Simplified Setup for Platform Single Sign-on for Mac (Jamf Pro + Intune)

Rev 20260901

Contents

Preface 3

Section 1: Update the Platform SSO configuration profile for Simplified Setup 5

Section 2: Configure the Jamf Pro PreStage Enrollment for Simplified Setup 11

Bonus Track A: Attended PreStage method for Simplified Setup using Jamf Pro 24

Bonus Track B: Authenticated Guest Mode with Microsoft Entra ID 66

Preface

What is Simplified Setup for Platform Single Sign-on for macOS (Platform SSO)?

Simplified Setup for Platform SSO is a macOS 26 feature that streamlines Automated Device Enrollment by pausing Setup Assistant for an identity provider (IdP) sign-in *before* the first local account is created. After the user authenticates with Microsoft Entra ID, macOS provisions the first account from the IdP token using the `TokenToUserMapping` dictionary. The user lands at the desktop already registered for Platform SSO, with no separate post-login registration prompt required.

Why this addendum exists

This addendum supplements the parent guide, How to Configure Jamf Pro and Intune Company Portal for macOS Platform SSO Integration, by adding three required keys to the existing Platform SSO configuration profile and configuring a PreStage Enrollment to enable the Setup Assistant pause. Before proceeding with this guide, you must first complete the steps outlined in the previous guide, as it covers most of the prerequisites and required steps needed to successfully follow this guide. The remaining sections of the parent guide (Microsoft Entra ID configuration, Microsoft Intune Company Portal deployment, registration verification) are unchanged. You don't need to redeploy Company Portal or rerun the Microsoft Entra MFA setup; you only need to update the Platform SSO profile and the PreStage Enrollment.

System Requirements:

Simplified Setup for Platform SSO requires *macOS 26+*. Mac computers running macOS 15 or earlier ignore the new keys and continue to honor the existing Platform SSO registration flow described in the parent guide.

This Addendum Covers

- Adding `EnableCreateFirstUserDuringSetup`, `EnableRegistrationDuringSetup`, and `UseSharedDeviceKeys` to the Platform SSO configuration profile created in the parent guide.
- Enabling **Simplified Setup for Platform Single Sign-on** in a Jamf Pro PreStage Enrollment and entering the **Platform Single Sign-on App Bundle ID**.
- Setting the **Account Settings** primary account type to `Standard Account` (or `Administrator Account`) and attaching the parent guide's configuration profiles.
- Adding the Microsoft Intune Company Portal installer (`CompanyPortal-Installer.pkg`) to the PreStage as an enrollment package.
- Verifying the end-to-end Simplified Setup experience on a fresh Mac computer with macOS 26+.

This guide was written using the following hardware and software:

NOTE: Simplified Setup keys live on the device channel of the single sign-on Extensions payload. If the parent guide's Platform SSO profile is scoped at the user level in Jamf Pro, recreate it at the computer level before following this addendum. `UseSharedDeviceKeys` is silently ignored on user-level profiles, and `EnableCreateFirstUserDuringSetup` depends on it.

NOTE: Known issue: pin Company Portal to `5.2604.0` or later. Microsoft Company Portal version `5.2603.0` contains a defect that, when combined with `EnableCreateFirstUserDuringSetup` or `EnableCreateUserAtLogin`, produces an unescapable Microsoft sign-in pane at Setup Assistant that accepts no credentials. The only recovery is a DFU restore. Microsoft fixed this in `5.2604.0` (released 2026-05-13), which is also the first build with formal Microsoft support for Entra ID Platform SSO during Automated Device Enrollment. Never deploy `5.2603.0` alongside the Simplified Setup keys. Direct download: Company Portal for macOS download (Microsoft).

- Microsoft Entra ID with the Microsoft Enterprise SSO plug-in
- Jamf Pro (Cloud Hosted) 11.20 or later with administrator credentials. The attended workflow in Bonus Track A requires Jamf Pro 11.29 or later.
- Microsoft Intune Company Portal installer `5.2604.0` or later (`CompanyPortal-Installer.pkg`)
- A test Mac computer running macOS 26+ enrolled in Apple Business Manager or Apple School Manager.

Section 1: Update the Platform SSO configuration profile for Simplified Setup

What You'll Need:

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

Hardware and Software:

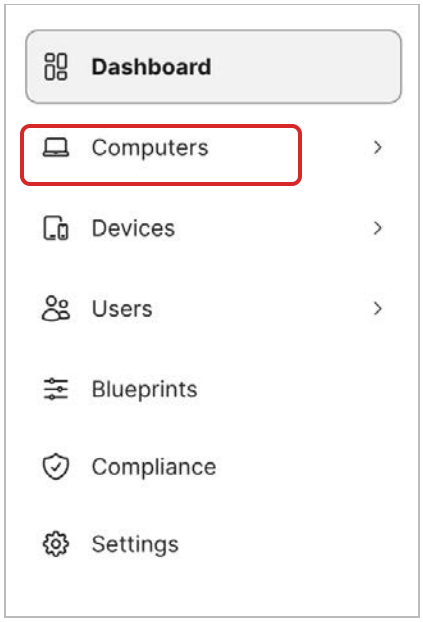
Requirements for following along with this section:

- Administrative access to your Jamf Pro server.
- The existing computer-level Platform SSO configuration profile created in the parent guide.
- A test Mac computer running macOS 26+ to verify the configuration.
- PlatformSSO.plist, adding the app allow-list and Platform SSO keys Microsoft documents for the Enterprise SSO Extension:
  platformSSO.plist reference (HCS GitHub)

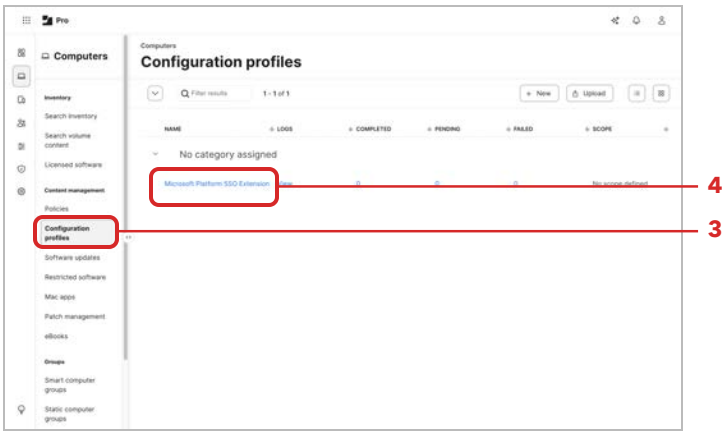
NOTE: The three required keys are added to the *existing* Single Sign-On Extensions profile. Do not create a second profile. Only one Single Sign-On Extensions payload may apply to a Mac computer, and a duplicate produces conflicting registrations and silent authentication failures.

In this section, you will edit the existing Platform SSO configuration profile to add the three keys that activate Simplified Setup. The keys are described below in the order they should be enabled, followed by a save and redistribution step.

1. If necessary, sign in to your Jamf Pro server with administrative credentials.
2. Click the **Computers** button.

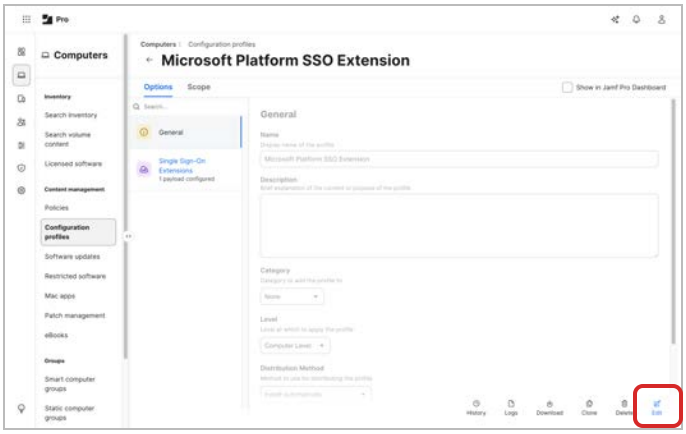


3. Click **Configuration Profiles**.

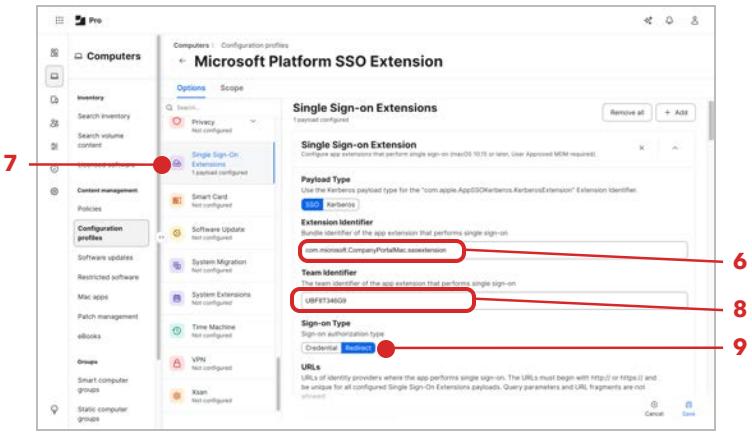


4. Click the existing **Platform SSO** configuration profile (the one created in the parent guide).

5. Click the Edit button.



6. Scroll to the **Single Sign-On Extensions** payload.

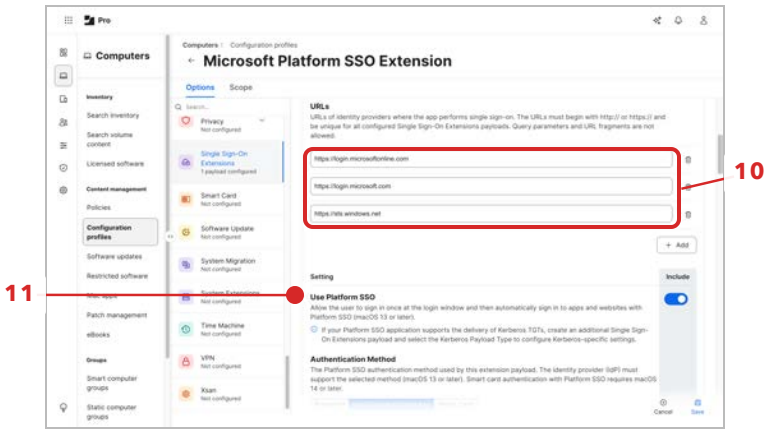


7. Confirm **Extension Identifier** is `com.microsoft.CompanyPortalMac.ssoextension`.

8. Confirm **Team Identifier** is `UBF8T346G9`.

9. Confirm **Type** is `Redirect`.

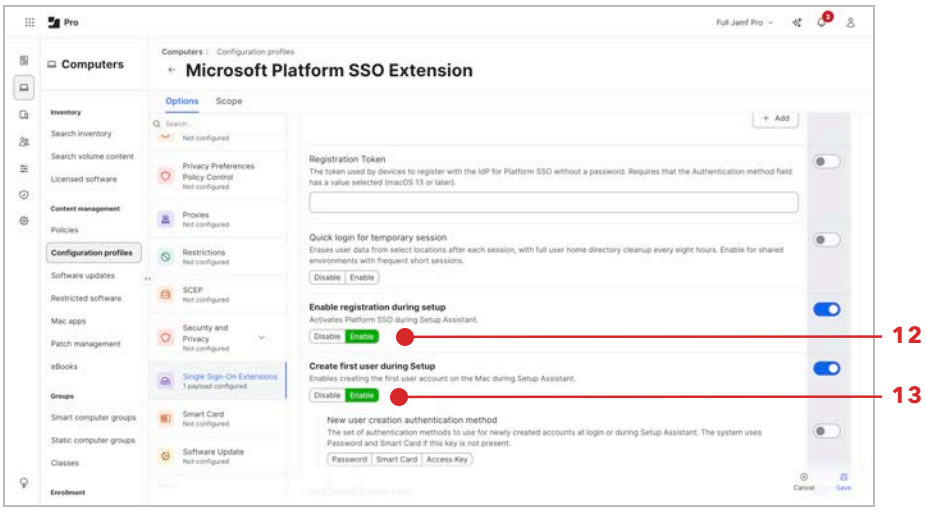
10. Confirm the three Microsoft URLs are present: `https://login.microsoftonline.com`, `https://login.microsoft.com`, and `https://sts.windows.net`.



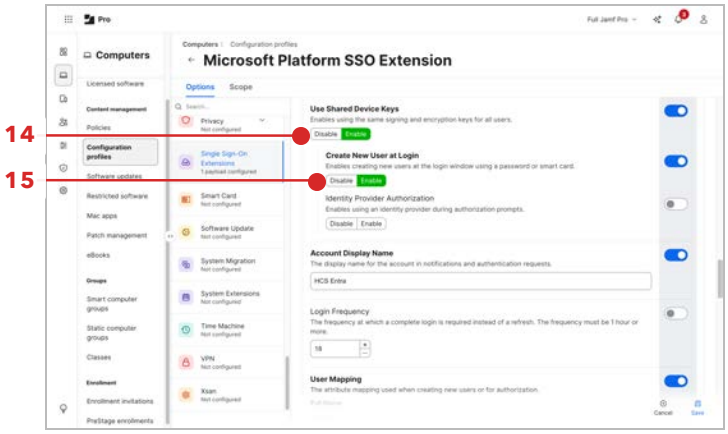
11. Find the **Platform SSO** section of the payload and verify it is Enabled.

12. Slide **Enable Registration During Setup** to ON and set the key to `Enable`.

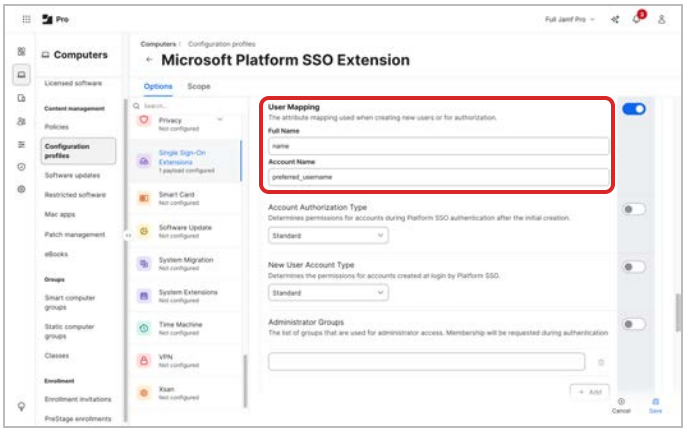
13. Slide **Enable Create First User During Setup** to ON and set the key to `Enable`.



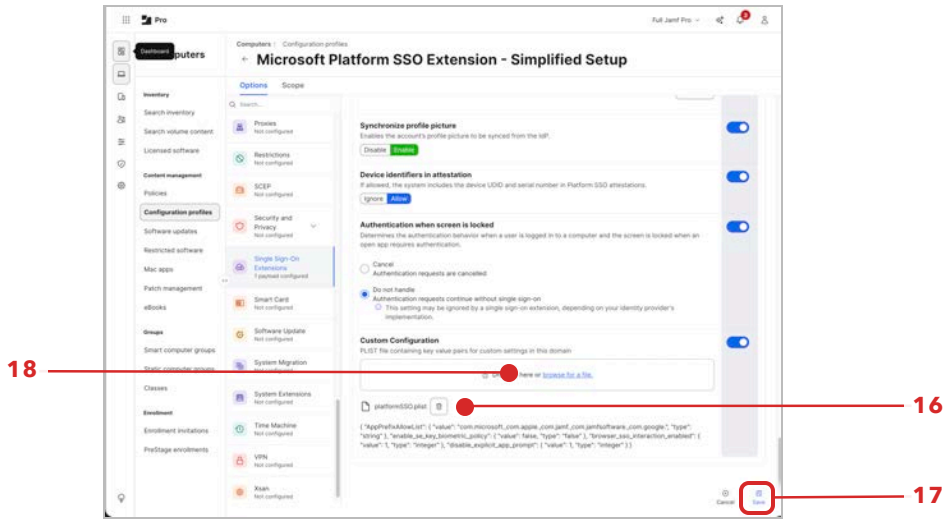
14. Slide **Use Shared Device Keys** to ON and set the key to `Enable`.



15. Under user mapping for the **full name** type `name` and **account name** `preferred_username`



16. Remove the PlatformSSO.plist you downloaded earlier in this section.



17. Upload the configuration profile you downloaded earlier.

18. Click the Save button.

This completes this section. In the next section, **Configure the Jamf Pro PreStage Enrollment for Simplified Setup**, you will build the PreStage Enrollment that pauses Setup Assistant for the Microsoft Entra ID sign-in and creates the first account from that identity.

Section 2: Configure the Jamf Pro PreStage Enrollment for Simplified Setup

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:

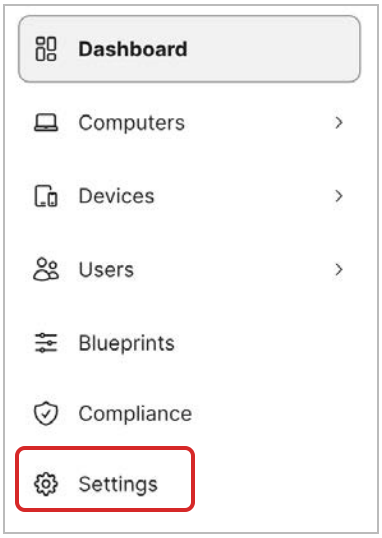
- Administrative access to your Jamf Pro server.
- An existing PreStage Enrollment scoped to the relevant automated device enrollment instance.
- Microsoft Intune Company Portal installer CompanyPortal-Installer.pkg (or later), uploaded to Jamf Pro. **The App Store version of Company Portal will not function with Simplified Setup.**

  Company Portal for macOS download (Microsoft)
- The updated Platform SSO configuration profile from Section 1.
- A test Mac running macOS 26+ enrolled in Apple Business and assigned to the PreStage Enrollment.

NOTE: The Simplified Setup feature is documented in *Jamf Pro Management – Automated Device Enrollment for Computers*. Only computers running macOS 26 or later honor the Simplified Setup PreStage settings; earlier macOS versions enroll using the standard ADE flow described in the parent guide.
https://learn.jamf.com/en-US/bundle/jamf-pro-documentation-current/page/Automated_Device_Enrollment_for_Computers.html

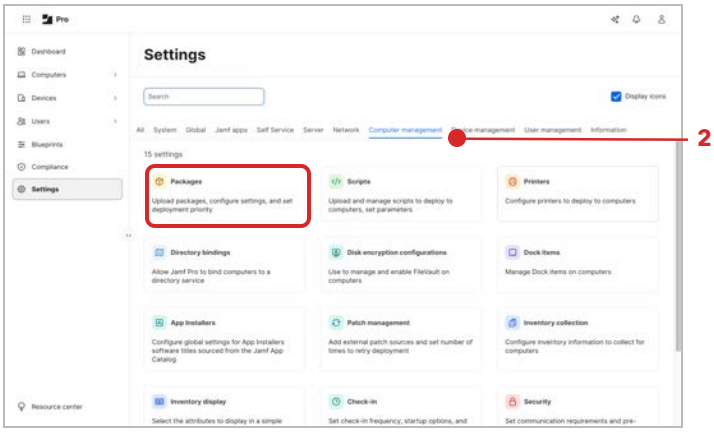
In this section, you will enable Simplified Setup on a PreStage Enrollment, add the Platform SSO configuration profile and the Microsoft Intune Company Portal package, set the primary account type, and verify the end-to-end experience on a test Mac computer.

1. In Jamf Pro, click **Settings** in the sidebar.

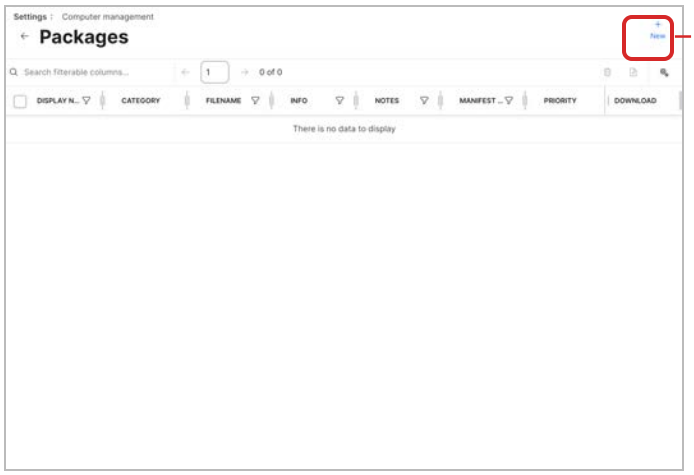


> **Note:** Before we can test Platform SSO with simplified setup we need to upload the PKG for Microsoft Intune Company Portal.

