud. Read-only. Returned only on \$select. Supports \$filter (eq).
onPremisesSyncEnabled	Boolean	true if this object is synced from an on-premises directory; false if this object was originally synced from an on-premises directory but is no longer synced; null if this object has never been synced from an on-premises directory (default). Read-only. Supports \$filter (eq, ne, not, in, and eq on null values).
operatingSystem	String	The type of operating system on the device. Required. Supports \$filter (eq, ne, not, ge, le, startsWith, and eq on null values).
operatingSystemVersion	String	The version of the operating system on the device. Required. Supports \$filter (eq, ne, not, ge, le, startsWith, and eq on null values).
physicalIds	String collection	For internal use only. Not nullable. Supports \$filter (eq, not, ge, le, startsWith, /\$count eq 0, /\$count ne 0).
profileType	deviceProfileType	The profile type of the device. Possible values: RegisteredDevice (default), SecureVM, Printer, Shared, IoT.
registrationDateTime	DateTimeOffset	Date and time of when the device was registered. The timestamp type represents date and time information

Property	Type	Description
		using ISO 8601 format and is always in UTC time. For example, midnight UTC on Jan 1, 2014 is <code>2014-01-01T00:00:00Z</code> . Read-only.
systemLabels	String collection	List of labels applied to the device by the system. Supports <code>\$filter</code> (<code>/\$count eq 0</code> , <code>/\$count ne 0</code>).
trustType	String	Type of trust for the joined device. Read-only. Possible values: <code>Workplace</code> (indicates <i>bring your own personal devices</i>), <code>AzureAd</code> (Cloud-only joined devices), <code>ServerAd</code> (on-premises domain joined devices joined to Microsoft Entra ID). For more information, see Introduction to device management in Microsoft Entra ID . Supports <code>\$filter</code> (<code>eq</code> , <code>ne</code> , <code>not</code> , <code>in</code>).

Relationships

[Expand table](#)

Relationship	Type	Description
extensions	<code>extension</code> collection	The collection of open extensions defined for the device. Read-only. Nullable.
memberOf	<code>directoryObject</code> collection	Groups and administrative units that this device is a member of. Read-only. Nullable. Supports <code>\$expand</code> .
registeredOwners	<code>directoryObject</code> collection	The user that cloud joined the device or registered their personal device. The registered owner is set at the time of registration. Read-only. Nullable. Supports <code>\$expand</code> .
registeredUsers	<code>directoryObject</code> collection	Collection of registered users of the device. For cloud joined devices and registered personal devices, registered users are set to the same value as registered owners at the time of registration. Read-only. Nullable. Supports <code>\$expand</code> .
transitiveMemberOf	<code>directoryObject</code> collection	Groups and administrative units that the device is a member of. This operation is transitive. Supports <code>\$expand</code> .

JSON representation

The following JSON representation shows the resource type.

JSON
<pre>{ "accountEnabled": "Boolean", "alternativeSecurityIds": [{"@odata.type": "microsoft.graph.alternativeSecurityId"}], "approximateLastSignInDateTime": "String (timestamp)", "complianceExpirationDateTime": "String (timestamp)", "deviceCategory": "String", "deviceId": "String",</pre>

```
"deviceMetadata": "String",
"deviceOwnership": "String",
"deviceVersion": "Int32",
"displayName": "String",
"enrollmentProfileName": "String",
"enrollmentType": "String",
"extensionAttributes": {"@odata.type": "microsoft.graph.onPremisesExtensionAttributes"},  
"id": "String (identifier)",
"isCompliant": "Boolean",
"isManaged": "Boolean",
"isRooted": "Boolean",
"managementType": "String",
"manufacturer": "String",
"mdmAppId": "String",
"model": "String",
"onPremisesLastSyncDateTime": "String (timestamp)",
"onPremisesSecurityIdentifier": "String",
"onPremisesSyncEnabled": "Boolean",
"operatingSystem": "String",
"operatingSystemVersion": "String",
"physicalIds": ["String"],
"profileType": "String",
"registrationDateTime": "String (timestamp)",
"systemLabels": ["String"],
"trustType": "String"
}
```

Related content

- [Add custom data to resources using extensions](#)
- [Add custom data to users using open extensions](#)
- [Add custom data to groups using schema extensions](#)

Microsoft Entra releases and announcements

Article • 04/30/2025

This article provides information about the latest releases and change announcements across the Microsoft Entra family of products over the last six months (updated monthly). If you're looking for information that's older than six months, see: [Archive for What's new in Microsoft Entra](#).

Get notified about when to revisit this page for updates by copying and pasting this URL:

`https://learn.microsoft.com/api/search/rss?search=%22Release+notes+-+Azure+Active+Directory%22&locale=en-us` into your  feed reader.

April 2025

Public Preview - Conditional Access Optimization Agent in Microsoft Entra

Type: New feature

Service category: Conditional Access

Product capability: Identity Security & Protection

[Conditional Access Optimization Agent in Microsoft Entra](#) monitors for new users or apps not covered by existing policies, identifies necessary updates to close security gaps, and recommends quick fixes for identity teams to apply with a single selection. For more information, see: [Microsoft Entra Conditional Access optimization agent](#).

