



How to Configure Jamf Connect with Microsoft Entra ID



Contents

Preface	3
Section 1: Configure Microsoft Entra ID	5
Section 2 - Create a package for branding Jamf Connect	21
Section 3 - Test connection to Microsoft Entra ID using the Jamf Connect Configuration App	27
Section 4: Create a Configuration Profile for Jamf Connect.....	33
Section 5: Create a policy in Jamf Pro to install Jamf Connect Login	55
Section 6: Install and test Jamf Connect on a Mac Computer	67



Preface

What is Jamf Connect?

Jamf Connect is an identity and access management solution that links a user's local macOS account to their organization's cloud identity provider. It enables secure authentication, allows organizations to customize the macOS login experience, and helps maintain password sync and compliance between local and network credentials. Administrators can also manage local account privileges and enforce identity-based access controls.

What is Jamf Connect ZTNA?

Jamf Connect's Zero Trust Network Access (ZTNA) service provides secure, encrypted access to corporate resources for remote users, regardless of their location. ZTNA is configured and managed through the Jamf Security Cloud portal and can be integrated with other Jamf security solutions, such as Jamf Protect, to extend protections like internet content filtering and usage controls across the organization's device fleet. Jamf Connect's Zero Trust Network Access (ZTNA) is not a requirement for Jamf Connect but is recommended for increased security. Learn more here: https://learn.jamf.com/en-US/bundle/jamf-connect-documentation-current/page/Private_Access.html

System Requirements:

This guide was written using Jamf Connect 3.3.0 and requires macOS 13 or later. ZTNA will not be covered in this guide.

Network Authentication Requirements:

If your organization employs an 802.1X network to enforce access control, it's critical to understand how authentication workflows interact with the macOS login window—particularly when using Jamf Connect.

At the login window, macOS operates without access to user-specific credentials, which limits the types of 802.1X authentication methods that can be used prior to user login. For successful network connectivity at this stage, the authentication method must be computer-based and supported by macOS natively at the system level.

For example, EAP-TLS (Extensible Authentication Protocol – Transport Layer Security), which uses a machine certificate for authentication, is supported and recommended for 802.1X environments in conjunction with Jamf Connect. This method allows the Mac to establish a network connection before a user logs in, ensuring Jamf Connect can reach the identity provider.

In contrast, authentication types that rely on user credentials, such as EAP-PEAP or EAP-TTLS, are NOT supported at the login window. Since Jamf Connect requires network access to function properly (e.g., to communicate with a cloud identity provider), and these methods rely on credentials that aren't available until after login, using them would prevent Jamf Connect from working as intended.

When designing a network authentication strategy for use with Jamf Connect, ensure that the 802.1X method can authenticate the machine itself, not just the user, to provide reliable pre-login connectivity.

<https://support.apple.com/guide/deployment/depabc994b84/>

This guide was written using the following hardware and software:

- Microsoft Entra ID
NOTE: This guide was created using Microsoft Entra with a P2 license. Depending on your license type, some features and options may vary. For example, certain screenshots or capabilities—such as creating groups in Microsoft Entra—may look different or be unavailable.
- Jamf Pro Server version 11.21 (Cloud Hosted)
- Jamf Connect version 3.3.0
- Self Service+ installed by default from Jamf Pro
- MacBook Air (M4) with macOS 26.1



The following items are needed to follow along with this guide:

- Self Service+: This guide installs it by default from Jamf Pro. You can also download it from your Jamf account.
- Jamf Composer: You can also download it from your Jamf account.
- Jamf Connect: Get it here: <http://jamf.it/JCDownload>
- A signing certificate. If you don't have one from Apple you can create one with Jamf Pro using instructions in the link below.
https://learn.jamf.com/en-US/bundle/technical-articles/page/Creating_a_Signing_Certificate_Using_Jamf_Pro's_Built-in_CA_to_Use_for_Signing_Configuration_Profiles_and_Packages.html

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

- The HCS Team
- Sean Rabbitt

Jamf Connect vs. Platform SSO

There has been some confusion regarding the role of Jamf Connect now that Platform SSO offers some overlapping functionality. The chart below provides a side-by-side comparison to highlight the features of each.

Feature	Jamf Connect	Platform SSO
User Account Creation	Creates the local macOS user account for the first or subsequent users. Supports zero-touch enrollment workflows.	Cannot create local user accounts on its own. A local account must exist before PSSO can be enabled.
Password Synchronization	Actively links the local account password with the cloud IdP password. A default check-in frequency (e.g., every 60 minutes) can be configured, and users can be prompted to change a mismatched password.	Syncs the password with the IdP but does not notify users when their IdP password has changed on another device. In some scenarios, users can use either the new or old password to log in.
Offline MFA	Provides offline multi-factor authentication (MFA) capabilities. Users can access their computer with a time-based one-time password (TOTP) from an authenticator app without an internet connection.	Does not provide offline MFA for macOS logins.
Privilege Management	Includes a privilege management feature that allows a standard user account to temporarily elevate to admin rights.	Does not offer a privilege management feature.
Branding and User Experience	Offers extensive branding and customization options for the macOS login window.	Customization and branding options are limited, as it uses the native macOS login window.
Zero-Touch Onboarding	Integral to streamlining zero-touch enrollment and providing a user-friendly setup experience.	Not designed for zero-touch enrollment on its own. Jamf Connect can create the user account needed for PSSO to be enabled later in the Setup Assistant.
Reliability	An extra layer between macOS and the IdP, which can introduce some friction during OS updates.	An Apple-native feature that is less likely to break with macOS updates.
Deployment	Deployed and configured via a Jamf Pro policy.	Deployed by pushing a single sign-on extension configuration profile via an Device Management Service solution like Jamf Pro.

To learn how to configure Jamf Pro and Intune Company Portal for macOS Platform SSO, please refer to our technical guide:

<https://hcsonline.com/support/resources/white-papers/how-to-configure-jamf-pro-and-intune-company-portal-for-macos-platform-sso-integration>



Section 1: Configure 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 section:

- Access to your Microsoft Entra ID with administrative privileges.
NOTE: This guide was created using Microsoft Entra with a P2 license. Depending on your license type, some features and options may vary. For example, certain screenshots or capabilities—such as creating groups in Microsoft Entra—may look different or be unavailable.

Jamf Connect supports an integration with Microsoft Entra ID as your cloud identity provider (IdP). With the integration, Jamf Connect and Microsoft Entra ID can communicate and provide several essential services:

- Sync local and network passwords
- Create local accounts and assign roles
- Secure the login window with network authentication, MFA, and Conditional Access controls

In this section, we will configure the following items to use Jamf Connect with Microsoft Entra ID:

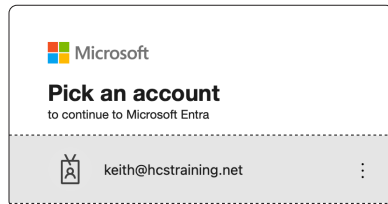
- Create an app registration
- Grant administrative consent for API calls
- Modify authentication settings
- Configure App Roles for Administrator and Standard users (Optional)
- Assign app roles to users and groups (Optional)
- Custom Branding the Microsoft Entra ID Sign In Logo (Optional)

NOTE: App roles and assignments are optional and not required. We will configure them in this section as they are used in a lot of organizations.

Learn more about app roles here:

<https://learn.jamf.com/en-US/bundle/jamf-connect-documentation-current/page/Designating-App-Roles.html>

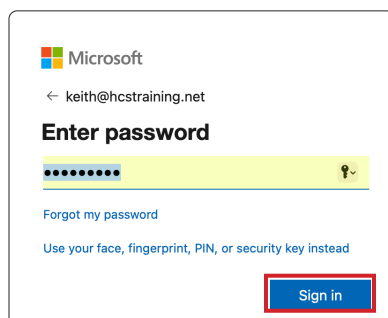
1. In a web browser, go to: <https://entra.microsoft.com/>
2. Log into Microsoft Entra ID with your administrative credentials.



3. Enter your password.

4. Click Sign in.

NOTE: This guide is using a password to sign in for simplicity. You should consider using a more secure authentication method such as you face, fingerprint, PIN or security key.

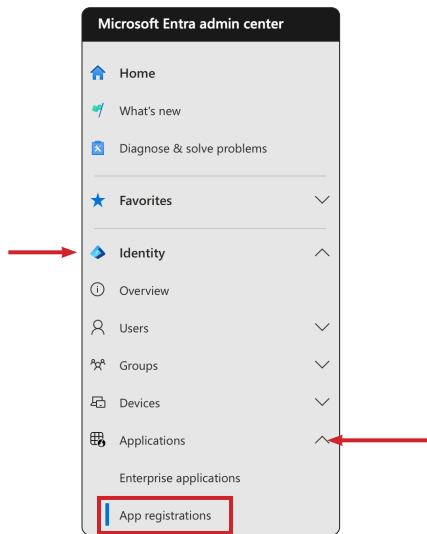




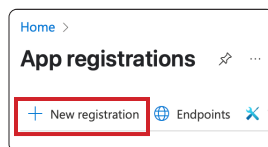
5. Make a selection of your choosing at the screen below. This guide will click Yes.



6. From the sidebar, select Identity > Applications > App registrations.



7. Click New registration.





8. Enter **Jamf Connect** for the Name.
9. Under Supported account types, select the radio button for Accounts in this organizational directory only ([YourCompanyName] only - Single tenant).
10. Under Redirect URI:
 - A. From the menu, select: Public client/native (mobile/desktop).
 - B. Enter `https://127.0.0.1/jamfconnect` in the field.
11. Click Register.

Home > App registrations > Register an application

Name
The user-facing display name for this application (this can be changed later).

8 Jamf Connect ✓

Supported account types
Who can use this application or access this API?

9 ☒ Accounts in this organizational directory only (HCS Training only - Single tenant)
☐ Accounts in any organizational directory (Any Microsoft Entra ID tenant - Multitenant)
☐ Accounts in any organizational directory (Any Microsoft Entra ID tenant - Multitenant) and personal Microsoft accounts (e.g. Skype, Xbox)
☐ Personal Microsoft accounts only

[Help me choose...](#)

Redirect URI (optional)
We'll return the authentication response to this URI after successfully authenticating the user. Providing this now is optional and it can be changed later, but a value is required for most authentication scenarios.

10A Public client/native (mobile ... 10B `https://127.0.0.1/jamfconnect`

Register an app you're working on here. Integrate gallery apps and other apps from outside your organization by adding from [Enterprise applications](#).

By proceeding, you agree to the [Microsoft Platform Policies](#)

11 Register

12. Open TextEdit.app and create a new document named Jamf Connect Info. Save it to your Desktop.





13. Switch back to Microsoft Entra and copy the following information and paste it into the Jamf Connect Info document we created in the previous step.
 - A. Application (client) ID.
 - B. Directory (tenant) ID.

Home > App registrations > Jamf Connect

Search

Delete Endpoints Preview features

Overview

Quickstart

Integration assistant

Diagnose and solve problems

Manage

Branding & properties

Authentication

Certificates & secrets

Token configuration

API permissions

Expose an API

App roles

Owners

Roles and administrators

Manifest

Support + Troubleshooting

New support request

Essentials

Display name: Jamf Connect

Application (client) ID: acb1b1b1-b1b1-b1b1-b1b1-b1b1b1b1b1b1

Object ID: 95a8b1b1-b1b1-b1b1-b1b1-b1b1b1b1b1b1

Directory (tenant) ID: d4c1b1b1-b1b1-b1b1-b1b1-b1b1b1b1b1b1

Client credentials: Add a certificate or secret

Redirect URIs: 0 web, 0 spa, 1 public client

Application ID URI: Add an Application ID URI

Managed application in local directory: Jamf Connect

Supported account types: My organization only

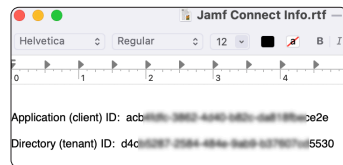
Welcome to the new and improved App registrations. Looking to learn how it's changed from App registrations (Legacy)? [Learn more](#)

Starting June 30th, 2020 we will no longer add any new features to Azure Active Directory Authentication Library (ADAL) and Azure Active Directory Graph. We will continue to provide technical support and security updates but we will no longer provide feature updates. Applications will need to be upgraded to Microsoft Authentication Library (MSAL) and Microsoft Graph. [Learn more](#)

Get Started Documentation

Copy these IDs and paste into a document for later use.

14. Confirm your document has the items shown below and save the changes.



15. Switch back to Microsoft Entra.
16. Click API permissions.
17. Click Grant admin consent for [Your company name] (HCS Training is shown in the example).

Home > App registrations > Jamf Connect

Jamf Connect | API permissions

Search

Refresh Got feedback?

Overview

Quickstart

Integration assistant

Diagnose and solve problems

Manage

Branding & properties

Authentication

Certificates & secrets

Token configuration

API permissions

Expose an API

App roles

Owners

Roles and administrators

Manifest

Granting tenant-wide consent may revoke permissions that have already been granted tenant-wide for that application. Permissions that users have already granted on their own behalf aren't affected. [Learn more](#)

The "Admin consent required" column shows the default value for an organization. However, user consent can be customized per permission, user, or app. This column may not reflect the value in your organization, or in organizations where this app will be used. [Learn more](#)

Configured permissions

Applications are authorized to call APIs when they are granted permissions by users/admins as part of the consent process. The list of configured permissions should include all the permissions the application needs. [Learn more about permissions and consent](#)

+ Add a permission

Grant admin consent for HCS Training

API / Permissions name	Type	Description	Admin consent
Microsoft Graph (1)			
User.Read	Delegated	Sign in and read user profile	No




18. Click Yes.

Grant admin consent confirmation.

Do you want to grant consent for the requested permissions for all accounts in HCS Training? This will update any existing admin consent records this application already has to match what is listed below.

19. Confirm Permission was granted.

 **Grant consent** ×

Grant consent successful

20. Click Authentication.

21. Scroll down to the Advanced settings section and select Yes to Allow public client flows.

22. Click Save. This completes the App registration configuration.

Home > App registrations > Jamf Connect

Jamf Connect | Authentication ×

Search « [Got feedback?](#)

Overview

- Quickstart
- Integration assistant
- Diagnose and solve problems

Manage

- Branding & properties
- Authentication**
- Certificates & secrets
- Token configuration
- API permissions
- Expose an API
- App roles
- Owners
- Roles and administrators
- Manifest

Support + Troubleshooting

- New support request


Supported account types

Who can use this application or access this API?

☒ Accounts in this organizational directory only (HCS Training only - Single tenant)

☐ Accounts in any organizational directory (Any Microsoft Entra ID tenant - Multitenant)

[Help me decide...](#)

 Due to temporary differences in supported functionality, we don't recommend enabling personal Microsoft accounts for an existing registration. If you need to enable personal accounts, you can do so using the manifest editor. [Learn more about these restrictions.](#) ×

Advanced settings

Allow public client flows ⓘ

Enable the following mobile and desktop flows:

- App collects plaintext password (Resource Owner Password Credential Flow) [Learn more](#)
- No keyboard (Device Code Flow) [Learn more](#)
- SSO for domain-joined Windows (Windows Integrated Auth Flow) [Learn more](#)

App instance property lock ⓘ

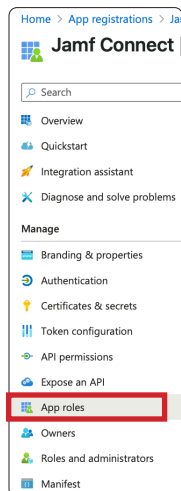
Configure the application instance modification lock. [Learn more](#) [Configure](#)

22

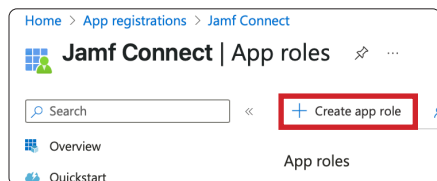


In Microsoft Entra, App Roles can be leveraged with Jamf Connect to manage access and enforce user permissions during macOS login. By evaluating role claims, App Roles allow organizations to dynamically assign local account privileges on macOS. For example, if a user holds an administrator role in Entra but is a standard user on the Mac, Jamf Connect can elevate the account to administrator. Conversely, if a user has admin rights on the Mac but is assigned a standard role in Entra, the account can be downgraded to a standard user to match the directory role. The next steps are optional and not required for Jamf Connect.

23. Click App roles.



24. Click Create app role.





25. Enter **Jamf Connect Administrators** for the Display Name.
26. Under Allowed member types, select the radio button for Users/Groups.
27. Enter **Administrator** for the Value (This defines the role assigned to the user).
28. Enter **This App role will assign administrative privileges to a local macOS account** for the Description.
29. Verify the checkbox is selected for Do you want to enable this app role?
30. Click Apply.

The screenshot shows the 'Create app role' dialog box with the following fields and annotations:

- 25**: Points to the 'Display name' field containing 'Jamf Connect Administrators'.
- 26**: Points to the 'Allowed member types' section, where the 'Users/Groups' radio button is selected.
- 27**: Points to the 'Value' field containing 'Administrator'.
- 28**: Points to the 'Description' field containing 'This App role will assign administrative privileges to a local macOS account'.
- 29**: Points to the 'Do you want to enable this app role?' checkbox, which is checked.
- 30**: Points to the 'Apply' button at the bottom left.

31. Confirm the Jamf Connect Administrators App role shows in the list.
32. Click Create app role (+).

The screenshot shows the 'Jamf Connect | App roles' page. The left sidebar contains navigation links: Overview, Quickstart, Integration assistant, Diagnose and solve problems, Manage, Branding & properties, Authentication, Certificates & secrets, Token configuration, API permissions, Expose an API, and App roles. The main content area shows the 'App roles' section with a table of existing roles.

32: Points to the '+ Create app role' button at the top of the main content area.

31: Points to the 'Jamf Connect Administrators' row in the table.

Display name	Description	Allowed member types	Value	ID	State
Jamf Connect Administrators	This App role will assign administr...	Users/Groups	Administrator	6b70c1da-17...	Enabled



33. Enter **Jamf Connect Standard Users** for the Display Name.
34. Under Allowed member types, select the radio button for Users/Groups.
35. Enter **Standard** for the Value (This defines the role assigned to the user).
36. Enter **This App role will assign standard privileges to a local macOS account** for the Description.
37. Verify the checkbox is selected for Do you want to enable this app role?
38. Click Apply.

