jamf | CONNECT

okta

How to Configure Jamf Connect with Okta

Contents

Preface

The purpose of this guide is to provide a workflow for Mac administrators to deploy Jamf Connect using Okta as the Identity Provider (IdP). This guide will cover a myriad of topics such as installing, customizing, and deploying Jamf Connect with Okta. Sections 9 - 11 of this guide are optional and cover configuring Jamf Connect Notify and Jamf Unlock.

Items required to follow along with this guide:

- Administrative access to your Okta web portal. If you don't have Okta and would like to following along, get an Okta developer account here: https://developer.okta.com/signup/
- Jamf Connect - You can download a trial here: http://jamf.it/JCDownload
- Administrative access to your Jamf Pro server.
- Administrative access to your Apple Business / School Manager portal.
- JC_Okta_Files - These are sample files that we use in the guide. Download them here: https://hcsonline.com/images/Apps/JC_Okta_Files.zip

This guide was written and tested using the following:

- Jamf Connect 2.14.0
- Jamf Connect Configuration app 2.14.0
- Jamf Unlock 1.4.0 - iOS App
- Jamf Pro Cloud Hosted Server 10.40.1
- Composer 10.40.1
- Okta Verify 7.8.0 - iOS App used for Okta multi factor authentication
- Okta Server - A development server was used to write this guide
- macOS Monterey 12.5.1 running on a MacBook Air with an M1 processor
- iOS 15.6.1 running on an iPhone 12

Assumptions:

- Your Jamf Pro server is already tied into Apple Business / School Manger for Automated Device Enrollment and Volume Purchasing.
- The Jamf Unlock app is already assigned to your Jamf Pro Server via Apps & Books from Apple Business / School Manager.
- We will NOT cover configuring the above items so please have them in place before you begin.
- For more Information on Integrating Apple Business Manager/Apple School Manager, please go to the links below:

  https://docs.jamf.com/jamf-pro/documentation/Volume_Purchasing_Integration.html?hl=apple%2Cbusiness%2Cmanager

  https://docs.jamf.com/10.41.0/jamf-pro/documentation/Automated_Device_Enrollment_Integration.html

This guide would not be possible without the support and guidance from the following people:

- Adam Karneboge
- Craig Cohen
- Daniel Allen
- Erin McDonald
- Richard Goon
- Sean Rabbitt
- William Smith

Section 1: Authenticate to Okta using the Jamf Connect Configuration App

Requirements for following along with this section:

- A Mac computer running macOS 10.15.4 or later. This guide will use macOS Monterey 12.5.1
- Jamf Connect installer DMG. This guide will use version 2.14.0
- The URL of your Okta server with an account you can use for testing login credentials.
- The Okta Verify app installed on your phone for MFA.

In this lesson we will configure the Jamf Connect Configuration App to use the Okta IDP with a few basic settings. Jamf Connect authenticates Okta users directly to your domain using Okta's authentication API, you do not need to perform any additional tasks in the Okta admin console to enable authentication and password syncing. This section will show you how easy it is to test connectivity to Okta using only your Okta URL and the Jamf Connect Configuration App.

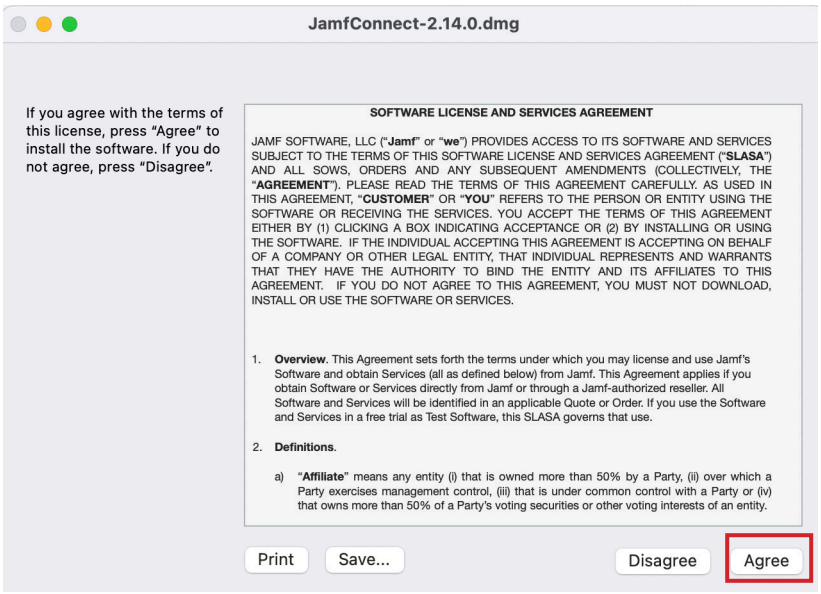
Okta also supports OpenID Connect. OpenID Connect app integrations are only required to do the following:

- Configuring local role assignment—You can determine if users are created with standard or administrator local accounts with Jamf Connect by creating different app integrations in Okta for standard users and administrators. You can then assign users to each app in Okta, and Jamf Connect uses the user's app assignment to create the correct local account type.
- Deploying Jamf Unlock—The Jamf Unlock app only uses the OpenID Connect authentication protocol to authenticate users during the pairing process.

NOTE: We will cover configuring Okta app integrations for role based user assignment in the next section of this guide.

1. Double click the JamfConnect-2.14.0 dmg.

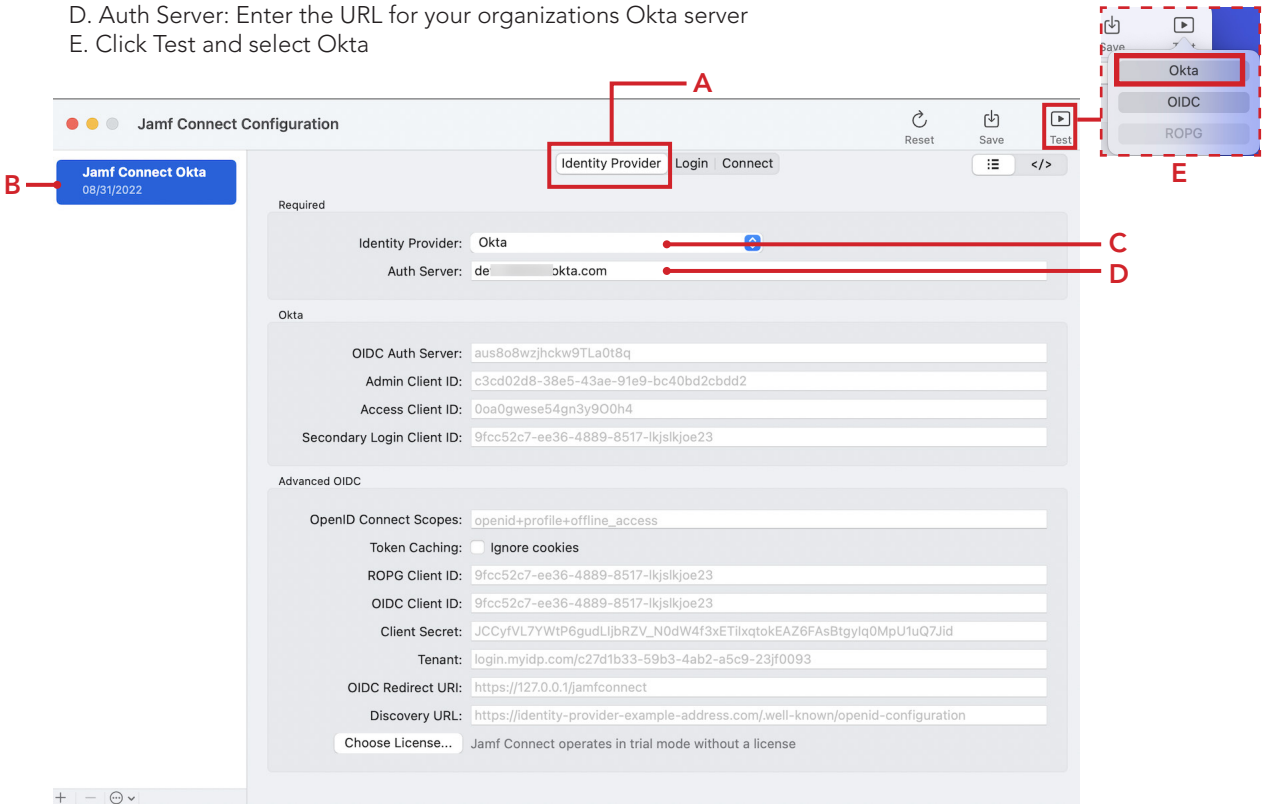
2. Click Agree.



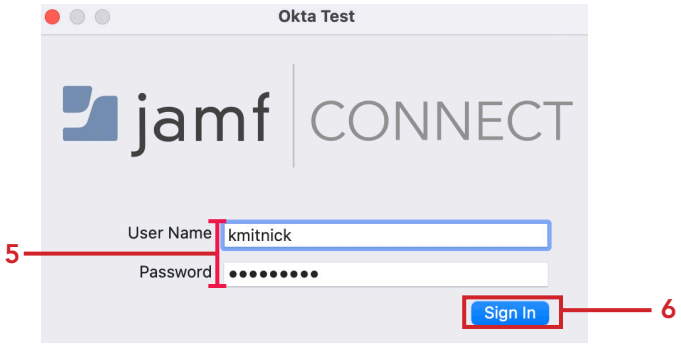
3. Drag the Jamf Connect Configuration App to your Applications folder. Open the app when done.

4. Follow these steps:

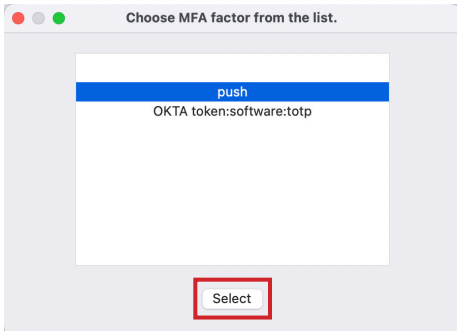
A. Click the Identity Provider tab
B. Name the configuration Jamf Connect Okta
C. Identity Provider: Okta
D. Auth Server: Enter the URL for your organizations Okta server
E. Click Test and select Okta



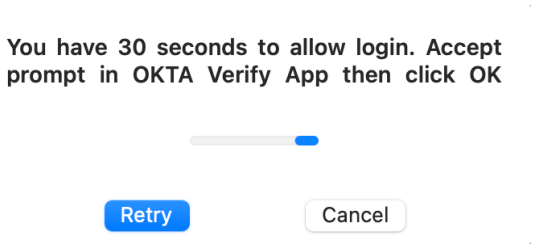
5. Enter your Okta account credentials
6. Click Sign In.



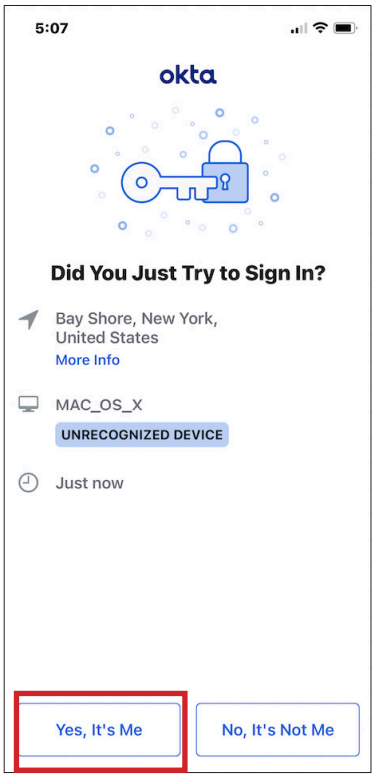
7. If you have MFA enabled in your Okta environment, you will be greeted with the message below. Select the option that applies to you. This guide will use push and an alert will be sent to the Okta verify app on your phone.



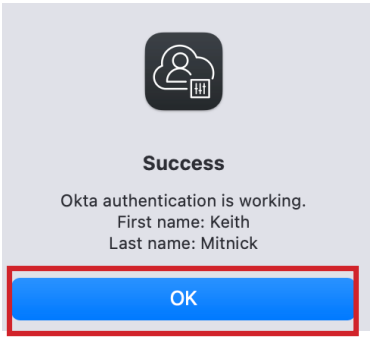
8. You have 30 seconds to accept the push message on your phone.



9. Tap Yes, It's me on your phone.



10. If authentication was successful, you will see the message below. Click OK.



That is all you need to configure Okta with Jamf Connect for basic authentication settings. We will cover configuring role based user assignment and enabling MFA in Okta in the next section of this guide.

This completes this section.

Section 2: Configure App Integrations, User Groups, and MFA in Okta

This section covers App Integration, role based user assignment with groups, and enabling MFA in Okta. If you are NOT interested in assigning user permissions based on their roles in Okta or enabling MFA, you can skip this section as it's NOT a requirement to use Okta with Jamf Connect. If you plan on using the Jamf Unlock app, that will use the OpenID Connect authentication protocol to authenticate users during the pairing process so you would need to complete this section if using Jamf Unlock.

Requirements for following along with this section:

- Administrative access to your Okta domain.
- Okta Verify app installed on your phone for MFA

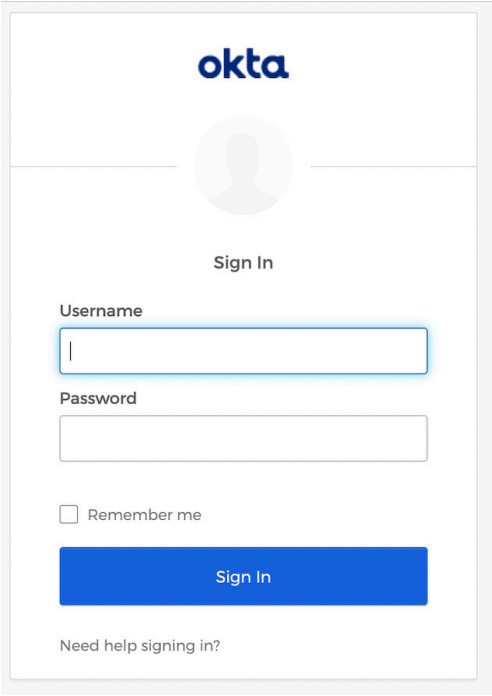
Okta communicates with its own API and authenticates users directly to your Okta domain. The applications we will configure in this section are used to separate administrative users from standard users in Okta. Once configured, you can create, demote or promote users on macOS using the role assignment of the users account in Okta. We will also configure MFA for all Okta users. To follow along with the MFA section of this guide, you will need to download the Okta Verify app to your phone so you can approve the MFA messages.