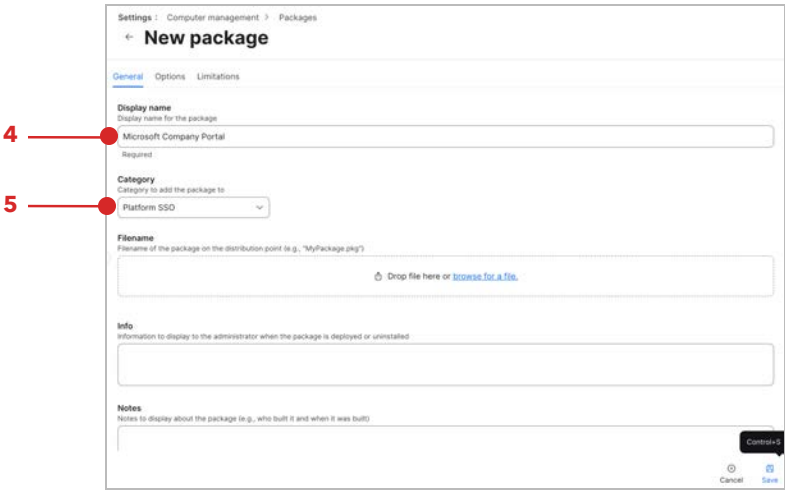
2. Under **Computer Management**, choose **Packages**.



3. Click **New**.

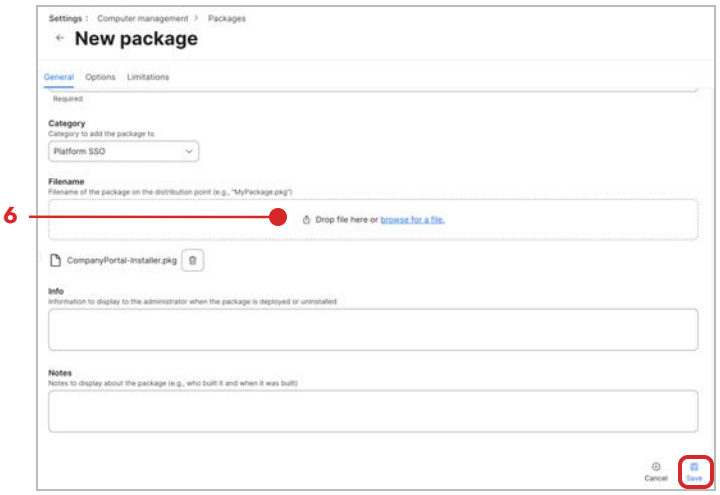


4. In the **Display Name** field, enter `Microsoft Company Portal`.



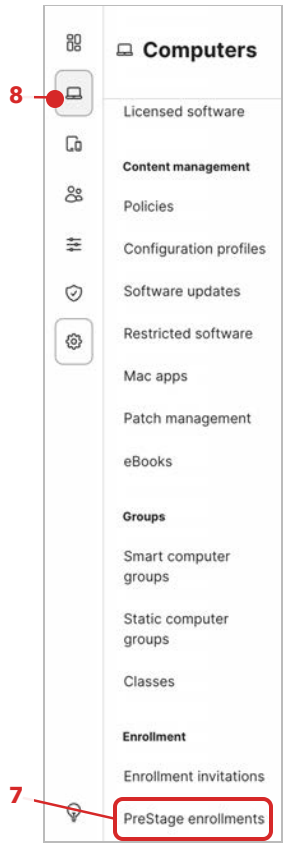
5. Select **Platform SSO** as the category that we created in the parent guide.

6. Click **Browse for a File**, select the `CompanyPortal-Installer.pkg` you downloaded, then click **Save**.



> **Note:** The Company Portal installer must be version `5.2604.0` or later. **Do not use** `5.2603.0`. It corrupts Setup Assistant when paired with the Simplified Setup keys (see the version pin in the preface note).

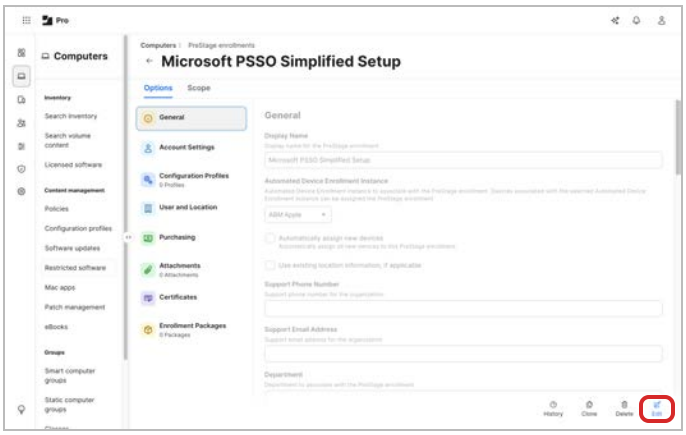
7. Click the Computers button.



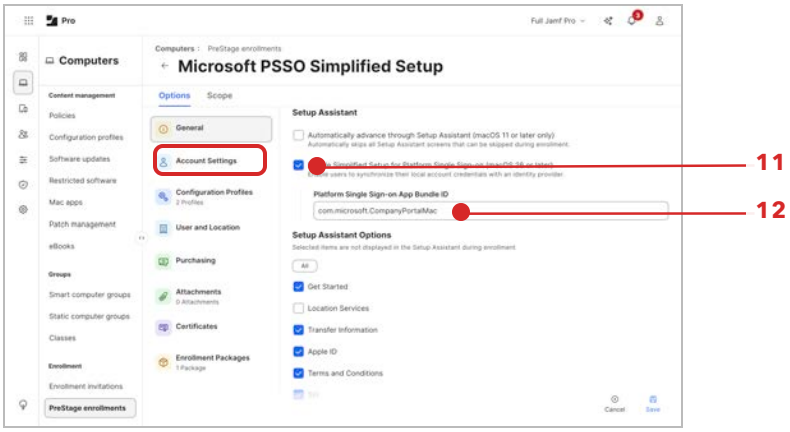
8. Click the **PreStage Enrollments** button.

9. Select the PreStage Enrollment you want to update.

10. Click **Edit**.



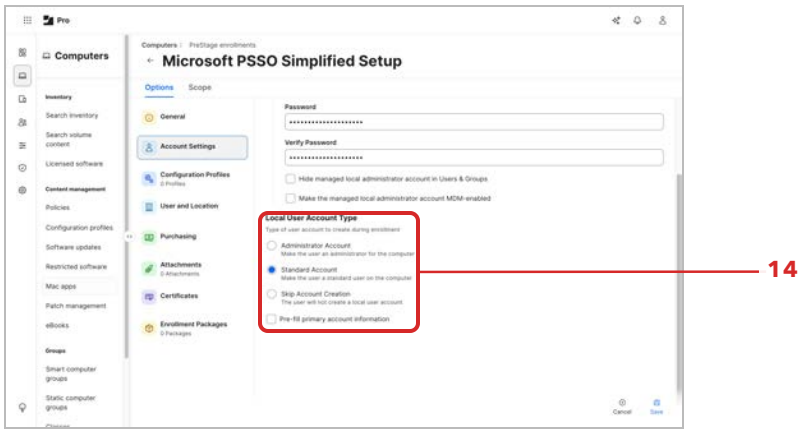
11. In the **General** pane, select the **Enable Simplified Setup for Platform single sign-in** checkbox.



12. In the **Platform Single Sign-on App Bundle ID** field, enter `com.microsoft.CompanyPortalMac`.

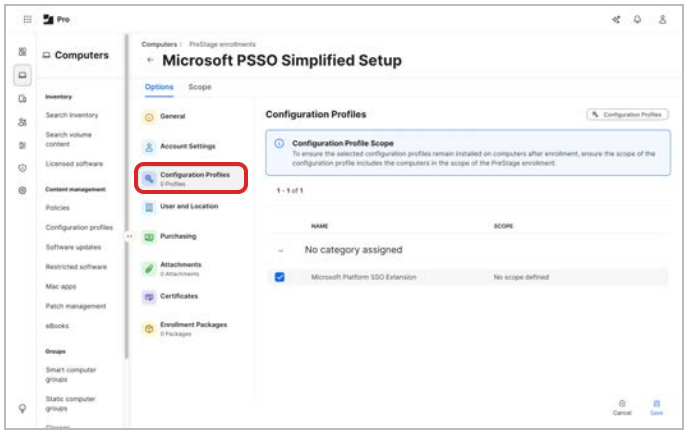
13. Click the **Account Settings** pane.

14. For your local account type, select **Standard Account** (or **Administrator Account**, depending on your organization's policy).



> **Note:** Don't click **Skip Account Creation** for Simplified Setup. **Skip Account Creation** is reserved for environments using a different solution (for example, *Jamf Connect*) to provision the primary user, and selecting it prevents Simplified Setup's account-creation step from running.

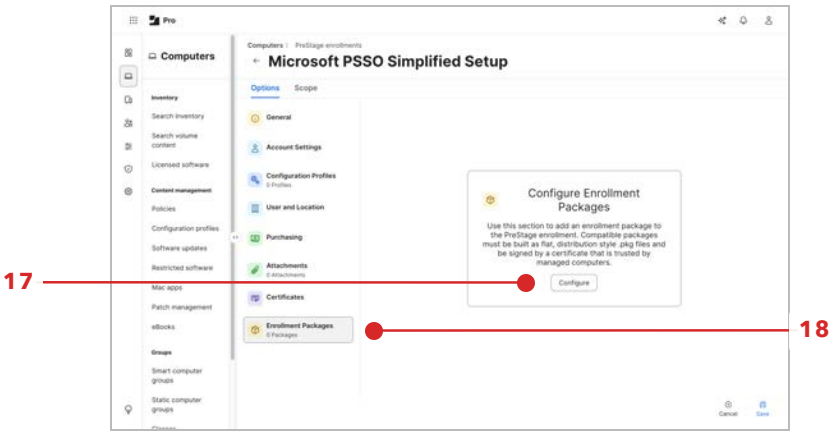
15. Click the **Configuration Profiles** pane.



16. Confirm that the updated Platform SSO configuration profile from Section 1 is selected, along with any supporting profiles (for example, the Wi-Fi profile from the parent guide).

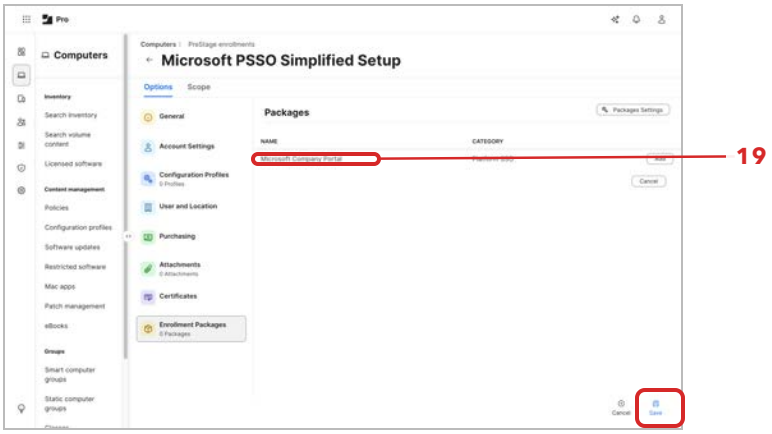
> **Note:** PreStage-scoped configuration profiles are delivered to the device *before* the Setup Assistant IdP sign in pane appears, which is required for Simplified Setup to function.

17. Click the **Enrollment Packages** button.



18. Click **Configure**.

19. Select the Microsoft Intune Company Portal installer `(CompanyPortal-Installer.pkg)` then click **Add**.

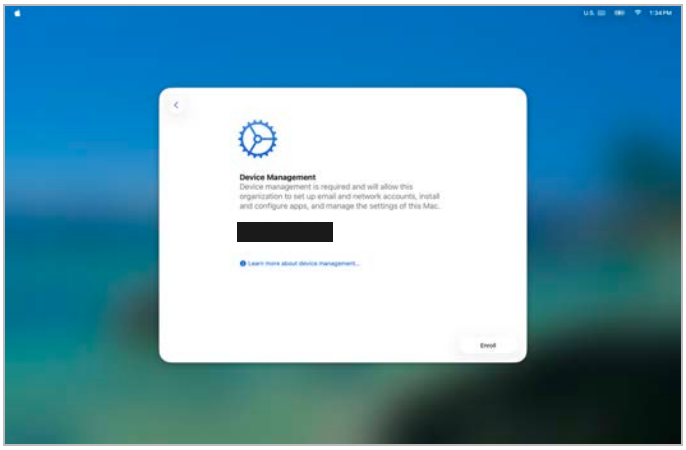


20. Click the Save button to commit the PreStage Enrollment.

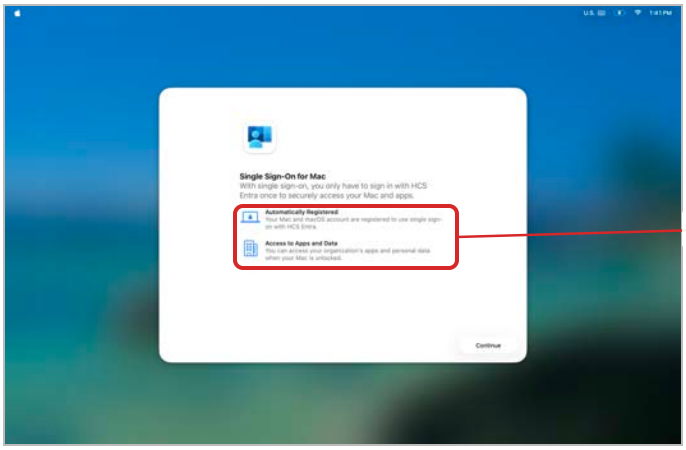
> **Note:** **The Mac App Store version of Company Portal will not function with Simplified Setup.** The package attached here must be the device-management-deployable Company Portal build documented at Install Company Portal for macOS as a macOS PKG app.
> Add the Company Portal app for macOS (Microsoft Intune documentation)

21. Power on your Mac and proceed through **Setup Assistant**.

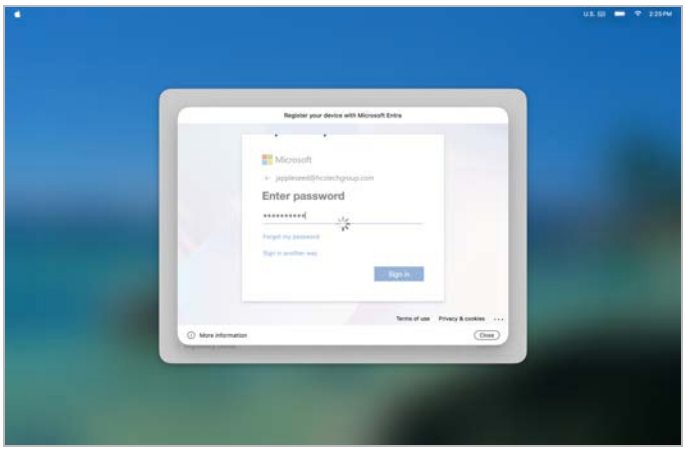
22. When the **Device Management** dialog appears, confirm the Mac is owned by your organization and click **Enroll**.



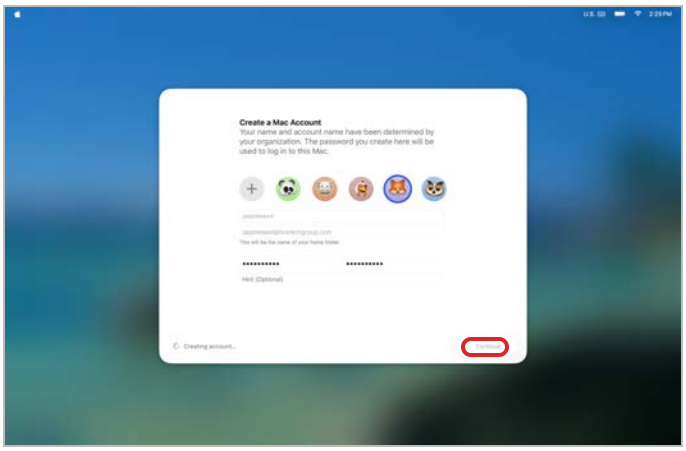
23. On the **Single Sign-On on Mac** screen, review the two features Simplified Setup grants: **Automatically Registered** and **Access to Apps and Data**, then click the **Continue** button.



24. At the **sign-in** sheet, enter your Microsoft Entra email and password, then click **Sign in** (or: press Enter).

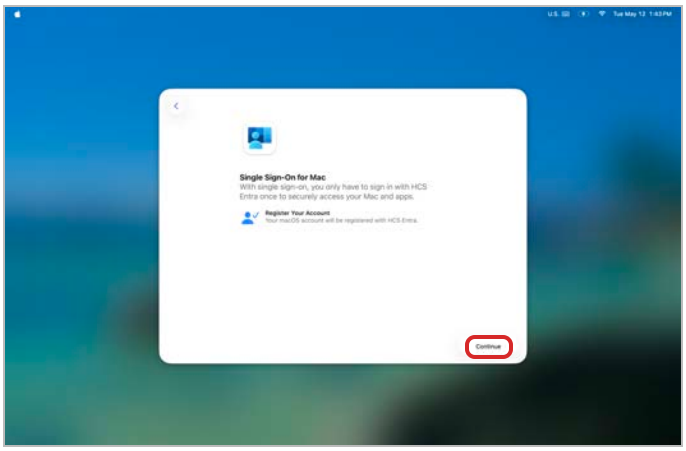


25. On the **Create a Mac Account** screen, set a local **Password**, then click **Continue**.

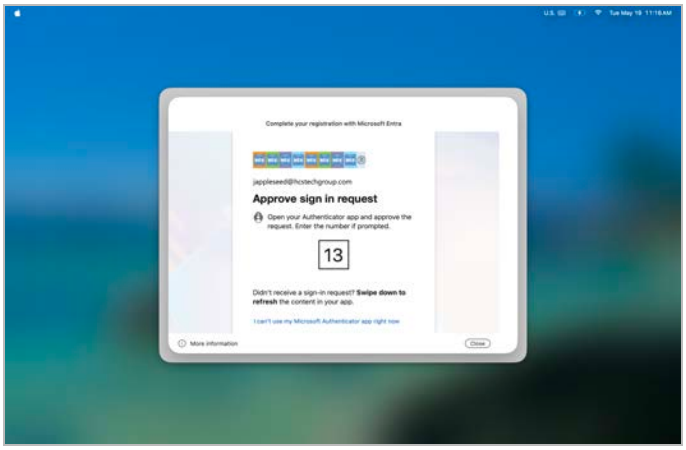


26. Setup Assistant returns to **Single Sign-On in macOS** with only the **Register Your Account** feature. The macOS account already exists, so all that's left is registering it with your Entra.

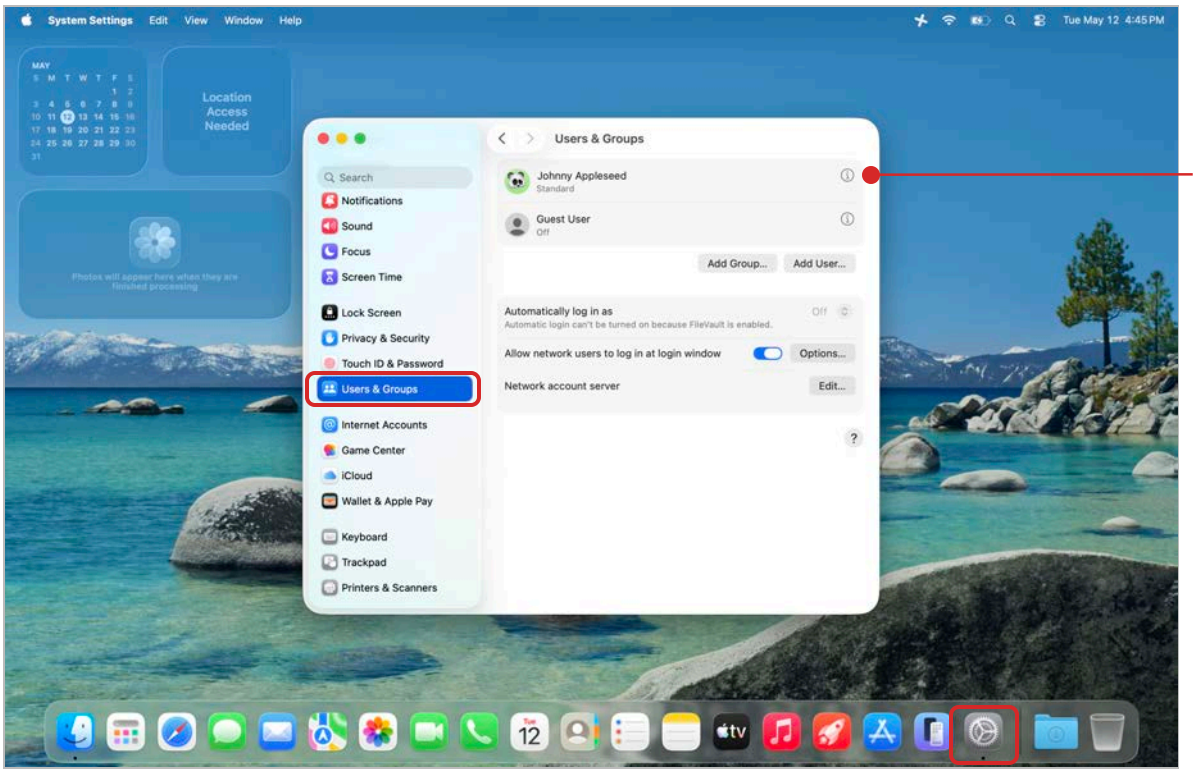
Click **Continue**.



