How to Configure Jamf Pro and Intune Company Portal for macOS Platform SSO Integration

Rev 20250519

Contents

Preface

What is Platform SSO
Platform SSO is a framework introduced in macOS 13 that enables single sign-on (SSO) at a system level, allowing users to authenticate once and then seamlessly access multiple apps and services without needing to re-enter credentials. Platform SSO integrates with identity providers (IdPs) like Microsoft Entra ID enabling organizations to streamline authentication across apps and services within their enterprise environment.

When integrated with Microsoft Entra ID, Platform single sign-on for macOS (Platform SSO) allows end users to authenticate to their computers using a smart card or their Entra ID credentials. Alternatively, it can be configured to create a secure, hardware-bound, non-phishable authentication factor used by Entra ID to access organization resources. In this "Secure Enclave Key" mode, the local account credentials are unchanged and knowledge of the local account password fulfills the need for multiple factors for conditional access policies.

This configuration qualifies as multi-factor authentication (MFA) because it combines two distinct types of authentication factors. When a user signs in with their local username and password along with the Secure Enclave–backed key, it satisfies "something you know" (the password) and "something you have" (the hardware-bound key stored in the Secure Enclave). Alternatively, if Touch ID is used along with the Secure Enclave key, it satisfies "something you are" (the biometric fingerprint) and "something you have" (the Secure Enclave–backed key), thus also meeting MFA requirements.

Key Features of Platform SSO
System-wide SSO After a user authenticates via an Identity Provider their session is maintained across multiple apps and services allowing them to access resources without re-authentication.

Integration with Enterprise SSO Plugin macOS supports the Microsoft Enterprise SSO plugin, which works with Microsoft's identity services such as Microsoft 365 and other supported enterprise services to allow smooth authentication without needing separate app logins.

Login Window SSO In some configurations, Platform SSO can work directly from the macOS login screen, allowing users to authenticate to their device using their enterprise credentials and access services without additional prompts. Platform SSO, when configured in password mode, supports user authentication with a newly updated password directly from the FileVault login screen or the standard macOS login window. When a user logs in with their updated Entra ID password and does not recall their previous local password, this workflow can initiate an automatic keychain reset. This helps maintain access continuity while reducing the need for manual keychain troubleshooting or IT intervention.

Device Compliance If integrated with Microsoft Intune or another MDM like Jamf Pro, Platform SSO can ensure that devices comply with organizational security policies before granting access to resources.

Platform SSO supports the following authentication methods:

- Password
- Secure Enclave
- Smart Card

Microsoft highly recommends using Secure Enclave as the authentication method when configuring Platform SSO. If using Platform SSO on a shared Mac, Password is the recommended authentication method by Microsoft over the Secure Enclave method as all users may not have a way to use multi factor authentication.

For more information on shared devices, go here:

https://learn.microsoft.com/en-us/entra/identity/devices/device-join-macos-platform-single-sign-on-multi-user-device

Feature	Secure Enclave	Smart Card	Password
Passwordless (phishing resistant)	✅	✅	❌
TouchID supported for unlock	✅	✅	✅
Can be used as passkey	✅	❌	❌
MFA mandatory for setup Multifactor authentication (MFA) is always recommended	✅	✅	❌
Local Mac password synced with Entra ID	❌	❌	✅
Supported on macOS 13.x +	✅	❌	✅
Supported on macOS 14.x +	✅	✅	✅
Optionally, allow new users to log in with Entra ID credentials (macOS 14.x +)	✅	✅	✅

TLS Inspection and Apple's SSO Framework

The number one support call at Microsoft for macOS SSO not functioning properly is due to TLS Inspection not being allowed access to the URL's below:

https://app-site-association.cdn-apple.com

https://app-site-association.cdn-apple.com

Microsoft recommends allowing the above URL's or preferably adding wildcards in your firewall for:

`*.cdn-apple.com`

`*.networking.apple`

What Platform SSO is NOT

- Not "Windows Hello for Business" for Macs.
- Not a replacement for passwords. Apple states, "Passcodes and passwords are essential to the security of Apple devices."
- Does not support FIDO2 authenticators at login or FileVault screens.
- Does not deploy automatically via zero-touch onboarding; an admin must register the device interactively for just-in-time account creation.
- Does not replace the FileVault authentication screen. On Apple Silicon, only a password or SecureCard linked to a local user can decrypt FileVault.
- Does not enforce Multi-Factor Authentication (MFA) for macOS, including FileVault decryption, login, or admin authorization prompts.
- Not a password-less login method. SmartCards remain the only macOS-native password-less option. However, Platform SSO allows SmartCard-based cloud identity account creation in macOS Sonoma.
- It does not support VisionOS, iOS, iPadOS, or tvOS. It is exclusive to macOS.
- Does not create MDM-enabled users or allow user-level configuration profiles.
- Does not allow password changes at the login window.
- Does not support RADIUS 802.1x

Requirements for Platform SSO with Microsoft Entra ID

This guide will use Microsoft Entra ID as the IdP and macOS 15 for the lessons in the guide. As of this writing, Microsoft Platform Single Sign-on is in public preview so please keep that in mind when following the lessons in this guide.

Get more information on Platform SSO features at the link below:

https://learn.microsoft.com/en-us/mem/intune/configuration/platform-sso-macos

Special thanks to the following individuals for making this guide possible:

- Christos Drosos
- John Hutchison
- Michael Epping
- Michael Lopez
- Sean Rabbitt
- Yash Patel

Section 1: Configure MFA in Microsoft Entra

What You'll Need:
Learn what hardware, software, and information you'll need to complete the tutorials in this section.

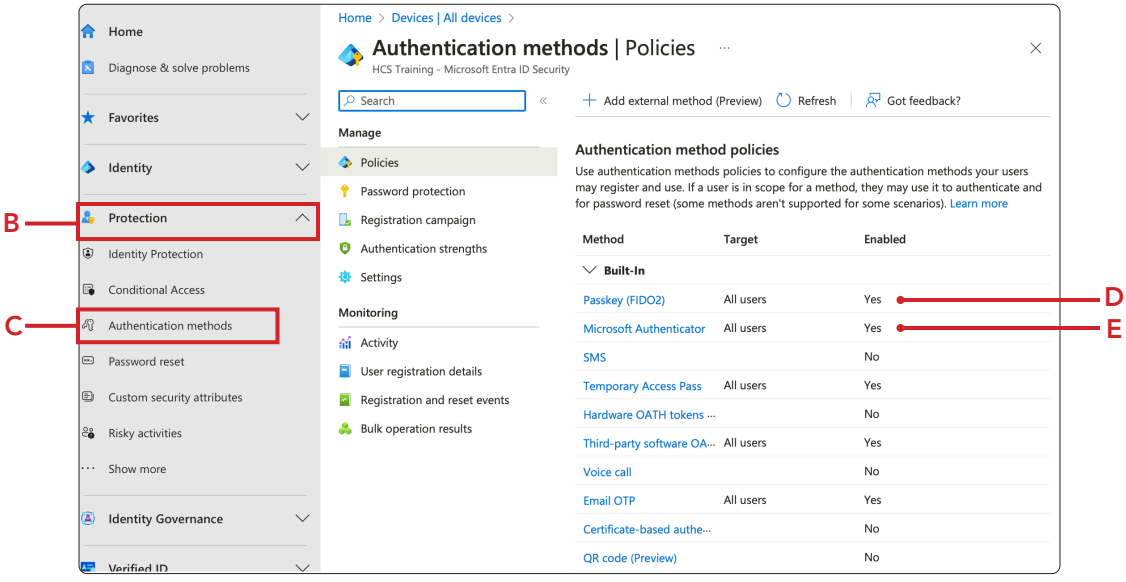
Hardware and Software:
Requirements for following along with this section:

- An authentication method policy in Microsoft Entra with Microsoft Authenticator and Passkey (FIDO2) enabled
- An active user account in Microsoft Entra
- Access to an iPhone or iPad running iOS 16 or later with the Microsoft Authenticator app installed
- A Personal Identification Device (PIV) This guide will use a Yubikey (Optional)

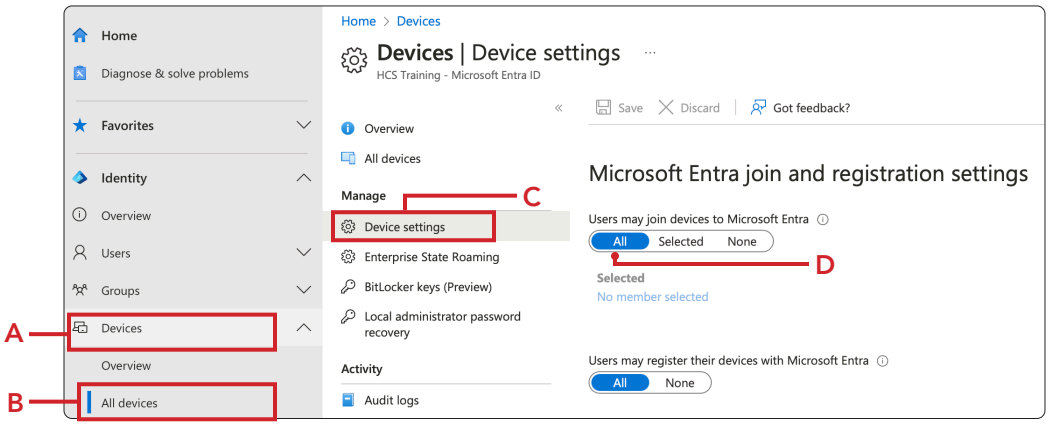
In this section, we will configure multi-factor authentication (MFA) settings in Microsoft Entra to utilize a Passkey stored on your iPhone and a YubiKey personal identification device. Both of these methods enable password-less authentication for your Mac while providing phishing-resistant credentials for WebAuthn challenges.

1. This step is a prerequisite. You cannot continue with the lessons in this guide without proper authentication methods in place on your Microsoft Entra tenant. Your Microsoft Entra Authentication method policy must have Microsoft Authenticator and Passkey (FIDO2) enabled and scoped to a target group of your choosing. This guide will use the All users group for simplicity. Administrative privileges on your Microsoft Entra tenant are required to configure these settings. Follow these steps below:

   A. Log into Microsoft Entra with administrative privileges. https://entra.microsoft.com
   B. Select Protection.
   C. Select Authentication methods.
   D. Select Passkey (FIDO2) and enable it with a Target of your choosing and save.
   E. Select Microsoft Authenticator and enable it with a Target of your choosing and save.



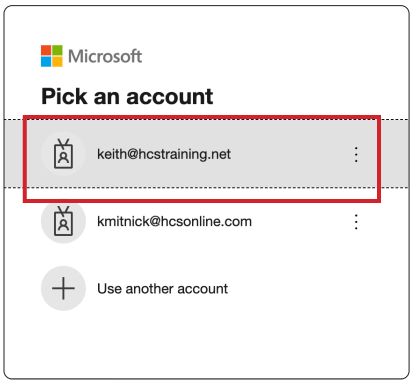
2. Users must be able to join devices in Microsoft Entra.
   A. Click Devices.
   B. Click All devices.
   C. Select Device settings.
   D. Under Users may join devices to Microsoft Entra, select how users join their device to connect to Microsoft Entra. This guide will select All.



3. Using a web browser of your choosing, go to

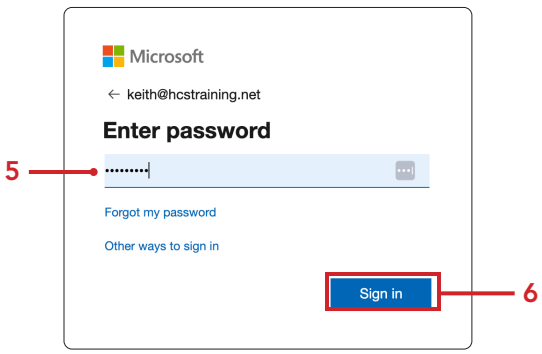
   https://mysignins.microsoft.com

4. Sign in with your Microsoft user account.



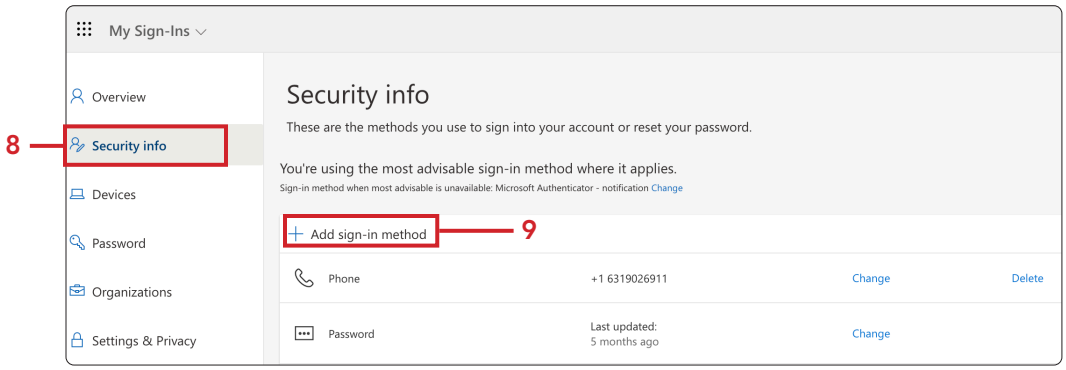
5. Enter your password.

6. Click Sign in.

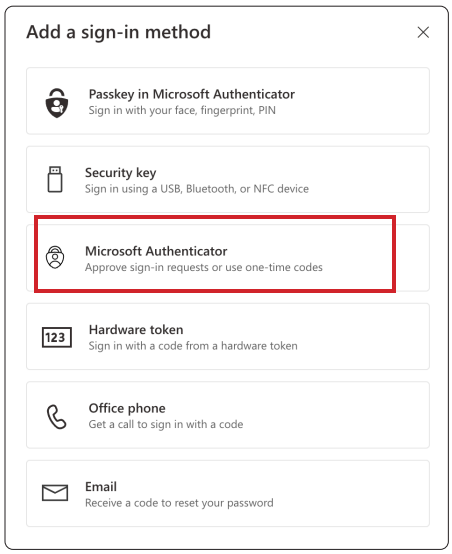


7. Select the option of reducing the number of times you are asked to sign in. This guide will select Yes.

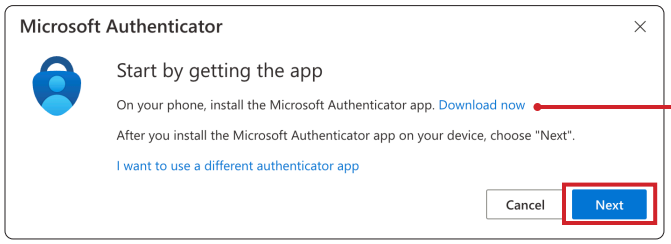
8. Click Security info.
9. Click Add sign-in method (+).



10. Select Microsoft Authenticator.

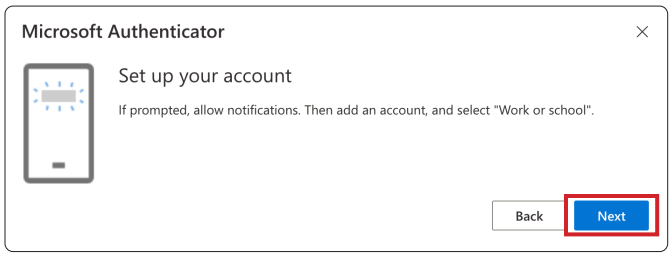


11. If you need to download the Microsoft Authenticator app on your device, click Download now, otherwise click Next.



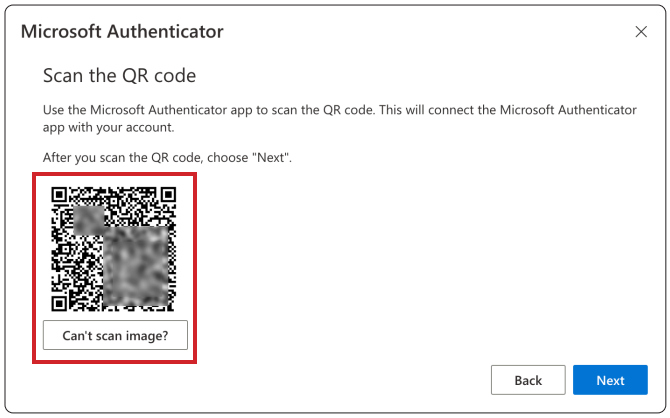
Click Download Now if you need to obtain the Microsoft Authenticator app

12. Click Next.

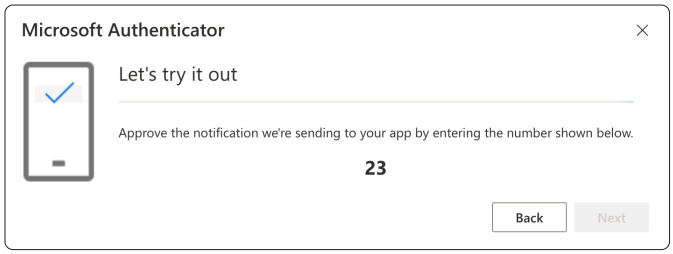


13. Scan the QR code with your device.

14. Click Next.

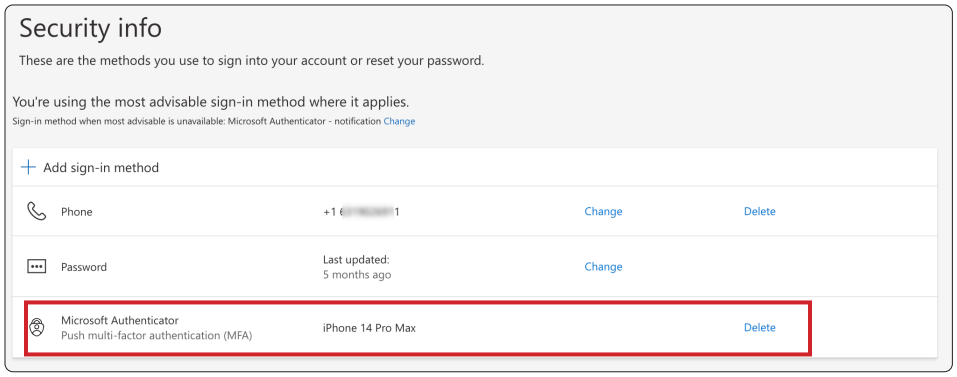


15. Enter the code in the Microsoft Authenticator app on your device.

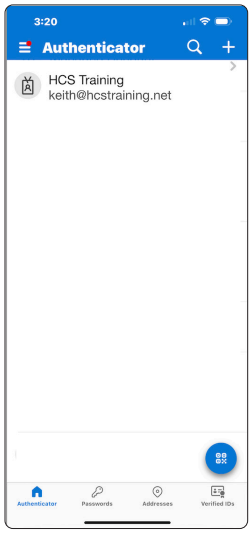


16. Click Next.

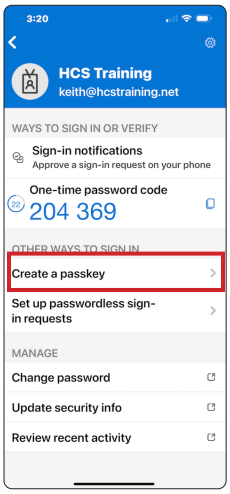
17. Confirm Microsoft Authenticator shows in the list below.



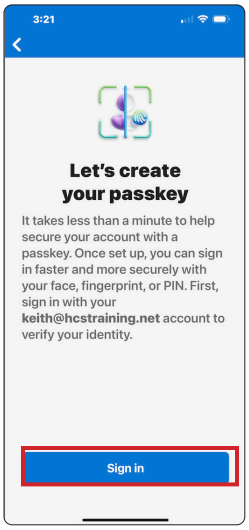
18. Open the Authenticator app on your device and tap your account.



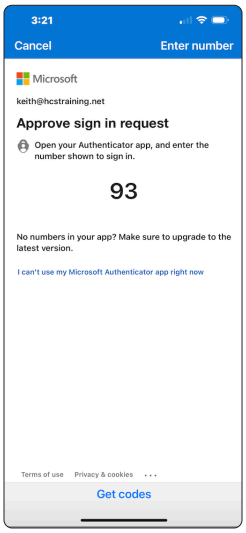
19. Tap Create a passkey.



20. Tap Sign in.

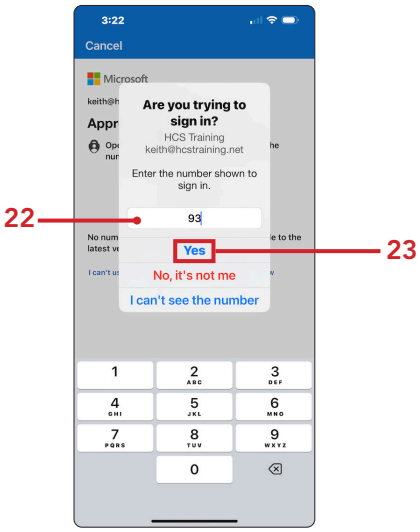


21. Confirm the app needs to approve your sign in request with a number.

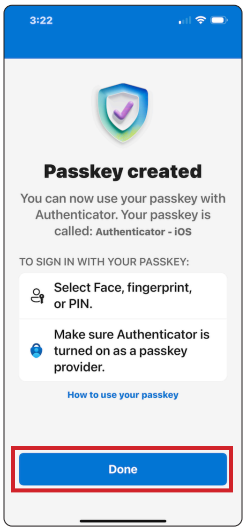


22. Enter the number.

23. Tap Yes.

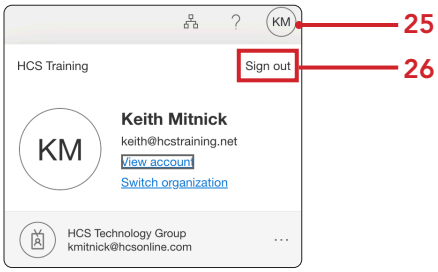


24. Tap Done.

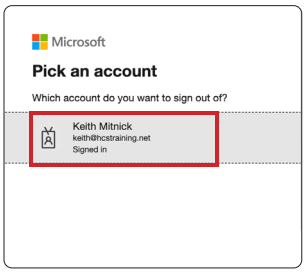


25. Let's test the passkey. Using a web browser of your choosing, go to https://mysignins.microsoft.com
Click on your account in the upper-right corner

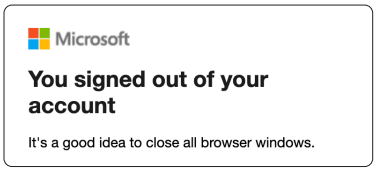
26. Click Sign out.



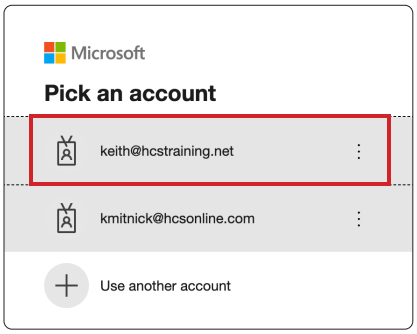
27. Select the account you want to sign out of.



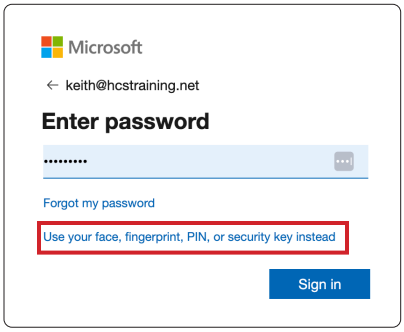
28. Confirm you have signed out of your account.



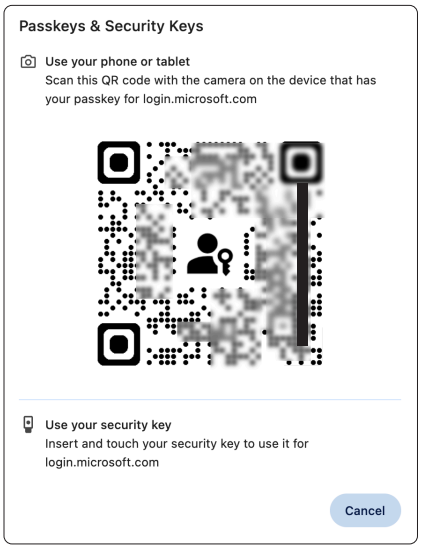
29. Select an account to sign in with.



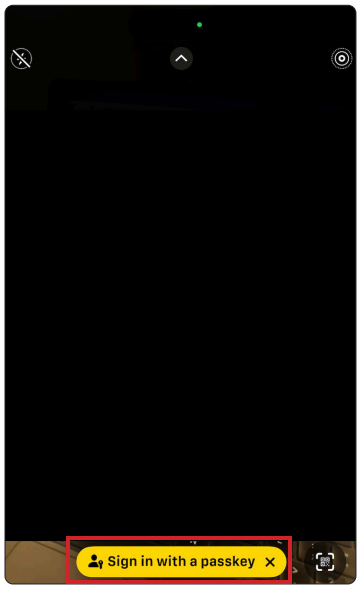
30. At the password login screen, select Use your face, fingerprint, PIN, or security key instead.



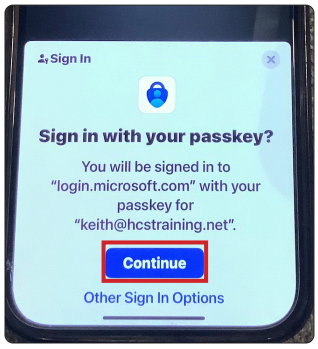
31. A QR code will appear. Scan this with the Camera.app on your device.



32. On your device, Tap Sign in with a passkey.

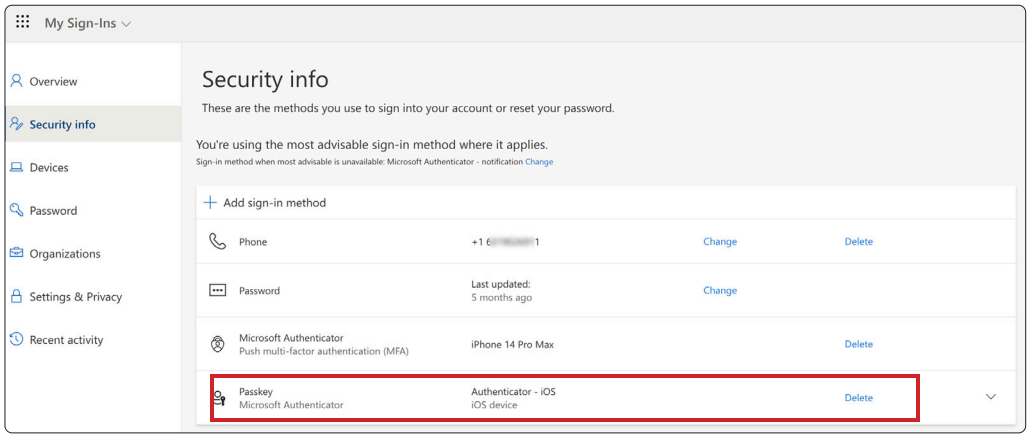


33. On your device, Tap Continue.



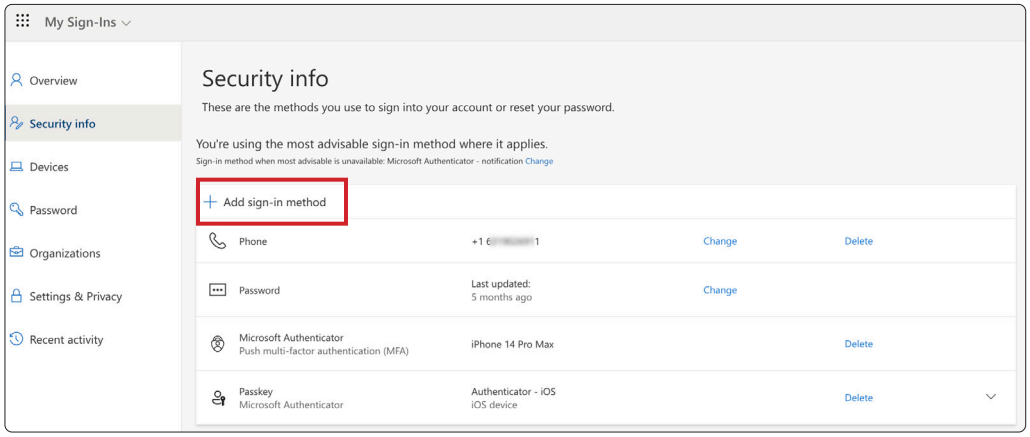
34. Select the option of reducing the number of times you are asked to sign in. This guide will select Yes.

35. Click Security Info, and confirm your Passkey shows in the list.

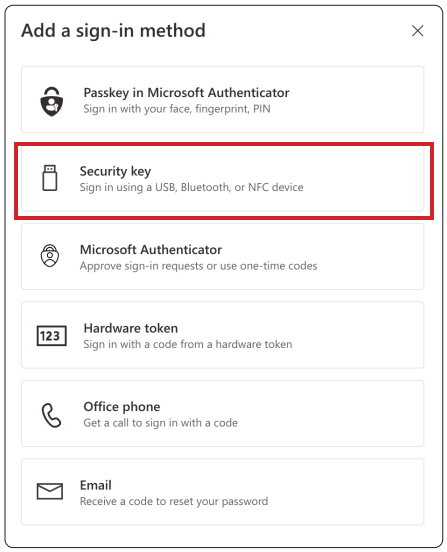


The next steps are optional and require a Personal Identification Device (PIV) This guide will use a Security Key (Yubikey shown below). You can skip these steps if they are not required by your organization.

