



How to Configure
Jamf Connect with Microsoft Azure



Contents

Preface:..... 3

Prerequisites:..... 4

Section 1: Create a code signing certificate using Jamf Pro's CA..... 8

Section 2: Create users and Groups in Microsoft Azure 17

Section 3: Create App Registrations in Microsoft Azure 24

Section 4: Test Connection to Microsoft Azure Using the Jamf Connect Configuration App 28

Section 5: Create a Basic Jamf Connect Login and Connect Configuration Profile..... 32

Section 6: Manually Install Jamf Connect Configuration Profiles and Application 38

Section 7: Create an Account on the Mac Computer Using Jamf Connect. 46

Section 8: Configure Jamf Connect to Enable FileVault 49

Section 9: Enable FileVault with Jamf Connect..... 57

Section 10: Create a package folder structure for Branding, Login Window, and Menu bar scripts. 62

Section 11: Add Branding and Scripts to the Jamf Connect Configuration Profiles 68

Section 12: Deploy Jamf Connect from Jamf Pro 81

Section 13: Configure Jamf Unlock..... 93



This guide was written using the following:

1. Microsoft Azure free trial account
2. Jamf Pro server 10.30.3
3. Jamf Connect version 2.4
4. Packaging Software of your choosing. This guide will use Composer
5. A Mac computer running macOS Big Sur 11.4 enrolled into a Jamf Pro server
6. A code signing certificate.

Special Thanks to the following people who assisted with this guide:

- The team at HCS
- Bill Smith
- Erin McDonald
- Paul Smith
- Sean Rabbitt

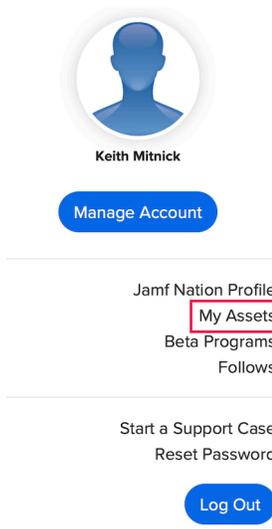


Prerequisites:

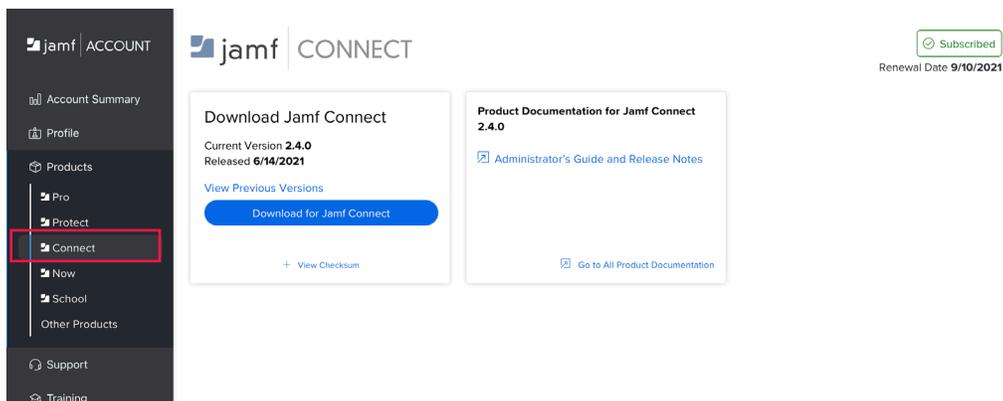
Before you begin this guide, you need to have the latest version of Jamf Connect which is 2.4 at the time this guide was written. Obtain your licensed version of Jamf Connect from your Jamf Nation account by following the instructions below.

NOTE: you can also download a demo of Jamf Connect from: <https://jamf.it/connectinstall>

1. Log in with your Jamf ID for your Jamf Nation account at: <https://www.jamf.com/jamf-nation/>.
Select the account icon in the upper right corner and select My Assets.

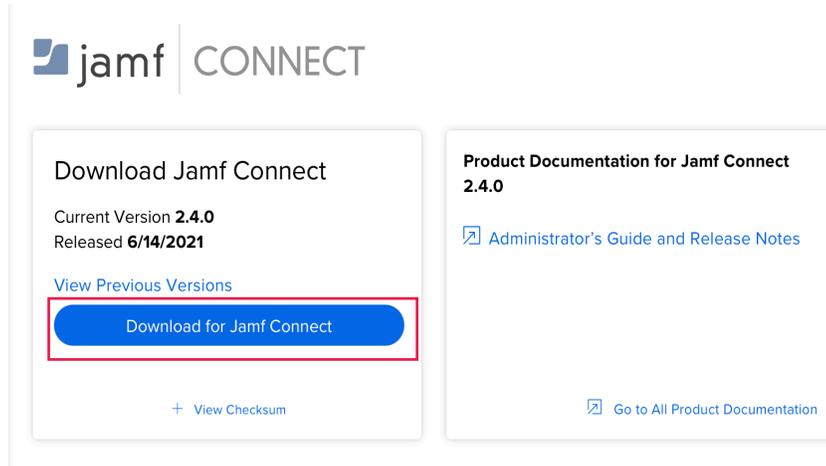


2. Under Products, select Connect





3. Click Download For Mac.



4. Once the download is completed, Open the JamfConnect-2.4.0.dmg.



5. Copy the Jamf Connect Configuration app to the Applications folder.
Keep the JamfConnect-2.4.0.dmg as we will need it later on in the guide.





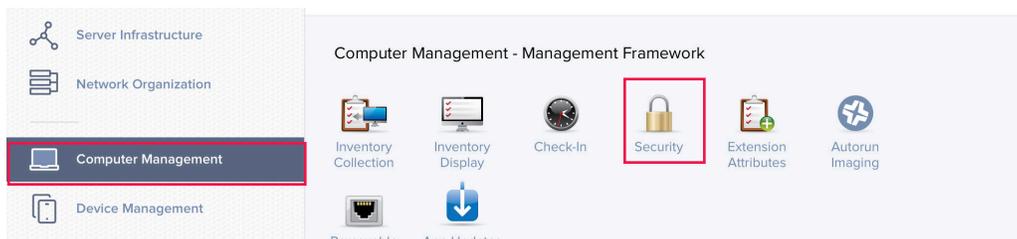
6. We will pre-configure the Jamf Pro server to allow Jamf Connect to enable FileVault and to pre approve notifications from Jamf Connect. Log into your Jamf Pro server.



7. Click Settings (looks like a gear) in the upper left-hand corner.



8. Click Computer Management, then click Security.



9. Select Edit at the bottom-right.





10. Enable the following checkboxes:

A. In the Automatically Install a Privacy Preferences Policy Control profile section, enable Jamf Connect.

B. In the Automatically Install a Jamf Notifications Profile section, enable Jamf Connect.

By enabling both of these settings for Jamf Connect, it will allow us to use Jamf Connect to Enable FileVault and auto approve any notifications for Jamf Connect.

11. Click Save.

Settings : Computer Management

← Security

Enable certificate-based authentication
Ensure that Jamf Pro verifies that device certificates on computers are valid

Enable push notifications
Allow Jamf Pro to send push notifications to Mac computers. This requires a push certificate and is required for macOS configuration profiles and macOS remote commands to work

Automatically install a Privacy Preferences Policy Control profile
Choose one or more applications to automatically install a Privacy Preferences Policy Control profile on user approved MDM computers and grant necessary permissions.

Jamf management framework
Automatically safelist the Jamf management framework (macOS 10.14 or later).

Jamf Connect
Automatically safelist FileVault enablement via Jamf Connect login window (macOS 10.15 or later).

Jamf Protect
Automatically safelist Jamf Protect (macOS 10.14 or later).

Automatically install a Jamf Notifications profile
Choose one or more applications to automatically install a Jamf Notifications profile on user approved MDM computers and grant necessary permissions.

Jamf management framework and Self Service
Automatically install a Jamf Notifications profile on macOS 10.15 or later computers to allow notifications for Jamf management framework and Self Service for macOS.

Jamf Connect
Automatically install a Jamf Notifications profile on macOS 10.15 or later computers to allow notifications for Jamf Connect.

SSL Certificate Verification
Ensure that computers verify that the SSL certificate on the Jamf Pro host server is valid and trusted. Choose "Always except during enrollment" if you are using the built-in certificate authority.

Always

Package Validation Conditions under which to use the checksum to validate packages

Cancel Save



Section 1: Create a code signing certificate using Jamf Pro's CA

We will use a code signing certificate to sign the Jamf Connect configuration profiles that we create later in this guide.

Why sign a configuration profile?

Jamf Pro attempts to import all file's values to associate with known settings within the Jamf Pro console and allow further editing. If the <PayloadType> or specific <key> values in the profile are unknown to Jamf Pro, the deployed configuration profile may not contain those values or install correctly. To avoid this, we can sign the configuration profile and upload it to Jamf Pro. When a configuration profile is signed, Jamf Pro will simply label it as a read only profile because it cannot be altered once signed. Another way to get all the settings you need to deploy from Jamf Pro is to upload a plist file. You can manually create a PLIST file that defines the properties for the preference domain you specify in Jamf Pro, and upload the PLIST file directly to Jamf Pro. This guide will focus on signing a configuration profile and creating a code signing certificate using Jamf Pro's Built in CA. If you already have a signing certificate, you can skip this section of the guide.

NOTE: When creating a code signing certificate using your Jamf Pro server, make sure to follow the steps in this guide on a Mac computer that is enrolled in Jamf Pro. Failure to do so will result in a code signing certificate that is not trusted.

1. Open Keychain Access located in /Applications/Utilities.



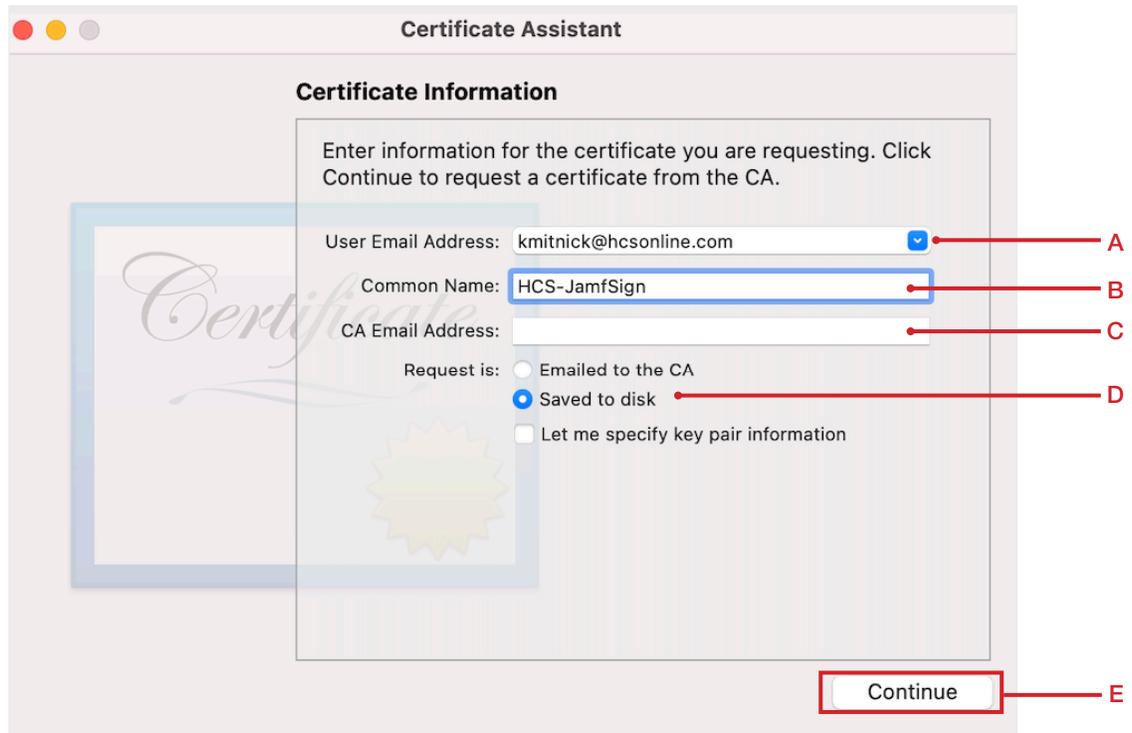
Keychain Access

2. Select Keychain Access > Certificate Assistant > Request a Certificate From a Certificate Authority.

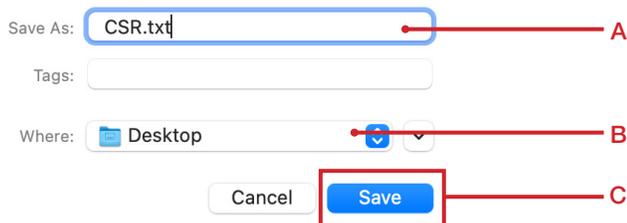




- 3. Configure the following:
 - A. User Email Address: Enter your email address
 - B. Common Name: Enter your company name. This guide will use HCS-JamfSign
 - C. CA Email Address: Leave this blank.
 - D. Request is: Saved to Disk.
 - E. Click Continue.

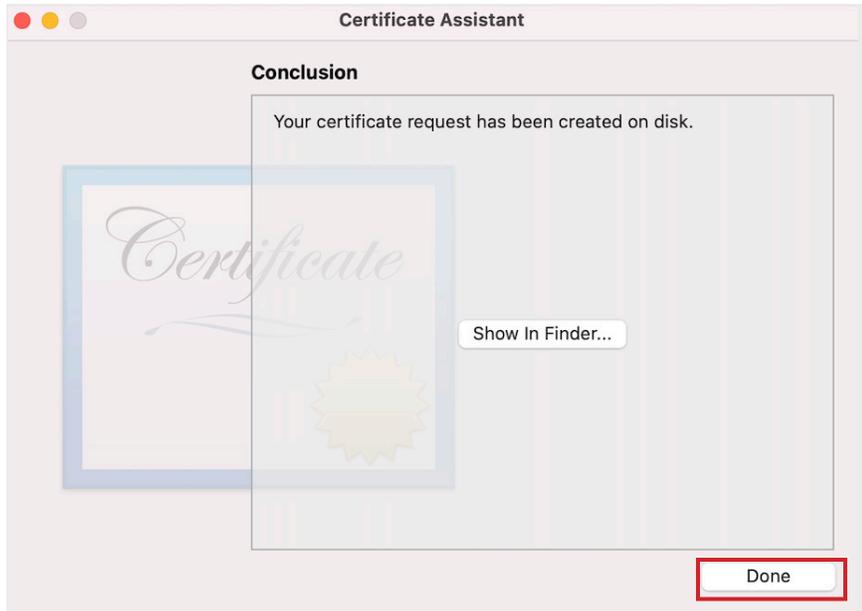


- 4. Configure the following:
 - A. Save as: CSR.txt
 - B. Where: Desktop
 - C. Click Save.





5. Click Done.



6. Open the CSR.txt file on your desktop with a text editor of your choice. This guide will use TextEdit.



7. Copy the entire CSR text.





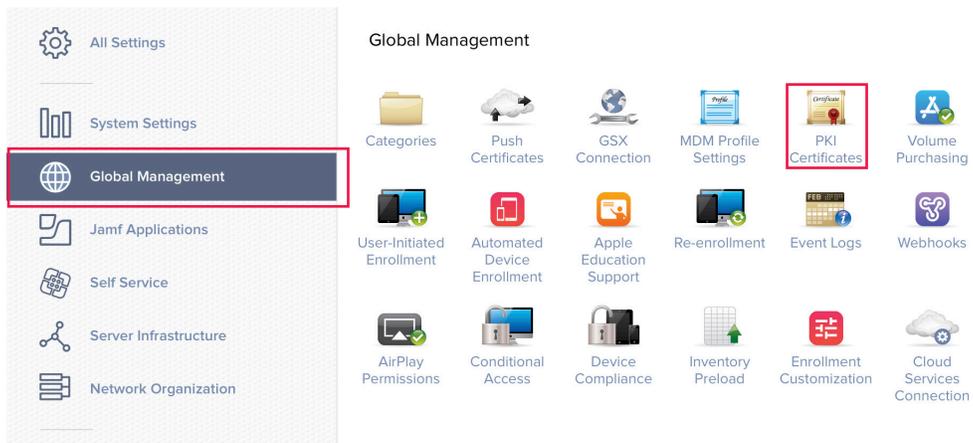
8. Log into your Jamf Pro server.



9. Select the Gear in the upper right corner.

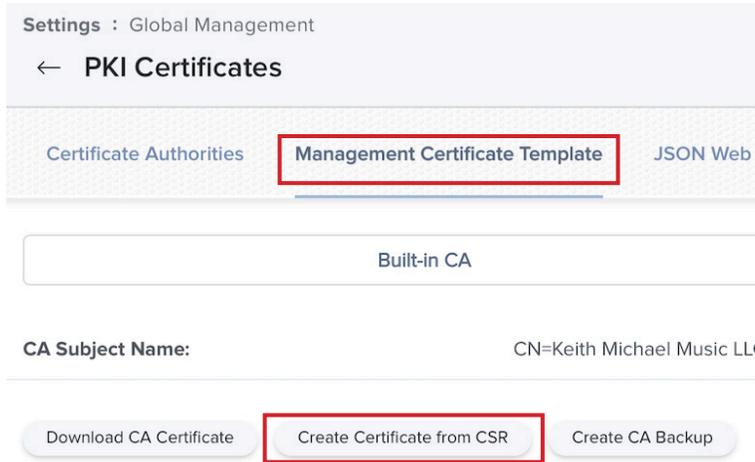


10. Click Global Management then click PKI Certificates.





11. Select Management Certificate Template, then select Create Certificate from CSR.

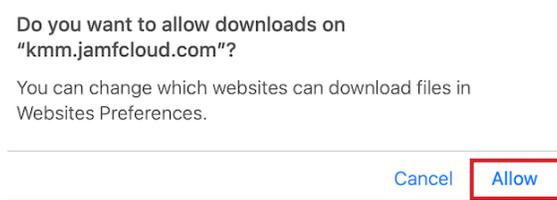


- 12. Configure the following:
 - A. Paste in the CSR text that you copied in step 7.
 - B. Certificate Type: Web Server Certificate
 - C. Click Create.





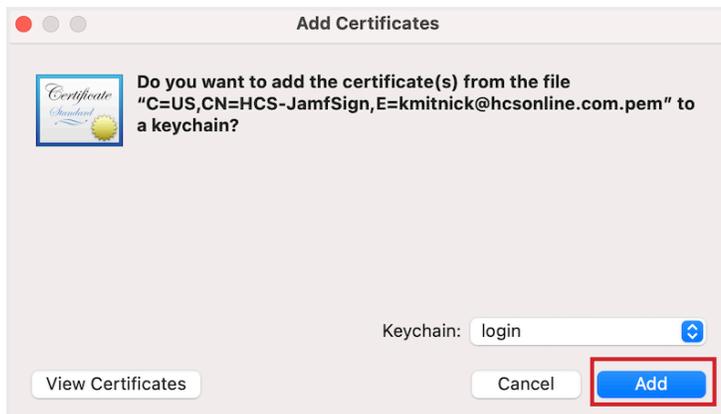
- 13. Select Allow at the message below.
NOTE: After downloading the file your web browser may need to be refreshed to properly display things in Jamf Pro.



- 14. The certificate will download to your Downloads folder. Drag the certificate to your desktop and double click it to open it.

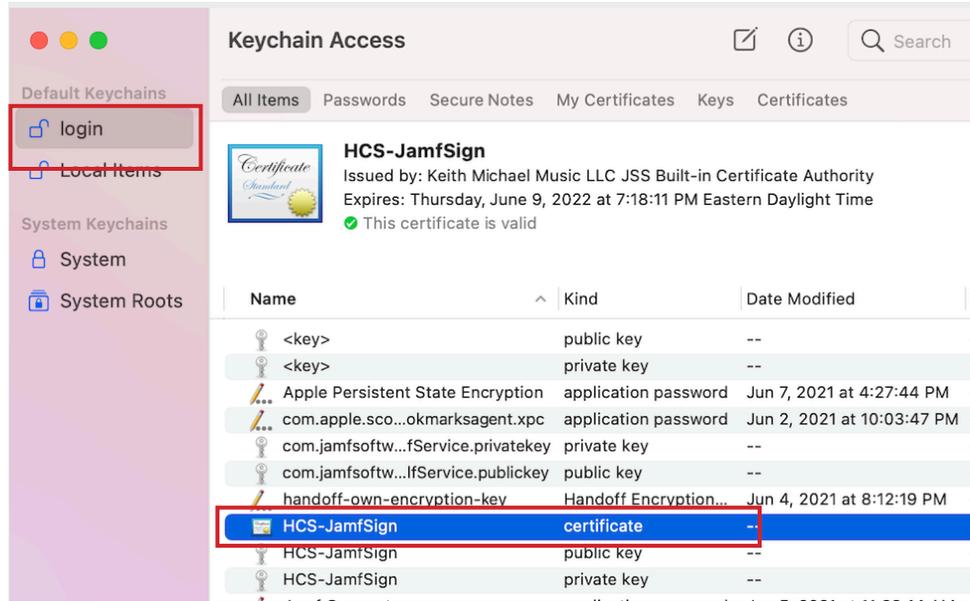


- 15. Select login from the Keychain dropdown menu then click Add.

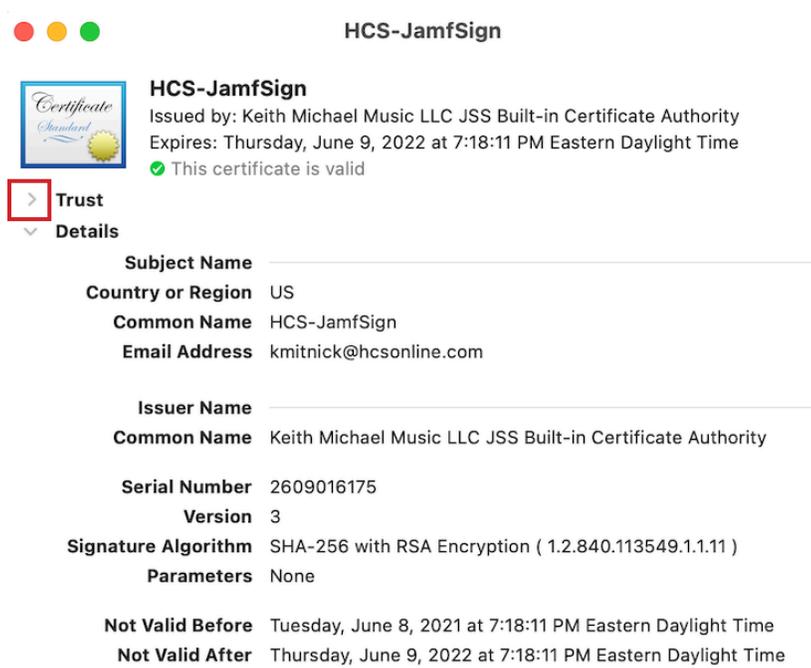




16. In Keychain Access select your login keychain, you will see the certificate on the right side. Double click on your certificate to see more settings.



17. Expand the Trust tab to view the settings.





18. Click the menu, When using this certificate.



19. Select Always Trust. Close the window.

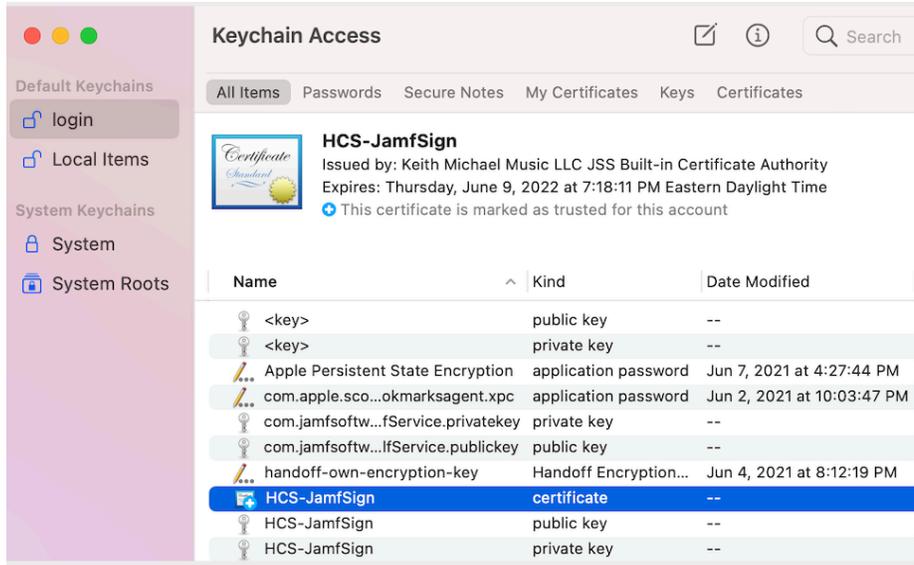


20. Enter your administrative credentials at the message below then click Update Settings.





21. The certificate shows up as trusted. Quit Keychain Access.



This completes this section.

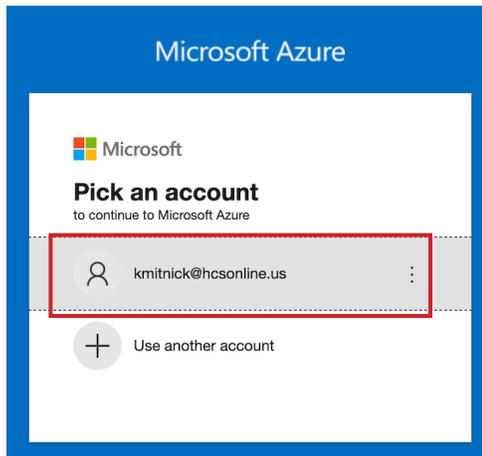


Section 2: Create users and Groups in Microsoft Azure

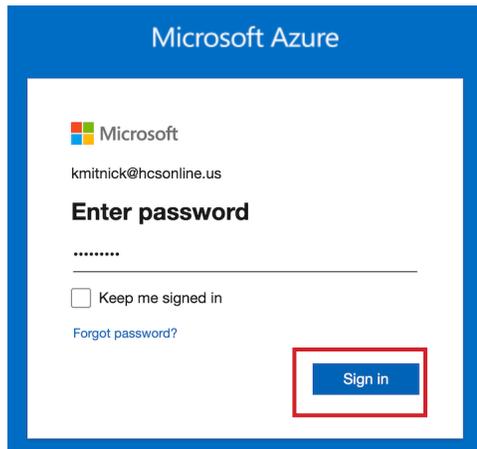
In this section we will create users and group in Microsoft Azure.