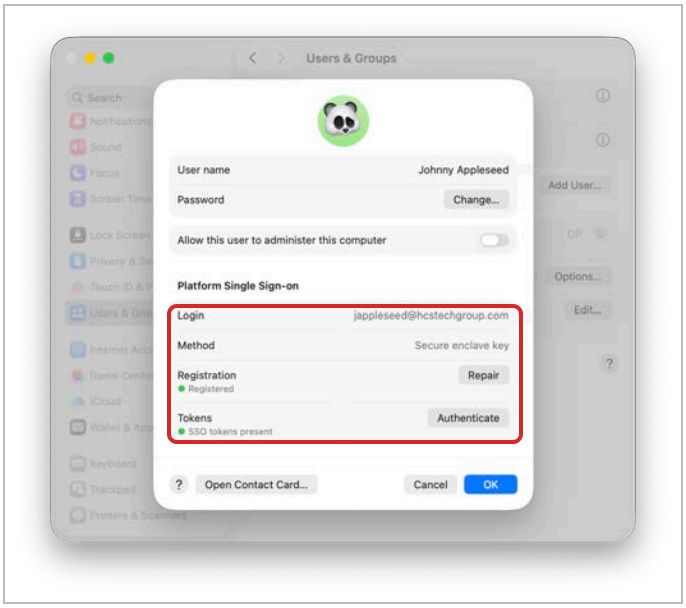
27. macOS prompts to authorize the registration with **HCS Entra**. Sign in with the **Authenticator app**, or click the **Use Password** button to fall back to your **Entra** password.



28. After Setup Assistant completes, open **System Settings > Users & Groups** and confirm the new **Platform SSO** account appears as a Standard user. Click the **info** button next to the Platform SSO user.



29. Now confirm the four end-to-end indicators in the **Platform Single Sign-on** section: **Sign in** is the user's Entra UPN, **Method** is **Secure enclave key**, **Registration** is **Registered**, and **Tokens** is **SSO tokens present**.



> **Note:** The two addenda that follow are optional. Bonus Track A covers the attended PreStage method for Simplified Setup, where the Platform SSO profile installs before enrollment. Bonus Track B covers Authenticated Guest Mode with Microsoft Entra ID.

This completes this section. In the next section, **Attended PreStage method for Simplified Setup using Jamf Pro**, you will configure the alternate workflow where the Platform Single Sign-on profile installs before enrollment completes.

Bonus Track A

Attended PreStage method for Simplified Setup using Jamf Pro

Bonus Track A: Attended PreStage method for Simplified Setup using 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 Bonus Track:

- Jamf Pro 11.29 or later for the attended workflow method. The unattended workflow method has been available since Jamf Pro 11.20.
- A test Mac computer running macOS 26 or later that you can erase.
- The updated Platform SSO configuration profile from Section 1 and the PreStage Enrollment you configured in Section 2.
- The signed Microsoft Intune Company Portal installer (`CompanyPortal-Installer.pkg` , version `5.2604.0` or later) uploaded to Jamf Pro and added to the PreStage Enrollment's **Enrollment Packages** payload, as in Section 2. During the attended workflow macOS downloads and installs the package automatically.
- Administrator privileges to your Jamf Pro instance and to your Microsoft Entra tenant, including privileges to configure single sign-on in both. This Bonus Track configures the SAML-based single sign-on the attended workflow method requires.

NOTE: Jamf recommends first validating your Platform SSO configuration profile using the unattended workflow, which enforces Platform SSO registration after enrollment. This lets you use a device erase command to reset and retest if an error occurs. Validate the unattended workflow first, then move to attended only if you need the profile in place before enrollment.

Key Differences Between Attended and Unattended Modes

Simplified Setup streamlines enrollment by enabling Platform SSO registration and account creation inside Setup Assistant during Automated Device Enrollment. Jamf Pro now offers two workflow configurations, selected with the **Set workflow method** pop-up menu in the **General** payload of a PreStage Enrollment. Section 2 of this guide configured the unattended method. The attended method is new in Jamf Pro 11.29.

Unattended (SSOe profile installs during enrollment)

The Mac computer enrolls, then Jamf Pro keeps it in Setup Assistant until the Company Portal app and its configuration profiles install. macOS begins the required Platform SSO registration on the next Setup Assistant screen, and the first user account is created from the authenticated identity. You identify the registration app with its **bundle ID** (Microsoft Company Portal is `com.microsoft.CompanyPortalMac`), and the app arrives through the **Enrollment Packages** payload. No manifest URL is involved.

Attended (SSOe profile installs before enrollment)

When the Mac computer attempts to enroll, Jamf Pro returns a 403 response that rejects enrollment until Platform SSO registration is complete. The 403 includes secured download links for the Platform SSO configuration profile and the Company Portal app package, which macOS downloads and installs automatically. The Mac computer prompts the user to register, then sends an authentication token to Jamf Pro, which verifies it against the server's SAML SSO integration and authorizes enrollment. Requires a Platform SSO configuration profile selected in the PreStage Enrollment and SAML-based SSO configured for end users in Jamf Pro. Jamf also notes that enrollment customizations cannot be used with the attended workflow method.

Jamf recommends validating your Platform SSO configuration with the unattended workflow method before you switch to attended, because unattended does not depend on SAML. That validation is the subject of the earlier sections of this guide. This Bonus Track picks up from a working unattended setup and covers only what attended adds.

NOTE: Nothing about the attended workflow requires you to host or point at a package manifest. Jamf Pro rejects the first enrollment attempt with a 403 response carrying secured download links for the Platform SSO configuration profile and the Company Portal app package, and macOS downloads and installs both automatically before prompting the user to register.

The SAML prerequisite comes first

The attended workflow method will not work, and the PreStage Enrollment will not save with attended selected, until SAML-based single sign-on is configured for end users in Jamf Pro.

The reason is the way the attended handshake ends: the Mac computer completes Platform SSO registration, sends an authentication token to Jamf Pro, and Jamf Pro validates that token against its SAML SSO integration before it authorizes enrollment.

No SAML integration means nothing to validate the token against, and the 403 gate never opens. That is why this Bonus Track starts there. If your Jamf Pro already has SAML SSO configured for end users, the first phase is a two-minute check and you move on.

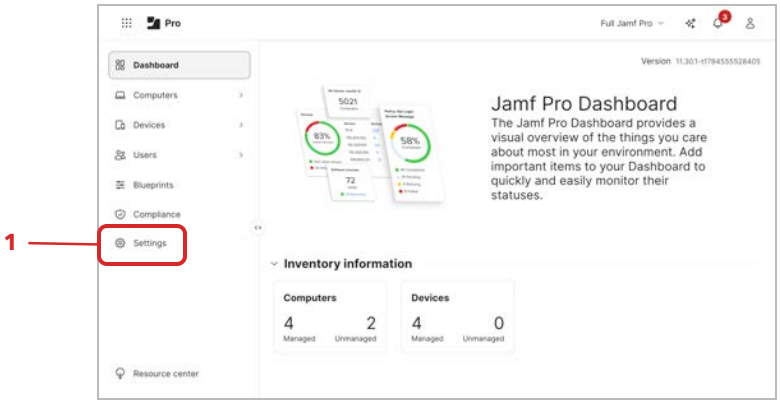
NOTE: Jamf splits the two kinds of SSO. Jamf Pro Management recommends OIDC-based SSO through Jamf Account for administrators, and states: "You can enable OIDC-based SSO in Jamf Account for administrators alongside SAML-based SSO in Jamf Pro for end users." The attended workflow method needs the end-user SAML side. You do not have to move your administrators behind SAML to use it.
SAML-Based Single Sign-On (Jamf Pro documentation)

In this Bonus Track, we will:

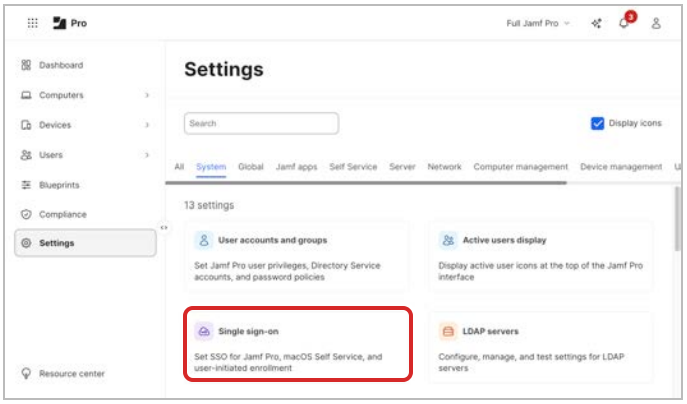
- Check whether SAML-based single sign-on for end users is already configured in Jamf Pro, and configure it with Microsoft Entra ID if it is not.
- Configure the attended workflow method: SAML SSO and the selected configuration profile.
- Test an attended enrollment end to end and cover recovery if a Mac computer is stuck in Setup Assistant.
- Verify Platform SSO by signing in to Microsoft 365 in Safari without entering a password.

Check whether SAML SSO is already configured in Jamf Pro

1. In Jamf Pro, click **Settings** in the sidebar.



2. In the **System** section, click **Single sign-on**.

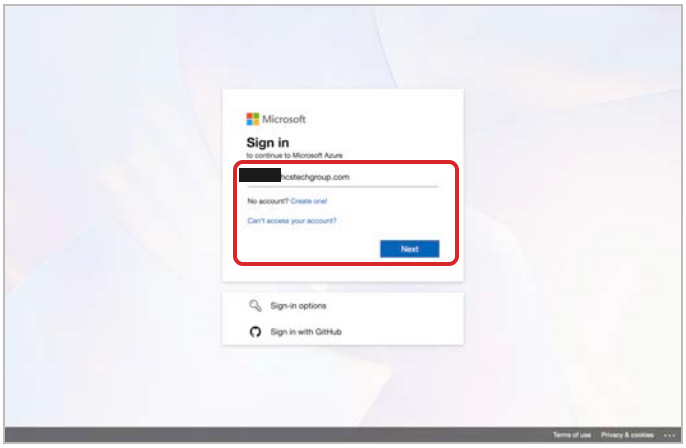


3. Confirm whether **Enable SSO Authentication** is already selected and Microsoft Entra ID is the configured **Identity Provider**. If it is, skip ahead to step 66. If it is not, continue with the next step.

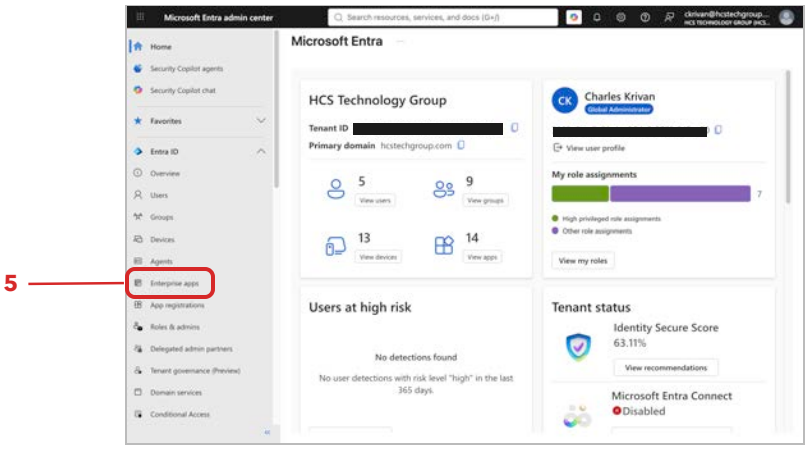
> **Note:** The attended workflow requires a Platform SSO configuration profile selected in the PreStage Enrollment and SAML-based SSO configured for end users in Jamf Pro. Without SAML SSO configured, the Mac computer cannot clear the 403 response Jamf Pro returns during enrollment until Platform SSO registration completes; that flow is covered later in this section. Jamf Pro Management lists "Jamf Pro user accounts or groups with matching IdP usernames or groups" as a prerequisite for enabling SAML SSO, and matches the incoming user first by user account, then by group name. If a directory service is integrated with Jamf Pro, add the directory users or groups you want to use for SSO as standard Jamf Pro users or groups first, under **Settings ▸ Jamf Pro User Accounts & Groups**.
> Configuring Simplified Setup for Platform Single Sign-on (Jamf Pro documentation)

Add the Jamf Pro app in Microsoft Entra ID

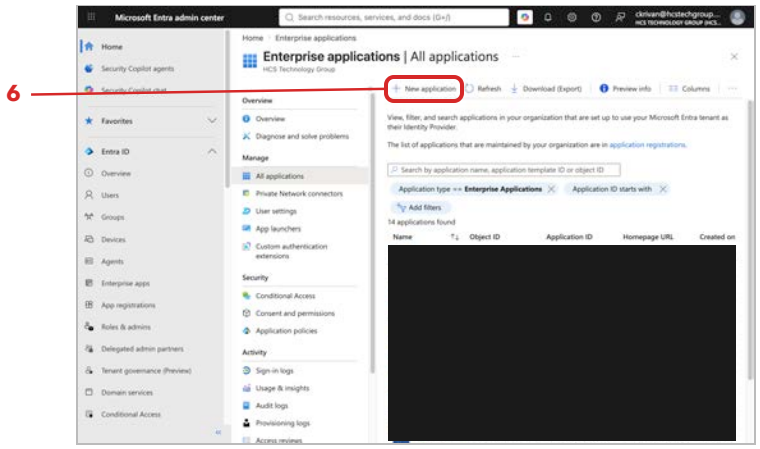
4. Sign in to the Microsoft Entra admin center as an **Application Administrator**, **Cloud Application Administrator**, or **Application Owner**.
   https://entra.microsoft.com
   https://learn.microsoft.com/en-us/entra/identity/saas-apps/jamfprosamlconnector-tutorial



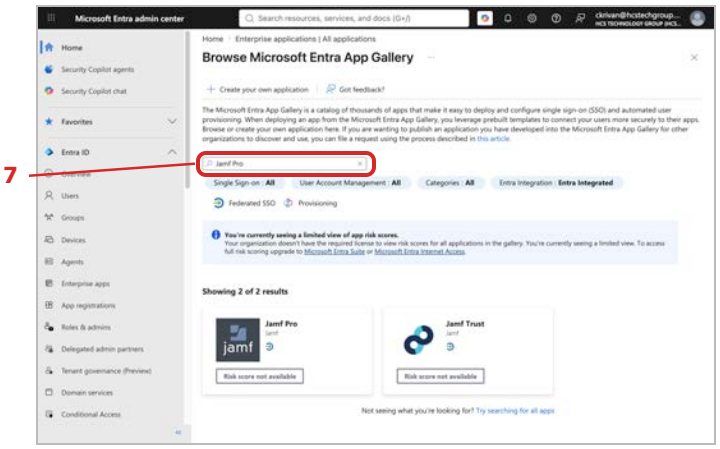
5. Click **Entra ID ▸ Enterprise apps**.



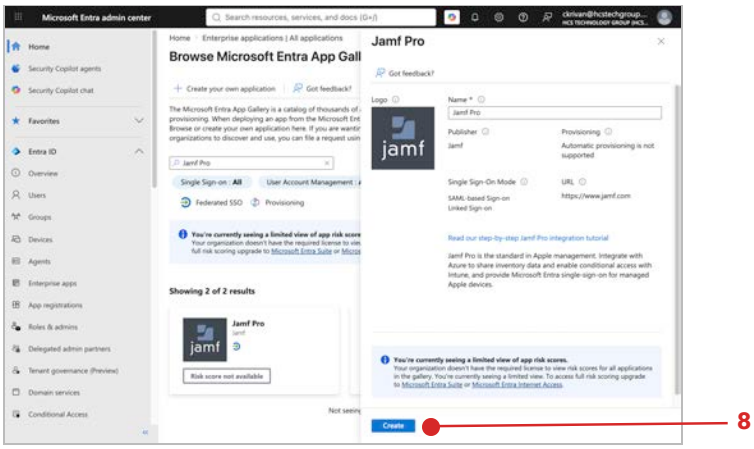
6. Click **New application**.



7. In the **Add from the gallery** section, enter `Jamf Pro` in the search box.

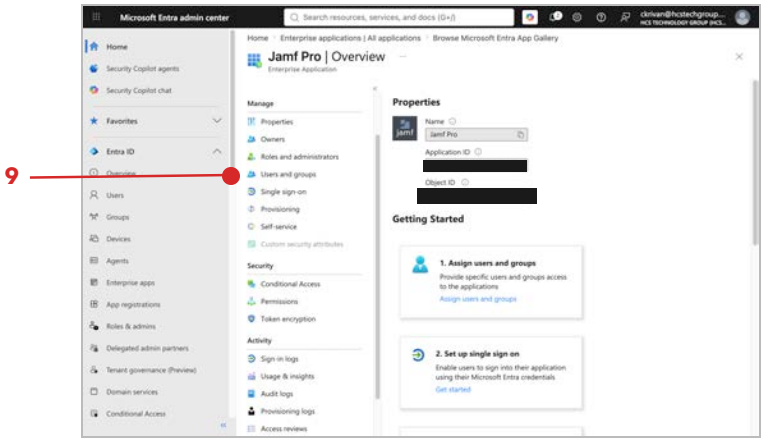


8. Select **Jamf Pro** from the results panel, then create the app.

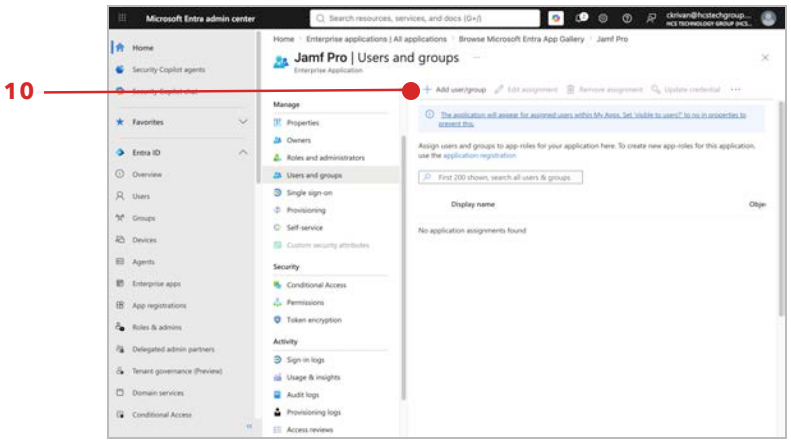


> **Note:** Wait a few seconds while the app is added to your tenant.
> Microsoft Entra SSO integration with Jamf Pro (Microsoft Learn)

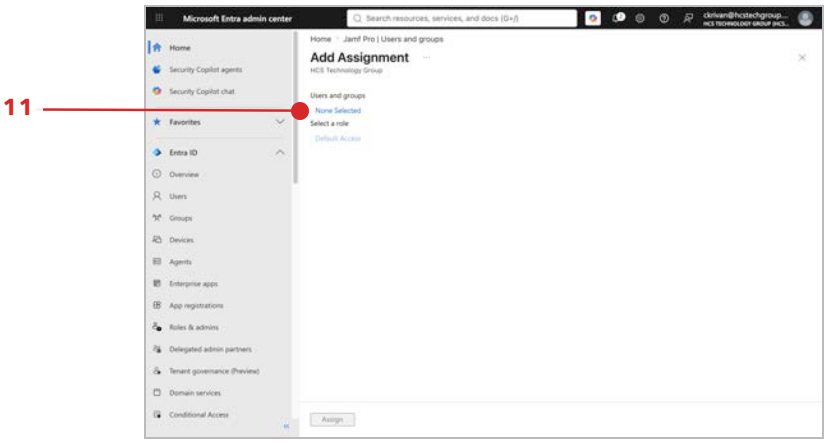
9. In the **Manage** section, click **Users and groups**.