The screenshot shows the 'Create app role' dialog box. Red callout numbers 33 through 38 point to specific fields and controls:

- 33: Display name field containing 'Jamf Connect Standard Users'.
- 34: Allowed member types section with 'Users/Groups' selected.
- 35: Value field containing 'Standard'.
- 36: Description field containing 'This App role will assign standard privileges to a local macOS account'.
- 37: 'Do you want to enable this app role?' checkbox, which is checked.
- 38: 'Apply' button at the bottom.

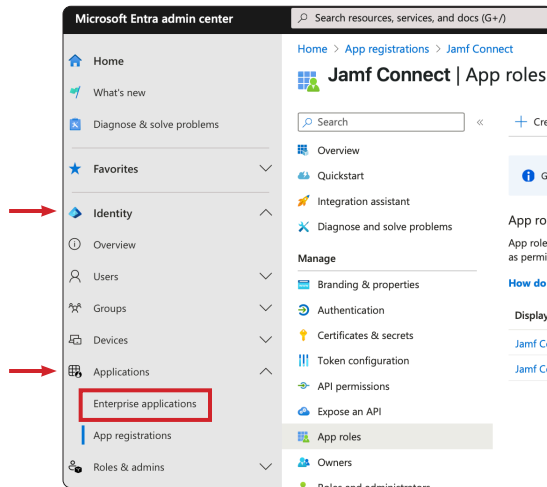
39. Confirm both App roles show in the list.

The screenshot shows the 'Jamf Connect | App roles' page. A table lists the created app roles. The first two roles, 'Jamf Connect Administrators' and 'Jamf Connect Standard Users', are highlighted with a red box.

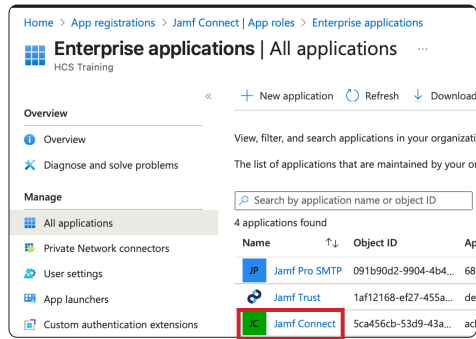
Display name	Description	Allowed member types	Value	ID	State
Jamf Connect Administrators	This App role will assign administr...	Users/Groups	Administrator	6b70c1da-17...	Enabled
Jamf Connect Standard Users	This App role will assign standard ...	Users/Groups	Standard	36a5d7d1-fcf...	Enabled



40. In the sidebar, select Identity > Applications > Enterprise applications.

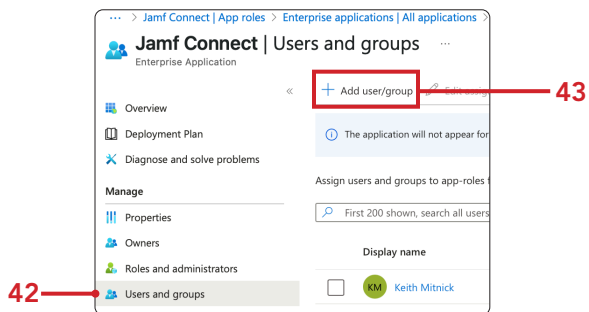


41. Click the Jamf Connect application.



42. Click Users and groups.

43. Click Add user/group (+).





44. Under Users and groups, click None Selected.

A screenshot of the 'Add Assignment' dialog box. The title bar shows 'Enterprise applications' and 'Add Assignment'. Below the title, it says 'HCS Training'. Under the 'Users and groups' section, there is a button labeled 'None Selected' which is highlighted with a red rectangle. Below that, it says 'Select a role *' and another button labeled 'None Selected'.

45. You can select a user or a group. This guide will select a user:

- A. Select a user of your choosing.
- B. Click Select.

A screenshot of the 'Users and groups' selection screen. At the top, there is a search bar and a message 'Try changing or adding filters if you don't see what you're looking for.' Below the search bar, it says '4 results found'. There are tabs for 'All', 'Users', and 'Groups'. The 'Users' tab is selected. Below the tabs is a table with columns 'Name', 'Type', and 'Details'. The table contains four rows: 'Craig Cohen' (User, craig@hcstraining.net), 'HCS Executives' (Group), 'Keith Mitnick' (User, keith@hcstraining.net), and 'JamfProSMTP' (Group, jamfsmtp@hcstraining.net). A red box labeled 'A' highlights the checkbox next to 'Craig Cohen'. At the bottom of the screen, there is a blue button labeled 'Select' which is highlighted with a red box labeled 'B'.

46. Under Select a role, click None Selected.

A screenshot of the 'Add Assignment' dialog box after selecting a user. The title bar shows 'Enterprise applications' and 'Add Assignment'. Below the title, it says 'HCS Training'. Under the 'Users and groups' section, it says '1 user selected.' Below that, it says 'Select a role *' and a button labeled 'None Selected' which is highlighted with a red rectangle.



47. Select Jamf Connect Standard Users.

48. Click Select.

A screenshot of a mobile application dialog box titled "Select a role" with a close button (X) in the top right corner. Below the title is the instruction "Only a single role can be selected". There is a search bar with the placeholder text "Enter role name to filter items...". Below the search bar, there are two list items: "Jamf Connect Administrators" and "Jamf Connect Standard Users". The "Jamf Connect Standard Users" item is highlighted with a red box, and a red arrow labeled "47" points to it. At the bottom of the dialog, there is a section titled "Selected Role" which displays "Jamf Connect Standard Users". Below this, there is a blue button labeled "Select" with a red box around it and a red arrow labeled "48" pointing to it.

49. Click Assign.

A screenshot of a mobile application screen titled "Add Assignment" with a breadcrumb trail "... > Enterprise applications |". Below the title is the text "HCS Training". There is a section titled "Users and groups" which contains the text "1 user selected." and "Select a role *". Below this, there is a list item "Jamf Connect Standard Users" which is highlighted with a red box. At the bottom of the screen, there is a blue button labeled "Assign" with a red box around it.



50. Confirm the user shows in the list and is assigned the Jamf Connect Standard Users role.

51. Click Add user/group.

Home > App registrations > Jamf Connect | App roles > Enterprise applications | All applications > Jamf Connect | Users and groups > Users > Enterprise applications

Jamf Connect | Users and groups

Enterprise Application

« **+ Add user/group** Edit assignment Remove assignment Update credential Refresh

The application will not appear for assigned users within My Apps. Set 'visible to users?' to yes in properties to enable this.

Assign users and groups to app-roles for your application here. To create new app-roles for this application, use the app roles page.

First 200 shown, search all users & groups

	Display name	Object type	Role assigned
<input type="checkbox"/>	Craig Cohen	User	Jamf Connect Standard Users

52. Under Users and groups, click None Selected.

... > Enterprise applications | HCS Training

Add Assignment

HCS Training

Users and groups

None Selected

Select a role *

None Selected

53. You can select a user or a group. This guide will select a user:

- A. Select a user of your choosing.
- B. Click Select.

Users and groups

Try changing or adding filters if you don't see what you're looking for.

Search

4 results found

All Users Groups

	Name	Type	Details
<input type="checkbox"/>	Craig Cohen	User	craig@hcstraining.net
<input type="checkbox"/>	HCS Executives	Group	
<input checked="" type="checkbox"/>	Keith Mitnick	User	keith@hcstraining.net
<input type="checkbox"/>	JamfProSMTP	Group	jamfsmtp@hcstraining.net

Select

54. Under Select a role, click None Selected.

... > Enterprise applications | HCS Training

Add Assignment

HCS Training

Users and groups

1 user selected.

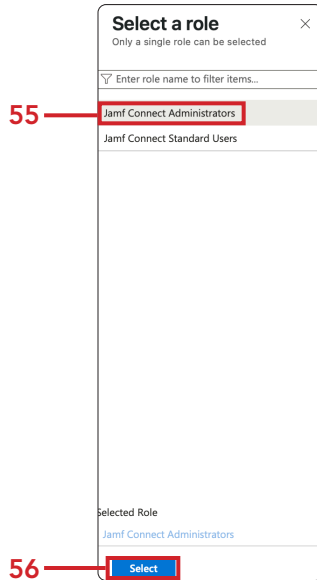
Select a role *

None Selected



55. Select Jamf Connect Administrators.

56. Click Select.

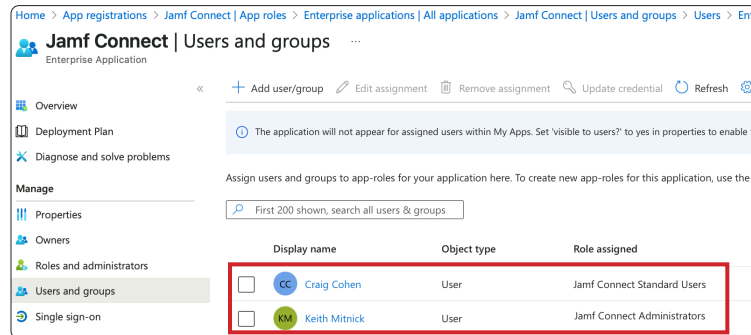


57. Click Assign.



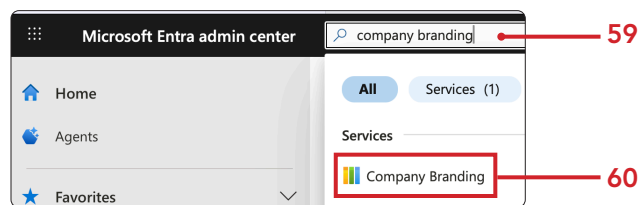


58. Confirm both users show in the list and are assigned the proper roles. This completes the role configuration.



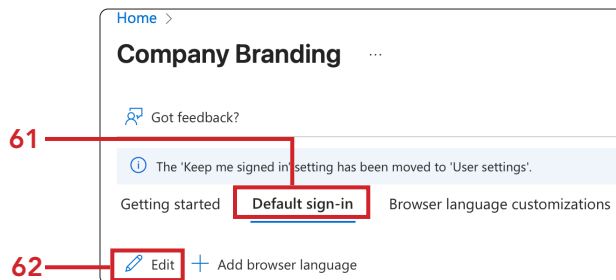
59. Let's configure the Microsoft Entra ID Sign In Logo to use your company logo. In the search field, Enter **company branding**.

60. Select Company Branding from the services section.



61. Click Default sign-in.

62. Click Edit.



63. Click Sign-in form.





64. Click browse to select and upload your branded sign in logo.
NOTE: the image size and file type show in the picture.

Basics Layout Header Footer **Sign-in form** Review

Configure other elements such as images, text and hyperlinks inside of the sign-in form.

Banner logo ⓘ **Browse**

Image size: 245x36px
Max file size: 50KB
File Type: Transparent PNG,
JPG, or JPEG

Follow the requirements for the image to be uploaded.

65. Click Review + save.

Basics Layout Header Footer **Sign-in form** Review

Configure other elements such as images, text and hyperlinks inside of the sign-in form.

Banner logo ⓘ **Browse**




Image size: 245x36px
Max file size: 50KB
File Type: Transparent PNG,
JPG, or JPEG

[Remove](#)

Review + save < Previous Next: Review >



66. Click Save.

This screenshot shows the 'Review' tab of a branding configuration interface. At the top, there are tabs for 'Basics', 'Layout', 'Header', 'Footer', 'Sign-in form', and 'Review', with 'Review' being the active tab. A warning message at the top states: 'Any file that you upload, or data that you input, will be publicly available to any user'. The interface is divided into sections: 'Basics' (Favicon, Background image, Page background color), 'Layout' (Template, Header, Footer, Custom CSS), 'Header' (Header), and 'Footer' (Show 'Privacy & Cookies', Display text). At the bottom, there is a blue 'Save' button highlighted with a red box, and 'Previous' and 'Next' navigation buttons.

67. Scroll down to the Sign-in form section and confirm the Banner logo says "Configured". This completes the branding. Log out of Microsoft Entra ID.

This screenshot shows the 'Sign-in form' section of the branding configuration interface. A red arrow points to the 'Sign-in form' tab. The 'Banner logo' is set to 'Configured', which is highlighted with a red box. The 'Square logo (light theme)' is set to 'Not provided'. Other options like 'Show 'Privacy & Cookies'', 'Display text', and 'URL' are also visible.

This completes this section. In the next section, we will use Jamf Composer to create a package for branding Jamf Connect with your organizations logo.



Section 2 - Create a package for branding Jamf Connect

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:

- Jamf Composer
- Branding images for your organization
- Scripts for Login Window and Menu Bar (optional)
- A signing certificate - If you don't have one, create one using these instructions.

https://learn.jamf.com/en-US/bundle/technical-articles/page/Creating_a_Signing_Certificate_Using_Jamf_Pro's_Built-in_CA_to_Use_for_Signing_Configuration_Profiles_and_Packages.html

The recommended size for branding icons: (This guide will use PNG files)

- Menu bar icons: 16 x 16 pixels
- Sign in Logo 449 x 131 pixels
- Login logo: 250 pixels height. The width is flexible

Follow the instructions in the link to download Jamf Composer.

<https://account.jamf.com/products/other/composer/download>

You may also use any other packaging software you are comfortable with.

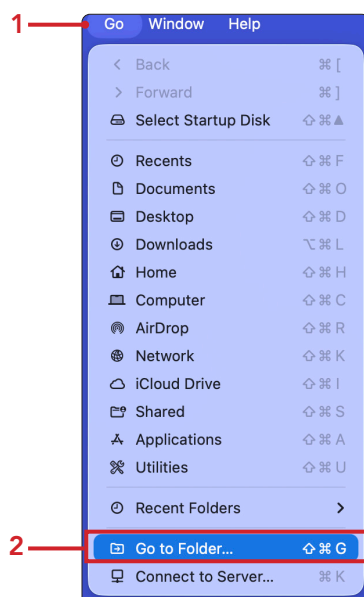
To follow along with this section you will need your branding images, Login Window scripts, and Menu bar scripts readily available. This guide assumes those items are located on your Desktop. If you don't have these items readily available, you may download HCS' branding images and scripts at:

<https://hcsonline.com/images/files/JamfConnectCustomizations.zip>

In this section we will create a folder structure for branding images, Login Window scripts, and Menu bar scripts. Once the structure is created, we will add our branding images, Login Window scripts, and Menu bar scripts to the corresponding folders and use Jamf Composer to set permissions and create a package to deploy to all computers.

1. In the Finder, click the Go menu.

2. Select Go To Folder.

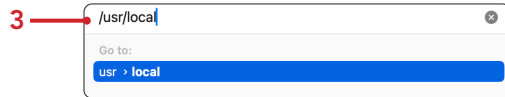




3. Enter the following path:

`/usr/local/`

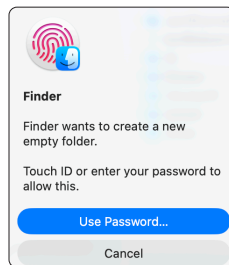
4. Press Enter.



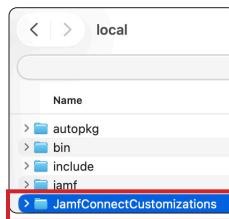
5. Click the File menu, then select New Folder.



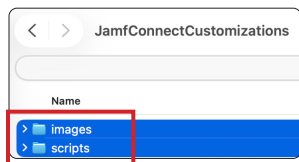
6. You will be prompted for Touch ID or your user name and password. This guide will use Touch ID.



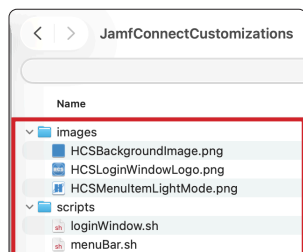
7. Name the folder JamfConnectCustomizations and open the folder.



8. Create two folders inside the JamfConnectCustomizations folder named images and scripts.



9. Move your images and scripts into the appropriate folders. If you downloaded the HCS images and scripts at the beginning of this guide, they will be located on your Desktop in a folder named images-scripts.



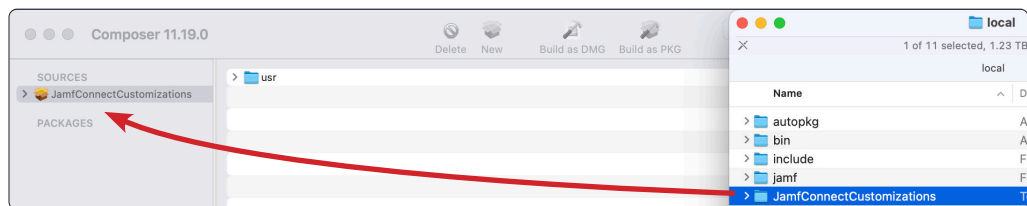


10. Open Jamf Composer located in the Applications folder.

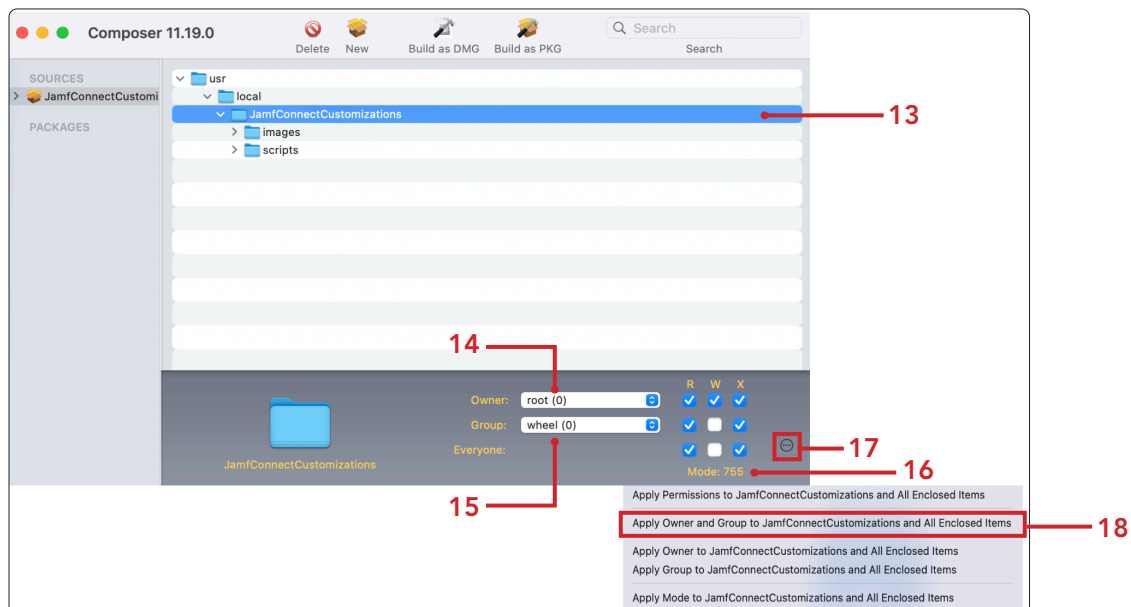


Composer.app

11. Drag the JamfConnectCustomizations folder from /usr/local to the SOURCES section of Jamf Composer.

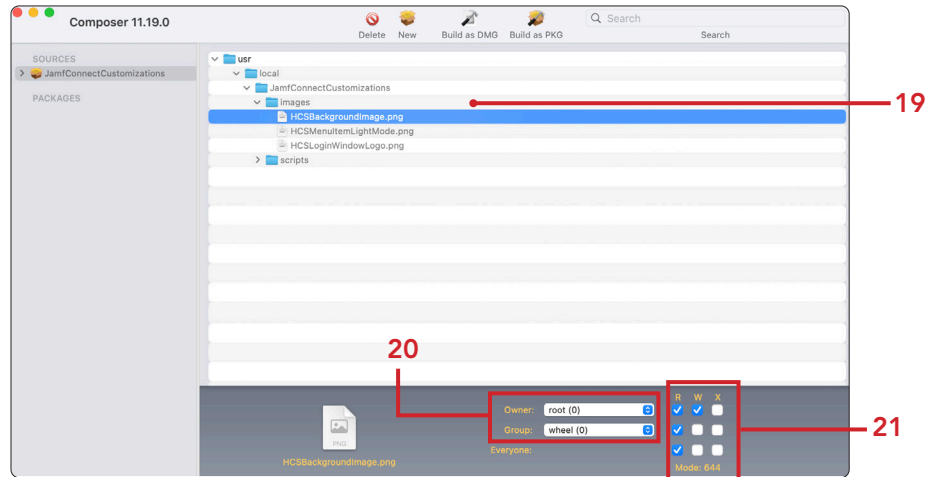


12. Expand /usr/local/ to show JamfConnectCustomizations.
13. Select the JamfConnectCustomizations folder.
14. Change the Owner to root (0).
15. Change the Group to wheel (0).
16. Confirm the permissions are set to 755 as shown in the screen shot below.
17. Click the Action Menu (ⓘ).
18. Select Apply Owner and Group to JamfConnectCustomizations and All Enclosed Items.