NOTE: This guide will not cover setting up Okta verify on your device as it's available for multiple device types and operating systems. The link below will cover setting up Okta verify based on the operating system and device type you are using.

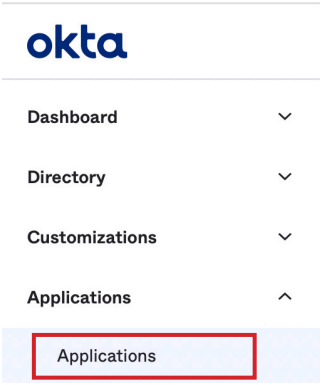
https://help.okta.com/eu/en-us/Content/Topics/end-user/ov-overview.htm?cshid=csh-user-ov-overview

What is an App Integration?
App Integration is the process of connecting disparate software applications in order to combine data, share workflows, and communicate in real-time. In this section, we will create two Okta App Integrations for use with Jamf Connect.

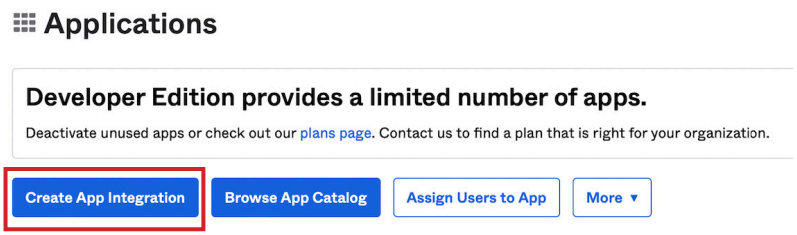
1. Using a web browser of your choice, sign in to Okta using your administrative credentials.



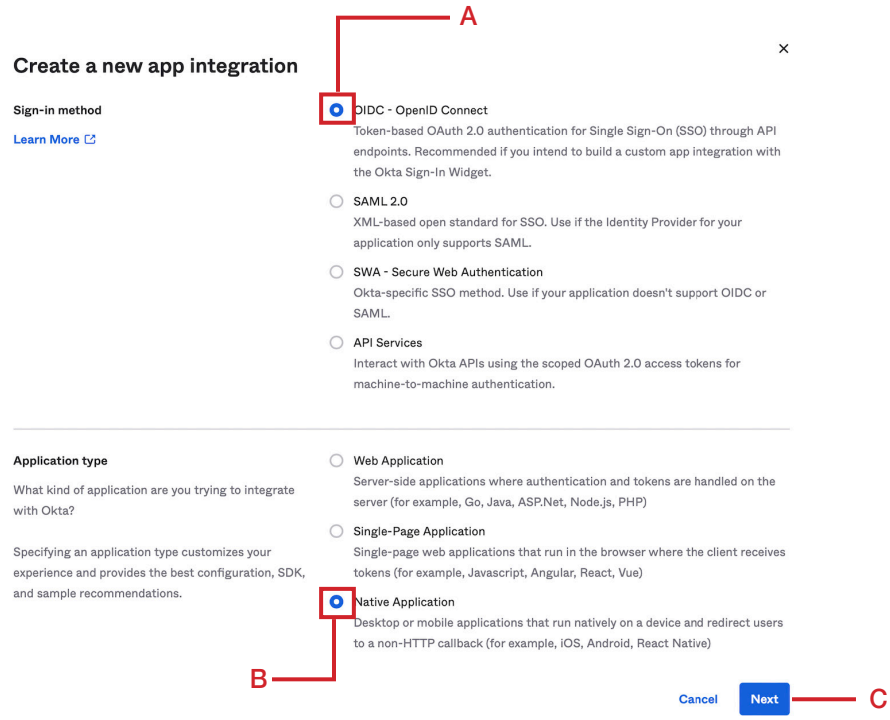
2. Expand Applications and click Applications.



3. Click Create App Integration.

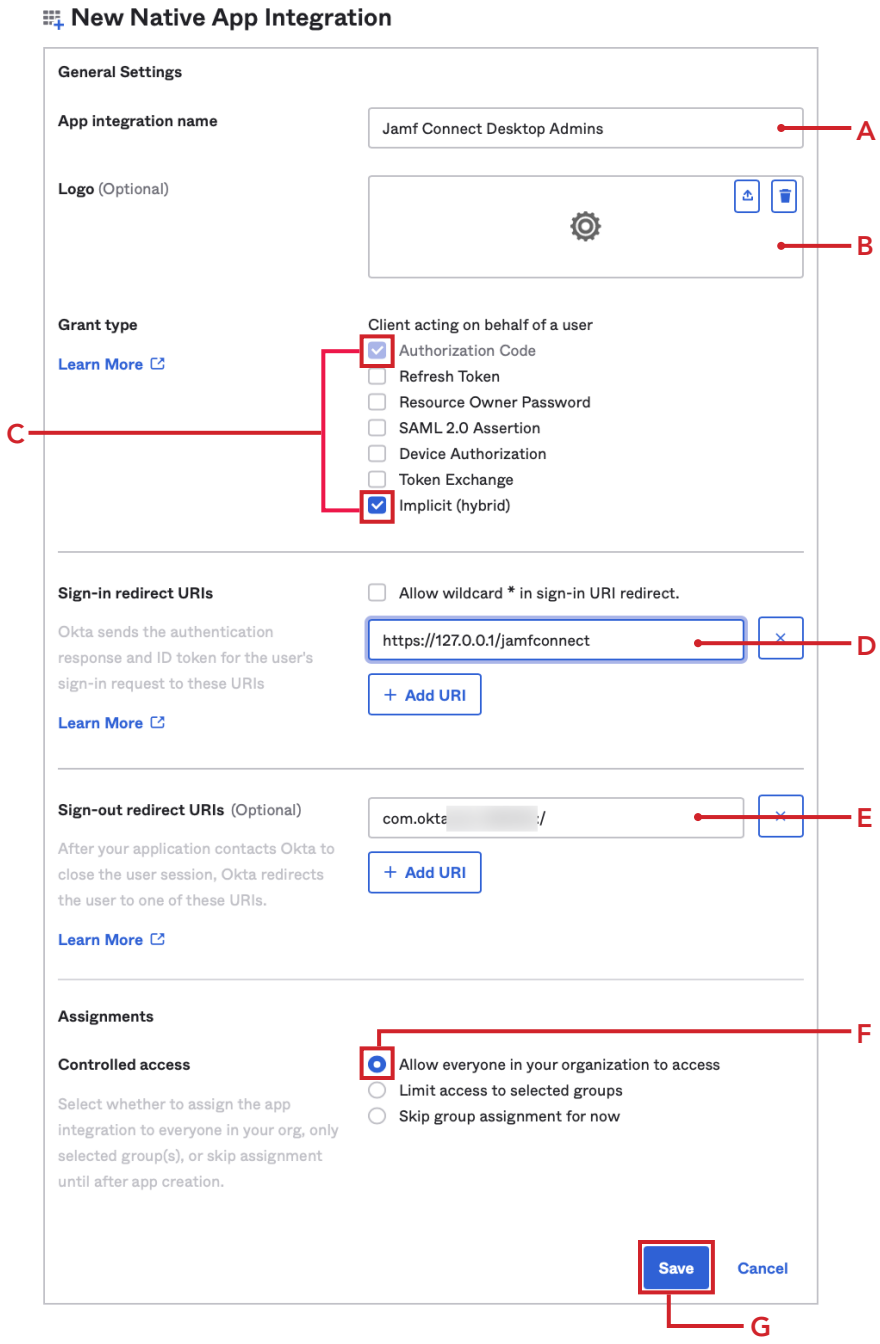


4. Configure the following:
   A. In the section, Sign-in method, select OIDC - OpenID Connect
   B. In the section, Application type, select Native Application
   C. Click Next

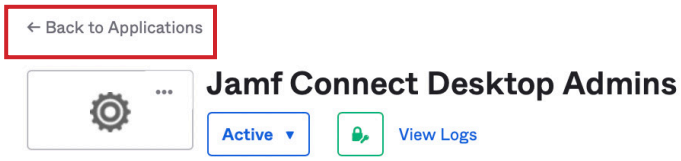


5. Configure the following:
   A. App Integration Name: Jamf Connect Desktop Admins
   B. Logo: This is optional
   C. Grant type: Enable Authorization Code and Implicit (Hybrid)
   D. Sign-in redirect URIs: https://127.0.0.1/jamfconnect (NOTE - This is case sensitive)
   E. Sign-out redirect URIs: Use default settings
   F. Assignments: Allow everyone in your organization to access
   G. Click Save

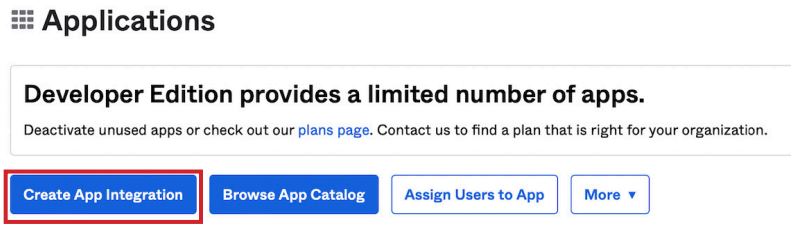
NOTE: For item D in the list above, you have the option of redirecting to macOS which will use https://127.0.0.1/jamfconnect or you can choose to use the Jamf Unlock iOS app for authentication which will redirect to jamfunlock://callback/auth. This guide will use the macOS redirection.



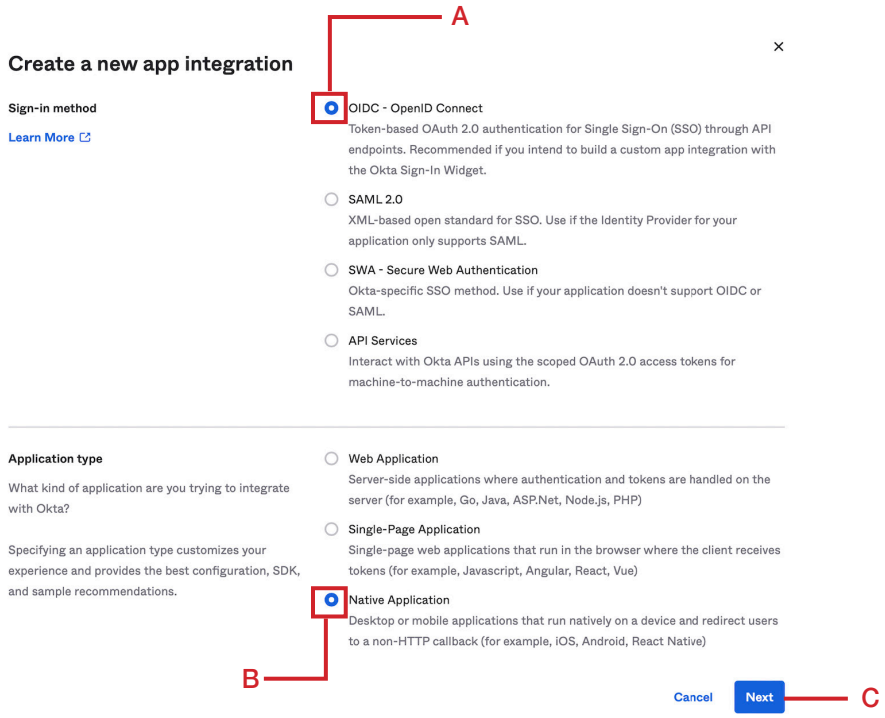
6. Click Back to Applications.



7. Click Create App Integration.

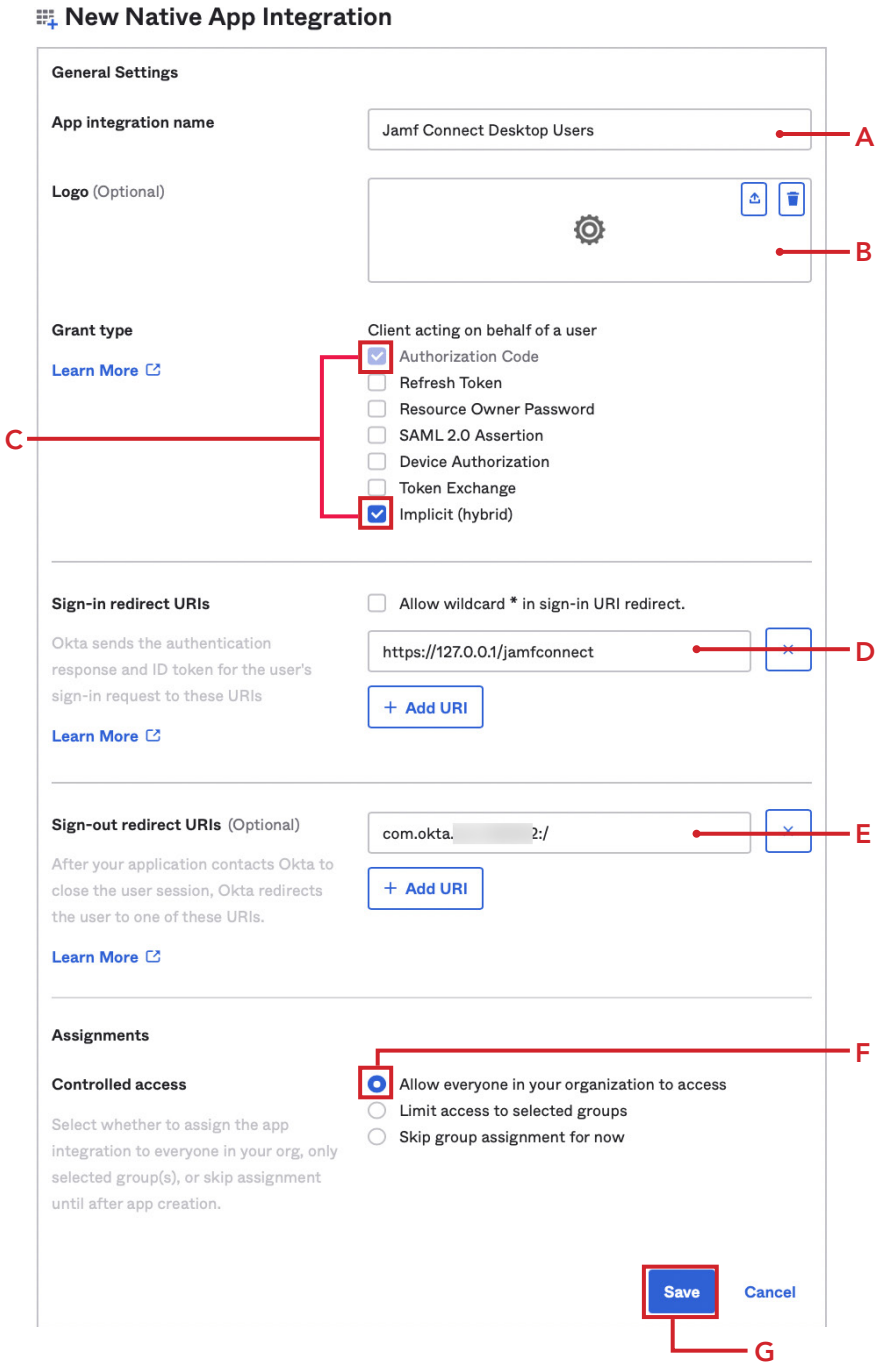


8. Configure the following:
   A. In the section, Sign-in method, select the radio button for OIDC - OpenID Connect
   B. In the section, Application type, select the radio button for Native Application
   C. Click Next