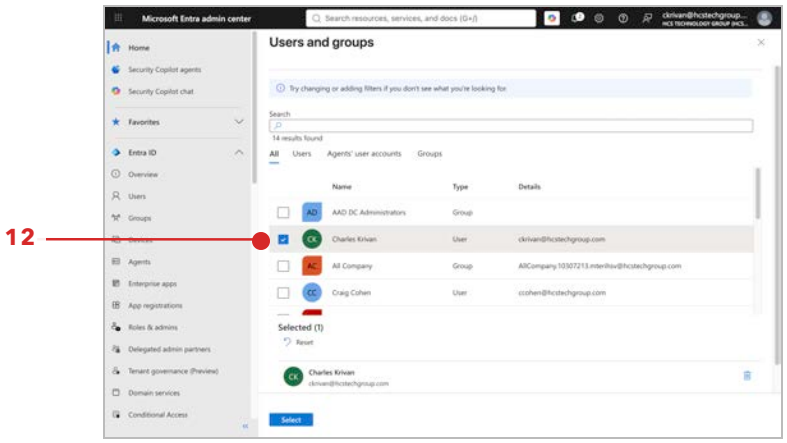
10. Click **Add user/group**.



11. Click Users and Groups > None Selected

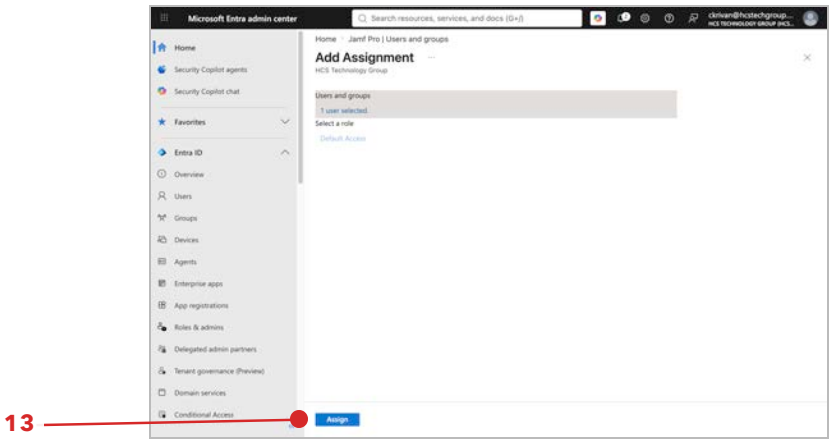


12. Assign the users or groups that need end-user access to Jamf Pro and click select.

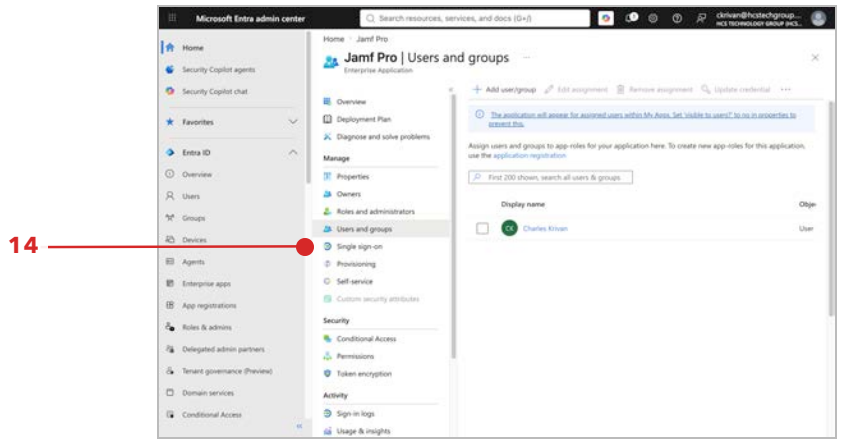


> **Note:** Jamf Pro Management lists "Jamf Pro user accounts or groups with matching IdP usernames or groups" as a prerequisite for enabling SAML SSO, and matches the incoming user first by user account, then by group name. Enabling Single Sign-On in Jamf Pro (Jamf Pro documentation)

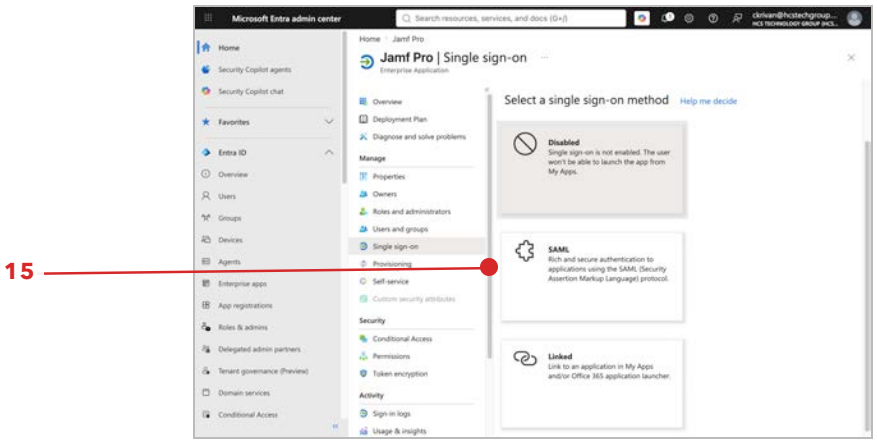
13. Click **Assign**.



14. In the **Manage** section, click **Single Sign-On**.

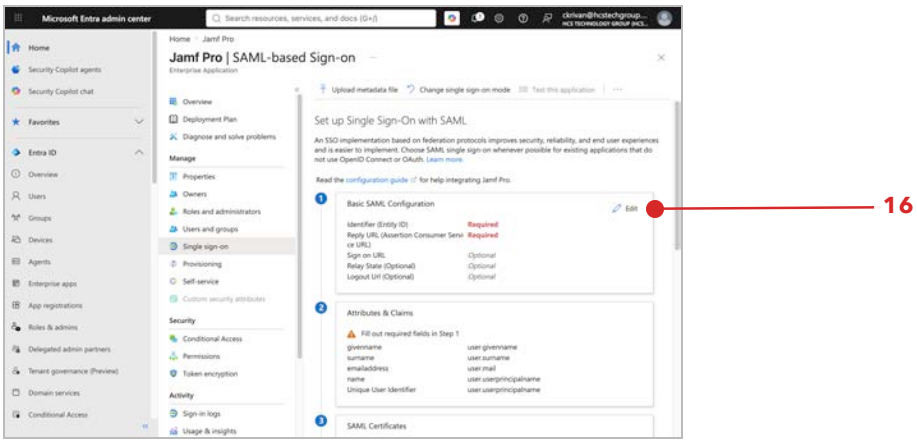


15. On the **Select a Single Sign-On Method** page, select **SAML**.

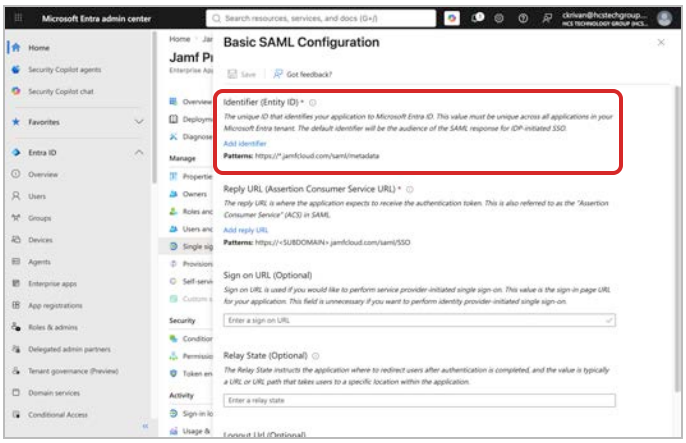


> **Note:** Microsoft Learn states that Jamf Pro supports SP-initiated and IdP-initiated SSO.
> Microsoft Entra SSO integration with Jamf Pro (Microsoft Learn)

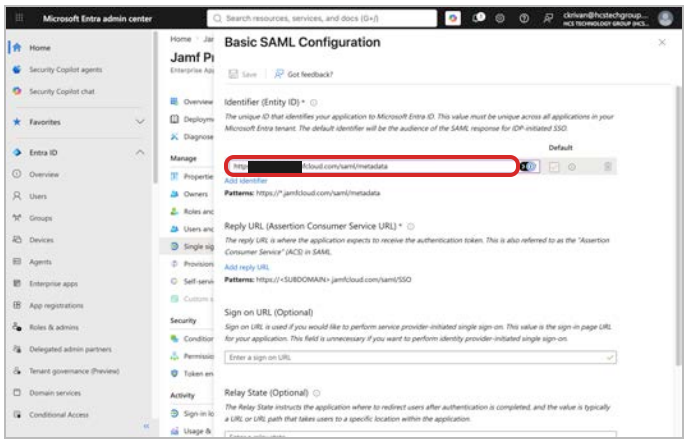
16. On the **Set up Single Sign-On with SAML** page, click the pencil icon for **Basic SAML Configuration**.



17. Click **Add identifier.**

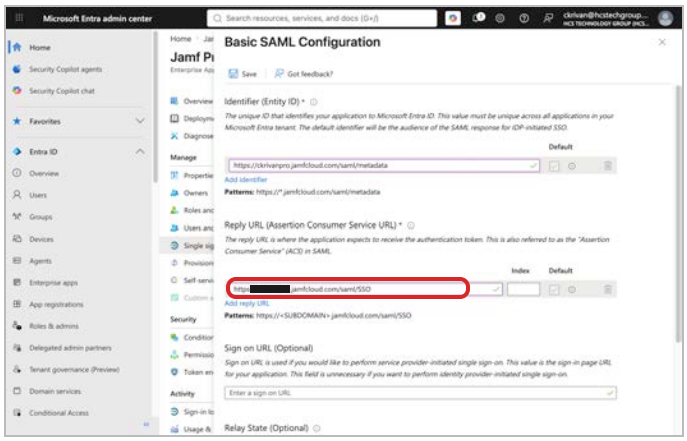


18. In the **Identifier** field, enter `https://<subdomain>.jamfcloud.com/saml/metadata`, replacing `<subdomain>` with your own Jamf Pro subdomain.



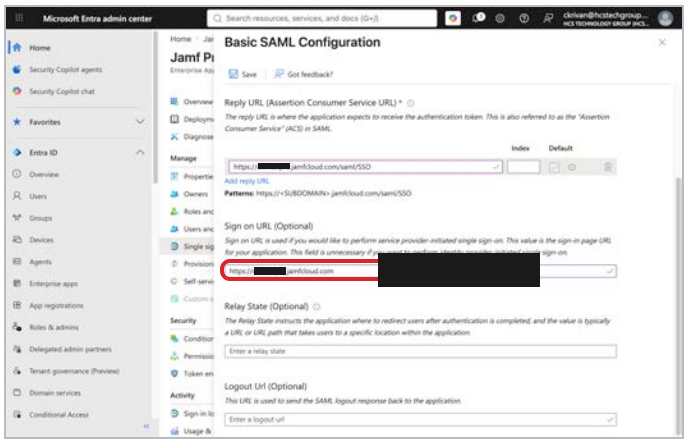
> **Note:** This value has to match the **Entity ID** Jamf Pro shows on its **Single sign-on** settings page, which you confirm in the next phase. Microsoft Learn notes you can extract the subdomain from that Entity ID value and reuse it for the reply URL and the sign-on URL.
> Microsoft Entra SSO integration with Jamf Pro (Microsoft Learn)

19. In the **Reply URL** field, enter `https://<subdomain>.jamfcloud.com/saml/SSO`, replacing `<subdomain>` with your own Jamf Pro subdomain.



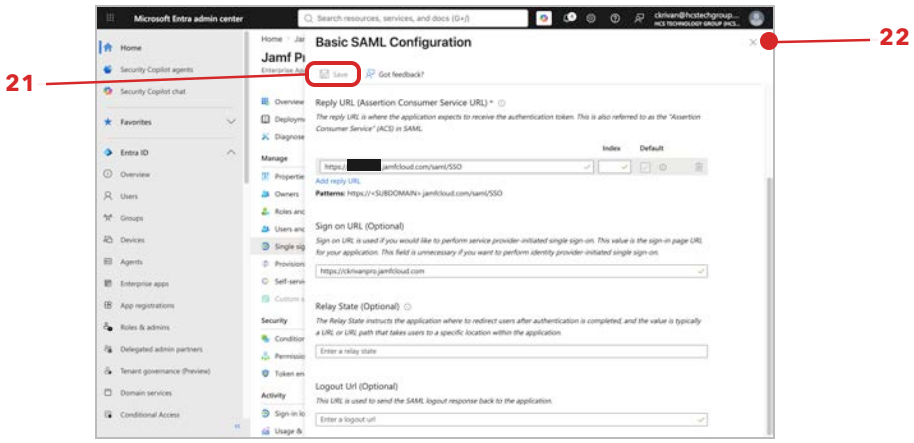
> **Note:** Microsoft Learn labels this field **Reply URL (Assertion Consumer Service URL)**.
> Microsoft Entra SSO integration with Jamf Pro (Microsoft Learn)

20. In the **Sign on URL** field, enter `https://<subdomain>.jamfcloud.com`, replacing `<subdomain>` with your own Jamf Pro subdomain.



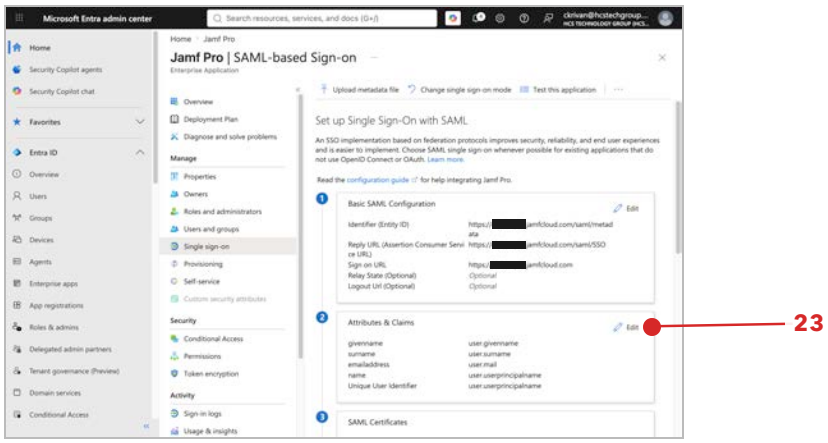
> **Note:** Microsoft's Jamf Pro tutorial still tells you to click **Set additional URLs** first. That control is gone: the Microsoft Entra admin center now shows **Sign on URL**, **Relay State**, and **Logout Url** expanded by default. Leave Relay State and Logout Url empty.

21. Click **Save**.

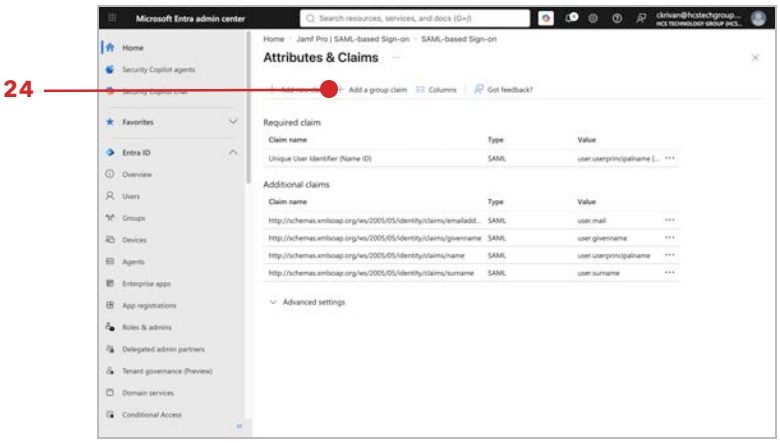


22. Click **X** after **Saving**.

23. In the **User Attributes & Claims** section, click the pencil icon.

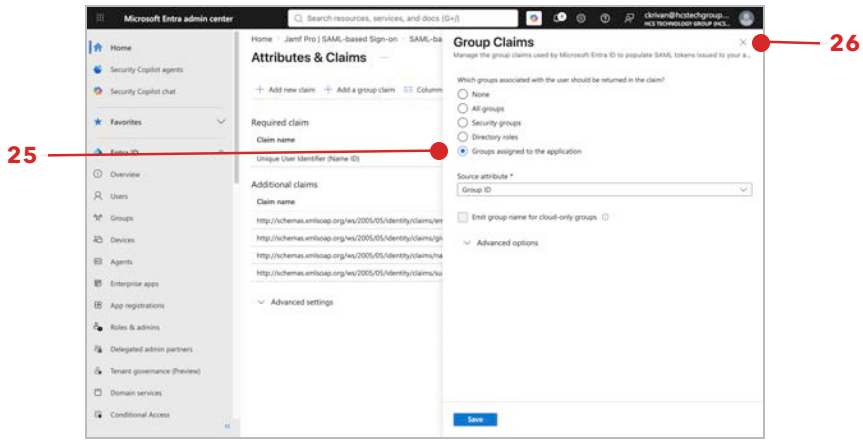


24. Click **Add a group claim**.



> **Note:** This replaces the manifest edit older guides used. Microsoft Learn documents the group claim as an option on the app's single sign-on configuration under **User Attributes & Claims**, and the `groupMembershipClaims` manifest edit as the alternative path under **App registrations**. Use the single sign-on page.
> Configure group claims for applications (Microsoft Entra documentation)

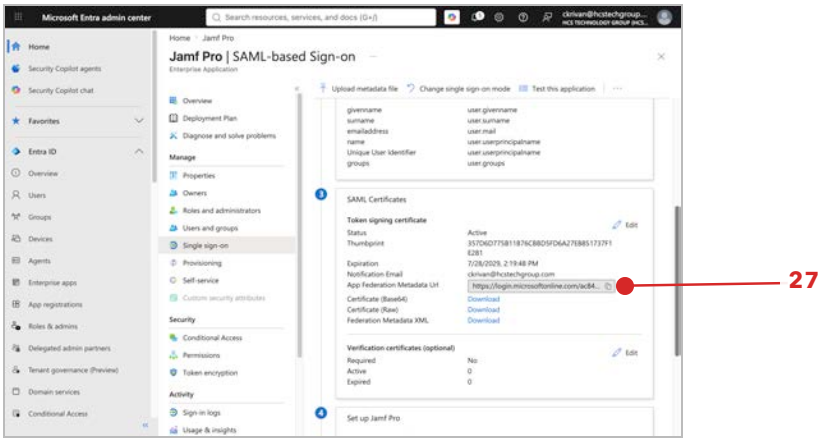
25. Select **Groups assigned to the application**, then click **Save**.



> **Note:** Microsoft Learn describes the four options: **All groups** sends security groups, distribution lists, and roles; **Security groups** sends the security groups the user is a member of; **Directory roles** sends assigned directory roles as a `wids` claim; **Groups assigned to the application** sends only groups explicitly assigned to the app, and is the option Microsoft recommends for large organizations because a SAML assertion is capped at 150 groups and exceeding the cap makes Microsoft Entra ID omit the group claim entirely. Choose **Security groups** instead if your Jamf Pro group names come from groups you do not want to assign to the app.
> Configure group claims for applications (Microsoft Entra documentation)

26. Click **the X** to dismiss the dialog box.

27. In the **SAML Signing Certificate** section, click the copy button next to **App Federation Metadata Url**, then save the URL. You paste it into Jamf Pro in the next phase.