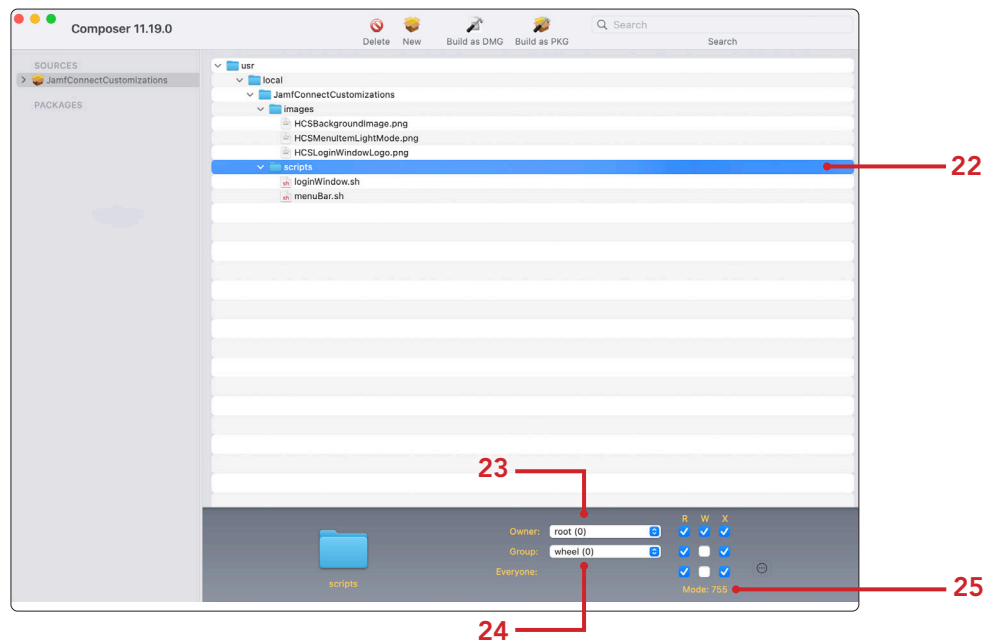




19. Expand the images folder.
20. For each file in the images folder, confirm the owner is: root and the group is wheel.
21. Set the permissions for each file in the images folder to 644 as shown in the screen shot below.



22. Select the scripts folder.
23. Confirm the owner is root (0).
24. Confirm sure the group is wheel (0).
25. Confirm the permissions are set to 755 for the scripts folder and all enclosed items as shown in the screen shot below.





26. Click the Composer menu.

27. Select Settings.



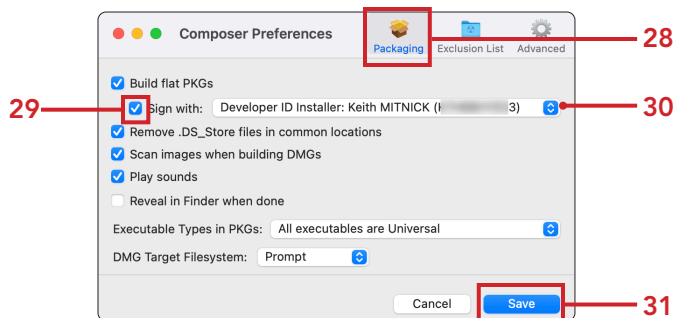
28. Select Packaging.

29. Confirm the checkbox is selected for Sign with.

30. From the menu, select your signing certificate.

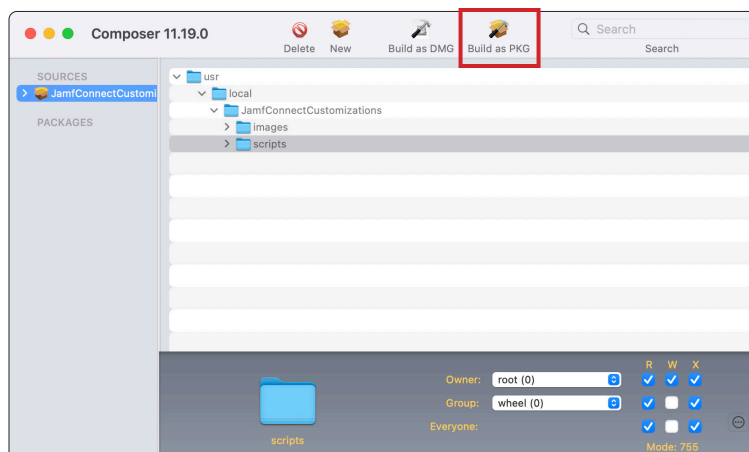
31. Click Save.

NOTE: This package must be signed if you want to use it in a Prestage enrollment.



32. Click Build as PKG.

NOTE: You may be prompted for administrative credentials to sign the package.





33. Save the package to your Desktop.



34. Confirm the package was created.



This completes this section. In the next section, we will test our connection to Microsoft Entra ID using the Jamf Connect Configuration App.



Section 3 - Test connection to Microsoft Entra ID using the Jamf Connect Configuration App

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 user account in Microsoft Entra ID
- Jamf Connect Configuration App. Get it here: <http://jamf.it/JCDownload>
- The Jamf Connect Info document created in section one of this guide

In this section, we will test OIDC and ROPG connections to Microsoft Entra ID using the Jamf Connect Configuration App.

What is OIDC and ROPG:

OIDC (OpenID Connect) is the recommended authentication method for Jamf Connect. It uses secure, standards-based flows (like authorization code with PKCE) to authenticate users through a browser. This allows support for MFA, SSO, and modern identity provider policies. It's ideal for macOS login, account creation, and secure token handling.

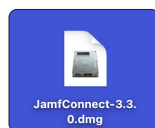
ROPG (Resource Owner Password Grant) is a legacy flow where the app directly collects the user's username and password to get a token. While supported by Jamf Connect for password syncing, it's discouraged by Microsoft and others due to security risks—it bypasses MFA and requires handling user credentials directly.

NOTE: Jamf Connect 2.45.1 was the last version to include Jamf Connect Login and Jamf Connect Menu Bar in the same package. With the introduction of Self Service+, Jamf Connect Menu Bar is incorporated into Self Service+. This guide will use Jamf Connect 3.3.0 with Self Service+ 2.6.0.

1. Using a web browser of your choosing, download the latest version of Jamf Connect here:

<http://jamf.it/JCDownload>

2. Open the JamfConnect-3.3.0.dmg. In this guide, it's located in the Downloads folder.

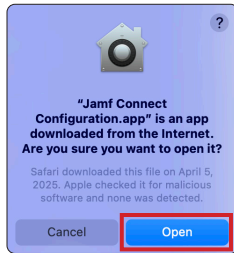


3. Drag the Jamf Connect Configuration.app to the Applications folder and open the app.

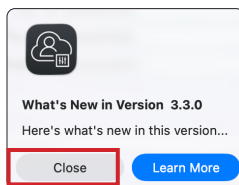




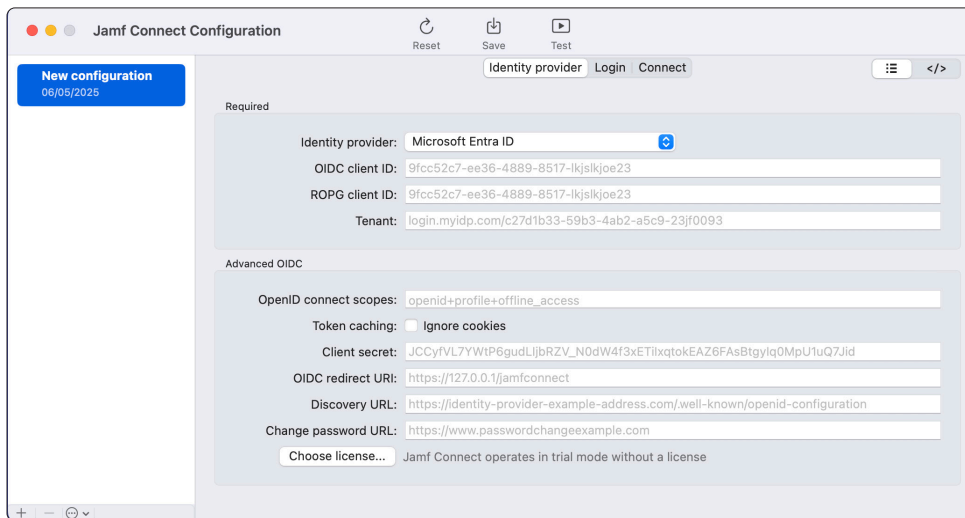
4. Click Open.



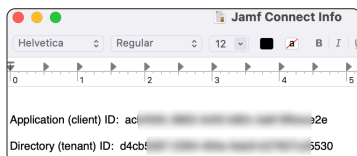
5. If presented with the screen below, make a selection of your choosing, this guide will click Close.



6. You are presented with a default configuration named New configuration.



7. Open the Jamf Connect Info file located on your Desktop. We created the file in section one of this guide.

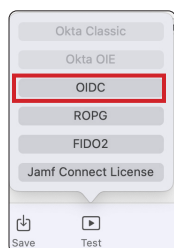




8. Switch back to the Jamf Connect Configuration app. Rename the configuration to JC Entra ID or a name of your choosing.
9. Click Identity provider.
10. Select Microsoft Entra ID for Identity provider.
11. Copy and paste the Application (client) ID from the Jamf Connect Info document in to the OIDC client ID field.
12. Copy and paste the Application (client) ID from the Jamf Connect Info document in to the ROPG client ID field.
13. Copy and paste the Directory (tenant) ID from the Jamf Connect Info document in to the Tenant field.
14. Enter <https://127.0.0.1/jamfconnect> in the OIDC redirect URL field.
15. Enter <https://mysignins.microsoft.com/security-info/password/change> in the Change password URL field. (This setting is optional. Only configure this if your organization allow users to change passwords).
16. Click the Test button.

The screenshot shows the 'Jamf Connect Configuration' app interface. On the left, a sidebar contains a list of configurations, with 'JC Entra ID' (dated 09/30/2025) highlighted by a red box and labeled with a red '8'. The main area is titled 'Identity provider' (labeled with a red '9') and has buttons for 'Login' and 'Connect'. Below this, there are two sections: 'Required' and 'Advanced OIDC'. The 'Required' section contains four fields: 'Identity provider' (set to 'Microsoft Entra ID', labeled with a red '10'), 'OIDC client ID' (labeled with a red '11'), 'ROPG client ID' (labeled with a red '12'), and 'Tenant' (labeled with a red '13'). The 'Advanced OIDC' section contains five fields: 'OpenID connect scopes' (set to 'openid+profile+offline_access'), 'Token caching' (set to 'Ignore cookies'), 'Client secret' (labeled with a red '14'), 'OIDC redirect URL' (set to 'https://127.0.0.1/jamfconnect', labeled with a red '14'), and 'Change password URL' (set to 'https://mysignins.microsoft.com/security-info/password/change', labeled with a red '15'). At the bottom of the 'Advanced OIDC' section, there is a 'Choose license...' button and a note: 'Jamf Connect operates in trial mode without a license'. A red '16' points to the 'Test' button at the top right of the app.

17. Select OIDC.

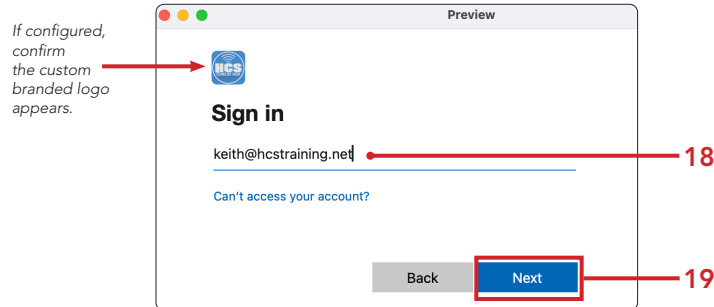




18. Enter your Microsoft Entra ID account name.

19. Click Next.

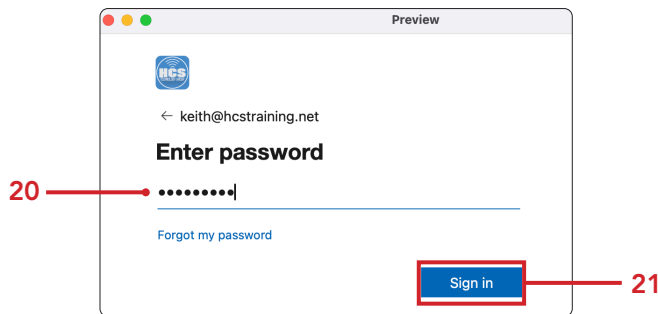
NOTE: If you configured the optional custom branded logo in section one of this guide, you will see your branded logo at the sign in screen instead of the Microsoft Entra logo.



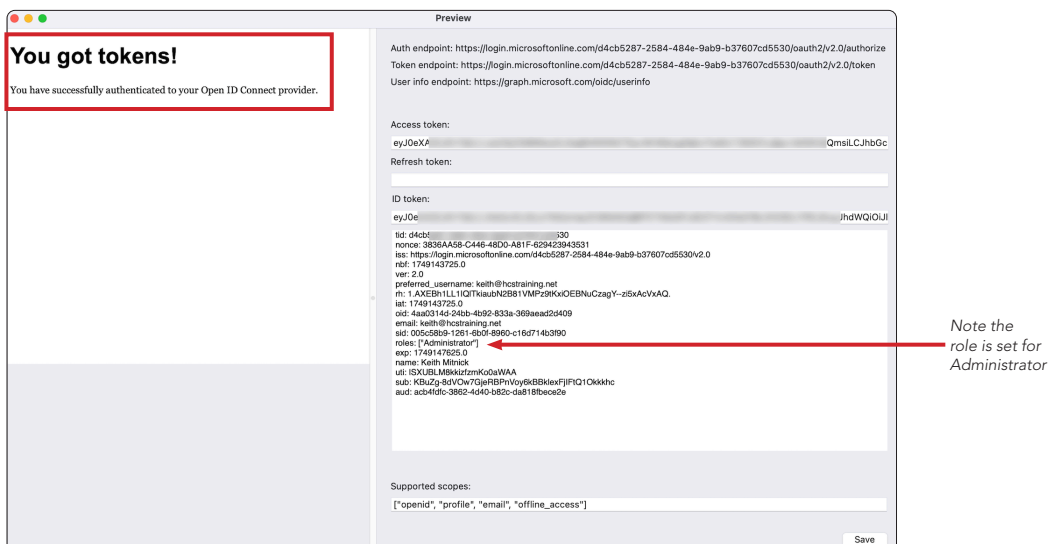
20. Enter your password.

21. Click Sign in.

NOTE: If your organization is using Multi Factor Authentication (MFA), you may see more authentication screens than shown in this guide.

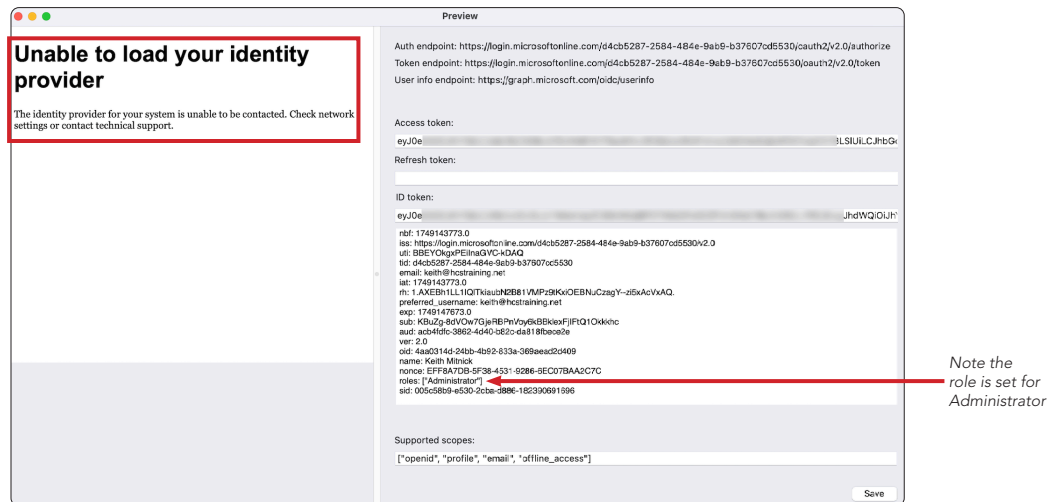


22. If you are greeted with "You got tokens!", the connection was successful. Have a look at the ID token section. You will see all the information returned in the token which includes the role of your account. Close this window when done.