Public Preview - Microsoft Entra ID Governance: Suggested access packages in My Access

Type: New feature

Service category: Entitlement Management

Product capability: Entitlement Management

In December 2024, we introduced a new feature in My Access: a curated list of suggested access packages. Users view the most relevant access packages, based on their peers' access packages and previous assignments, without scrolling through a long list. By May 2025, suggestions will be enabled by default and we'll introduce a new card in the Microsoft Entra

Admin Center Entitlement Management control configurations for admins to see My Access settings. We recommend admins turn on the peer-based insights for suggested access packages via this setting. For more information, see: [Suggested access packages in My Access \(Preview\)](#).

Public Preview - Conditional Access What If evaluation API

Type: New feature

Service category: Conditional Access

Product capability: Access Control

Conditional Access What If evaluation API – Leverage the What If tool using the Microsoft Graph API to programmatically evaluate the applicability of conditional access policies in your tenant on user and service principal sign-ins. For more information, see: [conditionalAccessRoot: evaluate](#).

Public Preview - Manage refresh tokens for mover and leaver scenarios with Lifecycle Workflows

Type: New feature

Service category: Lifecycle Workflows

Product capability: Identity Governance

Now customers can configure a Lifecycle workflows task to automatically revoke access tokens when employees move within, or leave, the organization. For more information, see: [Revoke all refresh tokens for user \(Preview\)](#).

General Availability - Use managed identities as credentials in Microsoft Entra apps

Type: New feature

Service category: Managed identities for Azure resources

Product capability: Identity Security & Protection

You can now use managed identities as federated credentials for Microsoft Entra apps, enabling secure, secret-less authentication in both single- and multi-tenant scenarios. This eliminates the need to store and manage client secrets or certificates when using Microsoft Entra app to access Azure resources across tenants. This capability aligns with Microsoft's

Secure Future Initiative [🔗](#) pillar of protecting identities and secrets across systems. Learn how to configure this capability in the [official documentation](#).

Plan for change - Roll out of Application Based Authentication on Microsoft Entra Connect Sync

Type: Plan for change

Service category: Microsoft Entra Connect

Product capability: Microsoft Entra Connect

What is changing

Microsoft Entra Connect creates and uses a [Microsoft Entra Connector account](#) to authenticate and sync identities from Active Directory to Microsoft Entra ID. The account uses a locally stored password to authenticate with Microsoft Entra ID. To enhance the security of the Microsoft Entra Connect application sync process, we will, in the coming week roll out support for "Application based Authentication" (ABA), which uses a Microsoft Entra ID application based identity and Oauth 2.0 client credential flow to authenticate with Microsoft Entra ID. To enable this, Microsoft Entra Connect will create a single tenant 3rd party application in customer's Microsoft Entra ID tenant, register a certificate as the credential for the application, and authorize the application to perform on-premises directory synchronization

The Microsoft Entra Connect Sync .msi installation file for this change will be exclusively available in the Microsoft Entra admin center within the [Microsoft Entra Connect pane](#) [🔗](#).

Check our [version history page](#) in the next week for more details of the change.

March 2025

Microsoft Entra Permissions Management end of sale and retirement

Type: Plan for change

Service category: Other

Product capability: Permissions Management

Effective April 1, 2025, Microsoft Entra Permissions Management (MEPM) will no longer be available for sale to new Enterprise Agreement or direct customers. Additionally, starting May

1, it will not be available for sale to new CSP customers. Effective October 1, 2025, we will retire Microsoft Entra Permissions Management and discontinue support of this product.

Existing customers will retain access to this product until September 30, 2025, with ongoing support for current functionalities. We have partnered with Delinea to provide an alternative solution, [Privilege Control for Cloud Entitlements \(PCCE\)](#), that offers similar capabilities to those provided by Microsoft Entra Permissions Management. The decision to phase out Microsoft Entra Permissions Management was done after deep consideration of our innovation portfolio and how we can focus on delivering the best innovations aligned to our differentiating areas and partner with the ecosystem on adjacencies. We remain committed to delivering top-tier solutions across the Microsoft Entra portfolio. For more information, see: [Important change announcement: Microsoft Entra Permissions Management end of sale and retirement](#).

Public Preview - Track and investigate identity activities with linkable identifiers in Microsoft Entra

Type: New feature

Service category: Authentications (Logins)

Product capability: User Authentication

Microsoft will standardize the linkable token identifiers, and expose them in both Microsoft Entra and workflow audit logs. This allows customers to join the logs to track, and investigate, any malicious activity. Currently linkable identifiers are available in Microsoft Entra sign in logs, Exchange Online audit logs, and MSGraph Activity logs.

For more information, see: [Track and investigate identity activities with linkable identifiers in Microsoft Entra \(preview\)](#).

General Availability- Conditional Access reauthentication policy

Type: New feature

Service category: Conditional Access

Product capability: Identity Security & Protection

Require reauthentication every time can be used for scenarios where you want to require a fresh authentication, every time a user performs specific actions like accessing sensitive

applications, securing resources behind VPN, or Securing privileged role elevation in PIM. For more information, see: [Require reauthentication every time](#).