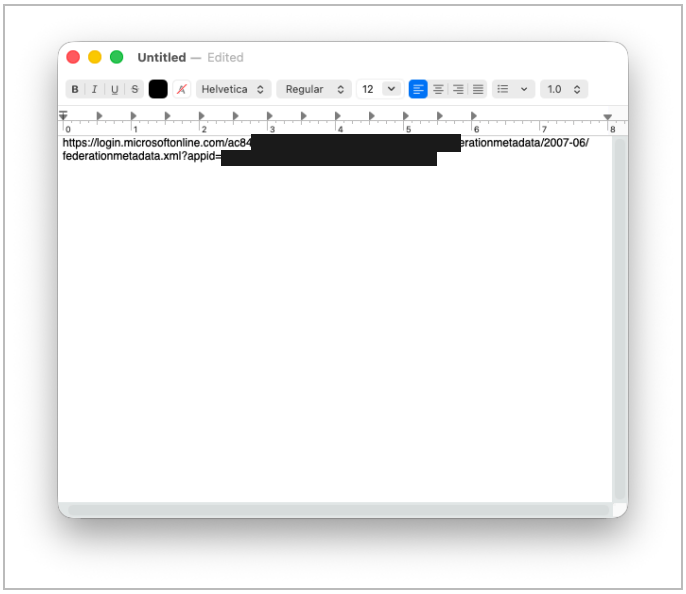


28. Open **Finder**.

29. Click **Applications**.

30. Open **TextEdit**.

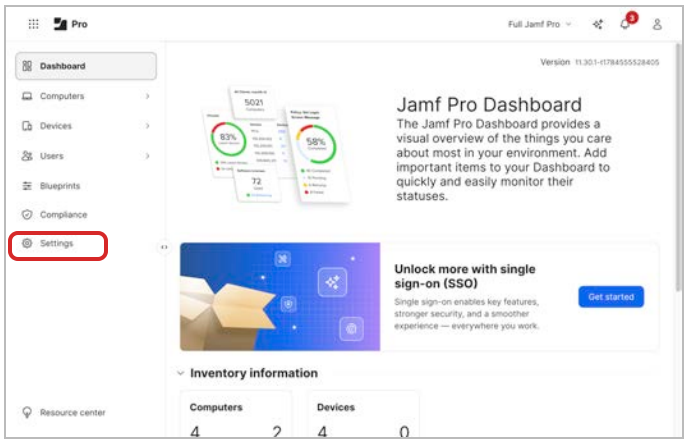
31. Copy the **App Federation Metadata Url**, then paste it into the TextEdit document.



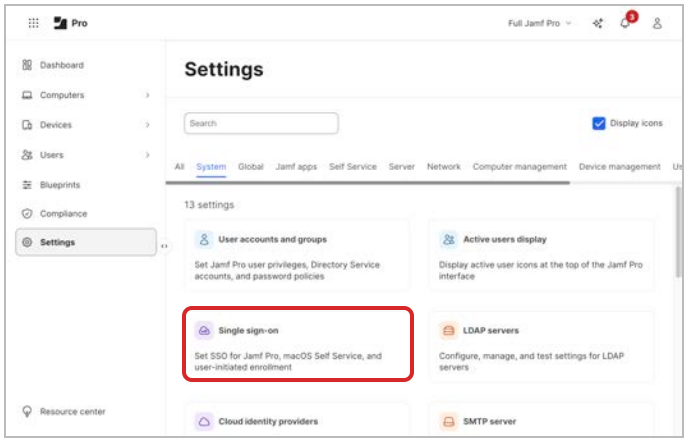
32. Save the document.

Enable SAML SSO for end users in Jamf Pro

33. In Jamf Pro, click **Settings** in the sidebar.

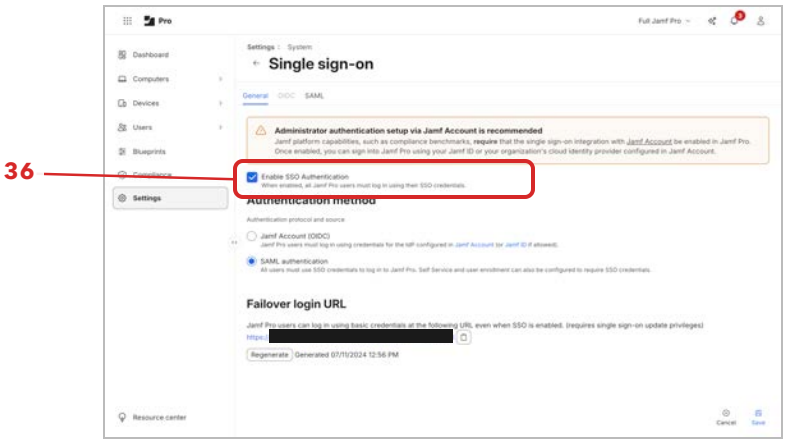


34. In the **System** section, click **Single sign-on**.



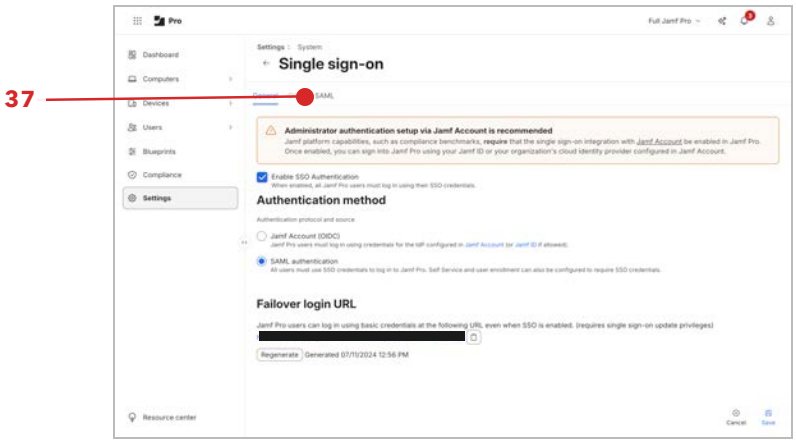
35. Click **Edit**.

36. Select **Enable SSO Authentication**.



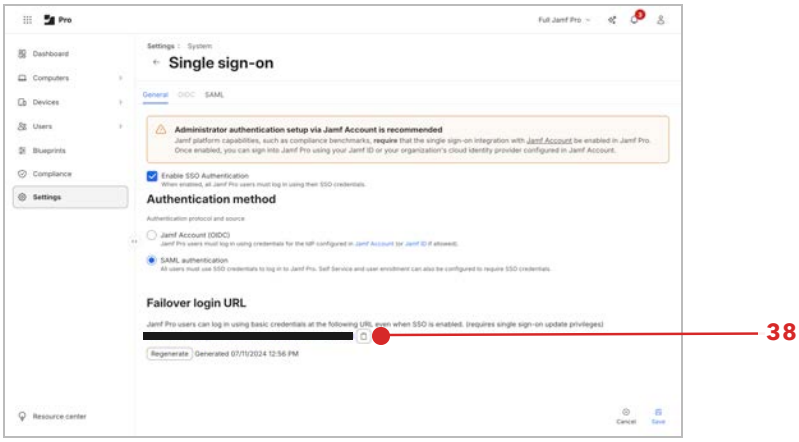
> **Note:** Jamf Pro Management warns that enabling SSO for Jamf Pro services and applications prevents users from authenticating with standard and directory credentials, and recommends notifying users about the change.
> Enabling Single Sign-On in Jamf Pro (Jamf Pro documentation)

37. Select **Use SAML authentication for end users (using IdP settings from Jamf Pro)**.



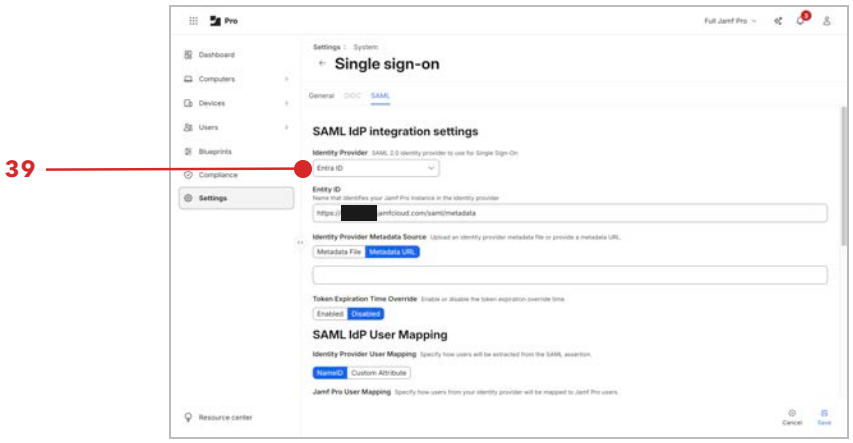
> **Note:** Jamf splits administrator SSO from end-user SSO. Jamf Pro Management recommends that administrators with supported environments use the OIDC-based SSO integration through Jamf Account, and states: "You can enable OIDC-based SSO in Jamf Account for administrators alongside SAML-based SSO in Jamf Pro for end users." The attended workflow method needs the end-user SAML side only. Choose **Use SAML authentication for end users (using IdP settings from Jamf Pro)** if your administrators sign in through Jamf Account OIDC. Choose **SAML authentication** only if you intend to put administrators behind SAML as well.
> SAML-Based Single Sign-On (Jamf Pro documentation)

38. In the **Failover Login URL** box, click **Copy to clipboard**, then save the failover login URL to your TextEdit note.



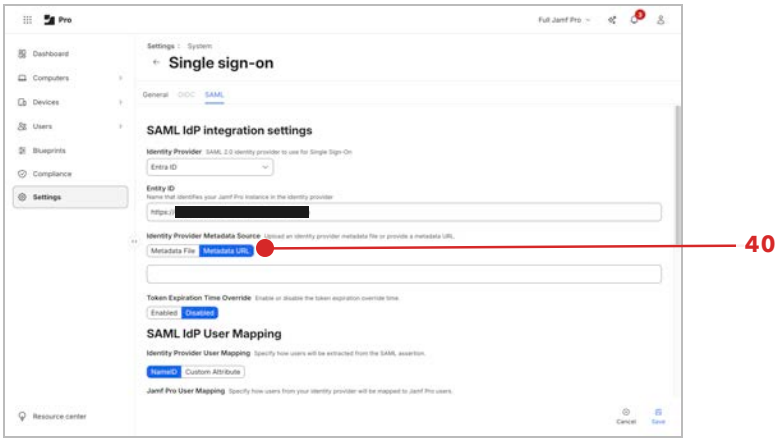
> **Note:** Copy this URL before you save, and store it where you can reach it without signing in to Jamf Pro. Always leave at least one Jamf Pro standard account with Administrator privileges that can sign in through the failover URL, so you have a way back in if the SAML integration breaks. Jamf Pro Management notes that if you enable the failover URL as an option for users while SSO authentication is enabled, those Jamf Pro user accounts need Read and Update privileges for SSO Settings.
> Enabling Single Sign-On in Jamf Pro (Jamf Pro documentation)

39. From the **Identity Provider** pop-up menu, choose the Microsoft Entra ID option.

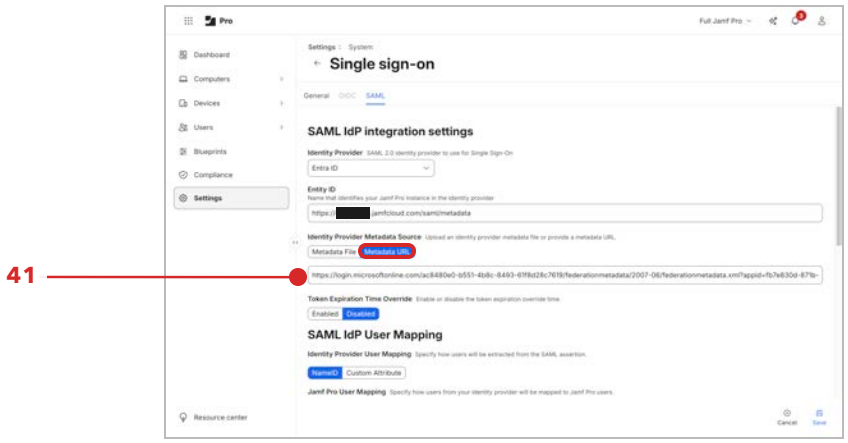


> **Note:** HCS field guidance, verify in your tenant: Microsoft's current tutorial still says to "Select **Azure** as an option from the **Identity Provider** drop-down menu", which is the pre-rename label. Jamf Pro Management does not publish the list of providers in the pop-up menu. Choose whichever entry names Microsoft's identity service in your Jamf Pro version. If no such entry exists, choose **Other** and enter `Microsoft Entra ID` in the **Other Provider** field.
> Microsoft Entra SSO integration with Jamf Pro (Microsoft Learn)
> A Guide to Integrate Azure Active Directory with Jamf Pro (HCS)

40. From the **Identity Provider Metadata Source** pop-up menu, choose **Metadata URL**.



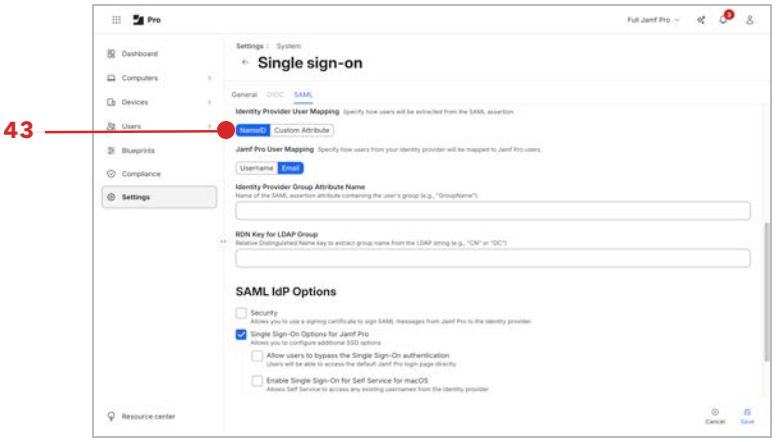
41. Paste the **App Federation Metadata URL** you saved in **TextEdit** into the **Metadata URL** field..



42. Confirm the **Entity ID** field matches the **Identifier** you entered in the Microsoft Entra ID app.

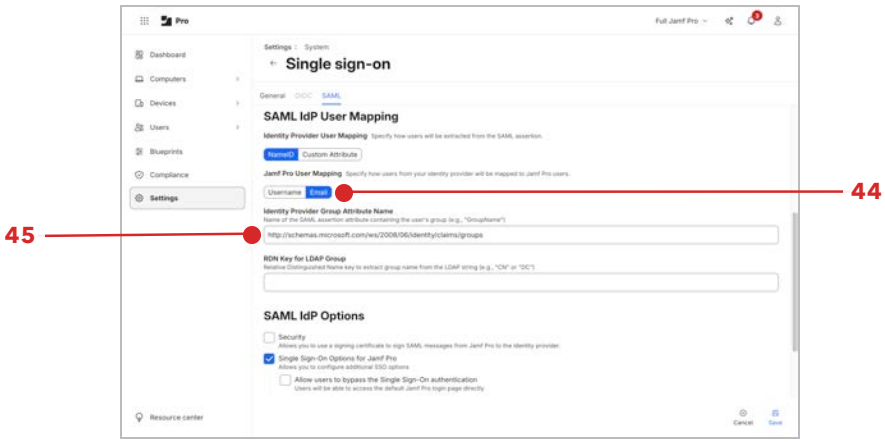
> **Note:** The field is pre-populated by default with `https://<subdomain>.jamfcloud.com/saml/metadata` (where `<subdomain>` is your own Jamf Pro subdomain). Jamf Pro Management notes that for most identity providers the **Entity ID** value should match the **Audience URI** value in the identity provider's configuration settings.
> Enabling Single Sign-On in Jamf Pro (Jamf Pro documentation)

43. For **Identity Provider User Mapping**, select **NameID**.



> **Note: NameID** is the default attribute name and the value Microsoft's tutorial specifies. Use **Custom Attribute** only if your assertion carries the Jamf Pro identity somewhere other than NameID.
> Microsoft Entra SSO integration with Jamf Pro (Microsoft Learn)

44. For **Jamf Pro User Mapping**, click **Email**.

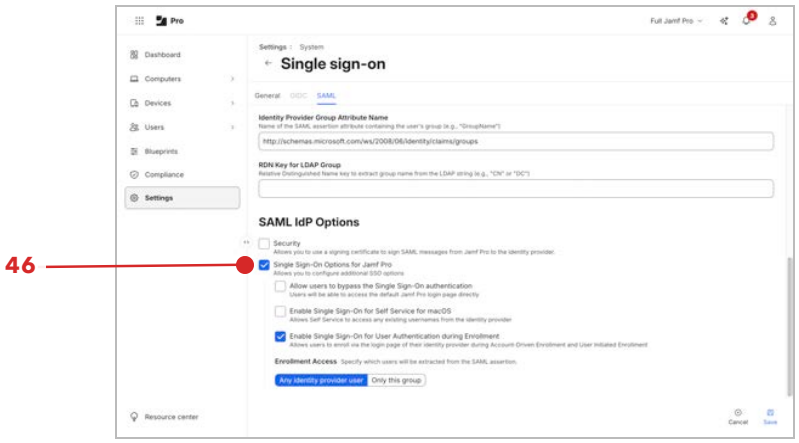


> **Note:** Microsoft's current tutorial specifies **Email**. Click **Username** instead if your Jamf Pro user accounts are named for the Microsoft Entra user principal name rather than the email address, which is how HCS's 2019 Azure Active Directory guide had it. Jamf Pro matches the incoming user against Jamf Pro user accounts first, and falls back to group name matching if no account matches. Jamf Pro Management lists "Jamf Pro user accounts or groups with matching IdP usernames or groups" as a prerequisite for enabling SAML SSO.
> Microsoft Entra SSO integration with Jamf Pro (Microsoft Learn)
> A Guide to Integrate Azure Active Directory with Jamf Pro (HCS)

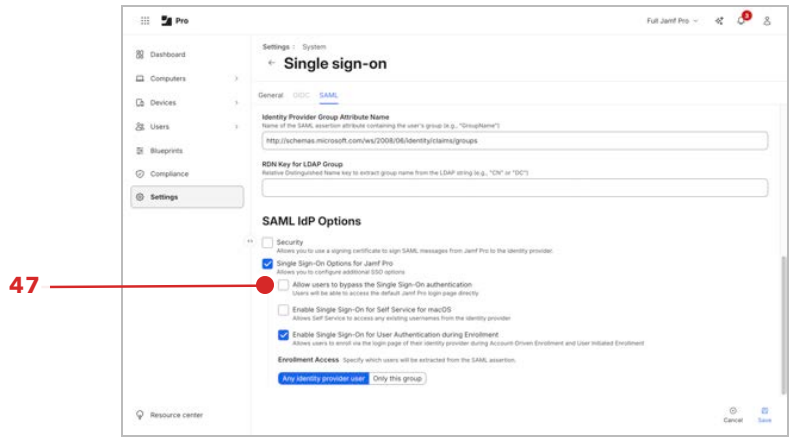
45. In the **Identity Provider Group Attribute Name** field, enter `http://schemas.microsoft.com/ws/2008/06/identity/claims/groups`.

> **Note:** This is the SAML assertion attribute Jamf Pro reads group membership from, and it is the value Microsoft's tutorial specifies for Microsoft Entra ID. By default the claim carries group object IDs, so the Jamf Pro groups you match against have to be named for those object IDs unless you picked an on-premises **Source attribute** when you added the group claim. Leave **RDN Key for LDAP Group** blank unless your assertion sends group names as Distinguished Names.
> Microsoft Entra SSO integration with Jamf Pro (Microsoft Learn)

46. Click **Single Sign-On Options for Jamf Pro**.

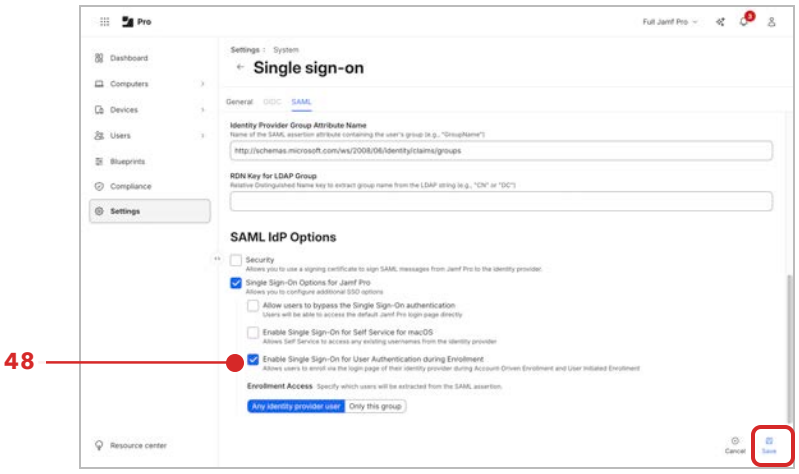


47. Deselect **Allow users to bypass the Single Sign-On authentication**.



> **Note:** Selected, users who go straight to the Jamf Pro URL get the standard Jamf Pro login page and can sign in without single sign-on, which also means the redirect check that follows never happens. Leave it deselected so single sign-on is enforced and the check is meaningful. You copied the failover login URL in step 38 if you need to get back in.