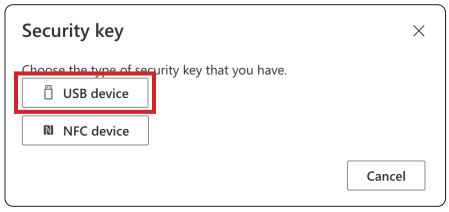
36. Click Add sing-in method.



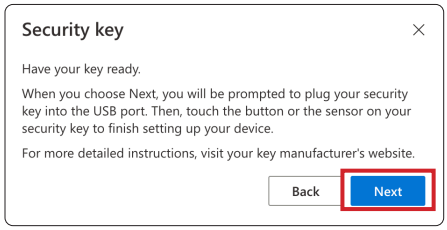
37. Select Security key.



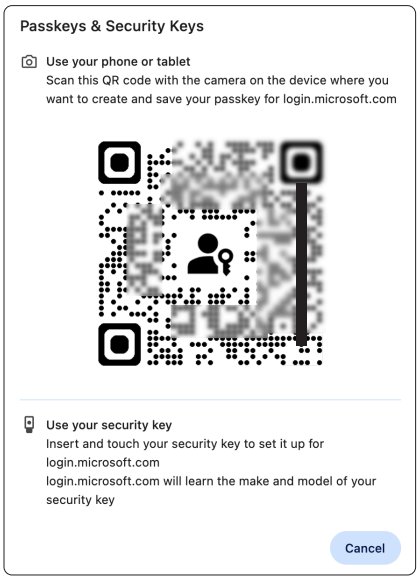
38. Select your security key type. This guide will select USB device.



39. Click Next.

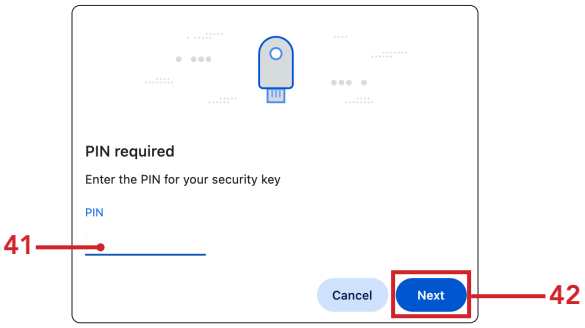


40. Connect your security key and activate the security key.
    NOTE: Follow the instructions on how to activate your security key.

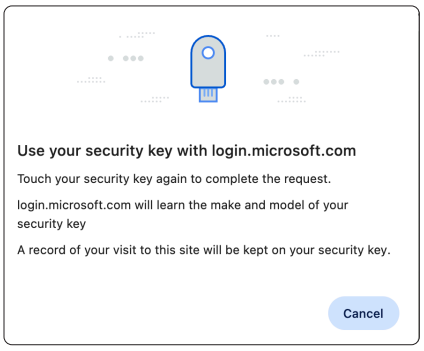


41. Enter your PIN for your security key if prompted.

42. Click Next.

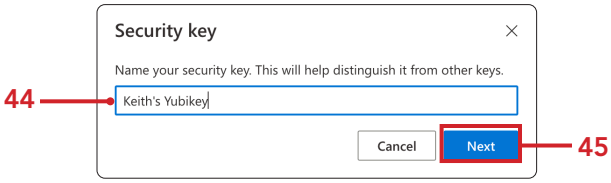


43. Activate your security key.

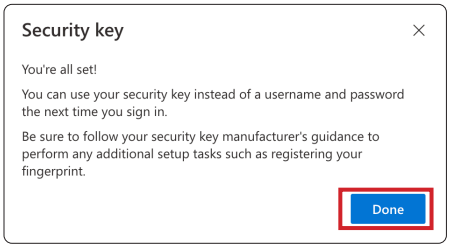


44. Enter a name your security key.

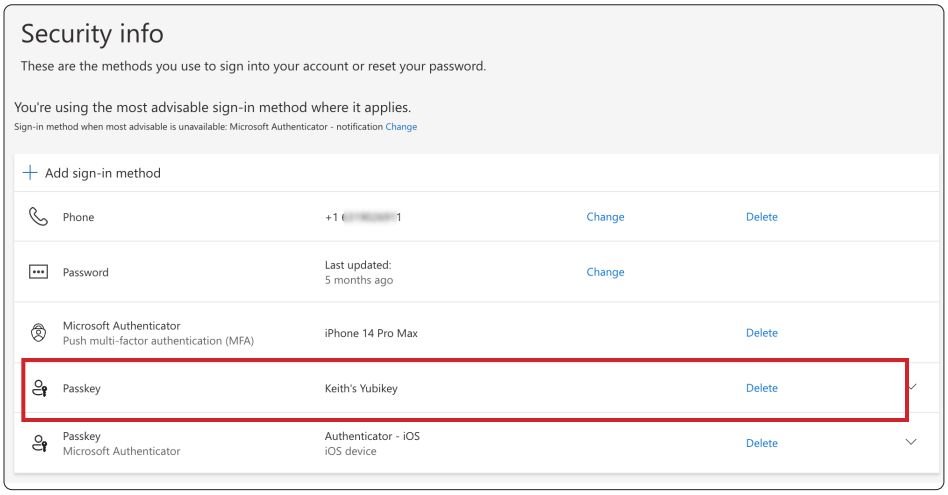
45. Click Next.



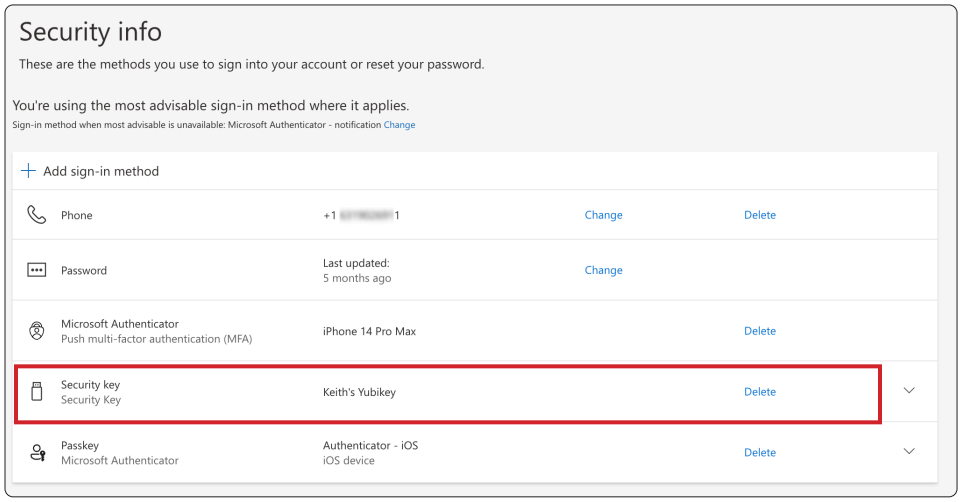
46. Click Done.



47. Confirm your security key shows in the list. It will show as Passkey with the name you provided for your key.



48. In the step above, the Security key showed up as a Passkey. This will change once you sign in to your Microsoft account with your security key. It will show up in the list as Security key going forward.



This completes this section. In the next section, we will create a smart computer group in Jamf Pro to find all Mac computers running macOS 14.5 or later. While macOS 13 supports Platform SSO, it is recommended to use macOS 14.5 or later to leverage the latest enhancements and features.

Section 2: Creating a smart computer group

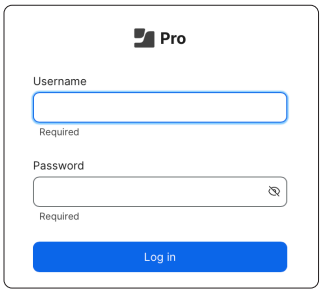
What You'll Need:
Learn what hardware, software, and information you'll need to complete the tutorials in this section.

Hardware and Software:
Requirements for following along with this section:

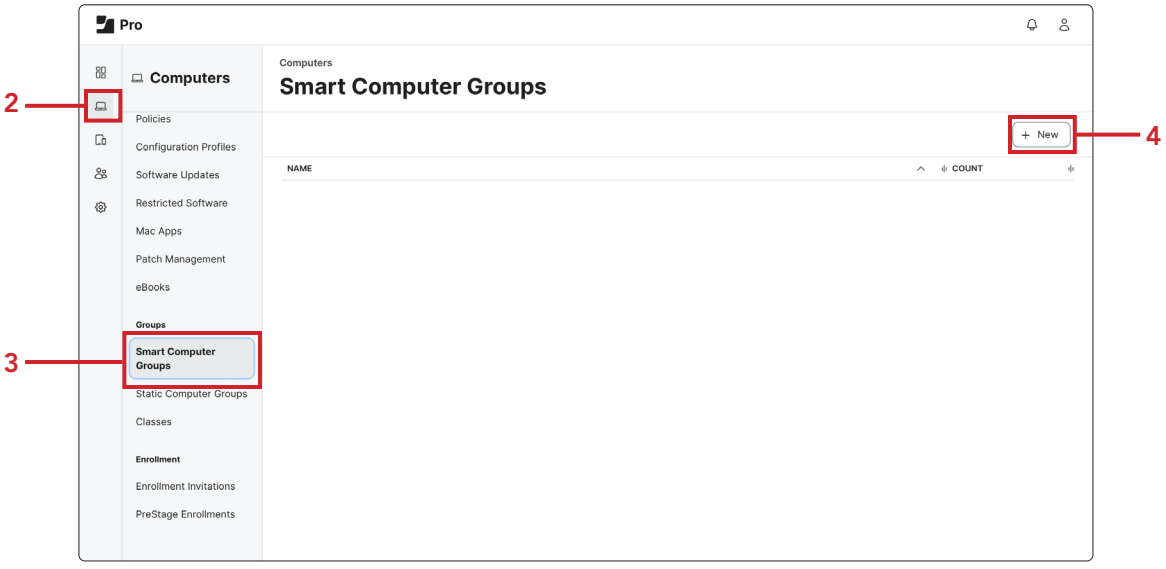
- Administrative access to your Jamf Pro server.

In this section, we will create a smart computer group in Jamf Pro to find all Mac computers running macOS 14.5 or later. While macOS 13 supports Platform SSO, it is recommended to use macOS 14.5 or later to leverage the latest enhancements and features. We will use this smart computer group as a scope to install the Intune Company Portal application in a later section of this guide.

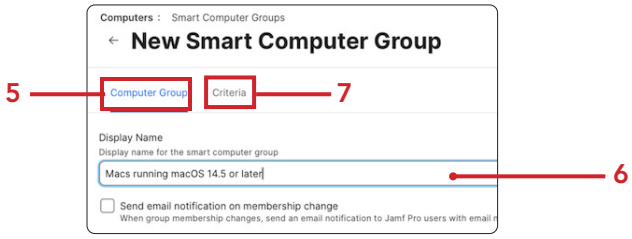
1. Log into your Jamf Pro server with administrative credentials.



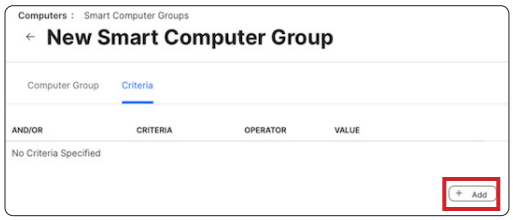
2. Select Computers.
3. Smart Computer Groups.
4. Click New.



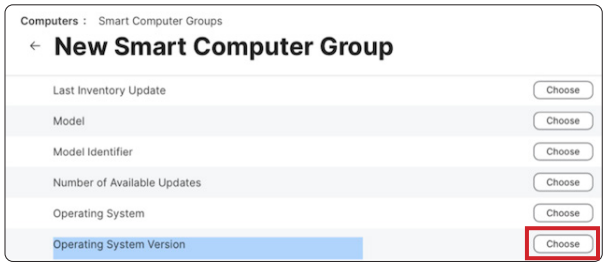
5. Click Computer Group if not already selected.
6. Enter Macs running macOS 14.5 or later for the Display Name.
7. Click Criteria.



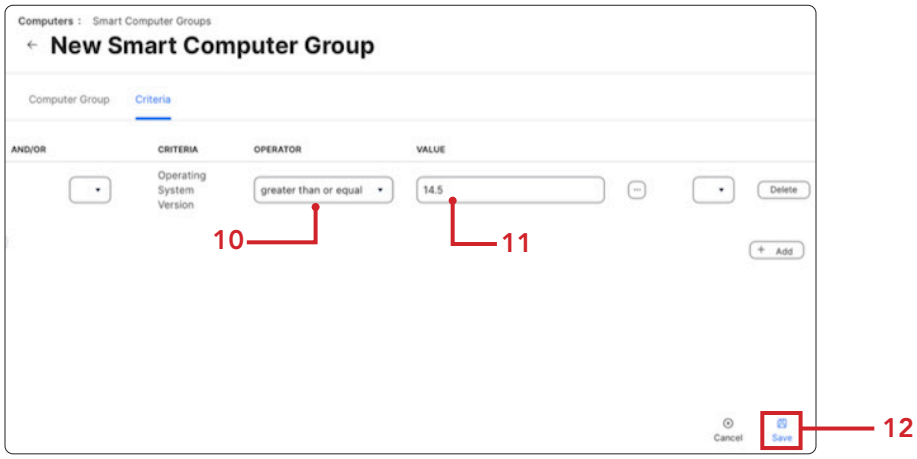
8. Click Add.



9. Select Choose for Operating System Version.

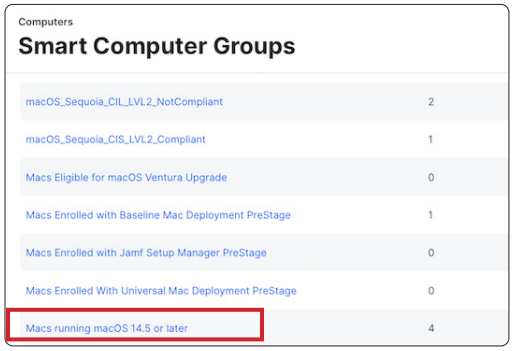


10. Select greater than or equal to for the Operator.
11. Enter 14.5 for the Value.
12. Click Save.



13. Click Previous.

14. Confirm the smart computer group named Macs running 14.5 or later shows up in the list.



This completes this section. In the next section, we will create configuration profiles in Jamf Pro to manage background notifications, Microsoft messages, and Microsoft PSSO settings.

Section 3: Creating Configuration Profiles in Jamf Pro

What You'll Need:
Learn what hardware, software, and information you'll need to complete the tutorials in this section.

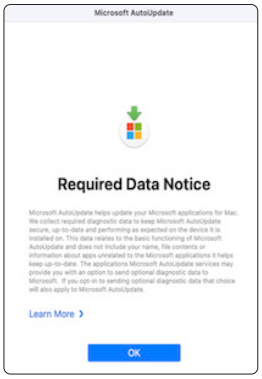
Hardware and Software:
Requirements for following along with this section:

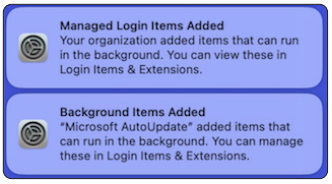
- Administrative access to your Jamf Pro server
- Download the customPSSO.plist:
  https://hcsonline.com/images/files/customPSSO.plist.zip

In this section, we will create the following configuration profiles in Jamf Pro:

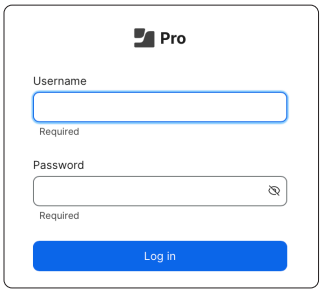
- Managed Background Item Notifications
- Managed Microsoft Messages
- Microsoft Platform SSO Extension

The Managed Background Item Notifications and Managed Microsoft Messages configuration profiles control the messages shown below so end users won't need to take action or make decisions based on them.

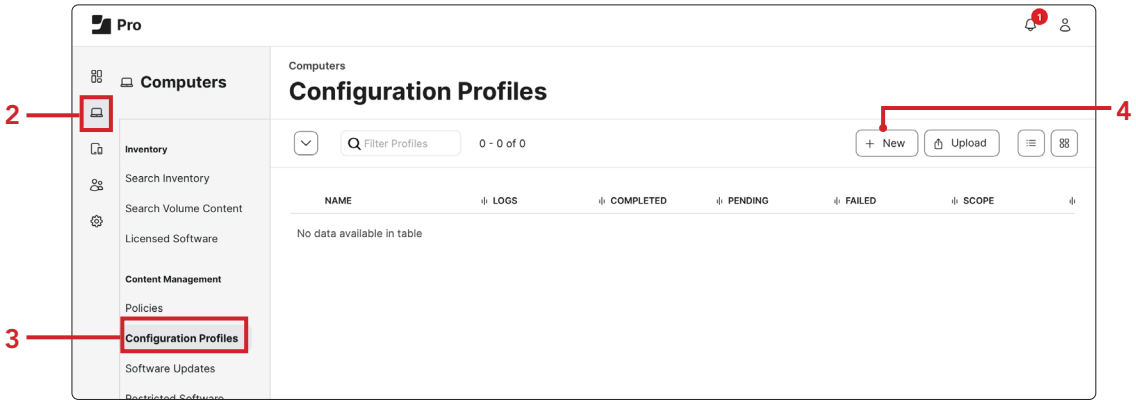




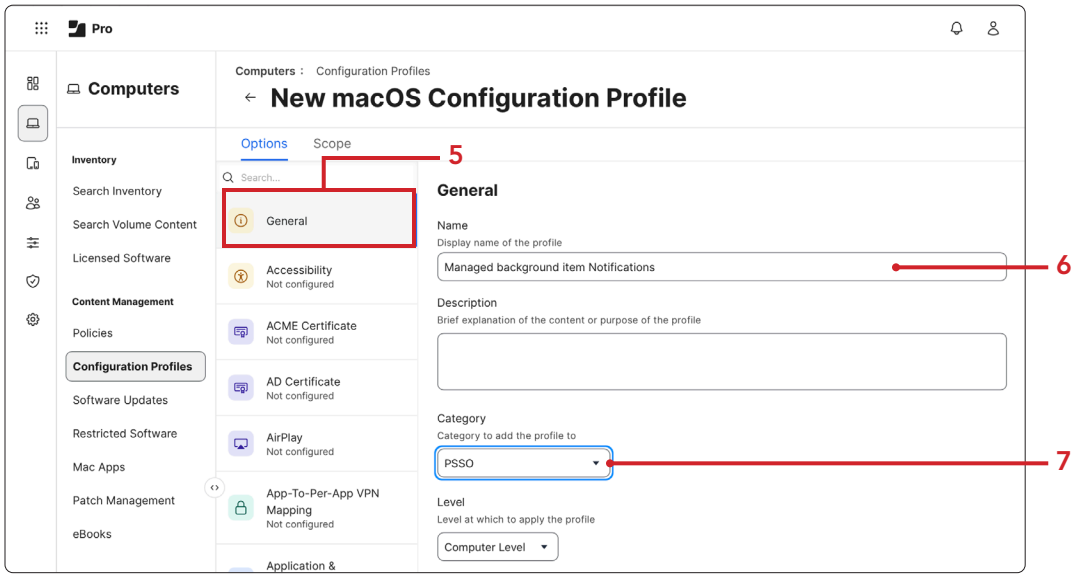
1. If necessary, Log into your Jamf Pro server with administrative credentials.



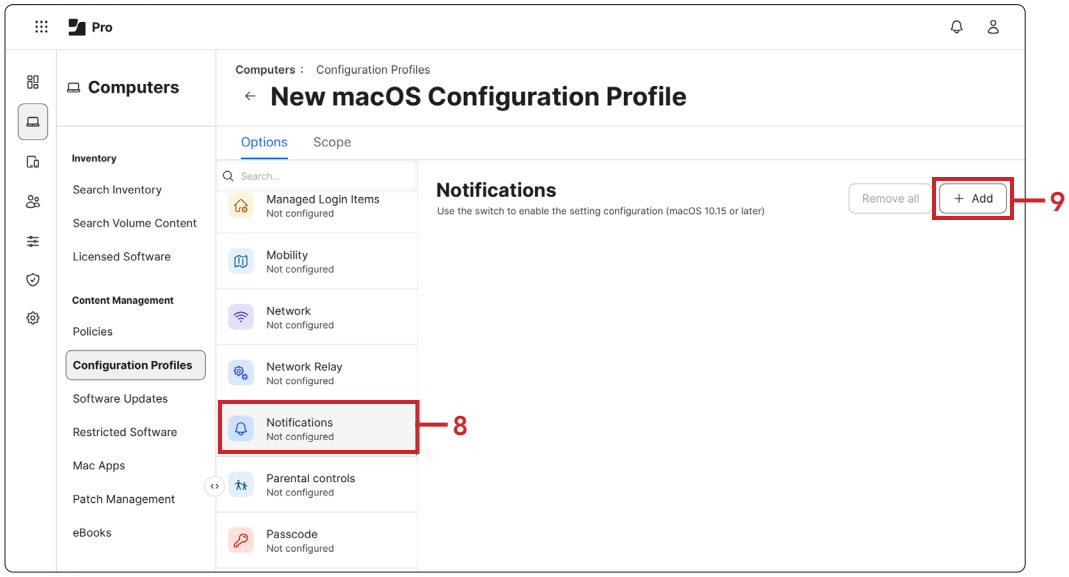
2. Click Computers.
3. Click Configuration Profiles.
4. Click New.



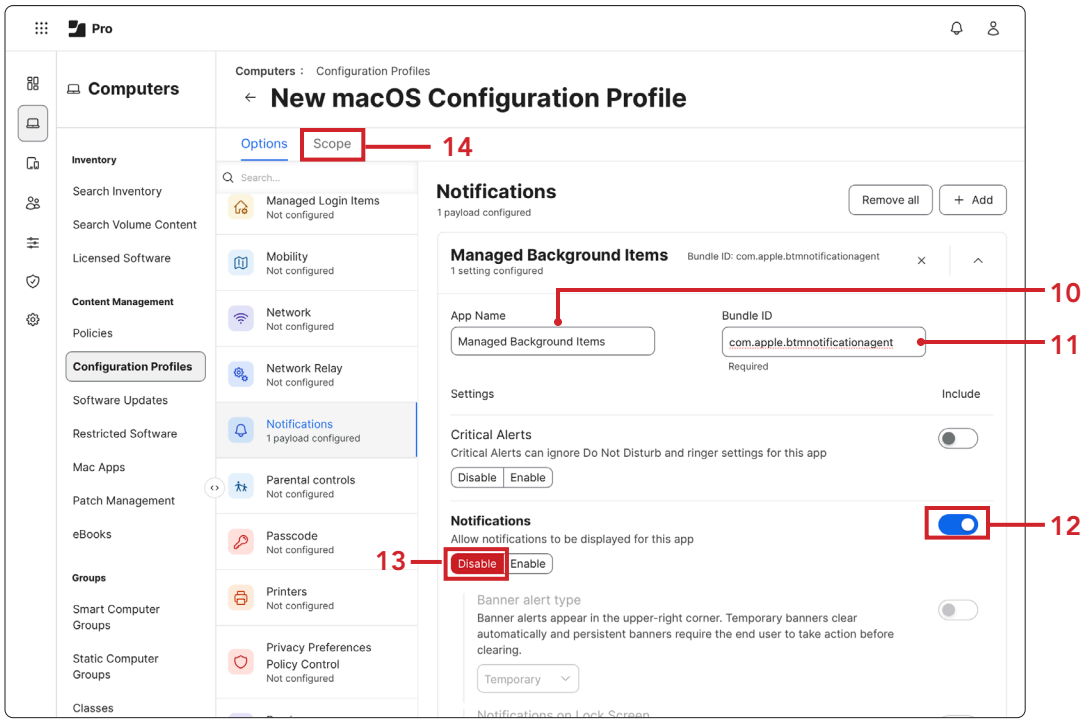
5. Click General, if not already selected.
6. Enter **Managed background item Notifications** for the Name.
7. Select a category of your choosing. This guide will use PSSO



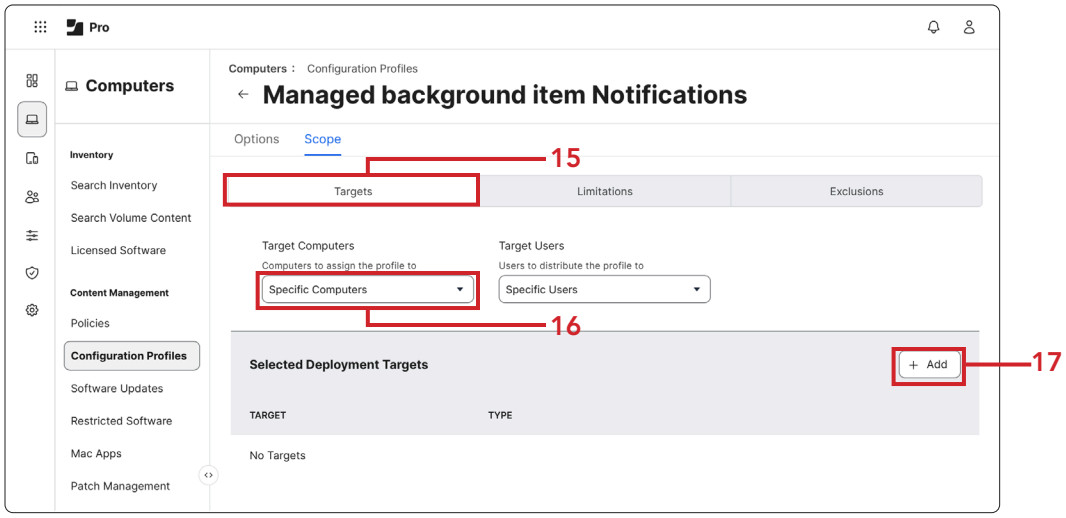
8. Scroll down and select Notifications.
9. Click Add (+).



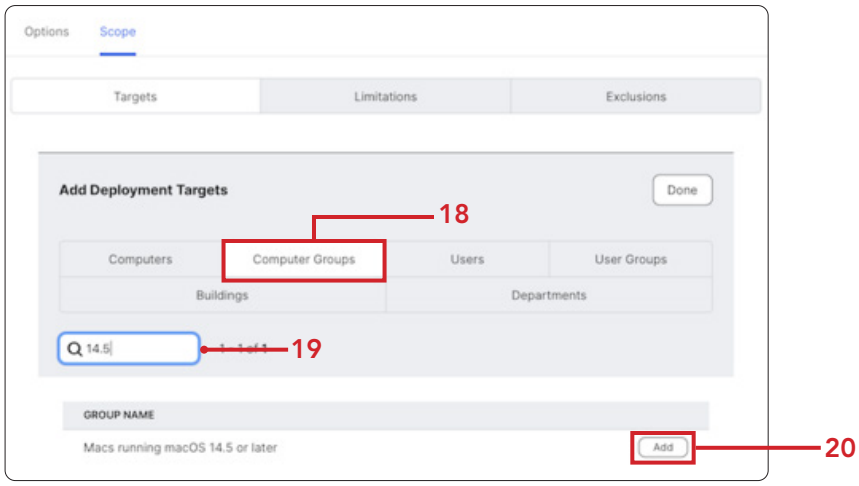
10. Enter **Managed Background Items** for the App Name.
11. Enter **com.apple.btmnotificationagent** for the Bundle ID.
12. Enable Notifications.
13. Select Disable.
14. Click Scope



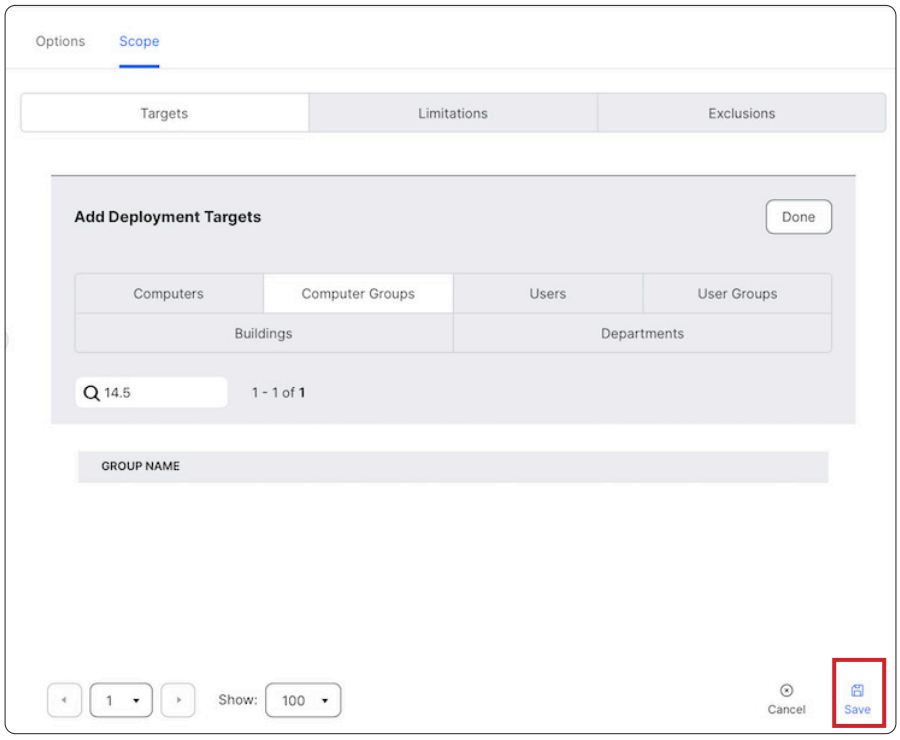
15. Click Targets.
16. Select Specific Computers.
17. Click Add (+).