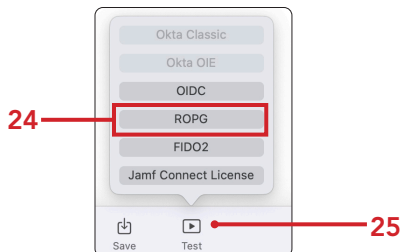


23. There is a known bug in the Jamf Connect Configuration App that will show an error message that says "Unable to load your identity provider". If you see this message, you will notice that all of the token information is valid which means the connection to Microsoft Entra ID was successful. Jamf is aware of this bug and hopefully it will be resolved in a later version. Close this window when done.



24. Click Test.

25. Select ROPG.

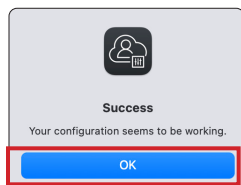


26. Enter your Microsoft Entra ID credentials and click Sign in.





27. If you are greeted with the message below, the connection was successful. Click OK.



This completes this section. In the next section, we will create a configuration profile for use with Jamf Connect.



Section 4: Create a Configuration Profile for Jamf Connect

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:

- Access to a Jamf Pro server with administrative privileges
- Jamf Connect Configuration App.
- Jamf Connect License (Optional)

NOTE: If you have a license for Jamf Connect, log into your Jamf Account at: <https://account.jamf.com> and select Solutions from the sidebar. Select View Details for Jamf Connect . Select the copy license to clipboard link and paste the license into a text document and save it on your Desktop. This is optional and not required to following along with this guide as Jamf Connect can run in trial mode.

In this section, we will add additional settings to the Jamf Connect configuration created in Section 3 of this guide.

1. In the Jamf Connect Configuration App, click Login.

The screenshot shows the Jamf Connect Configuration App interface. The title bar reads "Jamf Connect Configuration". Below the title bar, there are buttons for "Reset", "Save", "Test", "Identity provider", "Login" (highlighted with a red box), and "Connect". On the left side, there is a sidebar with a button labeled "JC Entra ID" and a date "09/30/2025". The main content area is divided into two sections: "Required" and "Advanced OIDC". The "Required" section contains fields for "Identity provider" (set to "Microsoft Entra ID"), "OIDC client ID" (set to "act...ce2e"), "ROPG client ID" (set to "act...ce2e"), and "Tenant" (set to "d4ct...5530"). The "Advanced OIDC" section contains fields for "OpenID connect scopes" (set to "openid+profile+offline_access"), "Token caching" (set to "Ignore cookies"), "Client secret" (set to "JCCyVVL7YYWtP6gudLjBtRZV_N0dW4f3xEtixqokEAZ6FAsBtgylq0MpU1uQ7Jid"), "OIDC redirect URI" (set to "https://127.0.0.1/jamfconnect"), "Discovery URL" (set to "https://identity-provider-example-address.com/well-known/openid-configuration"), and "Change password URL" (set to "https://mysignins.microsoft.com/security-info/password/change"). At the bottom of the "Advanced OIDC" section, there is a button labeled "Choose license..." and a note that says "Jamf Connect operates in trial mode without a license".



2. Enter **Administrator** for Admin roles (This is the role created in Microsoft Entra ID in section one of this guide.)
3. Enter **roles** for Admin attribute (This reports the role to Jamf Connect from Microsoft Entra ID. I.E. Administrator or Standard user.)
4. For Account migration, select the checkbox for:
 - Connect existing local users to a network account: Enabled.
 - Hide the "Create new user" option from users during account migration: Enabled.
5. In the Hide Users field, enter the name of a user you don't want to show in the migration screen. I.E. a local admin, Managed Admin, or Jamf Management Framework account. Separate each user with a comma.
6. Verify the checkbox is selected for Create Jamf Connect Keychain.
7. For Authentication, deselect the checkbox for Always require network authentication. (See NOTE).
8. For Local fallback, select the checkbox for:
 - Allow local authentication if a network is unavailable.
 - Use Passthrough Authentication.

NOTE: To use the Passthrough setting, the "Always Require Network Authentication" option must be disabled. If it is enabled, users will be prompted for their password twice; once at the FileVault pre-boot screen and again at the Jamf Connect login window. With Passthrough, the credentials entered at the FileVault pre-boot screen are automatically passed to the Jamf Connect login window, eliminating the need to enter them a second time. Initial password needs to be enabled and then disabled to create the key for Entra for passthrough to work. For more information, go to: <https://learn.jamf.com/en-US/bundle/jamf-connect-documentation-current/page/PassthroughAuthentication.html>

Initial password needs to be enabled and then disabled for passthrough to work

The screenshot shows the 'Identity provider' configuration window for Jamf Connect. The window is divided into two main sections: 'User creation' and 'Authentication'. Red lines with numbers 1 through 8 point to specific settings in the interface.

- 1. Points to the 'Initial password' section, where the checkbox 'Create a separate local password' is selected.
- 2. Points to the 'Admin roles' field, which contains the value 'Administrator'.
- 3. Points to the 'Admin attribute' field, which contains the value 'roles'.
- 4. Points to the 'Account migration' section, where both checkboxes 'Connect existing local users to a network account' and 'Hide the "Create new user" option from users during account migration' are selected.
- 5. Points to the 'Hide users' field, which contains the value 'hcs'.
- 6. Points to the 'Keychain' section, where the checkbox 'Create Jamf Connect keychain' is selected.
- 7. Points to the 'Authentication' section, where the checkbox 'Always require network authentication' is deselected.
- 8. Points to the 'Local fallback' section, where both checkboxes 'Allow local authentication if a network unavailable' and 'Use Passthrough Authentication' are selected.



9. Scroll down to the Appearance section. For Internet, select the checkbox for Allow network selection.
10. Enter **Welcome to HCS Technology Group** (Add your own message) for Login window message.
11. Enter `/usr/local/JamfConnectCustomizations/images/HCSBackgroundImage.png` for the Background field.
NOTE: Jamf recommends the following locations for storing branded images:
 - `/usr/local/`, `/Users/Shared/`,
 - `/Library/Application Support`.
- Learn more here:
<https://learn.jamf.com/en-US/bundle/jamf-connect-documentation-current/page/CustomBranding.html>
12. Enter `/usr/local/JamfConnectCustomizations/images/HCSLoginWindowLogo.png` for Login logo field.
13. From the Login window size menu, select a size that works best for you. This guide will select Max.

The screenshot shows the 'Appearance' configuration window. A red box labeled '9' highlights the 'Appearance' tab. A red box labeled '10' highlights the 'Login window message' field containing 'Welcome to HCS Technology Group'. A red box labeled '11' highlights the 'Background' field containing the path '/usr/local/JamfConnectCustomizations/images/HCSBackgroundImage.png'. A red box labeled '12' highlights the 'Login logo' field containing the path '/usr/local/JamfConnectCustomizations/images/HCSLoginWindowLogo.png'. A red box labeled '13' highlights the 'Login window size' dropdown menu, which is set to 'Max'.

14. Scroll down to the Script section and enter the path to your login script. This guide will use:
`/usr/local/JamfConnectCustomizations/scripts/loginWindow.sh`

The screenshot shows the 'Script' configuration window. A red box labeled '14' highlights the 'Script path' field containing the path '/usr/local/JamfConnectCustomizations/scripts/loginWindow.sh'.

15. Click the Identity provider tab.
16. Copy the contents of the Tenant field.

The screenshot shows the 'Identity provider' configuration window. A red box labeled '15' highlights the 'Identity provider' tab. A red box labeled '16' highlights the 'Tenant' field containing the value 'd4d5530'.



17. Click the Connect tab.
18. In the Authentication section, paste in the Tenant ID you copied in the previous step in the ROPG tenant field.
19. In the Sign in section, enter `/usr/local/JamfConnectCustomizations/images/HCSLoginWindowLogo.png` in the Sign in logo field.
20. In the Sign in section, select the checkbox for Automatic sign-in.
21. In the Custom Branding section, enter `/usr/local/JamfConnectCustomizations/images/HCSMenuitemLightMode.png` for the Light mode icon field.
22. In the Custom Branding section, enter `/usr/local/JamfConnectCustomizations/images/HCSMenuitemLightMode.png` for the Dark mode icon field.
23. In the Custom Branding section, Show welcome window: You need to enable it then disable it. This will set it to disabled. The xml is set to enable by default.
NOTE: For simplicity in this guide, the Login Window logo is the same logo as the Sign in Logo and the Light and Dark mode icons are also the same.

The screenshot shows the Jamf Connect configuration interface with the following sections and callouts:

- 17**: Points to the **Connect** tab in the top navigation bar.
- 18**: Points to the **ROPG tenant** field in the **Authentication** section.
- 19**: Points to the **Sign in logo** field in the **Sign in** section.
- 20**: Points to the **Automatic sign-in** checkbox in the **Sign in** section.
- 21**: Points to the **Light mode icon** field in the **Custom branding** section.
- 22**: Points to the **Dark mode icon** field in the **Custom branding** section.
- 23**: Points to the **Show welcome window** checkbox in the **Custom branding** section.



24. Scroll down to the Temporary User Permissions section.
25. Select the checkbox for Temporary user promotion.
26. Select the checkbox for User promotion timer.
27. Enter **15** minutes for User promotion duration.
28. Enter **5** per Month for User promotion limit.
29. Select the checkbox for Verify user promotion.
30. Select the checkbox for User promotion reason.
31. Enter **Install Software,Add Printer,General Use** for User promotion choices.
32. In the User help section, Help Options, Add a URL of your choosing. This guide will use:
<https://hconline.com/support/resources/remote-support>
33. Enter **URL** in the Help type field.
34. For Software Path, enter the path to Self Service+: **/Applications/Self Service+.app**
NOTE: Temporary User Permissions allow you to promote a standard user to an administrative user for set period of time.

The screenshot shows the 'Temporary User Permissions' and 'User help' configuration sections. Red callout numbers 25 through 34 point to specific fields and checkboxes.

Temporary User Permissions

- 25: ☒ Temporary user promotion
- ☐ URL Scheme and Command Line Elevation
- 26: ☒ User promotion timer
- User promotion duration: 15 minutes (27)
- User promotion limit: 5 / month (28)
- 29: ☒ Verify user promotion
- ☐ Verify User Promotion FIDO2
- ☐ User promotion biometrics
- 30: ☒ User promotion reason
- User promotion choices: Install Software,Add Printer,General Use (31)
- Admin attribute: [empty field]
- User promotion role: +

User help

- Help options: <https://hconline.com/support/resources/remote-support> (32)
- Help type: URL (33)
- Software path: /Applications/Self Service+.app (34)

35. Scroll down to the Scripting section, for On auth failure, enter:
/usr/local/JamfConnectCustomizations/scripts/menuBar.sh
NOTE: This script will run if Jamf Connect fails to authenticate after login.

The screenshot shows the 'Scripting' section with four input fields. The first field, 'On auth failure:', contains the path `/usr/local/JamfConnectCustomizations/scripts/menuBar.sh` and is highlighted with a red box.

Scripting

- On auth failure: /usr/local/JamfConnectCustomizations/scripts/menuBar.sh
- On auth success: [empty field]
- On password change: [empty field]
- On network change: [empty field]



36. Scroll down to the Menu Items section. Under Hidden menu items, Select the checkbox for the following items to hide them from the menu bar:

- Actions
- Home Directory
- Last user
- Password expiration
- Preferences
- Shares
- Quit

In the Custom menu items section you can change the Menu item names:

A. Get help: Remote Support.

B. Get Software: HCS App Store.

Menu items

Hidden menu items

- ☐ About
- ☒ Actions
- ☐ Change password
- ☐ Get help
- ☐ Get software
- ☒ Home directory
- ☒ Last user
- ☒ Password expiration
- ☒ Preferences
- ☐ Reset password
- ☒ Shares
- ☐ Connect
- ☒ Quit
- ☐ User Privileges

Custom menu items

About:

Actions:

Change password:

Get help: Remote Support A

Get software: HCS App Store B

Home directory:

Last user:

Password expiration:

Preferences:

Reset password:

Shares:

Connect:

Quit:

37. Log into your Jamf Pro server with administrative privileges.

Pro

Username

Required

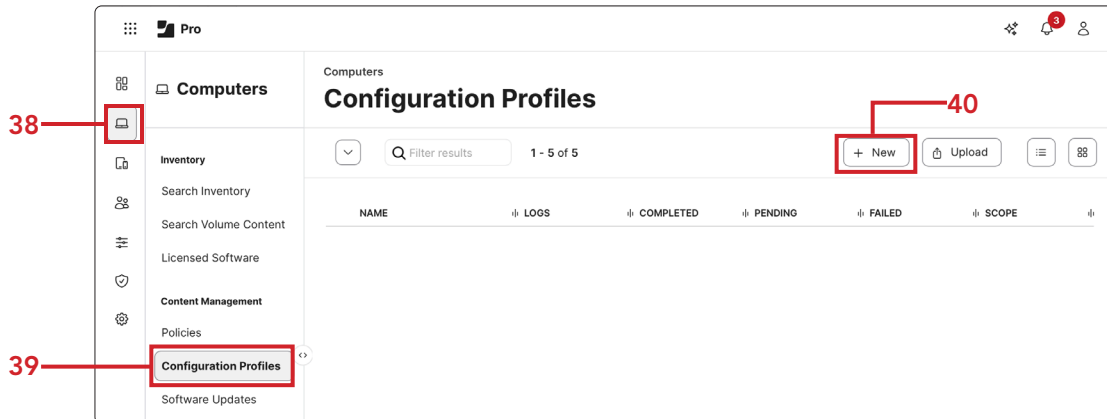
Password

Required

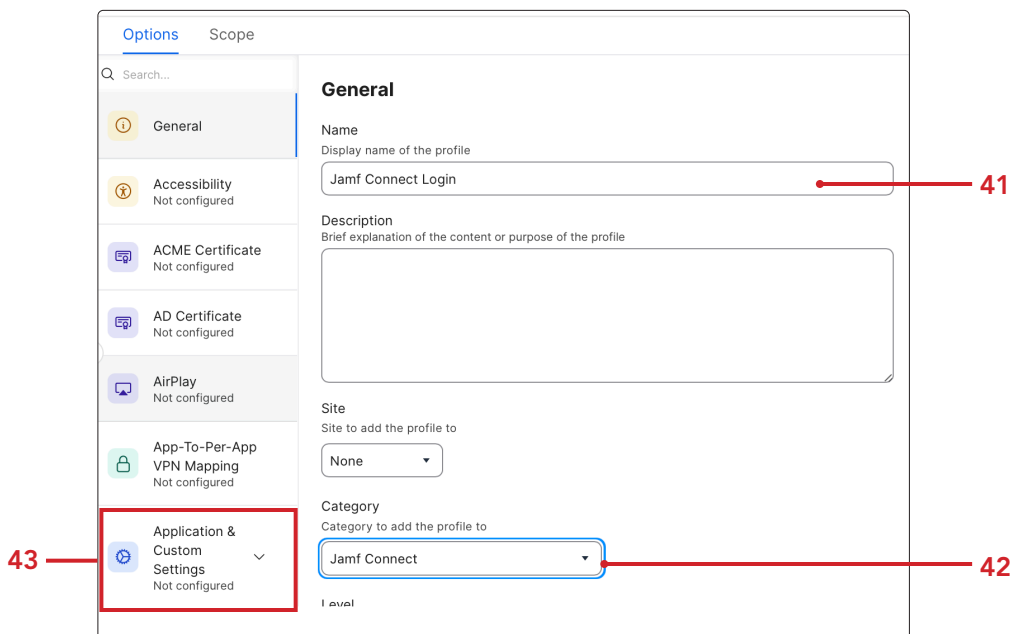
Log in



38. Click Computers.
39. Click Configuration Profiles.
40. Click New.



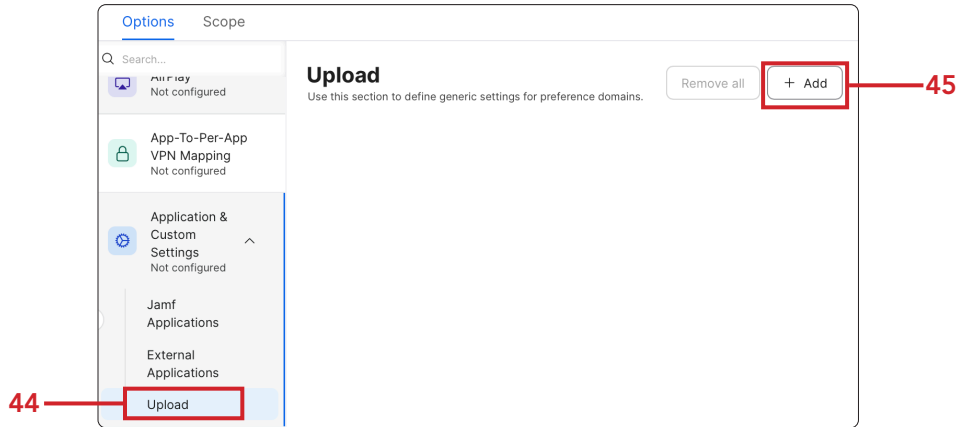
41. Enter **Jamf Connect Login** for Name.
NOTE: If you are using sites, select a site if necessary. You will only see the site section if sites are enabled in Jamf Pro.
42. Select a category of your choosing, this guide will use Jamf Connect. Leave all other settings at their defaults.
43. Click the Application & Custom Settings Payload from the sidebar.