NOTE: Skip to Section 3, if you already have Users and Groups configured in your Azure portal.

1. From a web browser of your choosing, go to <https://portal.azure.com> and enter a user name with appropriate privileges to manage the domain



2. Enter your password and click Sign in.



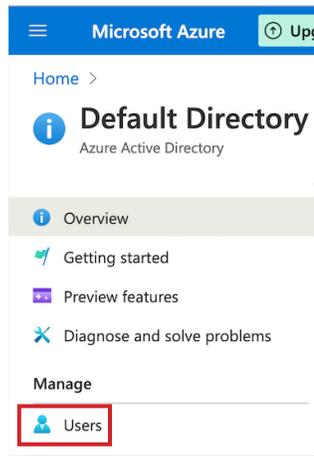
3. Select Azure Active Directory.

Azure services

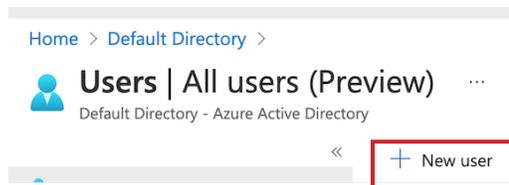




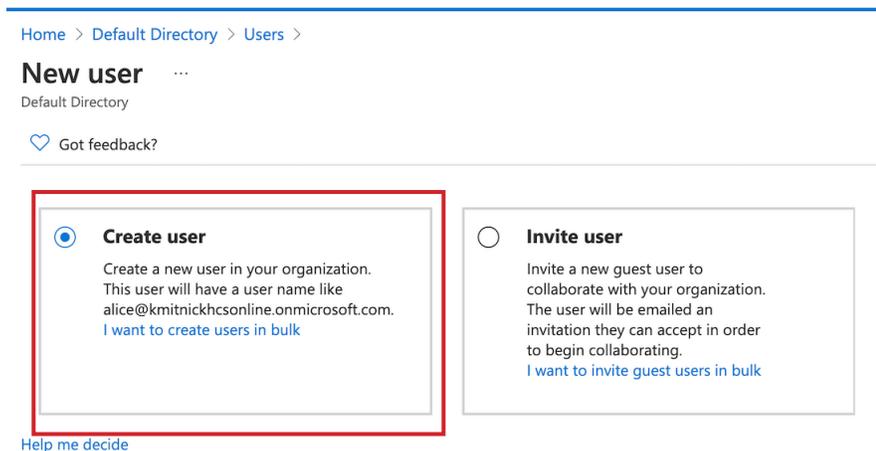
4. From the sidebar, under Manage, select Users.



5. Click New User.



6. Select Create User.





7. In the Identity section, enter your user information. In the Password section, select Let me create the password and enter a password of your choosing.

Identity

User name * @ The domain name I need isn't shown here

Name *

First name

Last name

Password

Auto-generate password

Let me create the password

Initial password *

8. Leave all other sections at their default settings then click the Create button.

Groups and roles

Groups 0 groups selected

Roles User

Settings

Block sign in Yes No

Usage location

Job info

Job title

Department

Company name

Manager No manager selected

Create



9. You will see the user you created show up in the list.

	Name	User principal name	User type	Directory synced	Identity issuer
<input type="checkbox"/>	Keith Mitnick	kmitnick_hconline.us#...	Member	No	kmitnickhconline.onmicr
<input type="checkbox"/>	Craig Cohen	ccohen@kmitnickhcon...	Member	No	kmitnickhconline.onmicr

10. In the upper-right corner click the Default Directory link.

Home > **Default Directory** >

Users | All users (Preview)
Default Directory - Azure Active Directory

11. From the sidebar, select Groups.

Home >

Default Directory
Azure Active Directory

- Overview
- Getting started
- Preview features
- Diagnose and solve problems

Manage

- Users
- Groups**

12. Click New group.

Home > Default Directory >

Groups | All groups ...
Default Directory - Azure Active Directory

<< **+ New group**



13. Enter the following:

- A. Group type: Select Security
- B. Group name: standard users
- C. Group Description: standard user group
- D. Click the No owners selected link, then in the Add owners section search for a user and select that user.
- E. Click the No members selected link

The screenshot shows the 'New Group' configuration page in Microsoft Azure. The 'Group type' is set to 'Security' (A), 'Group name' is 'standard users' (B), and 'Group description' is 'standard user group' (C). The 'Owners' section shows 'No owners selected' (D), and the 'Members' section shows 'No members selected' (E). The 'Add owners' dialog is open, showing a search for 'cc' and a list of users. 'Craig Cohen' is selected in the search results. A red line connects the 'No owners selected' link to the 'Add owners' dialog. The 'Select' button at the bottom of the dialog is highlighted.

14. In the Add owners section search for a user and select that user.

The screenshot shows the 'New Group' configuration page in Microsoft Azure. The 'Add members' dialog is open, showing a search for 'cc' and a list of users. 'Craig Cohen' is selected in the search results. The 'Selected items' section shows 'Craig Cohen' with a 'Remove' button. The 'Select' button at the bottom of the dialog is highlighted.



15. Click the create button.

Home > Default Directory > Groups >

New Group

Group type *

Group name *

Group description

Membership type

Owners
1 owner selected

Members
1 member selected

Create

16. Select New group.

Home > Default Directory >

Groups | All groups

Default Directory - Azure Active Directory

+ New group

17. Enter the following:

- A. Group type: Select Security
- B. Group name: HCS Administrators
- C. Group Description: HCS Administrators
- D. Select the No owners selected link, then in the Add owners section search for a user and select that user.
- E. Select the No members selected link,

Home > Default Directory > Groups >

New Group

A → Group type *

B → Group name *

C → Group description

Membership type

Owners
D → **No owners selected**

Members
E → **No members selected**

Create

Add owners

Search

- CC** Craig Cohen
ccohen@kmitnickhconline.onmicrosoft.com
- KM** Keith Mitnick
kmitnick@hconline.us
Selected

Owners

- KM** Keith Mitnick
kmitnick@hconline.us **Remove**

Select



18. In the Add owners section search for a user and select that user.

The screenshot shows the Microsoft Azure portal interface. On the left, the 'New Group' configuration page is visible, with fields for Group type (Security), Group name (HCS Administrators), Group description (HCS Administrators), and Membership type (Assigned). On the right, the 'Add members' dialog is open, showing a search bar with 'km' entered. Below the search bar, a search result for 'Keith Mtnick kmtnick@hcsonline.us' is shown and marked as 'Selected'. Below the dialog, a 'Select' button is highlighted with a red box.

20. You will see both groups configured.

NOTE: Jamf Connect can create user accounts on a Mac Computer based on the role assigned to the user in Azure. IE.. Admin or standard user. You could ignore the role assigned in Azure by selecting Ignore Roles in your Jamf Connect Login profile.

The screenshot shows the 'Groups' list view in the Azure portal. The table below contains the following data:

Name	Object Id	Group Type	Membership Type	Email
<input type="checkbox"/> HA HCS Administrators	eae1a8ed-7fce-4f94-af98-d...	Security	Assigned	
<input type="checkbox"/> SU standard users	da3ac1c1-0a20-4ed4-8dd3-...	Security	Assigned	

21. In the upper-right corner click the Default Directory link.

The screenshot shows the 'Users | All users (Preview)' page in the Azure portal. The breadcrumb navigation at the top includes 'Home' and 'Default Directory', with 'Default Directory' highlighted by a red box. Below the breadcrumb, there is a user icon and the text 'Users | All users (Preview)' and 'Default Directory - Azure Active Directory'.

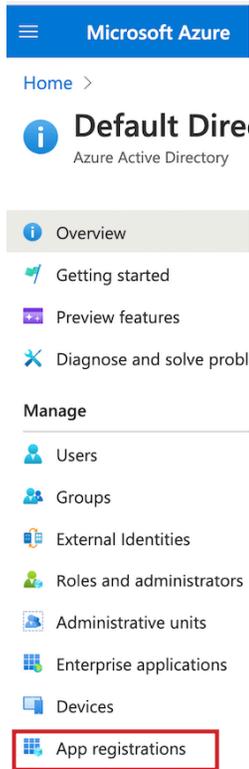
This completes this section.



Section 3: Create App Registrations in Microsoft Azure

In this section we will create an App Registration for Jamf Connect in Microsoft Azure. This is required so Jamf Connect can speak with Microsoft Azure via API's.

1. From the sidebar, select App registrations.



2. Select New registration.





3. Enter the following:

- A. The user-facing display name: **Jamf Connect**
- B. Redirect URI: Select Public client/native (mobile & desktop)
- C. Enter this URI: **https://127.0.0.1/jamfconnect**
- D. Click the Register button.

Microsoft Azure Upgrade Search resources, services, and docs (G+)

Home > Default Directory >

Register an application

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

A Jamf Connect ✓

Supported account types

Who can use this application or access this API?

- Accounts in this organizational directory only (Default Directory only - Single tenant)
- Accounts in any organizational directory (Any Azure AD directory - Multitenant)
- Accounts in any organizational directory (Any Azure AD directory - 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.

B Public client/native (mobile ... **C** 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](#)

D Register

4. Copy the Application (client) ID and paste it into a sticky note on your desktop. We will need this ID in a later step.

Delete Endpoints Preview features

Got a second? We would love your feedback on Microsoft identity platform (previously Azure AD for developer). →

Essentials

Display name	: Jamf Connect	Client credentials	: Add a certificate or secret
Application (client) ID	: a1e4f735-5b8fed3d-1859-466d-beff-d62c76695008	Redirect URIs	: 0 web, 0 spa, 1 public client
Object ID	: 5b8fed3d-1859-466d-beff-d62c76695008	Application ID URI	: Add an Application ID URI
Directory (tenant) ID	: 8a7e8fd4-c71b-46df-b0cc-f7d33febea76	Managed application in l...	: Jamf Connect
Supported account types	: My organization only		



5. From the sidebar, select API permissions.

Microsoft Azure

Home > Default Directory

Jamf Connect

Search (Cmd+)

- Overview
- Quickstart
- Integration assistant

Manage

- Branding
- Authentication
- Certificates & secrets
- Token configuration
- API permissions**

6. Select Grant admin consent for Default Directory.

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 Default Directory

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

To view and manage permissions and user consent, try [Enterprise applications](#).

7. Click Yes.

Grant admin consent confirmation.

Do you want to grant consent for the requested match what is listed below.



8. in the status column, it will say Granted for Default Directory.

Refresh | Got feedback?

Successfully granted admin consent for the requested permissions.

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 Default Directory

API / Permissions name	Type	Description	Admin consent requ...	Status
Microsoft Graph (1)				
User.Read	Delegated	Sign in and read user profile	No	Granted for Default Dire... ⋮

To view and manage permissions and user consent, try [Enterprise applications](#).

9. Select Default Directory, then select Authentication.

Microsoft Azure

Home > Default Directory > J

Jamf Connect

Search (Cmd+/)

- Overview
- Quickstart
- Integration assistant

Manage

- Branding
- Authentication

10. In the Advanced settings section, Set Allow public client flows to Yes.

Advanced settings

Allow public client flows ⓘ

Enable the following mobile and desktop flows:

Yes No

11. Click Save. This completes the Microsoft Azure configuration.

Authentication ⚙ ...

Save Discard | Got feedback?

Add URI



Section 4: Test Connection to Microsoft Azure Using the Jamf Connect Configuration App

In this section we will test basic authentication using the Jamf Connect Configuration app with a Microsoft Azure account using OIDC and ROPG. OIDC will test the users authentication and ROPG will test the users authorization.

1. Open the Jamf Connect Configuration App located in the Applications folder.



Jamf Connect Configuration

2. Follow these steps:

- A. Click Add (+) on the bottom left and name the configuration Azure Authentication.
- B. Click the Identity Provider tab.
- C. Identity Provider: Azure
- D. OIDC Client ID: Paste in the client ID that you copied in section 3 step 4 of this guide.
- E. ROPG Client ID: Paste in the client ID that you copied in section 3 step 4 of this guide.
- F. OIDC Redirect URI: <https://127.0.0.1/jamfconnect>
- G. In the upper-right corner, click the Test button. Select OIDC from the menu.

The screenshot shows the Jamf Connect Configuration app interface. The main window is titled "Jamf Connect Configuration" and has a sidebar on the left with a blue button labeled "Azure Authentica..." and the date "07/06/2021". The main area is divided into "Required" and "Advanced OIDC" sections. The "Required" section has fields for "Identity Provider" (set to "Azure"), "OIDC Client ID", and "ROPG Client ID". The "Advanced OIDC" section has fields for "Scopes" (set to "openid profile email"), "Token Caching" (set to "Ignore cookies"), "Client Secret", "Tenant", "OIDC Redirect URI" (set to "https://127.0.0.1/jamfconnect"), and "Discovery URL". A "Test" button is in the top right corner, and a menu is open over it with "OIDC" selected. Red lines and letters A through G point to these specific elements.



3. Enter one of your accounts in Microsoft Azure, then click Next.

 Microsoft

Sign in

ccohen@kmitnickhconline.onmicrosoft.com|

No account? [Create one!](#)

[Can't access your account?](#)

Next

4. Enter your account password, then click Sign in.

 Microsoft

← ccohen@kmitnickhconline.onmicrosoft.com

Enter password

.....|

[Forgot my password](#)

Sign in

5. If greeted with the message below, select Skip for now (14 days until this is required). Click Next.

 Microsoft

ccohen@kmitnickhconline.onmicrosoft.com

Help us protect your account

Microsoft has enabled Security Defaults to keep your account secure. [Learn more about the benefits of Security Defaults](#)

Skip for now (14 days until this is required)

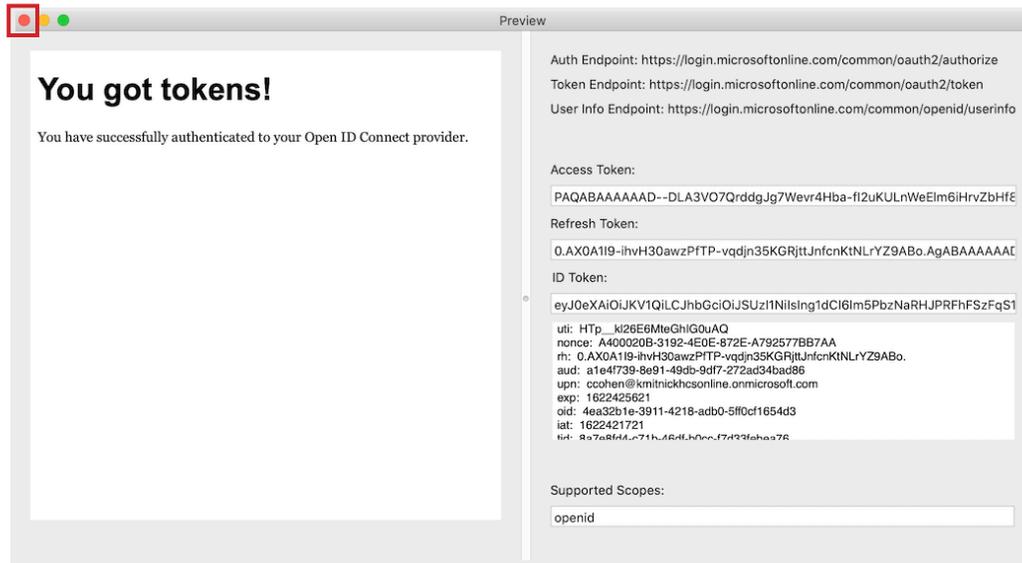
[Use a different account](#)

Next

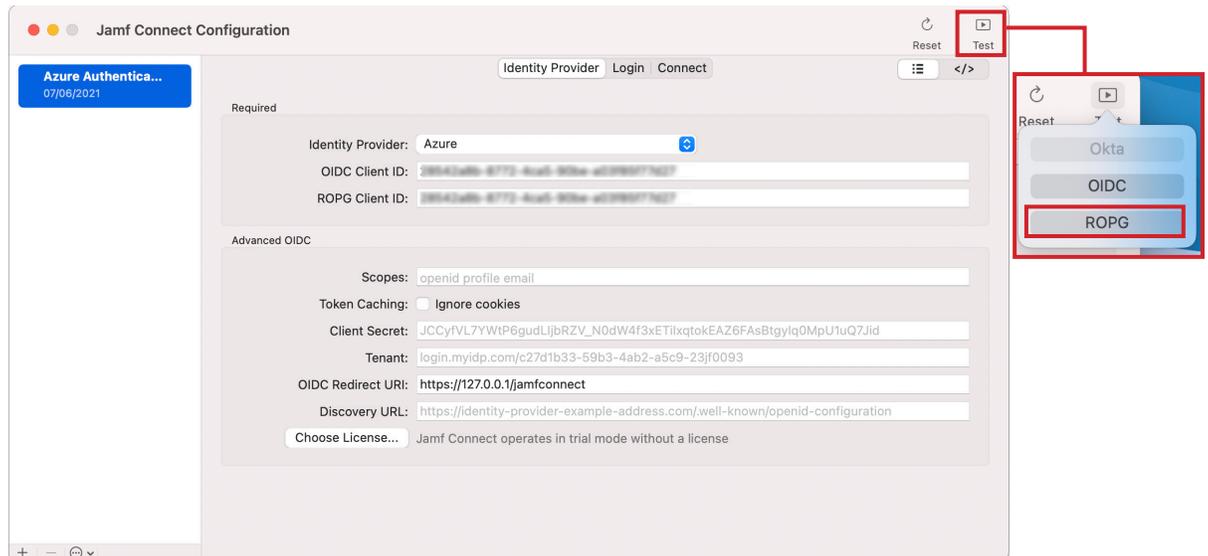


6. If all went well, you will be greeted with the message below. Close this window to return to the Jamf Connect Configuration app.

NOTE: We are testing this to confirm we can get authentication tokens from Azure using OIDC. Doing this now saves us from troubleshooting connection issues later.



7. Click the Test button again and select ROPG from the menu.





8. Enter your Microsoft Azure Account name and password, then click Sign in.

A screenshot of the Jamf Connect login interface. The header shows the Jamf logo and the word 'CONNECT'. Below the header, there are two input fields: 'Username:' with the value 'ccohen@kmitnickhconline.onmicros' and 'Password:' with a masked password of seven dots. A blue 'Sign In' button is located at the bottom right of the form, highlighted with a red border.

9. If all went well, you're greeted with the message below. Click OK.

NOTE: We are testing this to ensure the resource owner password grant (ROPG), which Jamf Connect uses for password verification and syncing, is correctly configured. Doing this now saves us from troubleshooting authentication issues later.

A screenshot of a success message dialog box. On the left is a circular icon containing a person silhouette and a gear. To the right of the icon, the text reads 'Success' in bold, followed by 'Your configuration seems to be working.' At the bottom right of the dialog is a blue 'OK' button, highlighted with a red border.

10. Close the Jamf Connect window and leave the Jamf Connect Configuration app open.

A screenshot of the Jamf Connect login interface, identical to the one in step 8. It shows the Jamf logo and 'CONNECT' header, the 'Username:' field with 'ccohen@kmitnickhconline.onmicros', the 'Password:' field with a masked password, and the 'Sign In' button.

This completes this section.

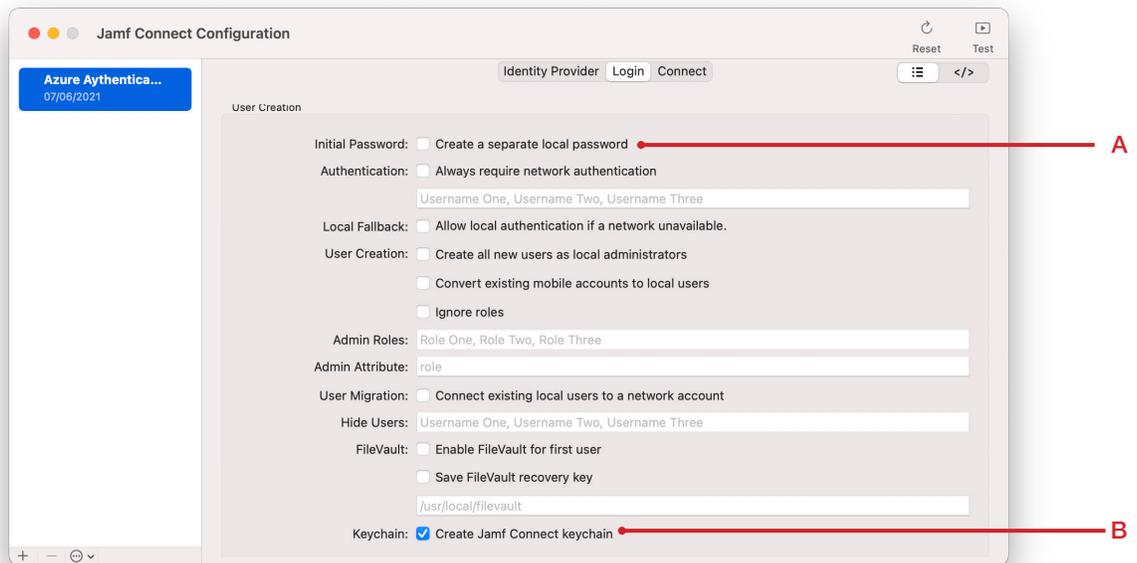


Section 5: Create a Basic Jamf Connect Login and Connect Configuration Profile

In this section we will create a configuration profile for the Jamf Connect Login window and the Jamf Connect Menu Bar Item. The Login window configuration profile is used exclusively at the Login window. The Connect configuration profile is used exclusively as a Menu Bar item and is required to keep users passwords in sync with Microsoft Azure.

1. Open the Jamf Connect Configuration App located in the Applications folder on your Mac computer. Select the Login tab, then configure the following:
 - A. Initial Password: Select then deselect the check box next to Create a separate local password. This is required so the setting key gets created and set to false.
 - B. Keychain: Make sure this is enabled.

NOTE: All other settings are optional and will be covered in later sections of this guide.



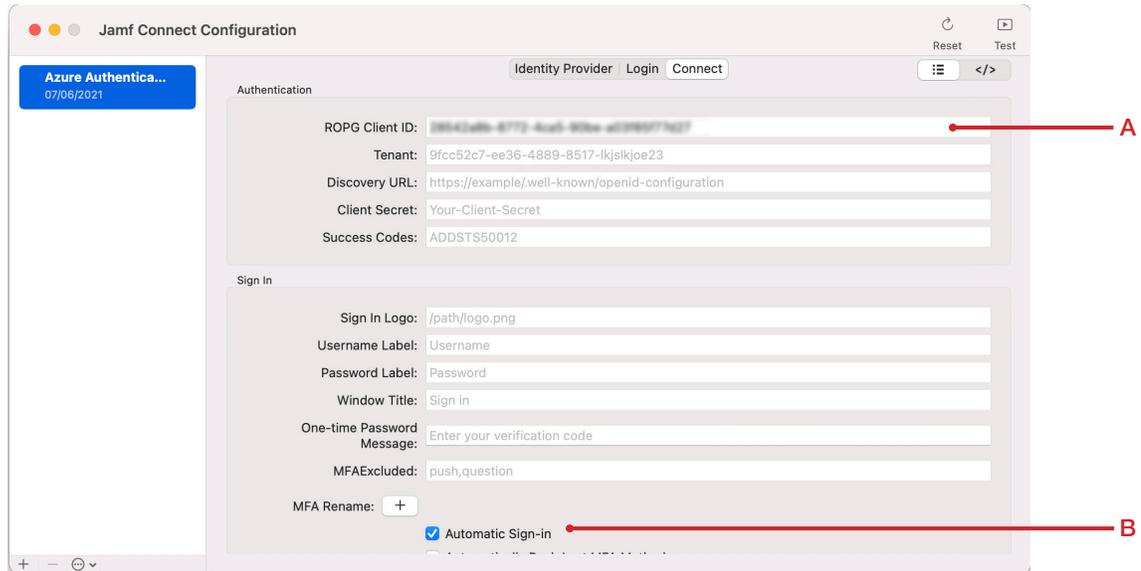


2. Select the Connect tab, then configure the following:

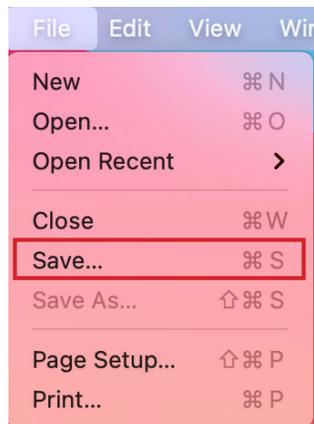
A. ROPG Client ID: Make sure it shows up in the field.

B. Automatic Sign-In: Make sure this is enabled.

NOTE: All other settings are optional and will be covered in later sections of this guide.