18. Click Computer Groups.
19. Enter **14.5** in the search field.
20. Click Add for Macs running macOS 14.5 or later.

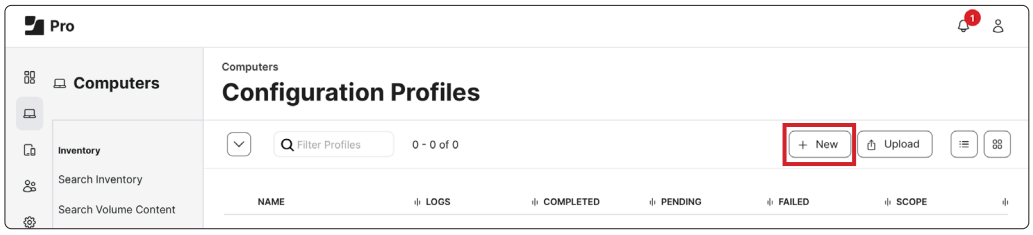


21. Click Save.

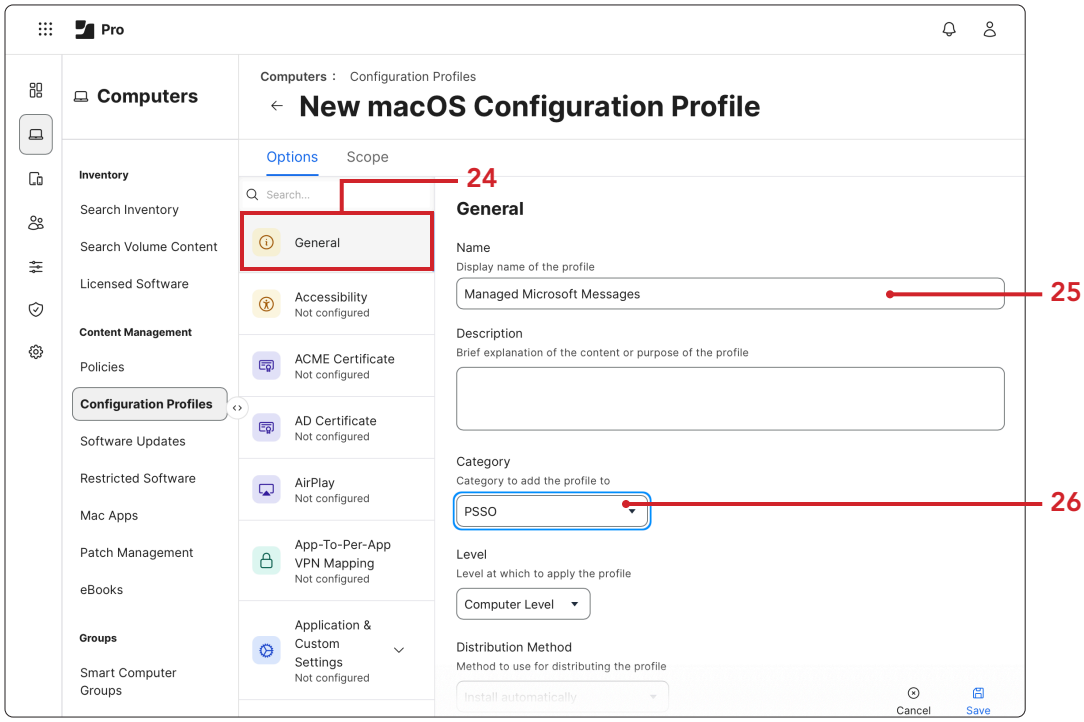


22. Click Previous (←).

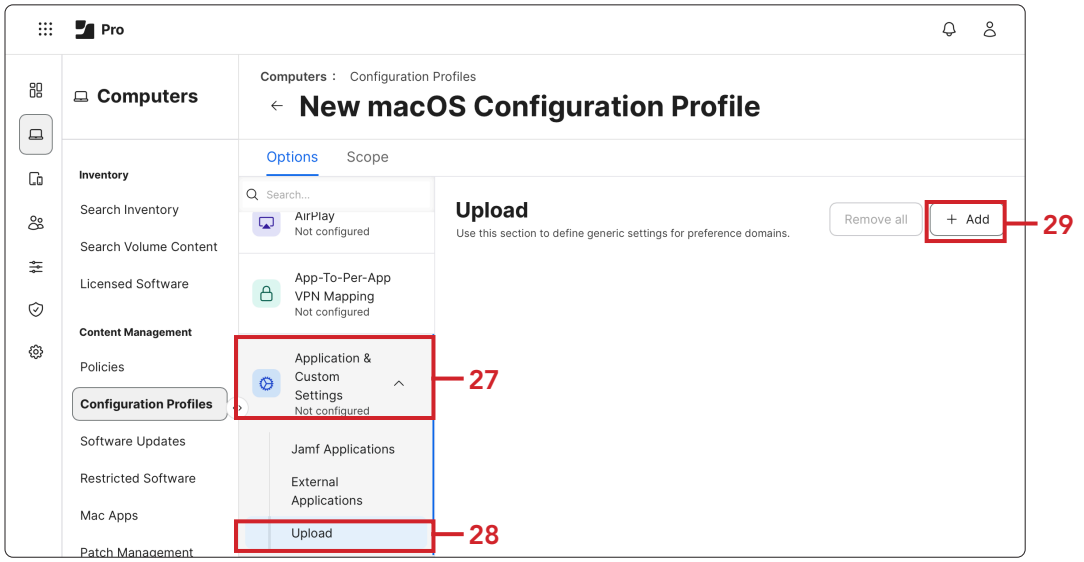
23. Click New.



24. Click General if it's not already selected.
25. Enter **Managed Microsoft Messages** for the Name.
26. Select a category of your choosing. This guide will use PSSO.



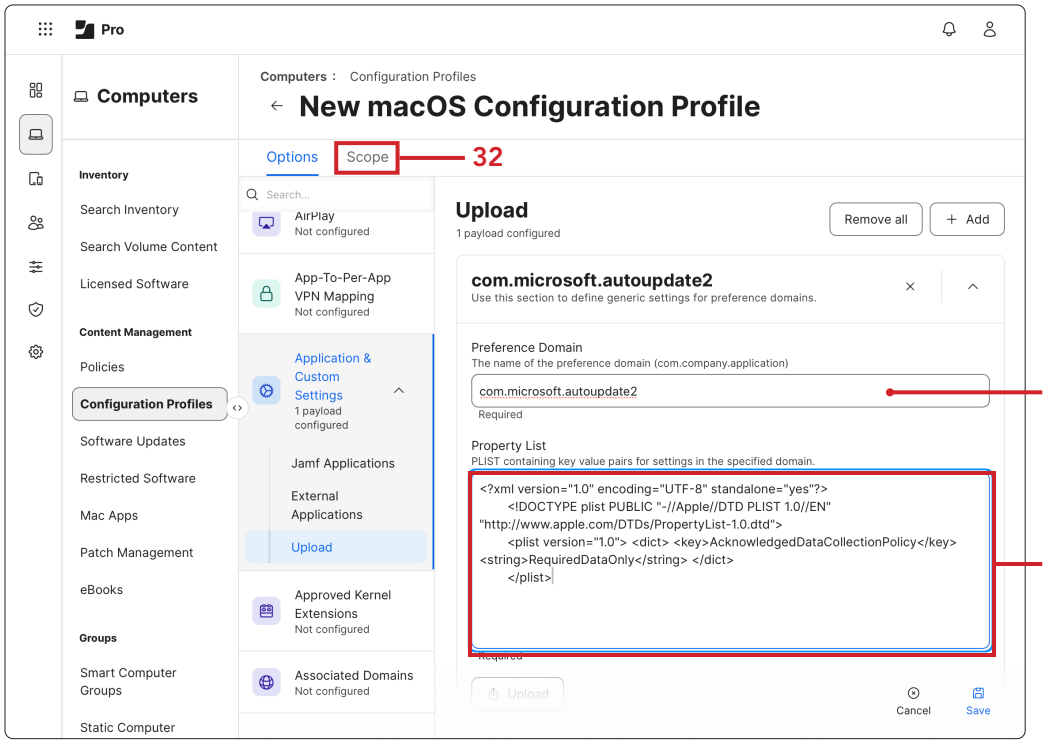
27. Scroll down and click Application & Custom Settings.
28. Click Upload.
29. Click Add (+).



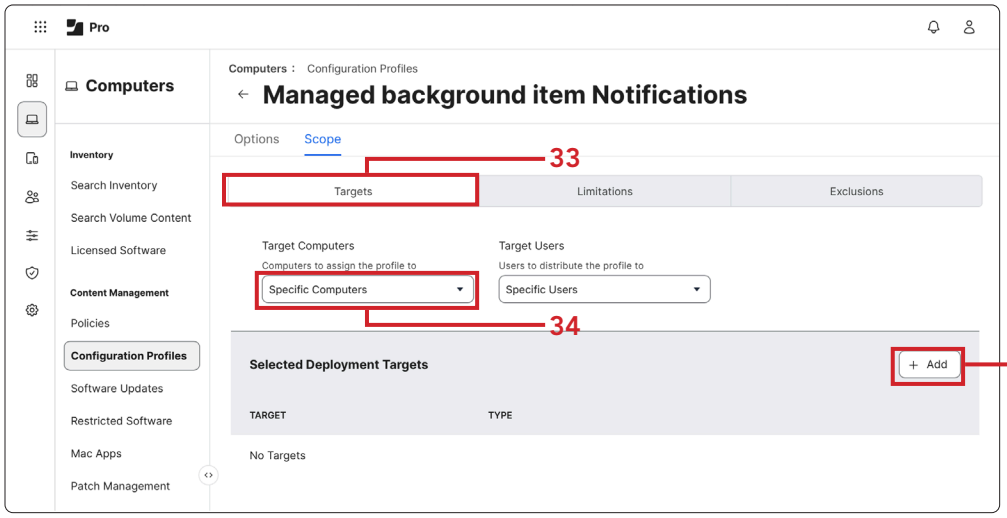
30. Enter **com.microsoft.autoupdate2** for the name of the Preference Domain.
31. Enter the XML below Into the Property List field.

```
<?xml version="1.0" encoding="UTF-8" standalone="yes"?>

<!DOCTYPE plist PUBLIC "-//Apple//DTD PLIST 1.0//EN" "http://www.apple.com/
DTDs/PropertyList-1.0.dtd">

<plist version="1.0"> <dict> <key>AcknowledgedDataCollectionPolicy</key>
<string>RequiredDataOnly</string> </dict>

</plist>
```

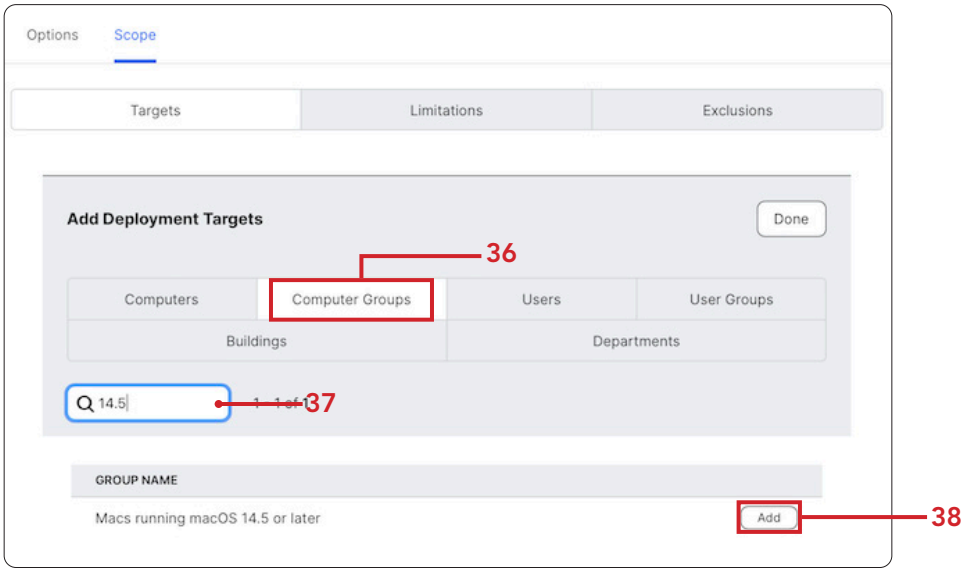
32. Click Scope.



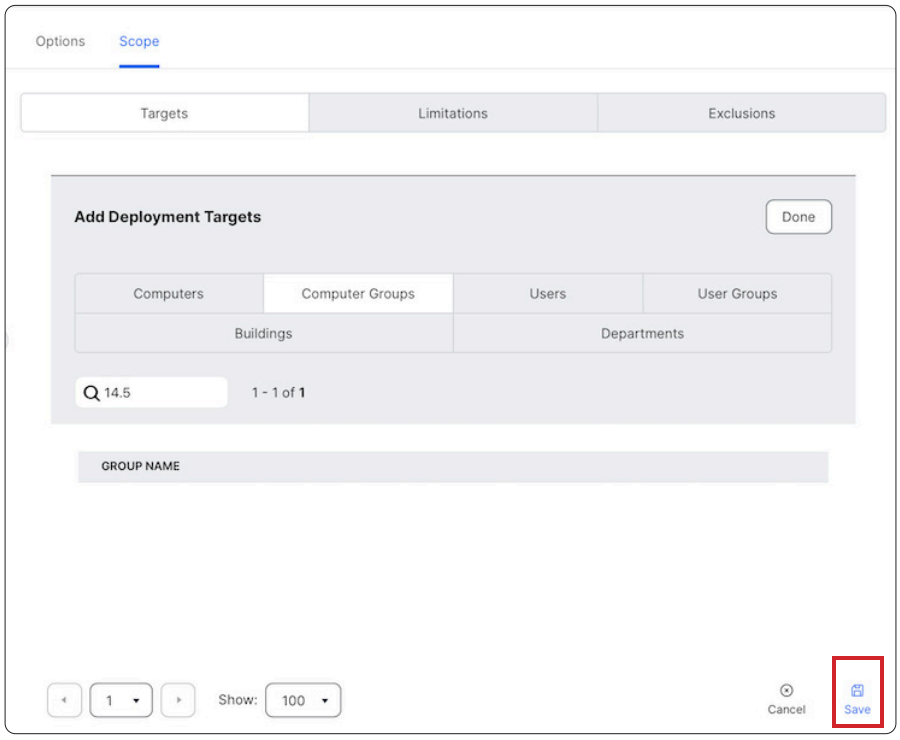
33. Click Targets.
34. Select Specific Computers.
35. Click Add (+).



36. Click Computer Groups.
37. Enter **14.5** in the search field.
38. Click Add for Macs running macOS 14.5 or later.

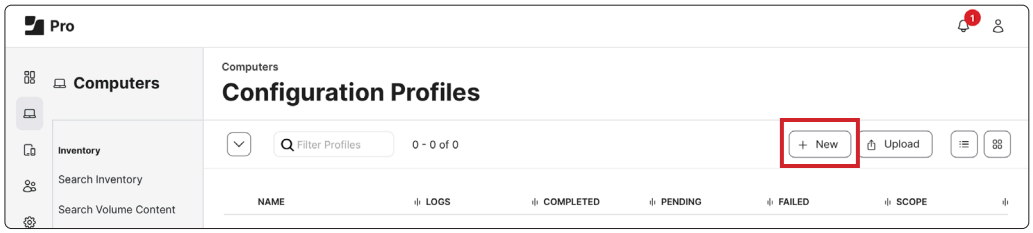


39. Click Save.

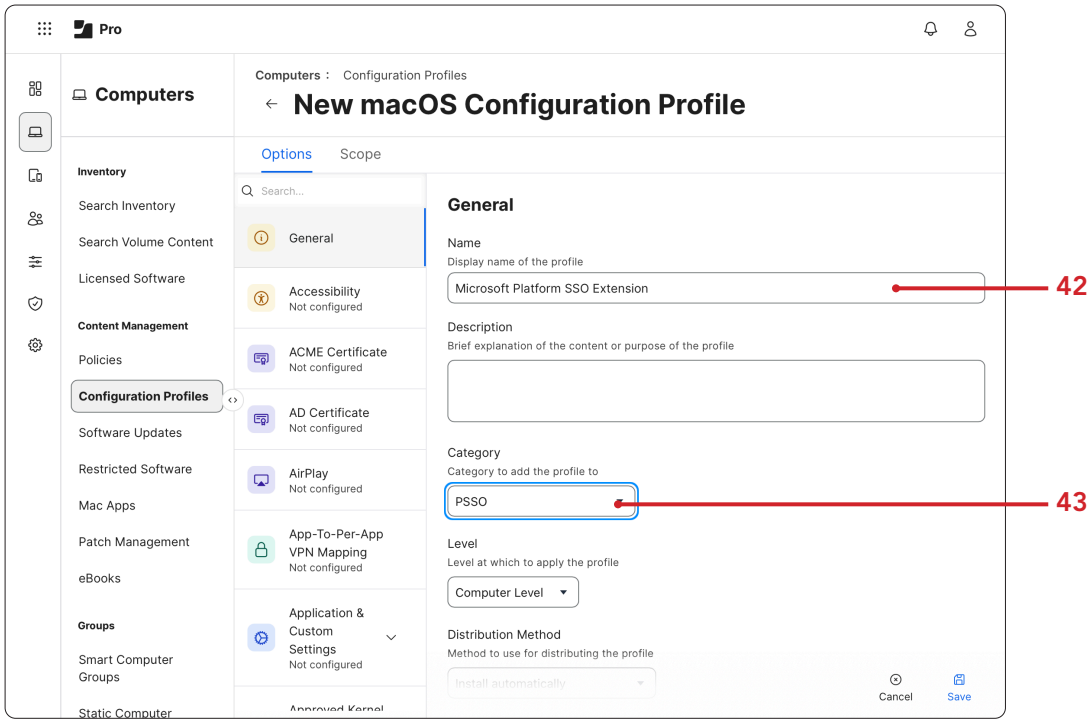


40. Click Previous (←).

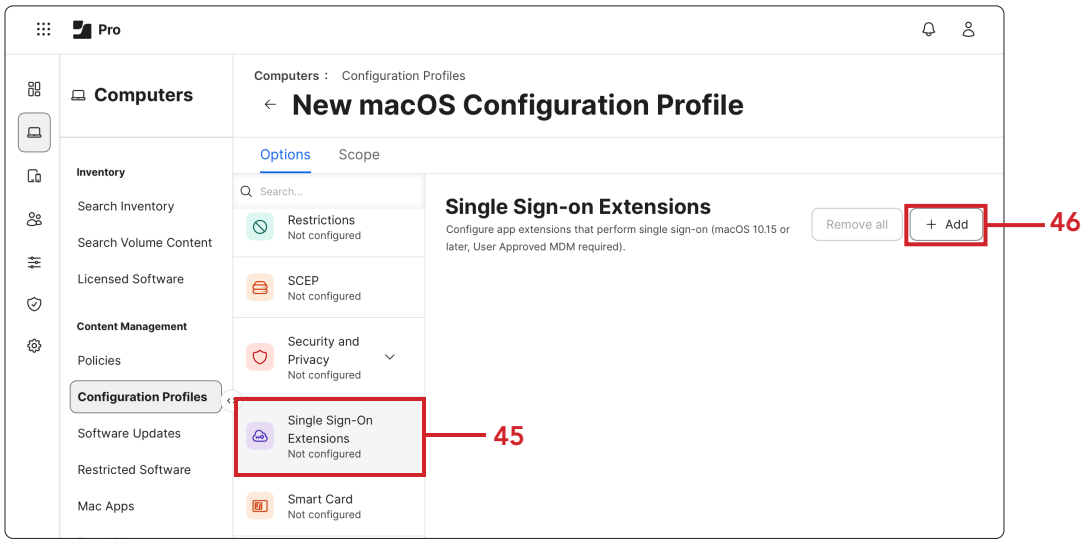
41. Click New.



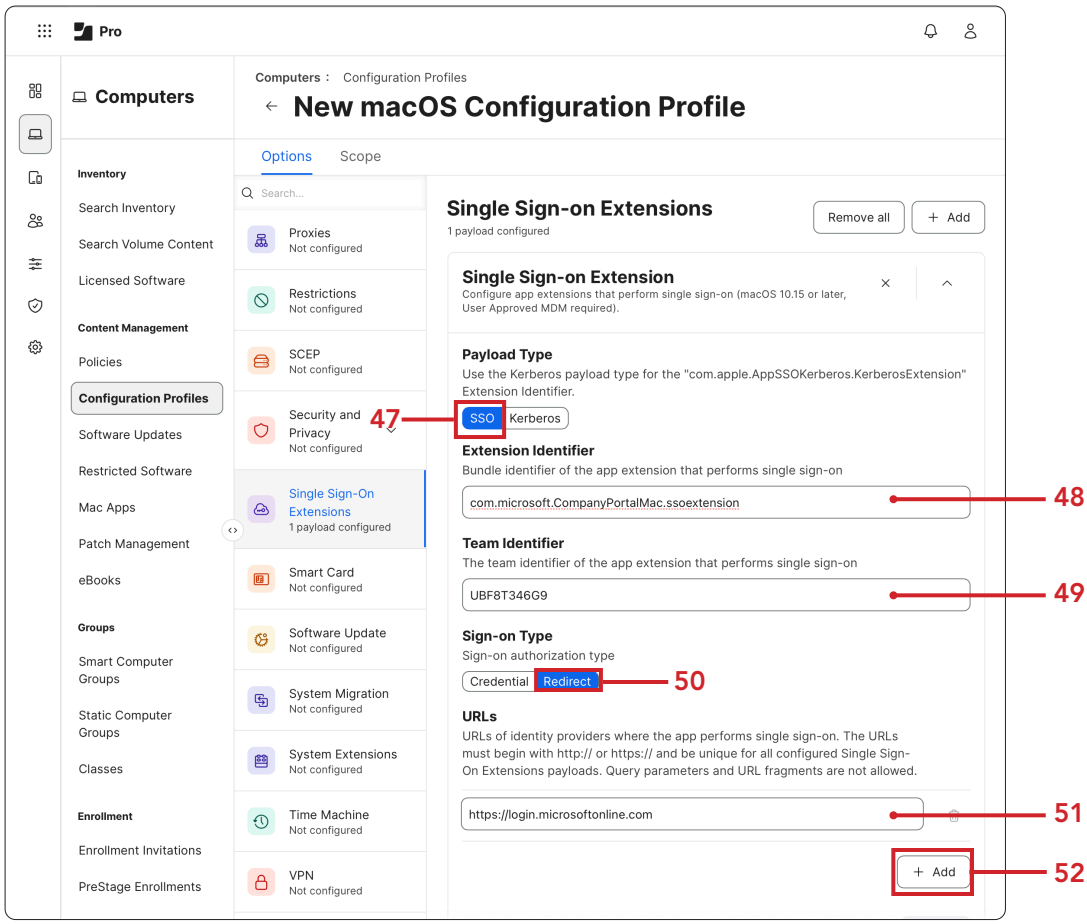
42. Enter **Microsoft Platform SSO Extension** for the Name.
43. Select a category of your choosing. This guide will use PSSO.
44. Leave the rest of the settings at their defaults.



45. Scroll down Select Single Sign-On Extension payload.
46. Click Add.



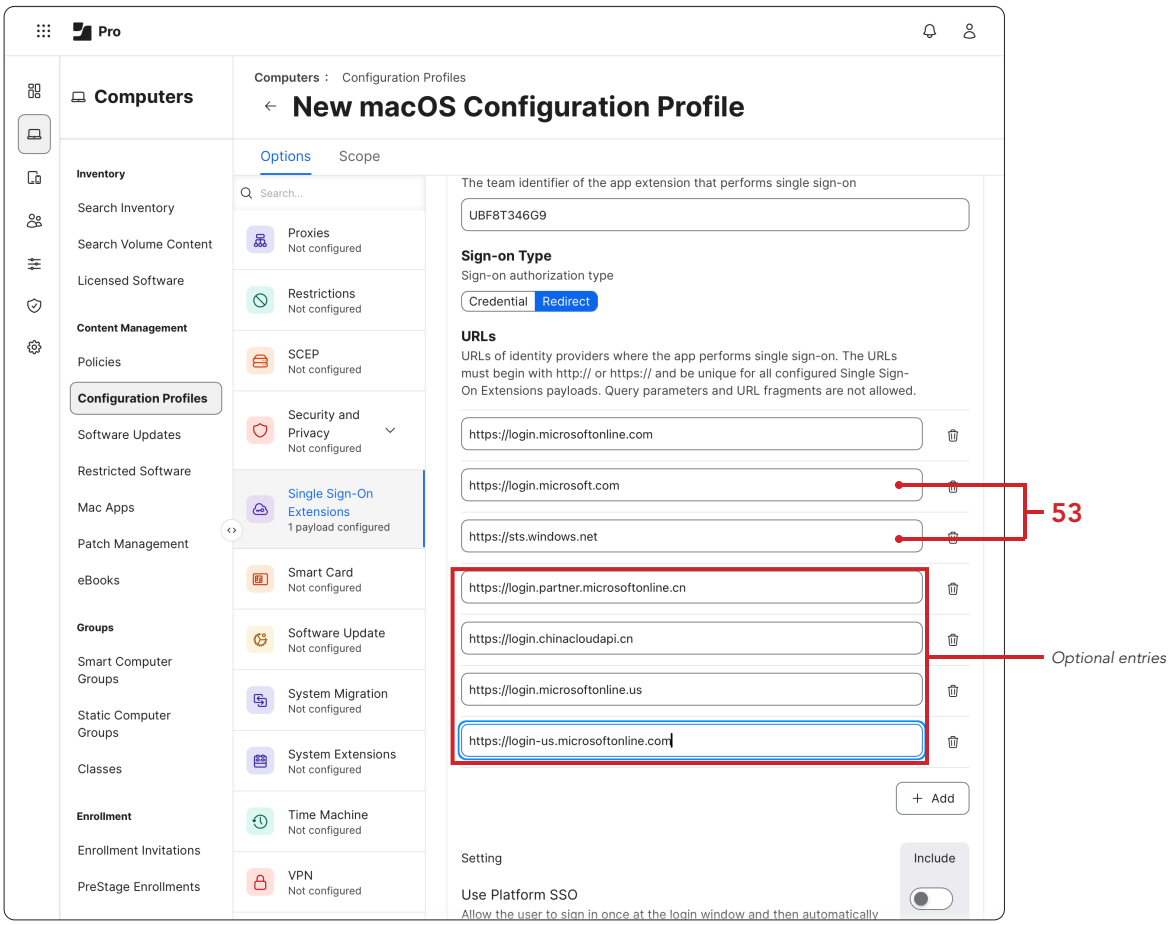
47. Select SSO for the Payload Type.
48. Enter **com.microsoft.CompanyPortalMac.ssoextensio**n for Extension Identifier
49. Enter **UBF8T346G9** for Team Identifier.
50. Select Redirect.
51. Enter **https://login.microsoftonline.com** for the URL.
52. Click Add.