48. Leave **Enable Single Sign-On for User Authentication during Enrollment** unchanged. The attended workflow does not use it.



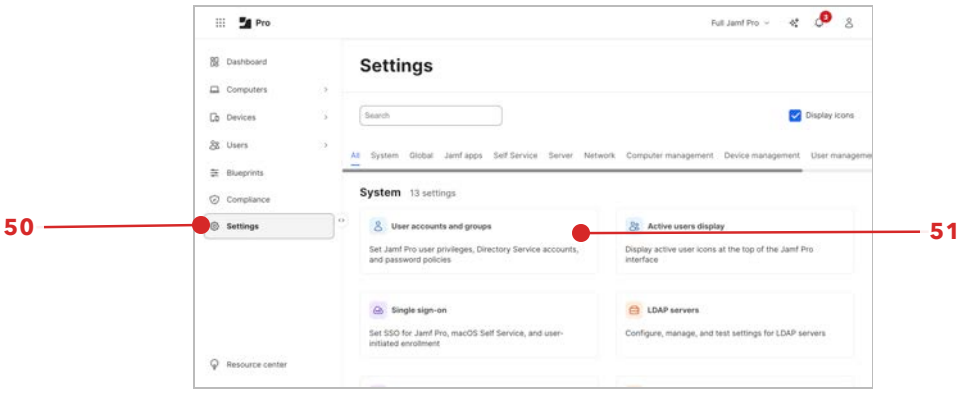
> **Note:** Jamf Pro Management (Enabling SSO with SAML in Jamf Pro) describes this setting as allowing users to enroll via the login page of their identity provider during user-initiated enrollment, account-driven User Enrollment, and account-driven Device Enrollment. The attended workflow runs over Automated Device Enrollment and authenticates the user through the token exchange described in the prologue, so this setting has no effect on it. Turn it on only if you also want single sign-on for those other enrollment methods.

49. Click **Save**.

> **Note:** Jamf recommends using SSL (HTTPS) endpoints and the POST binding for transmission of the SAML protocol, and configuring your identity provider settings using a SHA-256 or higher signature for SAML assertions.
> SAML-Based Single Sign-On (Jamf Pro documentation)

Confirm SAML is working before you continue

50. In Jamf Pro, click **Settings** in the sidebar.



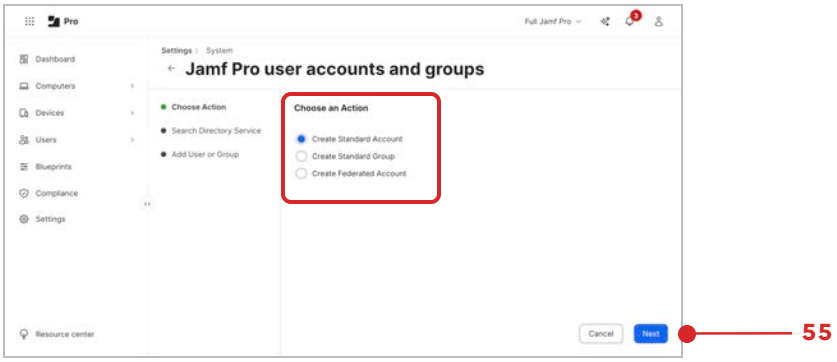
51. In the **System** section, click **User accounts & groups**.

52. Confirm an account exists whose email address matches the Microsoft Entra ID identity you will test with. If one exists, skip ahead to step 62.

> **Note:** HCS field guidance, verified by testing: the sign-in below only succeeds if the identity already has a Jamf Pro account, because you mapped **Jamf Pro User Mapping** to **Email** in step 44.

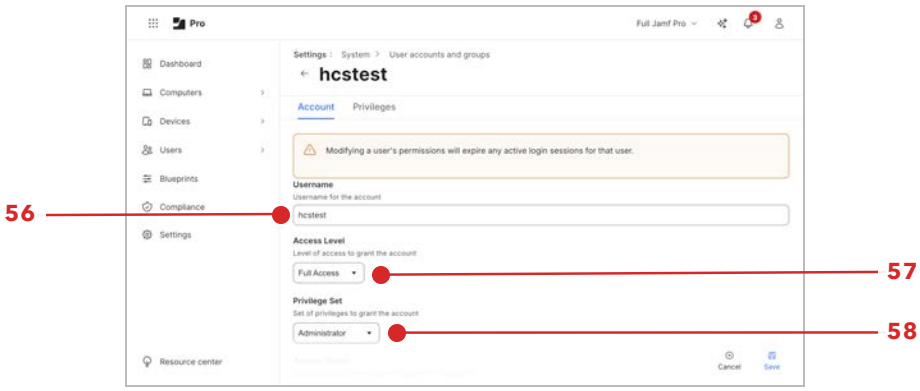
53. Click **New**.

54. Select **Create Standard Account**.



55. Click **Next**.

56. On the **Account** pane, enter a username for the account.

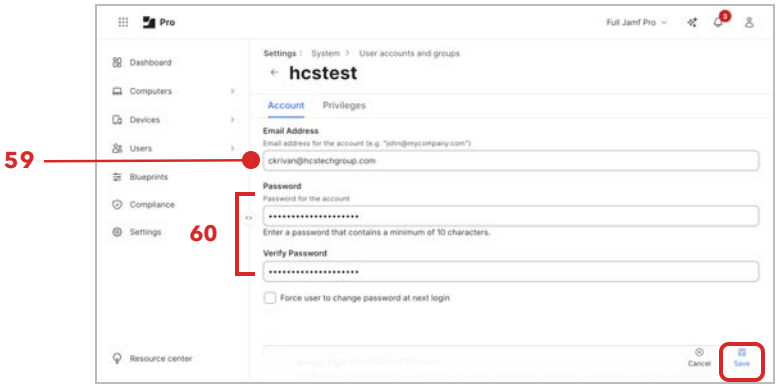


57. From the **Access Level** pop-up menu, choose **Full Access**.

58. From the **Privilege Set** pop-up menu, choose **Administrator**.

> **Note:** The account you are creating here is your own administrator identity, which is why it gets full access. Jamf Pro Management documents the other options: choose **Site Access** or **Group Access** from the Access Level menu if this account should be scoped instead.
> Creating a Jamf Pro User Account (Jamf Pro documentation)

59. Enter the email address that matches the Microsoft Entra ID identity you will test with.

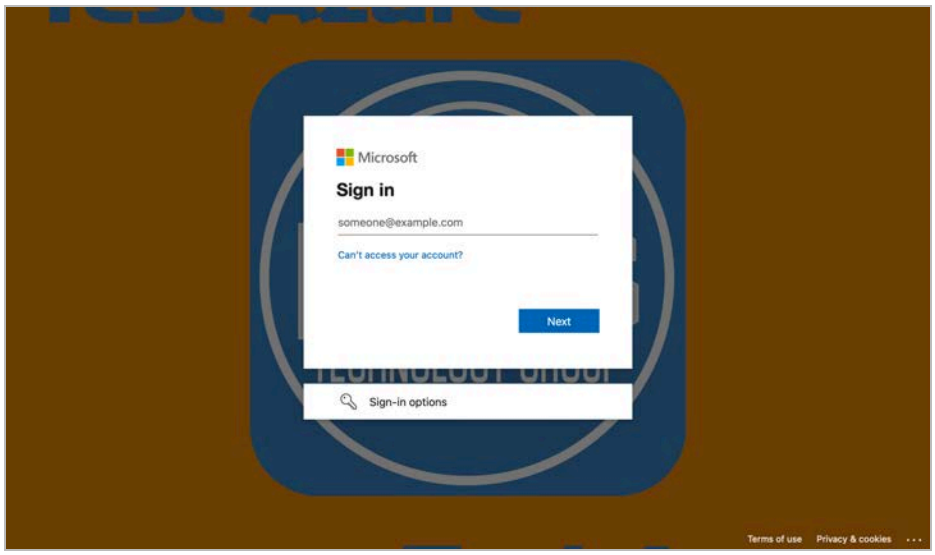


> **Note:** This is the value the sign-in depends on. You mapped **Jamf Pro User Mapping** to **Email** in step 44, so the SAML assertion is matched against this address. If it does not match the identity exactly, the redirect succeeds but the sign-in fails.

60. Enter and verify a password for the account.

61. Click **Save**.

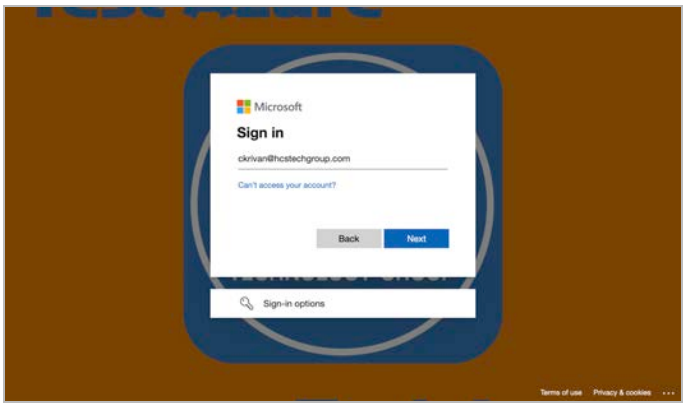
62. Enter your Jamf Pro URL.



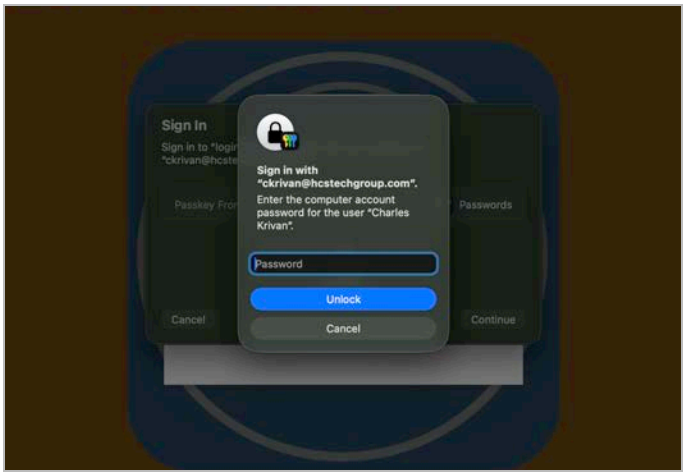
63. Confirm the browser redirects to the **Microsoft Entra** sign-in page.

> **Note:** The redirect is what we are testing. If it does not happen, SAML is not working, and finding that out now saves you the enrollment steps that follow. Use the failover login URL you saved in step 38 to get back into Jamf Pro.

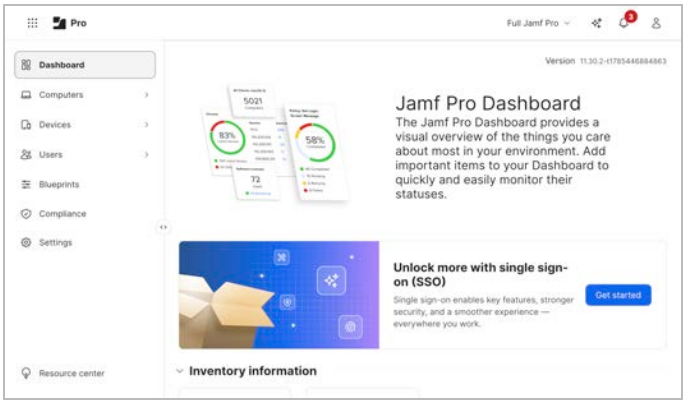
64. Sign in to the Jamf Pro server again with the Microsoft Entra ID identity you confirmed.



65. Confirm the Jamf Pro dashboard loads after you enter your computer password to sign in with your **Passkey**.

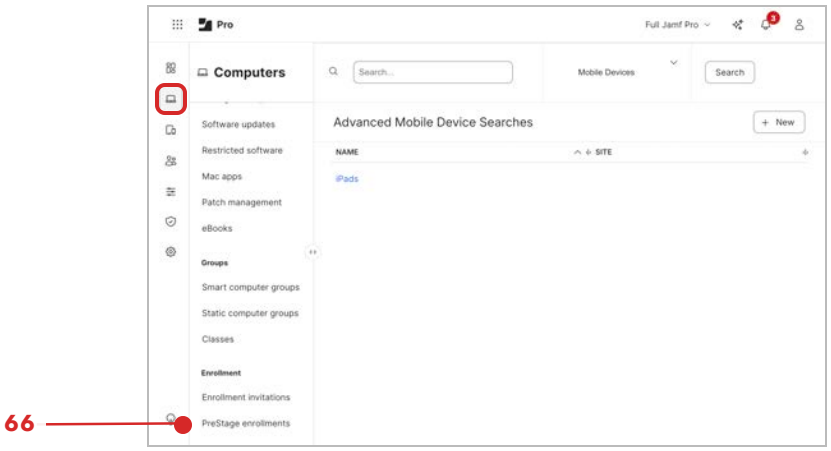


> **Note:** This confirms SAML between Microsoft Entra ID and Jamf Pro is working. It does not test Platform SSO. Its purpose is to rule SAML out as a cause if attended enrollment fails later in this section.

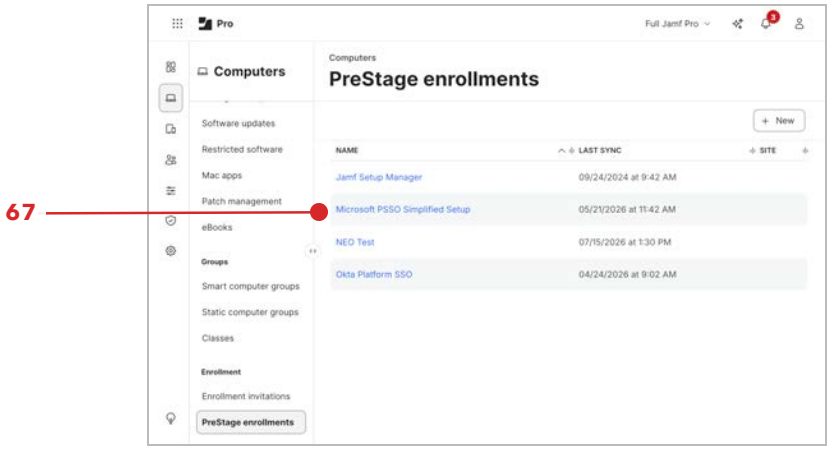


Switch the PreStage to the attended workflow method

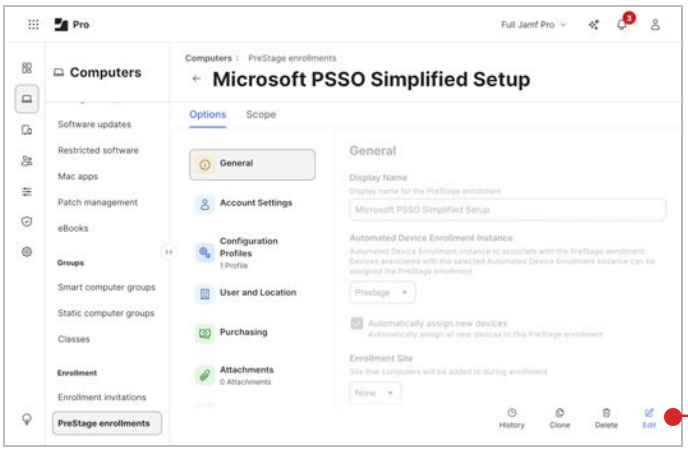
66. In Jamf Pro, click the **Computers** button, then click **PreStage Enrollments**.



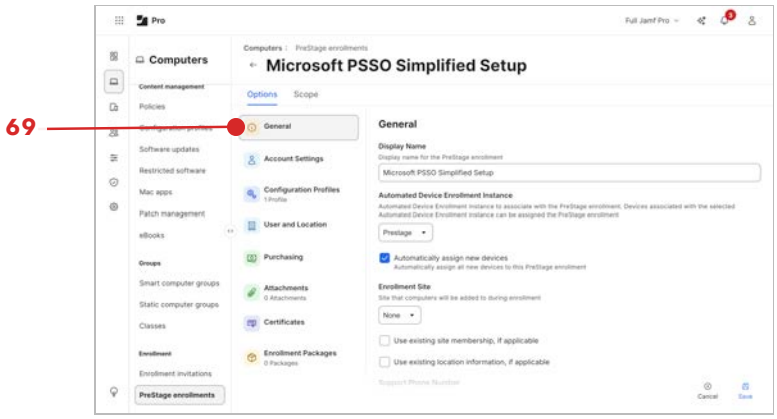
67. Select the PreStage Enrollment from Section 2.



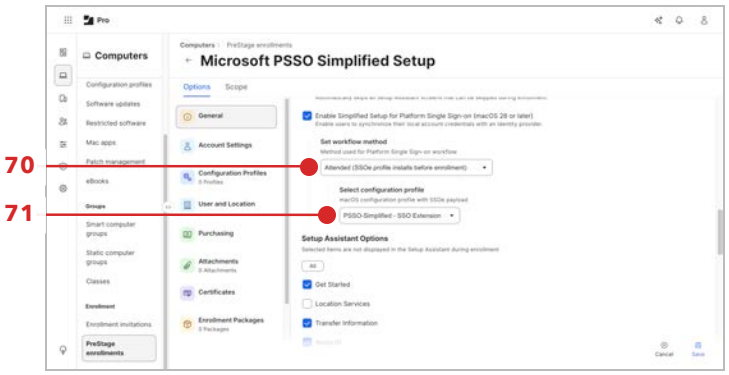
68. Click **Edit**.



69. Click the **General** pane.



70. From the **Set workflow method** pop-up menu, choose **Attended (SSOe profile installs before enrollment)**.



> **Note:** Jamf Pro Management states: "Enrollment customizations cannot be used with the attended workflow method." If this PreStage Enrollment uses an enrollment customization, remove it before you save, or stay on the unattended method.

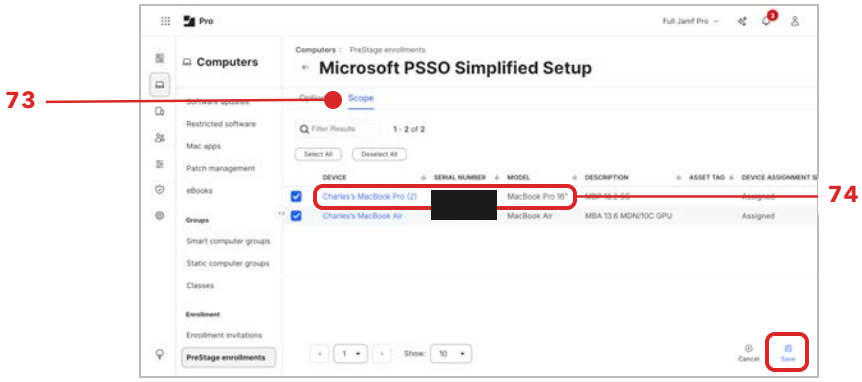
71. From the **Select configuration profile** pop-up menu, choose the Platform SSO configuration profile you updated in Section 1.

> **Note: HCS field guidance, verified by testing:** choosing the profile here does not deliver it on its own. It must also be scoped to reach the computers this PreStage Enrollment enrolls, which you did when you created the profile earlier in this guide. If it is not scoped, Jamf Pro ignores this selection, the Mac computer never receives the profile before enrollment, and it cannot register. Jamf's documentation does not state this.

72. Confirm the profiles you configured during the initial Platform SSO setup are selected, including the updated Platform SSO profile from Section 1.

> **Note:** Jamf flags this as important: specific settings must be enabled in the Single Sign-On Extensions profile for this workflow to function. Those are the settings you enabled in Section 1: **Enable Registration During Setup**, **Enable Create First User During Setup**, and **Use Shared Device Keys**.