General Availability- Custom Attributes support for Microsoft Entra Domain Services

Type: New feature

Service category: Microsoft Entra Domain Services

Product capability: Microsoft Entra Domain Services

Custom Attributes for Microsoft Entra Domain Services is now Generally Available. This capability allows customers to use Custom Attributes in their managed domains. Legacy applications often rely on custom attributes created in the past to store information, categorize objects, or enforce fine-grained access control over resources. For example, these applications might use custom attributes to store an employee ID in their directory and rely on these attributes in their application LDAP calls. Modifying legacy applications can be costly and risky, and customers might lack the necessary skills or knowledge to make these changes. Microsoft Entra Domain Services now supports custom attributes, enabling customers to migrate their legacy applications to the Azure cloud without modification. It also provides support to synchronize custom attributes from Microsoft Entra ID, allowing customers to benefit from Microsoft Entra ID services in the cloud. For more information, see: [Custom attributes for Microsoft Entra Domain Services](#).

Public Preview - Conditional Access Per-Policy Reporting

Type: New feature

Service category: Conditional Access

Product capability: Identity Security & Protection

Conditional Access Per-Policy Reporting enables admins to easily evaluate the impact of enabled and report-only Conditional Access policies on their organization, without using Log Analytics. This feature surfaces a graph for each policy in the Microsoft Entra Admin Center, visualizing the policy's impact on the tenant's past sign-ins. For more information, see: [Policy impact \(Preview\)](#).

Public Preview - Limit creation or promotion of multitenant apps

Type: New feature

Service category: Directory Management

Product capability: Developer Experience

A new feature has been added to the [App Management Policy Framework](#) that allows restriction on creation or promotion of multitenant applications, providing administrators with greater control over their app environments.

Administrators can now configure tenant default or custom app policy using the new '[audiences](#)' restriction to block new app creation if the signInAudience value provided in the app isn't permitted by the policy. In addition, existing apps can be restricted from changing their signInAudience if the target value isn't permitted by the policy. These policy changes are applied during app creation or update operations, offering control over application deployment and usage. For more information, see: [audiencesConfiguration resource type](#).

General Availability - Download Microsoft Entra Connect Sync on the Microsoft Entra admin center

Type: Plan for change

Service category: Microsoft Entra Connect

Product capability: Identity Governance

The Microsoft Entra Connect Sync .msi installation files are also available on Microsoft Entra admin center within the [Microsoft Entra Connect pane](#). As part of this change, we'll stop uploading new installation files on the [Microsoft Download Center](#).

General Availability - New Microsoft-managed Conditional Access policies designed to limit device code flow and legacy authentication flows

Type: Changed feature

Service category: Conditional Access

Product capability: Access Control

As part of our ongoing commitment to enhance security and protect our customers from evolving cyber threats, we're rolling out two new Microsoft-managed Conditional Access policies designed to limit device code flow and legacy authentication flows. These policies are aligned to the secure by default principle of our broader [Secure Future Initiative](#), which aims to provide robust security measures to safeguard your organization by default.

Deprecated - Upgrade your Microsoft Entra Connect Sync version to avoid impact on the Sync Wizard

Type: Deprecated

Service category: Microsoft Entra Connect

Product capability: Microsoft Entra Connect

As announced in the Microsoft Entra What's New [Blog](#) and in Microsoft 365 Center communications, customers should upgrade their connect sync versions to at least [2.4.18.0](#) for commercial clouds and [2.4.21.0](#) for non-commercial clouds before April 7, 2025. A breaking change on the Connect Sync Wizard will affect all requests that require authentication such as schema refresh, configuration of staging mode, and user sign in changes. For more information, see: [Minimum versions](#).

February 2025

General Availability - Authentication methods migration wizard

Type: New feature

Service category: MFA

Product capability: User Authentication

The authentication methods migration guide in the Microsoft Entra Admin Center lets you automatically migrate method management from the [legacy MFA and SSPR policies](#) to the [converged authentication methods policy](#). In 2023, it was announced that the ability to manage authentication methods in the legacy MFA and SSPR policies would be retired in September 2025. Until now, organizations had to manually migrate methods themselves by using [the migration toggle](#) in the converged policy. Now, you can migrate in just a few selections by using the migration guide. The guide evaluates what your organization currently has enabled in both legacy policies, and generates a recommended converged policy configuration for you to review and edit as needed. From there, confirm the configuration, and we set it up for you and mark your migration as complete. For more information, see: [How to migrate MFA and SSPR policy settings to the Authentication methods policy for Microsoft Entra ID](#).

Public Preview - Enhanced user management in Admin Center UX

Type: New feature

Service category: User Management

Product capability: User Management

Admins are now able to multi-select and edit users at once through the Microsoft Entra Admin Center. With this new capability, admins can bulk edit user properties, add users to groups, edit account status, and more. This UX enhancement will significantly improve efficiency for user management tasks in the Microsoft Entra admin center. For more information, see: [Add or update a user's profile information and settings in the Microsoft Entra admin center.](#)

Public Preview – QR code authentication, a simple and fast authentication method for Frontline Workers

Type: New feature

Service category: Authentications (Logins)

Product capability: User Authentication

We're thrilled to announce public preview of QR code authentication in Microsoft Entra ID, providing an efficient and simple authentication method for frontline workers.