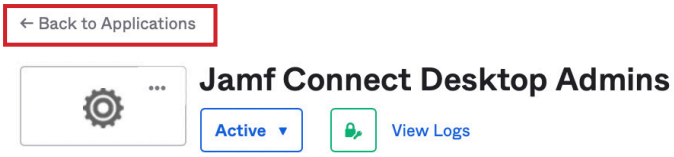


9. Enter the following:
   A. App Integration Name: Jamf Connect Desktop Users
   B. Logo: This is optional
   C. Grant type allowed: Enable Authorization Code and Implicit (Hybrid)
   D. Sign-in redirect URIs: https://127.0.0.1/jamfconnect
   E. Sign-out redirect URIs: Use default settings
   F. Assignments: Allow everyone in your organization to access
   G. Click Save

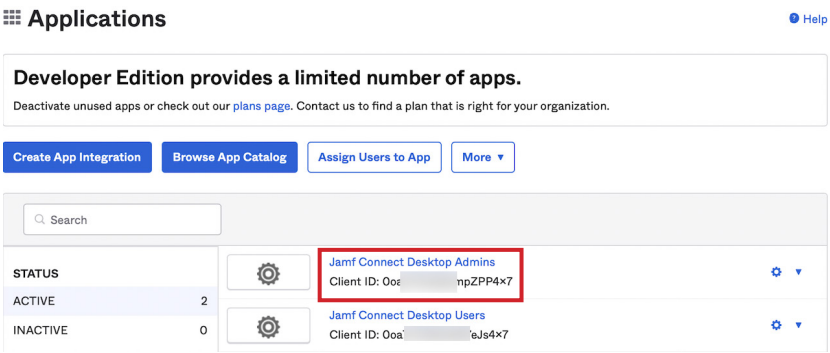
NOTE: For item D in the list above, you have the option of redirecting to macOS which will use https://127.0.0.1/jamfconnect or you can choose to use the Jamf Unlock iOS app for authentication which will redirect to jamfunlock://callback/auth. This guide will use the macOS redirection.



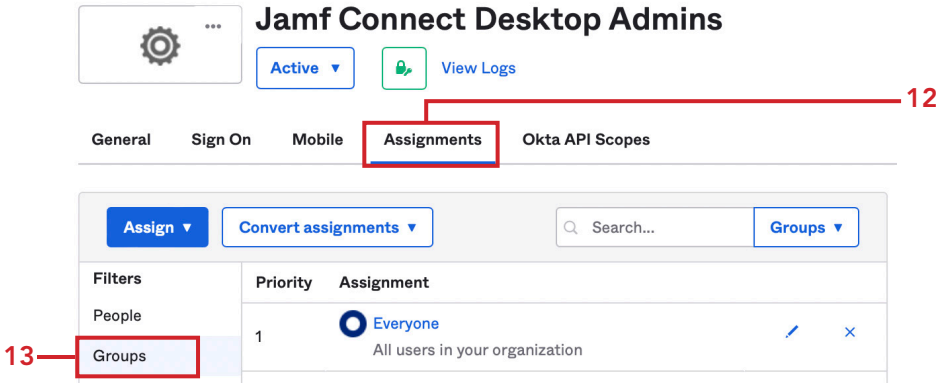
10. Click Back to Applications.



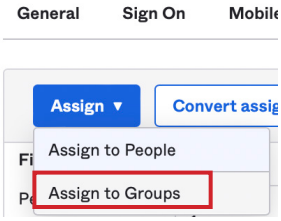
11. Click Jamf Connect Desktop Admins.



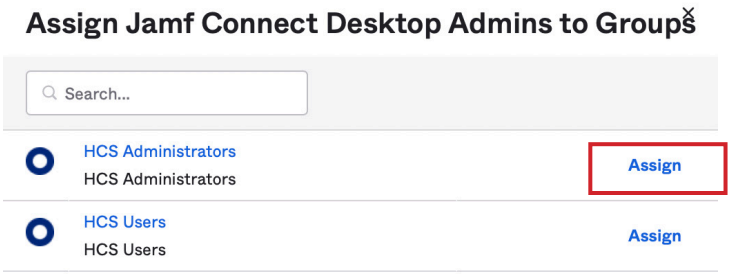
12. Click Assignments
13. Click Groups.



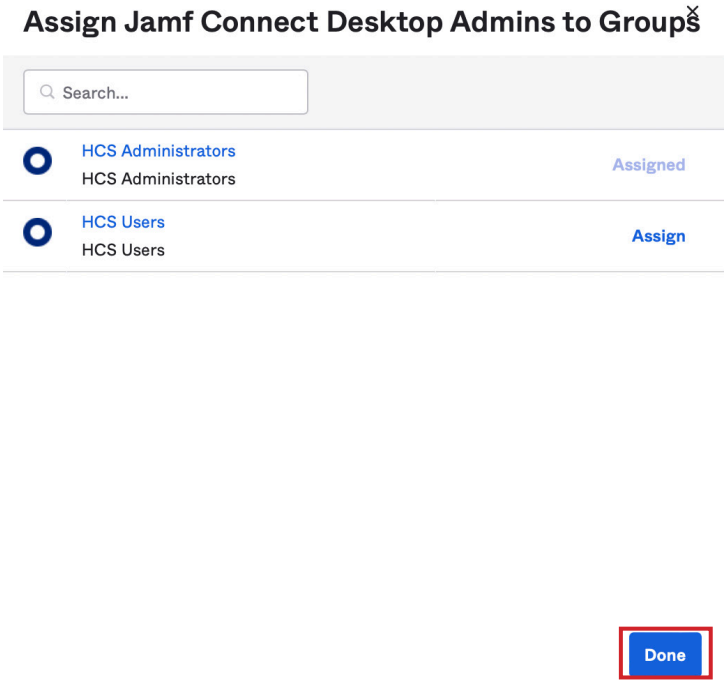
14. Click Assign and select Assign to Groups.



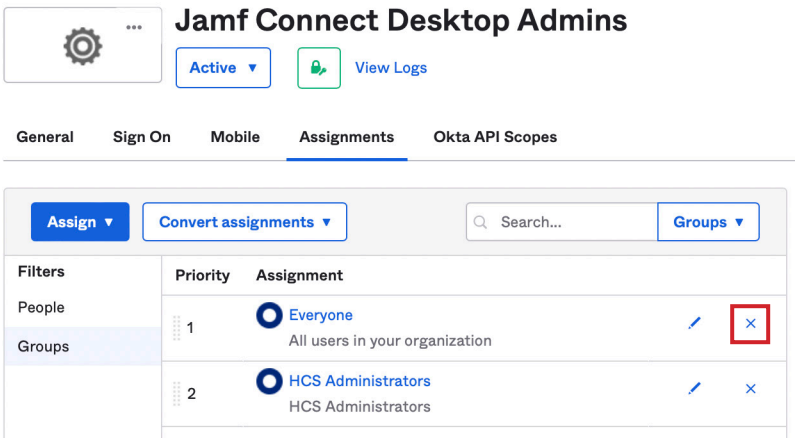
15. Select your administrators group. This guide will select HCS Administrators. Click Assign.



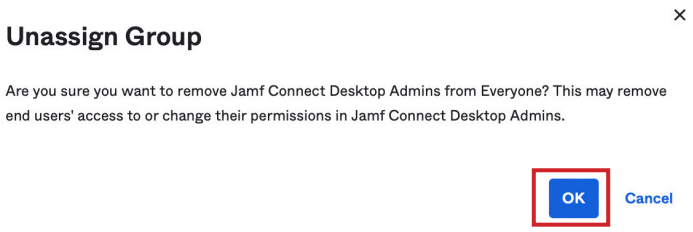
16. Click Done.



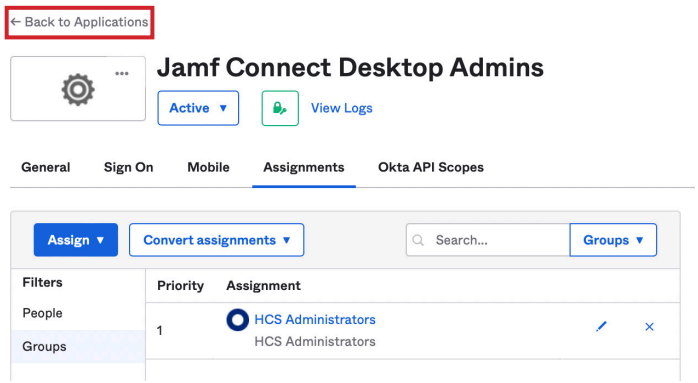
17. Remove the Everyone group.



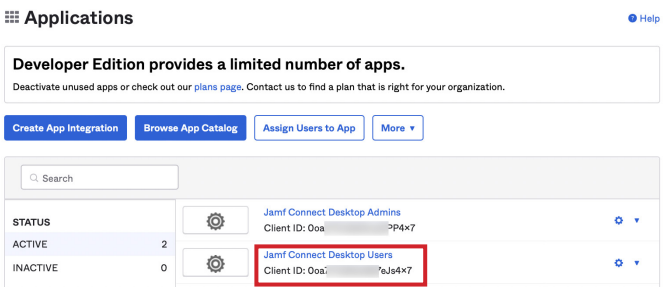
18. Click OK.



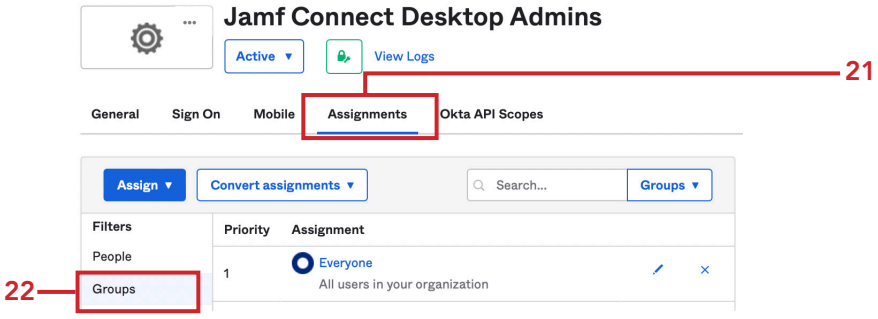
19. Click Back to Applications.



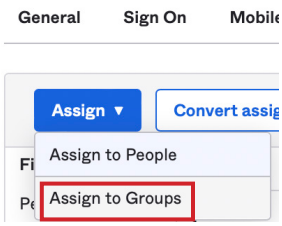
20. Click Jamf Connect Desktop Users.



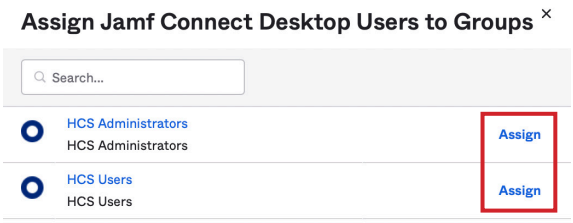
21. Click Assignments.
22. Click Groups.



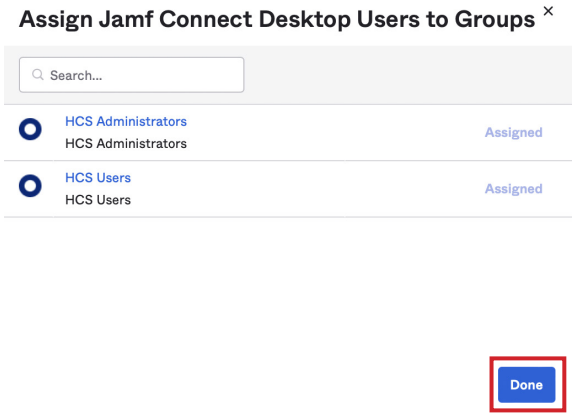
23. Click Assign and select Assign to Groups.



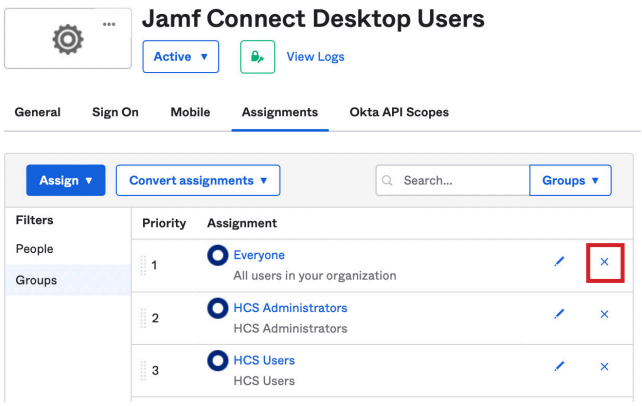
24. Assign your administrators and users groups by selecting Assign.
NOTE: For the Jamf connect desktop users group, your administrator user group MUST be assigned with your user group.