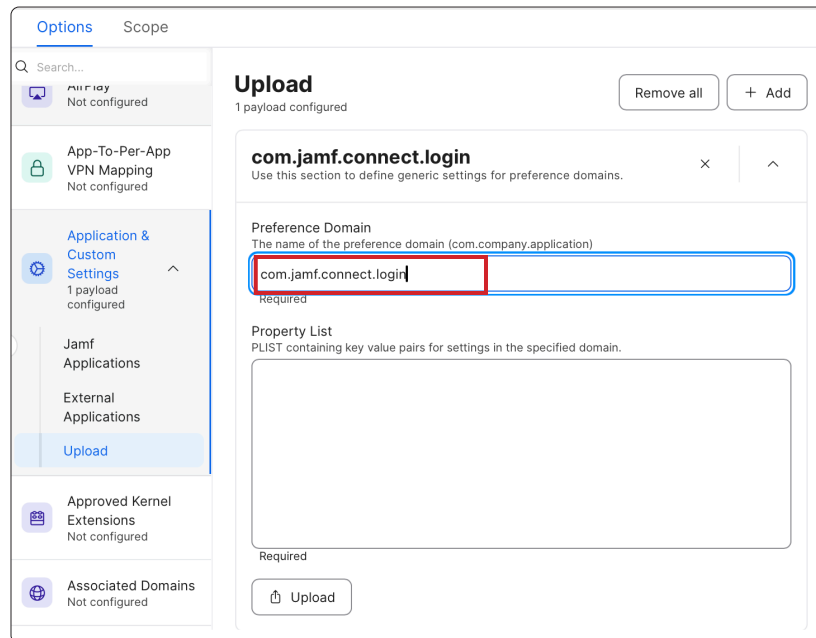


44. Select Upload.

45. Click the Add (+).

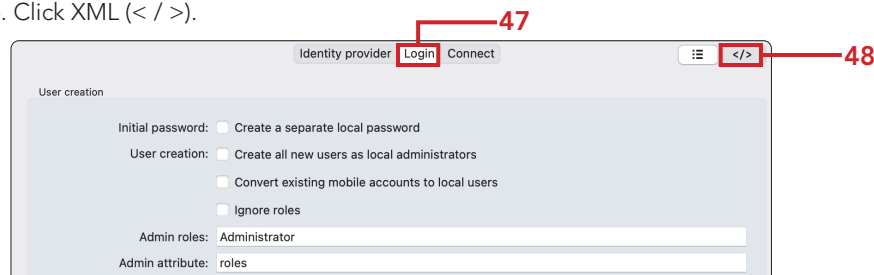


46. Enter com.jamf.connect.login for Preference Domain.



47. Switch back to the Jamf Connect Configuration App. Select Login.

48. Click XML (< / >).





49. Verify the Login tab is still selected and copy all the contents.

A screenshot of a code editor window. At the top, there are two tabs: 'Login' and 'Connect'. The 'Login' tab is selected and highlighted with a red rectangular box. The editor displays XML code for a plist file. The code is as follows:

```
<?xml version="1.0" encoding="UTF-8"?>
<!DOCTYPE plist PUBLIC "-//Apple//DTD PLIST 1.0//EN" "http://www.apple.com/DTDs/PropertyList-1.0.dtd">
<plist version="1.0">
<dict>
  <key>AllowNetworkSelection</key>
  <true/>
  <key>BackgroundImage</key>
  <string>/usr/local/JamfConnectCustomizations/images/HCSBackgroundImage.png</string>
  <key>CreateJamfConnectPassword</key>
  <true/>
  <key>CreateNewUserHide</key>
  <true/>
  <key>DenyLocal</key>
  <false/>
  <key>LocalFallback</key>
  <true/>
  <key>LoginLogo</key>
  <string>/usr/local/JamfConnectCustomizations/images/HCSLoginWindowLogo.png</string>
  <key>LoginWindowMessage</key>
  <string>Welcome to HCS Technology Group</string>
  <key>LoginWindowSize</key>
  <string>Max</string>
  <key>Migrate</key>
  <true/>
  <key>MigrateUsersHide</key>
  <array>
    <string>hcs</string>
  </array>
  <key>0IDCAdmin</key>
  <array>
    <string>Administrator</string>
  </array>
  <key>0IDCCClientID</key>
  <string>ac[REDACTED]ce2e</string>
  <key>0IDCNewPassword</key>
  <false/>
  <key>0IDCProvider</key>
```



50. Switch back to your Jamf Pro server and paste the contents of the Login tab in the Property List field. Make sure there are no trailing spaces at the end after pasting in the code.

51. Click Scope.

Options Scope **51**

Upload
1 payload configured

Remove all + Add

com.jamf.connect.login
Use this section to define generic settings for preference domains.

Preference Domain
The name of the preference domain (com.company.application)

com.jamf.connect.login

Required

Property List
PLIST containing key value pairs for settings in the specified domain.

```
<?xml version="1.0" encoding="UTF-8"?>
<!DOCTYPE plist PUBLIC "-//Apple//DTD PLIST 1.0//EN" "http://www.apple.com/DTDs/PropertyList-1.0.dtd">
<plist version="1.0">
<dict>
  <key>AllowNetworkSelection</key>
  <true/>
  <key>BackgroundImage</key>
  <string>/usr/local/JamfConnectCustomizations/images/HCSBackgroundImage.png</string>
  <key>CreateJamfConnectPassword</key>
  <true/>
  <key>CreateNewUserHide</key>
  <true/>
  <key>DenyLocal</key>
  <false/>
  <key>LocalFallback</key>
  <true/>
  <key>LoginLogo</key>
  <string>/usr/local/JamfConnectCustomizations/images/HCSLoginWindowL.png</string>
  <key>LoginWindowMessage</key>
  <string></string>
</dict>
</plist>
```

Required

Upload

50

52. From the Target Computers menu, select Specific Computers.

53. Click Add.

Options Scope

Targets Limitations Exclusions

Verify the Targets tab is selected.

Target Computers
Computers to assign the profile to

52 Specific Computers

Target Users
Users to distribute the profile to

Specific Users

Selected Deployment Targets

+ Add **53**

TARGET	TYPE
--------	------



54. Click Add next to your NON production Mac computer.

55. Click Done.

NOTE: Do NOT use a Mac in production for testing.

Options [Scope](#)

Targets Limitations Exclusions

Add Deployment Targets

Computers Computer Groups Users User Groups

Buildings Departments

Filter results 1 - 5 of 5

NAME	
Donna's MacBook	Add
Keith Macbook Pro	Add

56. Click Save.

Options [Scope](#)

Targets Limitations Exclusions

Target Computers
Computers to assign the profile to
Specific Computers

Target Users
Users to distribute the profile to
Specific Users

Selected Deployment Targets

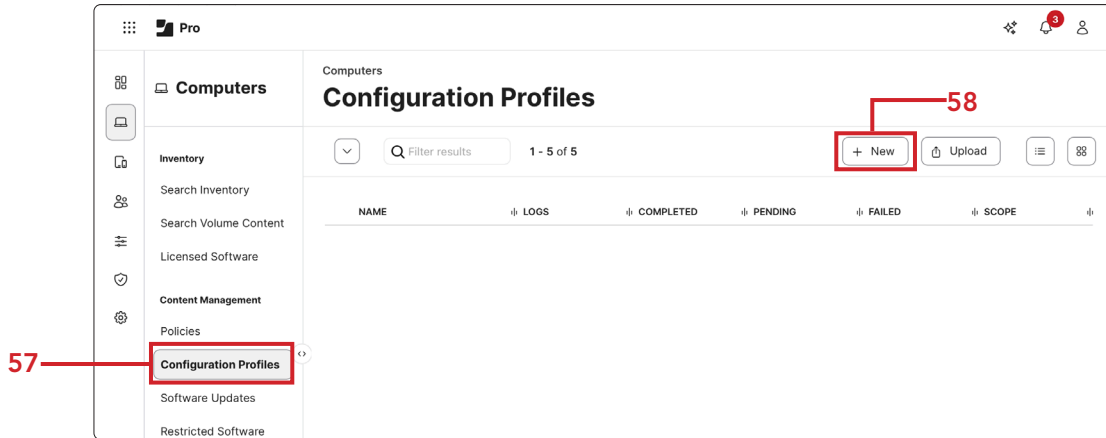
TARGET	TYPE	
Keith Macbook Pro	Computer	Remove

Cancel Save



57. Click Configuration Profiles.

58. Click New.

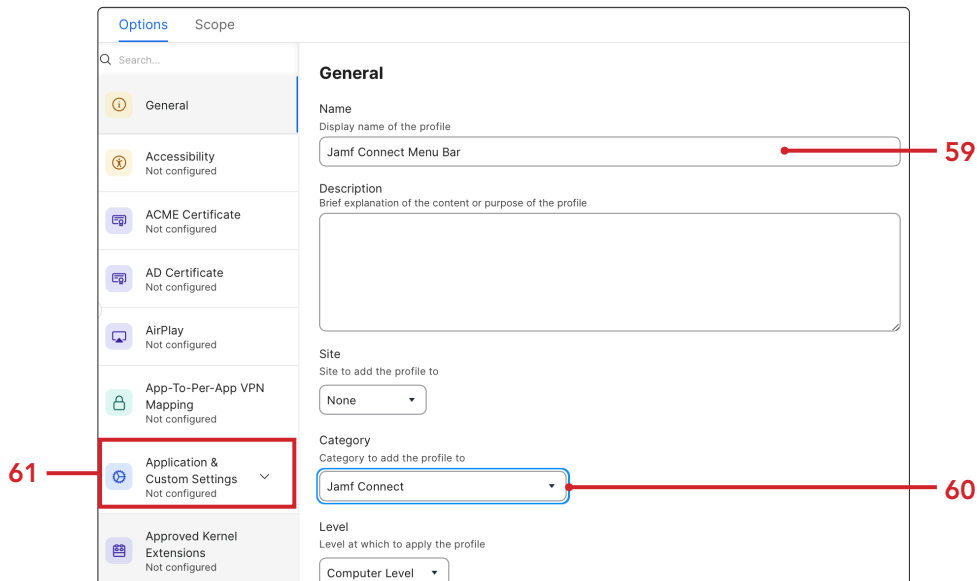


59. Enter Jamf Connect Menu Bar for the Name.

60. Select a category of your choosing, this guide will use Jamf Connect. Leave all other settings at their defaults.

NOTE: If you are using sites, select a site if necessary. You will only see the site section if sites are enabled in Jamf Pro.

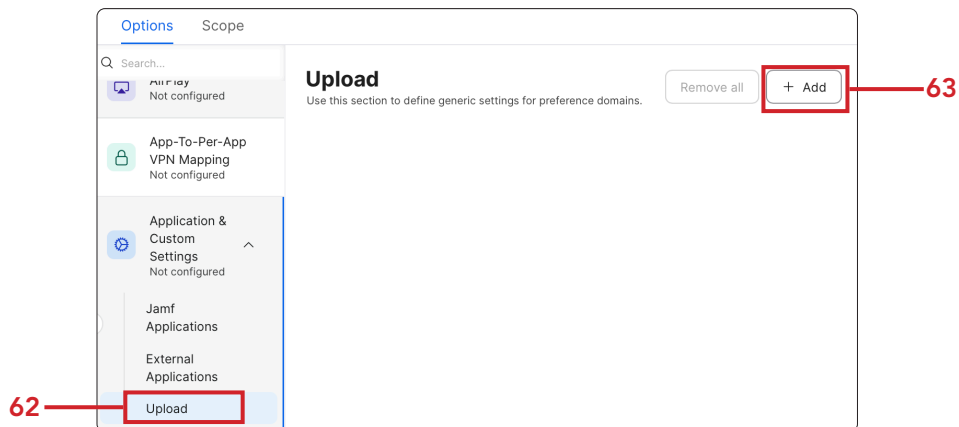
61. Select the Application & Custom Settings Payload from the sidebar.



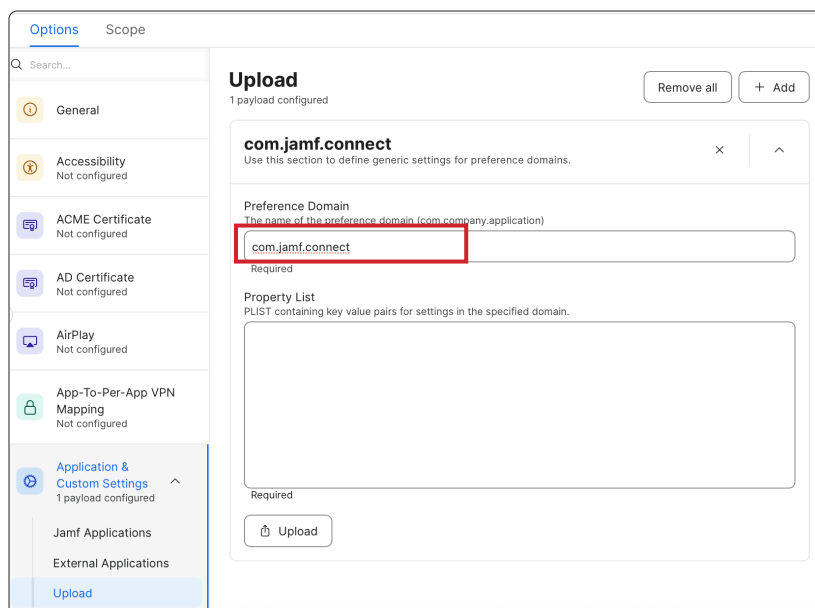


62. Select Upload.

63. Click the Add (+).



64. Enter com.jamf.connect for Preference Domain.





65. Switch back to the Jamf Connect Configuration App. Select Connect.

66. Copy all the contents.

The screenshot shows the Jamf Connect Configuration App interface. At the top, there are two buttons: "Login" and "Connect". The "Connect" button is highlighted with a red box and a red line pointing to the number 65. Below the buttons, the app displays the content of a plist file. The content is XML-formatted and includes various keys and values, such as "Appearance", "MenuBarIcon", "CustomMenuItems", "HiddenMenuItems", "IdPSettings", and "Scripting". A red line points from the number 66 to the entire content area of the plist file.

```
<?xml version="1.0" encoding="UTF-8"?>
<!DOCTYPE plist PUBLIC "-//Apple//DTD PLIST 1.0//EN" "http://www.apple.com/DTDs/PropertyList-1.0.dtd">
<plist version="1.0">
<dict>
  <key>Appearance</key>
  <dict>
    <key>MenuBarIcon</key>
    <string>/usr/local/JamfConnectCustomizations/images/HCSMenuItemLightMode.png</string>
    <key>MenuBarIconDark</key>
    <string>/usr/local/JamfConnectCustomizations/images/HCSMenuItemLightMode.png</string>
  </dict>
  <key>CustomMenuItems</key>
  <dict>
    <key>getsoftware</key>
    <string>HCS App Store</string>
  </dict>
  <key>HiddenMenuItems</key>
  <array>
    <string>actions</string>
    <string>home</string>
    <string>lastusername</string>
    <string>passwordexpiration</string>
    <string>preferences</string>
    <string>shares</string>
    <string>quitjamfconnect</string>
  </array>
  <key>IdPSettings</key>
  <dict>
    <key>Provider</key>
    <string>EntraID</string>
    <key>ROPGID</key>
    <string>ac[redacted]ce2e</string>
    <key>TenantID</key>
    <string>d4cb[redacted]d5530</string>
  </dict>
  <key>Scripting</key>
  <dict>
```



67. Switch back to your Jamf Pro server and paste the contents of the Connect tab in the Property List field. Make sure there are no trailing spaces at the end after pasting in the code.

68. Click Scope.

The screenshot shows the 'Scope' tab in the Jamf Pro interface. On the left, a sidebar lists various configuration options, with 'Upload' highlighted. The main area is titled 'Upload' and shows a single payload configured: 'com.jamf.connect'. Below this, the 'Property List' section is expanded, displaying a plist code block. A red line labeled '67' points to the code block. Another red line labeled '68' points to the 'Scope' tab header. The code in the plist field is as follows:

```
<?xml version="1.0" encoding="UTF-8"?>
<DOCTYPE plist PUBLIC "-//Apple//DTD PLIST 1.0//EN" "http://www.apple.com/DTDs/PropertyList-1.0.dtd">
<plist version="1.0">
<dict>
  <key>Appearance</key>
  <dict>
    <key>MenuBarIcon</key>
    <string>/usr/local/JamfConnectCustomizations/images/HCSMenuBarIconLightMode.png</string>
    <key>MenuBarIconDark</key>
    <string>/usr/local/JamfConnectCustomizations/images/HCSMenuBarIconLightMode.png</string>
  </dict>
  <key>CustomMenuItems</key>
  <dict>
    <key>getsoftware</key>
    <string>HCS App Store</string>
  </dict>
  <key>HiddenMenuItems</key>
  <array>
    <string>actions</string>
    <string>home</string>
    <string>lastusername</string>
    <string>passwordexpiration</string>
    <string>preferences</string>
  </array>

```

69. From the Target Computers menu, select Specific Computers.

70. Click Add.

The screenshot shows the 'Scope' tab in the Jamf Pro interface. The 'Targets' section is active, showing 'Target Computers' and 'Target Users'. The 'Target Computers' dropdown menu is open, and 'Specific Computers' is selected. A red line labeled '69' points to this dropdown. Below the dropdowns is a 'Selected Deployment Targets' section with a table with columns 'TARGET' and 'TYPE'. A red line labeled '70' points to the '+ Add' button in the top right corner of this section.



71. Click Add next to your NON production Mac computer.

72. Click Done.

NOTE: Do NOT use a Mac in production for testing.

Options [Scope](#)

Targets Limitations Exclusions

Add Deployment Targets

Computers Computer Groups Users User Groups

Buildings Departments

Filter results 1 - 5 of 5

NAME	
Donna's MacBook	Add
Keith Macbook Pro	Add

73. Click Save.

Options [Scope](#)

Targets Limitations Exclusions

Target Computers
Computers to assign the profile to
Specific Computers

Target Users
Users to distribute the profile to
Specific Users

Selected Deployment Targets

TARGET	TYPE	
Keith Macbook Pro	Computer	Remove

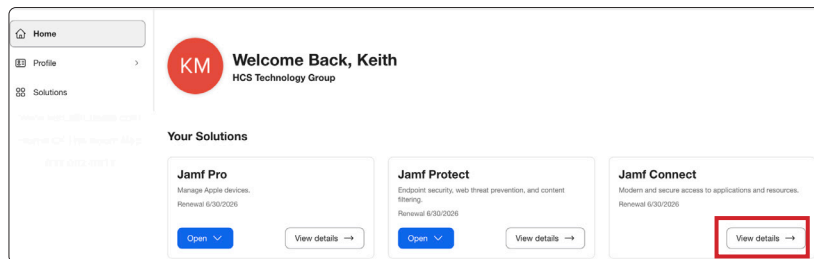
Cancel Save



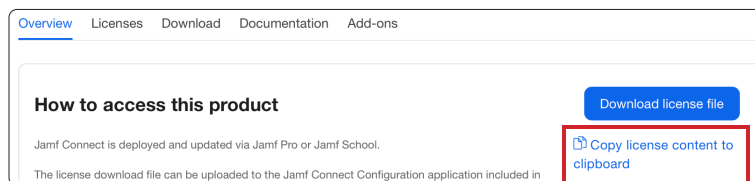
The following steps are optional

Jamf Connect includes a 30-day trial with full functionality. If you prefer, you can deploy a license file separately as its own configuration profile. This approach makes license management easier. When it's time to renew, simply update the Jamf Connect license configuration profile with the new license and push it out through Jamf Pro. Your other Jamf Connect configuration profiles will remain untouched and only the license file will be updated.