3. From the File Menu, Select Save.

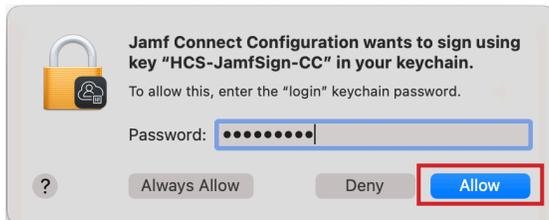




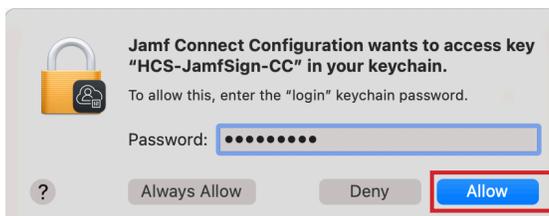
4. Configure the following:

- A. Application: Confirm Jamf Connect Login is selected
- B. File Format: Confirm configuration Profile .mobileconfig is selected
- C. Organization: Enter your organization name. This guide will use **HCS Technology Group**
- D. Payload Name: Jamf Connect Login
- E. Payload Description: Jamf Connect Login
- F. Signing Identity: Select the signing certificate the we created in section 1.
- G. Click Save.

5. At the message below, enter your administrative credentials to sign the configuration profile. Click Allow. You will see this prompt twice.



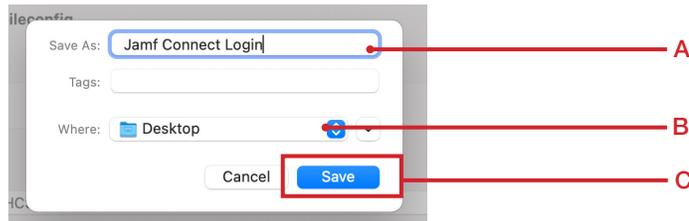
6. At the message below, enter your administrative credentials to sign the configuration profile. Click Allow.





7. Enter the following:

- A. Save As: **Jamf Connect Login**
- B. Where: Desktop
- C. Click Save

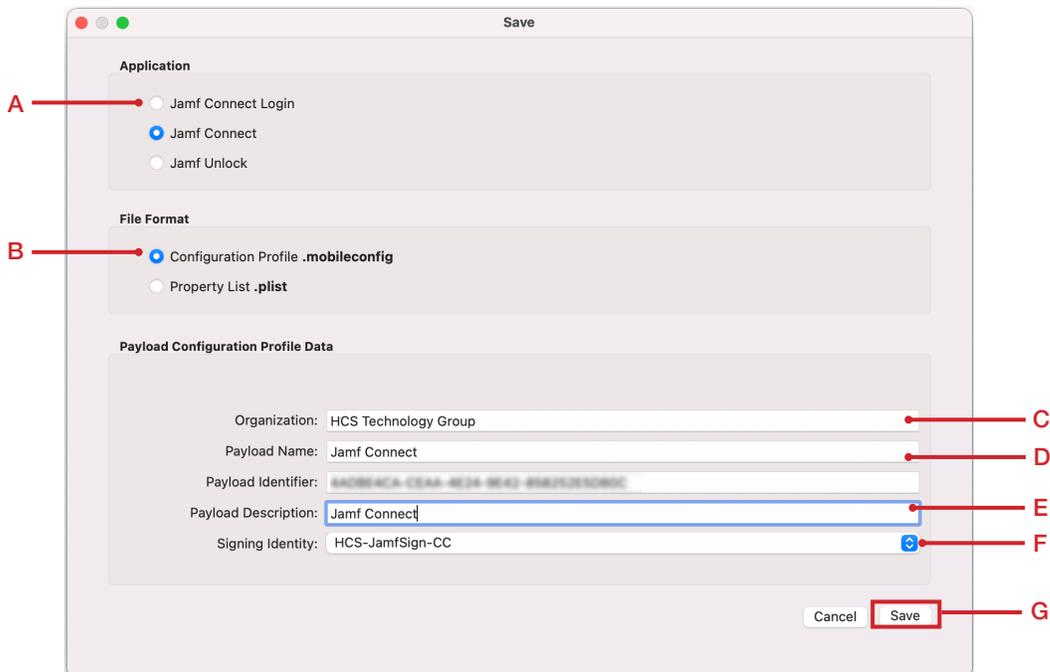


8. Click OK at the message below.



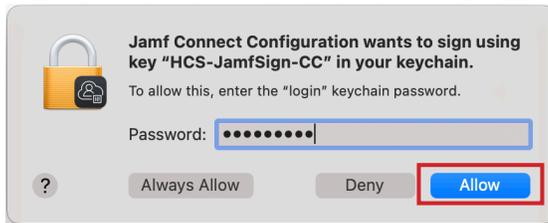
9. Configure the following:

- A. Application: Confirm Jamf Connect is selected
- B. File Format: Confirm configuration Profile `.mobileconfig` is selected
- C. Organization: Enter your organization name. This guide will use **HCS Technology Group**
- D. Payload Name: Jamf Connect
- E. Payload Description: Jamf Connect
- F. Signing Identity: Select the signing certificate the we created in section 1.
- G. Click Save.

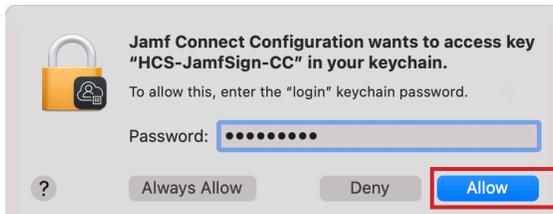




10. At the message below, enter your administrative credentials to sign the configuration profile. Click Allow. You will see this prompt twice.

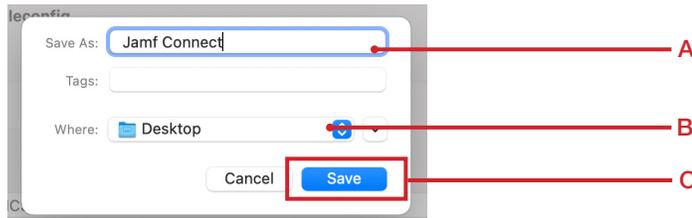


11. At the message below, enter your administrative credentials to sign the configuration profile. Click Allow.

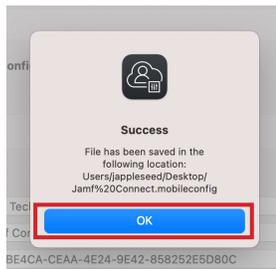


12. Enter the following:

- A. Save As: **Jamf Connect**
- B. Where: Desktop
- C. Click Save

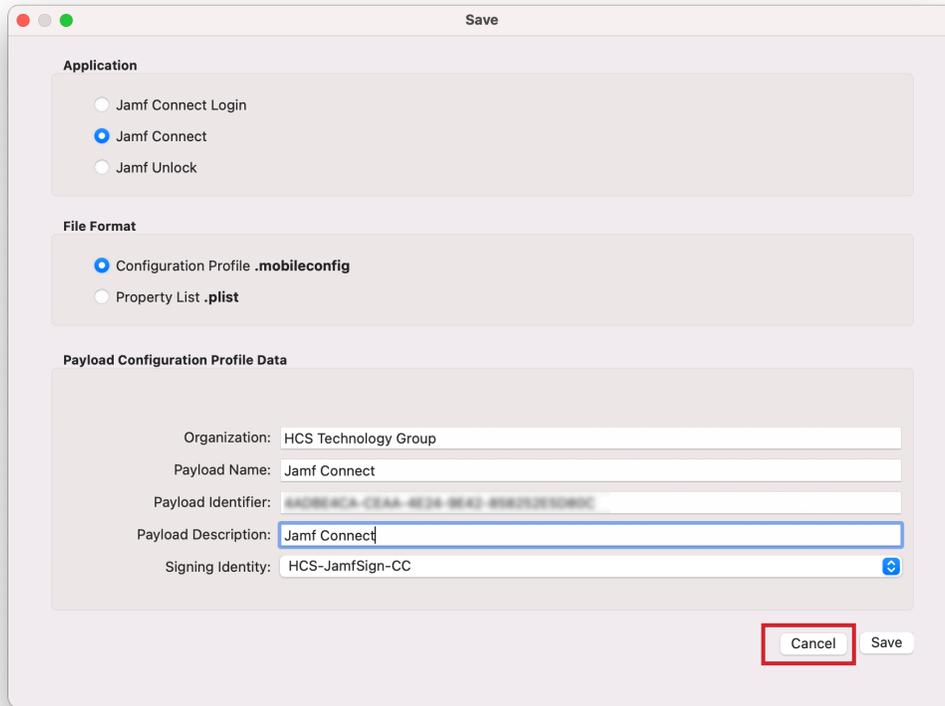


13. Click OK at the message below.





14. Click Cancel to close this window then quit the Jamf Connect Configurator application.



15. Confirm both .mobileconfig files are saved to your Desktop.



This completes this section.



Section 6: Manually Install Jamf Connect Configuration Profiles and Application

In this section we will manually install the Jamf Connect configuration profiles we created in section 5 of this guide, install the Jamf Connect Application, and install the Jamf Connect Launch Agent package that is used to auto launch Jamf Connect on startup. The reason we are manually installing all of these items first is to confirm everything is working. Once confirmed all is working, we will automate the install of all of these items using the Jamf Pro server.

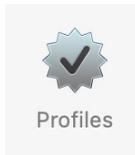
1. Double Click on the Jamf Connect Login.mobileconfig profile to install it.



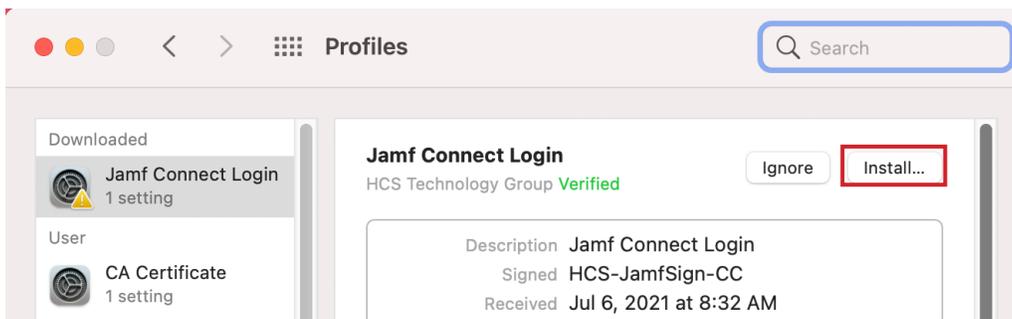
2. Open System Preferences located under the Apple menu.



3. Select the Profiles pane



4. The Jamf Connect profile is waiting to be installed. Click Install.





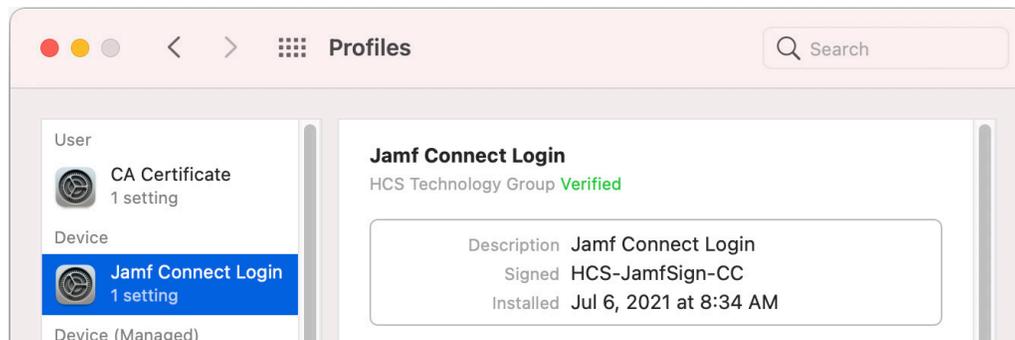
5. Click Install.



6. Enter your administrative credentials then click OK.

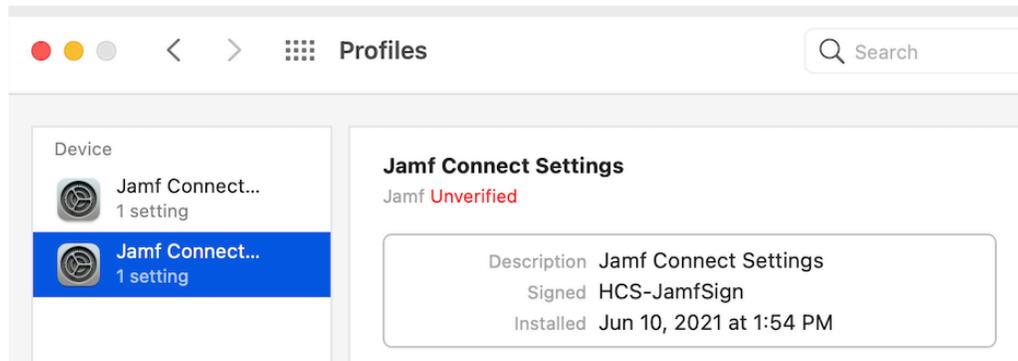


7. The Jamf Connect Login configuration profile is now installed. Follow steps 1-6 to install the Jamf Connect profile.





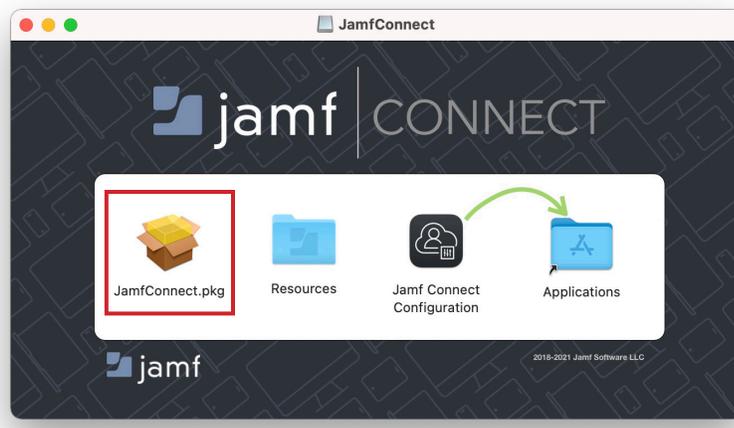
8. Once the Jamf Connect configuration profile is installed, you should have both configuration profiles installed as shown below. You may quit System Preferences if all looks good.



9. Open the JamfConnect-2.4.0.dmg. This was downloaded at the beginning of this guide

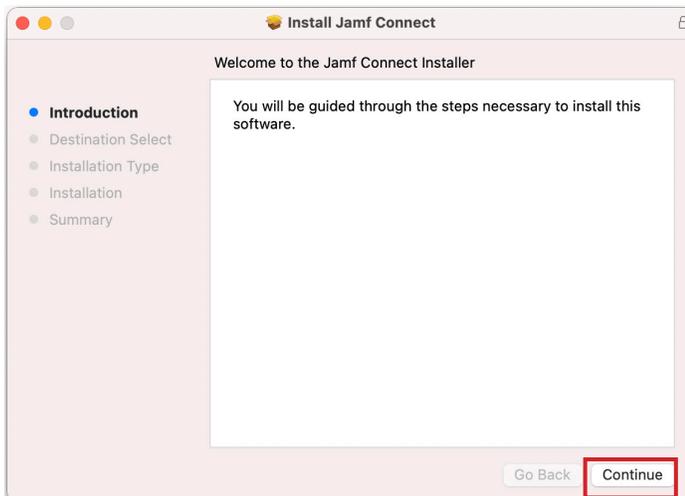


10. Double click the JamfConnect.pkg file to start the installation of Jamf Connect.

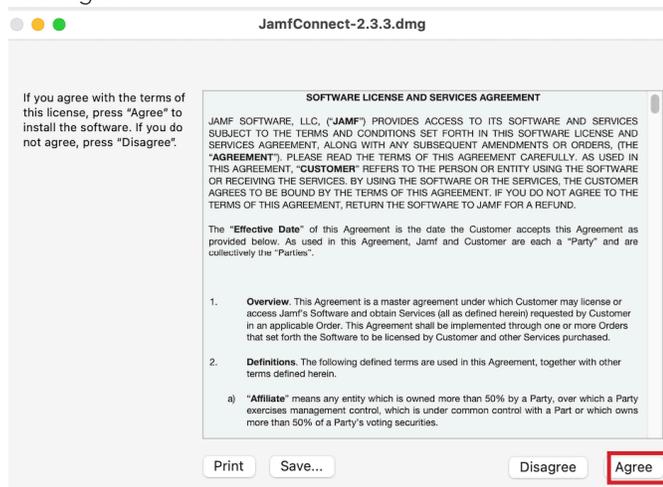




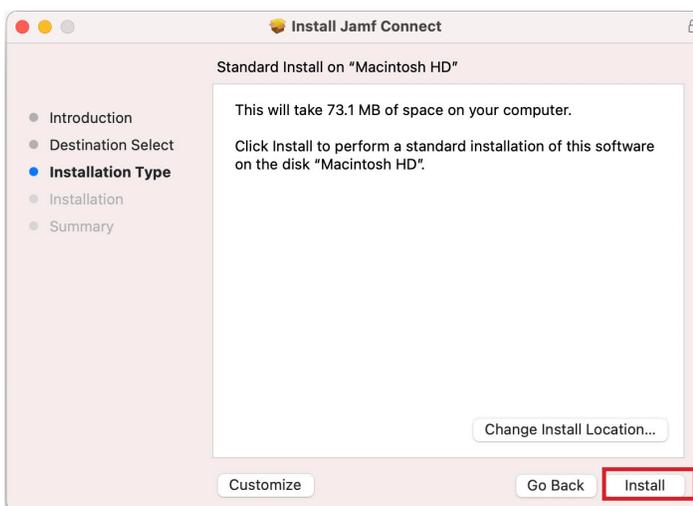
11. Click Continue.



12. Click Agree.

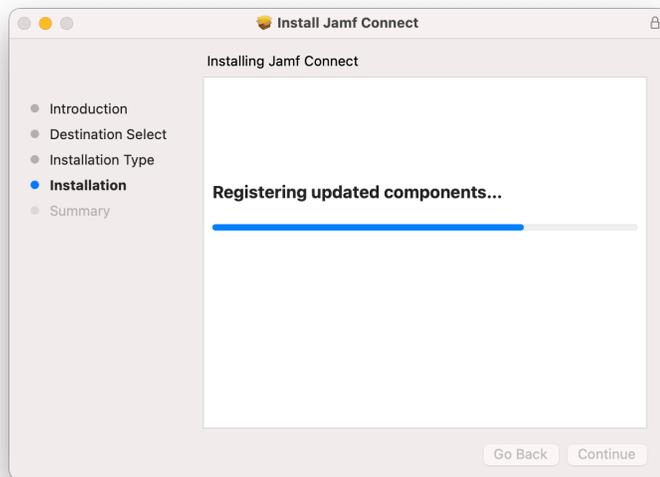


13. Click Install.

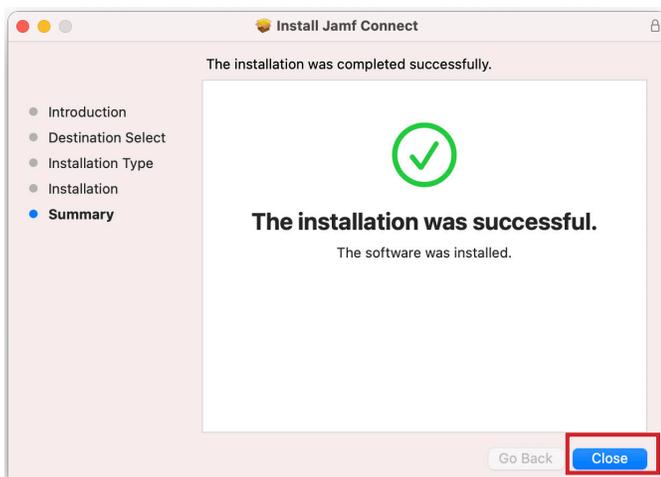




14. Enter your administrative credentials then click Install Software.



15. Click Close.

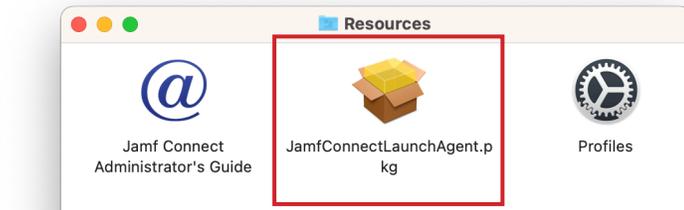




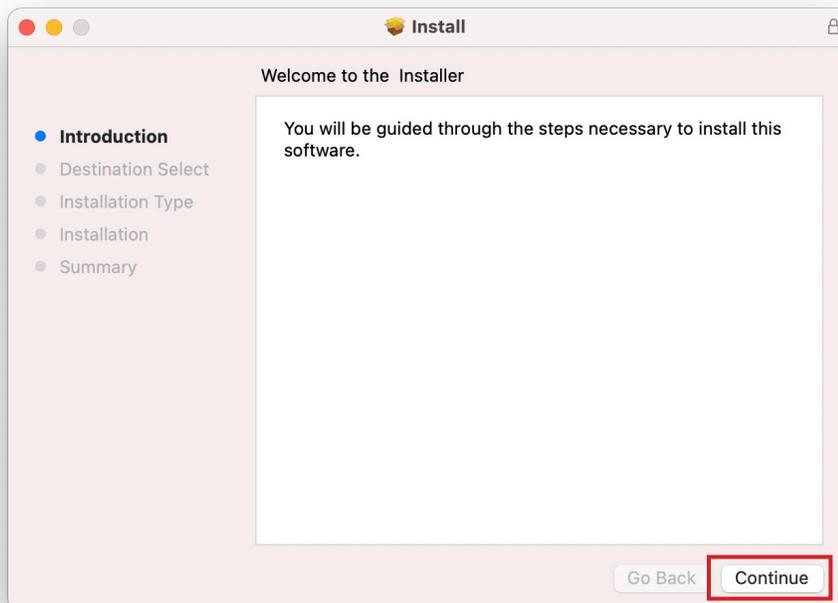
16. Open the Resources folder.



17. Double click the JamfConnectLaunchAgent.pkg file to install the launch agent. This is used to open Jamf Connect on startup.

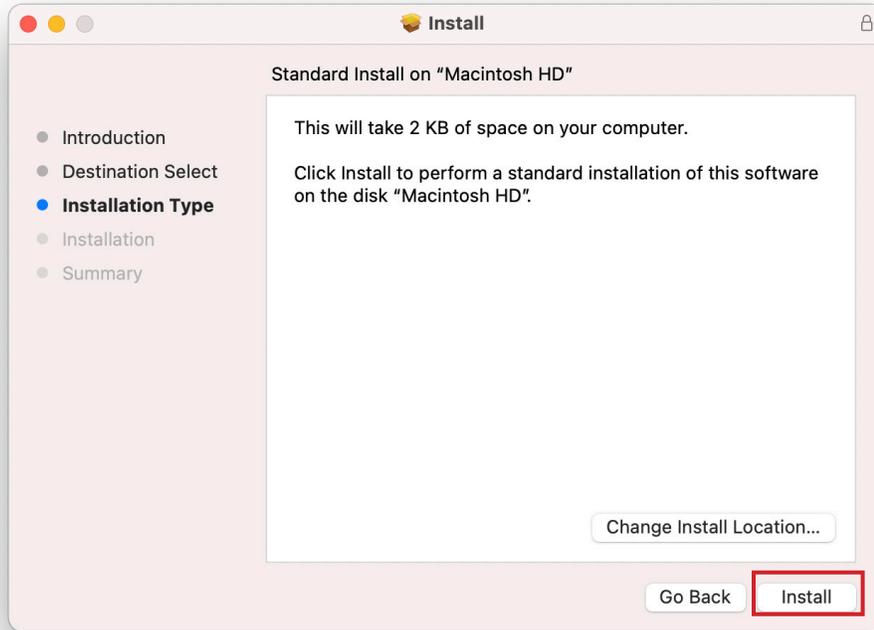


18. Click Continue.





19. Click Install.

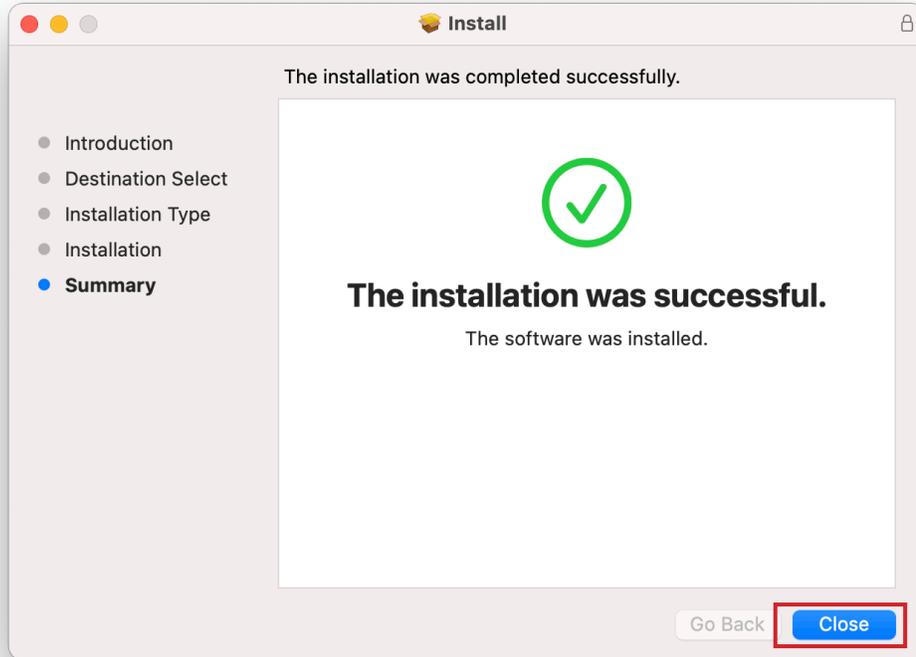


20. Enter your administrative credentials then click Install Software.





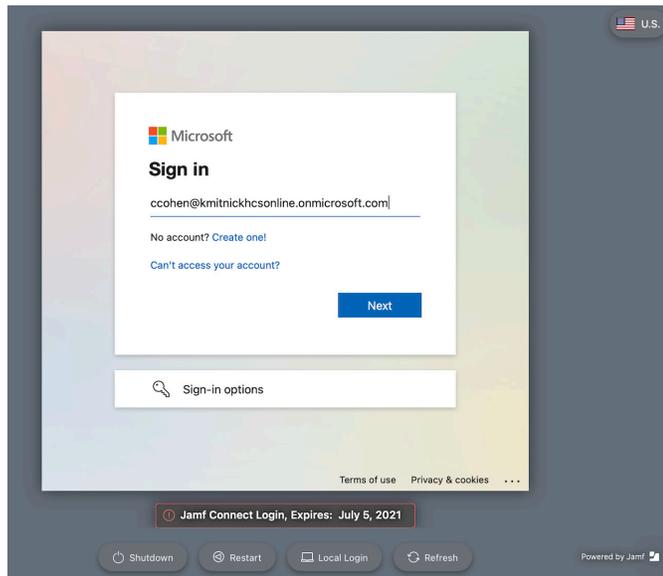
21. Click Close.