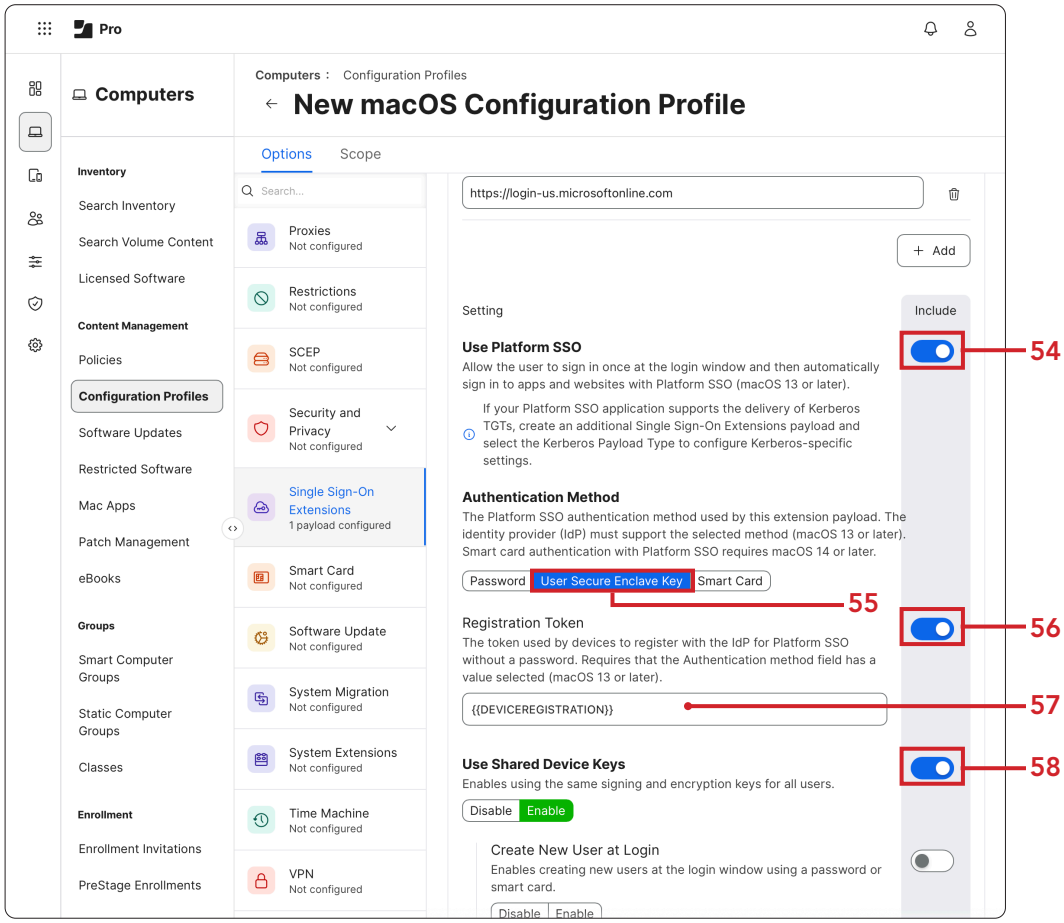
53. Enter the next two URLs:
    - https://login.microsoft.com
    - https://sts.windows.net

These URL's are optional and only required if you're using sovereign cloud domains: This guide will add them.

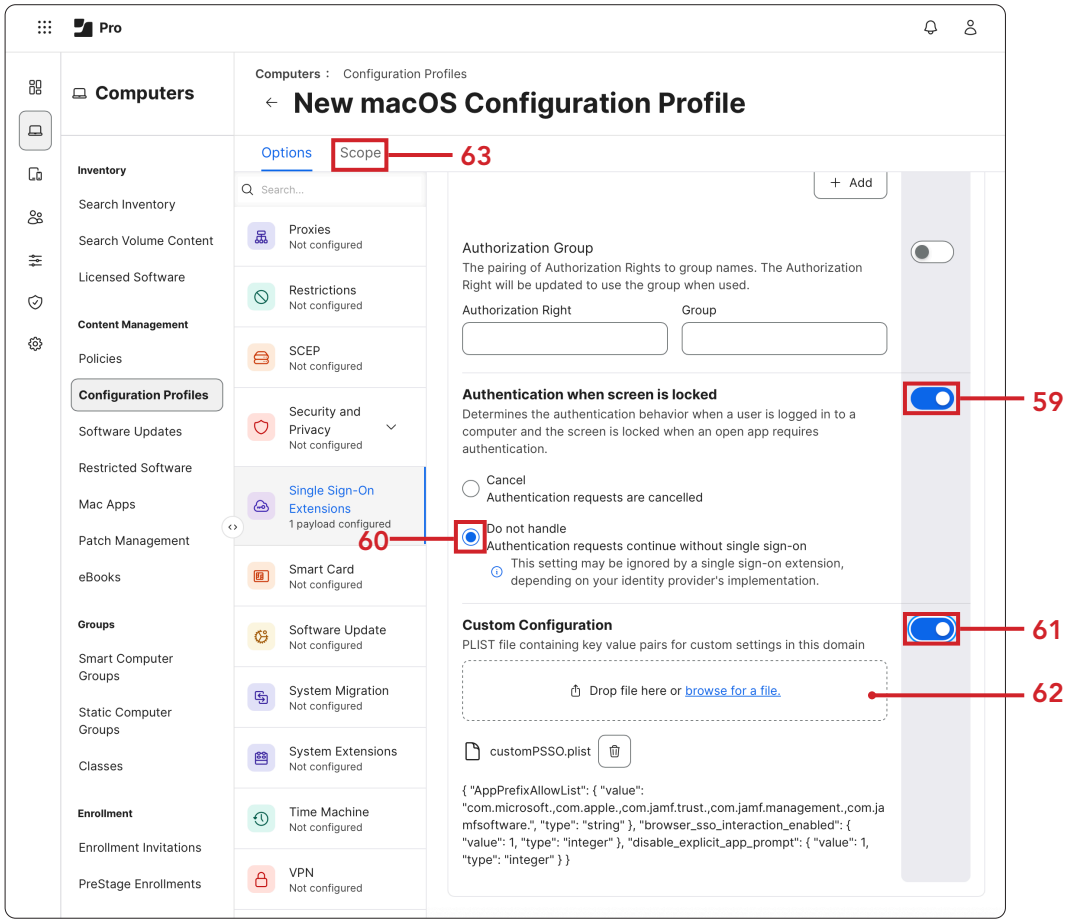
- https://login.partner.microsoftonline.cn
- https://login.chinacloudapi.cn
- https://login.microsoftonline.us
- https://login-us.microsoftonline.com



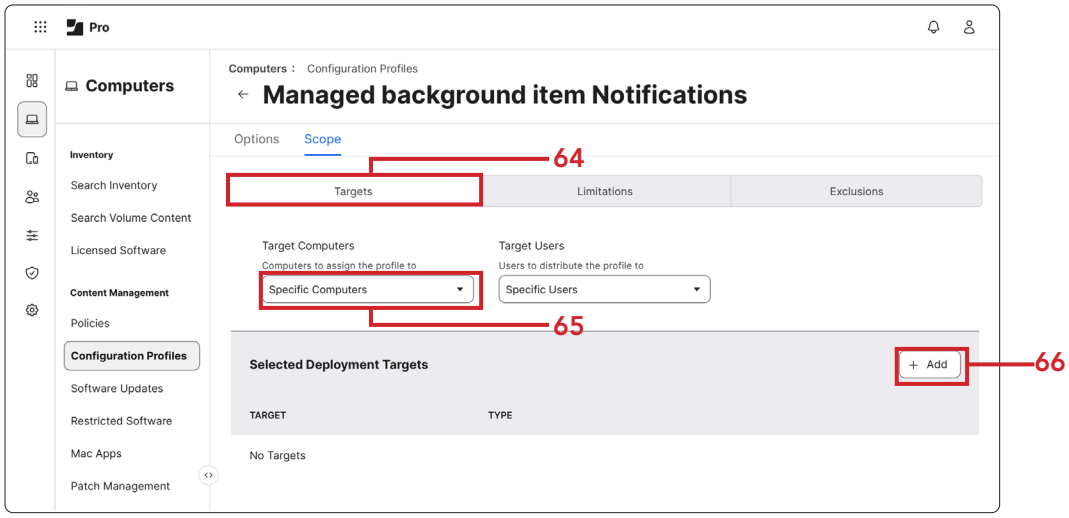
54. Scroll Down and Enable Use Platform SSO.
55. Select User Secure Enclave Key under Authentication Method.
56. Enable Registration Token.
57. Enter the following in the field {{DEVICEREGISTRATION}}
58. Enable Use Shared Device Keys.



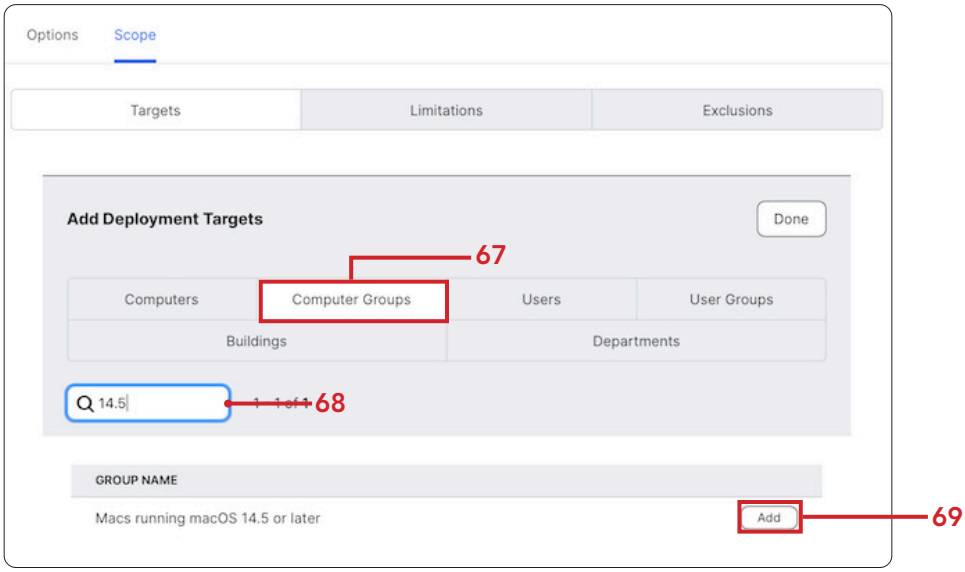
59. Scroll down and enable Authentication when screen is locked.
60. Select Do not handle.
61. Enable Custom Configuration.
62. Upload the file named customPSSO.plist (This was download at the beginning of this section)
63. Click Scope.



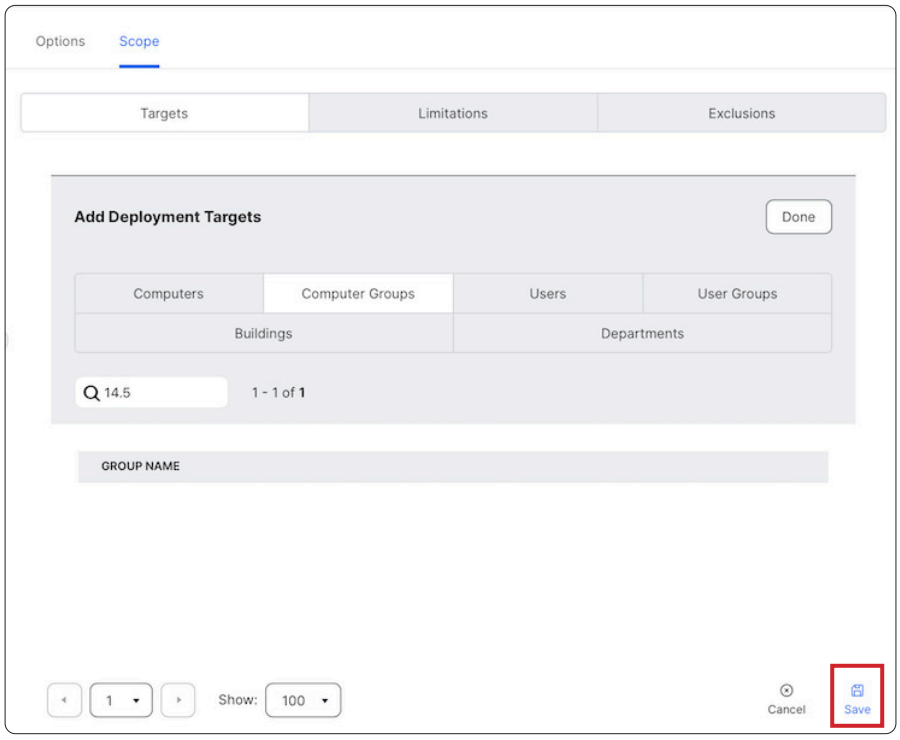
64. Click Targets.
65. Select Specific Computers.
66. Click Add (+).



67. Click Computer Groups.
68. Enter **14.5** in the search field.
69. Click Add for Macs running macOS 14.5 or later.

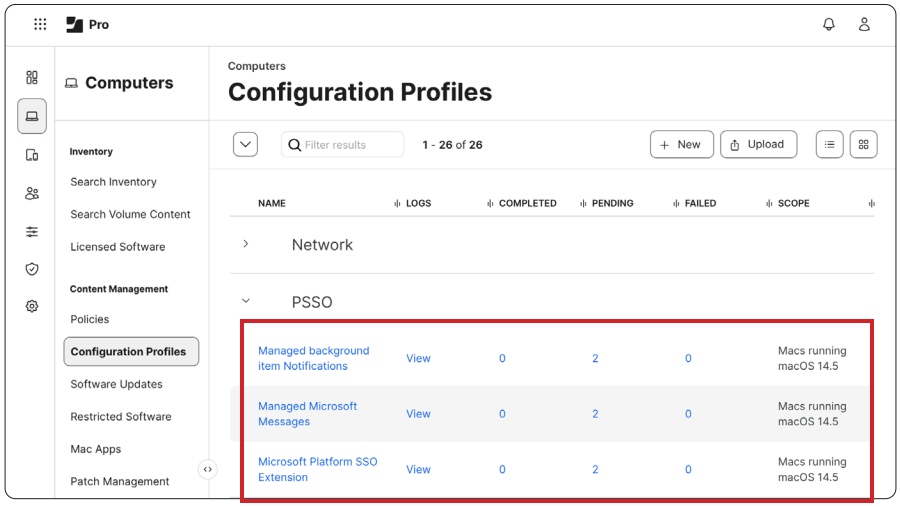


70. Click Save.



71. Click Previous (←).

72. Confirm all three configuration profiles were created.



This completes this section. In the next section, we will deploy the Microsoft Intune Company Portal application using the Jamf app catalog.

Section 4: Deploying Microsoft Intune Company Portal with Jamf Pro

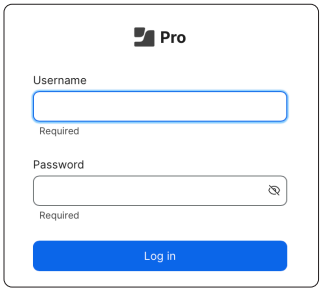
What You'll Need:
Learn what hardware, software, and information you'll need to complete the tutorials in this section.

Hardware and Software:
Requirements for following along with this section:

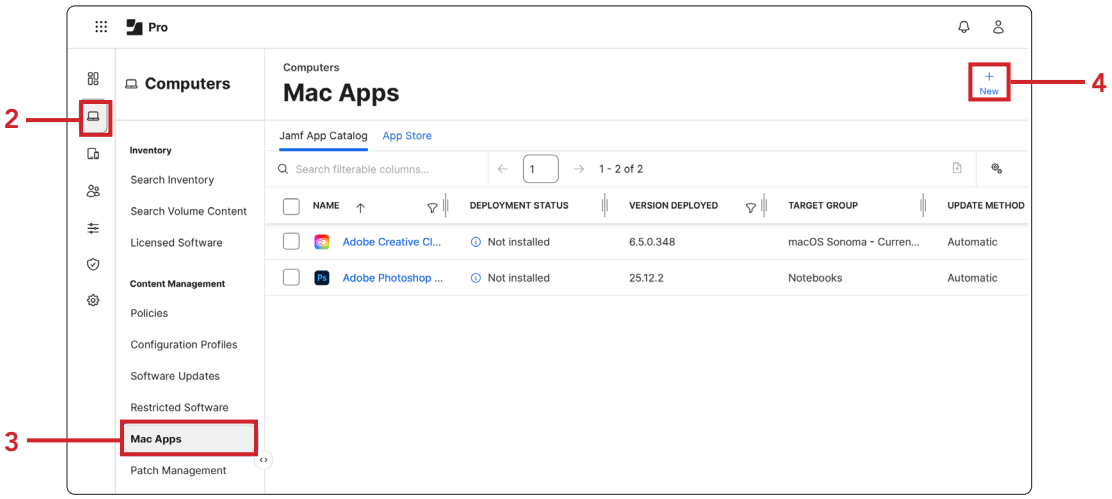
- Administrative access to your Jamf Pro server.

NOTE: Users in Microsoft Entra ID must have a strong authentication method, such as MFA, Federated MFA, FIDO, or a Temporary Access Pass. Additionally, they must have permission to join devices to Microsoft Entra ID. Ensure that this setting is not blocked in Microsoft Entra ID as discussed in section one of this guide.

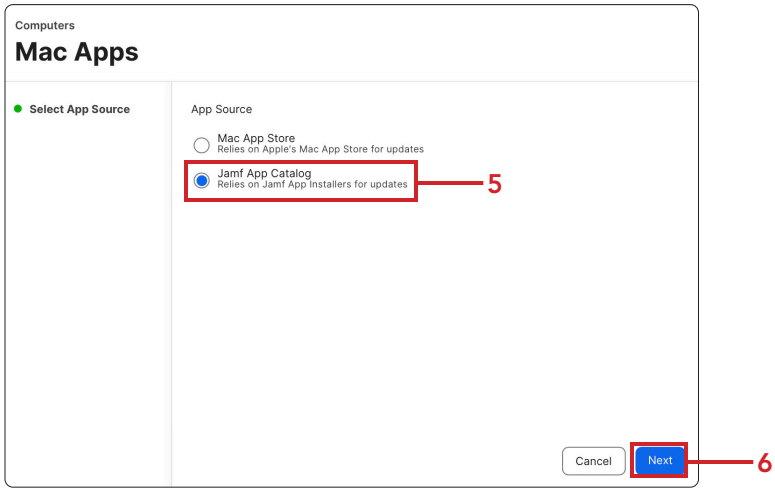
1. If necessary, Log into your Jamf Pro server with administrative credentials.



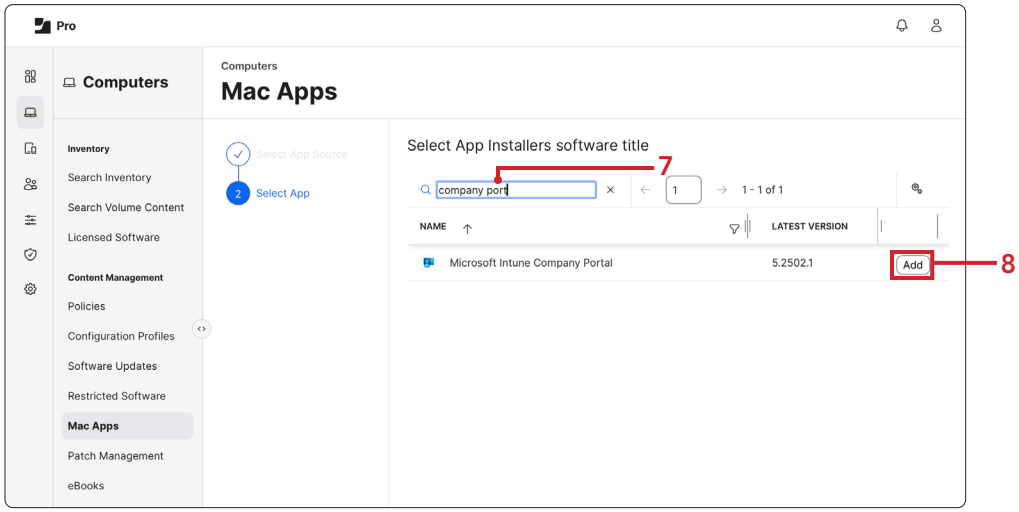
2. Click Computers.
3. Mac Apps.
4. Click New.



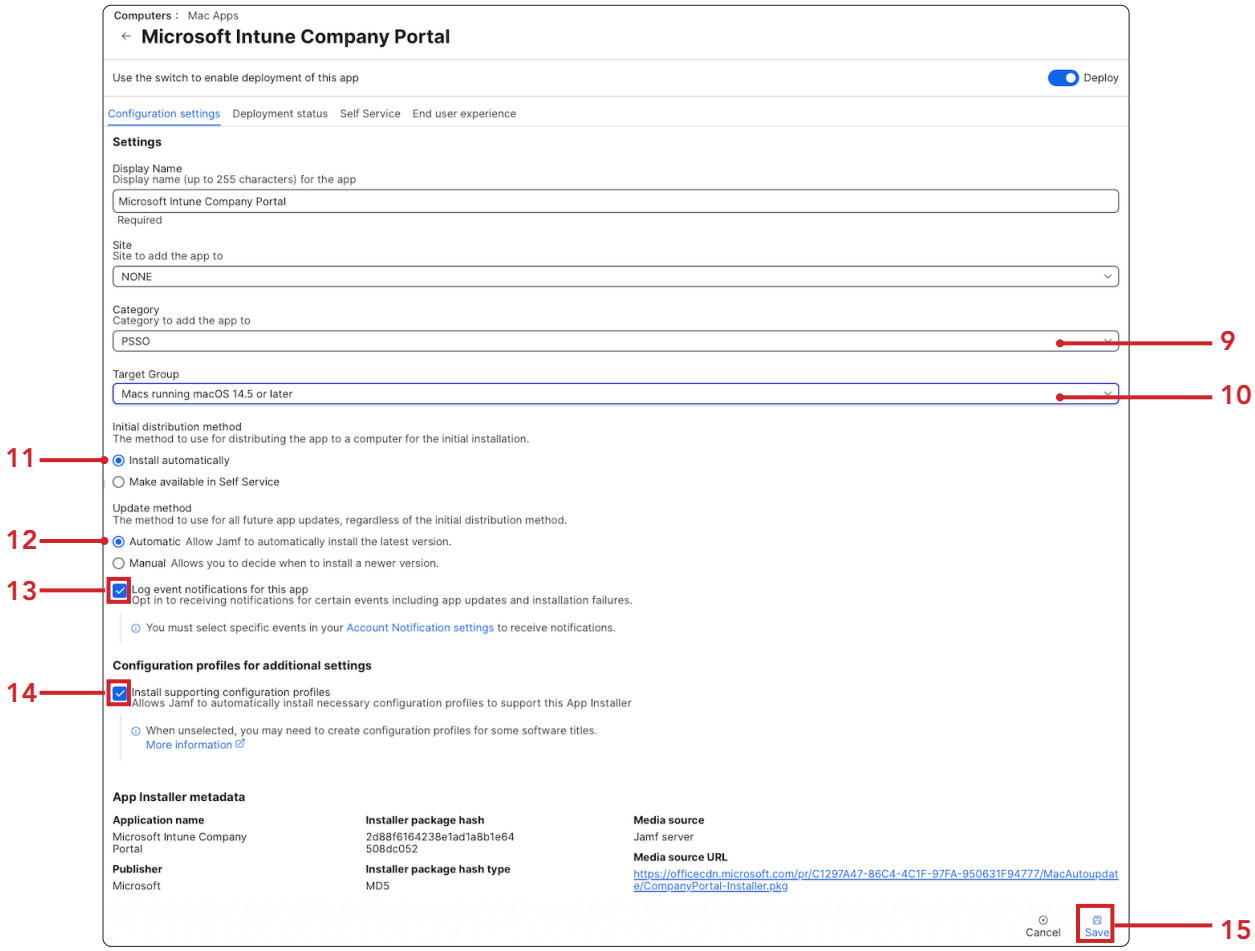
5. Select Jamf App Catalog.
6. Click Next.



7. In the search field, enter **company portal**.
8. Click Add.



9. Select a category of your choosing. This guide will use PSSO.
10. Select Macs running macOS 14.5 or later for the Target Group.
11. Select an install method that works for you. This guide will choose Install Automatically.
12. Select Automatic to allow Jamf to automatically install the latest version.
13. Select the checkbox for Log event notifications for this app.
14. Select the checkbox for Install supporting configuration profiles.
15. Click Save.



This completes this section. In the next section, we will register a Mac computer using Microsoft Intune Company Portal.

Section 5: Register a Mac using Microsoft Intune Company Portal App and Test Microsoft PSSO.

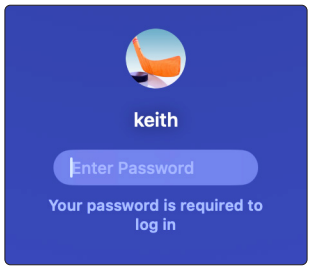
What You'll Need:
Learn what hardware, software, and information you'll need to complete the tutorials in this section.

Hardware and Software:
Requirements for following along with this section:

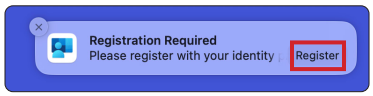
- A non production Mac computer running macOS 14.5 or later enrolled in Jamf Pro
- Google Chrome with the Microsoft single sign-on extension installed

In this section, we will register a Mac computer using the Microsoft Intune Company Portal App and test the Microsoft PSSO Extension by signing into Microsoft services using Safari and Google Chrome web browsers. This section will cover installing the Microsoft single sign-on extension for Google Chrome on versions prior to 136. Google Chrome version 136 added built in support for single sign-on. If you're using version 136, you can skip steps 25-31.

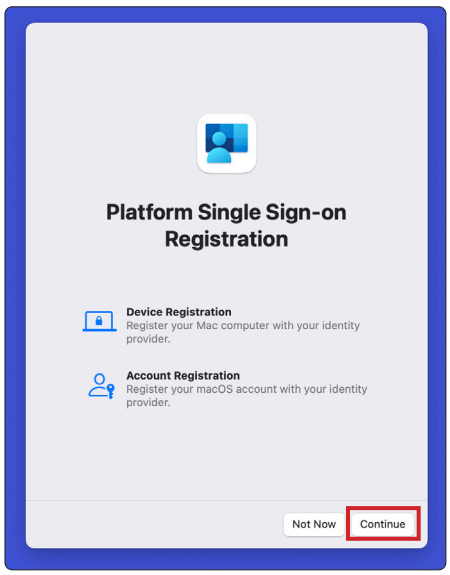
1. Log into your non production Mac computer.



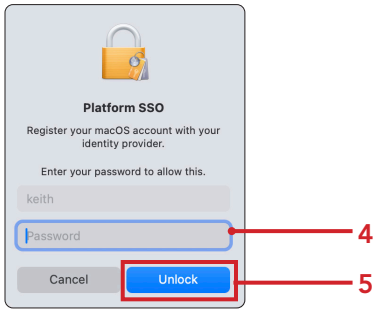
2. Confirm you get a Registration Required notification. Click Register.



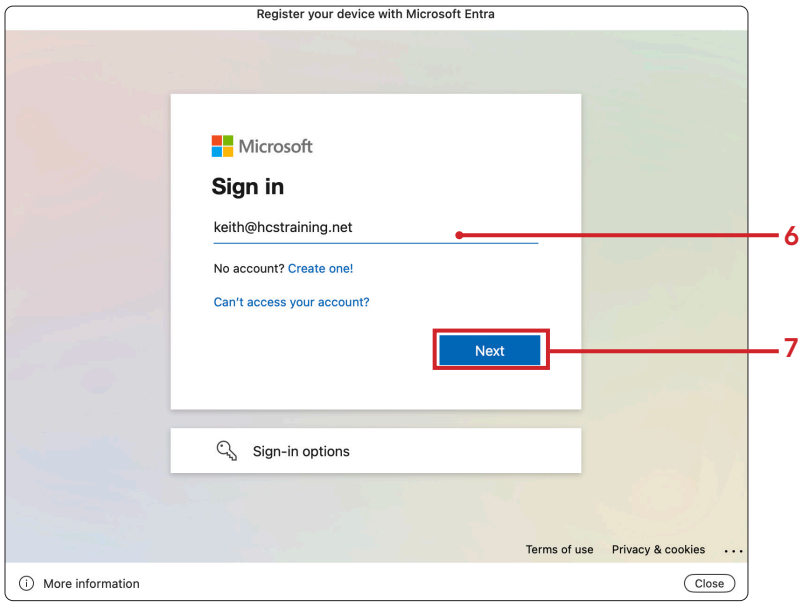
3. Click Continue.



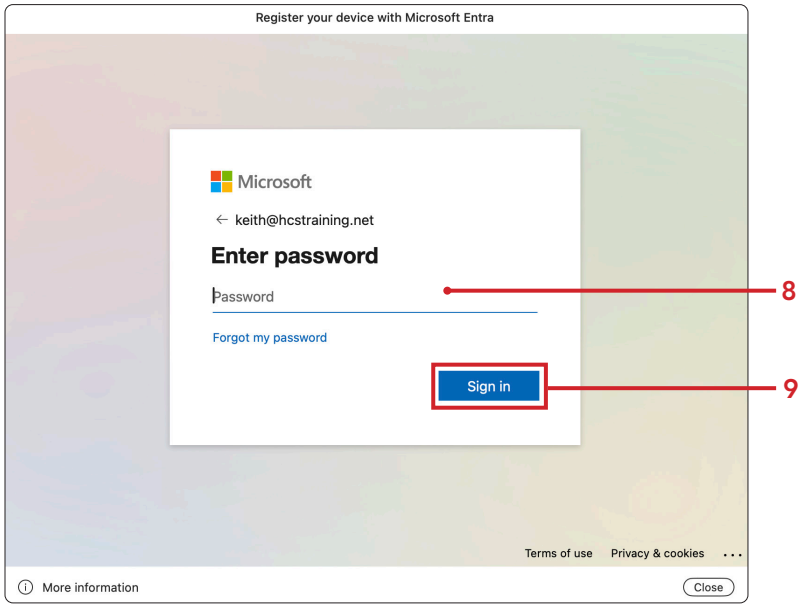
4. Enter your administrative credentials.
5. Click Unlock.