74. Log into your Jamf Account at: <https://account.jamf.com> and select Jamf Connect and View Details.

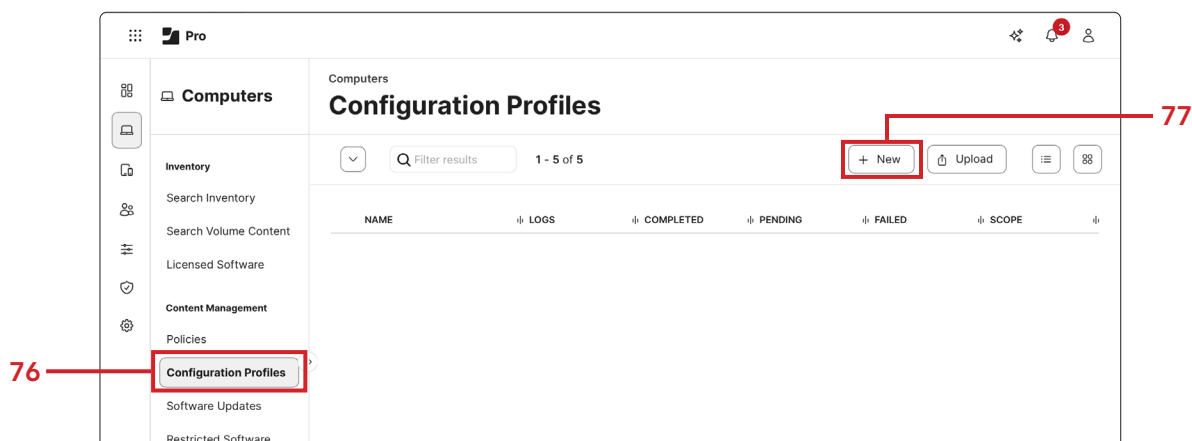


75. Click Copy license content to clipboard.



76. Switch back to your Jamf Pro server. In the sidebar, click Configuration Profiles.

77. Click New.





78. Verify the General Payload is selected.
79. Enter Jamf Connect License for the Name.
80. Select a category of your choosing, this guide will use Jamf Connect.
81. Leave the rest of the settings at their default values.
NOTE: If you are using sites, select a site if necessary. You will only see the site section if sites are enabled in Jamf Pro.

A screenshot of the Jamf Pro profile configuration interface. The interface is divided into two main sections: a left sidebar and a right main panel. The sidebar contains a list of payload categories, with 'General' highlighted by a red box and a red line pointing to the number '78'. Other categories include Accessibility, ACME Certificate, AD Certificate, AirPlay, App-To-Per-App VPN Mapping, Application & Custom Settings, Approved Kernel Extensions, Associated Domains, and Certificate. The main panel displays the 'General' configuration options. The 'Name' field is labeled 'Jamf Connect License' and is highlighted by a red line pointing to the number '79'. The 'Category' dropdown menu is set to 'Jamf Connect' and is highlighted by a red box and a red line pointing to the number '80'. Other visible fields include 'Description', 'Site' (set to 'None'), 'Level' (set to 'Computer Level'), and 'Distribution Method' (set to 'Install automatically').

Options Scope

Search...

78 General

Accessibility Not configured

ACME Certificate Not configured

AD Certificate Not configured

AirPlay Not configured

App-To-Per-App VPN Mapping Not configured

Application & Custom Settings Not configured

Approved Kernel Extensions Not configured

Associated Domains Not configured

Certificate Not configured

General

Name
Display name of the profile

Jamf Connect License **79**

Description
Brief explanation of the content or purpose of the profile

Site
Site to add the profile to

None

Category
Category to add the profile to

Jamf Connect **80**

Level
Level at which to apply the profile

Computer Level

Distribution Method
Method to use for distributing the profile

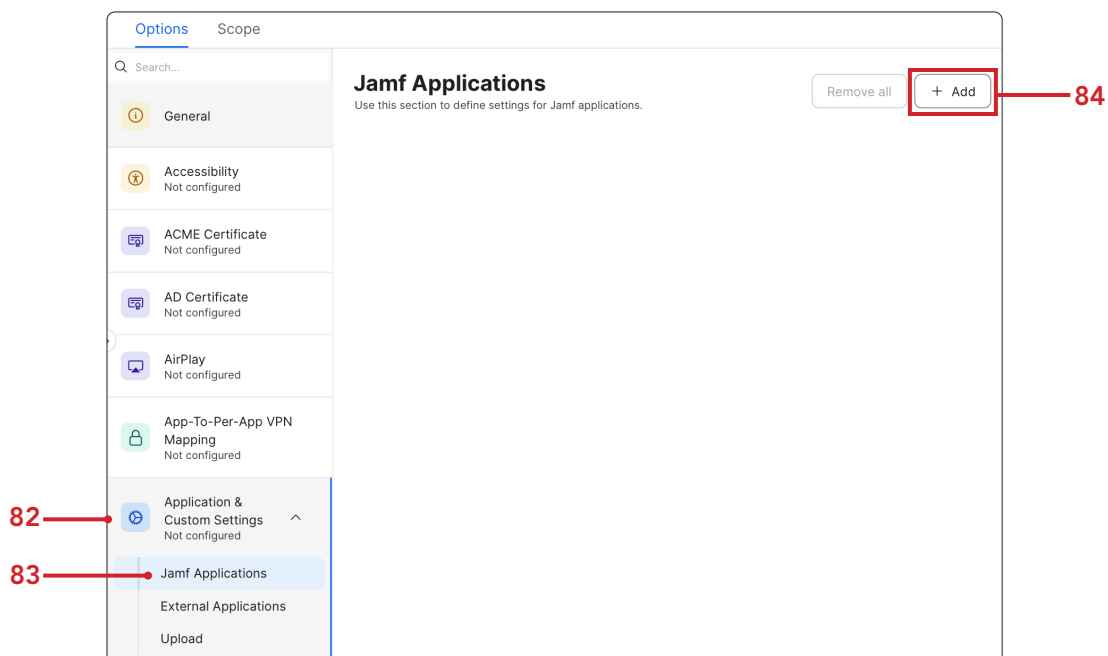
Install automatically



82. Click to expand the Application & Custom Settings payload.

83. Select Jamf Applications.

84. Click Add.

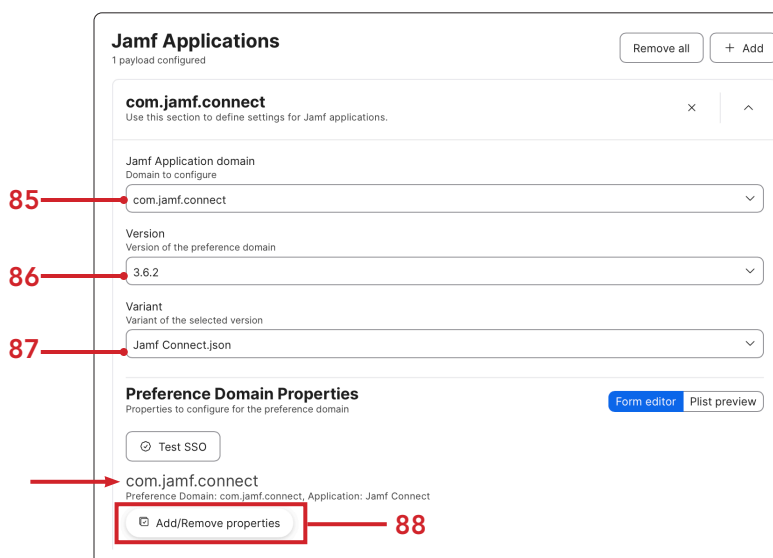


85. Select com.jamf.connect from the Jamf Application Domain menu.

86. Select 3.6.2 from the Version menu.

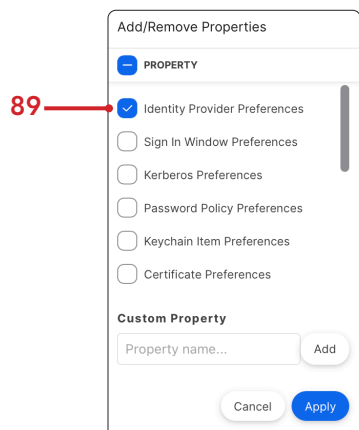
87. Select Jamf Connect.json from Variant menu.

88. Under com.jamf.connect, click Add/Remove properties.



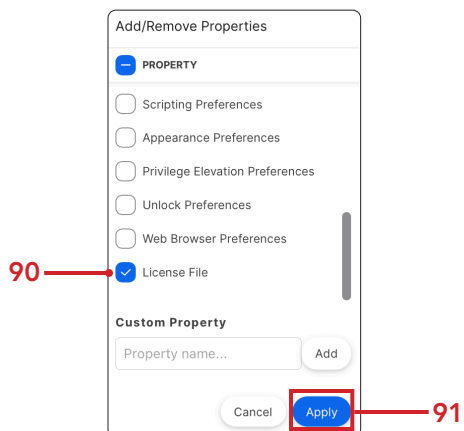


89. Deselect Identity Provider Preferences.



90. Scroll down and select License File.

91. Click Apply.





92. In the License File field, paste in your Jamf Connect license.
NOTE: You copied your license to the clipboard in an earlier step.
93. Click Scope.

94. Verify Targets is selected.
95. From the Target Computers menu, select Specific Computers.
96. Click Add.



97. Verify Computers is selected.

98. In the search field, enter the name of your test Mac computer.

99. Click Add.

100. Click Done.

Options Scope

Targets Limitations Exclusions

Add Deployment Targets

Computers Computer Groups Users User Groups

Buildings Departments

Q Keith Macbook pro 1 - 1 of 1

NAME
Keith Macbook Pro

Done

Add

101. Click Save.

Options Scope

Targets Limitations Exclusions

Target Computers
Computers to assign the profile to
Specific Computers

Target Users
Users to distribute the profile to
Specific Users

Selected Deployment Targets

TARGET	TYPE
Keith Macbook Pro	Computer

+ Add

Remove

Cancel Save

This completes this section. In the next section, we will create a policy in Jamf Pro to install Jamf Connect.



Section 5: Create a policy in Jamf Pro to install Jamf Connect Login

What You'll Need:

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

Hardware and Software:

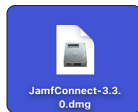
Requirements for following along with this section:

- Access to a Jamf Pro server with administrative privileges
- JamfConnectCustomizations.pkg created in section two of this guide.
- JamfConnect-3.3.0.dmg. Downloaded in section three of this guide.
- Self Service+ installed by default from the Jamf Pro server

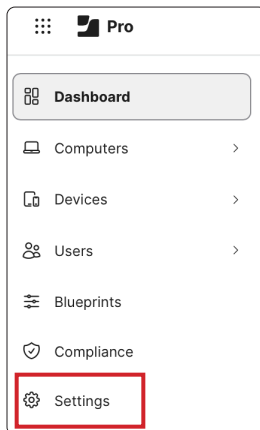
NOTE: This guide assumes Self Service+ is being installed by default on your Jamf Pro server. We will not cover enabling Self Service+ in this guide.

In this section, we will create a policy to install Jamf Connect Login and the JamfConnectCustomizations.pkg using Jamf Pro.

1. Open the JamfConnect-3.3.0.dmg. In this guide, it's located in the Downloads folder.

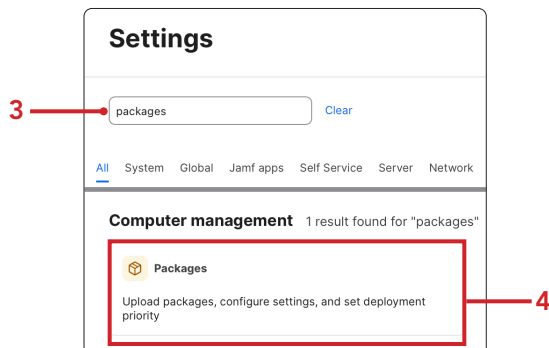


2. If necessary, Log into your Jamf Pro server with administrative privileges. Click Settings (⚙️).



3. In the search field, enter packages.

4. Click Packages.





5. Click New (+).



6. Select a category of your choosing. This guide will use Jamf Connect.

7. Click Browse for a file.

General Options Limitations

Display name
Display name for the package

Required

Category
Category to add the package to

Jamf Connect

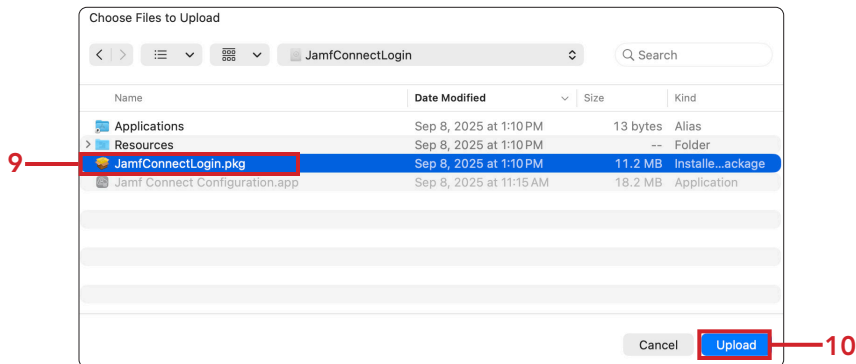
Filename
Filename of the package on the distribution point (e.g., "MyPackage.pkg")

Drop file here or [browse for a file.](#)

8. Navigate to the JamfConnectLogin disk image.

9. Select JamfConnectLogin.pkg.

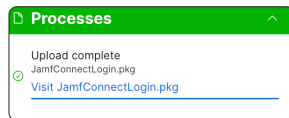
10. Click Upload.





11. Click Save.

12. The upload process is complete.



13. Click Previous (←).



14. Click New (+).



15. Select a category of your choosing. This guide will use Jamf Connect.

16. Click browse for a file.



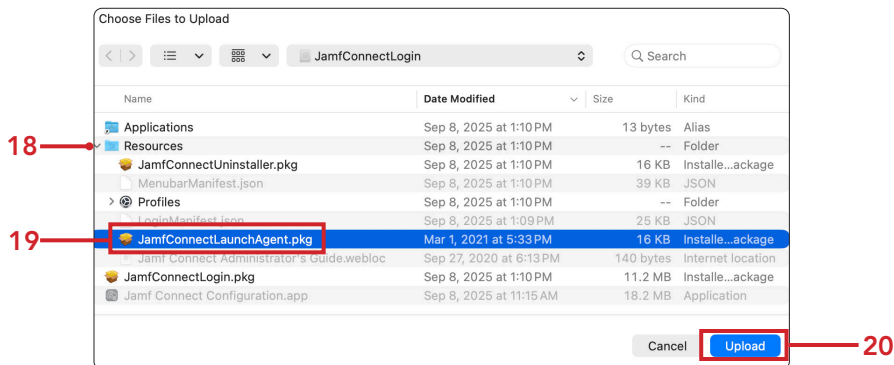
17. Navigate to the JamfConnectLogin disk image.

18. Expand the Resources folder.

19. Select JamfConnectLaunchAgent.pkg.

20. Click Upload.

NOTE: While Self Service+ includes the Jamf Connect launch agent, it has been reported to function inconsistently. To ensure reliability, we are also deploying the launch agent packaged with Jamf Connect Login as a fail-safe.



21. Click Save.

General Options Limitations

Display name
Display name for the package
JamfConnectLaunchAgent.pkg
Required

Category
Category to add the package to
Jamf Connect

Filename
Filename of the package on the distribution point (e.g., "MyPackage.pkg")
Drop file here or [browse for a file.](#)

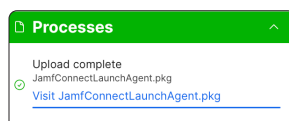
Info
Information to display to the administrator when the package is deployed or uninstalled

Notes
Notes to display about the package (e.g., who built it and when it was built)

Manifest file
Drop file here or [browse for a file.](#)

Cancel Save

22. The upload process is complete.





23. Click Previous (←).



24. Click New.

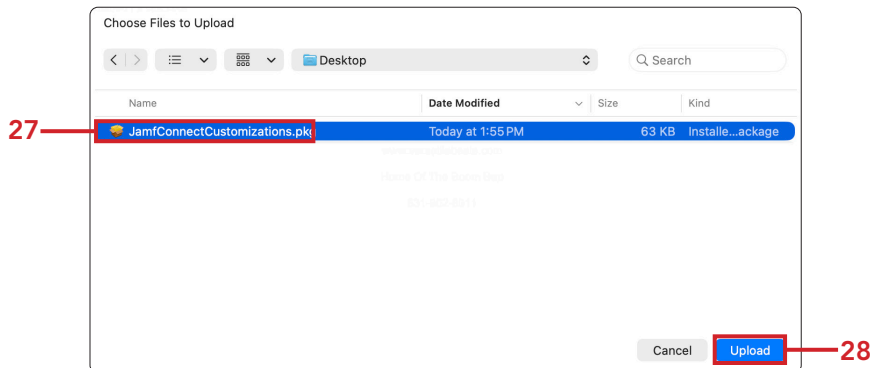


25. Select a category of your choosing. This guide will use Jamf Connect.

26. Click browse for a file.

27. Navigate to the JamfConnectCustomizations.pkg. (Should be on your Desktop).

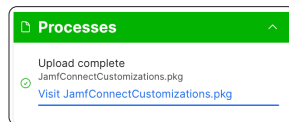
28. Click Upload.