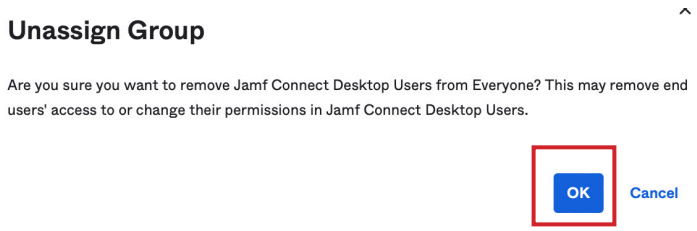
25. Click Done.



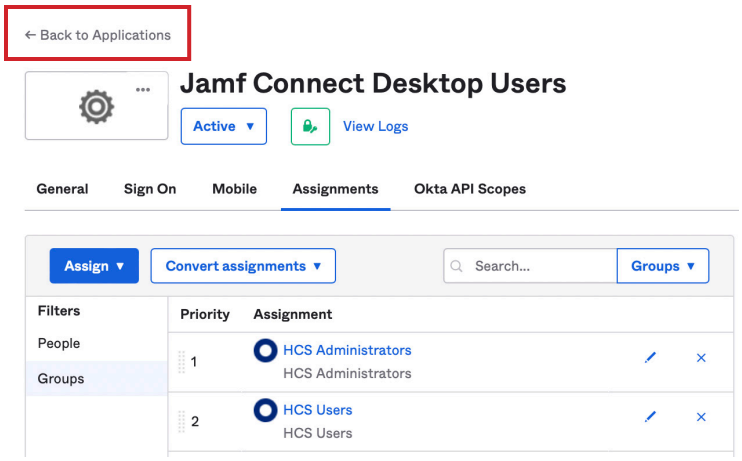
26. Remove the Everyone group.



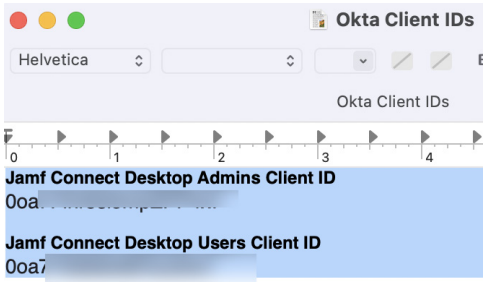
27. Click OK.



28. Click Back to Applications.



29. Open a text editor of your choice and save each client ID. Name the file Okta Client IDs. We will need these ID's in a later section of this guide.

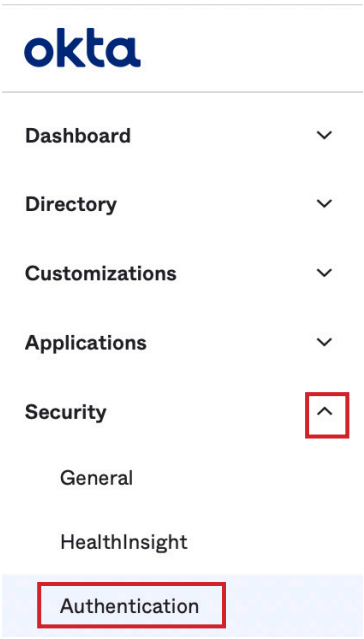


The next steps in this section are to enable MFA for all Okta users. These steps are optional so feel free to move on if MFA is not needed in your organization.

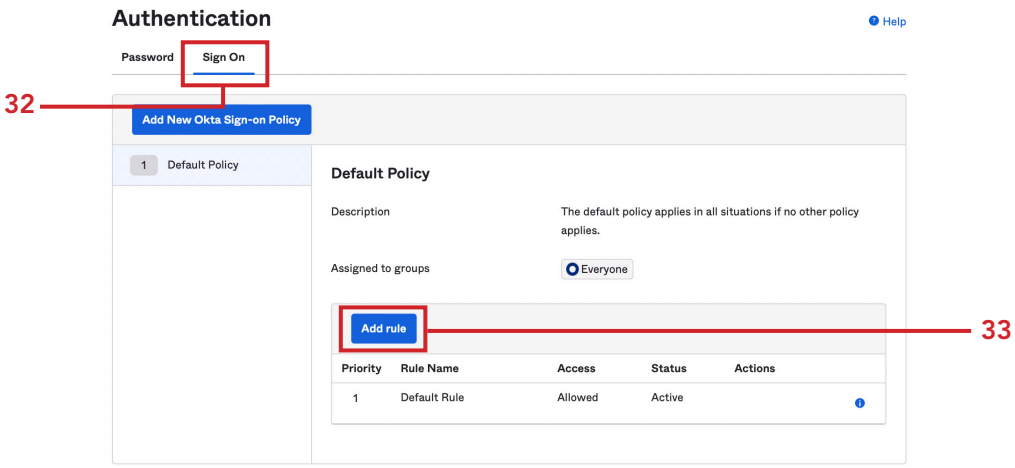
NOTE: If you want to enable multi-factor authentication (MFA) for users, you must enable MFA at the organization level rather than the app level. Enabling MFA at the app level is not recommended and may cause errors in Jamf Connect. Jamf Connect may allow users with the same username and password to log in to the incorrect local account. To ensure users can only log in to their account, a multi-factor authentication (MFA) method is recommended. Jamf does not accept any responsibility or liability for any damages or security exploitations due to identically provisioned account credentials.

What is MFA?
Multi-factor Authentication (MFA) is an authentication method that requires the user to provide two or more verification factors to gain access to a resource such as an application, online account, or a VPN. MFA is a core component of a strong identity and access management policy. Okta has an app called Okta Verify that can be used for MFA on your mobile device.

30. On the Okta sidebar menu, expand Security.
31. Click Authentication.

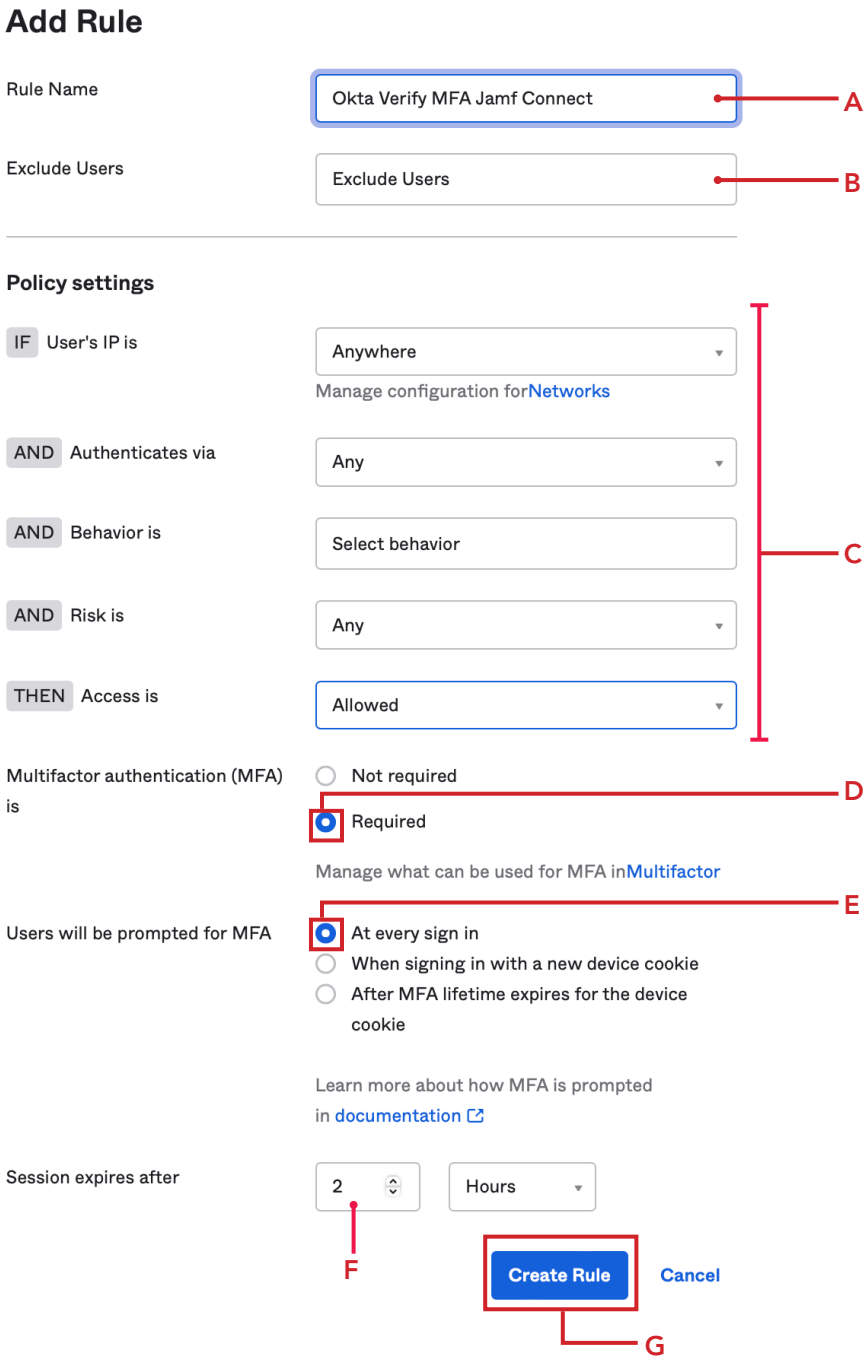


32. Click Sign-on.
33. Click Add rule.

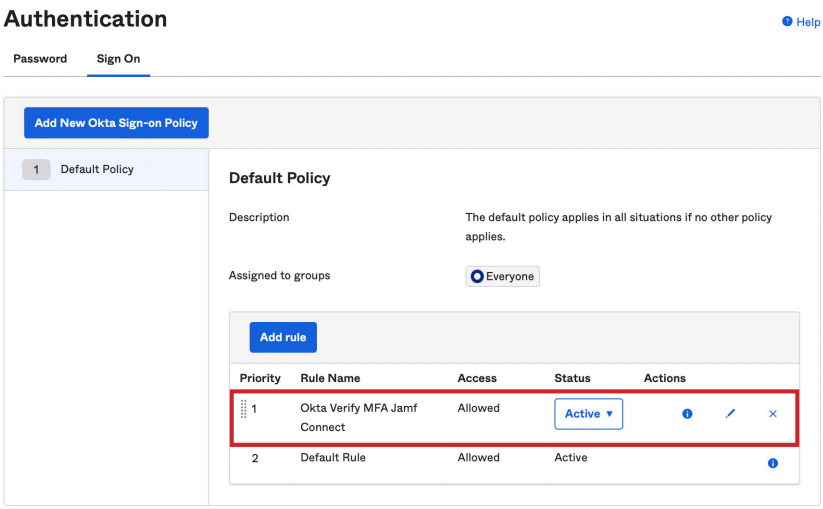


34. Enter the following:
    A. Rule Name: Okta Verify MFA Jamf Connect
    B. Exclude Users: Exclude Users
    C. Policy Settings: Match what is shown in the picture below.
    D. Multi-factor Authentication (MFA): Select the radio button for Required
    E. Users will be prompted for MFA: Select the radio button for At every sign in
    F. Session expires after: 2 hours
    G. Click Create Rule

NOTE: Feel free to set the items below to the needs of your organization. Items selected below are for simplicity.



35. Confirm the rule was created and listed as number 1 in the list. If all looks good, you can logout of the Okta portal.



This guide will not cover setting up Okta verify on your device as it's available for multiple operating systems. The link below will cover setting up Okta verify based on the OS and device type you are using. You will need to configure this now for your Okta account to follow along with the rest of this guide if you're using MFA.

https://help.okta.com/eu/en-us/Content/Topics/end-user/ov-overview.htm?cshid=csh-user-ov-overview

This completes this section.

Section 3: Creating a code signing certificate using Jamf Pro's CA

This section will cover creating a code signing certificate using your Jamf Pro server.

Requirements for following along with this section:

- A Mac computer running macOS 10.15.4 or later enrolled in your Jamf Pro server.
- Administrative access to your Jamf Pro server.

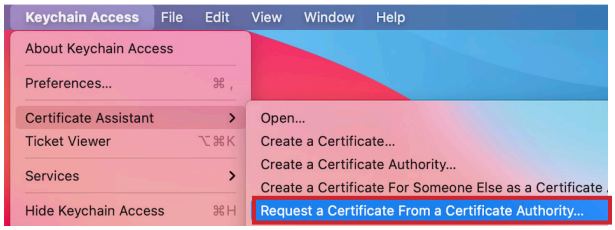
Why do we need a code signing certificate?
In order to deploy a package using a PreStage enrollment in Jamf Pro, the package must be signed. In the next section of this guide, we will create a custom package with images and scripts that will be used to customize the look of Jamf Connect. This package must be signed in order to deploy it using a PreStage Enrollment in Jamf Pro. If you have your own signing certificate, feel free to use that and skip this section of the guide.

When creating a code signing certificate using your Jamf Pro server, make sure to follow the steps in this section 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.

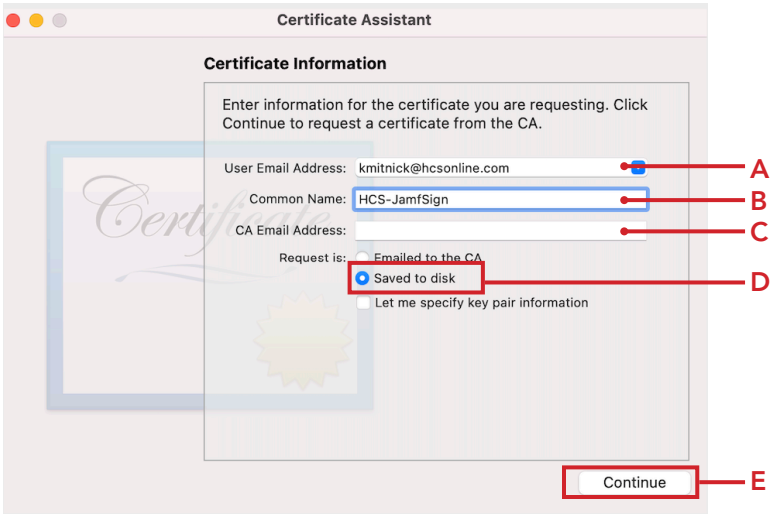
1. Open Keychain Access located in /Applications/Utilities.