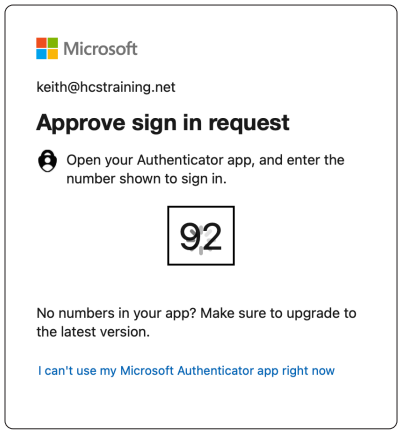
6. Enter your Microsoft Entra account.
7. Click Next.
   NOTE: Your sign in authentication steps may be different if you are using a passkey, security key., or Microsoft Authenticator.



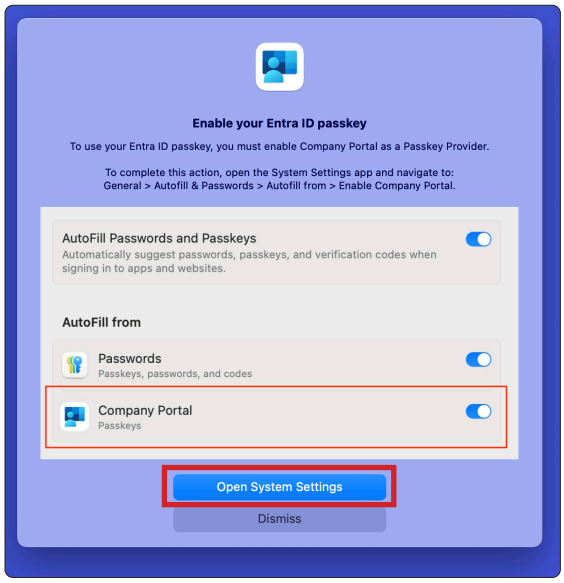
8. Enter your password.
9. Click Sign in.



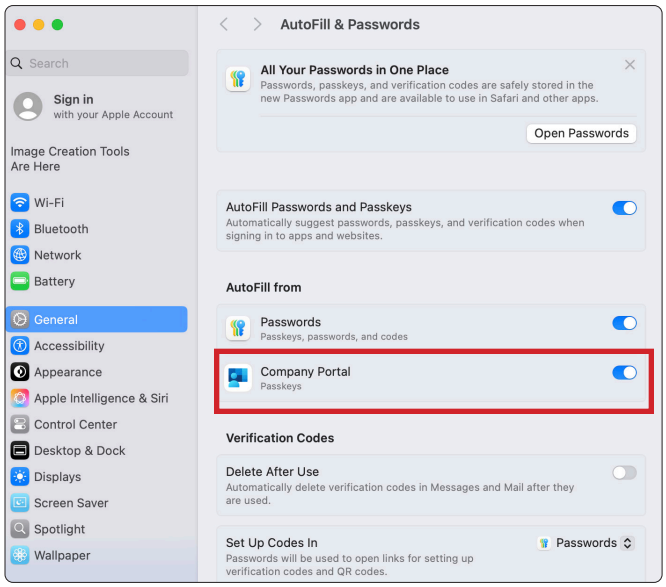
10. Enter the MFA code in your Microsoft Authenticator app.



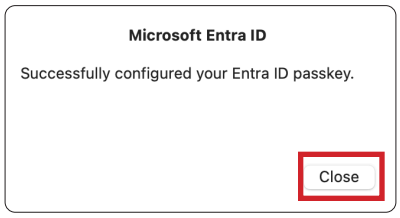
11. Click Open System Settings.



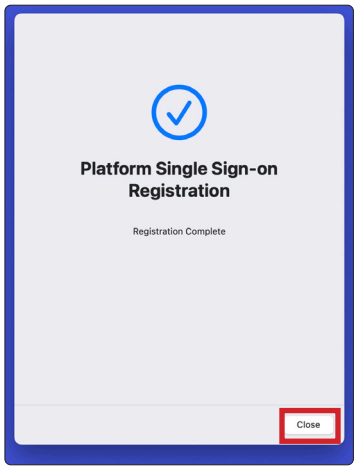
12. Enable Company Portal.



13. Click Close.



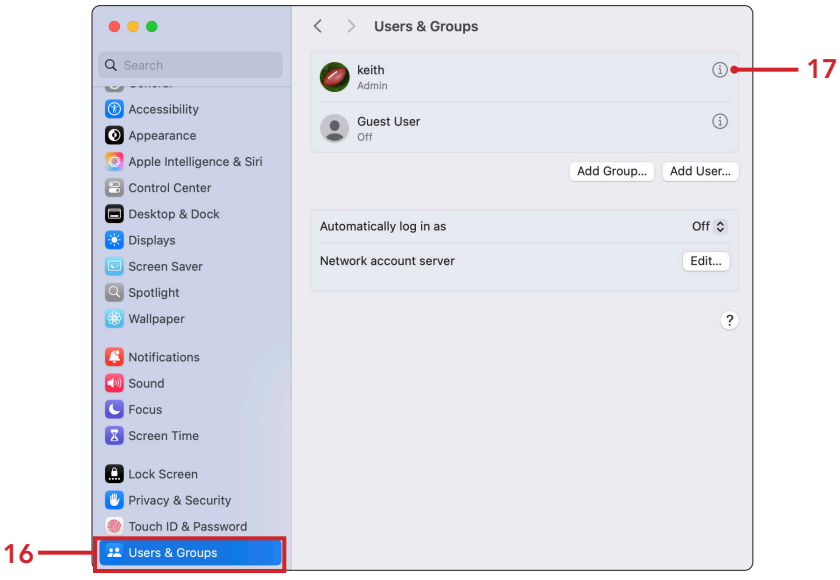
14. Click Close.



15. Let's check our registration and tokens. Open System Settings.

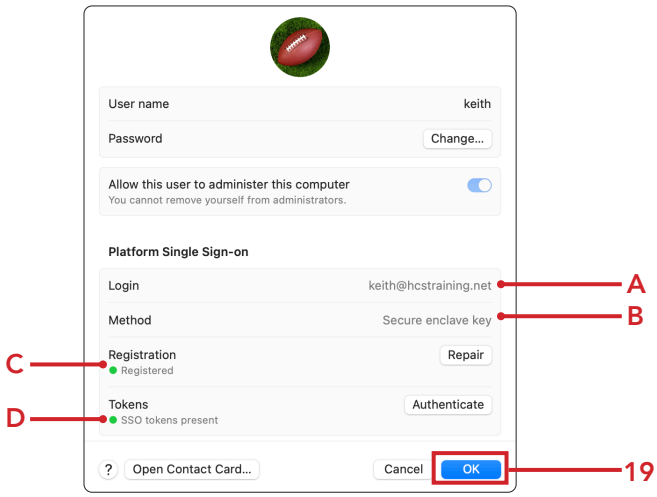
16. Click Users & Groups.

17. Click on info(ⓘ) next to your user name.

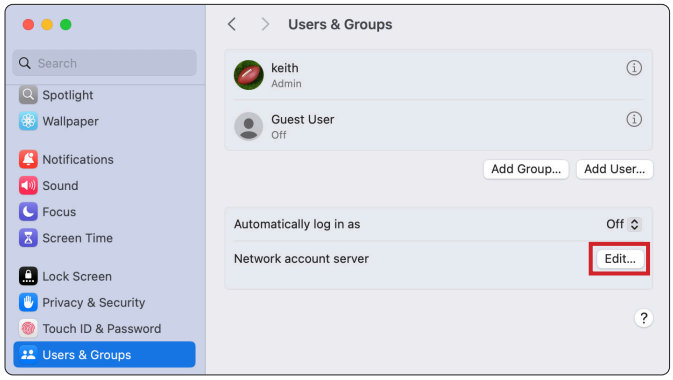


18. Look at the information in the Platform Single Sign-on section. Confirm the following:
    A. Login: Shows your user account in Microsoft Entra.
    B. Method: Secure Enclave.
    C. Registration: Shows as Registered.
    D. Tokens: SSO tokens are present.

19. Click OK.



20. Click Edit.

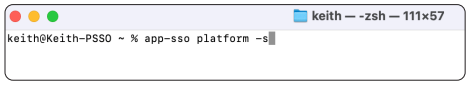


21. This will show the Mac SSO Extension as Registered. Click Done.

22. Open Terminal.app located in /Applications/Utilities.

23. Run the following command:

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



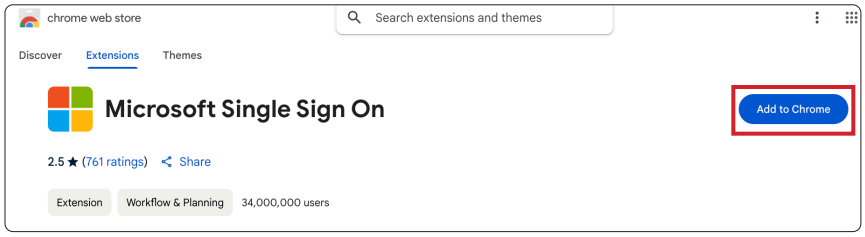
24. You will see a lot of information on the screen. Scroll to the bottom to view the SSO Token and Expiration information.

```
SSO Tokens:
Received:
2025-03-14T01:51:40Z
Expiration:
2025-03-28T01:51:39Z (Not Expired)
```

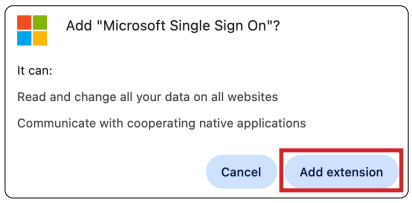
25. Let's test out the Microsoft Platform SSO Extension. Open Google Chrome.

26. Go to:
https://chromewebstore.google.com/detail/microsoft-single-sign-on/ppnbnpeolgkicgegkbkbjmhlideopiji?hl=en

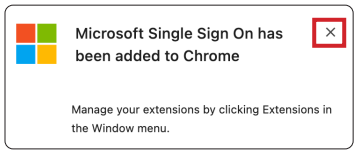
27. Click Add to Chrome.



28. Click Add extension.

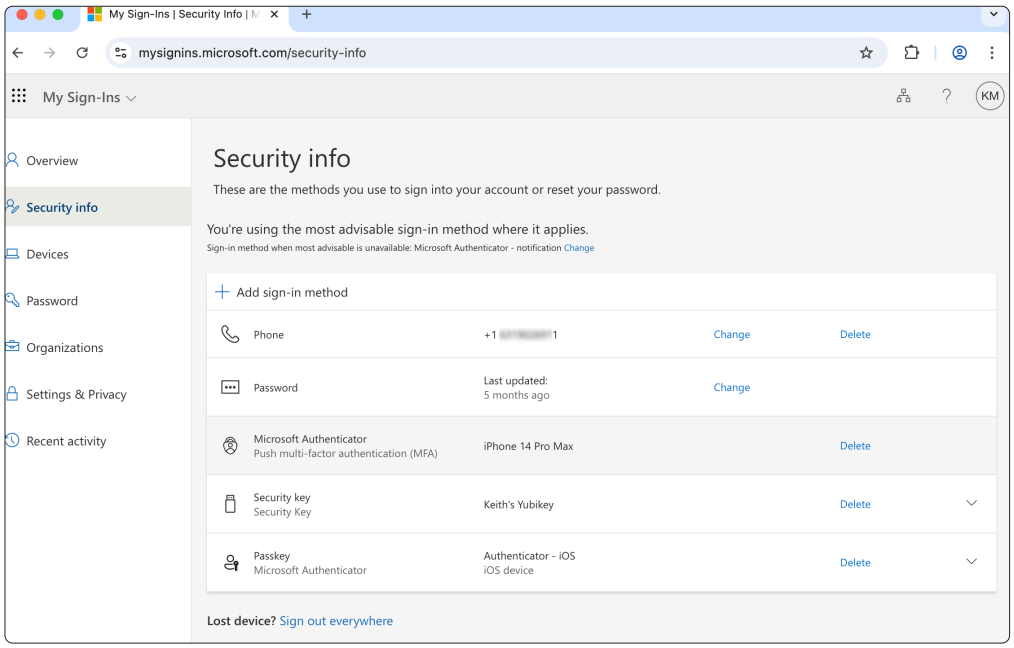


29. Click Close (X).



30. To test the Microsoft Single Sign on Google Chrome Extension. Go to: https://mysignins.microsoft.com/security-info

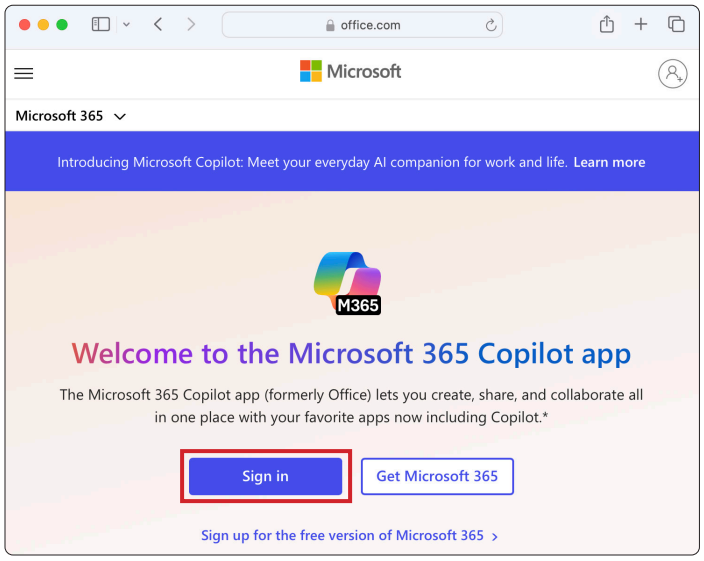
31. Confirm you were not prompted to sign in. This is because your Mac computer has a Platform SSO token.



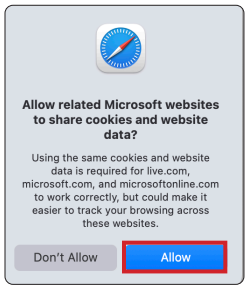
32. To test using Safari, sign into a different Microsoft service which has native support for Microsoft Platform SSO, Open Safari.

33. Go to: https://www.office.com

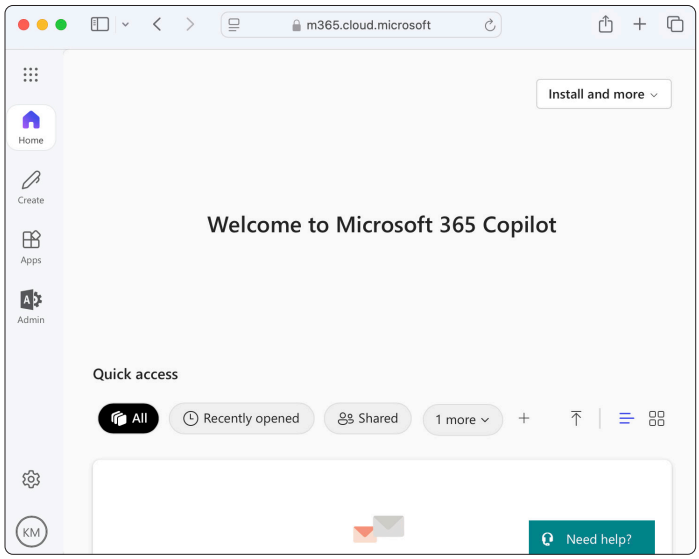
34. Click Sign in.



35. Make a selection of your choosing. This guide will select Allow.



36. You will not be prompted to sign in as your Mac computer has a Platform SSO token.



This completes this section. In the next section, we will use Jamf Connect with the Microsoft PSSO Extension to show how they can work together to provide a solution to Password syncing while using the Secure Enclave authentication method.

Section 6: Configuring Microsoft Entra for use with Jamf Connect and PSSO

What You'll Need:
Learn what hardware, software, and information you'll need to complete the tutorials in this section.

Hardware and Software:
Requirements for following along with this section:

- A Mac Computer with the Jamf Connect Configuration app installed. This guide will use version 2.45.1
- Administrative privileges in Microsoft Entra

To ensure Microsoft Authenticator is used instead of FIDO2 authentication methods with Jamf Connect, specific configuration in Microsoft Entra ID is required due to how Jamf Connect operates. Jamf Connect uses WebKit, the macOS-native rendering engine, at the login window which is not a full browser. This presents limitations when handling advanced authentication methods like FIDO2, which rely on features not supported in WebKit such as browser extensions or certain redirect behaviors.

Because of these limitations, Microsoft recommends enforcing the use of Microsoft Authenticator or password-based methods instead of FIDO2 for Jamf Connect when the secure enclave method is used and password syncing is required. This is achieved by:

- Configuring Conditional Access Policies in Microsoft Entra ID to target a specific cloud app.
- Modifying Jamf Connect's App Registration to support Conditional Access scenarios where only compatible authentication methods like Microsoft Authenticator are allowed.
- Avoiding FIDO2 because it may not complete successfully within the WebKit-based login window used by Jamf Connect.

This configuration ensures a smoother and more secure user experience during macOS login while maintaining compliance with organizational authentication policies. It also allows local account password syncing when using Jamf Connect with the secure enclave method.

In this section, we will configure the following:

- Configure an administrative account in Microsoft Entra with the required roles to create a custom security attribute for MFA exceptions.
- Create a custom security attribute for MFA exceptions.
- Create an application registration with a custom API.
- Create an application registration to call a custom scope.
- Apply the custom security attribute to Jamf Connect Enterprise application.
- Create a conditional access authentication strength to specify which combinations of authentication methods can be used to access Jamf Connect.
- Create a conditional access policy to enforce rules on the Jamf Connect application.
- Create a Jamf Connect configuration profile with conditional access settings.

While not required, Jamf recommends creating new application registrations for Jamf Connect instead of modifying existing application registrations. This will help prevent unexpected errors or conflicts during deployment to your organization. We recommend using a Microsoft Entra development server to test the steps in this section before using it in production. This guide will create all the app registrations needed for Jamf Connect.

This section discusses a topic that is often brought up by organizations when using the Secure Enclave method with Jamf connect to provide password syncing. Keep in mind, Microsoft's long term vision is to move organizations away from password syncing and recommends the guidance below.

Microsoft does not recommend using the Resource Owner Password Credential (ROPC) flow to synchronize the local macOS password with the user's Entra ID password. While authentication at the macOS login window via the OIDC (OpenID Connect) flow, such as with an authenticator app or Jamf Connect is supported, Microsoft's long-term vision is for organizations to treat the local Mac password similarly to the Windows Hello for Business (WHfB) PIN.

From Microsoft's perspective, tools like Jamf Connect at the macOS login window are acceptable for federated authentication, but password synchronization should be avoided as part of a broader security modernization effort. If organizations continue to implement password sync today, it is

recommended that they consider deprecating it in the medium to long term. This aligns with current Microsoft guidance for Windows environments, where passwordless and non-synced credential models (e.g., WHfB, FIDO2, and certificate-based auth) are becoming the standard.

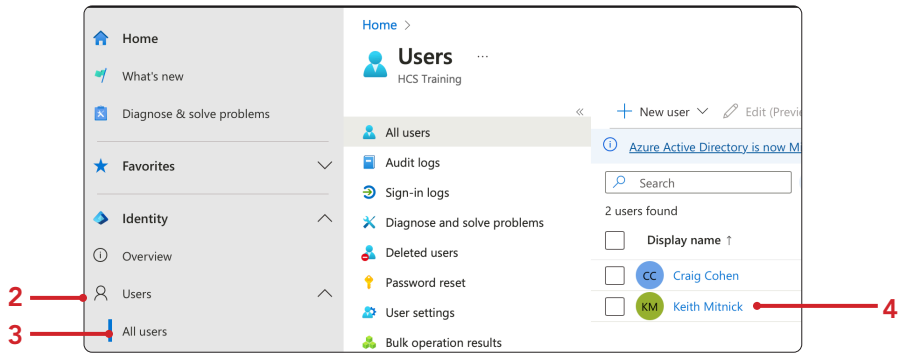
For more information on what we are configuring in this section, see the official Jamf documentation at the links below:

https://learn.jamf.com/en-US/bundle/jamf-connect-documentation-current/page/Entra_ID_Conditional_Access_and_All_Cloud_Apps.html

https://learn.jamf.com/en-US/bundle/jamf-connect-documentation-current/page/Modifying_Jamf_Connect_for_Conditional_Access_Polices.html

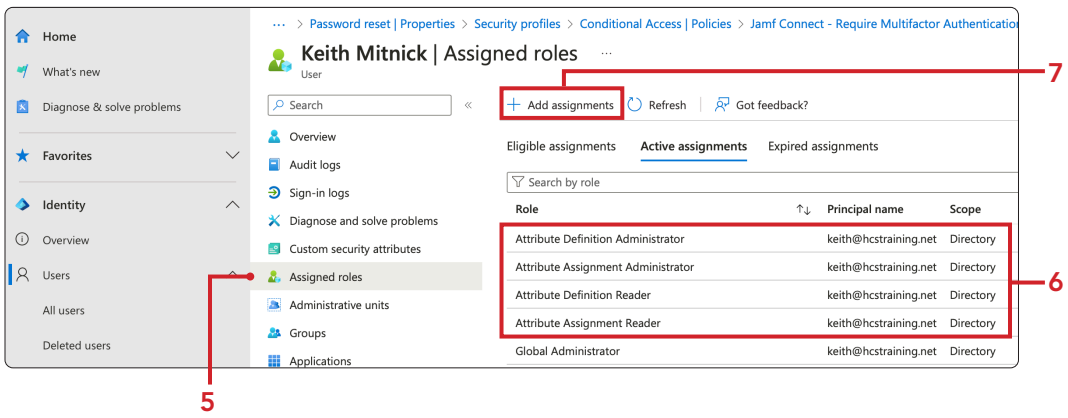
Here is a video from JNUC 2023 that explains conditional access with Jamf Connect.
https://www.youtube.com/watch?v=D9-4miD-3pM

1. To add the required roles to your account, log into Microsoft Entra.
2. Click Users.
3. Click All Users.
4. Select your user account.

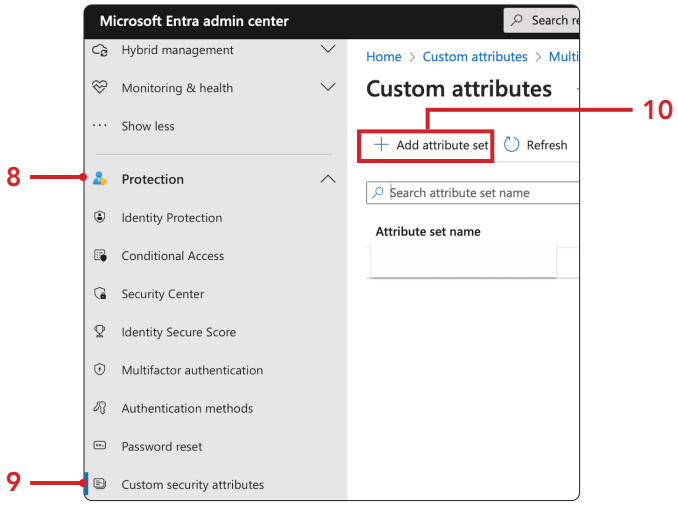


5. Click Assigned roles.
6. Confirm you have the following roles:
   - Attribute assignment administrator
   - Attribute assignment reader
   - Attribute definition administrator
   - Attribute definition reader

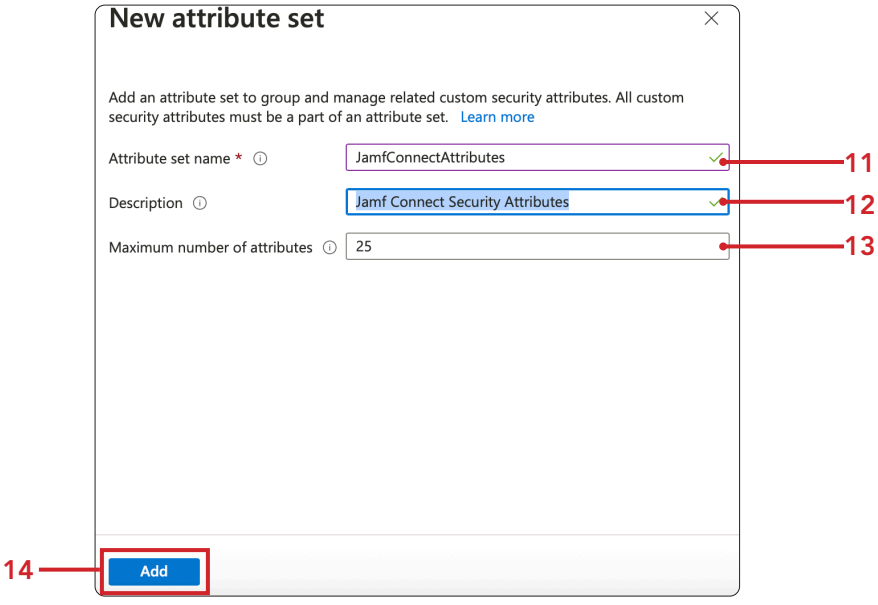
   NOTE: Having Global Administrator rights are not enough, you must assign the roles above to your Global Administrator account.
7. If the above roles are not assigned to you, Click Add assignments (+). You cannot continue with this section without having the above roles assigned to your account.



8. To create a custom security attribute, click Protection.
9. Click Custom security attributes.
10. Click Add attribute set.

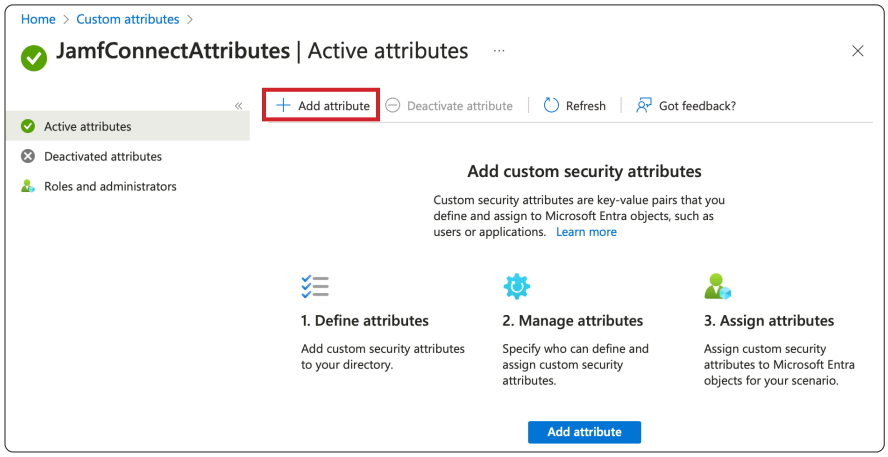


11. Enter **JamfConnectAttributes** for Attribute set name (The name cannot contain more than 32 characters, spaces, or special characters.)
12. Enter **Jamf Connect Security Attributes** for the Description.
13. Enter **25** for Maximum number of attributes.
14. Click Add.

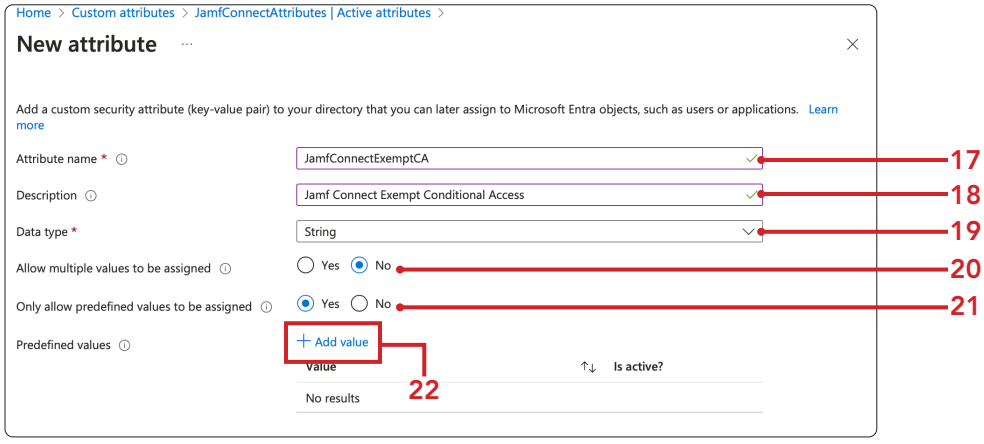


15. Click on JamfConnectAttributes to open it.

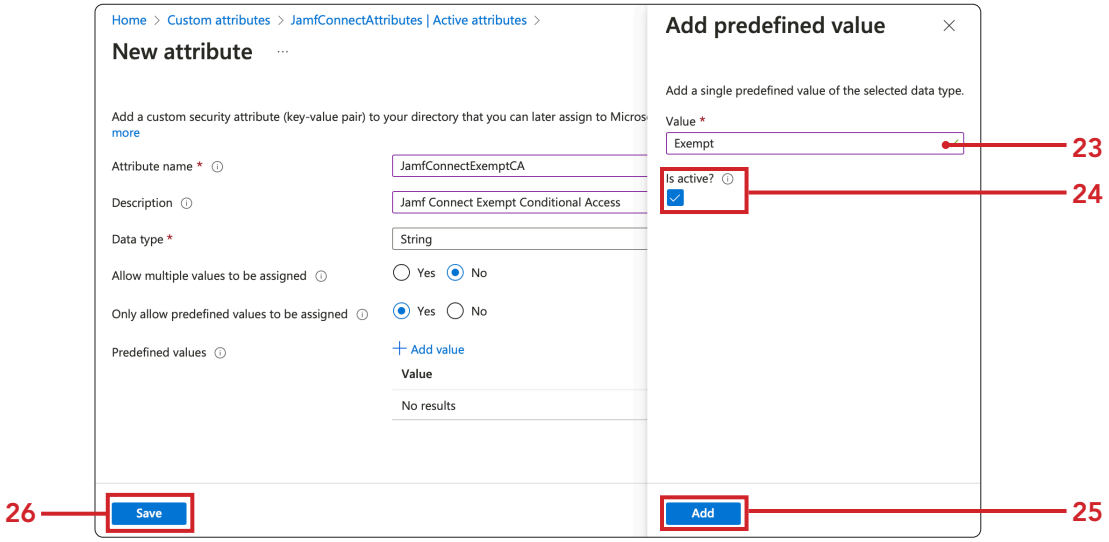
16. Click Add attribute (+).