You see a new authentication method 'QR code' in Microsoft Entra ID Authentication method Policies. You can enable and add QR code for your frontline workers via Microsoft Entra ID, My Staff, or MS Graph APIs. All users in your tenant see a new link 'Sign in with QR code' on navigating to <https://login.microsoftonline.com> > 'Sign-in options' > 'Sign in to an organization' page. This new link is visible only on mobile devices (Android/iOS/iPadOS). Users can use this auth method only if you add and provide a QR code to them. QR code auth is also available in BlueFletch and Jamf. MHS QR code auth support is generally available by early March.

The feature has a 'preview' tag until it's generally available. For more information, see: [Authentication methods in Microsoft Entra ID - QR code authentication method \(Preview\).](#)

Public Preview - Custom SAML/WS-Fed External Identity Provider Support in Microsoft Entra External ID

Type: New feature

Service category: B2C - Consumer Identity Management

Product capability: B2B/B2C

By setting up federation with a custom-configured identity provider that supports the SAML 2.0 or WS-Fed protocol, you enable your users to sign up and sign in to your applications using their existing accounts from the federated external provider.

This feature also includes domain-based federation, so a user who enters an email address on the sign-in page that matches a predefined domain in any of the external identity providers will be redirected to authenticate with that identity provider.

For more information, see: [Custom SAML/WS-Fed identity providers \(preview\)](#).

Public Preview - External Auth Methods support for system preferred MFA

Type: New feature

Service category: MFA

Product capability: 3rd Party Integration

Support for external auth methods as a supported method begins rolling out at the beginning of March 2025. When this is live in a tenant where system preferred is enabled and users are in scope of an external auth methods policy, those users will be prompted for their external authentication method if their most secure registered method is Microsoft Authenticator notification. External Authentication Method will appear as third in the list of most secure methods. If the user has a Temporary Access Pass (TAP) or Passkey (FIDO2) device registered, they'll be prompted for those. In addition, users in the scope of an external auth methods policy will have the ability to delete all registered second factor methods from their account, even if the method being deleted is specified as the default sign in method or is system preferred. For more information, see: [System-preferred multifactor authentication - Authentication methods policy](#).

General Availability - Granular Microsoft Graph permissions for Lifecycle workflows

Type: New feature

Service category: Lifecycle Workflows

Product capability: Identity Governance

Now new, lesser privileged permissions can be used for managing specific read and write actions in Lifecycle workflows scenarios. The following granular permissions were introduced in Microsoft Graph:

- LifecycleWorkflows-Workflow.ReadBasic.All
- LifecycleWorkflows-Workflow.Read.All
- LifecycleWorkflows-Workflow.ReadWrite.All
- LifecycleWorkflows-Workflow.Activate
- LifecycleWorkflows-Reports.Read.All
- LifecycleWorkflows-CustomExt.Read.All
- LifecycleWorkflows-CustomExt.ReadWrite.All

For more information, see: [Microsoft Graph permissions reference](#).

January 2025

Public Preview - Manage Lifecycle Workflows with Microsoft Security CoPilot in Microsoft Entra

Type: New feature

Service category: Lifecycle Workflows

Product capability: Identity Governance

Customers can now manage, and customize, Lifecycle Workflows using natural language with Microsoft Security CoPilot. Our Lifecycle Workflows (LCW) Copilot solution provides step-by-step guidance to perform key workflow configuration and execution tasks using natural language. It allows customers to quickly get rich insights to help monitor, and troubleshoot, workflows for compliance. For more information, see: [Manage employee lifecycle using Microsoft Security Copilot \(Preview\)](#).

General Availability - Microsoft Entra PowerShell

Type: New feature

Service category: MS Graph

Product capability: Developer Experience

Manage and automate Microsoft Entra resources programmatically with the scenario-focused Microsoft Entra PowerShell module. For more information, see: [Microsoft Entra PowerShell module now generally available ↗](#).

General Availability - Improving visibility into downstream tenant sign-ins

Type: New feature

Service category: Reporting

Product capability: Monitoring & Reporting

Microsoft Security wants to ensure that all customers are aware of how to notice when a partner is accessing a downstream tenant's resources. Interactive sign-in logs currently provide a list of sign in events, but there's no clear indication of which logins are from partners accessing downstream tenant resources. For example, when reviewing the logs, you might see a series of events, but without any additional context, it's difficult to tell whether these logins are from a partner accessing another tenant's data.

Here's a list of steps that one can take to clarify which logins are associated with partner tenants:

1. Take note of the "ServiceProvider" value in the CrossTenantAccessType column:

- This filter can be applied to refine the log data. When activated, it immediately isolates events related to partner logins.

2. Utilize the "Home Tenant ID" and "Resource Tenant ID" Columns:

- These two columns identify logins coming from the partner's tenant to a downstream tenant.