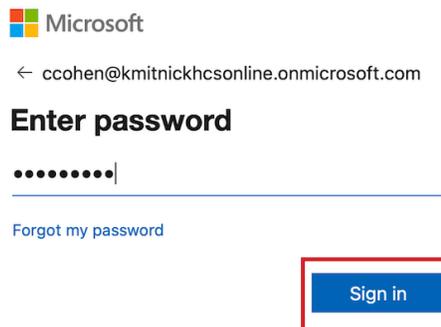


Section 7: Create an Account on the Mac Computer Using Jamf Connect.

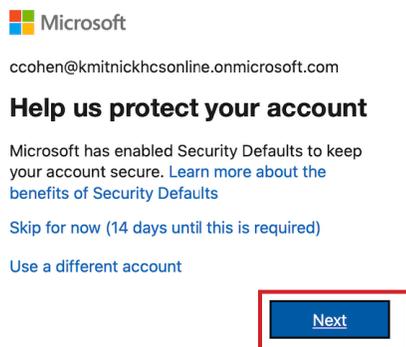
1. Logout of your Mac Computer. If all went well, you will see the Jamf Connect Login Window as shown below. Login with your Microsoft Azure credentials.



2. Enter your password then click Sign In.

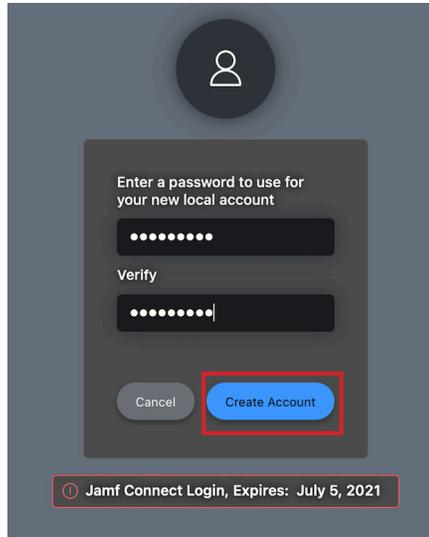


3. Select Skip for now, then click Next.



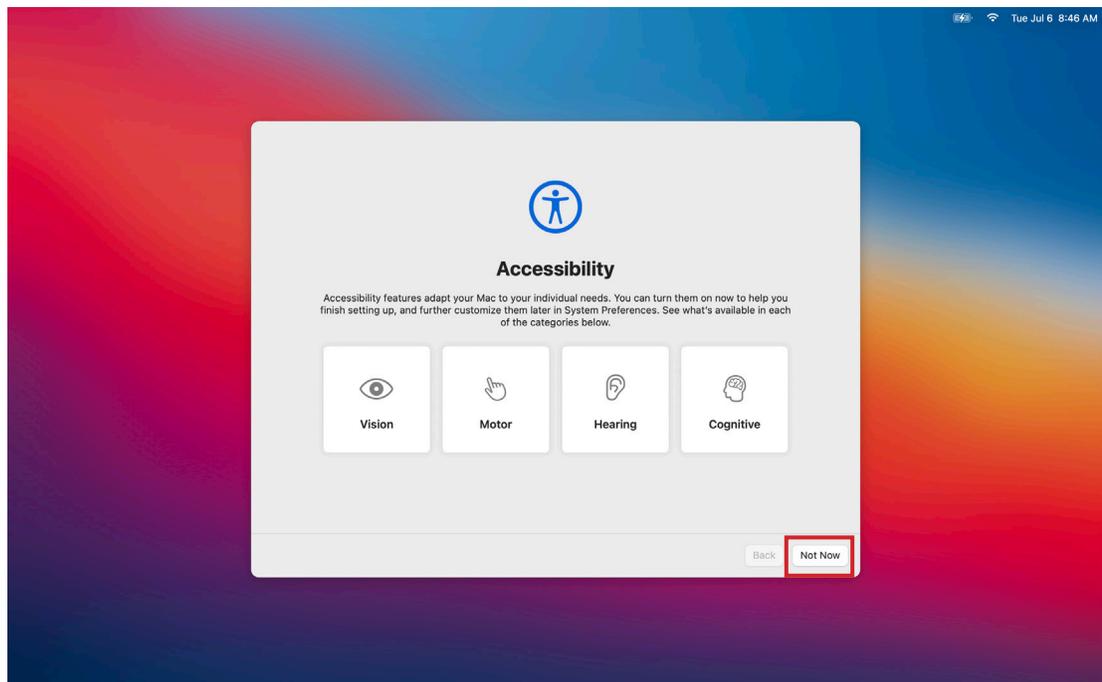


4. Enter the same password as your Microsoft Azure account, then click Create Account.



5. Click Not Now.

NOTE: Depending on how your Mac was configured, you may have more screens to configure before you are logged into your Mac Computer. This guide only shows the screen below.

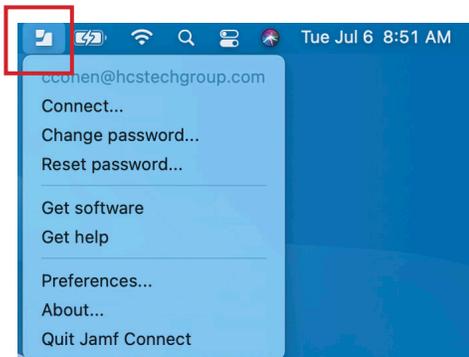




6. At the Jamf Connect message below, select Don't show this window again, then click Done.



7. You will notice a Jamf Connect Icon in the Menu Bar, click on it and you will see information about your account.



This completes this section.



Section 8: Configure Jamf Connect to Enable FileVault

Jamf Connect supports enabling FileVault on the following macOS versions:

- macOS Mojave
- macOS Catalina
- macOS Big Sur

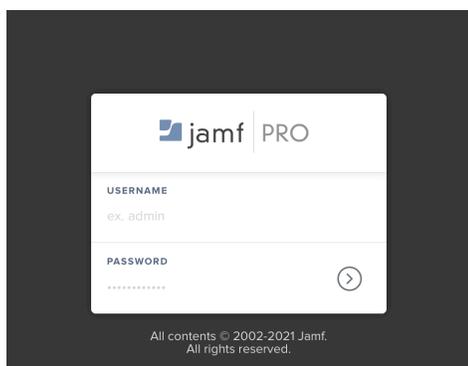
NOTE: macOS Mojave and Catalina require a LAPS user to enable FileVault. macOS Big Sur does not require a LAPS user and will use a secure token to enable FileVault. If you need more information on the LAPS user and requirements for macOS Mojave and Catalina, have a look here:

https://docs.jamf.com/jamf-connect/2.4.0/documentation/FileVault_Enablement_with_Jamf_Connect.html?hl=filevault

This guide will focus on macOS Big Sur. macOS Big Sur requires the following to enable FileVault using Jamf Connect:

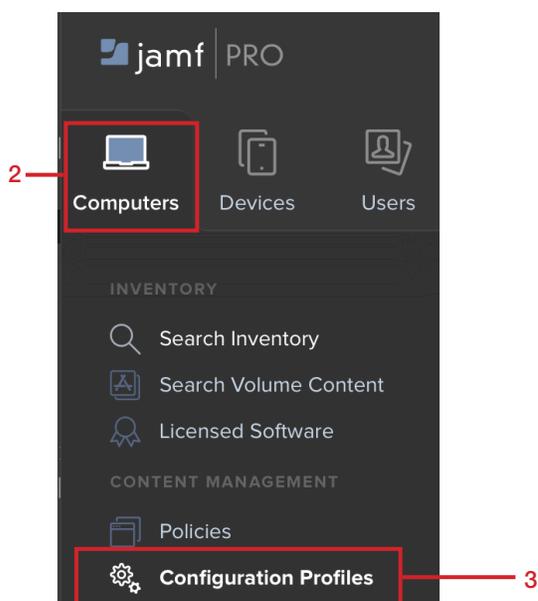
- A PPPC Profile to allow Jamf Connect to enable FileVault.
- A mobileconfig profile to escrow the FileVault key back to the Jamf Pro Server.
- A Jamf Connect Login Configuration Profile with FileVault set to enable for the first user.

1. If necessary, Log into your Jamf Pro server.



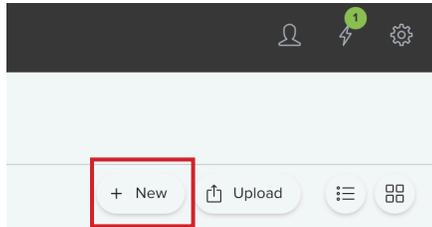
2. Click Computers.

3. Click Configuration Profiles.





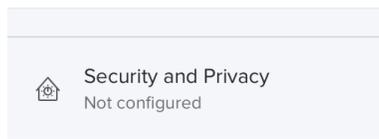
4. Click New.



5. Enter the following in the General section:

- A. Name: **Escrow FileVault Personal Recovery Key**
- B. Description: **This will escrow the FileVault Recovery Key in the Jamf Pro Server**
- C. Category: Select a category of your choosing, This guide will use the Security category.
- D. Level: Computer Level.
- E. Distribution Method: Install Automatically

6. Select the Security and Privacy payload.



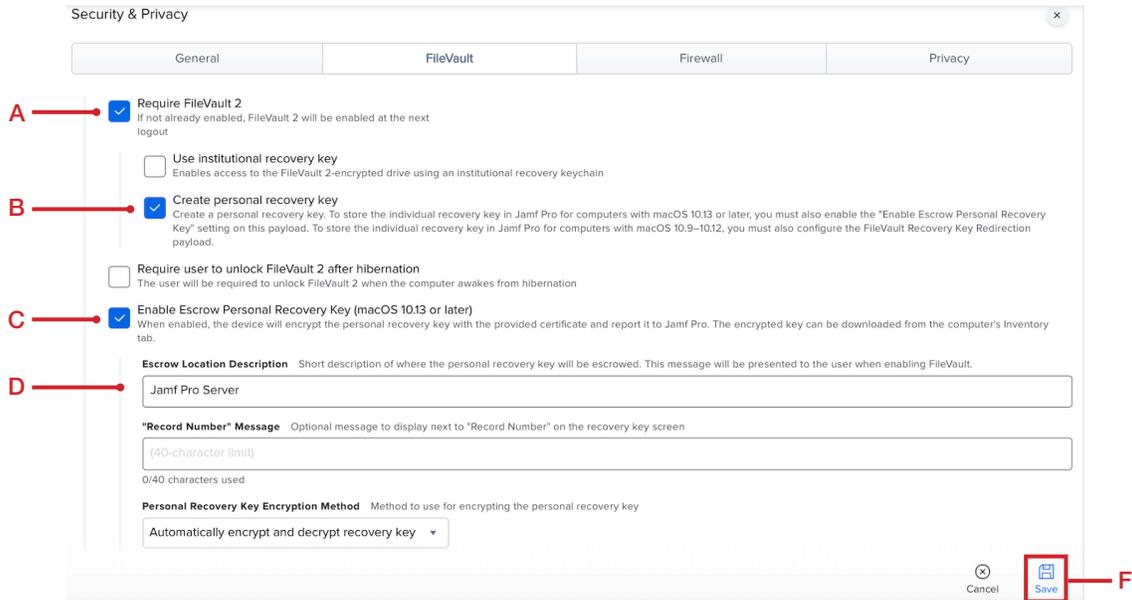
7. Select Configure.





8. Select the FileVault tab, then configure the following:

- A. Require FileVault 2
- B. Create personal recovery key
- C. Enable Escrow Personal Recovery Key (macOS 10.13 or later)
- D. Escrow Location Description: Jamf Pro Server.
- E. Scope the policy to your needs.
- F. Click Save.

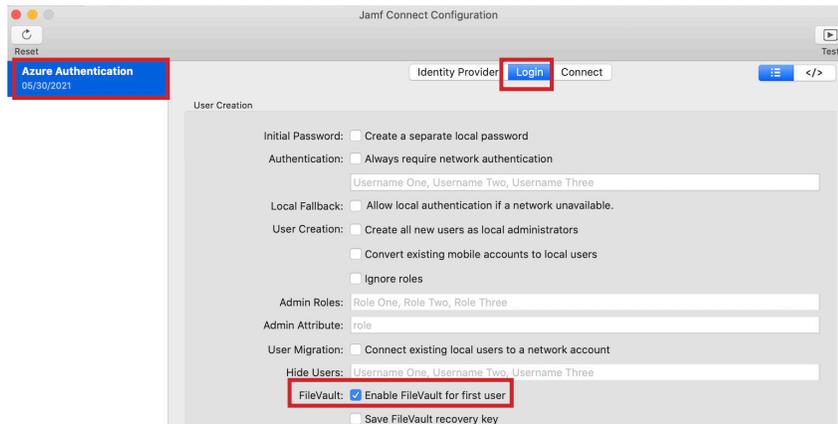


9. Go to the Applications folder and open the Jamf Connect Configuration App.



Jamf Connect Configuration

10. Select the existing Azure Authentication profile. Select the Login tab and enable the FileVault checkbox.



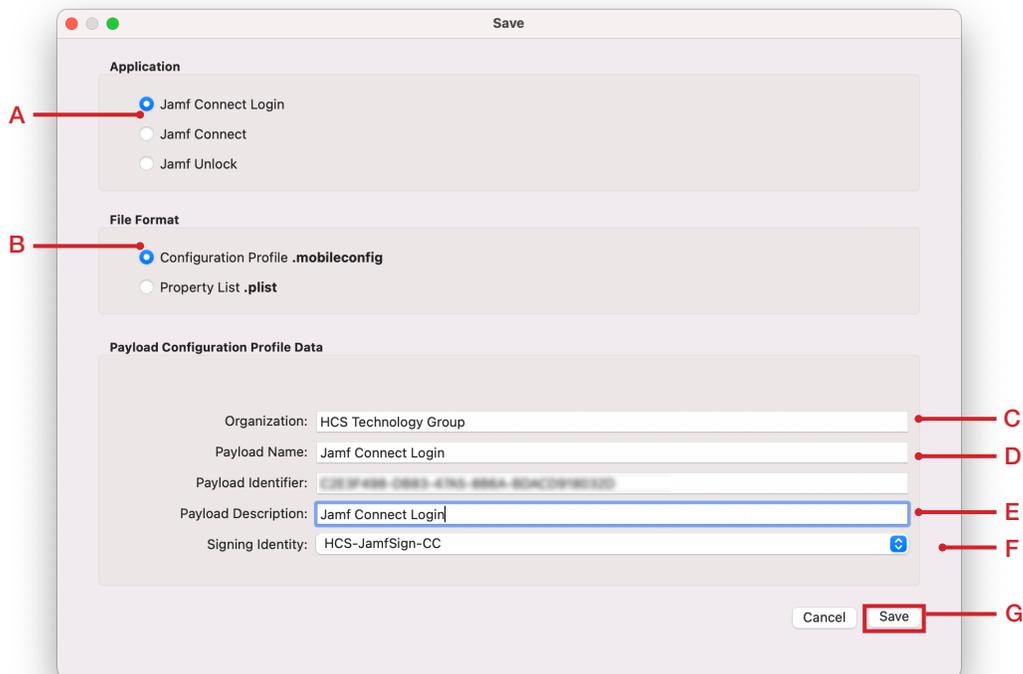


11. Select the File menu and choose Save.

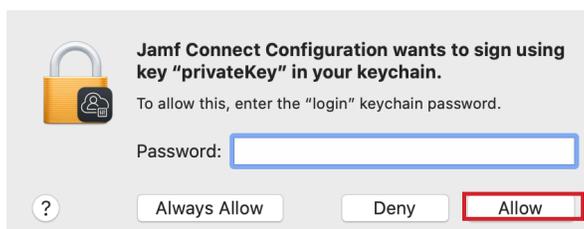


12. Enter the following:

- A. Applications: Jamf Connect Login
- B. File Format: Configuration Profile
- C. Organization: **HCS Technonology Group**
- D. Payload Name: **Jamf Connect Login**
- E. Payload Description: **Jamf Connect Login**
- F. Signing Identity: Select the signing certificate the we created in section 1.
- G. Click Save.

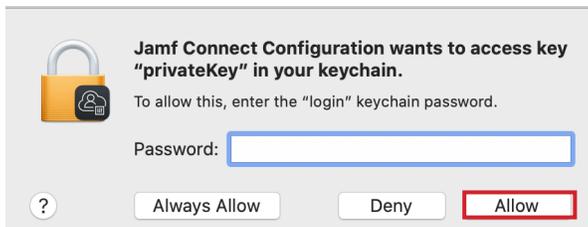


13. At the message below, enter your administrative credentials to sign the configuration profile. Click Allow. You will see this prompt twice.





14. At the message below, enter your administrative credentials to sign the configuration profile. Click Allow.

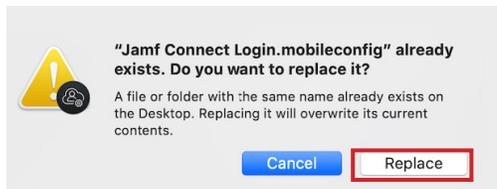


15. Enter the following:

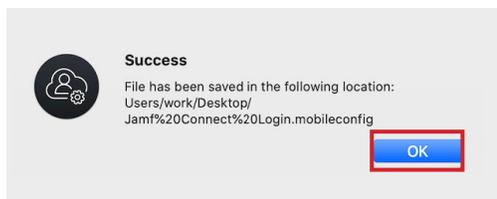
- A. Save As: **Jamf Connect Login**
- B. Where: Desktop
- C. Click Save



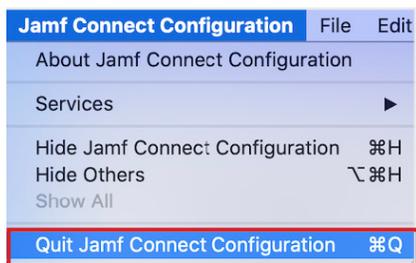
16. At the message below select Replace.



17. At the message below select OK.



18. Select the Jamf Connect Configuration menu then select Quit Jamf Connect Configuration.





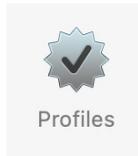
19. The updated Jamf Connect Login configuration profile should be on your desktop along with the Jamf Connect profile that we created in section 5 of this guide.



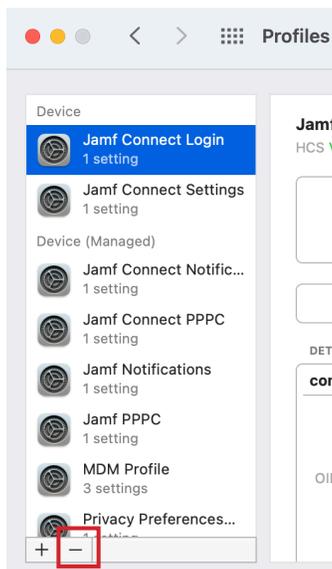
20. Click on the Apple icon in the upper left corner then select System Preferences.



21. Select the Profiles pane

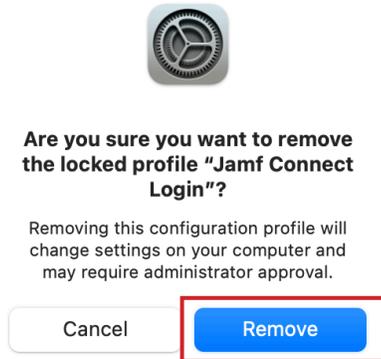


22. Click Remove (-) to delete the Jamf Connect Login configuration profile.





23. Click Remove at the message below.



24. Enter your administrative credentials then click OK.

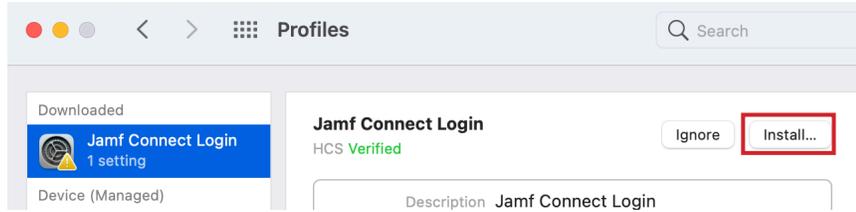


25. Double click the Jamf Connect Login.mobileconfig file to install it.

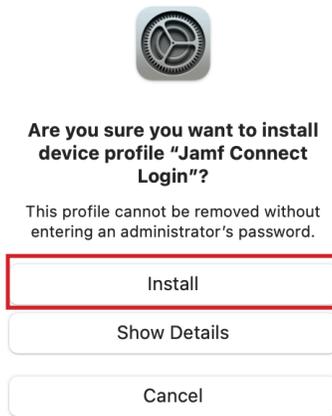




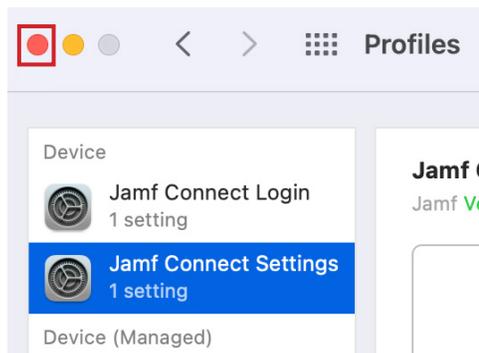
26. Click Install.



27. Click Install.



28. Quit System preferences.

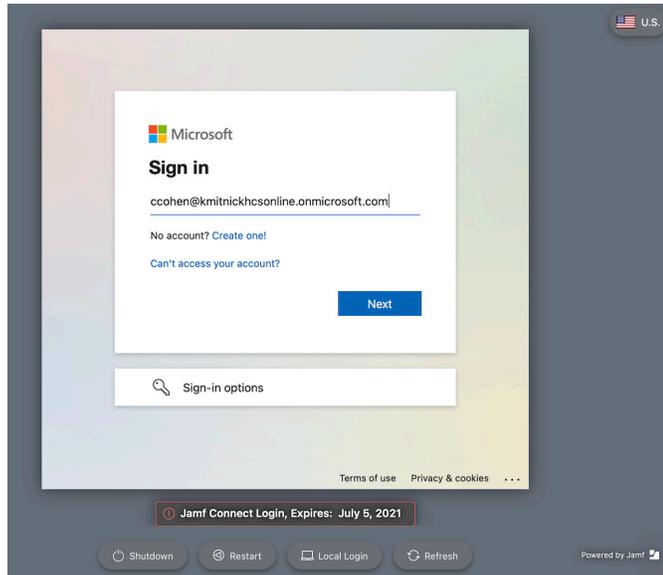


This completes this section.

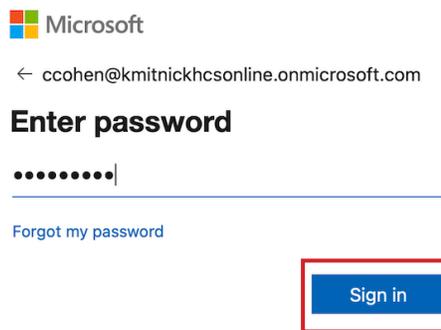


Section 9: Enable FileVault with Jamf Connect

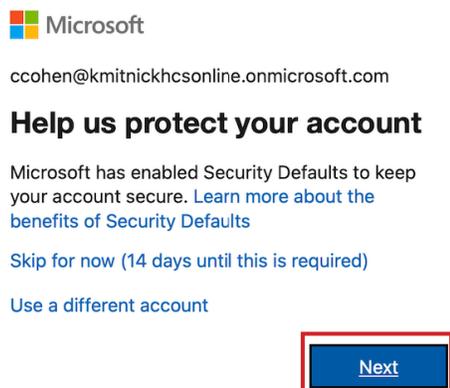
1. Enter your Microsoft Azure Credentials. Click Next.



2. Enter your password then click Sign In.

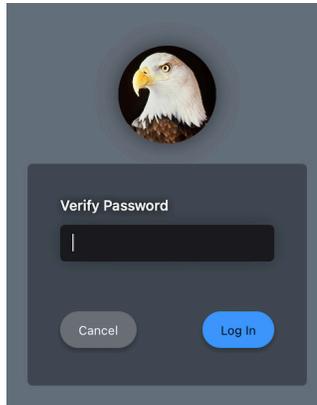


3. Select Skip for now, then click Next.

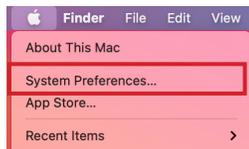




4. Enter your Microsoft Azure password. Click Log In.



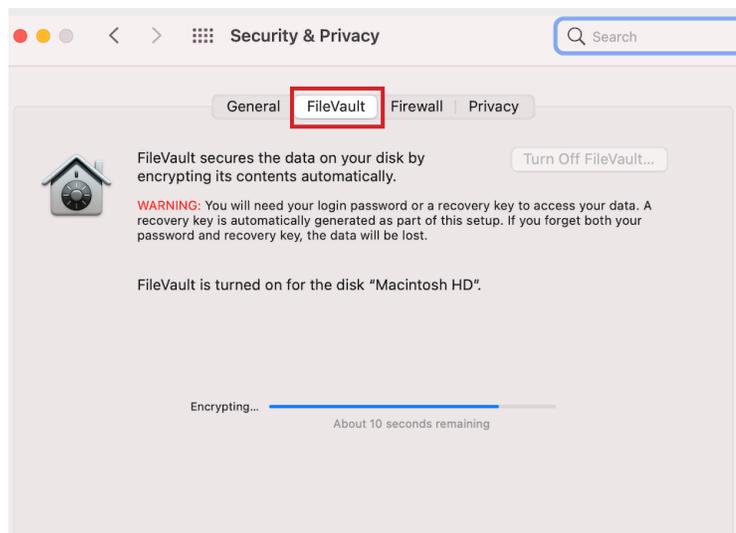
5. Click the Apple Icon, then select System Preferences.