Keychain Access

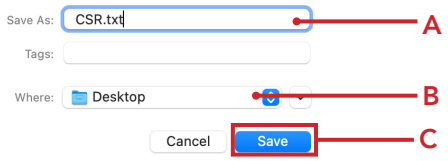
2. Select Keychain Access > Certificate Assistant > Request a Certificate From a Certificate Authority.



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



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

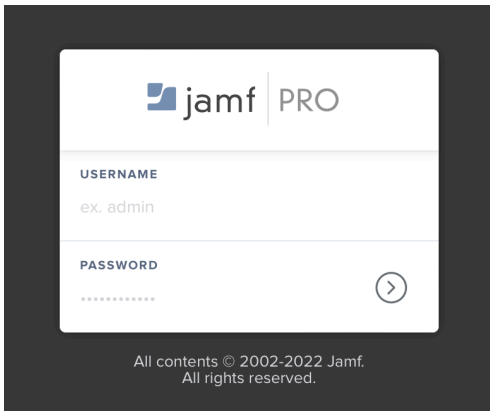


5. Click Done.

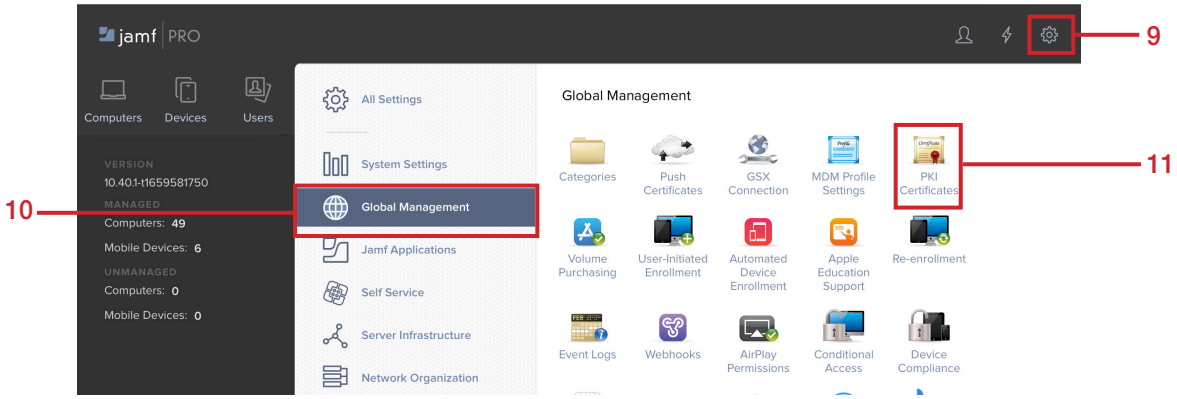
6. Open the CSR.txt file on your desktop with a text editor of your choice.

7. Copy the entire CSR text.

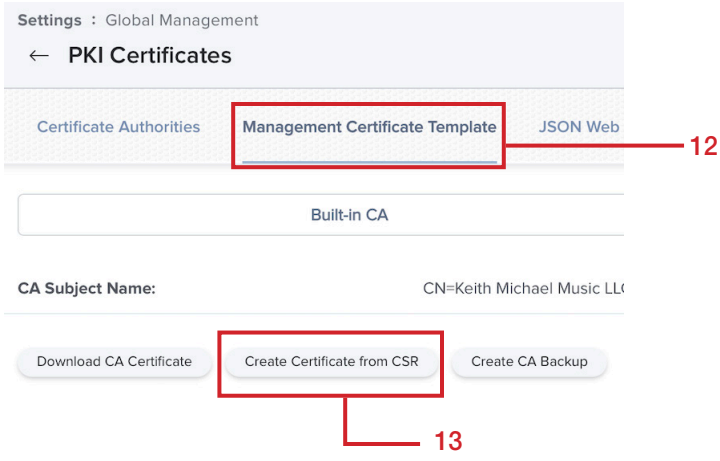
8. Log into your Jamf Pro Server.



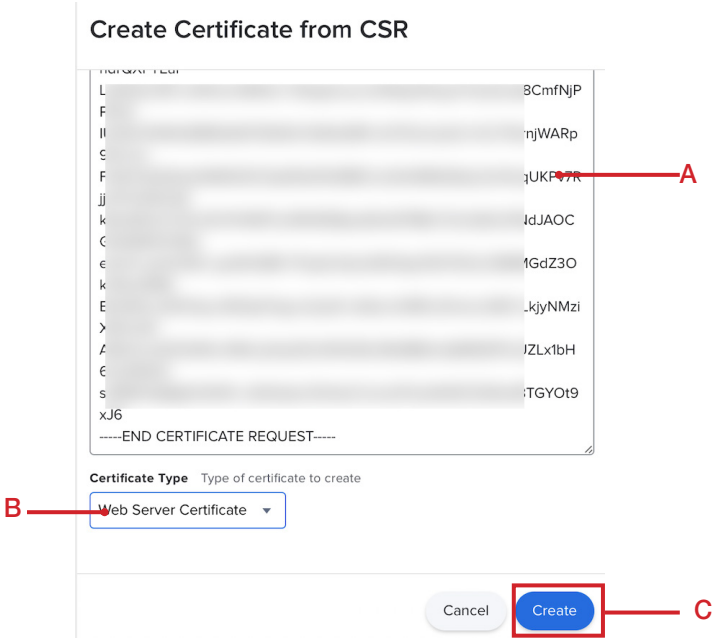
9. Click Settings (⚙) in the upper-right corner.
10. Click Global Management.
11. Click PKI Certificates.



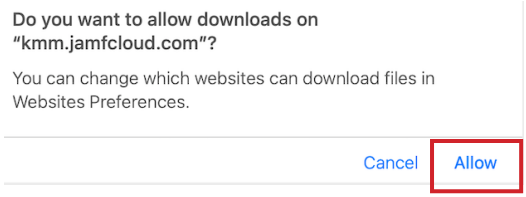
12. Click Management Certificate Template
13. Click Create Certificate from CSR.



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

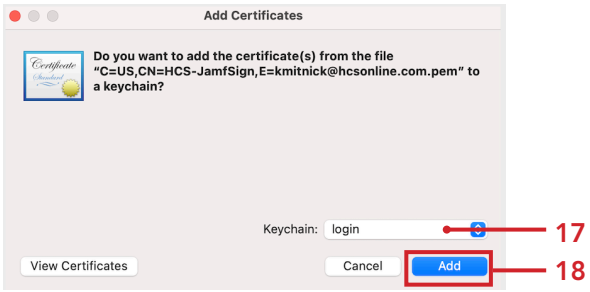


15. Click Allow.
    NOTE: After downloading the file your web browser may need to be refreshed to properly display things in Jamf Pro.

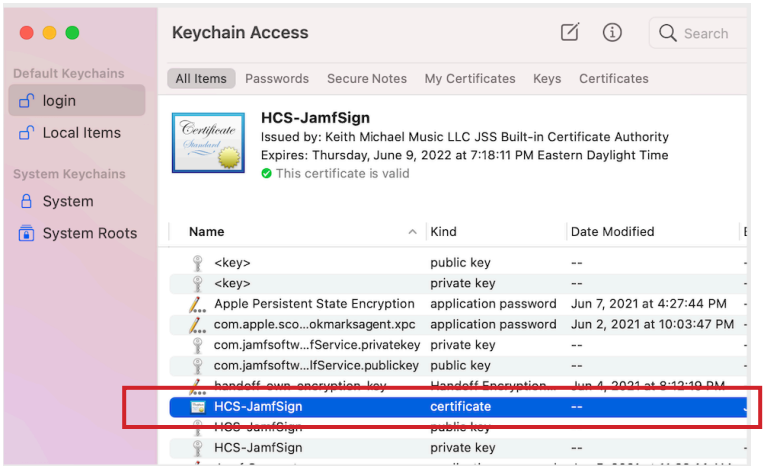


16. The certificate will download to your Downloads folder. Drag the certificate to your Desktop and double-click to open the file.

17. From the Keychain menu, select login.
18. Click Add.

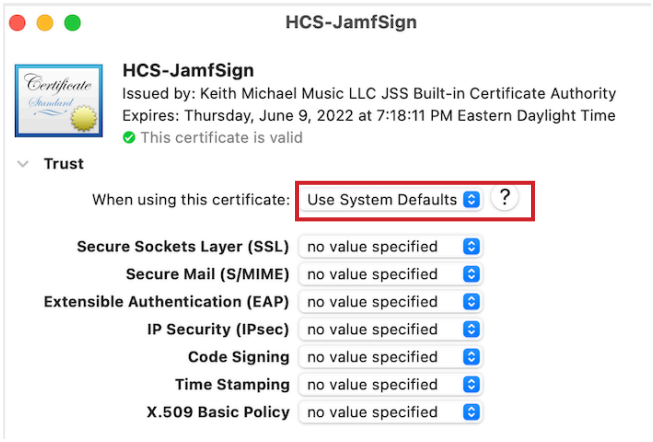


19. In Keychain Access Click your login keychain, you will see the certificate on the right side. Double click on your certificate to see more settings.

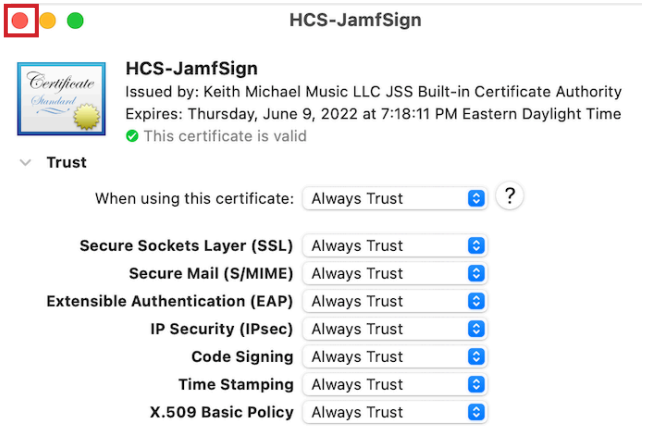


20. Expand (>) Trust to view the settings.

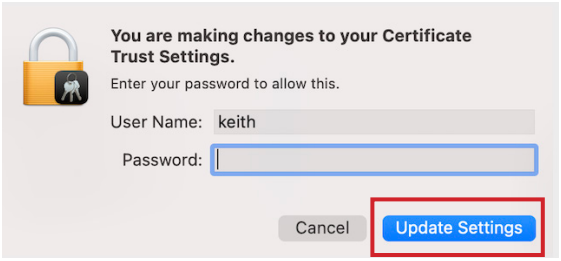
21. On the first item, When using this certificate section, click the menu and select Always Trust.



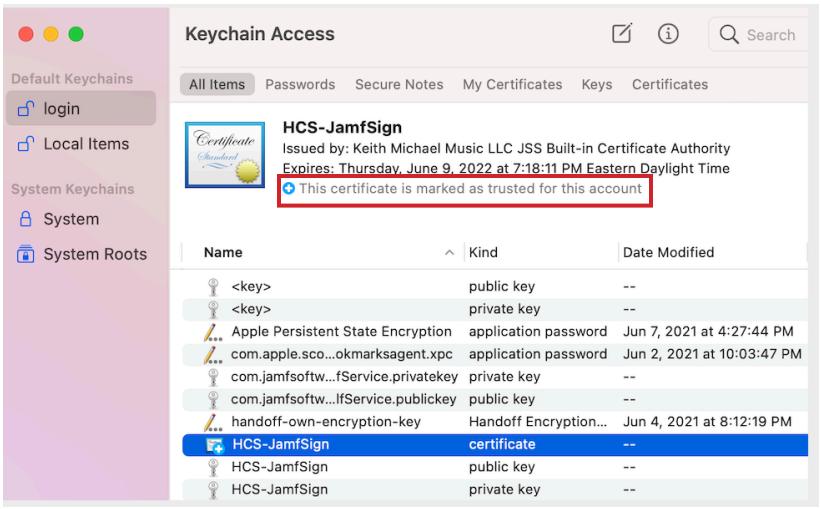
22. Close the window.



23. Enter your admin credentials and click Update Settings.



24. Confirm the certificate shows up as trusted. Quit Keychain Access.



In the next section, we will build a custom package that includes images and scripts to be used when deploying Jamf Connect.

This completes this section.

Section 4: Packaging Images and Scripts for Branding Jamf Connect

Requirements for following along with this section:

- A Mac computer running macOS 10.15.4 or later enrolled in Jamf Pro
- A code signing certificate installed on your Mac Computer
- Branding Images and Scripts
- Jamf Composer
- JC_Okta_FIles downloaded from: https://hcsonline.com/images/Apps/JC_Okta_Files.zip

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

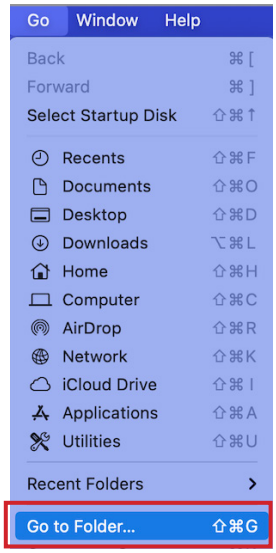
To follow along with this section you will need your branding images, Login Window scripts, and Menu bar scripts readily available. This guide assumes those items are located on your Desktop.

The recommended size for branding icons:

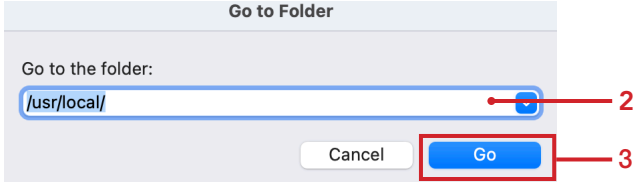
- Menu bar icons: 16x16 pixels
- Login logo: 250 x 250 pixels
- Sign in Logo 449 x 131 pixels

NOTE: This guide will use Composer for packaging. You can get Composer from your assets in your Jamf account located at https://id.jamf.com

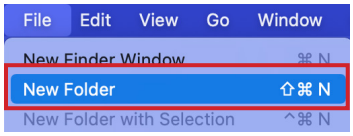
1. In the Finder, go to the Go menu and select Go To Folder.



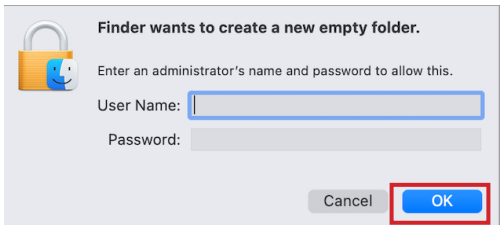
2. Enter the following path: /usr/local
3. Click Go.