After seeing a partner logging into a downstream tenant's resources, an important follow-up activity to perform is to validate the activities that might have occurred in the downstream environment. Some examples of logs to look at are Microsoft Entra Audit logs for Microsoft Entra ID events, Microsoft 365 Unified Audit Log (UAL) for Microsoft 365 and Microsoft Entra ID events, and/or the Azure Monitor activity log for Azure events. By following these steps, you're able to clearly identify when a partner is logging into a downstream tenant's resources and subsequent activity in the environment, enhancing your ability to manage and monitor cross-tenant access efficiently.

To increase visibility into the aforementioned columns, Microsoft Entra will begin enabling these columns to display by default when loading the sign-in logs UX starting on March 7, 2025.

Public Preview - Auditing administrator events in Microsoft Entra Connect

Type: New feature

Service category: Microsoft Entra Connect

Product capability: Microsoft Entra Connect

We have released a new version of Microsoft Entra Connect, version 2.4.129.0, that supports the logging of the changes an administrator makes on the Connect Sync Wizard and PowerShell. For more information, see: [Auditing administrator events in Microsoft Entra Connect Sync \(Public Preview\)](#).

Where supported, we'll also autoupgrade customers to this version of Microsoft Entra Connect in February 2025. For customers who wish to be autoupdated, [ensure that you have auto-upgrade configured](#).

For upgrade-related guidance, see [Microsoft Entra Connect: Upgrade from a previous version to the latest](#).

Public Preview - Flexible Federated Identity Credentials

Type: New feature

Service category: Authentications (Logins)

Product capability: Developer Experience

Flexible Federated Identity Credentials extend the existing Federated Identity Credential model by providing the ability to use wildcard matching against certain claims. Currently available for GitHub, GitLab, and Terraform Cloud scenarios, this functionality can be used to lower the total number of FICs required to manage similar scenarios. For more information, see: [Flexible federated identity credentials \(preview\)](#).

General Availability - Real-time Password Spray Detection in Microsoft Entra ID Protection

Type: New feature

Service category: Identity Protection

Product capability: Identity Security & Protection

Traditionally, password spray attacks are detected post breach or as part of hunting activity. Now, we've enhanced Microsoft Entra ID Protection to detect password spray attacks in real-

time before the attacker ever obtains a token. This reduces remediation from hours to seconds by interrupting attacks during the sign-in flow.

Risk-based Conditional Access can automatically respond to this new signal by raising session risk, immediately challenging the sign-in attempt, and stopping password spray attempts in their tracks. This cutting-edge detection, now Generally Available, works alongside existing detections for advanced attacks such as Adversary-in-the-Middle (AitM) phishing and token theft, to ensure comprehensive coverage against modern attacks. For more information, see: [What is Microsoft Entra ID Protection?](#)

General Availability - Protected actions for hard deletions

Type: New feature

Service category: Other

Product capability: Identity Security & Protection

Customers can now configure Conditional Access policies to protect against early hard deletions. Protected action for hard deletion protects hard deletion of users, Microsoft 365 groups, and applications. For more information, see: [What are protected actions in Microsoft Entra ID?](#).

Public Preview - Elevate Access events are now exportable via Microsoft Entra Audit Logs

Type: New feature

Service category: RBAC

Product capability: Monitoring & Reporting

This feature enables administrators to export and stream Elevate Access events to both first-party and third-party SIEM solutions via Microsoft Entra Audit logs. It enhances detection and improves logging capabilities, allowing visibility into who in their tenant has utilized Elevate Access. For more information on how to use the feature, see: [View elevate access log entries](#).

Deprecated - Action Required by February 1, 2025: Azure AD Graph retirement

Type: Deprecated

Service category: Azure AD Graph

Product capability: Developer Experience

The Azure AD Graph API service was [deprecated] in 2020. [Retirement of the Azure AD Graph API service](#) began in September 2024, and the next phase of this retirement starts February 1, 2025. This phase will impact new and existing applications unless action is taken. The latest updates on Azure AD Graph retirement can be found here: [Take action by February 1: Azure AD Graph is retiring](#).

Starting from February 1, both new and existing applications will be prevented from calling Azure AD Graph APIs, unless they're configured for an extension. You might not see impact right away, as we're rolling out this change in stages across tenants. We anticipate full deployment of this change around the end of February, and by the end of March for national cloud deployments.

If you haven't already, it's now urgent to review the applications on your tenant to see which ones depend on Azure AD Graph API access, and mitigate or migrate these before the February 1 cutoff date. For applications that haven't migrated to Microsoft Graph APIs, [an extension](#) can be set to allow the application access to Azure AD Graph through June 30, 2025.

Microsoft Entra Recommendations are the best tool to identify applications that are using Azure AD Graph APIs in your tenant and require action. Reference this blog post: Action required: [Azure AD Graph API retirement](#) for step by step guidance.

General Availability - Microsoft Entra Connect Version 2.4.129.0

Type: Changed feature

Service category: Microsoft Entra Connect

Product capability: Microsoft Entra Connect

On January 15, 2025, we released Microsoft Entra Connect Sync Version 2.4.129.0 which supports auditing administrator events. More details are available in the [release notes](#). We'll automatically upgrade eligible customers to this latest version of Microsoft Entra Connect in February 2025. For customers who wish to be auto-upgraded, [ensure that you have auto-upgrade configured](#).