6. Click the Security & Privacy pane.

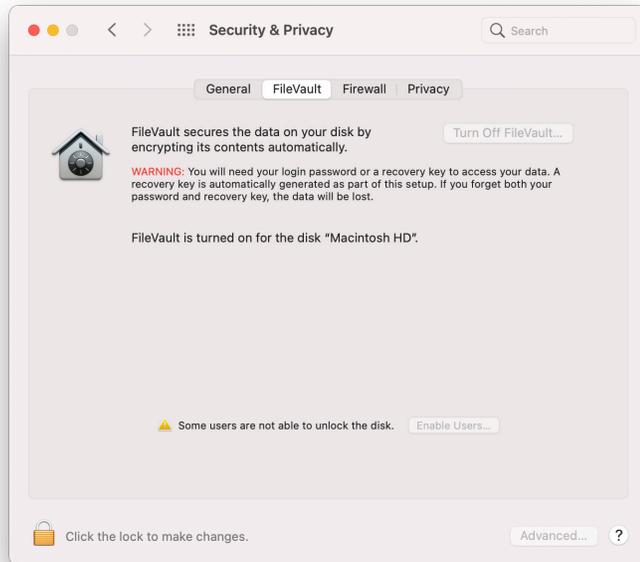


7. Click FileVault. The FileVault encryption process has started.





8. Once the FileVault encryption process is complete, quit System Preferences.

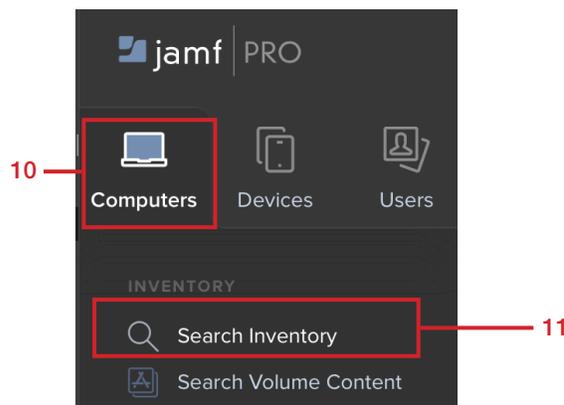


9. Let's check to make sure the FileVault Individual recovery key was escrowed on the Jamf Pro server. If necessary, log into your Jamf Pro server.



10. Click Computers.

11. Click Configurations Profiles.

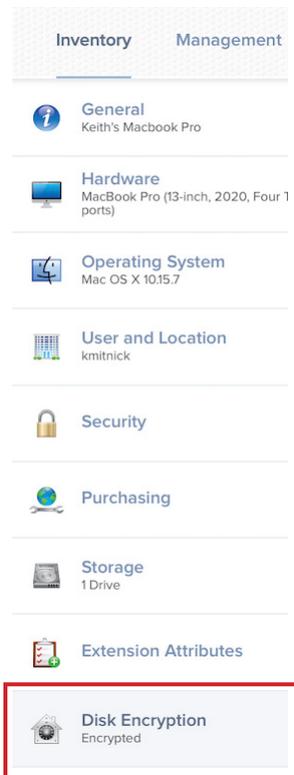




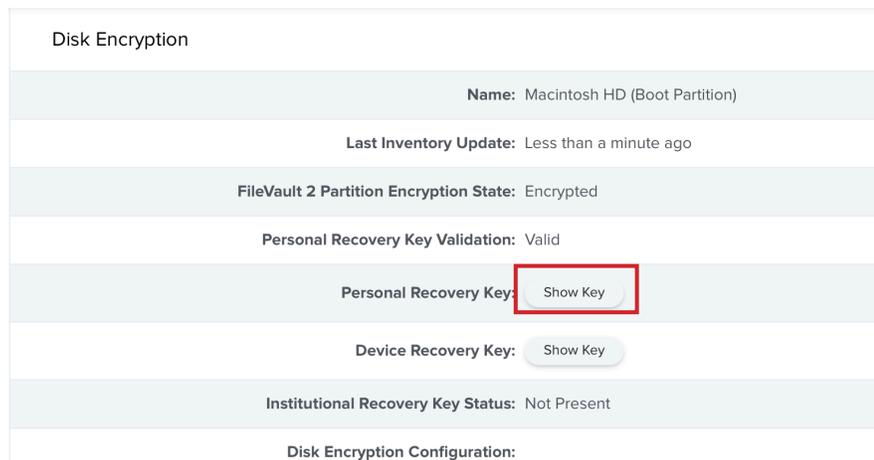
12. Enter the name of the computer that you just enabled FileVault on then click Search.



13. Open the computer record. In the Inventory section, Select Disk Encryption.



14. Next to Personal Recovery Key, click Show Key.





15. Confirm your individual FileVault key was successfully escrowed to the Jamf Pro server.

Disk Encryption

Name: Macintosh HD (Boot Partition)
Last Inventory Update: Less than a minute ago
FileVault 2 Partition Encryption State: Encrypted
Personal Recovery Key Validation: Valid
Personal Recovery Key: DEMZ [REDACTED]
Device Recovery Key: Show Key
Institutional Recovery Key Status: Not Present
Disk Encryption Configuration:

This completes this section.



Section 10: Create a package folder structure for Branding, Login Window, and Menu bar scripts.

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 Composer to set permissions and create a package to deploy to all computers.

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. You may download HCS' branding images at:

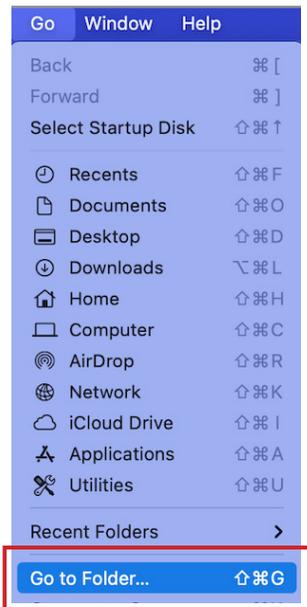
<https://hconline.com/images/banners/branding.zip>

The recommended size for branding icons:

- Menu bar icons: 16x16 pixels
- Login logo: 250 x 250 pixels
- Sign in Logo 512x512 pixels

NOTE: This guide will use Composer for packaging. You can get Composer from your Jamf Nation account. If you want to use other packaging software, feel free.

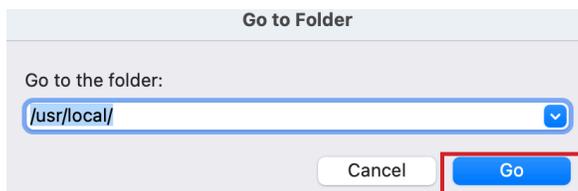
1. In the Finder, click the Go menu then select Go To Folder.



2. Enter the following path:

/usr/local/

Click Go.

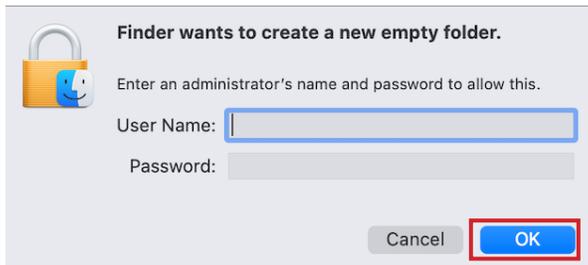




3. Click the File menu, then select New Folder.



4. Enter your administrative credentials the click OK.

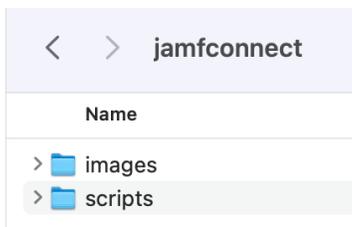


5. Name the folder jamfconnect then open the jamfconnect folder.



6. Follow steps 3 and 4 to create the following two folders inside the jamfconnect folder:

- images
- scripts

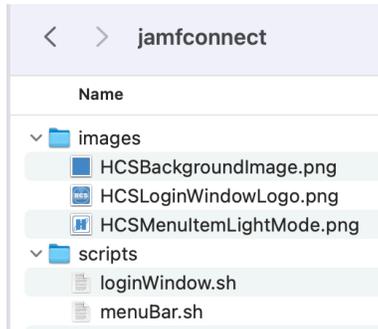




- 7. Drag your branding images from the Desktop to the Images folder. You may download HCS' branding images at:

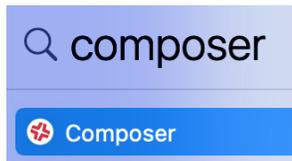
<https://hcsonline.com/images/banners/branding.zip>

NOTE: If you have Login window scripts or Menu bar scripts, drag them into the scripts folder now.

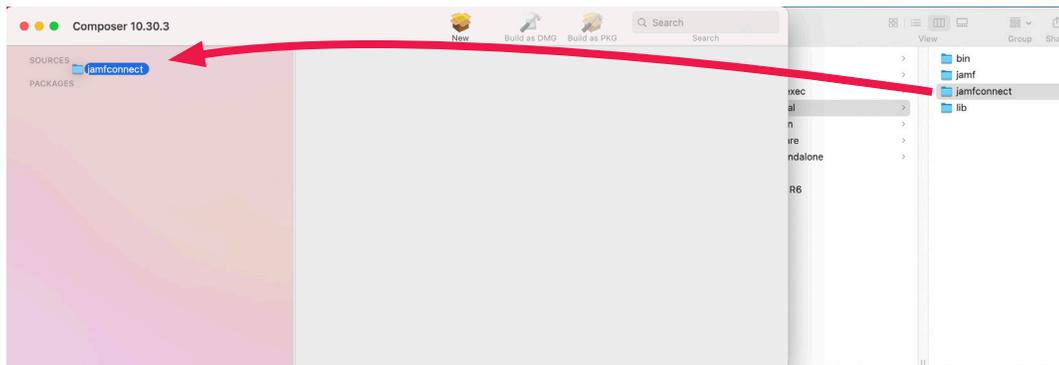


- 8. Perform a Spotlight search for Composer.

NOTE: This guide uses Composer for packaging. You can get Composer from your Jamf Nation account. If you want to use other packaging software, feel free.



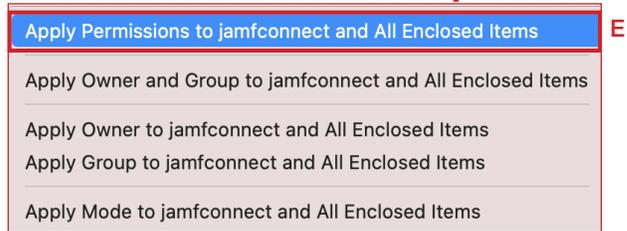
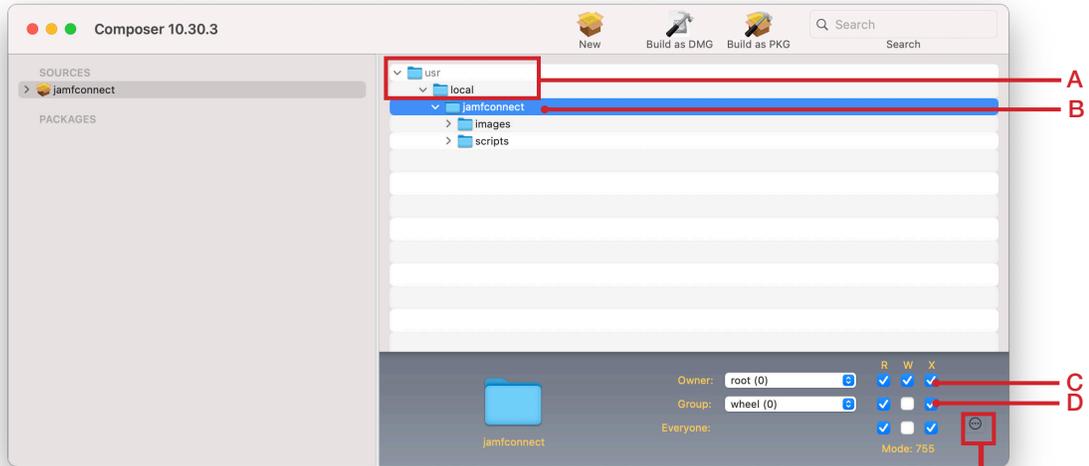
- 9. Drag the jamfconnect folder to the SOURCES section of Composer.





10. Perform the following steps:

- A. Expand the folders /usr/local/ to show jamfconnect
- B. Select the jamfconnect folder.
- C. Change the Owner to: root
- D. Change the Group to: wheel
- E. Confirm the permissions are set to 755 as shown in the screen shot below.
- F. Click the ellipse icon and select Apply Permissions to jamfconnect and All Enclosed items.

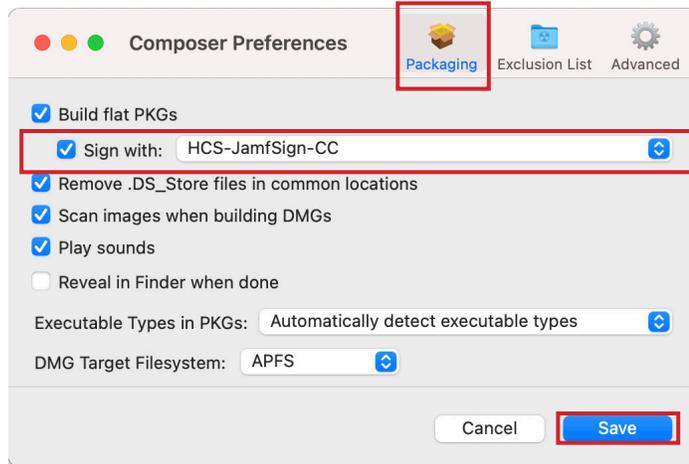


11. Click the Composer menu then select Preferences.

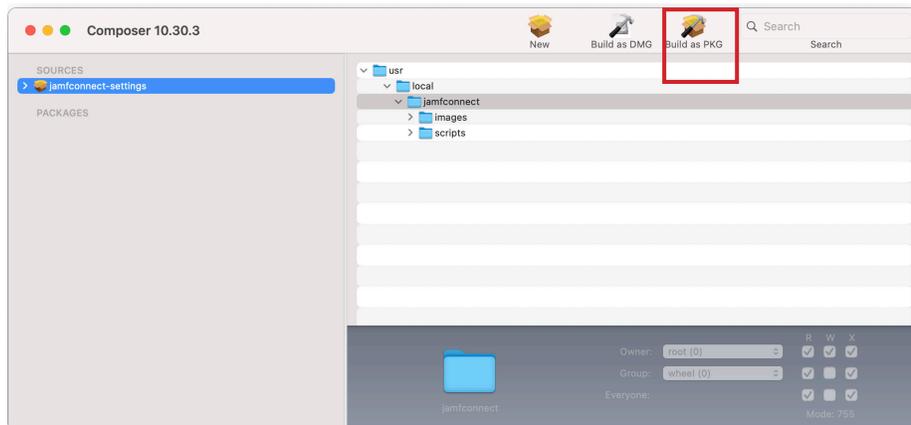




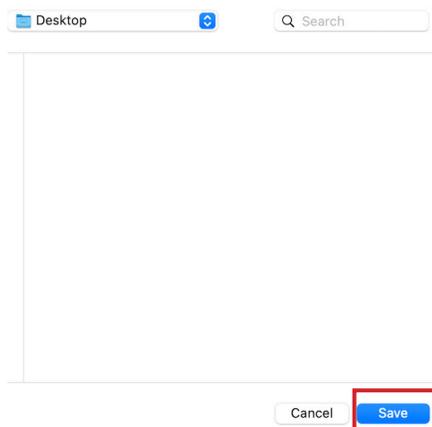
12. Select Packaging, then check the Sign with checkbox and select your signing certificate. Click Save.
NOTE: We need to sign this package if we want to use it in a Prestage enrollment.



13. Rename the package to jamfconnect-settings, then select Build as PKG.

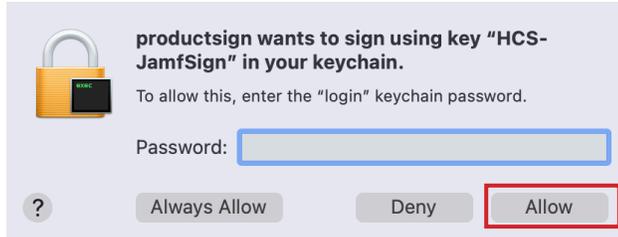


14. Select Desktop, then click Save

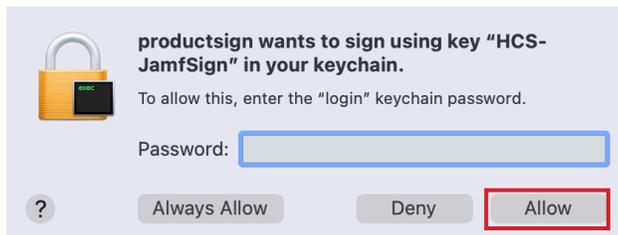




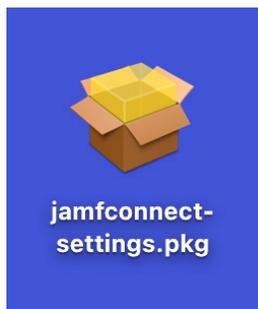
15. Enter your administrative password to sign the package then click Allow. You will see this message twice.



16. Enter your administrative password to sign the package then click Allow.



17. Confirm the package was created on our Desktop.



This completes this section.



Section 11: Add Branding and Scripts to the Jamf Connect Configuration Profiles

This section requires your Mac Computer to be enrolled into Jamf Pro. If your Mac Computer is not enrolled in Jamf Pro, some steps in this guide will not work,

NOTE: Jamf Connect version 2.4 was released when this section was written. Some screen shots will include the new Jamf Unlock radio button when saving a configuration profile.

In this section we will add the paths to the images and scripts we created in section 10 of this guide and confirm the branding and scripts work.

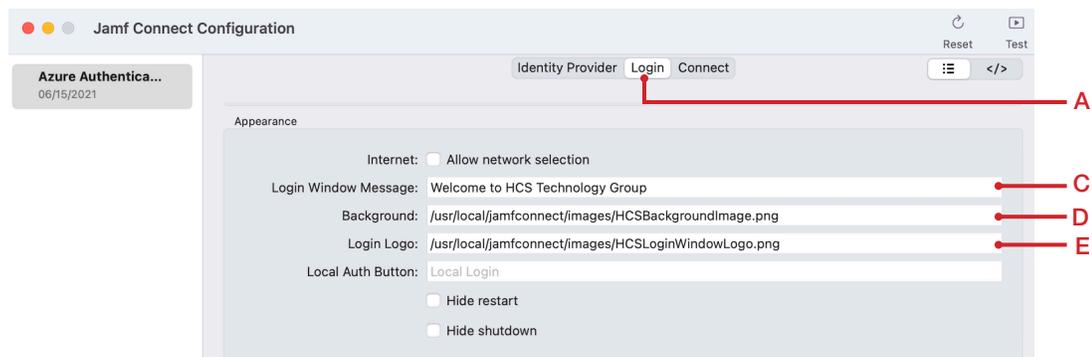
1. Open the Jamf Connect Configuration app



Jamf Connect Configuration

2. Select the Azure Authentication configuration then configure the following:
 - A. Select the Login tab.
 - B. Go to the Appearance section.
 - C. Login Window message: this guide will use “Welcome to HCS Technology Group”
 - D. Background: Add the path to your background image. This guide will use:
/usr/local/jamfconnect/images/HCSBackgroundImage.png
 - E. Login Logo: Add the path to your login image. This guide will use:
/usr/local/jamfconnect/images/HCSLoginWindowLogo.png
 - F. Scroll down to the Script section.

NOTE: The Background and Login Logo images will display custom branded background image and a custom logo at the login window.





- 3. Script Path: Add the path to your login window script. This guide will use: /usr/local/jamfconnect/scripts/loginWindow.sh

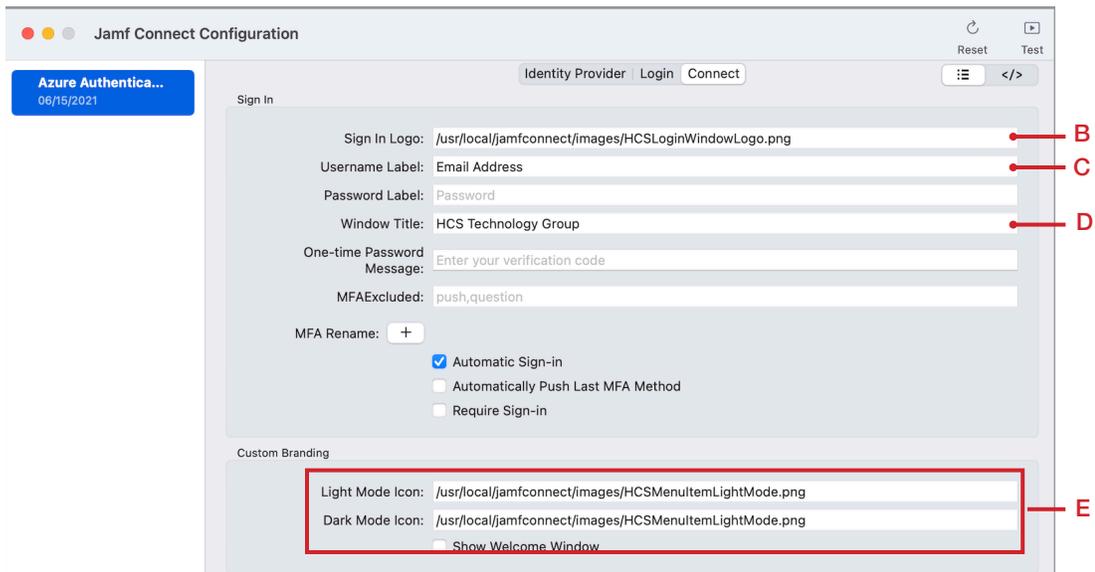
NOTE: The loginWindow.sh script will run when the user logs in. This sample script will open Safari and go to the HCS webpage on login.



- 4. Select the Connect tab then configure the following

- A. Go to the Sign In section.
- B. Sign in Logo: Add the path to your icon. This guide will use: /usr/local/jamfconnect/images/HCSLoginWindowLogo.png
- C. Username Label: Email Address (this will change Username to Email Address at the Jamf Connect Login Window)
- D. Window Title: this guide will use "HCS Technology Group"
- E. Fill out the following in the Custom Branding section.
 - Light Mode Icon: Add the path to your icon. This guide will use: /usr/local/jamfconnect/images/HCSMenuItemLightMode.png
 - Dark Mode Icon: Add the path to your icon. This guide will use: /usr/local/jamfconnect/images/HCSMenuItemLightMode.png

NOTE: The Light and Dark mode images will be displayed in the menubar. It's a customized Jamf connect menu bar logo.





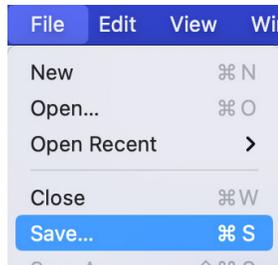
5. On Auth Failure: Enter the path to your script. This guide will use:

`/usr/local/jamfconnect/scripts/menuBar.sh`

NOTE: The menuBar.sh script will present a Jamf Helper message to the user if there was a failure to authenticate to Azure.



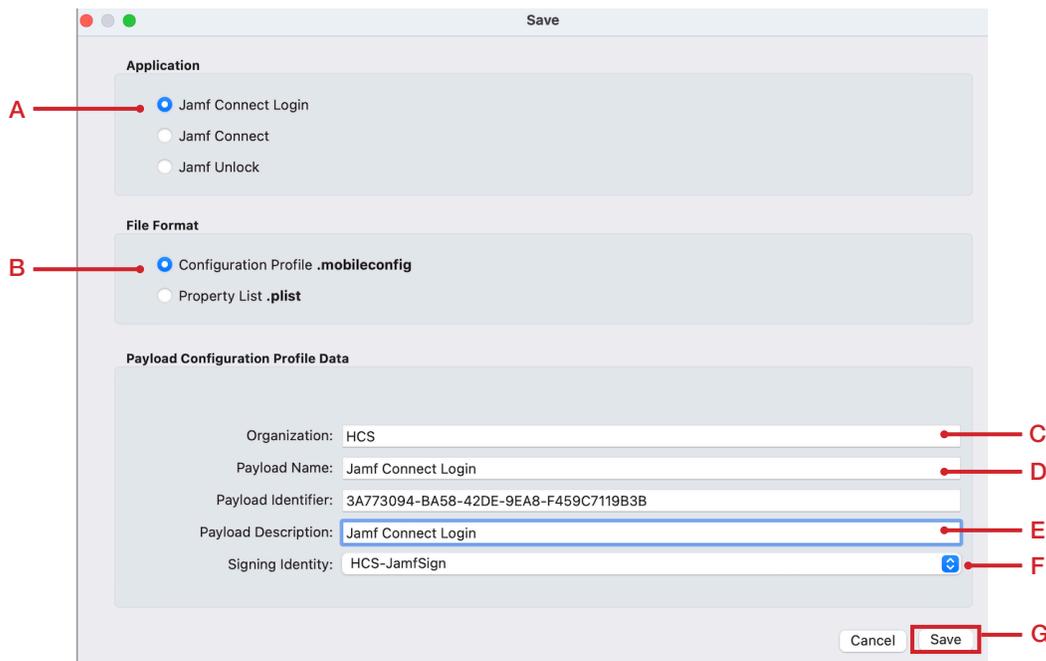
6. Click the File menu then select Save.