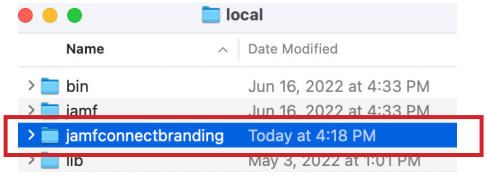
4. Create a New Folder.



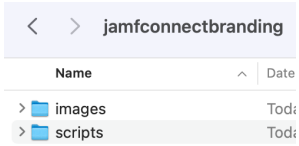
5. Enter your Admin credentials then click OK.



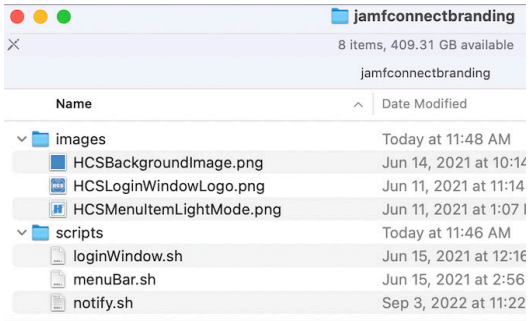
6. Name the folder jamfconnectbranding.
7. Open the jamfconnectbranding folder.



8. Follow steps 3 and 4 to create two folders within the jamfconnectbranding folder:
   - images
   - scripts



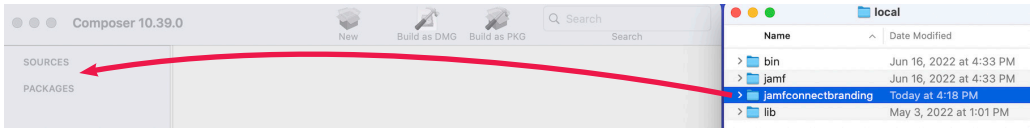
9. Drag your branding images to the Images folder. If you have scripts, drag them to the scripts folder. NOTE: You can use the sample files provided with this guide if you don't have your own scripts or images.



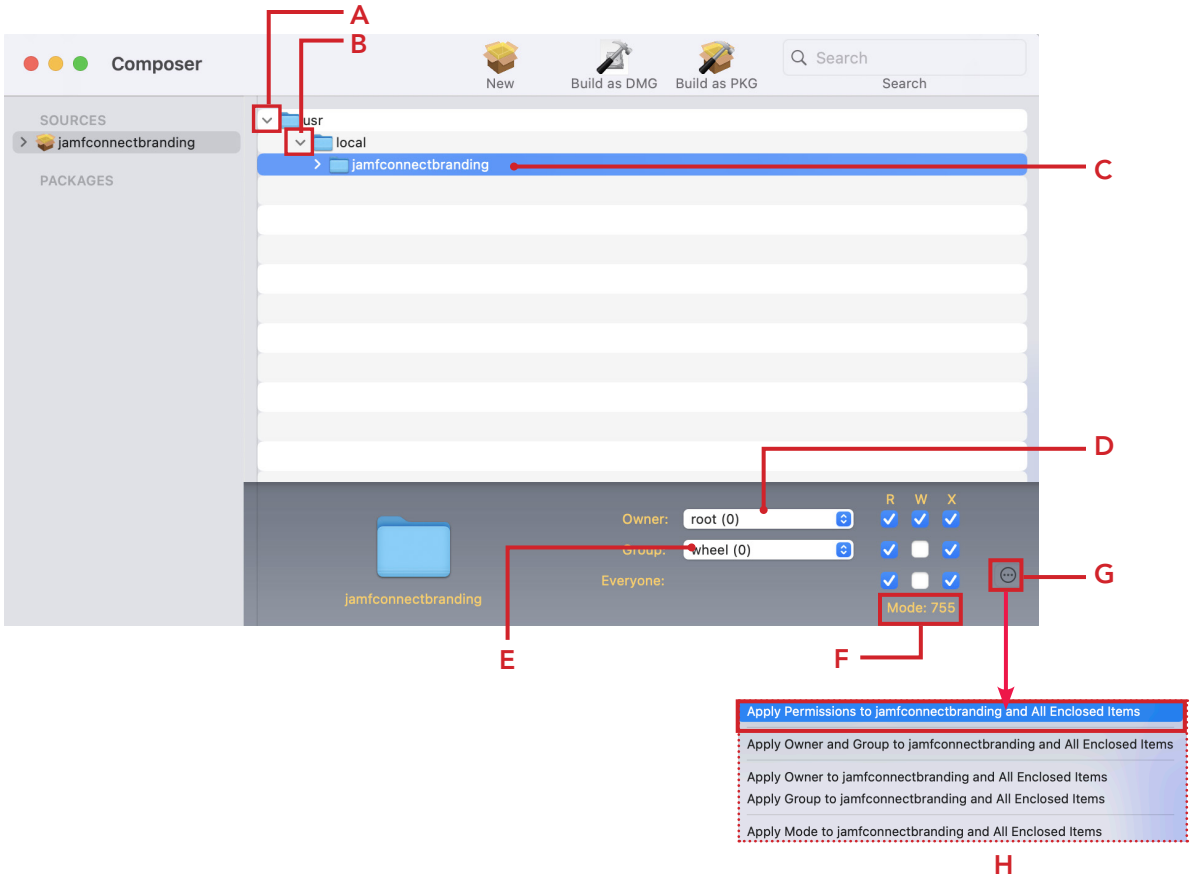
10. Launch Composer located in /Applications/Jamf Pro.

Composer

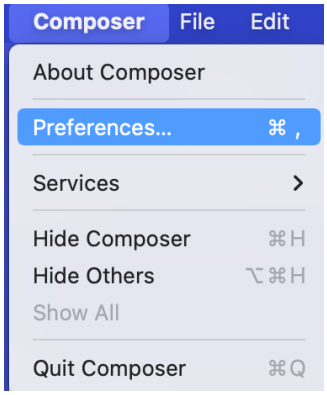
11. Drag the jamfconnectbranding folder to Sources.



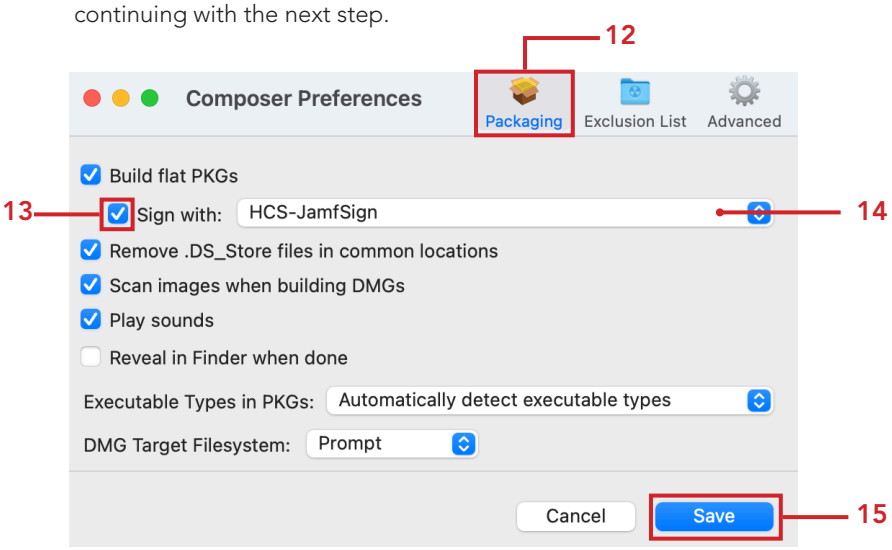
12. Configure the following:
    A. Expand the usr folder
    B. Expand the local folder
    C. Select the jamfconnectbranding folder.
    D. Change the Owner to: root
    E. Change the Group to: wheel
    F. Confirm the permissions are set to 755.
    G. Click the Apply Permissions (⋯).
    H. Click Apply Permissions to jamfconnectbranding and All Enclosed items.



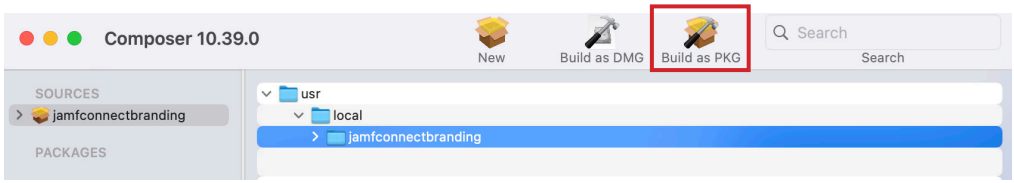
13. Click the Composer menu then select Preferences.



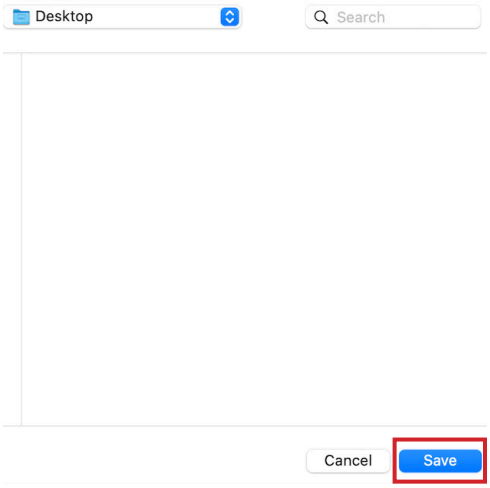
12. Click Packaging.
13. Select the checkbox for Sign with.
14. From the menu, select your signing certificate.
15. Click Save.
    NOTE: We need to sign this package if we want to use it in a PreStage enrollment in Jamf Pro. If you don't have a code signing certificate, refer to section 3 of this guide to create one before continuing with the next step.



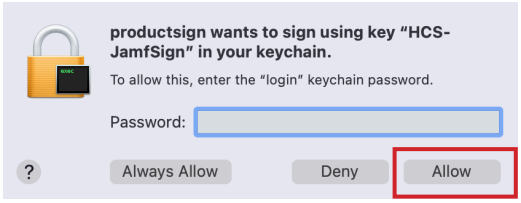
16. Confirm your settings.
17. Click Build as PKG.



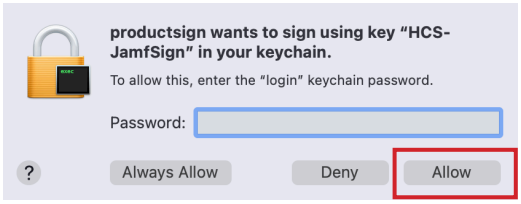
18. Save the package to your Desktop.



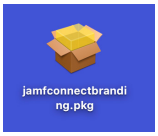
19. Enter your Admin password to sign the package.
20. Click Allow. You will see this message twice.



21. Enter your Admin password to sign the package.
22. Click Allow.



23. Confirm the package was created on your Desktop. Leave this package on your Desktop as we will need to upload it to Jamf Pro later in this guide.



In the next section, we will use the Jamf Configuration App to configure a Login Window and Menu Bar profile to customize the settings needed to use our branded images, scripts, and other configurations for Jamf Connect.

This completes this section.

Section 5: Create a Jamf Connect Login and Menu Bar Configuration Profile

In this section we will create settings for the Jamf Connect Login Window and Menu Bar using the Jamf Connect Configuration App. There are a lot of optional settings for Jamf Connect and this guide will not cover all of them. Please refer to the Jamf Connect Admin Guide for more information.

If you downloaded the sample files for this guide and want to following along, be sure to fill out all the fields as shown in the pictures in this section. There are many optional configurations discussed in this section and we will not configure all of them.

https://docs.jamf.com/jamf-connect/documentation/Jamf_Connect_Documentation.html

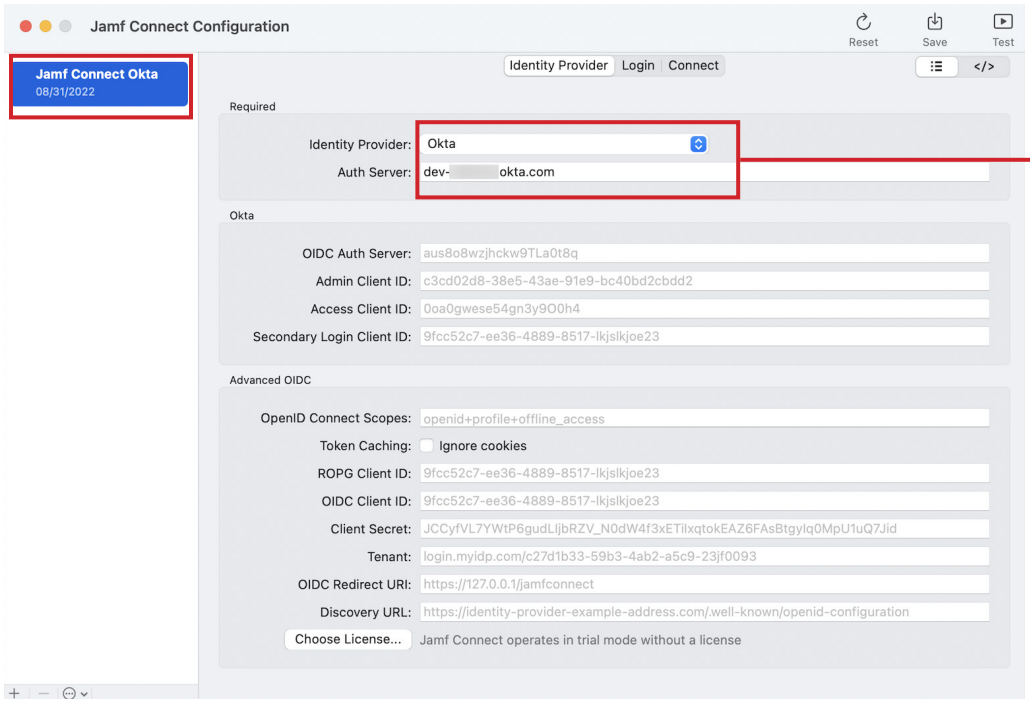
Requirements for following along with this section:

- A Mac Computer running 10.15.4 or later.
- Jamf Connect Configuration App
- Okta Client IDs file. Created in section 2 of this guide

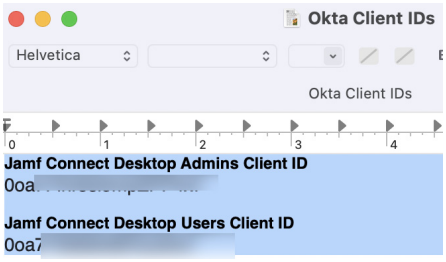
1. Open the Jamf Connect Configuration App.