Deprecated - Take action to avoid impact when legacy MSOnline and AzureAD PowerShell modules retire

Type: Deprecated

Service category: Legacy MSOnline and AzureAD PowerShell modules

Product capability: Developer Experience

As announced in Microsoft Entra [change announcements](#) and in the Microsoft Entra [Blog](#), the MSOnline, and Microsoft Azure AD PowerShell modules (for Microsoft Entra ID) retired on March 30, 2024.

The retirement for MSOnline PowerShell module starts in early April 2025, and ends in late May 2025. If you're using MSOnline PowerShell, you must take action by March 30, 2025 to avoid impact after the retirement by migrating any use of MSOnline to [Microsoft Graph PowerShell SDK](#) or [Microsoft Entra PowerShell](#).

Key points

- MSOnline PowerShell will retire, and stop working, between early April 2025 and late May 2025
- AzureAD PowerShell will no longer be supported after March 30, 2025, but its retirement will happen in early July 2025. This postponement is to allow you time to finish the MSOnline PowerShell migration
- To ensure customer readiness for MSOnline PowerShell retirement, a series of temporary outage tests will occur for all tenants between January 2025 and March 2025.

For more information, see: [Action required: MSOnline and AzureAD PowerShell retirement - 2025 info and resources](#).

December 2024

General Availability - What's new in Microsoft Entra

Type: New feature

Service category: Reporting

Product capability: Monitoring & Reporting

What's new in Microsoft Entra offers a comprehensive view of Microsoft Entra product updates including product roadmap (like Public Previews and recent GAs), and change announcements (like deprecations, breaking changes, feature changes and Microsoft-managed policies). It's a one stop shop for Microsoft Entra admins to discover the product updates.

Public Preview - Microsoft Entra ID Governance: Approvers can revoke access in MyAccess

Type: New feature

Service category: Entitlement Management

Product capability: Entitlement Management

For Microsoft Entra ID Governance users, approvers of access package requests can now revoke their decision in MyAccess. Only the person who took the approve action is able to revoke access. To opt into this feature, admins can go to the [Identity Governance settings page](#), and enable the feature. For more information, see: [What is the My Access portal?](#).

General Availability - Expansion of SSPR Policy Audit Logging

Type: New feature

Service category: Self Service Password Reset

Product capability: Monitoring & Reporting

Starting Mid-January, we are improving the audit logs for changes made to the SSPR Policy.

With this improvement, any change to the SSPR policy configuration, including enablement or disablement, will result in an audit log entry that includes details about the change made. Additionally, both the previous values and current values from the change will be recorded within the audit log. This additional information can be found by selecting an audit log entry and selecting the Modified Properties tab within the entry.

These changes are rolled out in phases:

- Phase 1 includes logging for the Authentication Methods, Registration, Notifications, and Customization configuration settings.
- Phase 2 includes logging for the On-premises integration configuration settings.

This change occurs automatically, so admins take no action. For more information and details regarding this change, see: [Microsoft Entra audit log categories and activities](#).

General Availability - Update Profile Photo in MyAccount

Type: New feature

Service category: My Profile/Account

Product capability: End User Experiences

Users can now update their profile photo directly from their MyAccount portal. This change exposes a new edit button on the profile photo section of the user's account.

In some environments, it's necessary to prevent users from making this change. Global Administrators can manage this using a tenant-wide policy with Microsoft Graph API, following the guidance in the [Manage user profile photo settings in Microsoft 365](#) document.

General Availability - Temporary Access Pass (TAP) support for internal guest users

Type: New feature

Service category: MFA

Product capability: Identity Security & Protection

Microsoft Entra ID now supports issuing Temporary Access Passes (TAP) to internal guest users. TAPs can be issued to internal guests just like normal members, through the Microsoft Entra ID Admin Center, or natively through Microsoft Graph. With this enhancement, internal guests can now seamlessly onboard, and recover, their accounts with time-bound temporary credentials.

For more information, see: [Configure Temporary Access Pass to register passwordless authentication methods](#).

Public Preview - Microsoft Entra ID Governance: access package request suggestions

Type: New feature

Service category: Entitlement Management

Product capability: Entitlement Management

Opt-In As communicated [earlier](#), we're excited to introduce a new feature in [My Access](#): a curated list of suggested access packages. This capability allows users to quickly view the most relevant access packages (based off their peers' access packages and previous requests) without scrolling through a long list. In December you can [enable the preview in the Opt-in Preview Features for Identity Governance](#). From January, this setting is enabled by default.

Public Preview - Security Copilot embedded in Microsoft Entra

Type: New feature

Service category: Other

Product capability: Identity Security & Protection

We've announced the public preview of Microsoft Security Copilot embedded in the Microsoft Entra admin Center. This integration brings all identity skills previously made generally available for the Security Copilot standalone experience in April 2024, along with new identity capabilities for admins and security analysts to use directly within the Microsoft Entra admin center. We've also added brand new skills to help improve identity-related risk investigation. In December, we broaden the scope even further to include a set of skills specifically for App Risk Management in both standalone and embedded experiences of Security Copilot and Microsoft Entra. These capabilities allow identity admins and security analysts to better identify, understand, and remediate the risks impacting applications and workload identities registered in Microsoft Entra.