7. Configure the following:

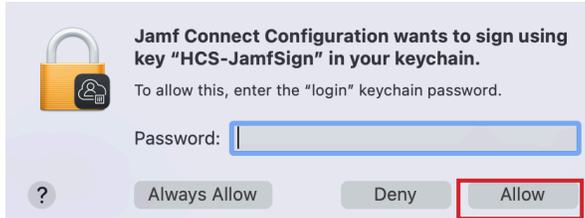
- A. Application: Select Jamf Connect Login
- B. File Format: Select Configuration Profile
- C. Organization: This guide will use HCS
- D. Payload Name: Jamf Connect Login
- E. Payload Description: Jamf Connect Login
- F. Signing Identity: Select your signing certificate
- G. Click Save.

NOTE: Notice the Jamf Unlock radio button in the Application section, this was added in Jamf Connect Configuration 2.4.

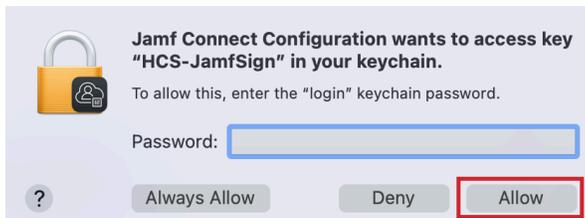




8. Enter your administrative password. Click Allow. You will see this prompt twice.

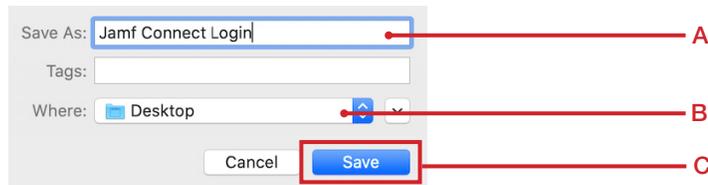


9. Enter your administrative password. Click Allow.



10. Enter the following:

- A. Save As: Jamf Connect Login
- B. Where: Desktop
- C. Click Save



11. Select Replace and the message below.



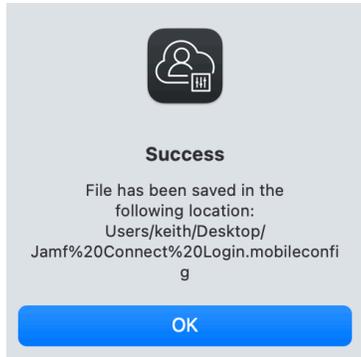
"Jamf Connect Login.mobileconfig" already exists. Do you want to replace it?

A file or folder with the same name already exists on the Desktop. Replacing it will overwrite its current contents.



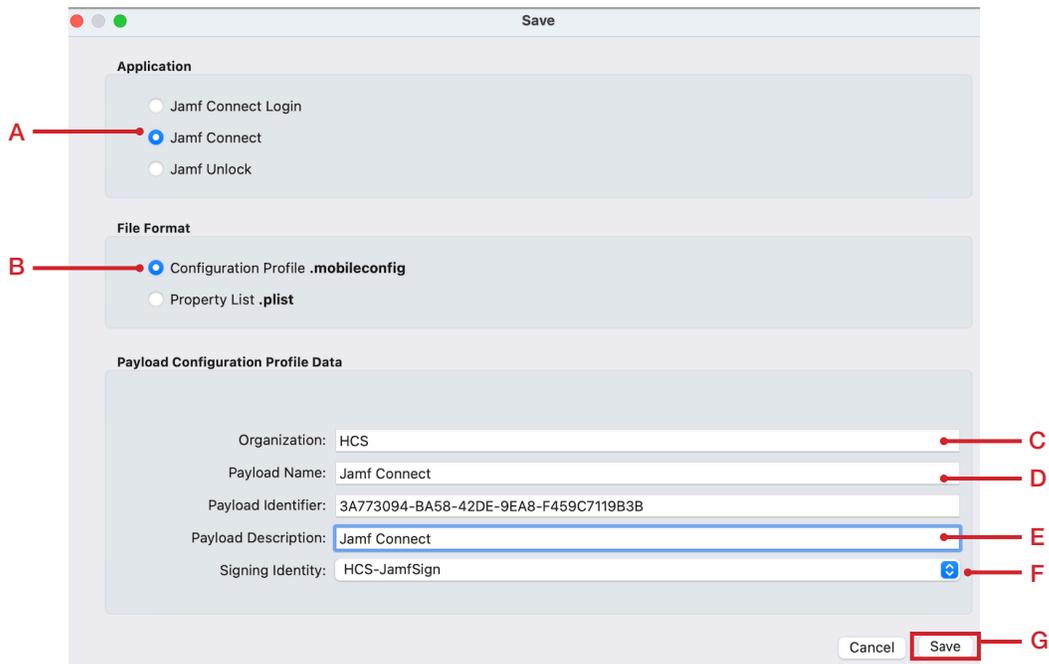


12. Select OK at the message below.



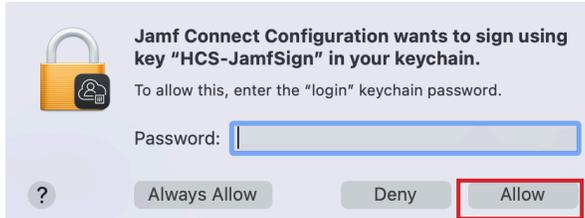
13. Configure the following:

- A. Application: Select Jamf Connect
- B. File Format: Select Configuration Profile
- C. Organization: This guide will use HCS
- D. Payload Name: Jamf Connect
- E. Payload Description: Jamf Connect
- F. Signing Identity: Select your signing certificate
- G. Click Save.

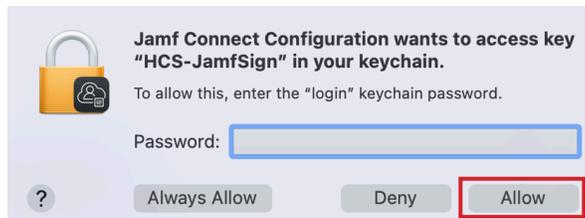




14. Enter your administrative password. Click Allow. You will see this prompt twice.



15. Enter your administrative password. Click Allow.



10. Enter the following:

- A. Save As: Jamf Connect
- B. Where: Desktop
- C. Click Save



17. Select Replace and the message below.



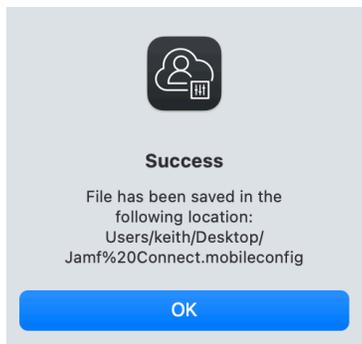
**"Jamf Connect.mobileconfig"
already exists. Do you want to
replace it?**

A file or folder with the same name
already exists on the Desktop. Replacing
it will overwrite its current contents.

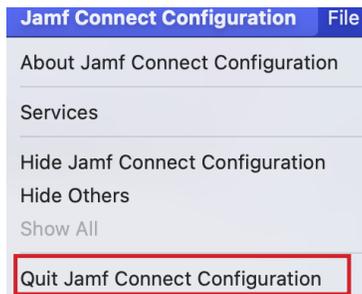




18. Select OK at the message below.



19. Go to the Jamf Connect Configuration menu and select Quit Jamf Connect Configuration.



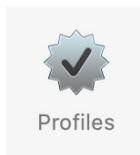
20. You should have two configuration profiles on your Desktop.



21. Click on the Apple icon in the upper left corner then select System Preferences.

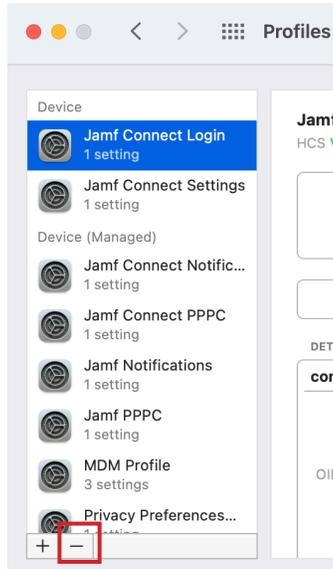


22. Select the Profiles pane





23. Click Remove (-) to delete the Jamf Connect Login configuration profile.



24. Click Remove at the message below.

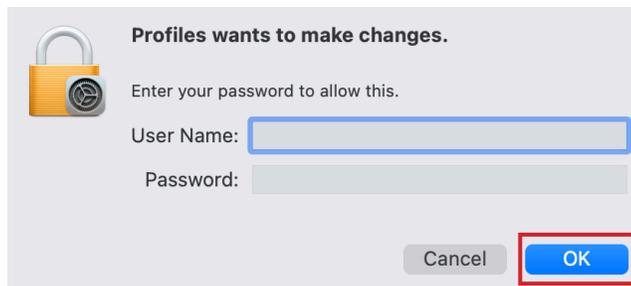


Are you sure you want to remove the locked profile "Jamf Connect Login"?

Removing this configuration profile will change settings on your computer and may require administrator approval.

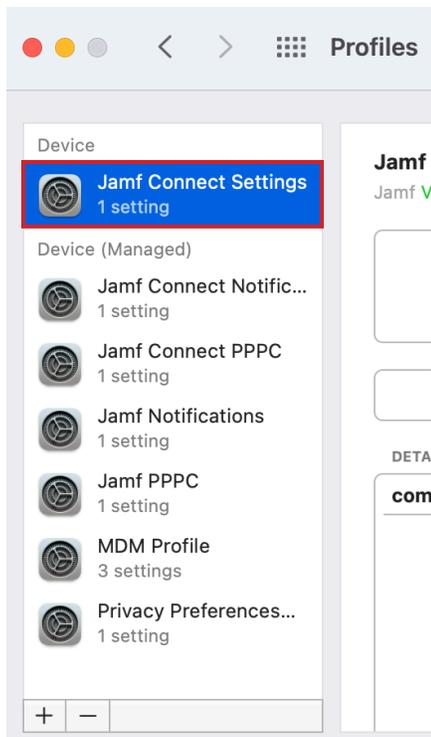


25. Enter your administrative credentials then click OK.





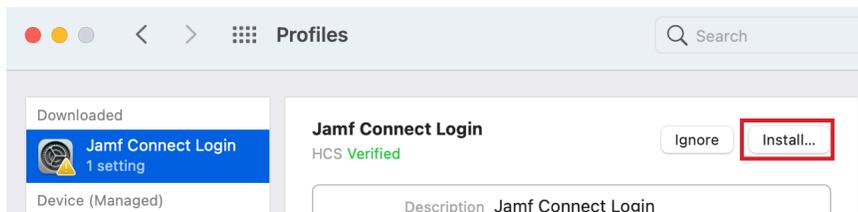
26. Follow steps 23 -25 to remove the Jamf Connect Settings configuration profile.



27. Double-click the Jamf Connect Login.mobileconfig file to install it.



28. Click Install.

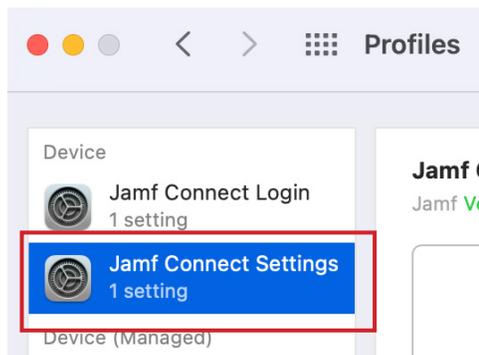




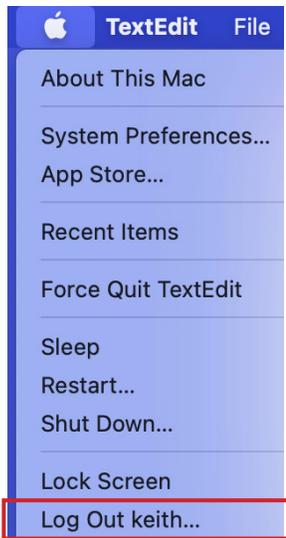
29. Click Install.



30. Follow steps 27 - 29 to install the Jamf Connect Settings configuration profile. Once both configuration profiles are installed, quit System preferences.

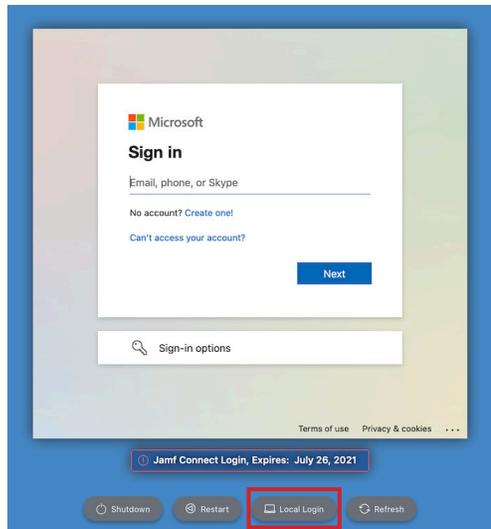


31. Click on the Apple icon in the upper left corner then select Logout.

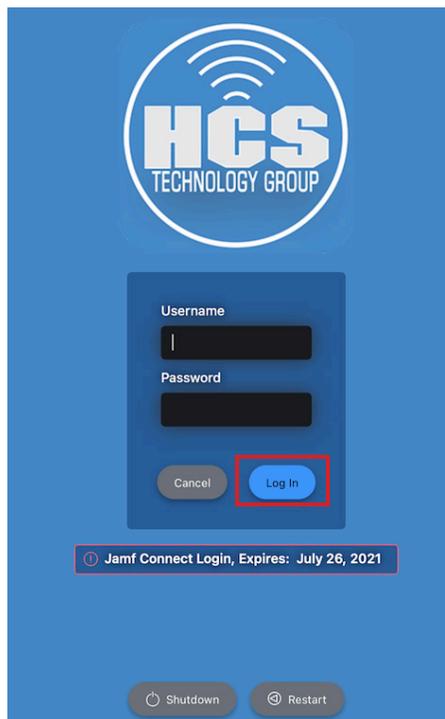




32. Notice the Login Window background is now blue. This is using our custom background image. Select the Local Login button.

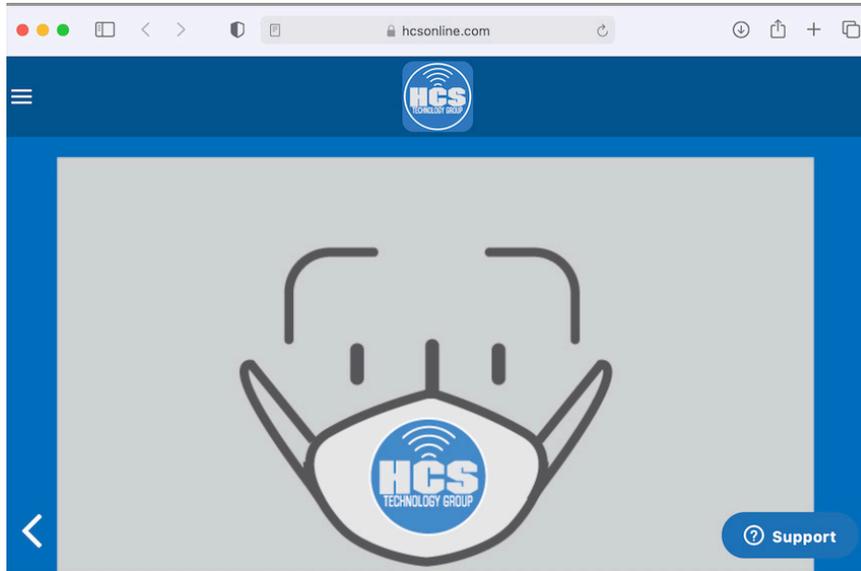


33. Notice we now have a custom login window logo. Enter your local user credentials then select Log In.





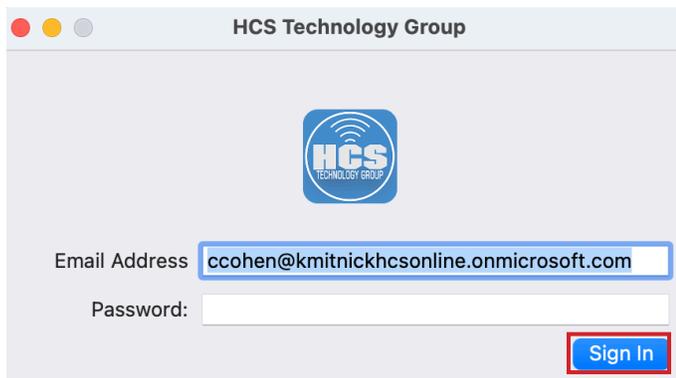
34. Upon login you will notice Safari will open and go to <https://www.hcsonline.com>. Our loginWindow.sh script was programmed to do this on login.



35. In the menu bar, notice the customized Jamf Connect icon.

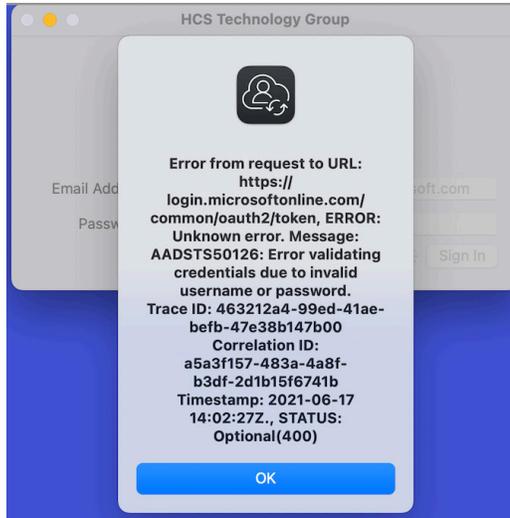


36. In the Jamf Connect window, enter in a email address and password then click Sign In. We are doing this to confirm our menuBar.sh script runs on authentication failure.
NOTE: The Email Address was a custom setting. It used to say "User name". Also notice the customized logo.





37. You will see the error message below. DO NOT click OK. The menuBar.sh script is programmed to show a failure message in the next step.



38. This is our menuBar.sh script letting us know there was an authentication failure. Click OK and it will close both alert messages. All of our branding and scripts are working. This completes the section.

NOTE: This alert is running the menuBar.sh script. That script will run on authentication failure. The script uses Jamf Helper which is why your Mac computer needs to be enrolled into Jamf Pro.





Section 12: Deploy Jamf Connect from Jamf Pro

JAMF Pro version 10.30 introduced a new way to deploy Jamf Connect directly from JAMF Pro. You no longer need to add Jamf Connect to a prestage in JAMF Pro to deploy it. If you require the Jamf Connect Launch Agent, that still needs to be deployed from a prestage or via a policy in JAMF Pro

This section requires the following:

- A. JAMF Pro server version 10.30 or later.
- B. Jamf Connect License mobile configuration profile.
- C. Jamf Connect Login and Jamf Connect settings mobile configuration profiles.
- D. Jamf Connect Launch Agent which is located in the Resources folder of the Jamf Connect 2.4 installer DMG.
- E. A prestage enrollment configured on your JAMF Pro server that skips account creation at setup.

1. Open the Jamf Connect 2.4 DMG file.



2. Open the Resources folder.



3. Drag the JamfConnectLaunchAgent.pkg to the Desktop.





4. You should have the following files on your Desktop

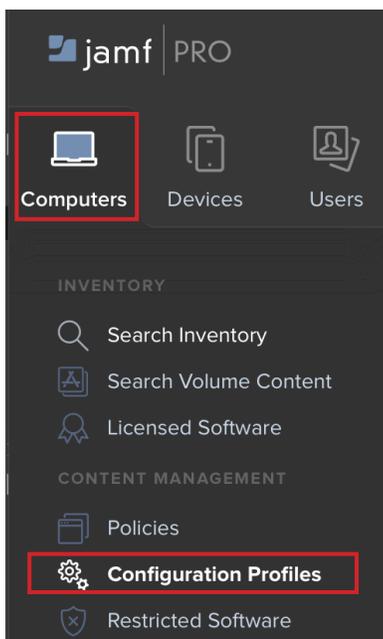
- Jamf Connect License.mobileconfig
- Jamf Connect Settings.mobileconfig
- Jamf Connect Login.mobileconfig
- JamfConnectLaunchAgent.pkg



5. If necessary, Log into your Jamf Pro server.

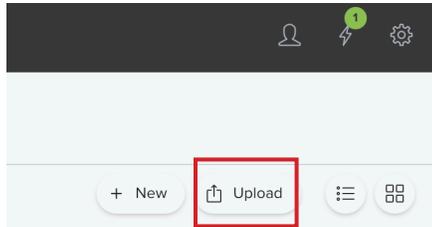


6. Click on Computers, then click Configuration Profiles.



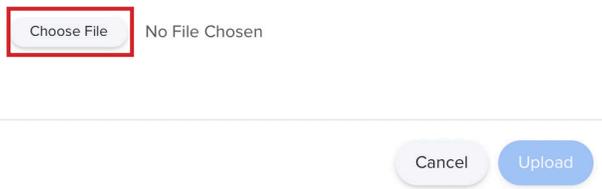


7. Click Upload.

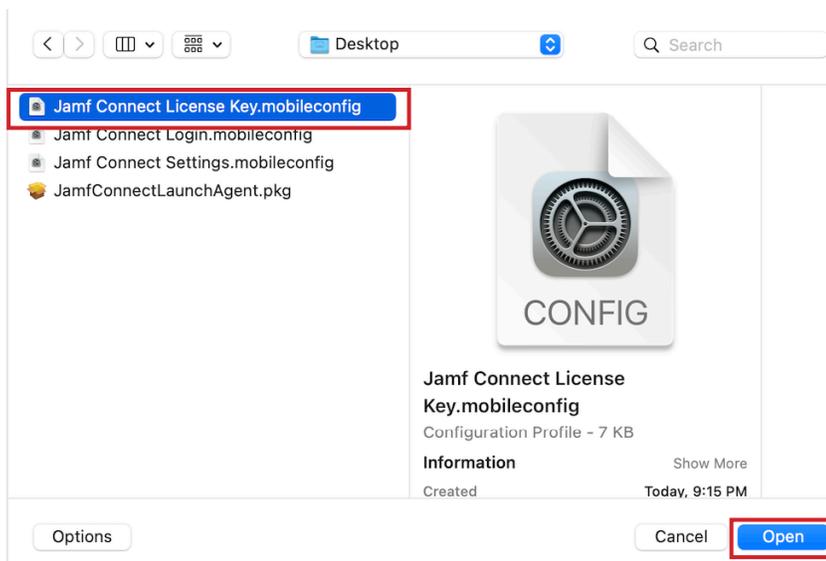


8. Click Choose File.

Upload OS X Configuration Profile



9. Select your Jamf Connect License Key.mobileconfig file, then click Open.





10. Click Upload.

Upload OS X Configuration Profile

Choose File Jamf Connect License Key.mobileconfig

Cancel Upload

11. Select a category then click Scope.

← New macOS Configuration Profile Signed

Options Scope

General

Application & Custom Settings
Payloads configured: 2

SIGNED PROFILE
This profile is read-only because it is signed. Remove Signature

General

Name Display name of the profile
Jamf Connect License Key

Description Brief explanation of the content or purpose of the profile

Category Category to add the profile to
Security

Level Level at which to apply the profile
Computer Level

Cancel Save

12. Scope to your needs. This guide will scope to All Computers. Click Save.

← New macOS Configuration Profile Signed

Options Scope

Targets Limitations Exclusions

Target Computers
Computers to assign the profile to
All Computers

Target Users
Users to distribute the profile to
Specific Users

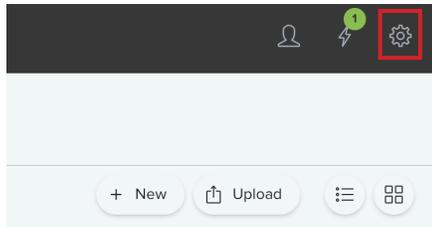
Selected Deployment Targets + Add

TARGET	TYPE
No Targets	

Cancel Save



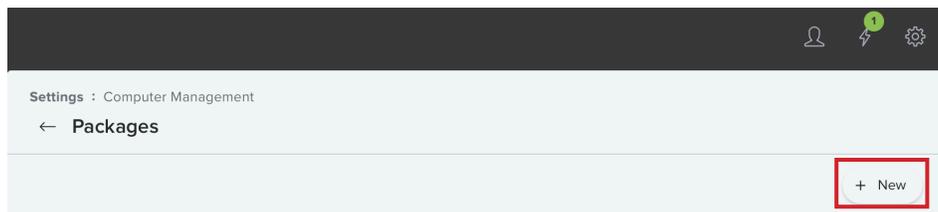
13. Click Settings (Looks like a gear) in the upper-right corner.



14. Click Computer Management then click Packages.



15. Click New.





- 16. Select a Category.
- 17. Click Choose File.

← **New Package**

General Options Limitations

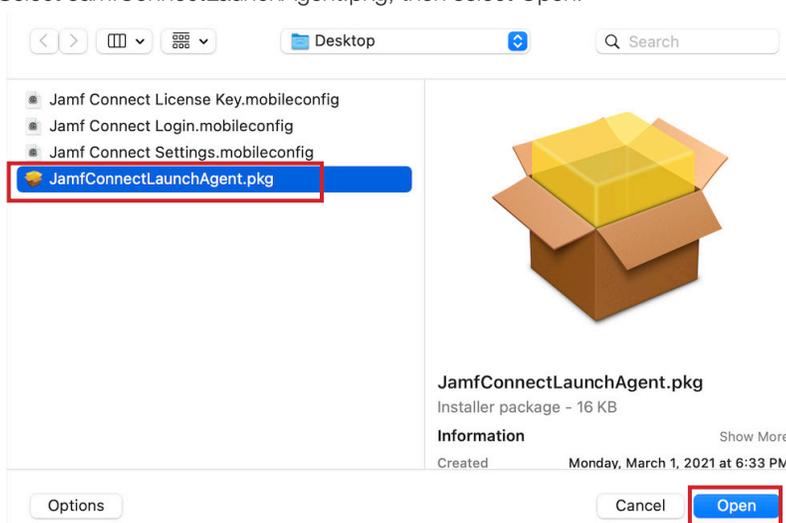
Display Name Display name for the package
[Required]

Category Category to add the package to
Security

Filename Filename of the package on the distribution point
Choose File

16 →
17 →

- 18. Select JamfConnectLaunchAgent.pkg, then select Open.