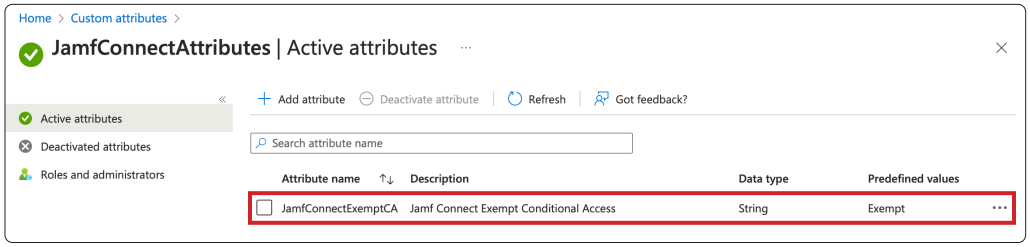
17. Enter **JamfConnectExemptCA** for the Attribute name.
18. Enter **Jamf Connect Exempt Conditional Access** for the Description.
19. Select String for Description.
20. Select No for Allow multiples values to be assigned.
21. Select Yes for Only allow predefined values to be assigned.
22. Click Add Value.



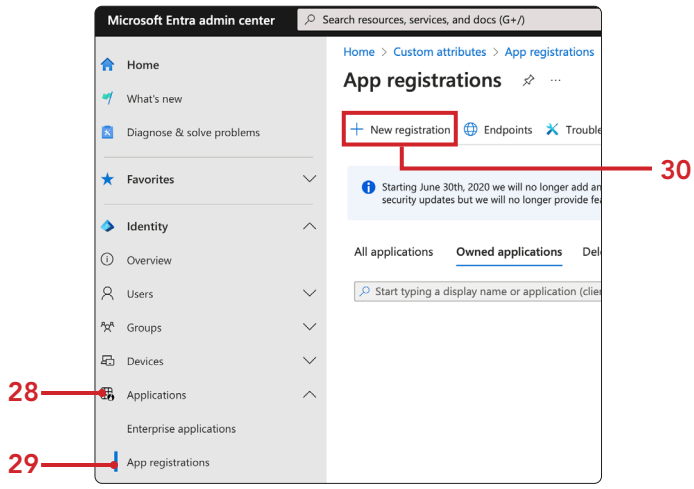
23. Enter **Exempt** for the Value.
24. Select the checkbox for Is active?.
25. Click Add.
26. Click Save.



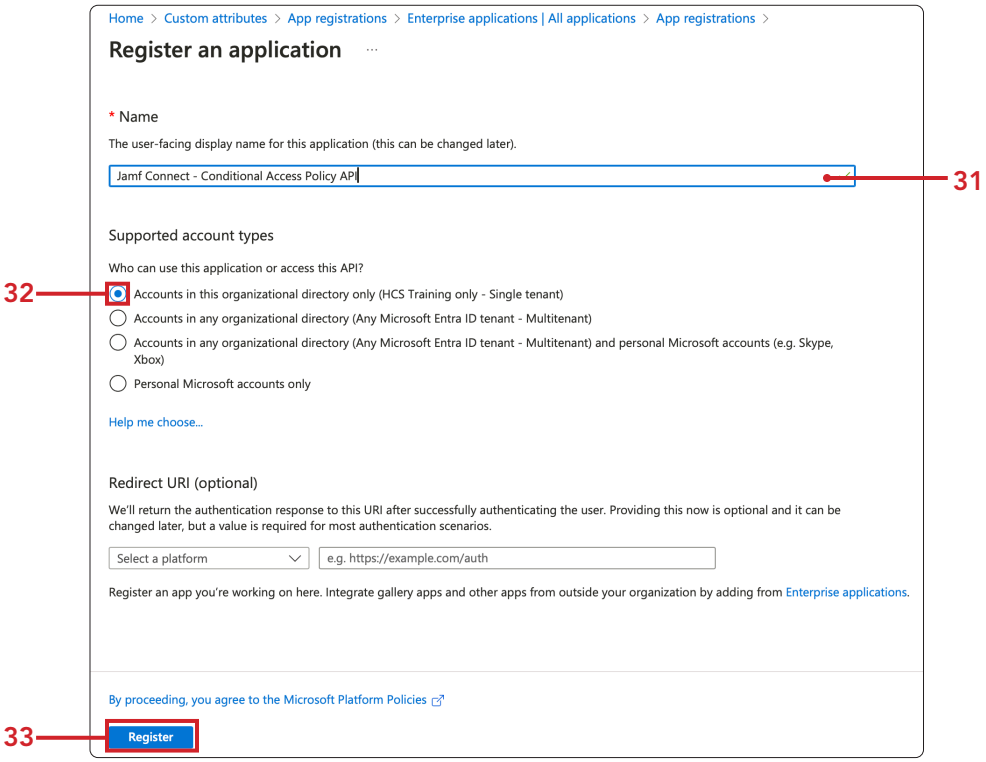
27. Confirm the active attribute shows in the list.



28. To create an app registration with a custom API, click Applications.
29. Select App registrations.
30. Click New registration (+).

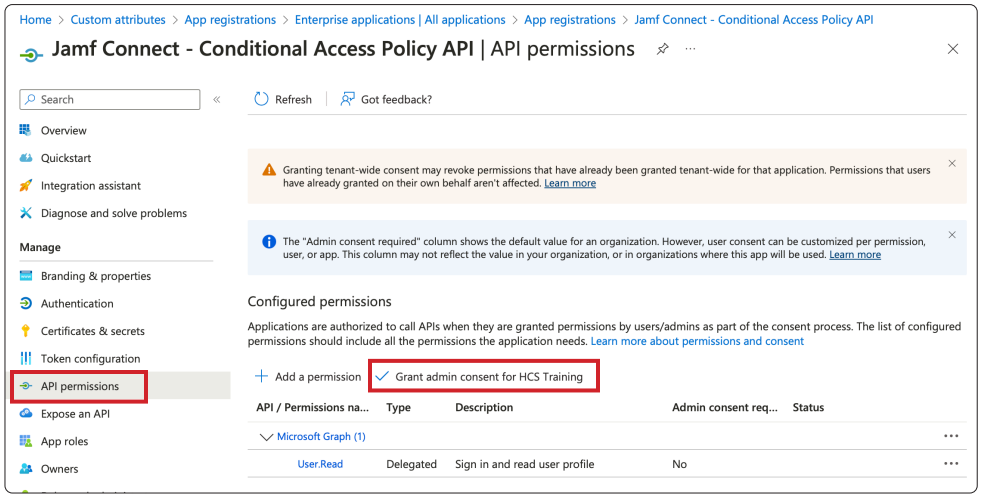


31. Enter **Jamf Connect - Conditional Access Policy API** for the Name.
32. Select the Radio Button for Accounts in this organizational directory only (<Company Name> only - Single tenant). [HCS Training is used for the company name in this example].
33. Click Register.

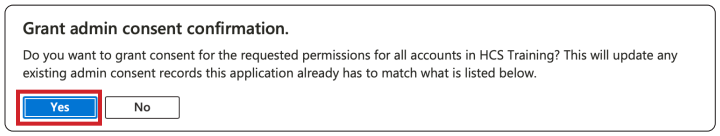


34. Click API permissions.

35. Click Grant admin consent for <Company Name>. (HCS Training is used in the example)

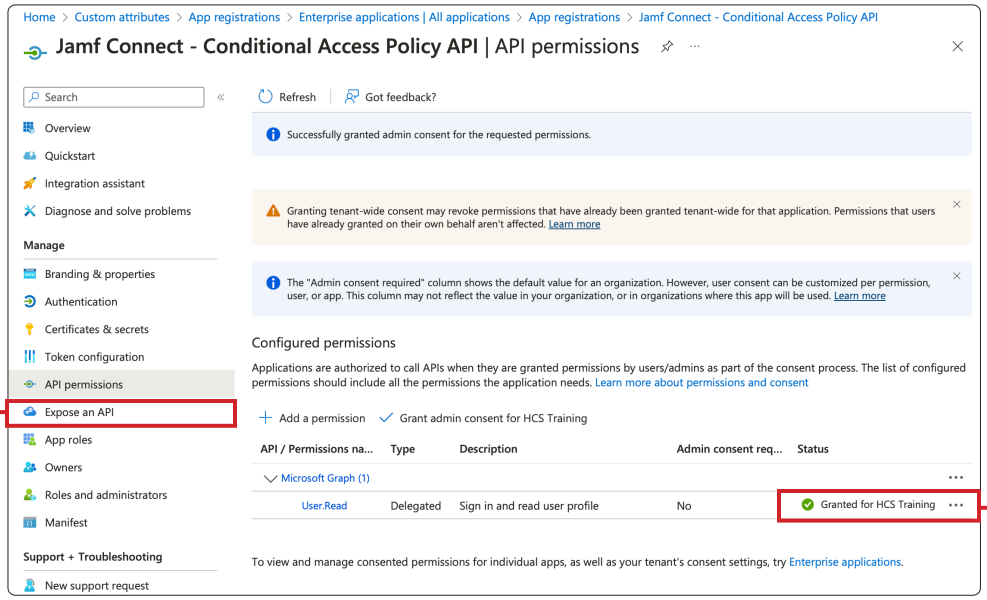


36. Click Yes.

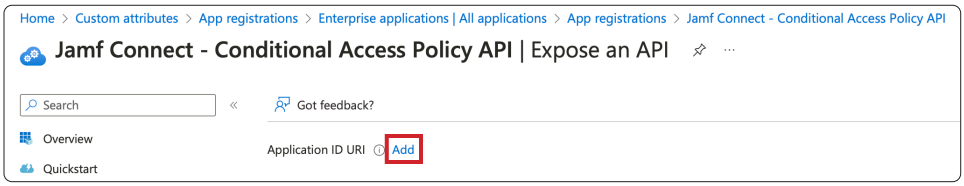


37. Under Status, confirm "Granted for <Company Name>" is active. This is indicated with a ✅ (HCS Training is used for the company name in the example)

38. In the sidebar, click Expose an API.

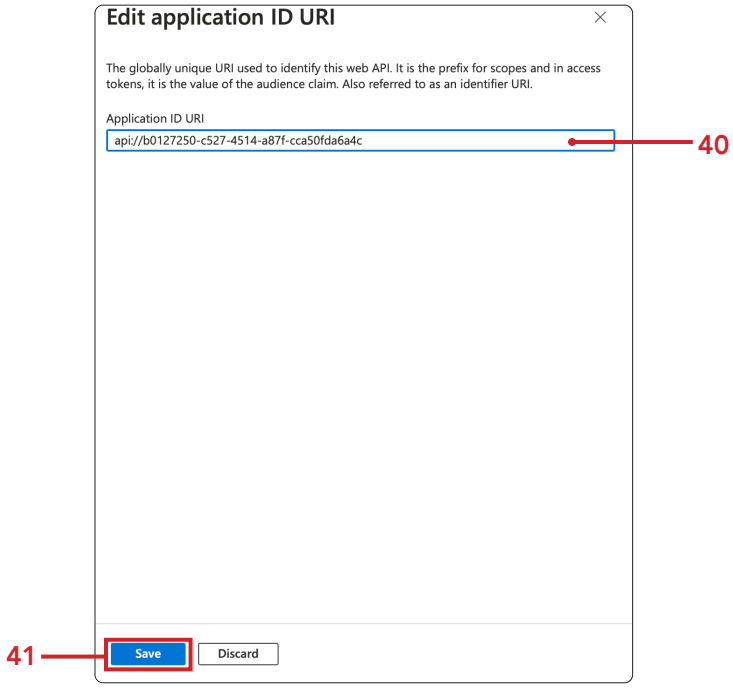


39. In the Application ID URI section, click Add.

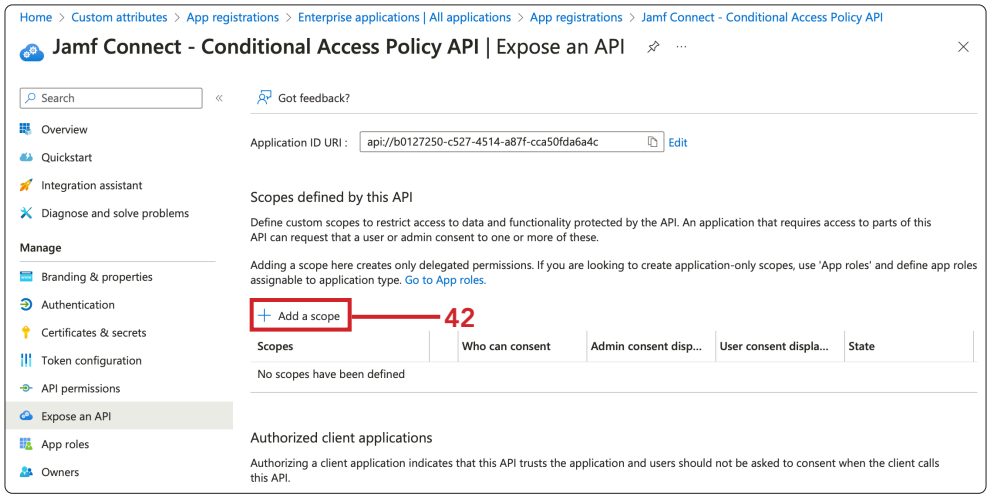


40. Confirm the Application ID URI. Leave it at it's default value.

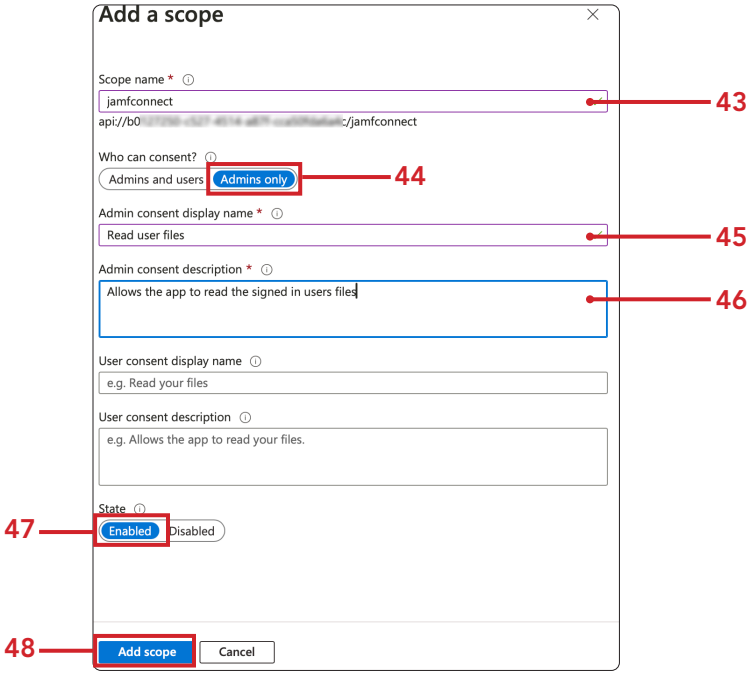
41. Click Save.



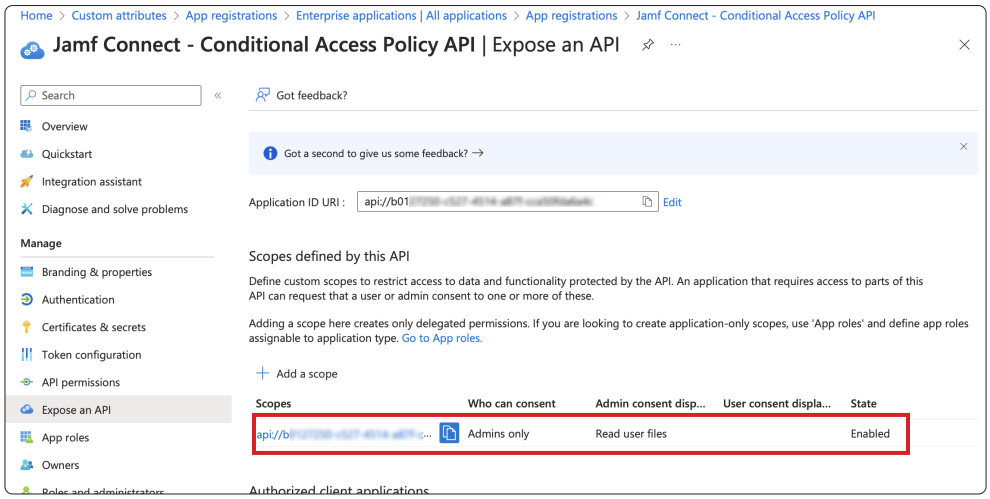
42. Click Add a scope (+).



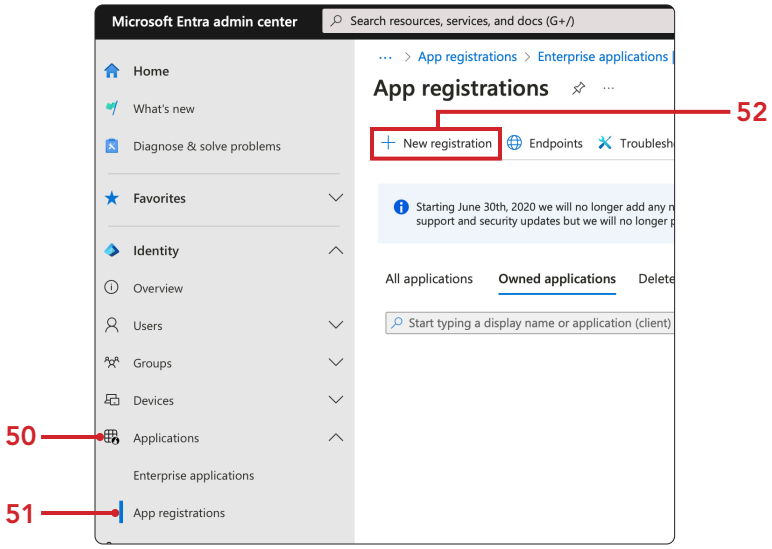
43. Enter **jamfconnect** for the Scope name.
44. Set who can consent. This guide will use Admins only.
45. Enter **Read user files** for Admin consent display name.
46. Enter **Allows the app to read the signed in users files** for Admin consent description.
47. Set the State to Enabled.
48. Click Add Scope.
    NOTE: We are not actually reading the users files, we are reading the users information in Entra. For more info on this, go here: https://learn.microsoft.com/en-us/graph/permissions-reference#userread



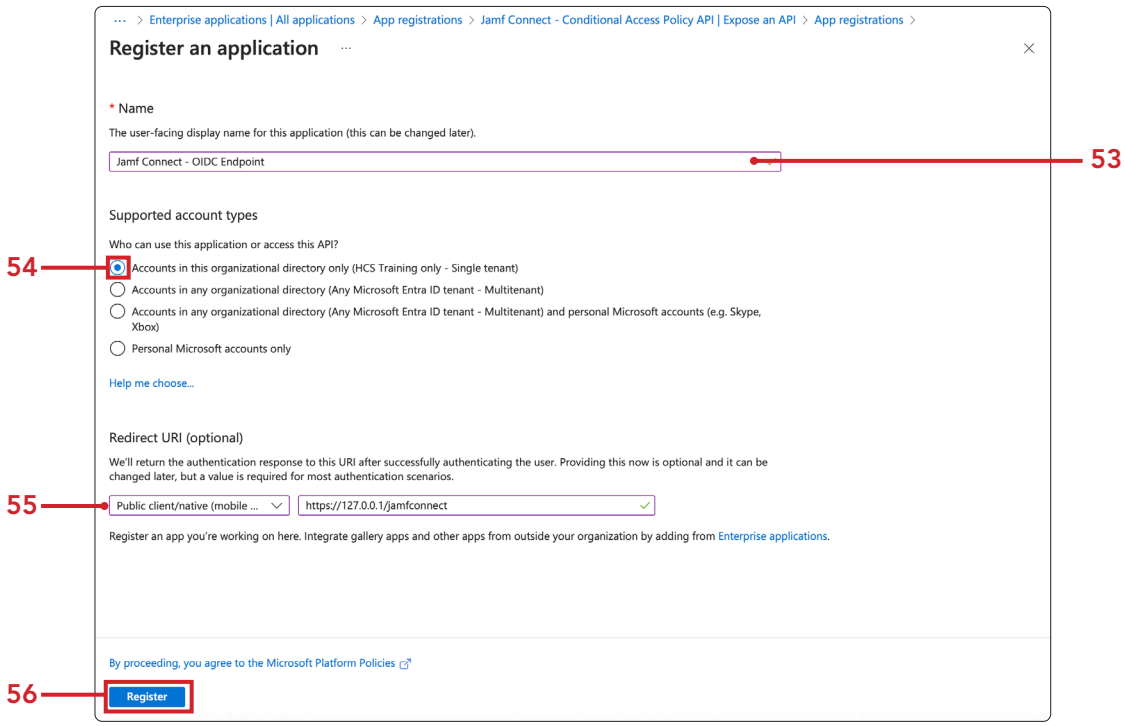
49. Confirm the Application ID URI and Scope were created.



50. Let's create an app registration to call a custom scope. Click Applications.
51. Select App registrations.
52. Click New registration (+).



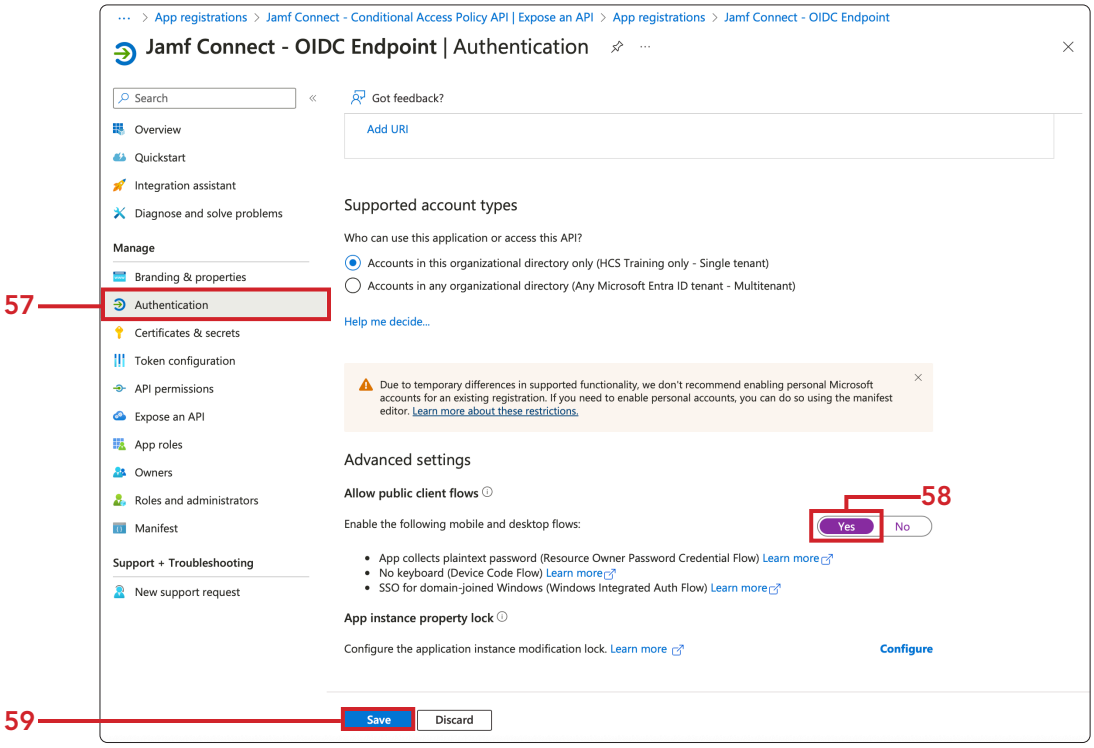
53. Enter **Jamf Connect - OIDC Endpoint** for the Name.
54. Select the radio button for Accounts in this organizational directory only (<Company Name> only - Single tenant) [HCS Training is used for the company name in the example].
55. Select Public client/native (mobile) under Redirect URI.
56. Click Register.



57. Click Authentication.

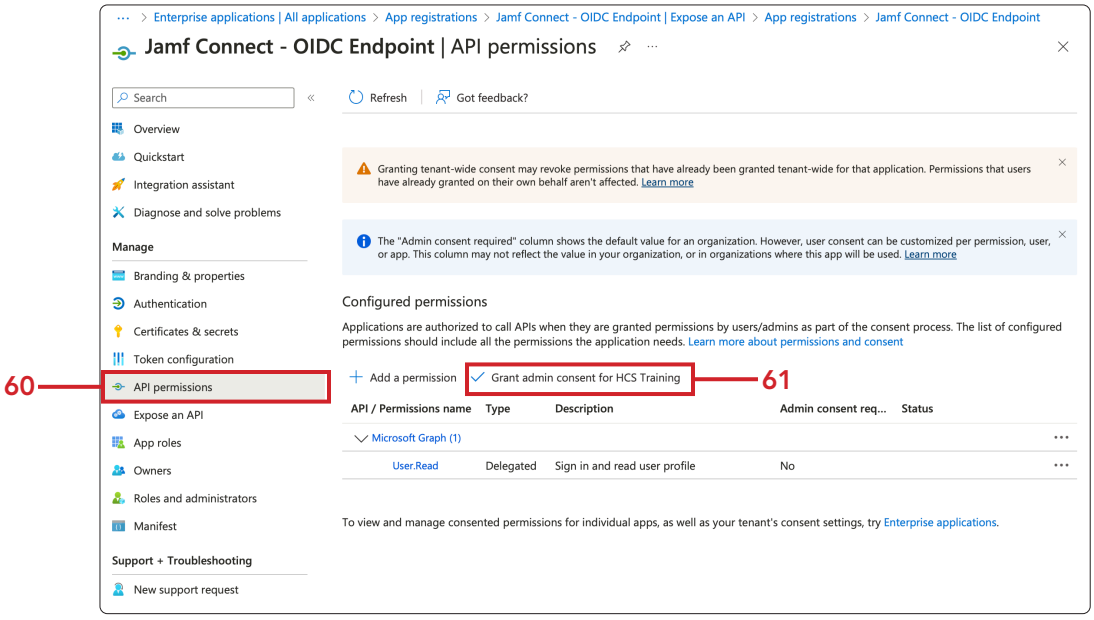
58. Select Yes for Allow public client flows.

59. Click Save.

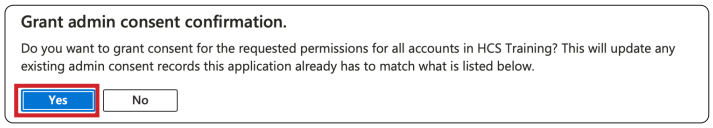


60. Click API permissions.

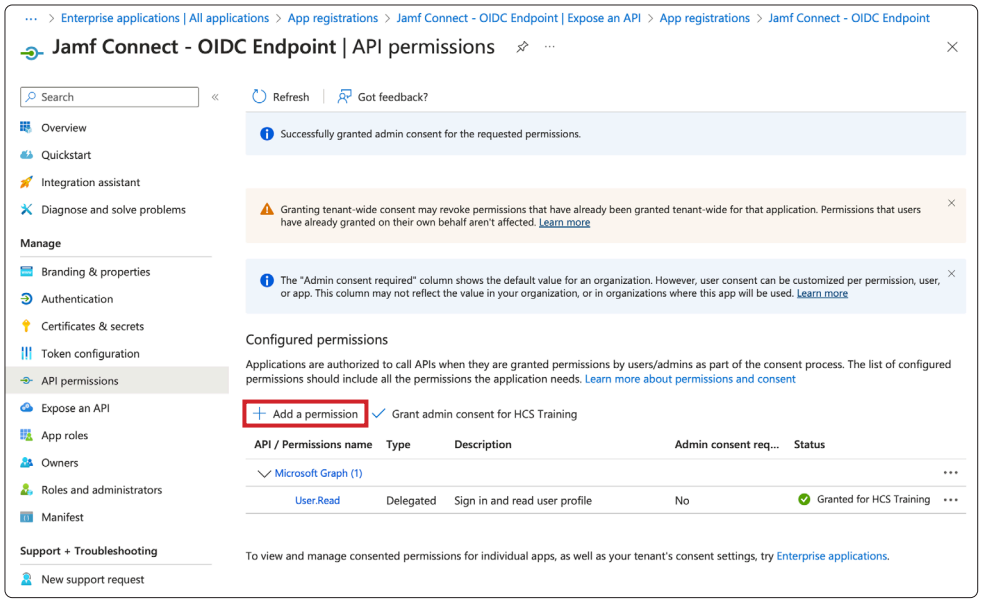
61. Click Grant admin consent for <Company Name> (HCS Training is used in the example).