29. Click Save.

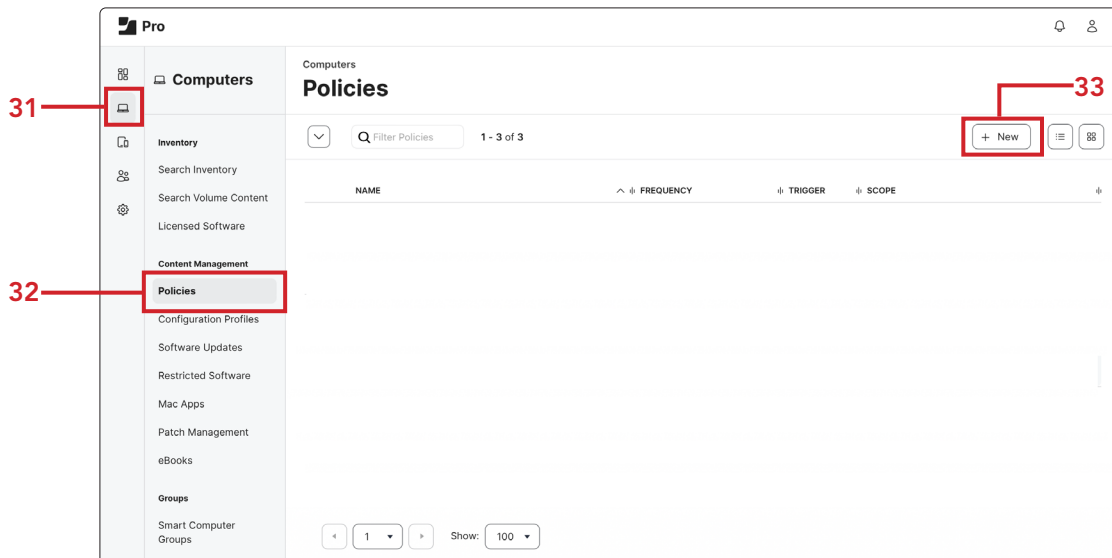
30. The upload process is complete.



31. Select Computers.

32. Click Policies.

33. Click New.





34. Click General.
35. Enter **Install Jamf Connect** for the Display Name.
36. Select Jamf Connect for the Category.
NOTE: If you are using sites, select a site if necessary. You will only see the site section if sites are enabled in Jamf Pro.
37. Do not select anything for the Trigger.
38. Under Execution Frequency, select Once per computer from the menu.
39. Click the Packages payload.

34. General

39. Packages

35. Display Name: Install Jamf Connect

36. Category: Jamf Connect

38. Execution Frequency: Once per computer

Nothing is to be selected under Trigger

40. Click Configure.

Options Scope Self Service User Interaction

General

Packages

Software Updates

Scripts

Printers

Disk Encryption

Configure Packages

Use this section to install, cache, and uninstall packages. Also use this section to install a single cached package.

Configure



41. Navigate to JamfConnectLaunchAgent.pkg.

42. Click Add.

Options	Scope	Self Service	User Interaction
General	JamfConnectLaunchAgent.pkg	Jamf Connect	Add

43. Leave the default settings. Click Add (+).

Options	Scope	Self Service	User Interaction
Packages 1 Package	Packages		
Software Updates Not Configured	Distribution Point Distribution point to download the package(s) from Each computer's default distribution point		
Scripts 0 Scripts	JamfConnectLaunchAgent.pkg		
Printers 0 Printers	Action Action to take on computers Install		
Disk Encryption Not Configured			

44. Navigate to JamfConnectLogin.pkg.

45. Click Add.

Options	Scope	Self Service	User Interaction
Packages 1 Package	JamfConnectLogin.pkg	Jamf Connect	Add

46. Click Add (+).

Options	Scope	Self Service	User Interaction
Packages 2 Packages	Packages		
Software Updates Not Configured	Distribution Point Distribution point to download the package(s) from Each computer's default distribution point		
Scripts 0 Scripts	JamfConnectLaunchAgent.pkg		
Printers 0 Printers	Action Action to take on computers Install		
Disk Encryption Not Configured	JamfConnectLogin.pkg		
Dock Items 0 Dock Items	Action Action to take on computers Install		
Local Accounts 0 Accounts			

47. Navigate to JamfConnectCustomizations.pkg.

48. Click Add.

JamfConnectCustomizations.pkg	Jamf Connect	Add
-------------------------------	--------------	-----



49. Click Scope.

The screenshot shows the 'Scope' tab in the Jamf Pro console. The left sidebar contains a list of configuration categories: Packages (3 Packages), Software Updates (Not Configured), Scripts (0 Scripts), Printers (0 Printers), Disk Encryption (Not Configured), Dock Items (0 Dock Items), Local Accounts (0 Accounts), Management Accounts (Not Configured), Directory Bindings (0 Bindings), and EFI Password (Not Configured). The main area displays a list of packages under the heading 'Packages'. The first package is 'JamfConnectCustomizations.pkg' with an 'Action' of 'Action to take on computers' and an 'Install' button. The second package is 'JamfConnectLaunchAgent.pkg' with an 'Action' of 'Action to take on computers' and an 'Install' button. The third package is 'JamfConnectLogin.pkg' with an 'Action' of 'Action to take on computers' and an 'Install' button.

50. From the Target Computers menu, select Specific Computers.

51. Click Add.

The screenshot shows the 'Scope' tab in the Jamf Pro console, specifically the 'Targets' section. The 'Target Computers' dropdown is set to 'Specific Computers' (indicated by a red box and arrow labeled 50). The 'Target Users' dropdown is set to 'Specific Users'. Below these, there is a 'Selected Deployment Targets' section with a table header 'TARGET' and 'TYPE'. A red box and arrow labeled 51 point to the '+ Add' button in the top right corner of the 'Selected Deployment Targets' section.



52. Click Add next to your NON production Mac computer.

53. Click Done.

NOTE: Do NOT use a Mac in production for testing.

Options **Scope**

Targets Limitations Exclusions

Add Deployment Targets

Computers Computer Groups Users User Groups

Buildings Departments

Filter results 1 - 5 of 5

NAME

Donna's MacBook Add

Keith Macbook Pro Add

54. Click Self Service.

Options **Scope** **Self Service** User Interaction

Targets Limitations Exclusions

Target Computers Target Users

Computers to deploy the policy to Users to deploy the policy to

Specific Computers Specific Users

Selected Deployment Targets + Add

TARGET	TYPE
Keith Macbook Pro	Computer

Remove



55. Select the checkbox for Make the policy available in Self Service.

Options Scope **Self Service** User Interaction

☒ Make the policy available in Self Service

Self Service Display Name
Display name for the policy in Self Service (Self Service 10.0.0 or later)

Install Jamf Connect

Button Name
Name for the button that users click to initiate the policy

Install

56. Scroll down to the Display in section.

57. Select a category of your choosing. This guide will use Jamf Connect.

58. Click Save.

Options Scope **Self Service** User Interaction

Display in	Feature in
<input type="checkbox"/> Applications	<input type="checkbox"/> Applications
<input type="checkbox"/> DEPNotify	<input type="checkbox"/> DEPNotify
<input type="checkbox"/> Disabled Policies	<input type="checkbox"/> Disabled Policies
<input type="checkbox"/> Extension Attribute	<input type="checkbox"/> Extension Attribute
<input type="checkbox"/> FileVault Tools	<input type="checkbox"/> FileVault Tools
<input type="checkbox"/> Firmware Tools	<input type="checkbox"/> Firmware Tools
<input type="checkbox"/> Games	<input type="checkbox"/> Games
<input type="checkbox"/> Global Policies	<input type="checkbox"/> Global Policies
<input type="checkbox"/> IBM Migrator	<input type="checkbox"/> IBM Migrator
<input type="checkbox"/> iOS Apps for Macs with Apple Silicon	<input type="checkbox"/> iOS Apps for Macs with Apple Silicon
<input type="checkbox"/> iOS18_cis_lvl2_byod	<input type="checkbox"/> iOS18_cis_lvl2_byod
<input checked="" type="checkbox"/> Jamf Connect	<input type="checkbox"/> Jamf Connect
<input type="checkbox"/> Jamf Connect Saved Profiles	<input type="checkbox"/> Jamf Connect Saved Profiles

Cancel Save

59. Click Policies.

Computers

Inventory

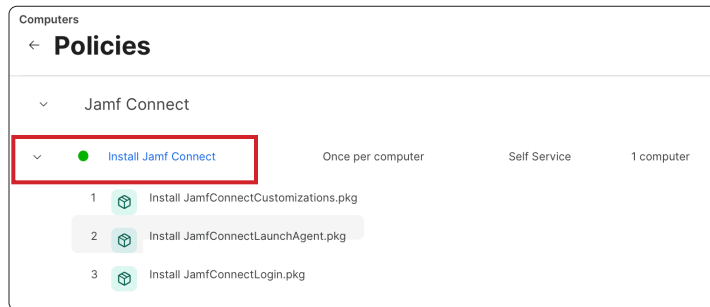
- Search Inventory
- Search Volume Content
- Licensed Software

Content Management

- Policies**



60. Confirm the policy was created.



This completes this section. In the next section, we will install Jamf Connect.



Section 6: Install and test Jamf Connect on a Mac Computer

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 with FileVault enabled and enrolled in Jamf Pro
- Self Service+ installed by default from Jamf Pro
- On your Jamf Pro Server, Go to Settings>Computer Management>Security and make sure the three Jamf connect settings are enabled.

NOTE: FileVault is enabled here to demonstrate Jamf Connect's Passthrough feature. This feature was highly requested because it eliminates the need for users to enter their login credentials twice when starting up or restarting a Mac computer.

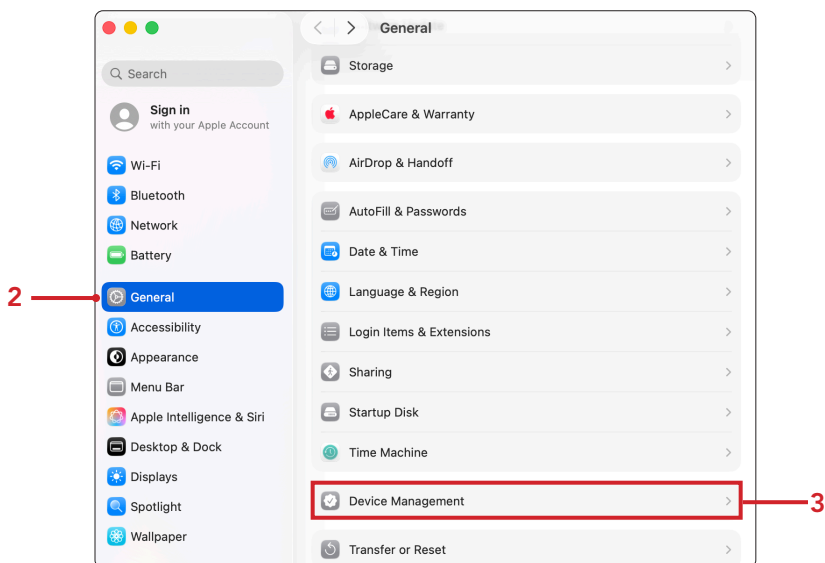
In this section, we will install Jamf Connect using Self Service+ to validate the results of the previous sections in this guide. Before proceeding, ensure that the configuration profiles created in section three of this guide have been successfully deployed to your NON production Mac computer. These profiles contain the required settings for Jamf Connect and must be in place prior to installation.

Let's verify the Jamf Connect Login and Menu Bar configuration profiles are installed.

1. On your Non Production Mac computer, Open System Settings.



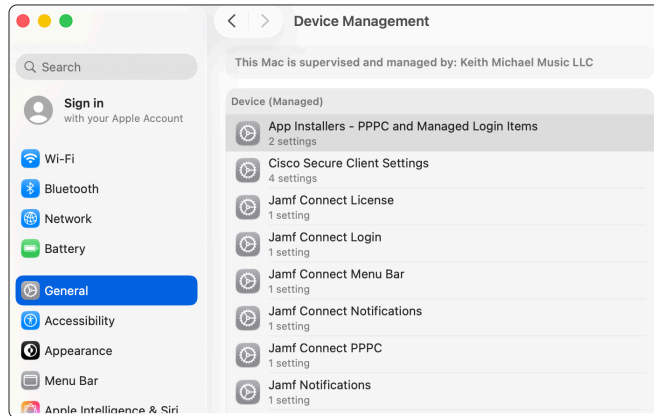
2. Click General.
3. Click Device Management.



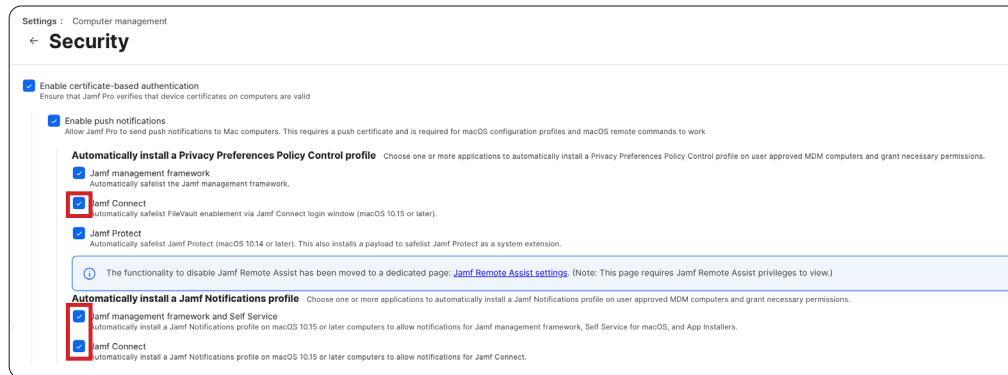


4. Confirm the following Jamf connect profiles are shown.

- Jamf Connect License(Optional)
- Jamf Connect Login
- Jamf Connect Menu Bar
- Jamf Connect Notifications
- Jamf Connect PPC.

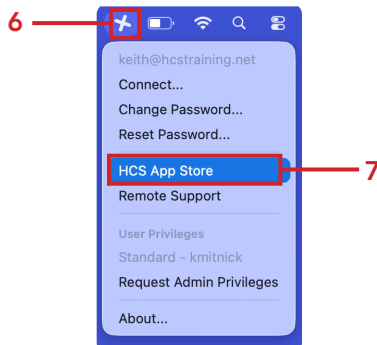


5. If you don't see Jamf Connect Notifications, and Jamf Connect PPC, you will need to enable those on your Jamf Pro server. Go to Settings > Computer Management > Security and make sure the three Jamf connect settings are enabled as shown in the picture B below. Quit System Settings when done.



6. Click Self Service+ on the menu bar.

7. Select HCS App Store.

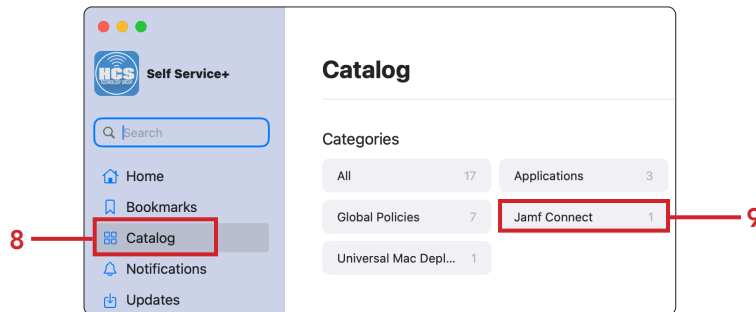




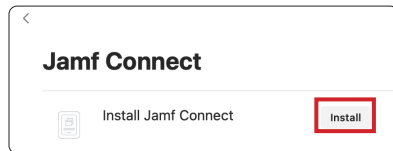
8. Click Catalog.

9. Click Jamf Connect.

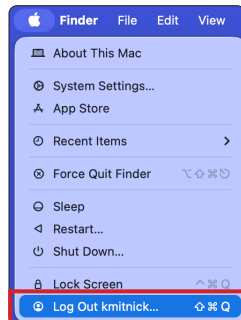
NOTE: This guide used Jamf Connect as the category, if you used a different category, select it.



10. Click Install. Quit Self Service+ when the installation is completed.



11. Log out of your Mac computer.



You are presented with the Jamf Connect Login screen. What appears after signing in will depend on how the existing account names on your Mac computer are spelled.

Scenario A

On our test Mac there is an existing standard account named "kmitnick." In Microsoft Entra ID, there is an account named "Keith" In this case, Jamf Connect will prompt you to select which local account to sync with your Microsoft Entra ID account.

Scenario B

On our test Mac there is an existing administrator account named "Craig" which matches the account name in Microsoft Entra ID. Jamf Connect will automatically sync with the "Craig" account and you may be prompted to sync your password if it differs from your local Mac account password.



Scenario A:

12. Enter your Microsoft Entra ID user name and click Next.

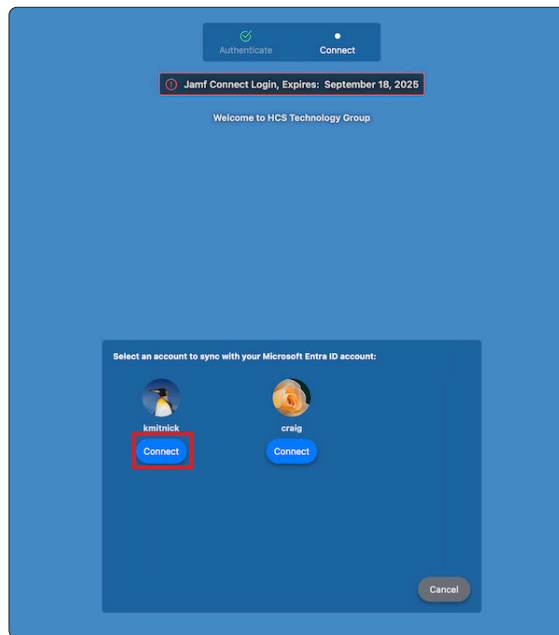
A screenshot of the Microsoft Entra ID sign-in page. The page has a white background with a blue header bar. The header bar contains the Microsoft Entra ID logo on the left and the text 'Sign in' in the center. Below the header bar, there is a text input field containing the email address 'keith@hcstraining.net'. Below the input field, there is a link that says 'Can't access your account?'. At the bottom of the page, there are two buttons: a grey 'Back' button and a blue 'Next' button. The 'Next' button is highlighted with a red rectangular border. Below the buttons, there is a link that says 'Sign-in options'.

13. Enter your password and click Sign in.

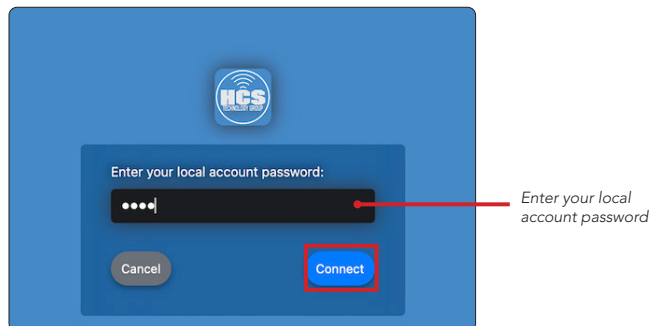
A screenshot of the Microsoft Entra ID 'Enter password' screen. The page has a white background with a blue header bar. The header bar contains the Microsoft Entra ID logo on the left and the text 'Enter password' in the center. Below the header bar, there is a text input field containing a series of dots representing a password. Below the input field, there is a link that says 'Forgot my password'. Below the link, there is a link that says 'Use your face, fingerprint, PIN, or security key instead'. At the bottom of the page, there is a blue 'Sign in' button. The 'Sign in' button is highlighted with a red rectangular border.