- 19. Click Save.

Settings : Computer Management > Packages

← **New Package**

General Options Limitations

Display Name Display name for the package
JamfConnectLaunchAgent.pkg

Category Category to add the package to
Security

Filename Filename of the package on the distribution point (e.g. "MyPackage.pkg")
Choose File JamfConnectLaunchAgent.pkg

Manifest File
Upload Manifest File

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

Cancel **Save**

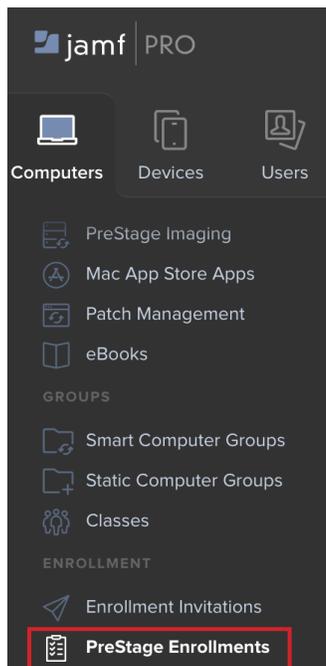


20. The upload has completed. Click Back (←).

The screenshot shows the Jamf Connect interface for a package named "JamfConnectLaunchAgent.pkg". A red box highlights the back arrow icon in the top left corner. Below the package name, there is a yellow warning banner that says "Availability pending" with a "Refresh" button. The page has three tabs: "General", "Options", and "Limitations", with "General" selected. The "General" tab contains the following fields: "Display Name" (JamfConnectLaunchAgent.pkg), "Category" (Security), and "Filename" (JamfConnectLaunchAgent.pkg). At the bottom right, there are three icons: "History", "Delete", and "Edit".

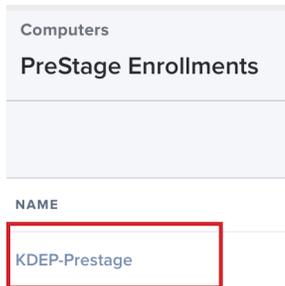
21. Click Computers then click PreStage Enrollments.

NOTE: This guide assumes you already have a pre stage enrollment configured to skip account creation during setup assistant and a test Mac Computer scoped to the prestage.

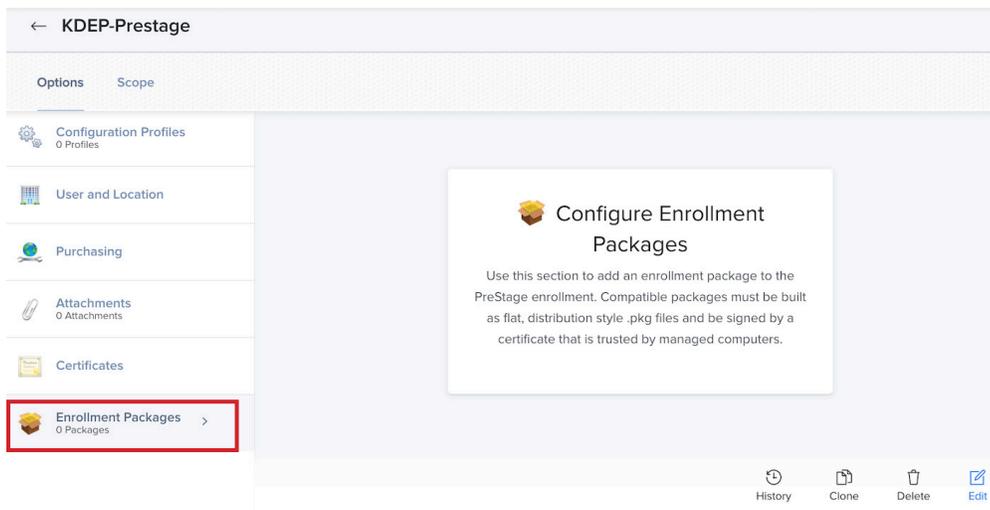




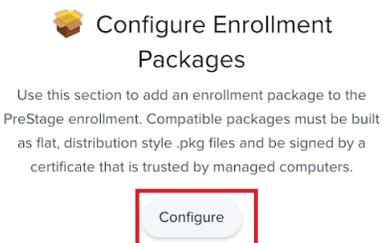
22. Open your prestage enrollment.



23. Click Enrollment Packages then click Edit.

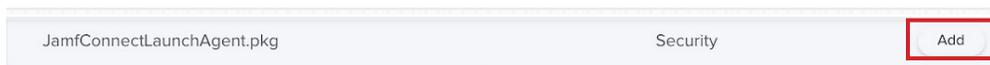


24. Click Configure.



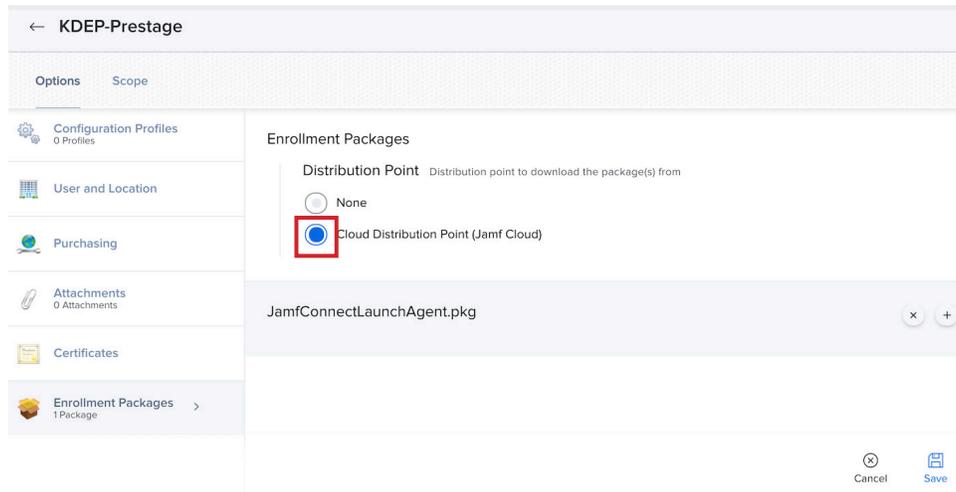
25. Add the JamfConnectLaunchAgent.pkg.

NOTE: If you followed along this guide from the beginning and have the custom logos pkg that we created in section 10, you can add that package as well provide it's signed

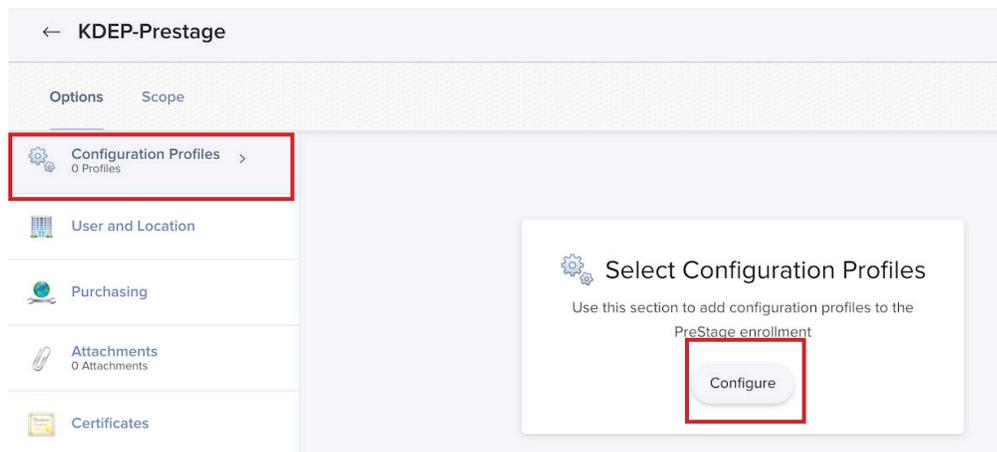




26. Select Cloud Distribution Point (Jamf Cloud)

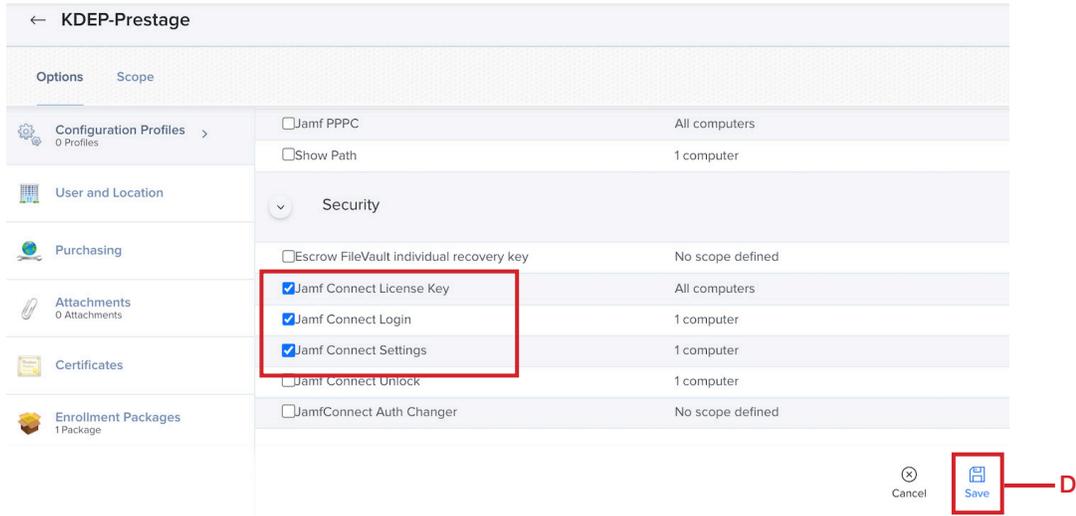


27. Select Configurations Profiles then select Configure.

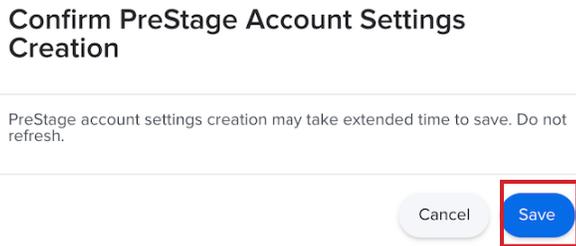




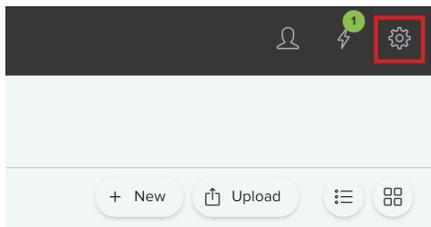
- 28. Select the following configuration profiles:
 - A. Jamf Connect License Key
 - B. Jamf Connect Login
 - C. Jamf Connect Settings
 - D. Click Save



- 28. Click Save

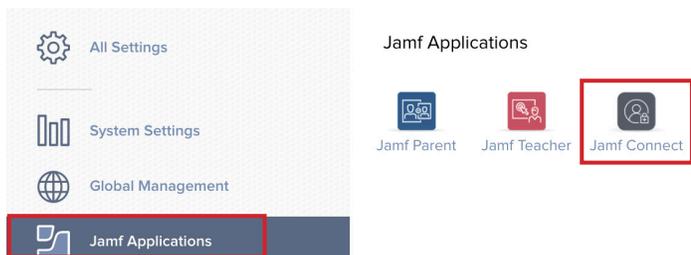


- 29. Click Settings (Looks like a gear) in the upper-right corner.

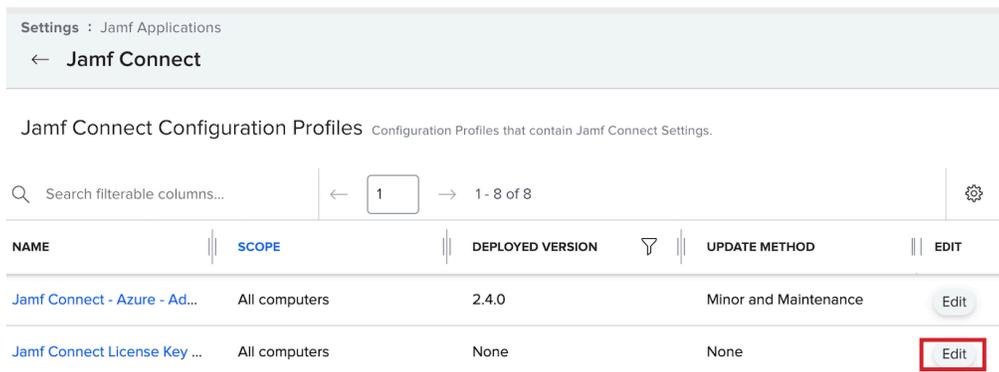




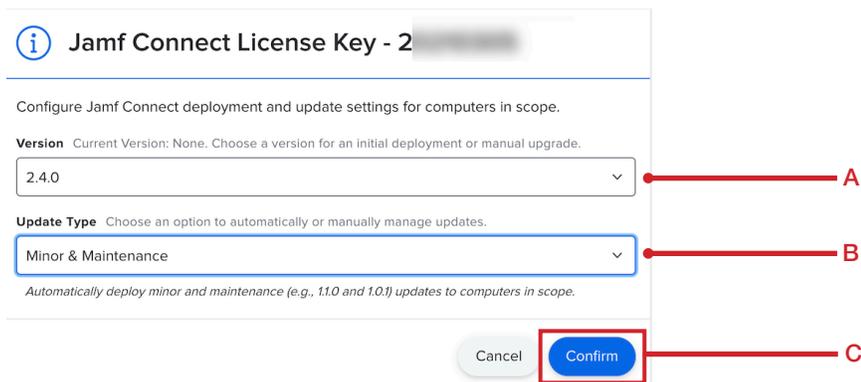
30. Click Jamf Applications then click Jamf Connect.



31. Click Edit on your Jamf Connect License Key.



32. Select the following:
A. Version: 2.4.0
B. Update Type: Minor & Maintenance
C. Click Confirm.





33. The Jamf Connect License key is now configured for auto deployment of Jamf Connect from JAMF Pro.

Settings : Jamf Applications

← Jamf Connect

Jamf Connect Configuration Profiles Configuration Profiles that contain Jamf Connect Settings.

Search filterable columns... 1 1 - 8 of 8

NAME	SCOPE	DEPLOYED VERSION	UPDATE METHOD	EDIT
Jamf Connect - Azure - Ad...	All computers	2.4.0	Minor and Maintenance	Edit
Jamf Connect License Key ...	All computers	2.4.0	Minor and Maintenance	Edit

34. Using a Mac Computer running macOS Mojave or greater and scoped to your prestage in JAMF Pro, enroll the Mac Computer into JAMF Pro via Automated Device Enrollment. During the setup assistant, you should be presented with a Microsoft Login Screen. Login with your Azure credentials and a local account will be created on your Mac Computer. If you used the custom icons and scripts created in this guide, then confirm all your customization are in place and the scripts run.

This completes this section.



Section 13: Configure Jamf Unlock

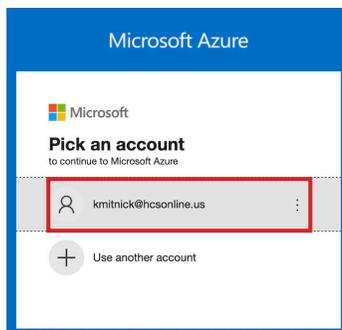
In this section we will configure Jamf Unlock. Jamf Unlock is a mobile device app that allows a user to unlock their Mac with a mobile device without using a password. With Jamf Unlock, users complete a setup process to create or generate identity credentials (certificate) on their device, which is then used to pair and establish trust with a Mac. Jamf Unlock does NOT allow you to login to your Mac Computer upon startup or reboot. It is only used in the following scenarios.

- Unlocking a Mac
- Prompts to change settings in System Preferences
- Commands executed with root privileges with the sudo command

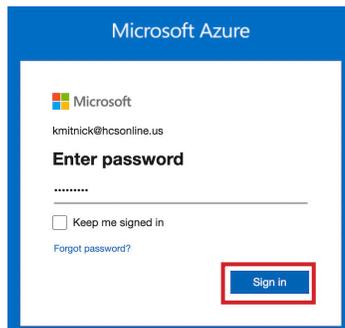
A standard macOS user can only use Jamf Unlock to unlock their Mac Computer. To use the other features, you must be an Administrator on your Mac computer to run commands with sudo privileges and unlock items in system preferences. This guide will use an Administrator user account in order to show all of what Jamf Unlock can do.

This section requires Jamf Connect version 2.4 and the Jamf Unlock App assigned to your Jamf Pro Server from either Apple Business or School Manager. An iOS device with touch or Face ID and iOS version 14 or later enrolled into your Jamf Pro Server is also required.

1. From a web browser of your choosing, go to <https://portal.azure.com> and enter a user name with appropriate privileges to manage the domain.



2. Enter your password and click Sign in.



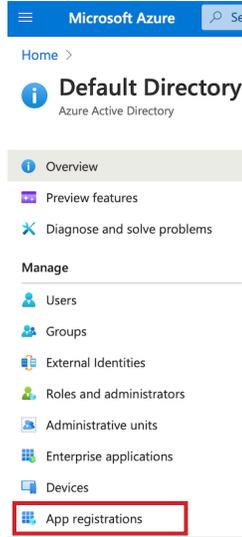
3. Click Azure Active Directory.

Azure services

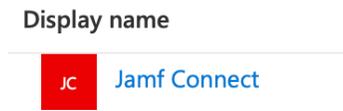




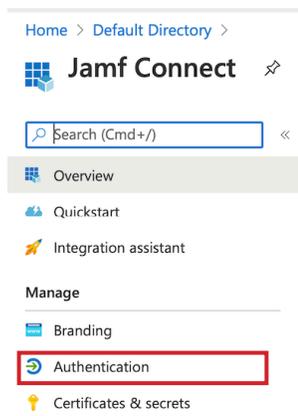
4. Click App registrations.



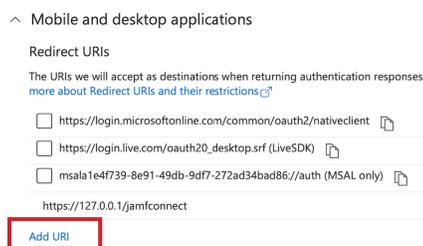
5. Select the Jamf Connect app configuration.



6. Click Authentication.



7. Go to the Mobile and desktop applications section and select Add URI.





8. In the URI field, enter: **jamfunlock://callback/auth**

^ Mobile and desktop applications

Redirect URIs

The URIs we will accept as destinations when returning authentication responses [more about Redirect URIs and their restrictions](#)

- https://login.microsoftonline.com/...
- https://login.live.com/... (LiveSDK)
- msal...://auth (MSAL only)

https://127.0.0.1/jamfconnect

jamfunlock://callback/auth

Add URI

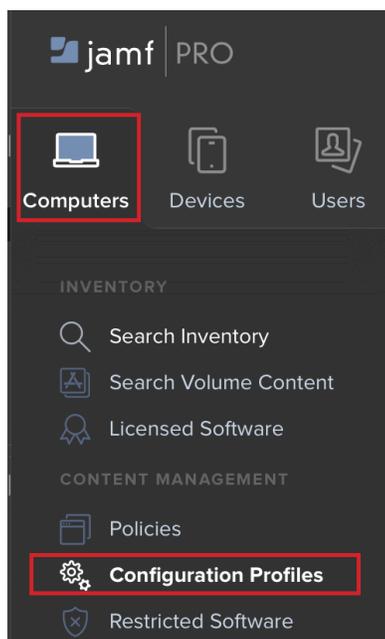
9. Click Save. We are done with the Azure AD configuration. Logout of your Azure portal.



10. If necessary, Log into your Jamf Pro server.

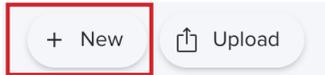


11. Click on Computers, then click Configuration Profiles.





12. Click the New button.



13. In the General section, Enter the following information:

- A. Name: **Jamf Connect Unlock**
- B. Description - **Enter a description of your choosing**
- C. Category - Enter a category of your choosing - this guide will use Security
- D. Leave all other settings at their defaults

General

Name Display name of the profile
Jamf Connect Unlock A

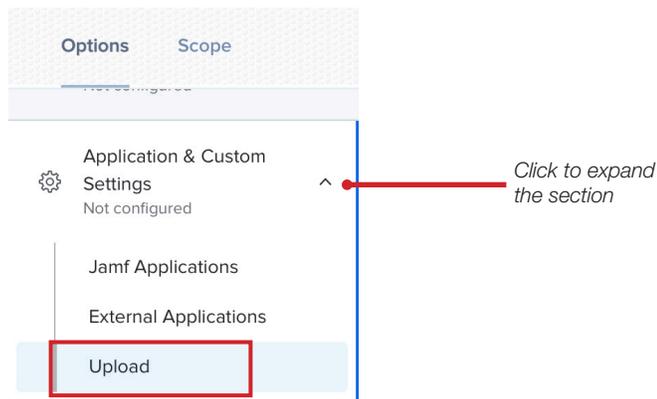
Description Brief explanation of the content or purpose of the profile
This will enable the Jamf Unlock feature in the Jamf Connect Menu Bar. B

Category Category to add the profile to
Security C

Level Level at which to apply the profile
Computer Level

Distribution Method Method to use for distributing the profile
Install Automatically

14. In the payload section, scroll down to the Application & Custom Settings payload. Click the expansion arrow and select Upload.





15. Click Add.

Upload

Use this section to define generic settings for preference domains.

Remove all

+ Add

16. Enter the following information:

A. Preference Domain: **com.jamf.connect**

B. Property List. Paste in the property settings below:

```
<?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>Unlock</key>
<dict>
<key>EnableUnlock</key>
<true/>
<key>RequirePIN</key>
<true/>
</dict>
</dict>
</plist>
```

NOTE: We are adding this configuration profile as a separate setting to enable Jamf Unlock. This will allow you to remove Jamf Unlock if you choose to at a later date without effecting your other jamf connect menu bar settings. If you want only one Jamf Connect configuration profile, you could add the above Unlock keys to your existing JamfConnect mobile configuration file for a singular solution.

Upload

1 payload configured

com.jamf.connect

Use this section to define generic settings for preference domains.

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

com.jamf.connect

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>Unlock</key>
<dict>
<key>EnableUnlock</key>
<true/>
<key>RequirePIN</key>
<true/>
</dict>
</dict>
</plist>
```



17. Click Scope and scope to your needs.

The screenshot shows the 'Scope' configuration page. At the top, there are two tabs: 'Options' and 'Scope', with 'Scope' highlighted by a red box. Below the tabs are two sections: 'Targets' and 'Limitations'. Under 'Targets', there are two dropdown menus. The first is labeled 'Target Computers' with the subtext 'Computers to assign the profile to' and has 'All Computers' selected. The second is labeled 'Target Users' with the subtext 'Users to distribute the profile to' and has 'Specific Users' selected.

18. Click Save.

The screenshot shows a dialog box with two buttons: 'Cancel' (with a close icon) and 'Save' (with a floppy disk icon). The 'Save' button is highlighted with a red box.

19. Click Devices, then click Mobile Device Apps.

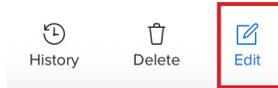
The screenshot shows the Jamf Pro mobile app interface. At the top, there are three menu items: 'Computers', 'Devices', and 'Users'. The 'Devices' item is highlighted with a red box. Below the menu items, there are several sections: 'INVENTORY' with 'Search Inventory' and 'Search Volume Content'; 'CONTENT MANAGEMENT' with 'Configuration Profiles', 'Provisioning Profiles', and 'Personal Device Profiles'; and 'Mobile Device Apps' which is highlighted with a red box; and 'eBooks'.

20. Select the Jamf Unlock App.

The screenshot shows a list of apps. At the top, there is a dropdown menu with 'No category assigned'. Below the menu, there is a table of apps. The first row is 'Jamf Unlock' with version '1.0.0' and 'App Store' as the source. The 'Jamf Unlock' text is highlighted with a red box.

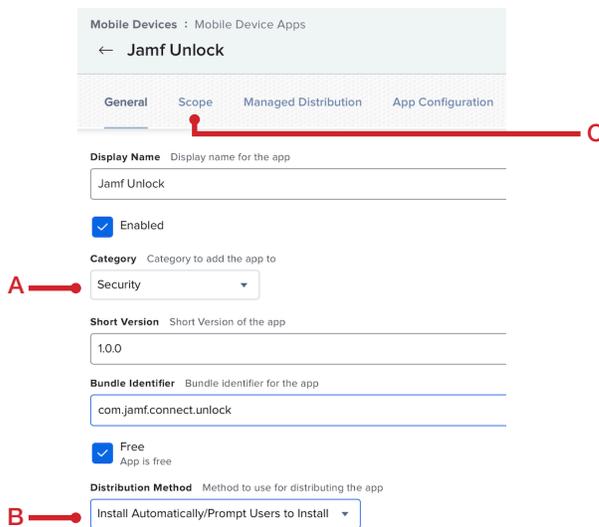


21. Click Edit.

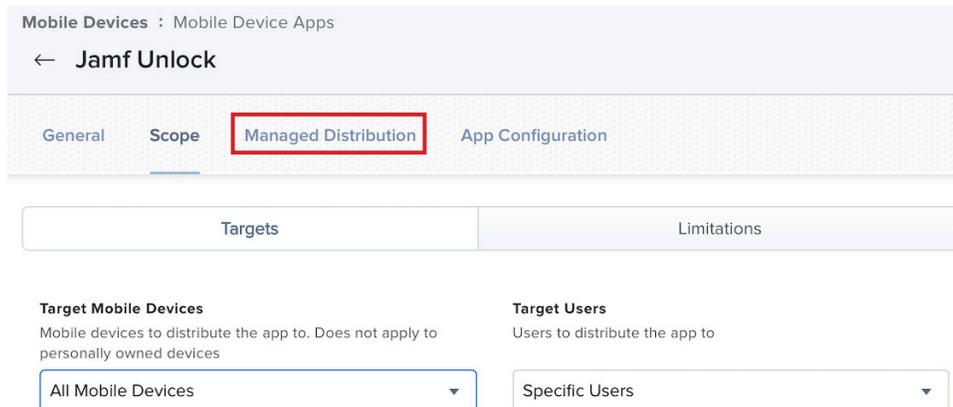


22. Configure the following:

- A. Category - Select a Category of your choosing. This guide will use Security
- B. Distribution Method - Select Install Automatically/Prompt Users to Install
- C. Select the Scope tab



23. Scope to your needs then click Managed Distribution.





- 24. Do the following:
 - A. Confirm Assign Content Purchased in Volume is selected
 - B. Select your Location from the dropdown menu.
 - C. Click App Configuration.

Mobile Devices : Mobile Device Apps

← Jamf Unlock

General Scope Managed Distribution **App Configuration**

Device Assignments

Volume Content

Assign Content Purchased in Volume
Assign content purchased in volume to mobile devices with iOS 9 or later

Location Volume purchasing location to use to assign content
KDEP-Apps&Books

TOTAL CONTENT	IN USE
10	0

25. Paste the XML below in the preferences field.