With Security Copilot now embedded in Microsoft Entra, identity admins get AI-driven, natural-language summaries of identity context and insights tailored for handling security incidents, equipping them to better protect against identity compromise. The embedded experience also accelerates troubleshooting tasks like resolving identity-related risks and sign-in issues, without ever leaving the admin center.

Public Preview - Security Copilot in Microsoft Entra: App Risk skills

Type: New feature

Service category: Other

Product capability: Identity Security & Protection

Identity admins and security analysts managing Microsoft Entra ID registered apps can identify and understand risks through natural language prompts. Security Copilot has links to the Microsoft Entra Admin Center for admins to take needed remediation actions. For more information, see: [Assess application risks using Microsoft Security Copilot in Microsoft Entra](#).

Public Preview - Provision custom security attributes from HR sources

Type: New feature

Service category: Provisioning

Product capability: Inbound to Entra ID

With this feature, customers can automatically provision "*custom security attributes*" in Microsoft Entra ID from authoritative HR sources. Supported authoritative sources include: Workday, SAP SuccessFactors, and any HR system integrated using API-driven provisioning.

Public Preview - Sign in with Apple

Type: New feature

Service category: B2C - Consumer Identity Management

Product capability: Extensibility

This new feature adds Apple to our list of preconfigured social identity providers. As the first social identity provider implemented on the eSTS platform, it introduces a "*Sign in with Apple*" button to the sign-in options, allowing users to access applications with their Apple accounts. For more information, see: [Add Apple as an identity provider \(preview\)](#).

General Availability - Microsoft Entra External ID Custom URL Domains

Type: New feature

Service category: Authentications (Logins)

Product capability: Identity Lifecycle Management

This feature allows users to customize their Microsoft default sign in authentication endpoint with their own brand names. Custom URL Domains help users to change Ext ID endpoint < tenant-name >.ciamlogin.com to login.contoso.com.

General Availability - Privileged Identity Management integration in Azure Role Based Access Control

Type: New feature

Service category: RBAC

Product capability: Access Control

Privileged Identity Management (PIM) capabilities are now integrated into the Azure Role Based Access Control (Azure RBAC) UI. Before this integration, RBAC admins could only manage standing access (active permanent role assignments) from the Azure RBAC UI. With this integration, just-in-time access and timebound access, which are functionalities supported

by PIM, are now brought into the Azure RBAC UI for customers with either a P2, or Identity Governance, license.

RBAC admins can create assignments of type eligible and timebound duration from the Azure RBAC add role assignment flow, see the list of different states of role assignment in a single view, as well as convert the type and duration of their role assignments from the Azure RBAC UI. In addition, end users now see all their role assignments of different state straight from the Azure RBAC UI landing page, from where they can also activate their eligible role assignments. For more information, see: [List role assignments at a scope](#).

General Availability - Dedicated new 1st party resource application to enable Active Directory to Microsoft Entra ID sync using Microsoft Entra Connect Sync or Cloud Sync

Type: Changed feature

Service category: Provisioning

Product capability: Directory

As part of ongoing security hardening, Microsoft deployed Microsoft Entra AD Synchronization Service, a dedicated first-party application to enable the synchronization between Active Directory and Microsoft Entra ID. This new application, with Application ID `6bf85cfa-ac8a-4be5-b5de-425a0d0dc016`, was provisioned in customer tenants that use Microsoft Entra Connect Sync or the Microsoft Entra Cloud Sync service.

November 2024

Public Preview - Universal Continuous Access Evaluation

Type: New feature

Service category: Provisioning

Product capability: Network Access

Continuous Access Evaluation (CAE) revokes, and revalidates, network access in near real-time whenever Microsoft Entra ID detects changes to the identity. For more information, see: [Universal Continuous Access Evaluation \(Preview\)](#).

Public Preview - Microsoft Entra new store for certificate-based authentication

Type: New feature

Service category: Authentications (Logins)

Product capability: User Authentication

Microsoft Entra ID has a new scalable PKI (Public Key Infrastructure) based CA (Certificate Authorities) store with higher limits for the number of CAs and the size of each CA file. PKI based CA store allows CAs within each different PKI to be in its own container object allowing administrators to move away from one flat list of CAs to more efficient PKI container based CAs. PKI-based CA store now supports up to 250CAs, 8KB size for each CA and also supports issuers hints attribute for each CA. Administrators can also upload the entire PKI and all the CAs using the "Upload CBA PKI" feature or create a PKI container and upload CAs individually. For more information, see: [Step 1: Configure the certificate authorities with PKI-based trust store \(Preview\)](#).

Public Preview - Updating profile photo in MyAccount

Type: New feature

Service category: My Profile/Account

Product capability: End User Experiences

On November 13, 2024, users received the ability to update their profile photo directly from their [MyAccount](#) portal. This change exposes a new edit button on the profile photo section of the user's account.

In some environments, it's necessary to prevent users from making this change. Global Administrators can manage this using a tenant-wide policy with Microsoft Graph API, following the guidance in the [Manage user profile photo settings in Microsoft 365](#) document.