14. Click Connect next to the account you want to sync. In this guide, we will select kmitnick.
NOTE: This guide used a trial version of Jamf Connect which is why you see a license expiration date. If you followed the optional licensing steps in section four, you will not see the expired license warning. Notice the custom background image is set to solid blue and includes the login window message that we configured in the Jamf Connect Login configuration profile. The local user name HCS does not appear as an account that we can connect to because we added that user to be hidden from account migration.

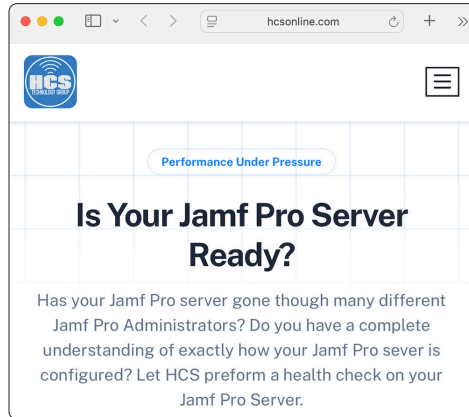


15. Your local Mac account password may be different from your Microsoft Entra ID account password. If so, you are prompted to enter your local Mac account password. This will sync your Microsoft Entra ID password with your local Mac account password. Future logins will only require your Microsoft Entra ID password. Click Connect.





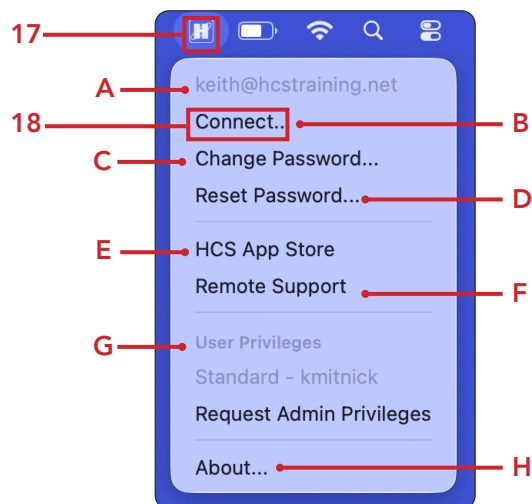
16. If you are using the provided scripts for this guide, we configured a login script to run in the Jamf Connect login configuration profile. The script will open the HCS webpage on login.



17. If you are using the provided images for this guide, we configured a custom image to replace the default Self Service+ icon in the menu bar. Let's have a look at the items in the menu bar that we configured to show in the Jamf Connect configuration profile:

- A. User Info: keith@hcstraining.net is currently signed in.
- B. Connect: This will open the Jamf Connect sign in window.
- C. Change Password: This will re direct you to a Microsoft Entra ID sign in window so you change your password.
- D. Reset Password: This will re-direct you to a Microsoft Entra ID reset password window so you can reset your password.
- E. HCS App Store: This will open Self Service+.
- F. Remote Support: This will bring you to a remote support link on the HCS website.
- G. User Privileges: This will show you if you are a standard or administrator user on your Mac computer.
- H. About: This will show your the version of Jamf Connect that is running and will also allow you to collect log files for troubleshooting.

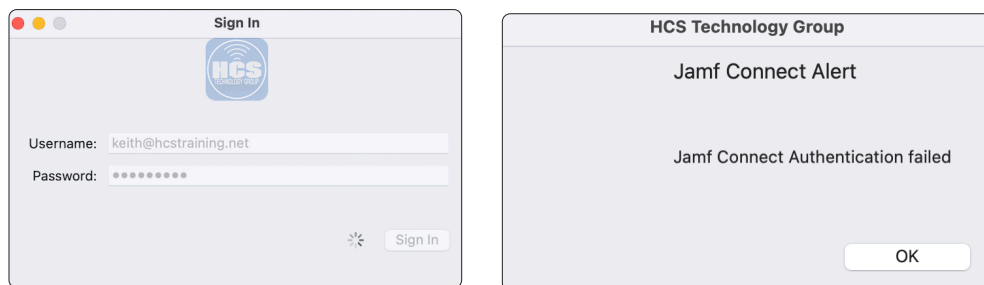
18. Select Connect from the menu.





19. The Jamf Connect sign in screen will pop up and quick go away since you are already signed in. Notice the branded HCS logo in the Sign In window.

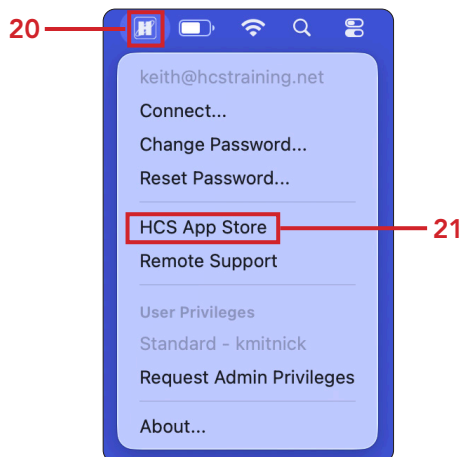
NOTE: If Jamf Connect failed to sign in, the script we configured in the Jamf Connect configuration profile to run on failure will present the Jamf Connect Alert message shown below.



20. Click the Self Service+ icon in the menu bar. Notice the logo has changed to a branded logo.

NOTE: You will only see this if you installed the branding files we created in section two of this guide.

21. Select HCS App Store.

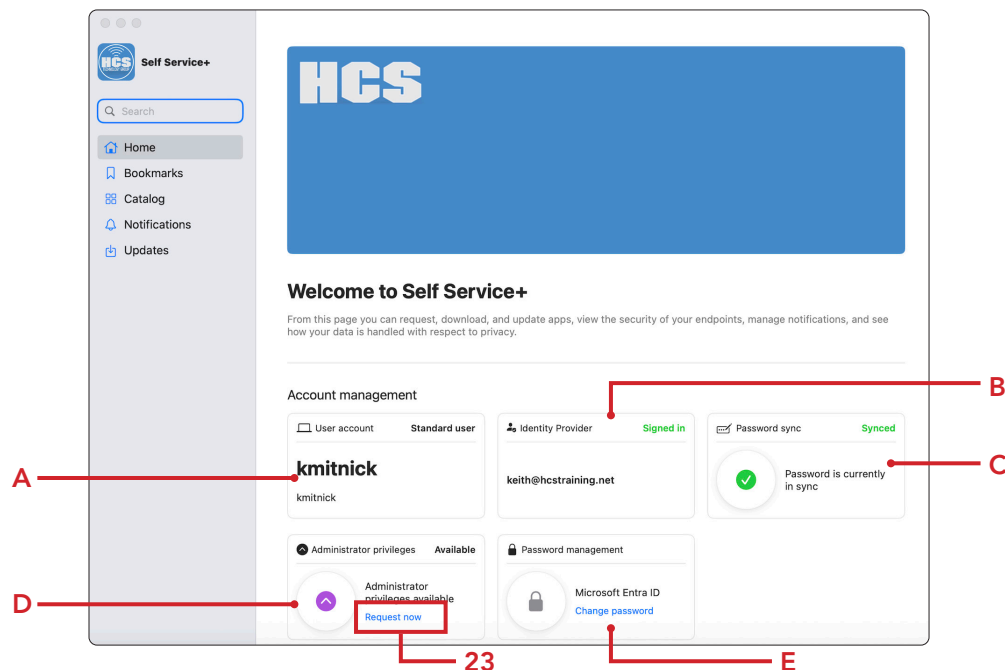




22. Self Service+ will open. The Jamf Connect Menu Bar is now part of Self Service+. Let's have a look at some of the features. If necessary, click Home in the sidebar. An account management page shows the following:

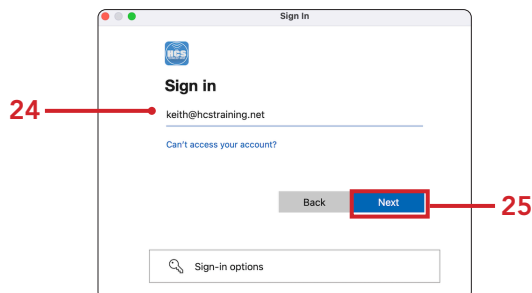
- A. User Account: Displays the current logged in user and their privileges. I.E. Administrator or Standard user.
- B. Identity Provider: Displays the current logged in user account status.
- C. Password Sync: Displays the password sync status.
- D. Administrator Privileges available: This allows you to elevate a standard user account to an administrator for a set amount of time.
- E. Password Management: This will re-direct you to a Microsoft Entra ID sign in window so you can change your password.

23. Select Request now on Administrator privileges.



24. Enter your Microsoft Entra ID user name.

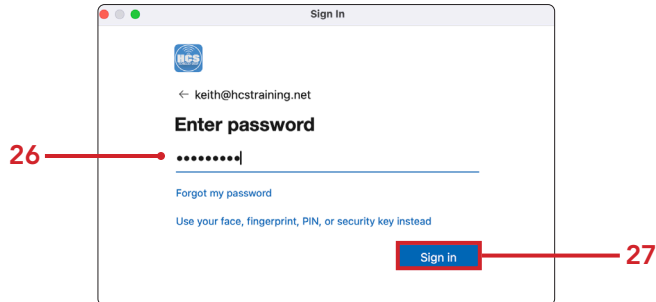
25. Click Next.





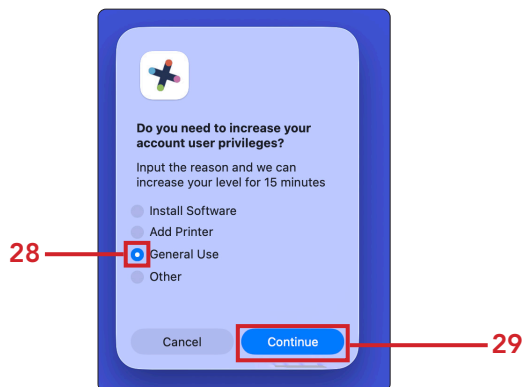
26. Enter your password.

27. Click Sign in.

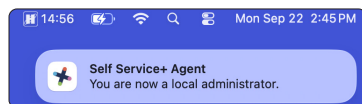


28. You are presented with a window asking you to select a reason for promoting you to an administrator. Select a radio button of your choosing. This guide will select General Use.

29. Click Continue.

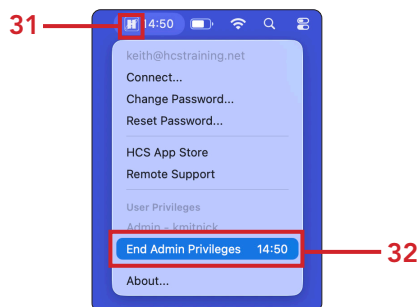


30. A notification will appear letting you know you are now a local administrator.



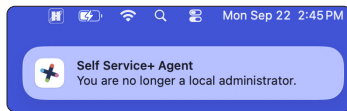
31. Click on Self Service+ on the menu bar. You will see "End Admin Privileges" with the time remaining. We set this to 15 minutes in the Jamf Connect configuration profile.

32. Select "End Admin Privileges".



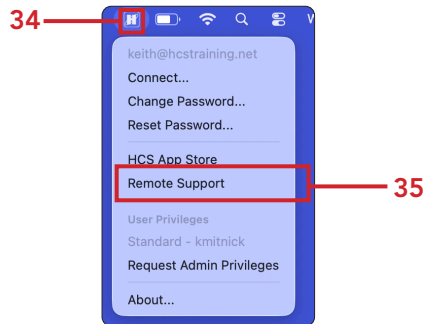


33. A notification will appear letting you know you are no longer a local administrator.

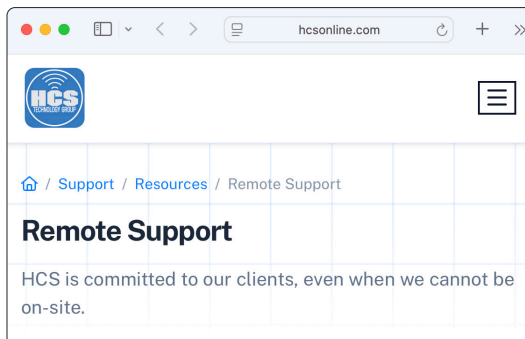


34. Click on Self Service+ on the menu bar.

35. Select Remote Support.



36. Remote Support takes you to the Remote Support page on the HCS website. We configured this in the Jamf Connect configuration profile.





Scenario B

NOTE: All of the customizations shown in scenario A will be exactly the same in scenario B. We will not cover the customization steps in scenario B. Just the login differences.

37. Enter your Microsoft Entra ID user name.

38. Click Next.

A screenshot of the HCS 'Sign in' page. At the top is the HCS logo. Below it is the heading 'Sign in'. A text input field contains the email address 'craig@hcstraining.net', with a red line and the number '37' pointing to it. Below the input field is a link that says 'Can't access your account?'. At the bottom of the main content area are two buttons: a grey 'Back' button and a blue 'Next' button, with a red line and the number '38' pointing to the 'Next' button. At the very bottom is a section titled 'Sign-in options' with a key icon.

39. Enter your password.

40. Click Sign in.

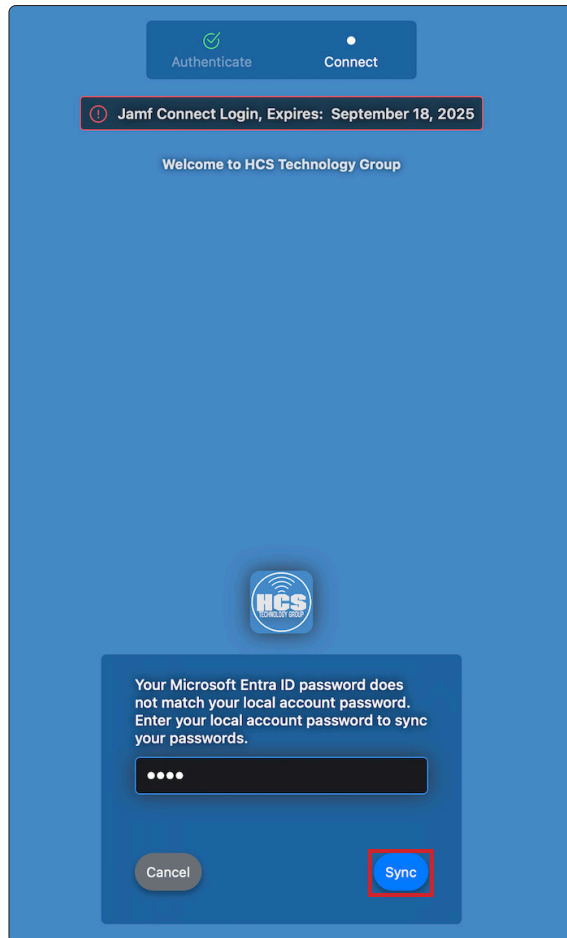
A screenshot of the HCS 'Enter password' page. At the top is the HCS logo. Below it is a back arrow followed by the email address 'craig@hcstraining.net'. The heading 'Enter password' is centered. Below it is a password input field filled with dots, with a red line and the number '39' pointing to it. Below the input field are two links: 'Forgot my password' and 'Use your face, fingerprint, PIN, or security key instead'. At the bottom right is a blue 'Sign in' button, with a red line and the number '40' pointing to it.



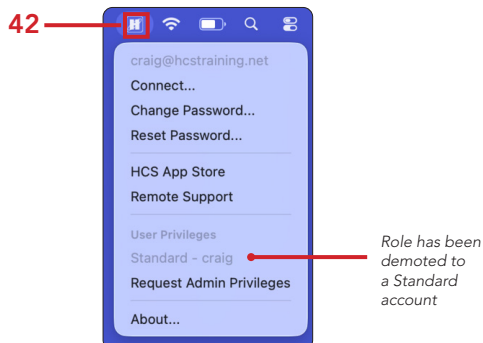
41. Jamf Connect found the local Mac account named "Craig" and automatically selected it. Since Craig's local Mac account password is different from his password in Microsoft Entra ID, he will be prompted to sync his Microsoft Entra ID password with his local Mac account password. Future logins will only require your Microsoft Entra ID password.

Enter your local Mac account password and click Sync.

NOTE: This guide used a trial version of Jamf Connect which is why you see a license expiration date.



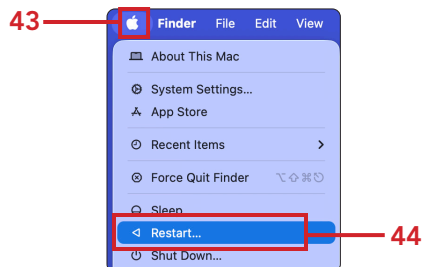
42. Click on Self Service+ on the menu bar. Notice you are connected to your Microsoft Entra ID account and you were demoted to a standard account based on your account role in Microsoft Entra ID.



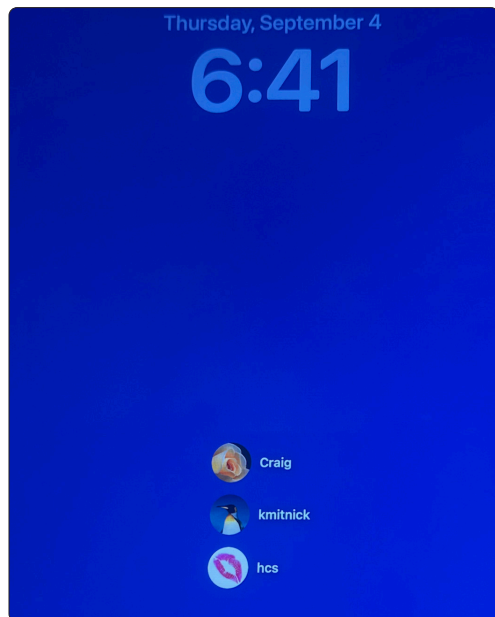


43. Let's test out the FileVault Passthrough setting we configured in the Jamf Connect configuration profile. Click the Apple menu.

44. Select Restart.



45. At the FileVault pre-boot screen, select a user and enter the password. You will not be asked for your credentials a second time and will be brought directly to your desktop.



This completes the guide.