```
<dict>  
  <key>com.jamf.config.idp.oidc.provider</key>  
  <string>Azure</string>  
  <key>com.jamf.config.idp.oidc.client-id</key>  
  <string>abcd65c-52fe-4b63-8dde-d658abc0aee8</string>  
  <key>com.jamf.config.idp.oidc.redirect-uri</key>  
  <string>jamfunlock://callback/auth</string>  
</dict>
```

Change the com.jamf.config.idp.oidc.client-id string to the OIDC Client ID that you copied in section 3 step 4 of this guide.

Mobile Devices : Mobile Device Apps

← Jamf Unlock

General Scope Managed Distribution **App Configuration**

Preferences Configuration dictionary to be applied to the app on mobile devices with iOS 7 or later

```
<dict>  
  <key>com.jamf.config.idp.oidc.provider</key>  
  <string>Azure</string>  
  <key>com.jamf.config.idp.oidc.client-id</key>  
  <string>a1e4f739-8e91-49db-9df7-272ad34bad86</string>  
  <key>com.jamf.config.idp.oidc.redirect-uri</key>  
  <string>jamfunlock://callback/auth</string>  
</dict>
```

For help generating the PLIST file for preferences, use the [AppConfig Generator](#)



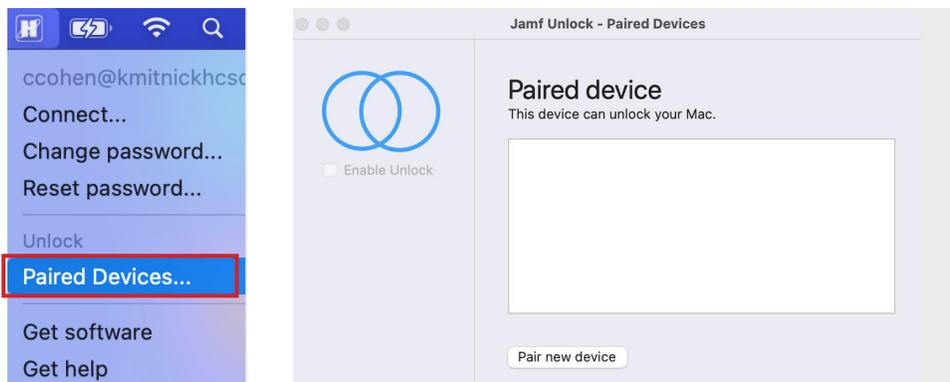
26. Click Save.



27. Open Jamf Unlock on an iOS device that is enrolled in Jamf Pro and has the Jamf Unlock app scoped to it.



28. Confirm you have a Mac Computer with Jamf Connect installed and Unlock shows up in the Menu Bar app. Select Paired Devices. This will open the Jamf Unlock Paired Devices Screen. Leave this screen open as we will need it in a later step

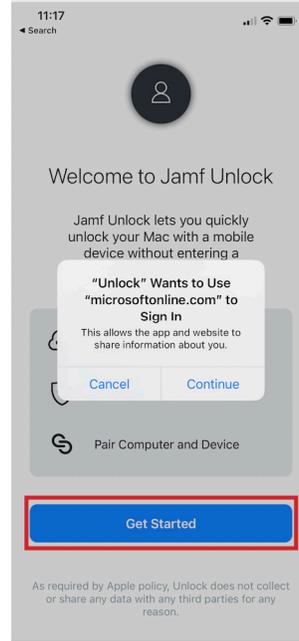




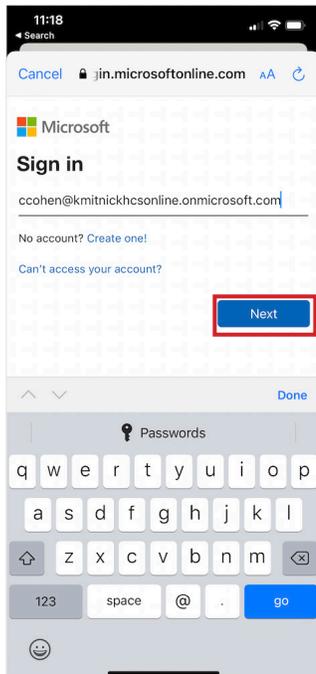
29. On your iOS device, tap Get Started.



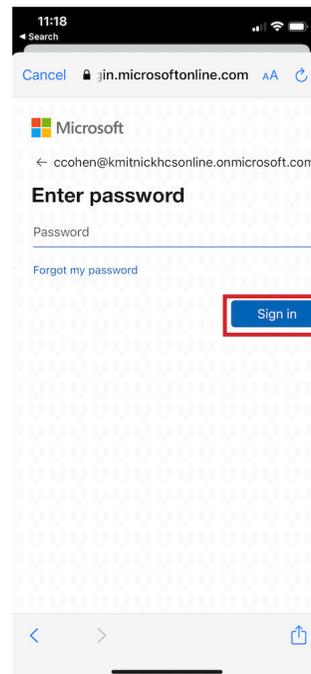
30. Tap Continue at the message below.



31. Enter your Microsoft Azure account then tap Next.

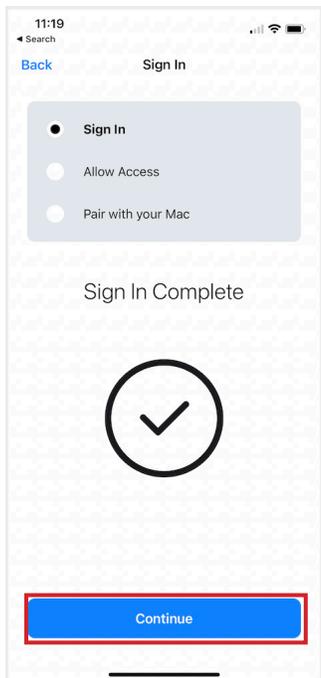


32. Enter your Microsoft Azure password, then tap Sign In.





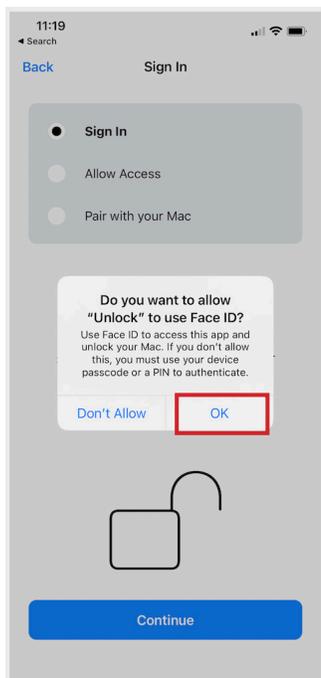
33. Tap Continue.



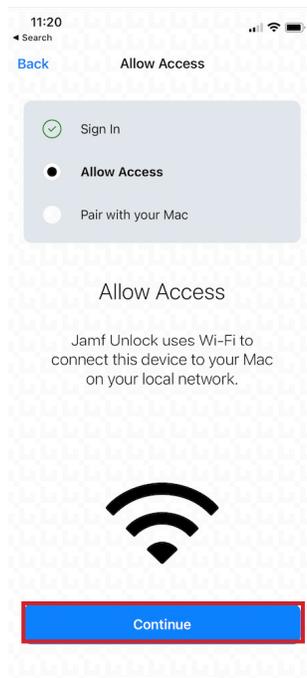
34. Tap Continue.



35. Tap OK at the message below.

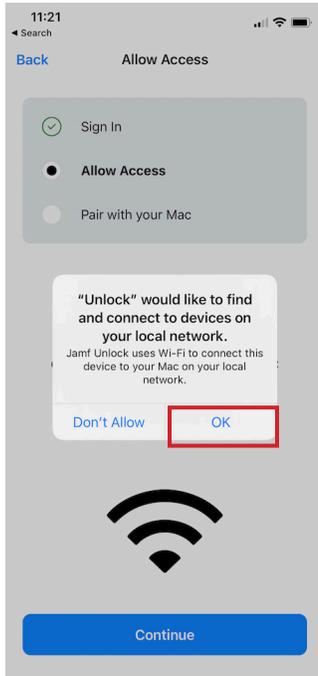


36. Tap Continue.

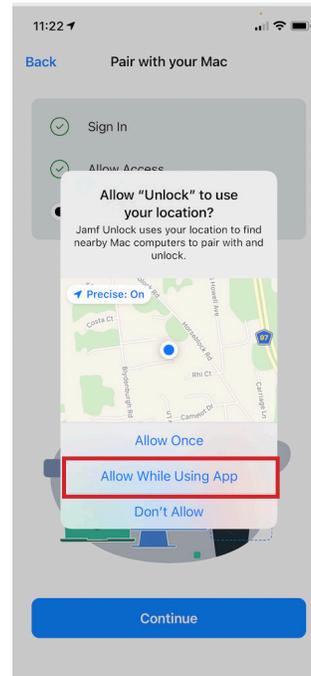




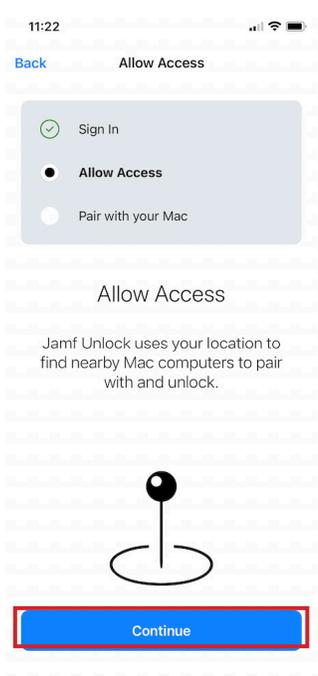
37. Tap OK at the message below.



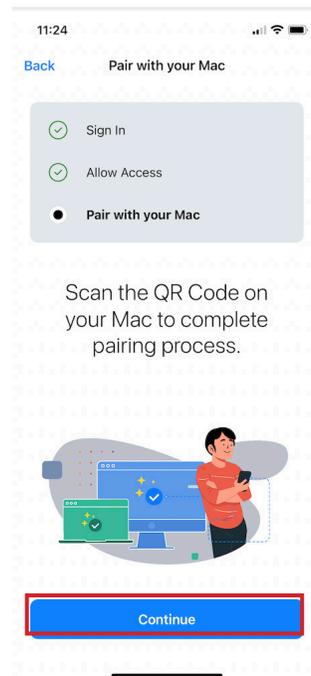
38. At the message below, make a selection of your choosing. This guide will use Allow While Using App.



39. Tap Continue.

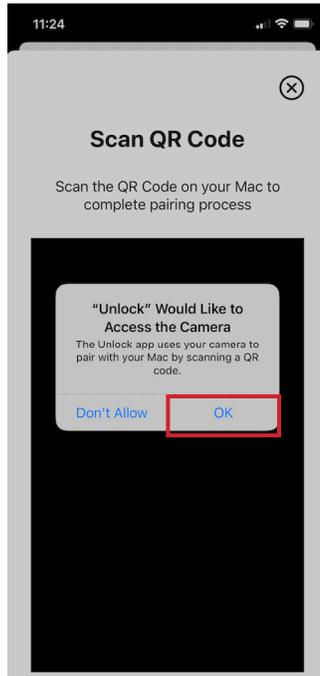


40. Tap Continue.

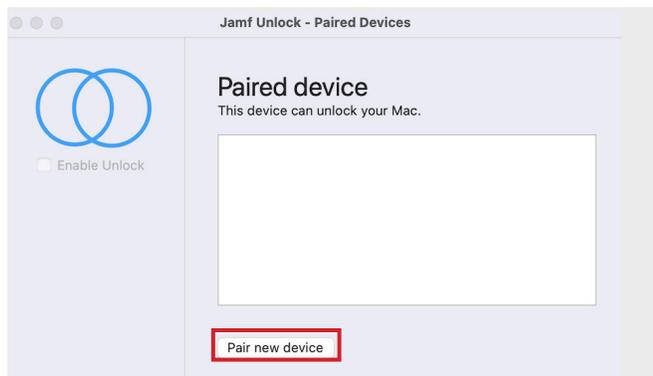




41. Select OK at the message below the use your camera to scan the QR code on your Mac Computer.



42. On your Mac Computer, click Pair new device.

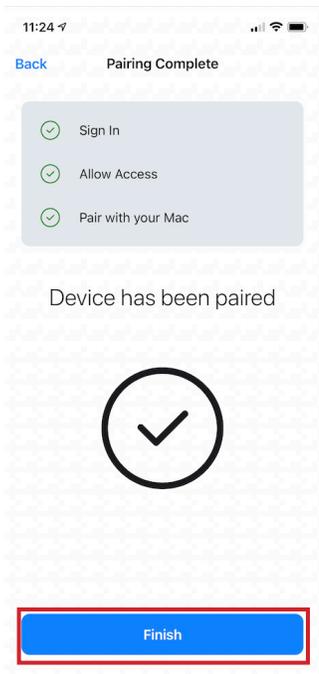


43. Scan the QR code with your iOS device to begin the pairing process.

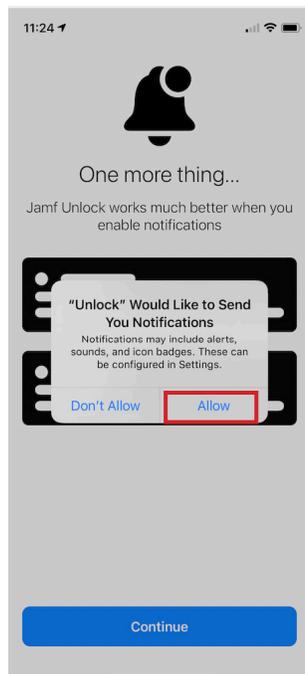




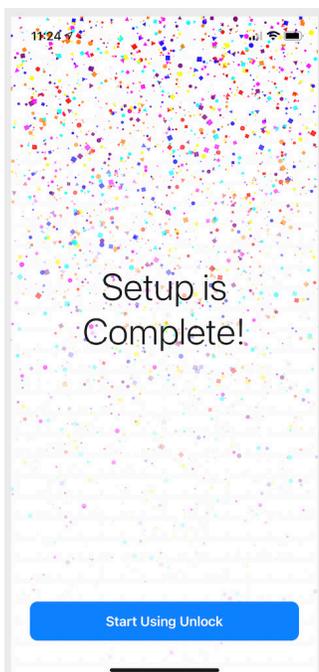
44. On your iOS device, Tap Finish.



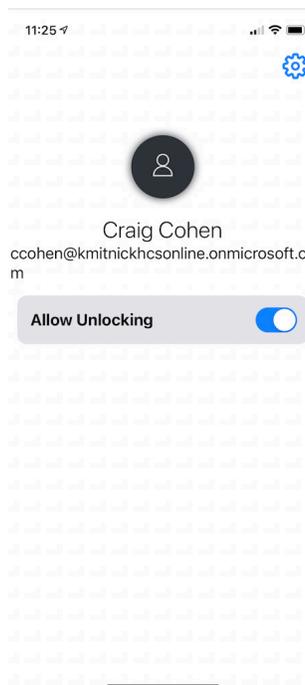
45. Tap Allow at the message below.



46. The setup process is done on the iOS device.

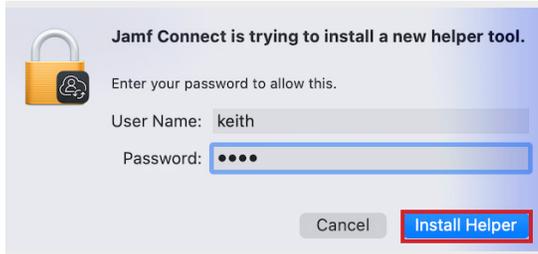


47. The unlock user is configured and ready for use.





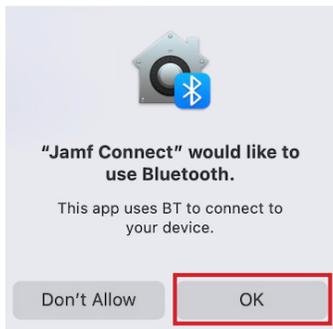
48. Switch back to your Mac computer. Enter your administrative credentials at the message below. Click Install Helper.



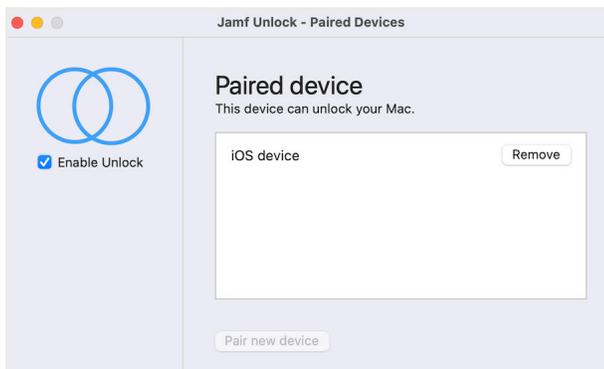
49. Enter your administrative credentials at the message below. Click OK.



50. Click OK at the message below.



51. The pairing process has completed on the Mac Computer.





52. Select the Jamf Connect Menu Bar icon, Unlock should be Enabled.

NOTE: We recommend turning Enable Unlock off then back on for best results. We've seen issues with the Mac computer not responding to Jamf Unlock until it's switched on and off.



53. Let's test the unlocking process. On your Mac Computer, Select the Apple Icon in the upper left corner, then select Lock Screen.

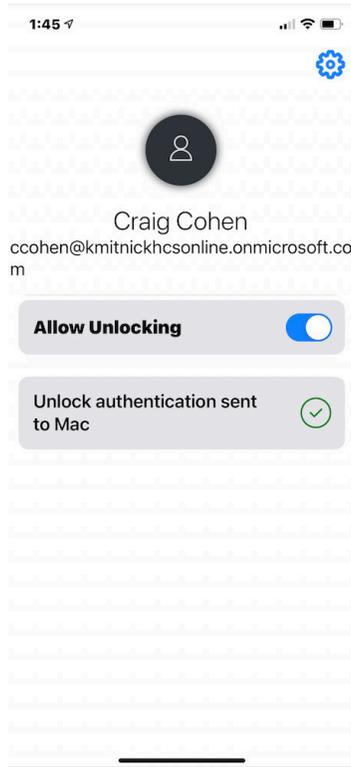


54. You will see the word PIN in the password field, click in the password field and press the Return key on the keyboard.





55. On your iOS device, an unlock code was sent to your Mac Computer. Your Mac Computer should be unlocked and at the Desktop.



56. Click the Apple Menu and select System Preferences.

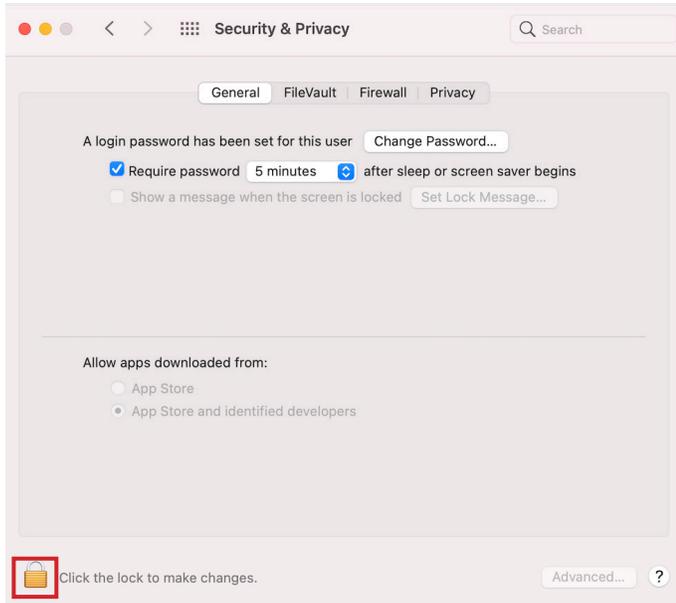


57. Click Security & Privacy.

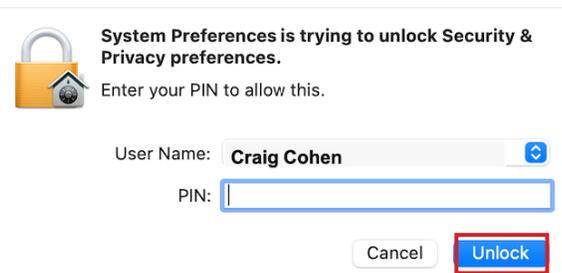




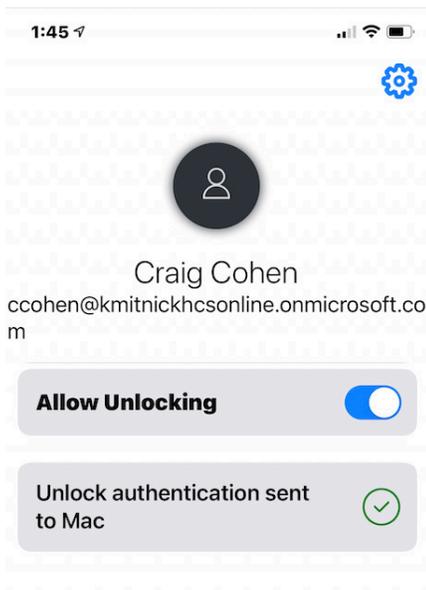
58. Click the lock at the bottom left corner.



59. You will see the word PIN in the password field, click the Unlock button.

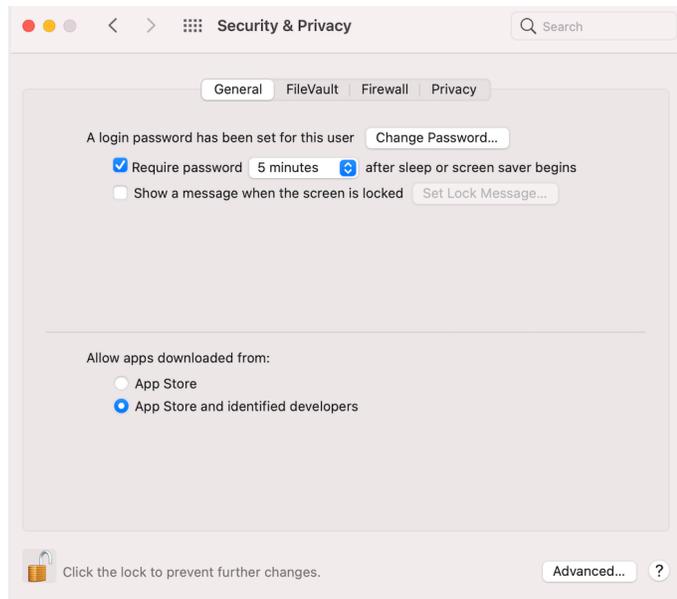


60. On your iOS device, you will see a code was sent to unlock the Security & Privacy pane.





61. Notice the lock on the bottom left is now unlocked. You can quit System Preferences.



62. Open the Terminal application located in /Applications/Utilities.



Terminal

63. Enter the following command: `sudo jamf recon`. When prompted for the password, you will see the word PIN, press the return key on your keyboard.

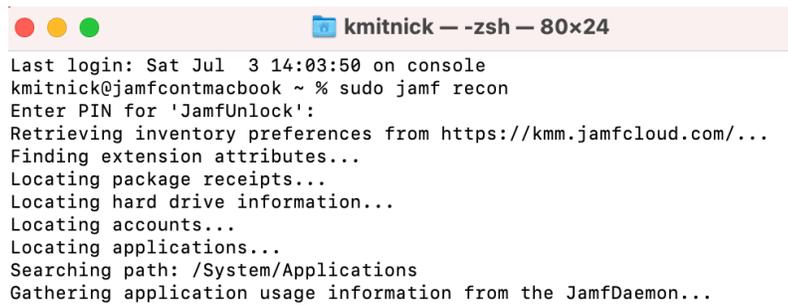




64. On your iOS device, you will see a code was sent to the Terminal app so the command can run.



65. The sudo jamf recon command is now running. This completes this section.



If you'd like help implementing the solution in this white paper, we are ready to help; contact us at info@hcsonline.com or (866) 518-9672.

If you have corrections please send them to info@hcsonline.com.

... and only real pizza comes from NY. 🍕 One slice from a pie is all you need.