73. Click the **Scope** tab.

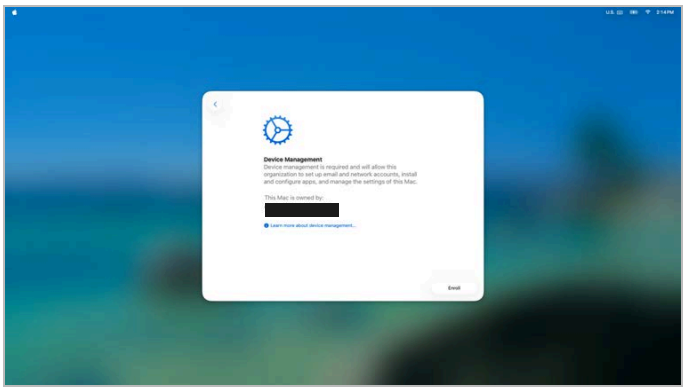


74. Select the test Mac computer you want to enroll with the attended workflow.

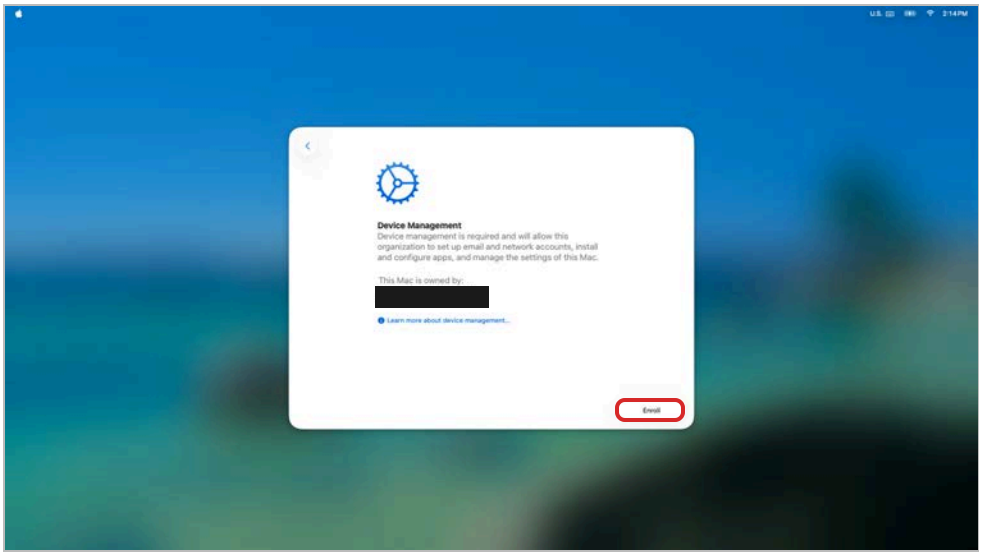
75. Click the **Save** button.

Test the attended workflow

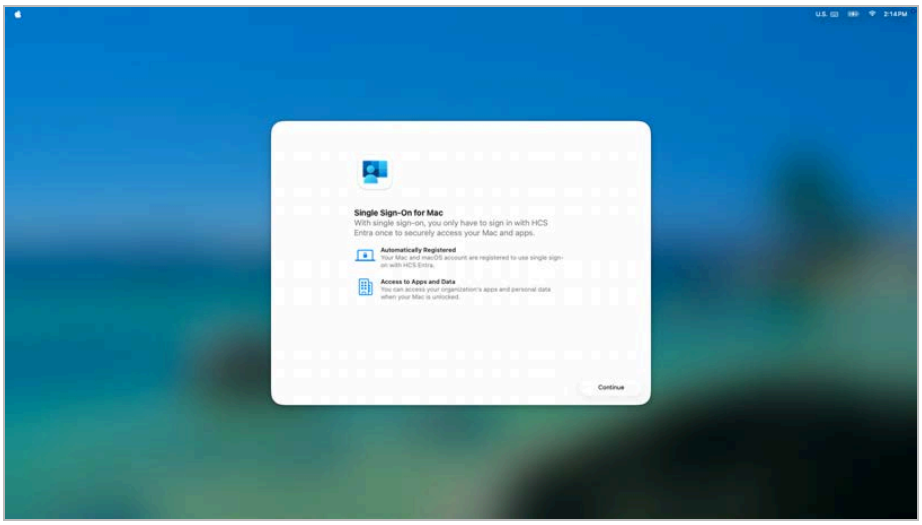
76. Power on the erased test Mac computer and proceed through Setup Assistant until the **Device Management** screen appears.



77. Click **Enroll**.

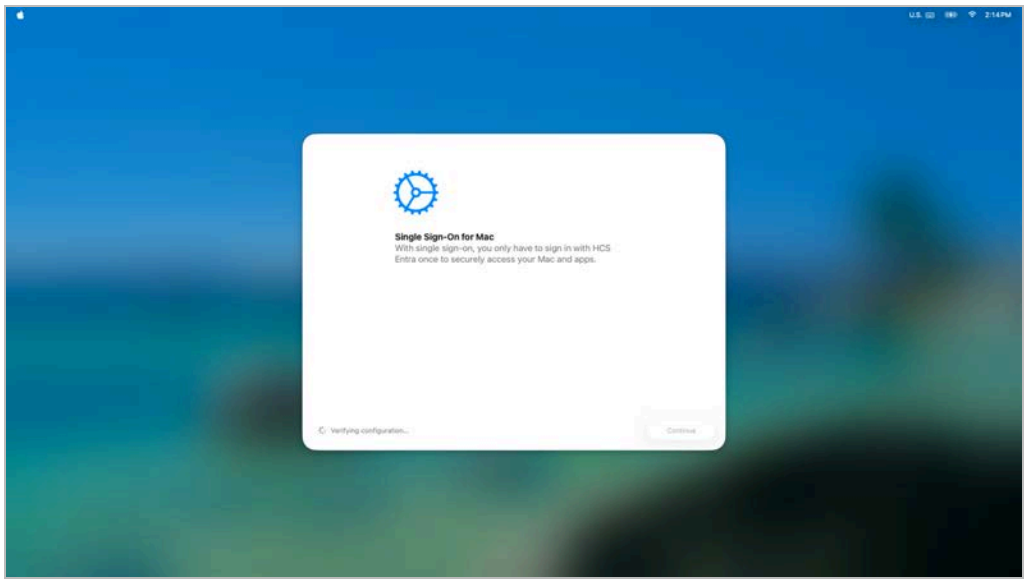


78. Let the Mac computer download and install the Platform SSO configuration profile and the Company Portal package automatically, and wait for the Platform SSO registration prompt.

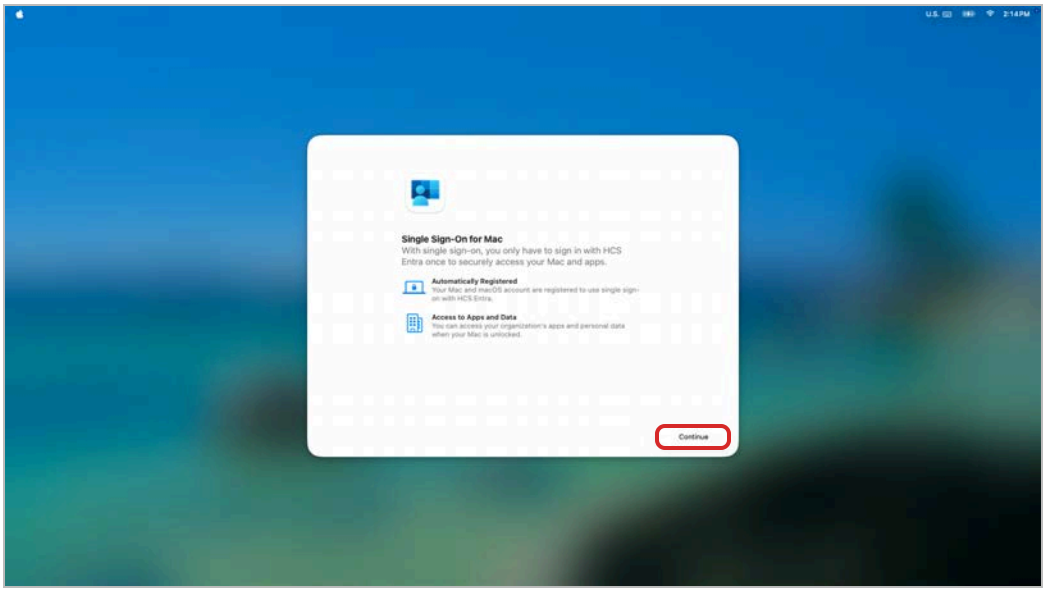


> **Note:** Behind the scenes, Jamf Pro returns a 403 response that rejects enrollment until the Mac computer completes Platform SSO registration. The 403 carries secured download links for the Platform SSO configuration profile and the Company Portal app package, which macOS downloads and installs on its own. The Mac computer then prompts the user to register before it can attempt to enroll again.
>
> **HCS field guidance, verified by testing:** the attended workflow completed successfully with no Company Portal package added to this PreStage Enrollment's **Enrollment Packages** payload. The package arrived entirely through the 403 response's secured download link. Jamf's published procedure lists the Enrollment Packages step as applying to both workflow methods, but field testing shows it is not required for the attended workflow to succeed.

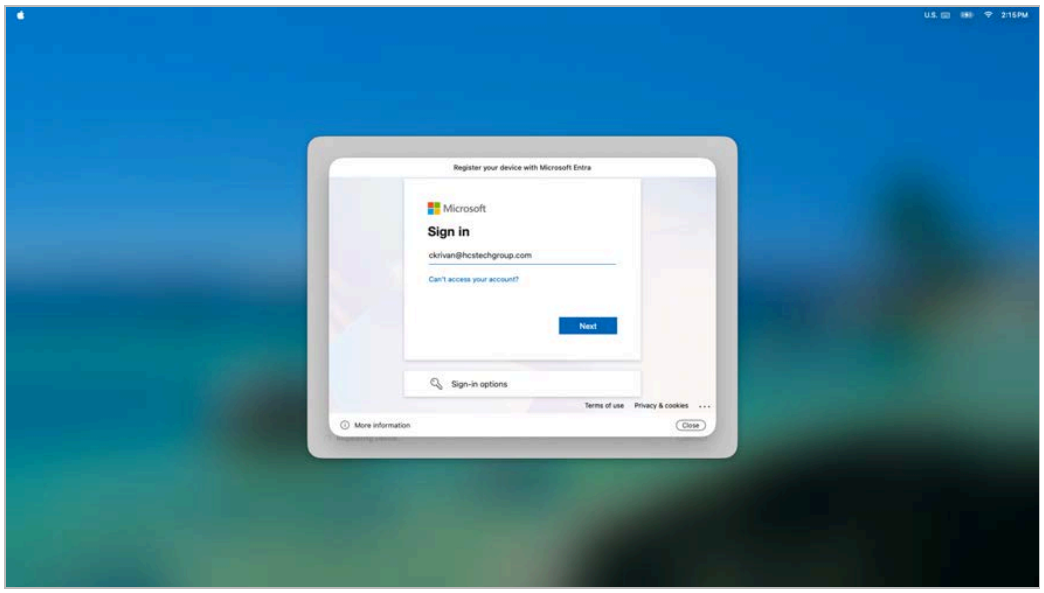
79. Confirm the **Single Sign-On for Mac** screen appears and verifies the configuration.



80. On the **Single Sign-On for Mac** screen, click the **Continue** button.

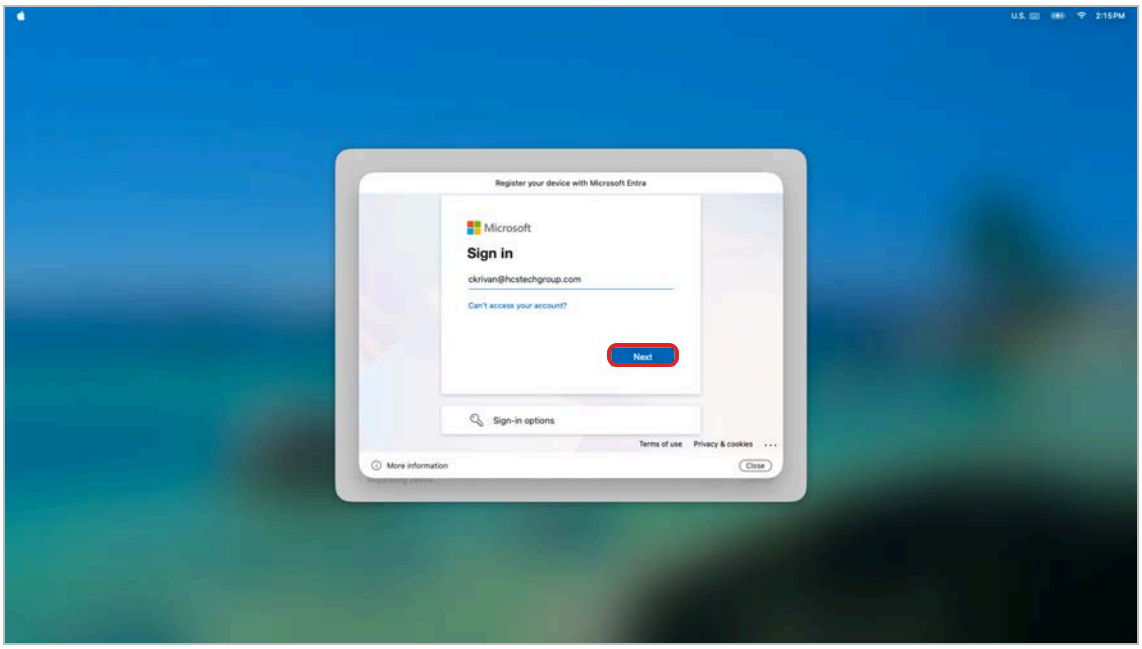


81. At the sign-in sheet, enter your Microsoft Entra email.



> **Note: HCS field guidance, verified by testing:** the attended workflow asks the user to sign in twice, and both prompts are expected. The first signs in to register the Mac computer with Platform SSO. The second signs in to the organization so enrollment can continue. A user who is not told to expect the second prompt will assume the first one failed.

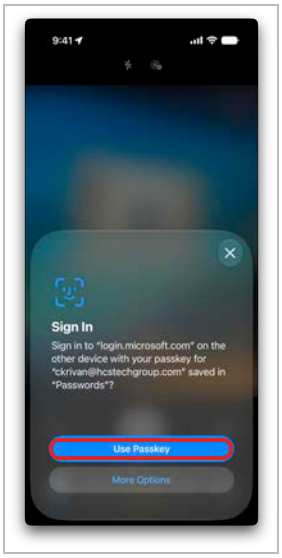
82. Click **Next**.



> **Note:** Your sign-in authentication steps may be different if you are using a password, security key, or Microsoft Authenticator.

83. If your account uses a passkey, the **Scan QR Code** sheet appears. Scan the QR code with your iPhone.

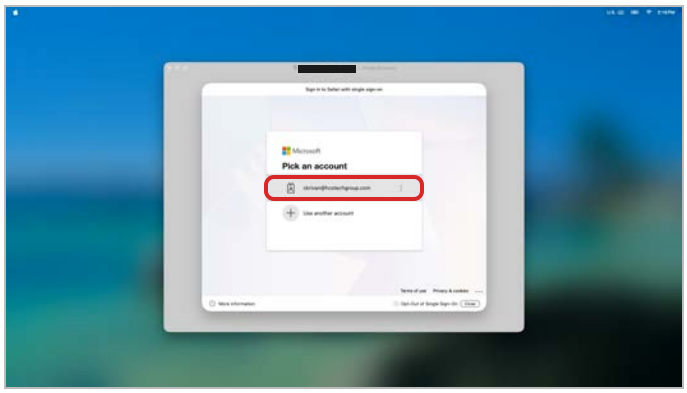
84. On your iPhone, tap **Use Passkey**.



85. When the second sign-in prompt appears, the **Sign in to Safari with single sign-on** window opens. Wait for the sign-in page to load.

> **Note: HCS field guidance, verified by testing:** two sign-ins are expected in the attended workflow. The first registers the Mac computer with Platform SSO. This second one signs in to the organization so enrollment can continue. A user who is not warned will assume the first attempt failed.

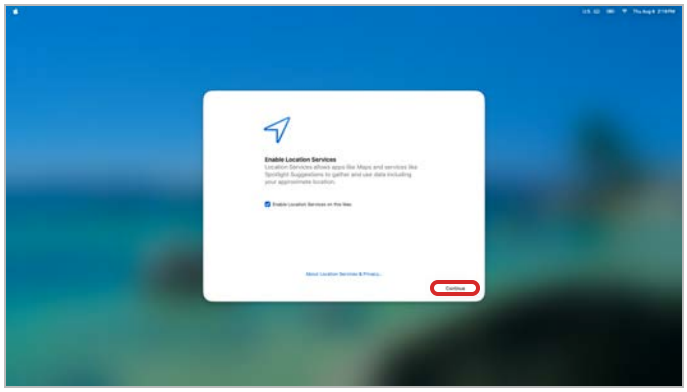
86. Click your Microsoft Entra ID account under **Pick an account**.



87. When the **Scan QR Code** sheet appears again, scan it with your iPhone and tap **Use Passkey**.

> **Note:** The attended workflow signs in twice, so the passkey prompt also appears a second time.

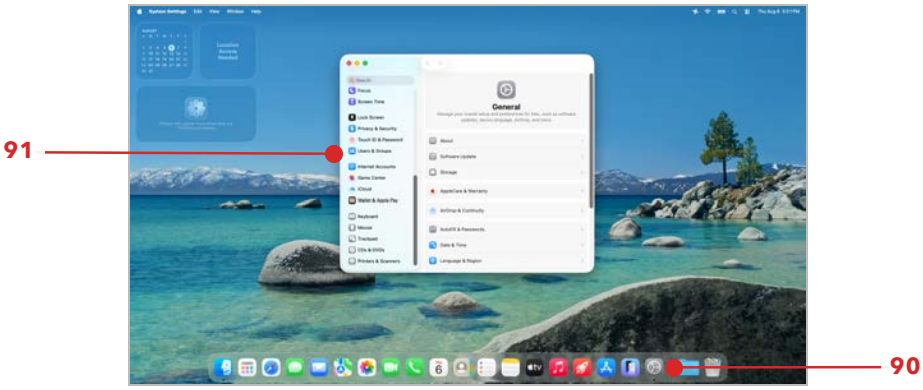
88. On the **Enable Location Services** screen, click **Continue**.



89. Confirm the Mac computer completes registration and enrollment continues into account creation.

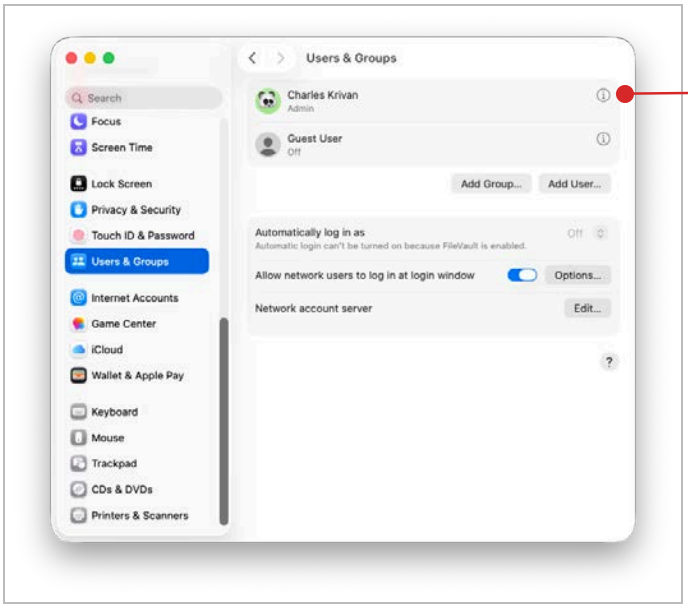
> **Note:** Once registration completes, the Mac computer sends an authentication token to Jamf Pro. Jamf Pro verifies the token against the server's SAML SSO integration and authorizes enrollment. Account creation and the remaining Setup Assistant screens then follow the settings in the PreStage Enrollment, exactly as they do in the unattended workflow.