Jamf Connect Configuration

2. In Section 1 of this guide, we created a configuration named Jamf Connect Okta. Select that configuration. Confirm it should have two settings configured in the Identity Provider tab. Identity Provider is Okta and the Auth Sever has your Okta domain listed. Nothing else should be configured.

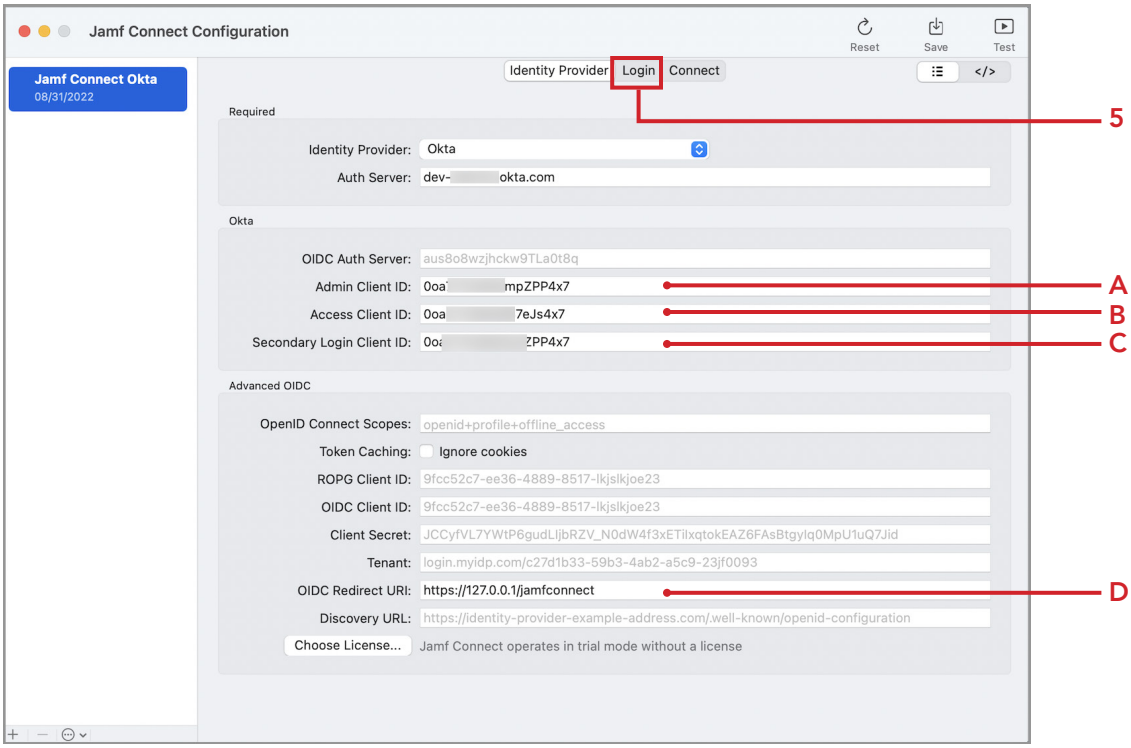


3. Open the Okta Client IDs file that we created in Section 2 of this guide.



4. In the Okta section, enter the following:
   A. Admin Client ID: Enter the client ID for the admin group that you created in Okta. This guide will use the Jamf Connect Desktop Admin group.
   B. Access Client ID: Enter the client ID for the standard user group that you created Okta. This guide will use the Jamf Connect Desktop Users group.
   C. Secondary Login Client ID: This guide will enter the client ID of the Jamf Connect Desktop Admin group.
   NOTE: The Secondary Login Client ID field can be configured in multiple ways. This field is used to restrict who can make a second account on a client device. It could be an additional user group or and existing user group. This is most commonly configured with the admin group client ID for added security.
   D. In the Advanced OIDC section: OIDC Redirect URI: https://127.0.0.1/jamfconnect

5. Click the Login.



6. The Login tab has many options and we will not cover all of them in this guide however, I will discuss some of them briefly. Configure these settings to your needs.

User Creation

Initial Password: Create a separate local password - In order to set this key to false, you need to check the box next to Create a separate local password, then un check it. This will generate the XML key value pair and set it to false. If set to true, it would generate a different password than the one you used to login with your Okta credentials which may confuse your users.

User Creation

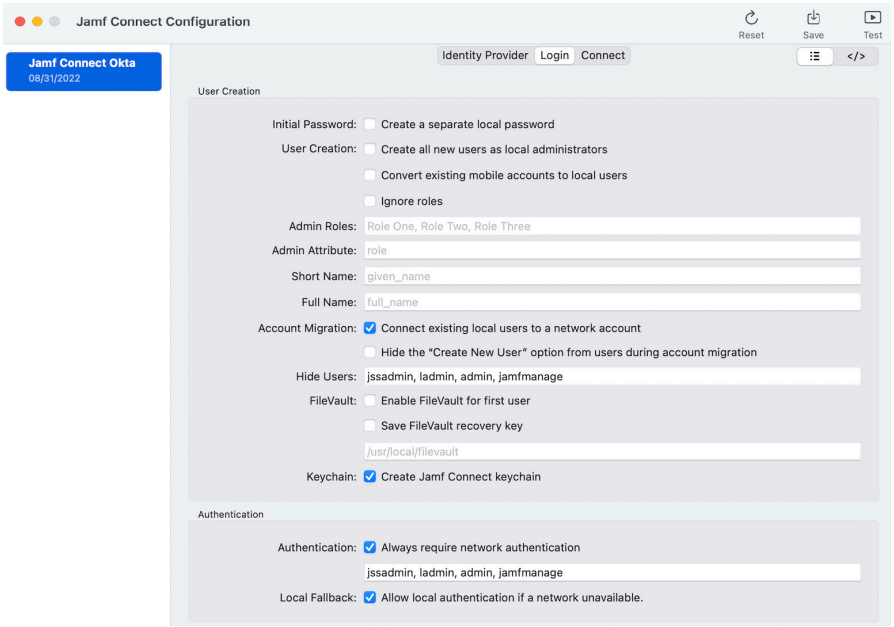
- Create all new users as local administrators. Check this if you want all users to be created as admins when they log in with their Okta credentials.
- Convert existing mobile accounts to local users. Check this if you want to migrate your mobile accounts to local Mac accounts.
- Ignore roles. Check this is you want to ignore the role of the user in Okta. I.E. If a user is an admin in Okta but you want them to be a standard user on their Mac.

Account Migration

- Check this if your users already have a local account on the Mac and they want to link it to their Okta login. This will avoid the user having two separate accounts when they log in with their Okta credentials. It adds an alias to their existing user account on the Mac with the Okta username.
  NOTE: If the name of your home folder matches your Okta account, you will not be prompted to migrate when logging in. It will use your exisiting home folder.
- Hide the "Create New User" option from users during account migration. Check this if you don't want a user to create a new account during the migration process from a mobile account to a local Mac account. This can avoid accidentally creating a second account for the user.
- Hide Users. If you have local administrators on the Mac and you don't want to link them with a network account when they log in, add their account short name to the field. If there are multiple users, separate them with a comma.
- FileVault. Since this guide is written using Jamf Pro as the MDM server, I recommend handling FileVault using your Jamf Pro server and allow the key to be escrowed back to the Jamf pro server.
- Keychain. Check the box to create the Jamf Connect Keychain.

Authentication

- Authentication: Check the box to Always require network authentication. This provides added security.
- In the field below, you can enter the short names of accounts that can bypass requiring a network connection to authenticate. Useful for local Mac admin accounts.
- Local Fallback: Check the box to Allow local authentication if a network is unavailable. This is useful when you don't have an internet connection but still need to log in to your Mac. Works in conjunction with the Always require network authentication check box.



7. Continuation from Step 6.

Appearance (optional)

- Internet: Check the box to Allow network selection. This will allow you to select a Wi-Fi network at the Login Window.
- Login Window Message: This will show a custom message at the login window
- Background: Enter the path of the background image you want to use at the Login Window.
- Login Logo: Enter the path of the Login Logo image you want to use at the Login Window.
- Local Auth Button: You can change the name of the local auth button to a custom name.
- Hide restart and Hide shutdown. Check the box if you want to hide these buttons at the Login Window.

Help section: (Optional)

- Help URL: URL to a help page of your choosing.
- Local Help File: You can create a custom help file that lives in the same location on all Macs.

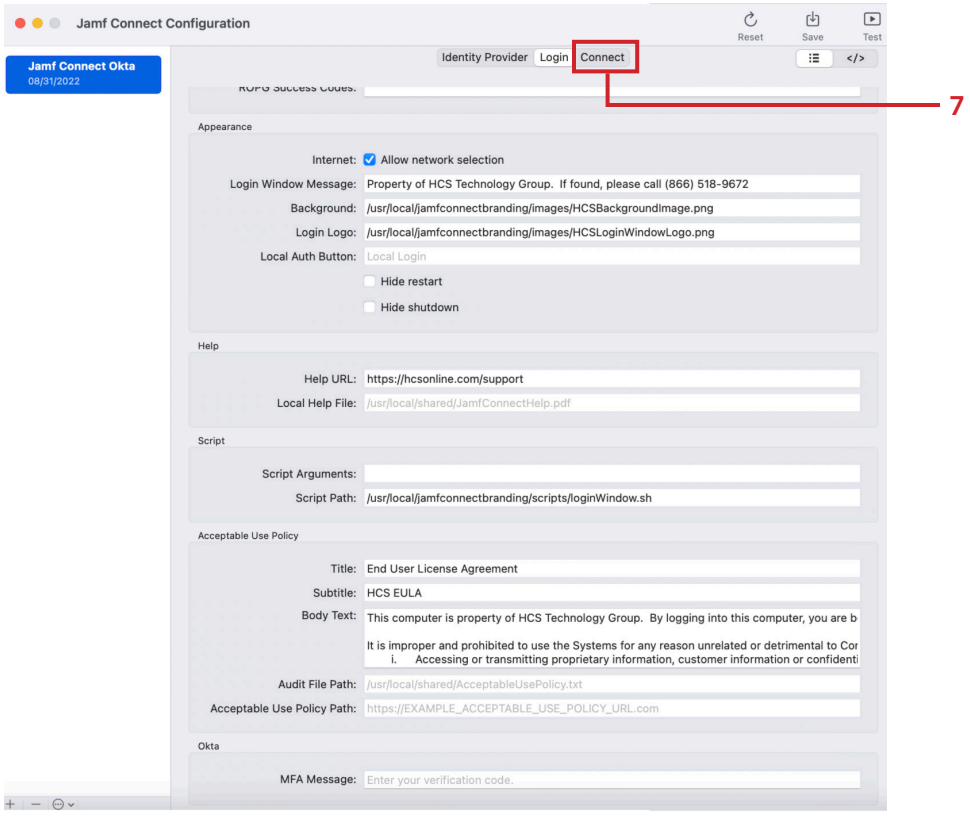
Script (optional)

- Script Arguments: You can run commands entered in this field. For example, if you wanted to run a script on a successful Login, enter the path to the script you want to run in the field. See the Script Path in the picture below.
- Script Path: Location of a script that will run at login on all Macs.

Acceptable Use Policy (optional)

- You have the option of entering in text in all the the following fields: Title, Subtitle, Body Text.
- Audit File Path: You can specify a file location to record all users that have accepted the Acceptable Use Policy. NOTE: Jamf recommends using /Users/Shared as the path.
- Acceptable Use Policy Path: You can create your own acceptable use policy and place it on a website or in a local file on all Macs in the same location.
- MFA Message: You can add custom text to be displayed to the user telling them to enter their Okta verification code sent to their device.

8. After reviewing, click Connect.



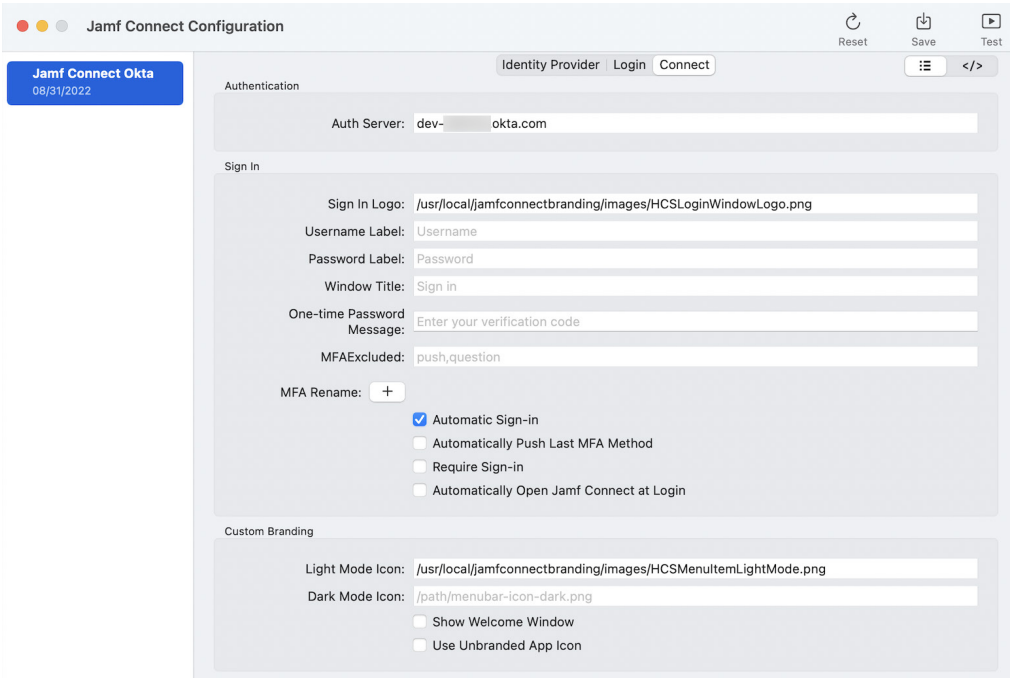
9. Under **Authentication**, in the Auth Server field, will show the URL of your Okta server.