62. Click Yes.



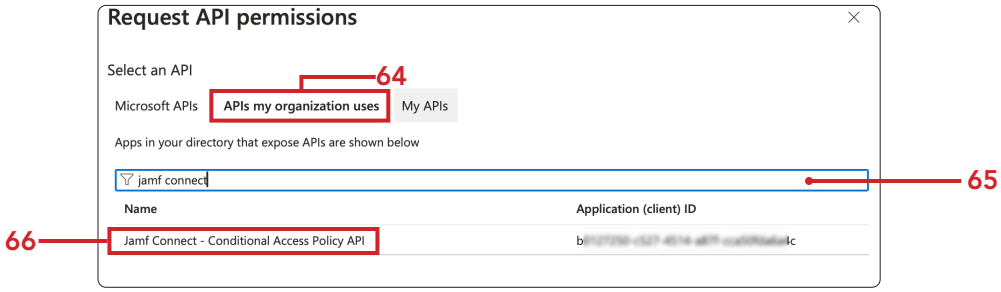
63. Click Add a permission (+).



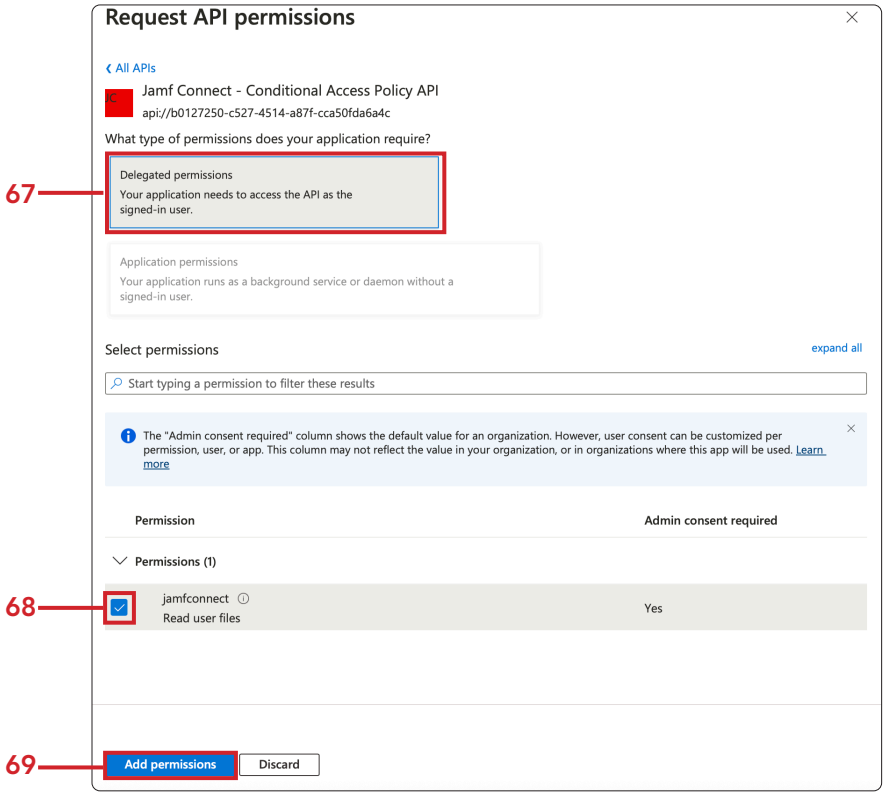
64. Click APIs my organization uses.

65. In the search field, enter **Jamf Connect**.

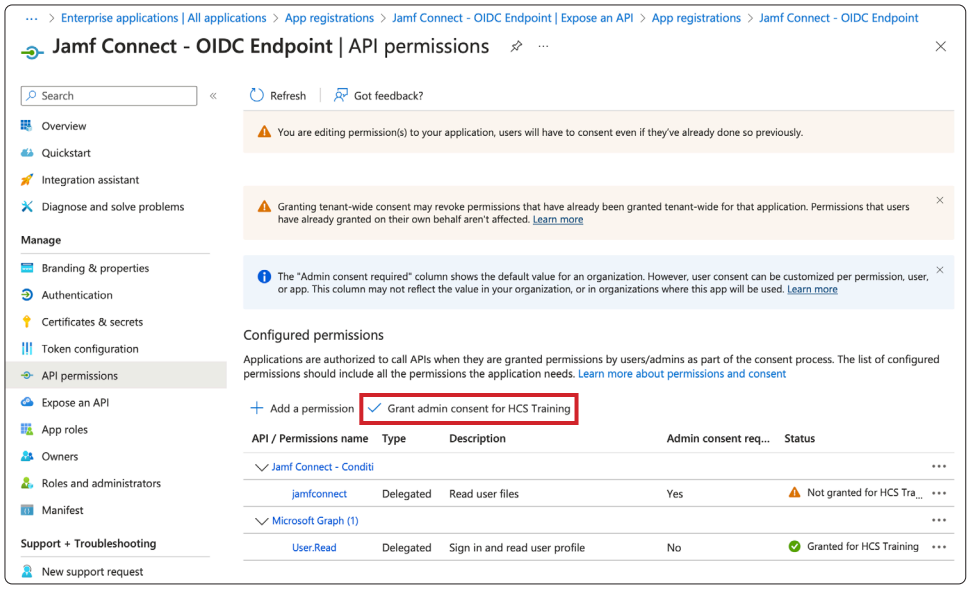
66. Select Jamf Connect - Conditional Access Policy API.



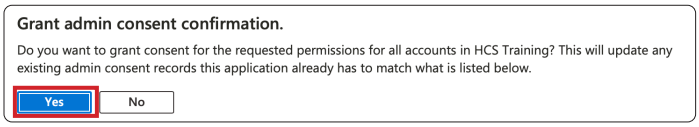
67. Select Delegated permissions.
68. Select the checkbox for jamfconnect under Permissions.
69. Click Add permissions.



70. Click Grant admin consent for <Comapny Name> (HCS Training is used in the example).

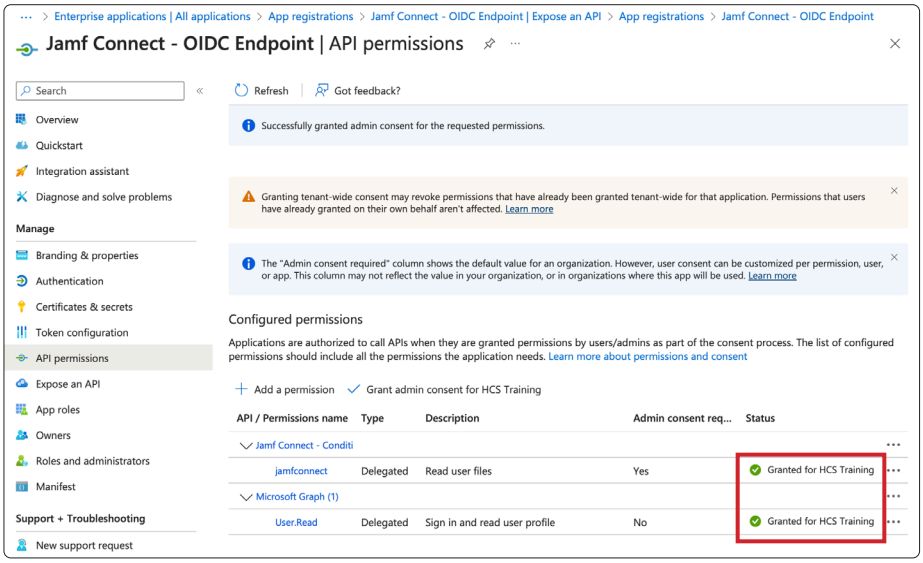


71. Click Yes.



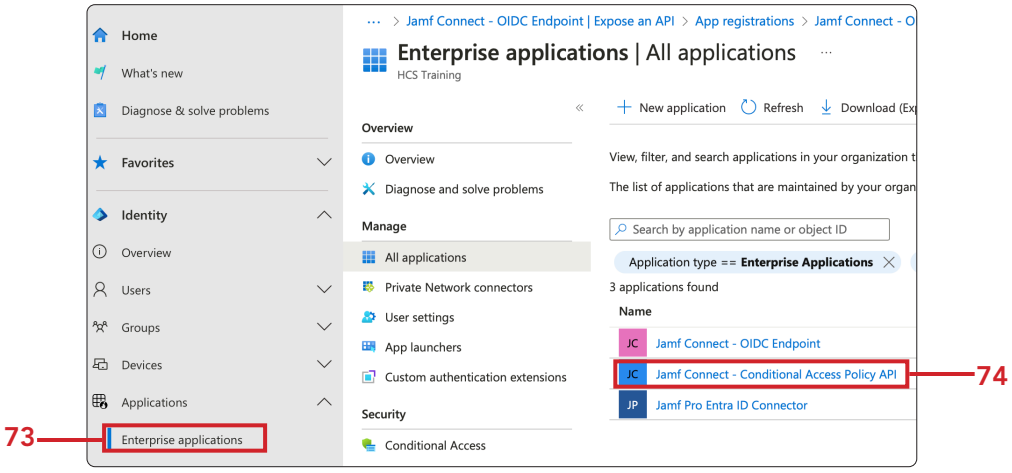
72. In the Status section, confirm Granted for <Company Name> is active for both entries. This is indicated with a ✅ (HCS Training is used for the company name in the example).

NOTE: Roles can be added to this app registration if required but we will not configure them in this guide. Roles allow a user that logs in with Jamf Connect, to query Microsoft Entra and if the user is an administrator in Entra, they will be created or converted to an administrator on their Mac. If they are a standard user in Microsoft Entra, they will be created or converted to a standard user on their Mac. To add roles to this app registration, follow the instructions for optional roles here: https://learn.jamf.com/en-US/bundle/jamf-connect-documentation-current/page/Modifying_Jamf_Connect_for_Conditional_Access_Polices.html#ariaid-title3

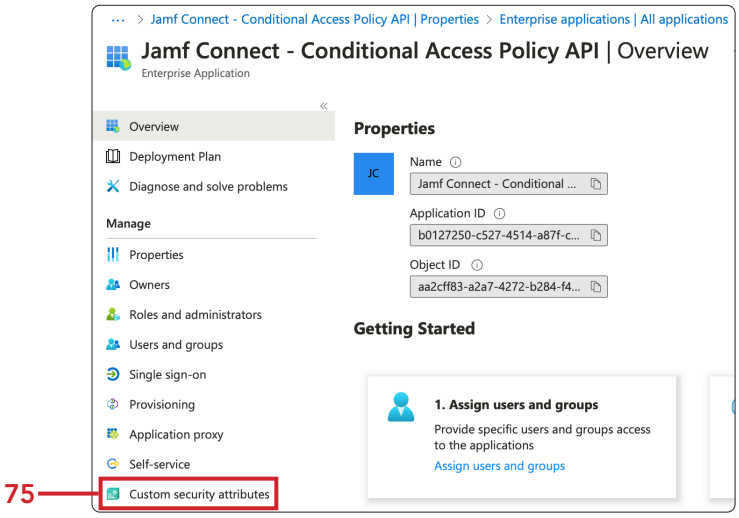


73. Let's apply the custom security attribute to the Jamf Connect Enterprise application. From the sidebar, Click Enterprise applications.

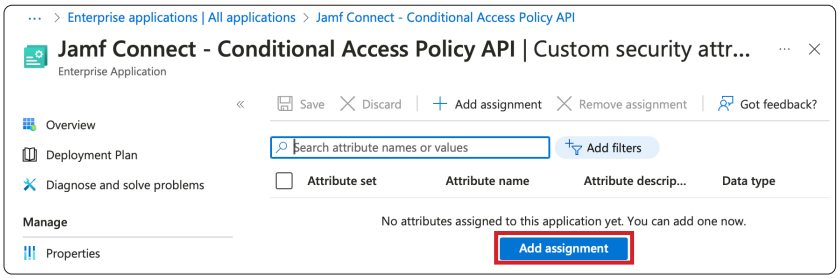
74. Click Jamf Connect - Conditional Access Policy API.



75. Click Custom security attributes.



76. Click Add assignment.



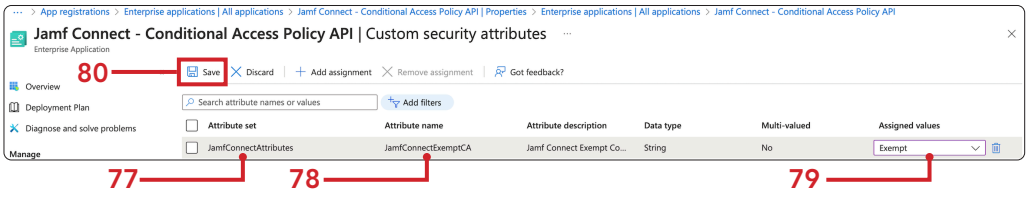
77. Under Attribute set, from the menu, select JamfConnectAttributes.

78. Under Attribute Name, from the menu, select JamfConnectExemptCA.

79. Under Assigned Value, select Exempt.

80. Click Save.

81. Confirm the settings as shown below.

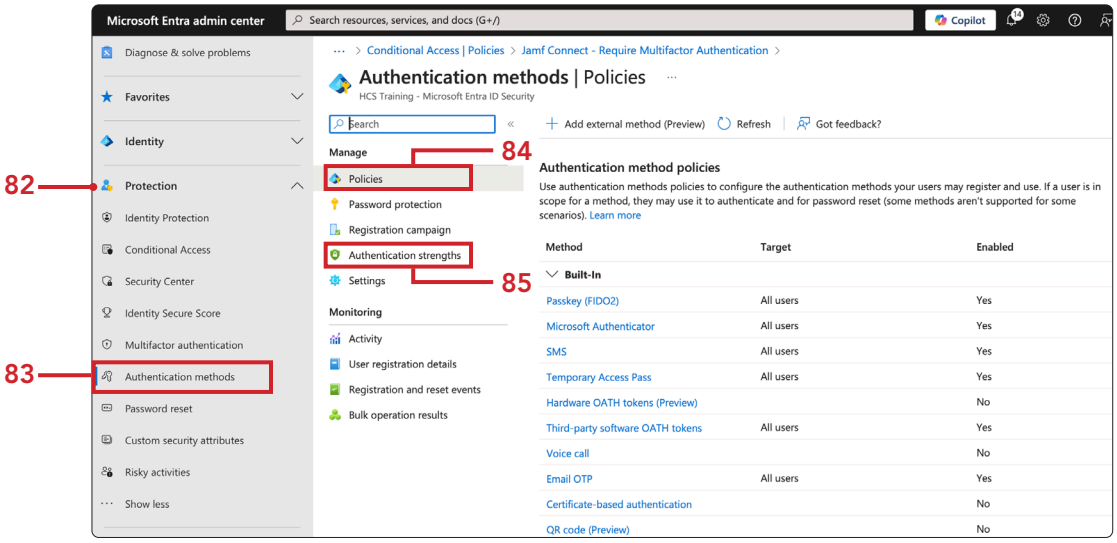


82. Let's create a conditional access authentication strength to specify which combinations of authentication methods can be used to access Jamf Connect. From the sidebar, click Protection.

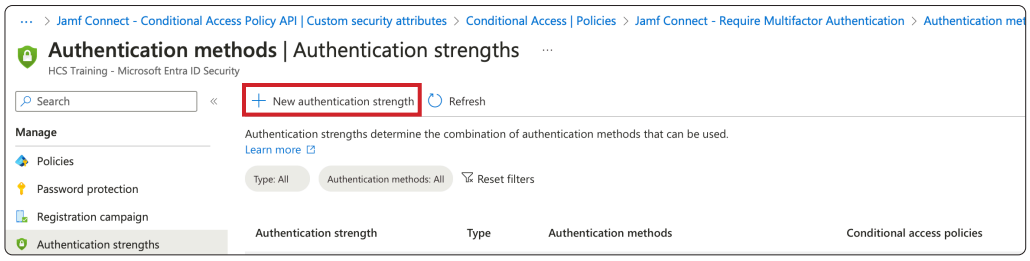
83. Click Authentication methods.

84. Click Policies and view the different authentication methods that are enabled.

85. Click Authentication strengths.
When there are multiple authentication method policies enabled, some methods like Passkey FIDO2 and other FIDO2 methods will not work at the Jamf Connect Login window. A conditional access authentication strength will allow us to force authentication methods that are supported by Jamf Connect at the login window like Microsoft Authenticator.



86. Click New authentication strength.

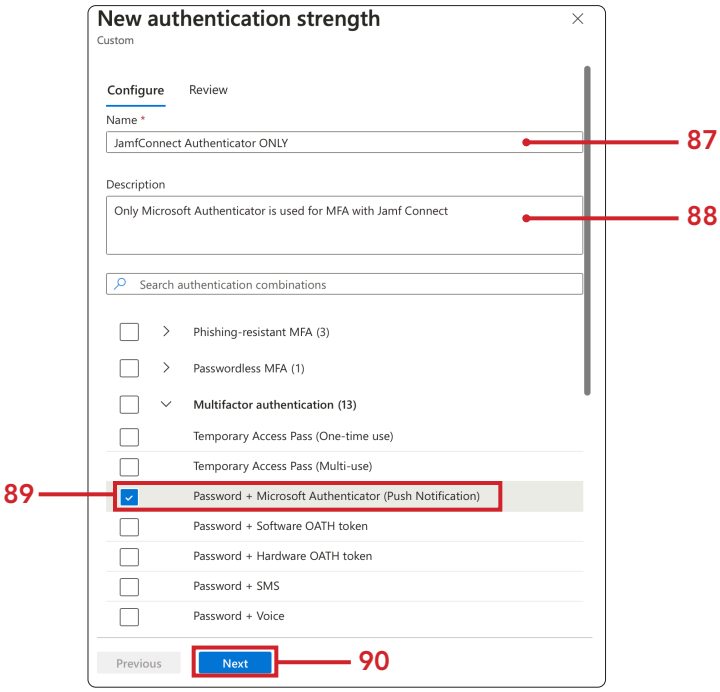


87. Enter **JamfConnect Authenticator ONLY** for the Name.

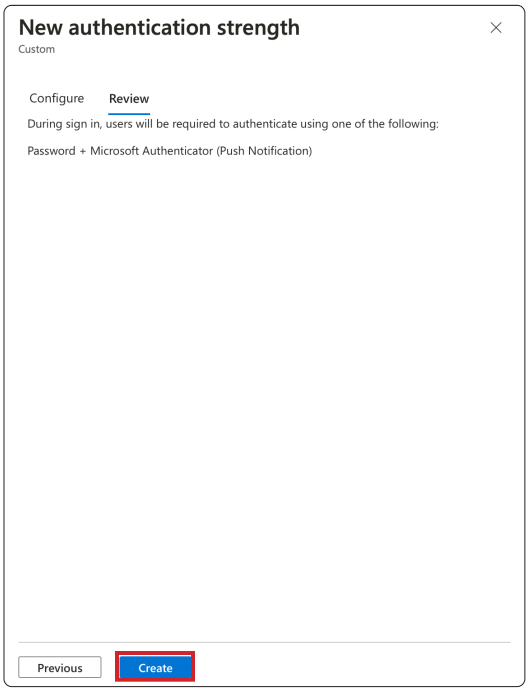
88. Enter **Only Microsoft Authenticator is used for MFA with Jamf Connect** for the Description.

89. In the Multifactor authentication section, select the checkbox for Password + Microsoft Authenticator (Push Notifications).

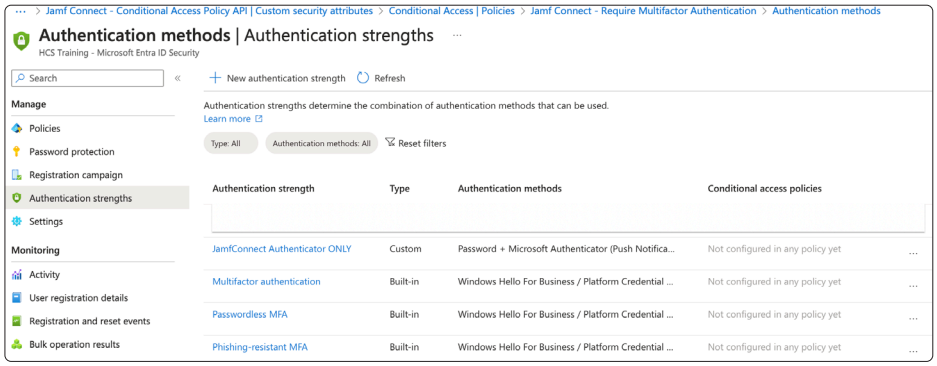
90. Click Next.



91. Click Create.



92. Confirm the authentication strength shows in the list.

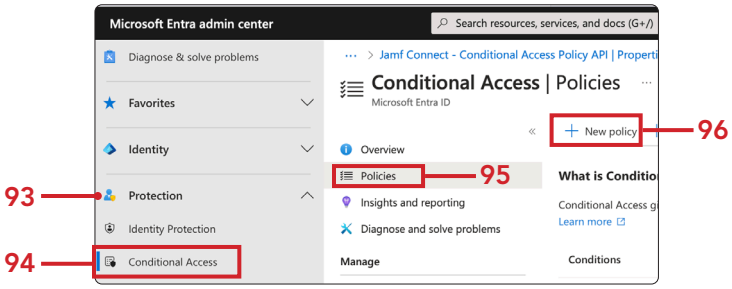


93. Let's create a conditional access policy and assign the authentication strength we just created to it. From the sidebar, select Protection.

94. Click Conditional access.

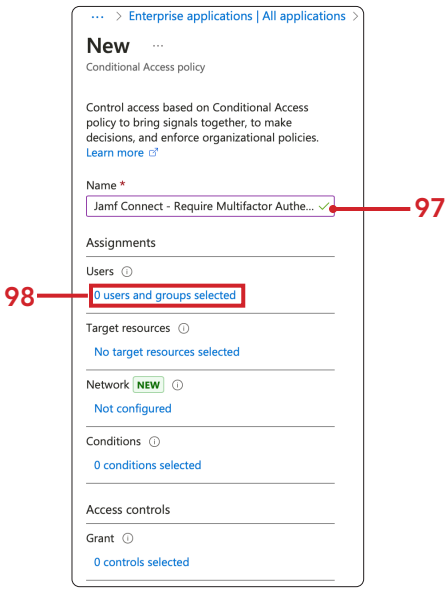
95. Click Policies.

96. Click New policy (+).



97. Enter **Jamf Connect - Require Multifactor Authentication** for the Name.

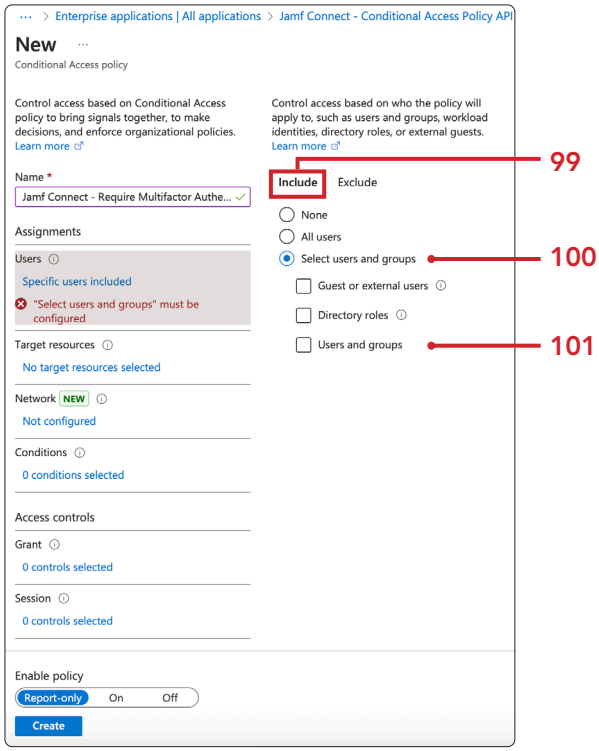
98. Users: Click the users and groups selected link.



99. Click Include.

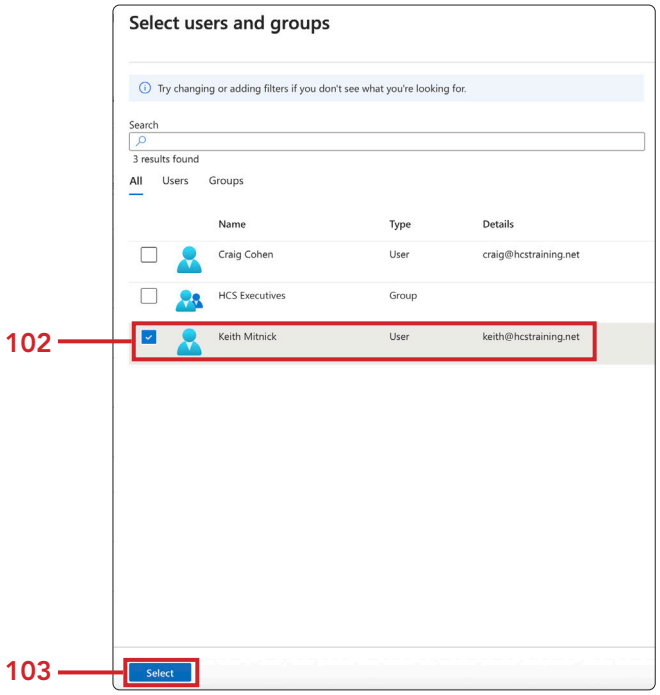
100. Select the Radio button for Select users and groups.

101. Enable Users and groups.



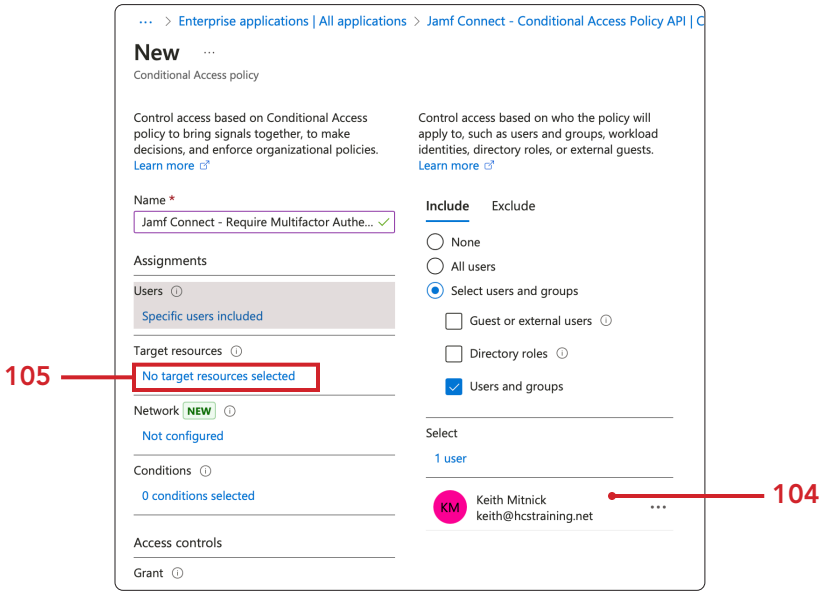
102. Select the appropriate Users or Groups. This guide will select one user for simplicity.