90. Click **System Settings** in the Dock.

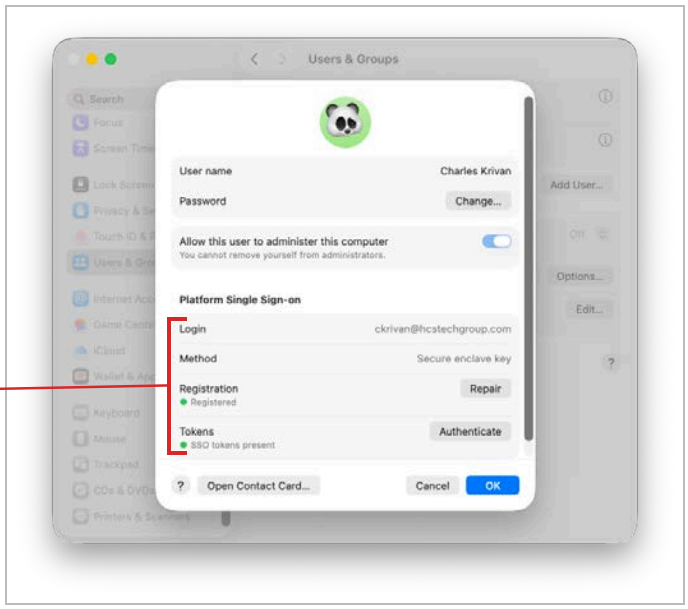


91. Click **Users & Groups** in the System Settings sidebar.

92. Click the **info** button next to the Platform SSO user.



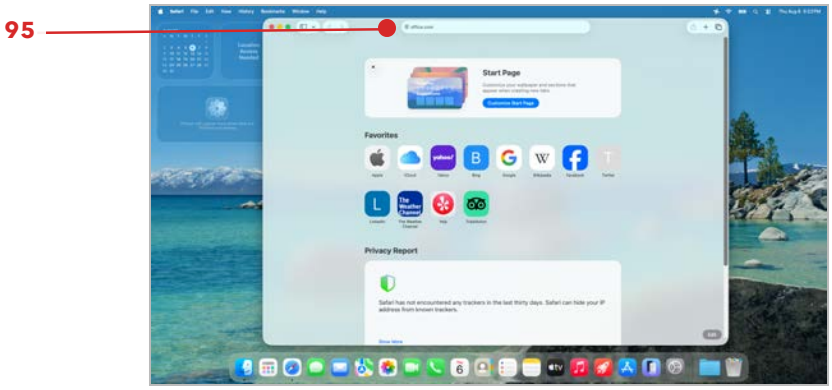
93. Confirm the **Platform Single Sign-on** section shows the same four indicators you verified in Section 2: Login, Method, Registration, and Tokens.



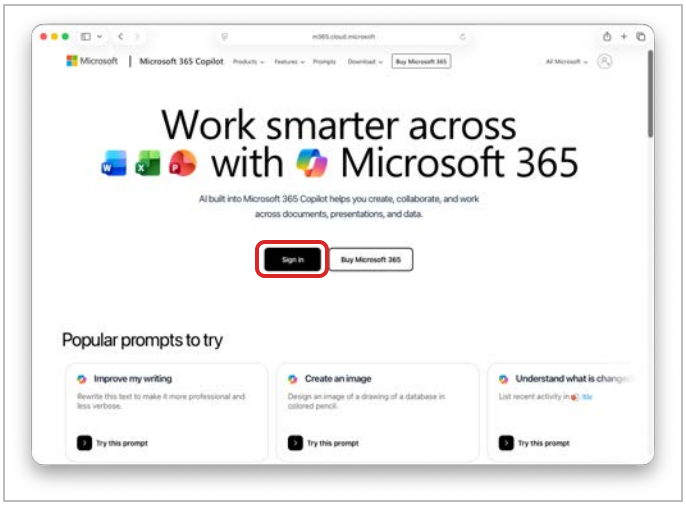
94. If the Mac computer enters Platform SSO registration during Setup Assistant and cannot complete it, erase and reset the Mac computer before you retest.

> **Note:** A Mac computer that cannot finish Platform SSO registration stays stuck in Setup Assistant, and recovering it requires an erase and reset. On a Mac computer with Apple silicon running macOS 26, use the **Wipe Computer** command. That is the reason Jamf tells you to prove the profile with the unattended workflow first.

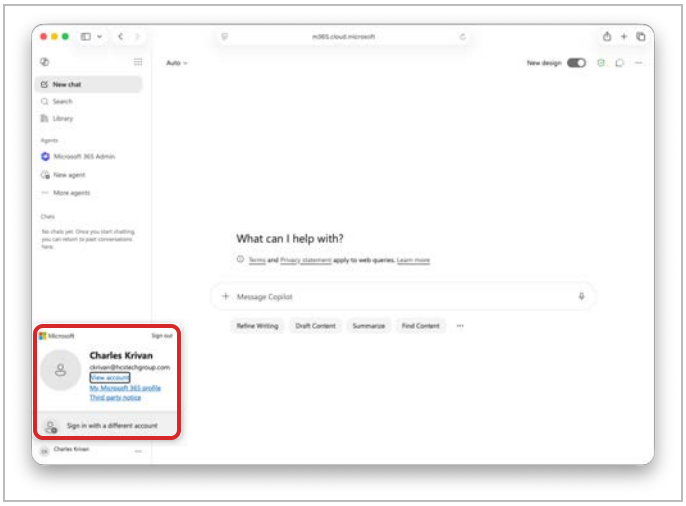
95. On the test Mac computer, open Safari and enter **office.com** in the address bar.



96. Click **Sign in**.



97. Confirm you are signed in with your Microsoft Entra ID identity and were not asked for a password.



This completes this section. In the next section, **Authenticated Guest Mode with Microsoft Entra ID**, you will let a user sign in at the login window with their Microsoft Entra ID credentials and receive a temporary session.

Bonus Track B

Authenticated Guest Mode with Microsoft Entra ID

Bonus Track B: Authenticated Guest Mode with Microsoft Entra ID

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 Bonus Track:

- The Platform SSO configuration profile from Section 1, deployed by the PreStage Enrollment from Section 2.
- The Microsoft Intune Company Portal app installed on the Mac computer. It provides the single sign-on extension that Platform SSO registers through. Section 2 uploads the installer and adds it to the PreStage Enrollment.
- A Mac computer that has already completed Platform SSO registration, as verified in Section 2 and again in Bonus Track A. Authenticated Guest Mode signs people in with the shared device keys that registration creates, so a Mac computer that has never registered cannot create a guest session.
- A Microsoft Entra ID email address and password to sign in with at the login window.

NOTE: Apple requires **Use Shared Device Keys** for **Create New User at Login**, which is why registration has to happen first and why the key is delivered on the device channel. Accounts created at the login window authenticate with a password or a smart card. A Secure Enclave key belongs to one registered user, so it is not available for guest sessions.
Extensible Single Sign-On payload schema (Apple device management on GitHub)

What this Bonus Track adds

Authenticated Guest Mode lets a person sign in at the login window with a Microsoft Entra ID email address and password and receive a temporary session. Everything it needs is already in place from the earlier sections: this Bonus Track turns on four keys in the same **Single Sign-On Extensions** payload you configured in Section 1, and the profile reaches the Mac computer you enrolled in Section 2.

NOTE: HCS field results: Simplified Setup and Authenticated Guest Mode run together in one configuration profile on the same Mac computer. Simplified Setup registers with a Secure Enclave key, and Authenticated Guest Mode signs in with a password.

NewUserAuthorizationMode = Temporary

Applies a temporary session configuration to accounts created at the login window. Apple lists `Temporary` as a value of this key. Microsoft documents this key as **New User Authorization Mode** and currently supports only `Standard` and `Admin`, so `Temporary` falls under the undocumented-settings caveat above.

NewUserAuthenticationMethods = Password

Sets the authentication method for accounts created at the login window or during Setup Assistant. Apple introduced this key in macOS 26.

EnableCreateUserAtLogin = true

Enables creating users at the login window. Apple's schema requires `UseSharedDeviceKeys` to be `true` for this key. Microsoft documents this key as **Enable Create User At Login**.

TemporarySessionQuickLogin = true

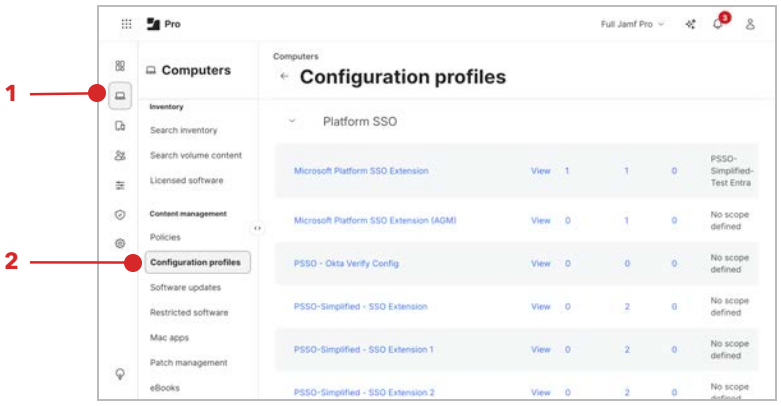
Turns on the quicker Authenticated Guest Mode login and the session data erase behavior described above. Apple introduced this key in macOS 26 and recommends it for shared environments with a high frequency of short sessions.

UseSharedDeviceKeys = true (already set in Section 1)

Enabled on the Platform SSO profile in Section 1. Authenticated Guest Mode depends on it: shared device keys are what let macOS create accounts on demand at the login window, and `EnableCreateUserAtLogin` requires it.

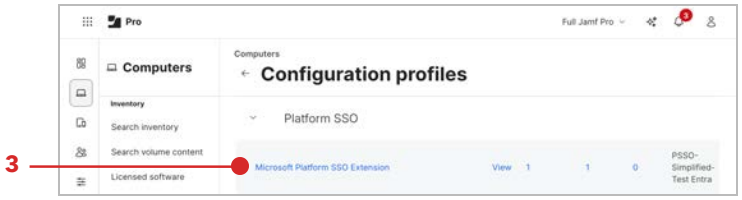
NOTE: Authenticated Guest Mode does not require any particular multifactor authentication configuration, but as of macOS 26, Microsoft's **per-user multifactor authentication** set to **Enforced** prevents the login window sign-in from completing. Microsoft's own guidance is not to combine the two: leave per-user multifactor authentication disabled and enforce multifactor authentication with Conditional Access instead. Conditional Access requires Microsoft Entra ID P1 or P2, and Microsoft 365 Business Premium includes P1. Users continue to appear as **Disabled** on the per-user multifactor authentication page while Conditional Access is active, which is expected and not a misconfiguration. Enable per-user multifactor authentication (Microsoft Entra documentation)

1. In Jamf Pro, click **Computers** in the sidebar.

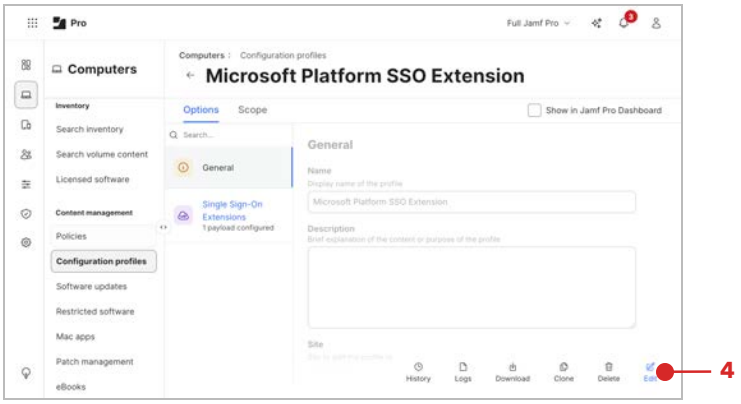


2. Click **Configuration profiles**.

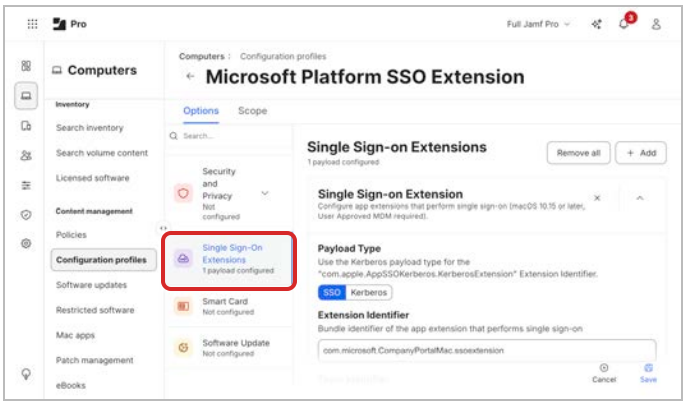
3. Click the Platform SSO configuration profile you updated in Section 1.



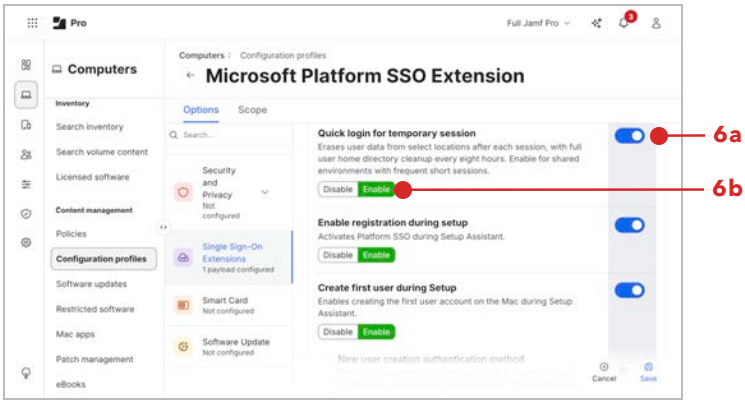
4. Click **Edit**.



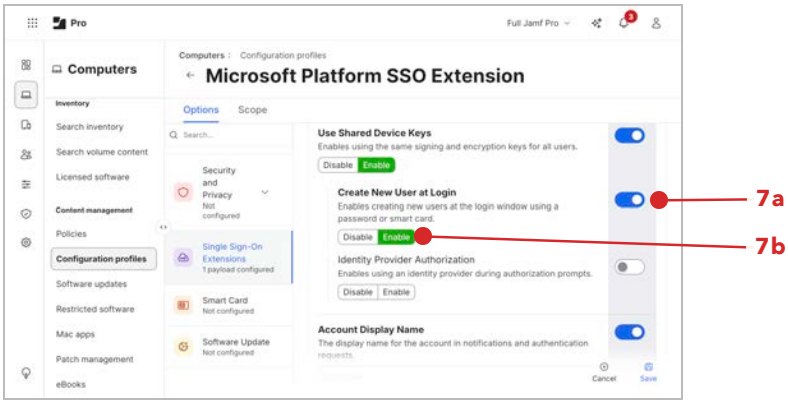
5. Scroll to the **Single Sign-On Extensions** payload.



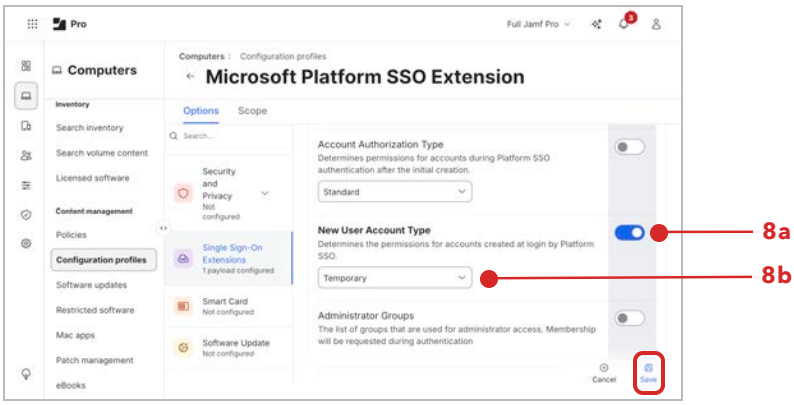
6. Slide **Quick Login for temporary session** to ON and **Enable**.



7. Slide **Create New User at Login** to **ON** and **Enable**.



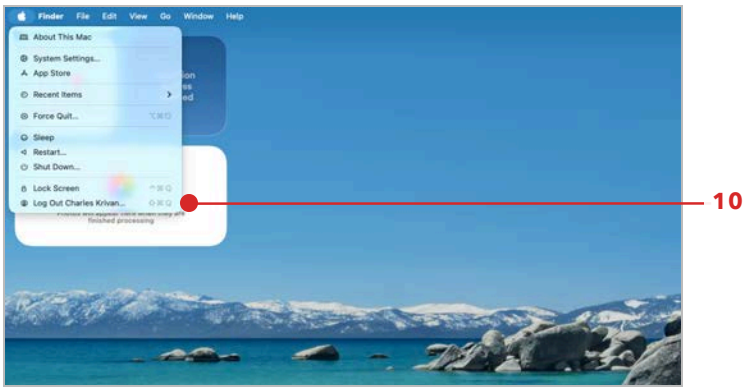
8. Set **New User Account Type** to ON and select **Temporary**.



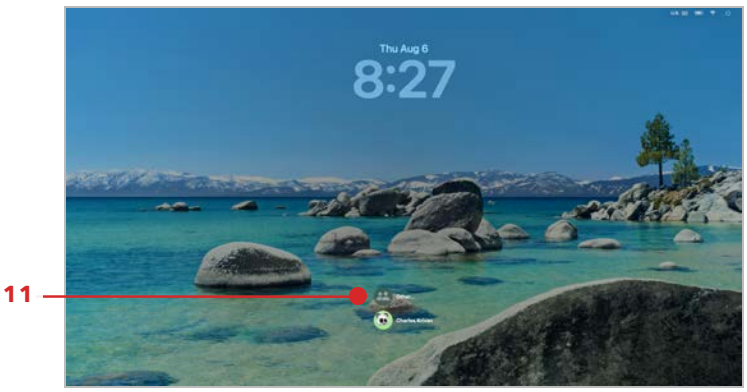
9. Click **Save**.

> **Note:** The profile redistributes automatically to its scoped computers, including the Mac computer you will test with. Nothing needs to be re-enrolled.

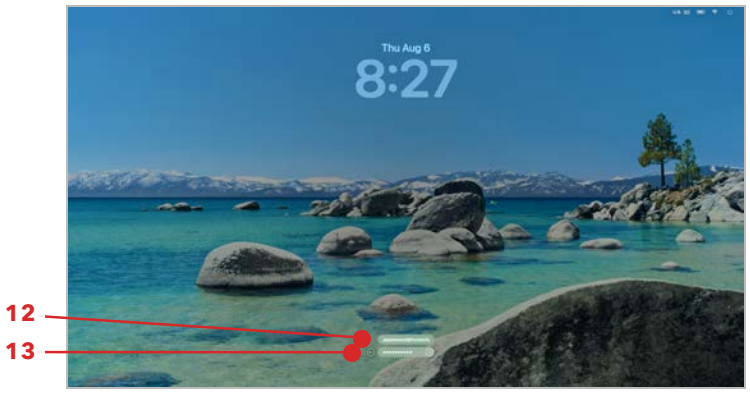
10. On the Mac computer enrolled in Jamf Pro, log out.



11. At the login window, click **Other**.



12. Enter your Microsoft Entra ID email address.

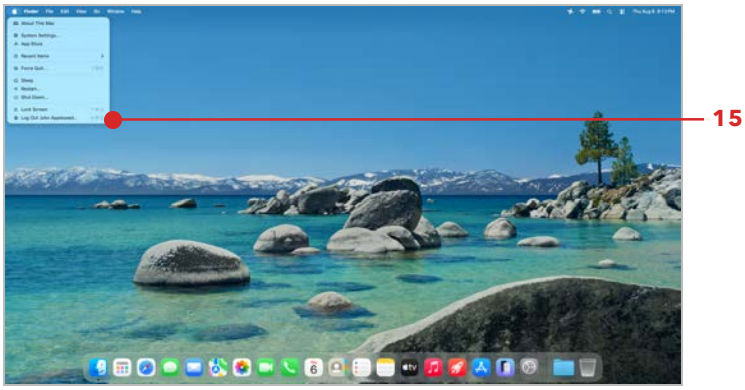


13. Enter its password, then press Return.

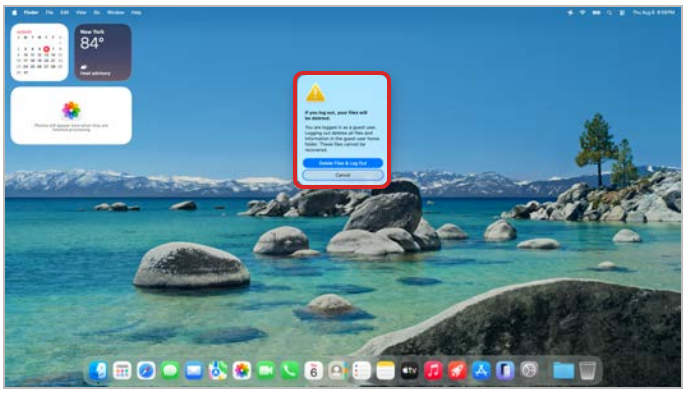
> **Note:** HCS field guidance, verified by testing: there is no web sign-in view and no visible indication that Microsoft Entra ID is checking the credentials. If they are valid, the Mac computer logs in directly.

14. The Mac computer signs in.

15. Log out of the temporary session.



16. Confirm the session's user data is removed after logout.



17. This concludes the guide.