General Availability - Microsoft Entra Health Monitoring, Health Metrics Feature

Type: New feature

Service category: Reporting

Product capability: Monitoring & Reporting

Microsoft Entra health monitoring, available from the Health pane, includes a set of low-latency pre-computed health metrics that can be used to monitor the health of critical user scenarios

in your tenant. The first set of health scenarios includes MFA, CA-compliant devices, CA-managed devices, and SAML authentications. This set of monitor scenarios will grow over time. These health metrics are now released as general availability data streams with the public preview of an intelligent alerting capability. For more information, see: [What is Microsoft Entra Health?](#)

General Availability - Microsoft Entra Connect Sync Version 2.4.27.0

Type: Changed feature

Service category: Provisioning

Product capability: Identity Governance

On November 14, 2025, we released Microsoft Entra Connect Sync Version 2.4.27.0 that uses the OLE DB version 18.7.4 that further hardens our service. Upgrade to this latest version of connect sync to improve your security. More details are available in the [release notes](#).

Changed feature - expansion of WhatsApp as an MFA one-time passcode delivery channel for Microsoft Entra ID

Type: Changed feature

Service category: MFA

Product capability: User Authentication

In late 2023, Microsoft Entra ID started using WhatsApp as an alternate channel to deliver multifactor authentication (MFA) one-time passcodes to users in India and Indonesia. We saw improved deliverability, completion rates, and satisfaction when using the channel in both countries. The channel was temporarily disabled in India in early 2024. Starting early December 2024, we'll be re-enabling the channel in India, and expanding its use to more countries.

Starting December 2024, users in India, and other countries can start receiving MFA text messages via WhatsApp. Only users that are enabled to receive MFA text messages as an authentication method, and already have WhatsApp on their phone, get this experience. If a user with WhatsApp on their device is unreachable or doesn't have internet connectivity, we'll quickly fall back to the regular SMS channel. In addition, users receiving OTPs via WhatsApp for the first time will be notified of the change in behavior via SMS text message.

If you don't want your users to receive MFA text messages through WhatsApp, you can disable text messages as an authentication method in your organization or scope it down to only be

enabled for a subset of users. Note that we highly encourage organizations move to using more modern, secure methods like Microsoft Authenticator and passkeys in favor of telecom and messaging app methods. For more information, see: [Text message verification](#).

Retirement - MFA Fraud Alert will be retired on March 1st 2025

Type: Deprecated

Service category: MFA

Product capability: Identity Security & Protection

Microsoft Entra multifactor authentication (MFA) fraud alert allows end users to report MFA voice calls, and Microsoft Authenticator push requests, they didn't initiate as fraudulent. Beginning March 1, 2025, MFA Fraud Alert will be retired in favor of the replacement feature [Report Suspicious Activity](#) which allows end users to report fraudulent requests, and is also integrated with [Identity Protection](#) for more comprehensive coverage and remediation. To ensure users can continue reporting fraudulent MFA requests, organizations should migrate to using Report Suspicious Activity, and review how reported activity is remediated based on their Microsoft Entra licensing. For more information, see: [Configure Microsoft Entra multifactor authentication settings](#).

Public Preview - Microsoft Entra Health Monitoring, Alerts Feature

Type: Changed feature

Service category: Other

Product capability: Monitoring & Reporting

Intelligent alerts in Microsoft Entra health monitoring notify tenant admins, and security engineers, whenever a monitored scenario breaks from its typical pattern. Microsoft Entra's alerting capability watches the low-latency health signals of each scenario, and fires a notification if an anomaly is detected. The set of alert-ready health signals and scenarios will grow over time. This alerts feature is now available in Microsoft Entra Health as an API-only public preview release (UX release is scheduled for February 2025). For more information, see: [How to use Microsoft Entra Health monitoring alerts \(preview\)](#).

General Availability - Log analytics sign-in logs schema is in parity with MSGraph schema

Type: Plan for change

Service category: Authentications (Logins)

Product capability: Monitoring & Reporting

To maintain consistency in our core logging principles, we've addressed a legacy parity issue where the Azure Log Analytics sign-in logs schema didn't align with the MSGraph sign-in logs schema. The updates include fields such as ClientCredentialType, CreatedDateTime, ManagedServiceIdentity, NetworkLocationDetails, tokenProtectionStatus, SessionID, among others. These changes take effect in the first week of December 2024.

We believe this enhancement provides a more consistent logging experience. As always, you can perform pre-ingestion transformations to remove any unwanted data from your Azure Log Analytics storage workspaces. For guidance on how to perform these transformations, see:

[Data collection transformations in Azure Monitor](#).

Deprecated - MIM hybrid reporting agent

Type: Deprecated

Service category: Microsoft Identity Manager

Product capability: Monitoring & Reporting

The hybrid reporting agent, used to send a MIM Service event log to Microsoft Entra to surface in password reset and self-service group management reports, is deprecated. The recommended replacement is to use Azure Arc to send the event logs to Azure Monitor. For more information, see: [Microsoft Identity Manager 2016 reporting with Azure Monitor](#).