103. Click Select.



104. Confirm your users or groups show in the list.

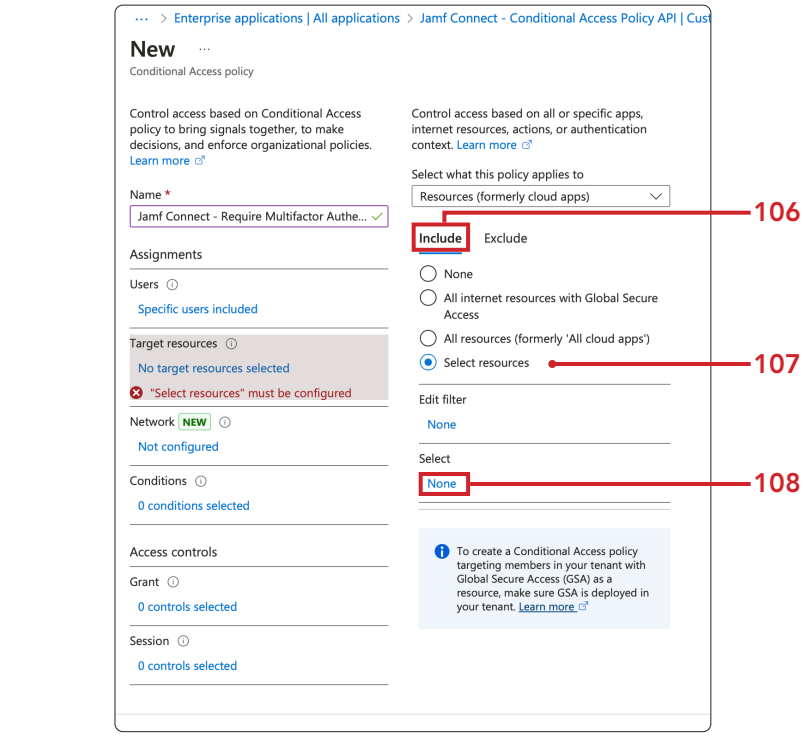
105. Under Target resources, click the link, No target resources selected.



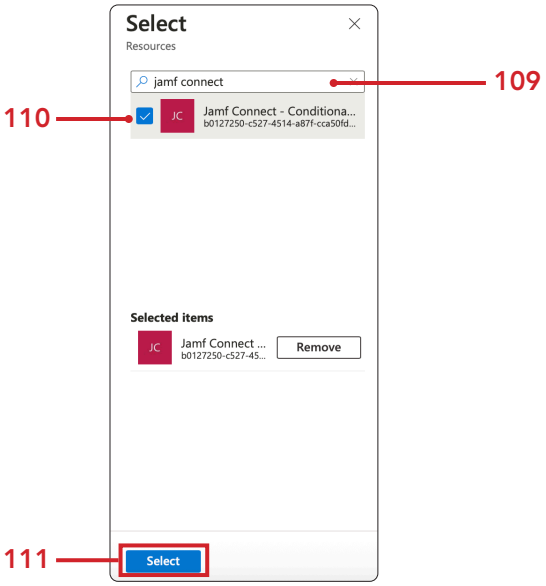
106. Click Include.

107. Select the radio button for Select resources.

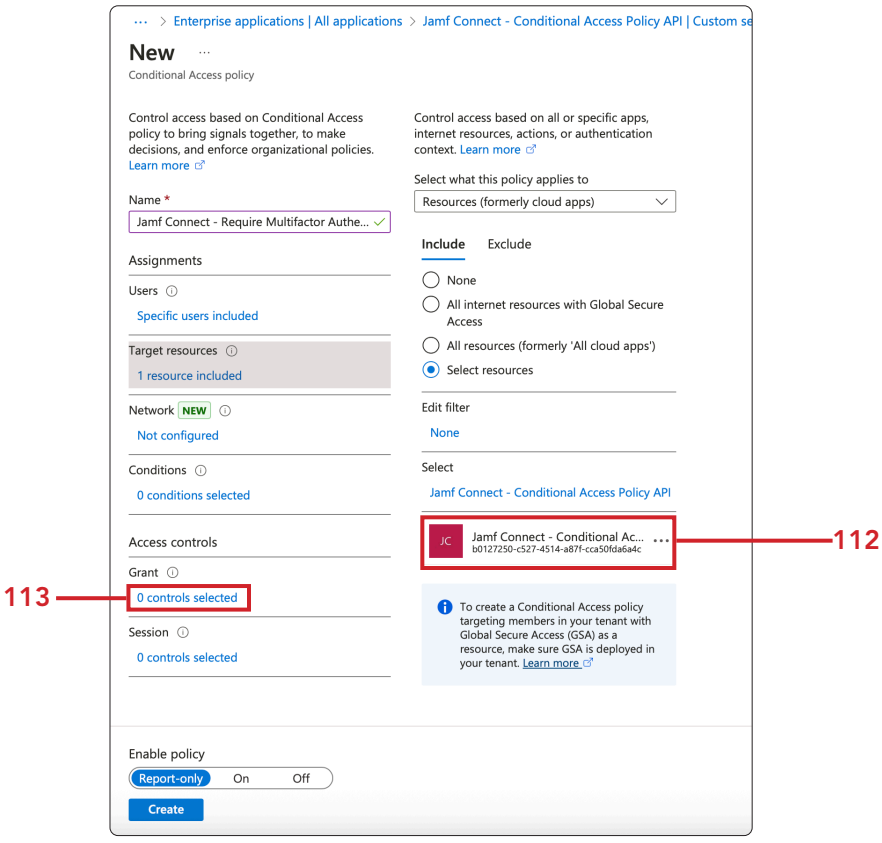
108. Under Select, click None.



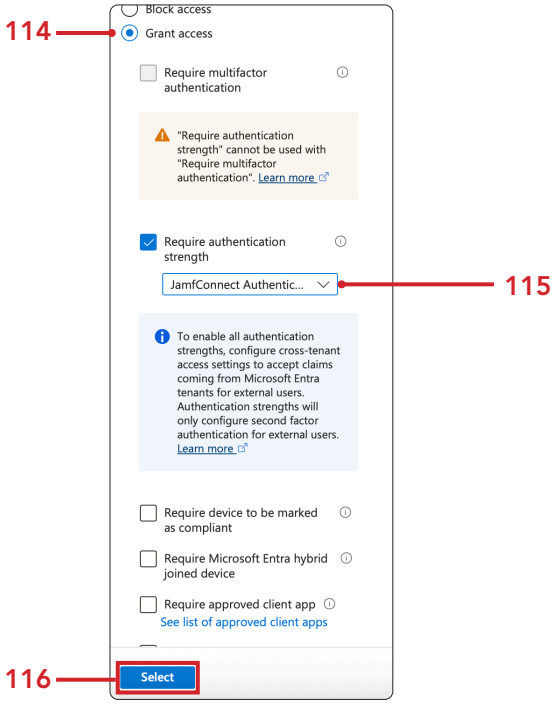
109. Perform the following: In the search field, enter **jamf connect**.
110. Select the checkbox for Jamf Connect - Conditional Access Policy API.
111. Click Select.



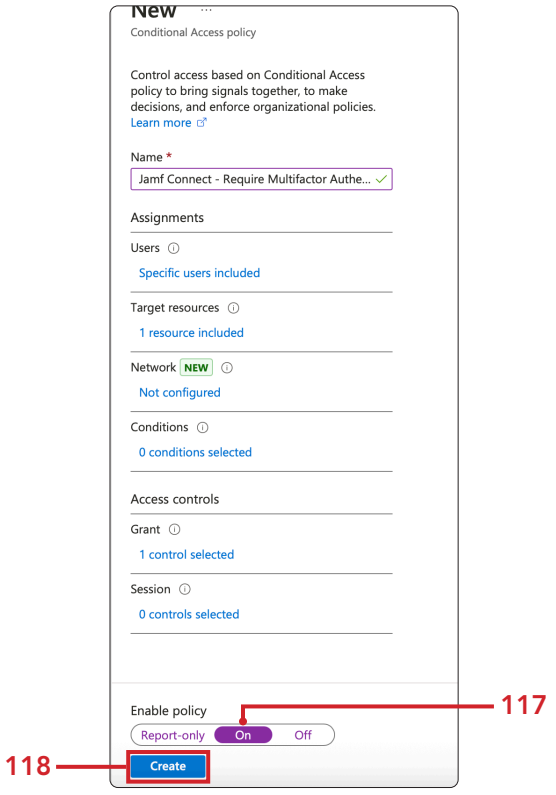
112. Confirm Jamf Connect - Conditional Access Policy API shows in the list.
113. Under Grant, Click 0 Controls selected.



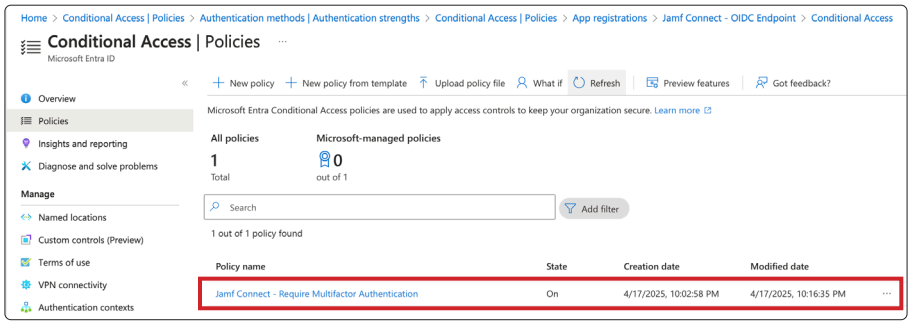
114. Enable Grant access.
115. Select JamfConnect Authenticator ONLY under Require authentication strength.
116. Click Select.



117. Select On for Enable Policy.
118. Click Create.



119. Confirm the policy shows in the list and the State is On.

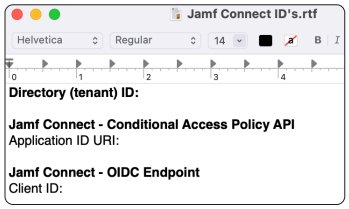


120. Let's create a TextEdit document to gather all the ID's needed to configure Jamf Connect settings. Open Text Edit.

121. Name the document, Jamf Connect ID's.

122. Enter the following info in the document:
    - **Directory (tenant) ID:**
    - **Jamf Connect - Conditional Access Policy API Application ID URI:**
    - **Jamf Connect - OIDC Endpoint Client ID:**

123. Save the document to your Desktop.

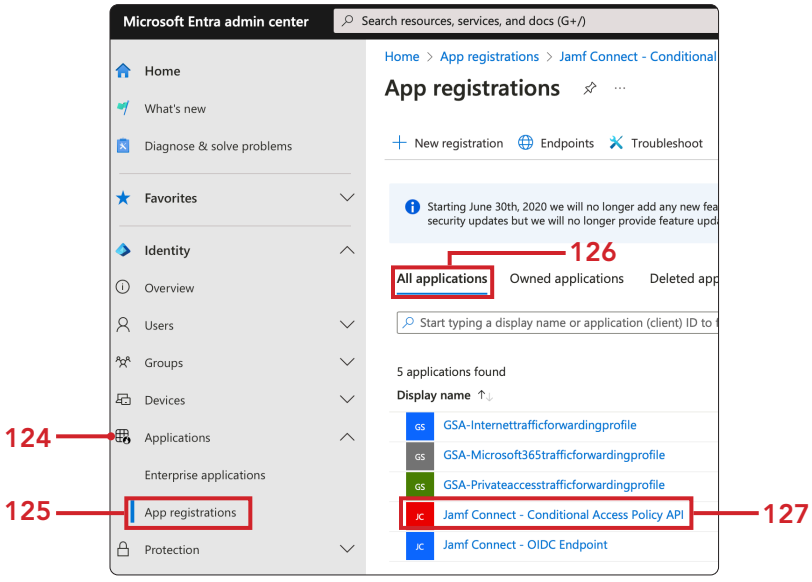


124. Switch back to Microsoft Entra. In the sidebar, Select Applications.

125. Select App registrations.

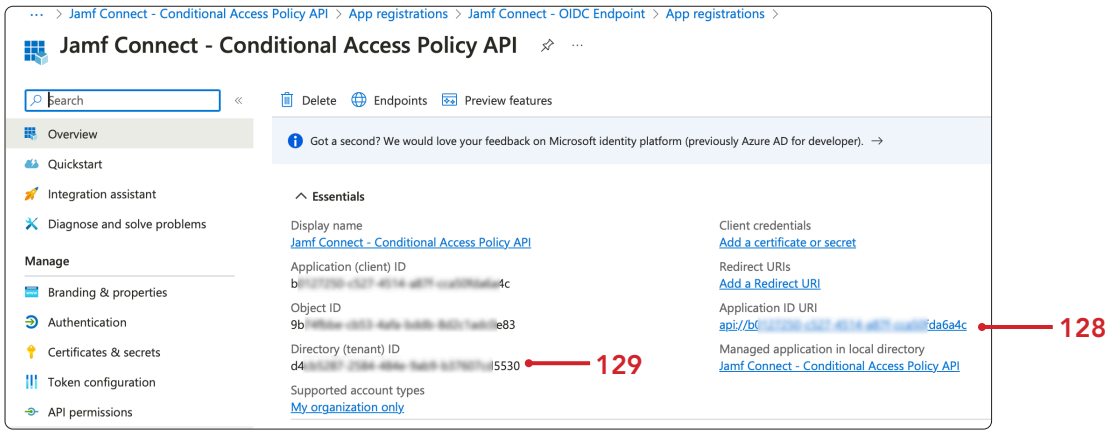
126. Select All applications.

127. Select the Jamf Connect - Conditional Access Policy API.



128. Copy the Application ID URI and paste the URI to the Application ID URI section of the Jamf Connect ID's document.

129. Copy the Directory (tenant) ID and paste this ID to the Directory (tenant) ID section of the Jamf Connect ID's document.

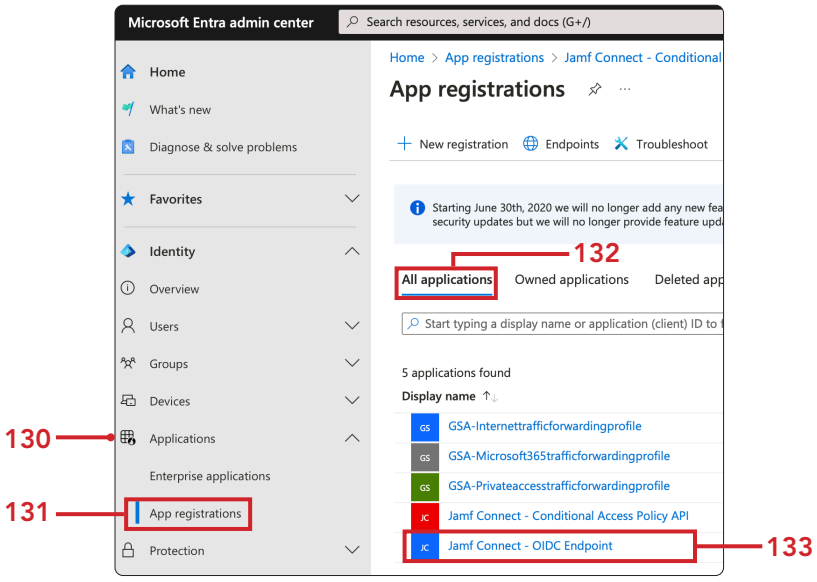


130. In the sidebar, Select Applications.

131. Select All applications.

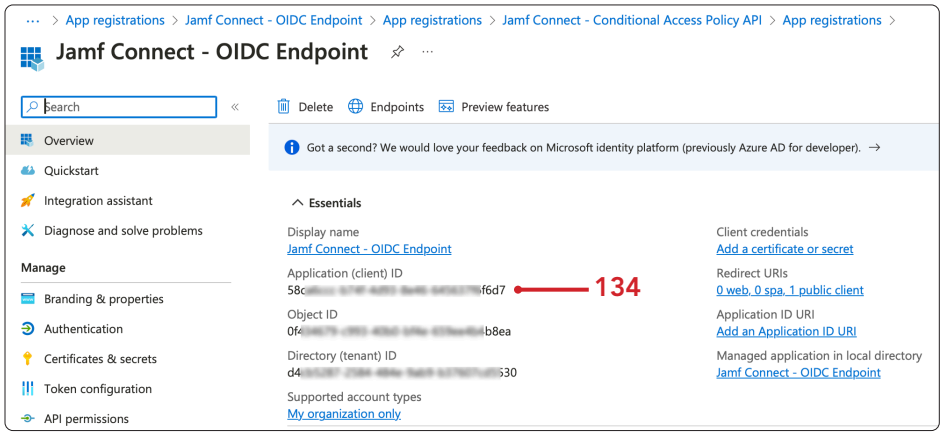
132. Select App registrations.

133. Select the Jamf Connect - OIDC Endpoint.

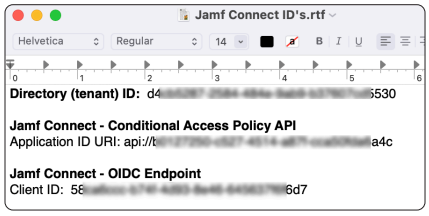


134. Copy the Application (client) ID and paste this ID to the Client ID section of the Jamf Connect ID's document.

135. Save the changes to the Jamf Connect ID's document.

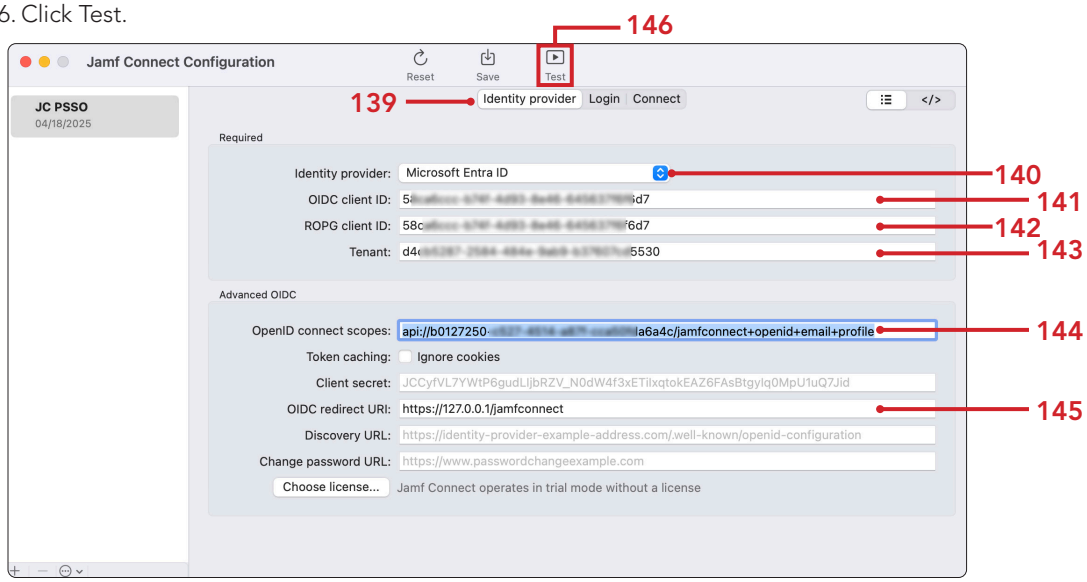


136. Confirm your Jamf Connect ID's document looks similar to the picture below.

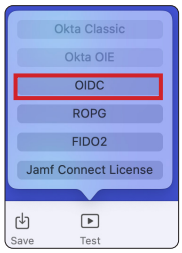


137. Let's create a Jamf Connect configuration profile with conditional access settings using the Jamf Connect Configuration App. Open the Jamf Connect Configuration App.
NOTE: We will only test OIDC and ROPG connections using the Jamf Connect Configuration app. This guide will not cover configuring a Jamf Connect profile for production use.

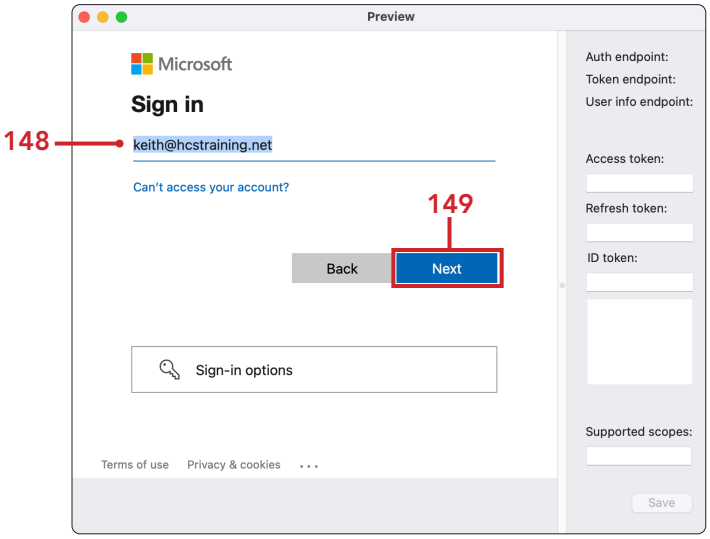
138. Enter a name for your profile. This guide will use JC PSSO.
139. If necessary, click Identity provider.
140. Select Microsoft Entra ID for Identity Provider.
141. Copy the Client ID from the Jamf Connect ID's file on your Desktop and paste it into the field for OIDC client ID.
142. Copy the Client ID from the Jamf Connect ID's file on your Desktop and paste it into the field for ROPG client ID.
143. Copy the Directory (tenant) ID from the Jamf Connect ID's file on your Desktop and paste it into the field for Tenant.
144. Copy the Application ID URI from the Jamf Connect ID's file on your Desktop and paste it into the field for OpenID connect scopes. Add this to the end: **/jamfconnect+openid+email+profile**
145. Enter **https://127.0.0.1/jamfconnect** for OIDC redirect URL.
146. Click Test.



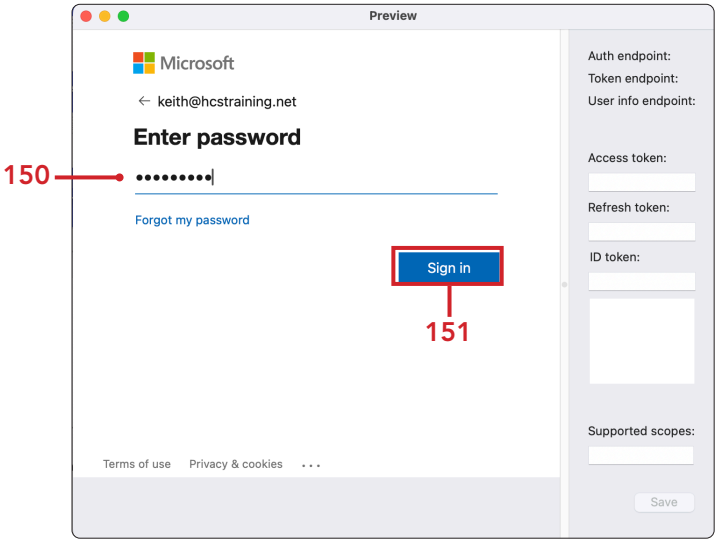
147. Select OIDC.



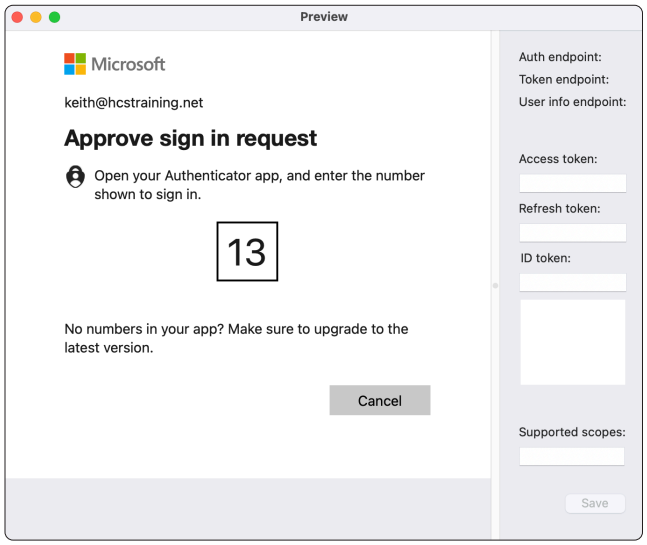
148. Enter your Microsoft Entra account name.
149. Click Next.



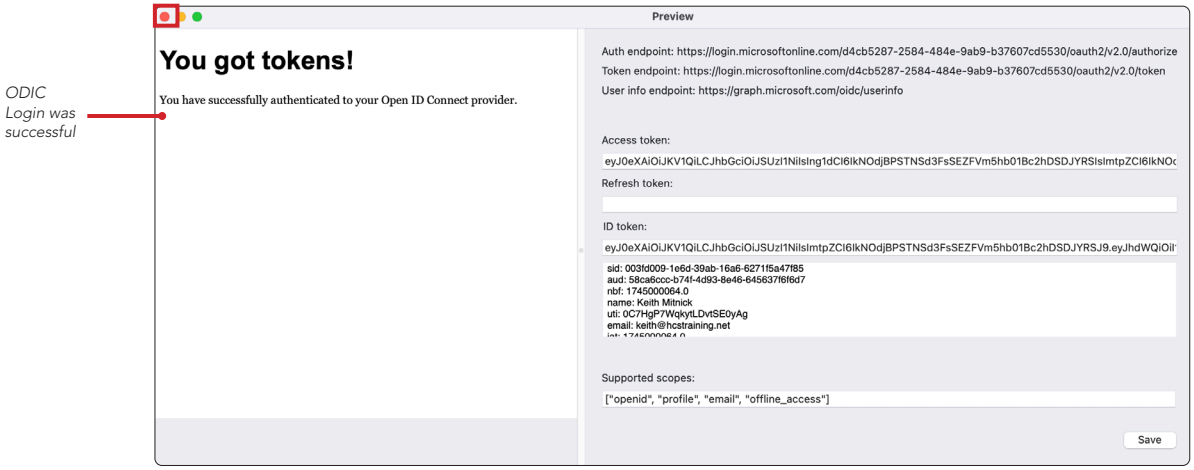
150. Enter your password.
151. Click Sign in.



152. Enter the code into Microsoft Authenticator on your device.

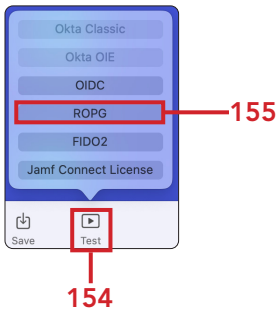


153. Confirm OIDC Login was successful. Click Close (⊗).



154. Click Test.

155. Select ROPG.

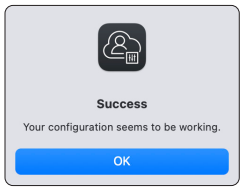


156. Enter your Microsoft Entra account name.

157. Enter your password.

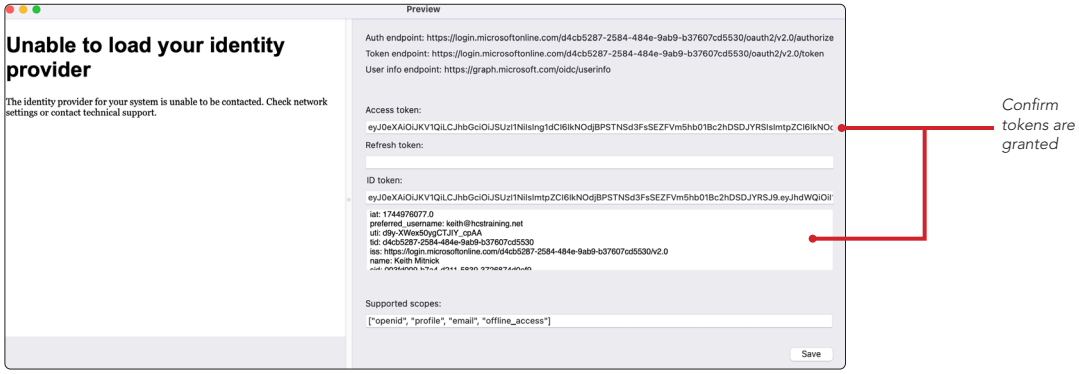
158. Click Sign in.

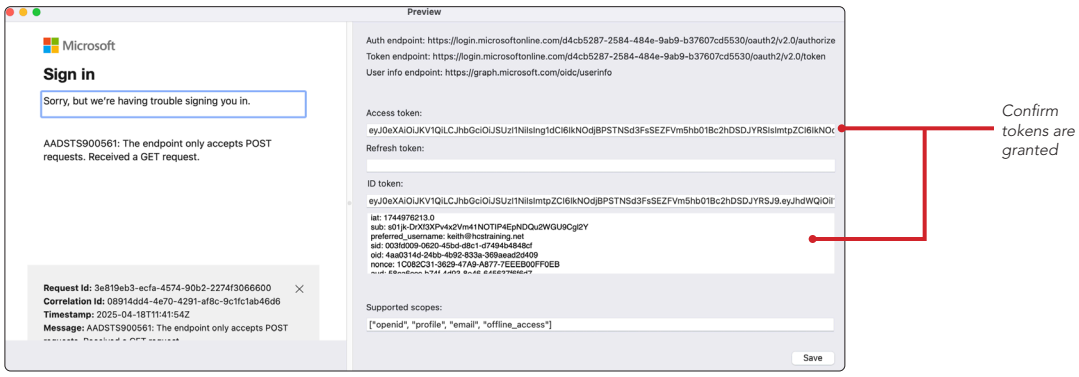
159. Confirm ROPG Login was successful.



NOTE: When testing to make sure your Microsoft Entra credentials work, we only need to test OIDC and ROPG connections using the Jamf Connect Configuration app. This guide will not cover configuring a Jamf Connect profile for production use.

160. There is a bug in the Jamf Connect Configuration application that will sometimes show an error message. If you see any of the errors listed below, as long as you see a tokens were granted, the connection was successful. Jamf is aware of this product issue.





This completes the guide.