   Sign In (Optional).

   - Sign In Logo: Location of the branded logo to use at the Jamf Connect sign in window.
   - The following field names can be customized to your needs. For example, the Username Label can be changed to a name of your choosing like Email address.
   - Username Label, Password Label, Window Title, One-time-Password Message, MFA Excluded.
   - Automatic Sign-In - Check this box to enable Jamf Connect to automatically sign in using your stored credentials in your keychain.

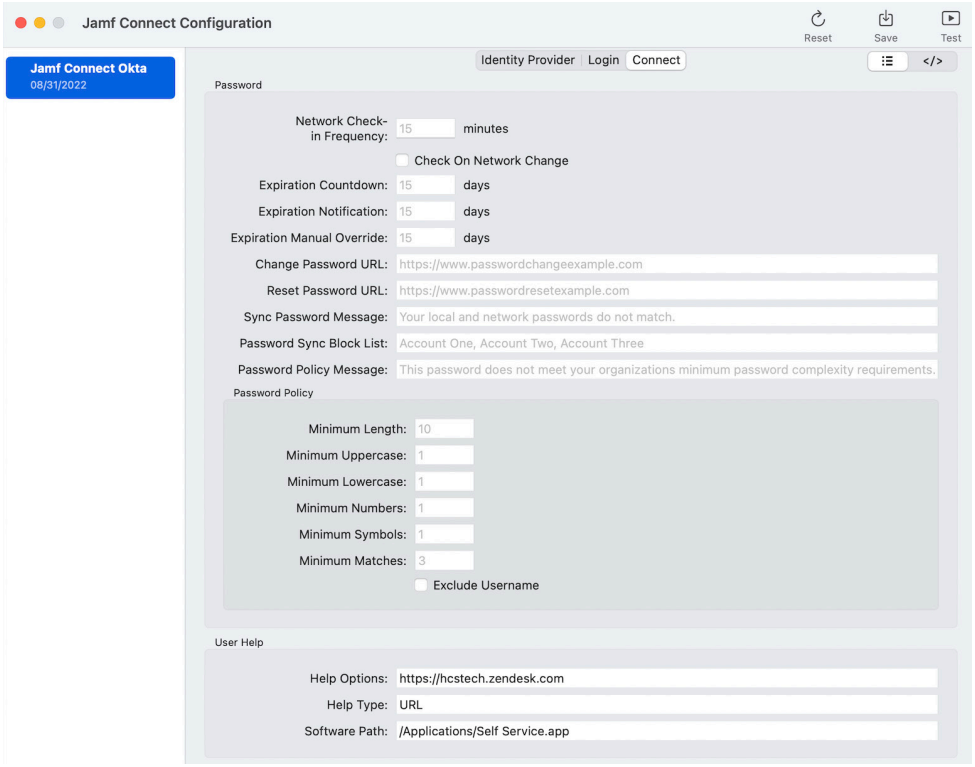
   Custom Branding (Optional).

   - Light Mode Icon: Location of the Menu Bar icon on all Macs using Jamf Connect.
   - Dark Mode Icon: Location of the Menu Bar icon on all Macs using Jamf Connect.
   - Show Welcome Window - I recommend checking the box then un checking the box to disable the Welcome Message from showing up on each login. That will generate the xml key value pair and set it to false.
   - Use Unbranded App Icon. This will replace the Jamf Connect Menu Bar icon with a generic logo (Shown to the right). Use this if you don't want the users to see the Jamf icon in the menu bar or if you don't have your own branded icon. This guide will use a branded icon so there's no need to check this box.



10. Password (Optional).
    - Network Check-in Frequency: By default, Jamf Connect will check every 60 minutes to see if the Okta password matches the local account of the user on the Mac. If they are out of sync, Jamf Connect will prompt the user to sync them. If you want to change this to happen more frequently, add a number to this field.
    - The other items in the password section will not be discussed in this guide.
    - Please refer to the Jamf Connect admin guide for more info on these items.

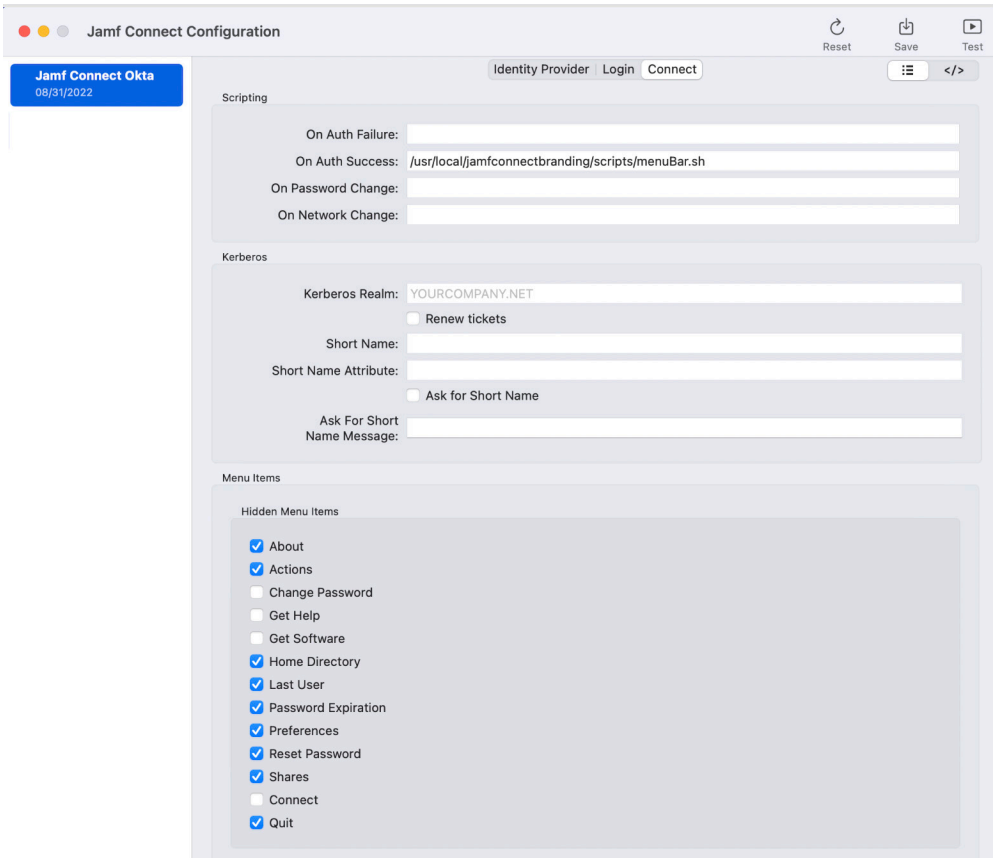
    User Help (Optional).
    - Help Options: Enter a URL to a help page or path to a help file located on all Macs using Jamf Connect.
    - Help Type: The type of help option to be used by Jamf Connect. URL or File
    - Software Path: Enter the path to an application that you would like to open via the Jamf Connect Menu Bar.



11. Scripting (Optional).
    - You can add the path to a script in each field listed. For example, if you wanted to run a script on a successful Authentication, enter the path to the script you want to run in the field. See the path in the On Auth Success field in the picture below.

Kerberos (Optional).
- If you require Kerberos, enter the information for your Kerberos Realm in this section. NOTE: Kerberos will require a connection to an on premise Active Directory server.

Menu Items (Optional).
- You can enable or disable any of the items listed in this section from showing up in the Jamf Connect Menu bar.

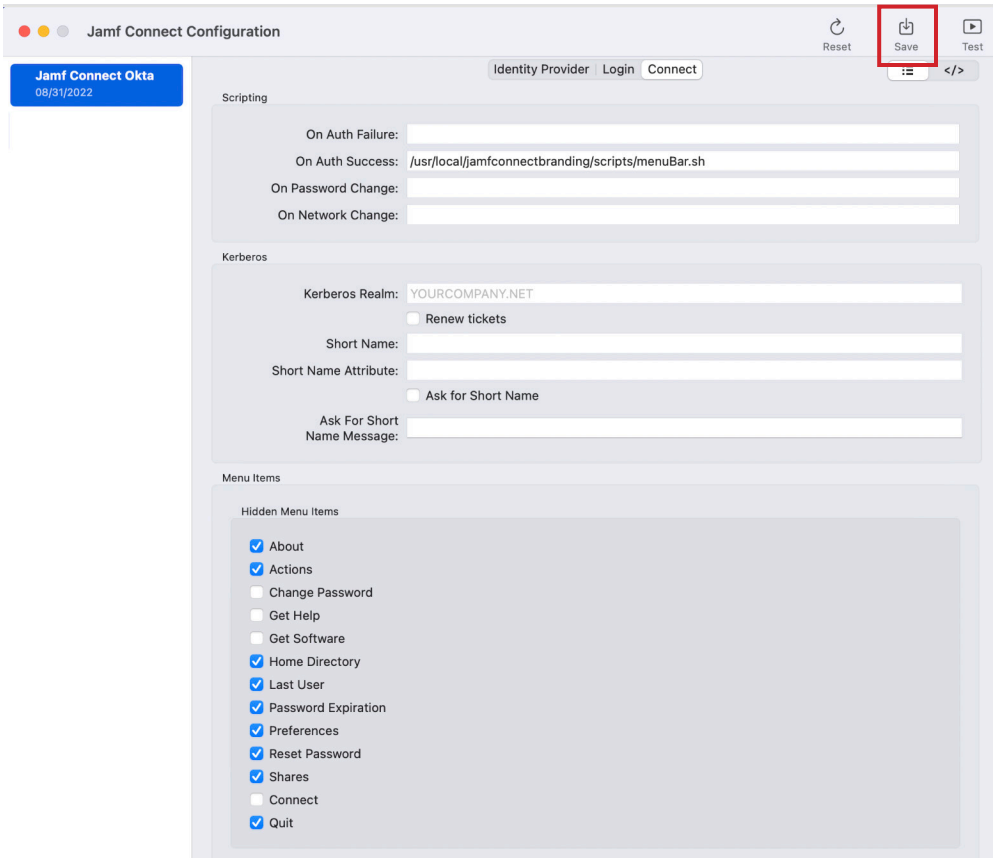


12. Custom Menu Items (Optional).
    - You can change the names of the items listed in the Jamf Connect Menu Bar to fit your needs. For example, the Get Help menu item can be changed to Open a Help Desk Ticket. This will use the URL if you entered one in the Help section in step 10.

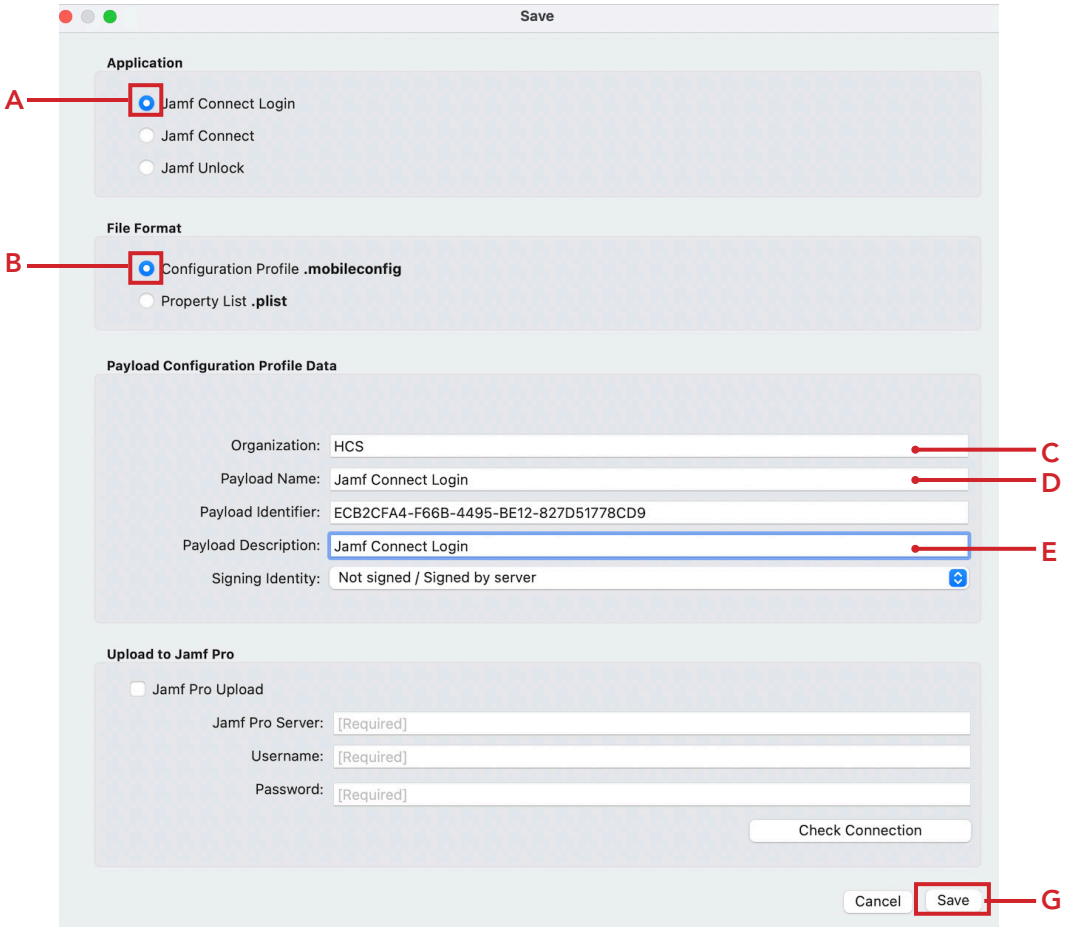
    Web Browser (Optional).
    - Select a web browser of your choosing, then check the box to Launch Browser. This will open the browser of your choosing when accessing the Okta dashboard.

    Jamf Unlock (Optional).
    - Jamf Unlock is a mobile app that enables users to unlock their Mac without using a password. With Jamf Unlock, users complete a setup process to generate identity credentials (a certificate) on their mobile device and pair the device with their Mac.

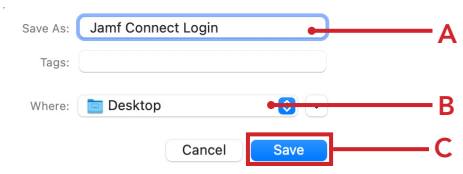
13. Click Save.



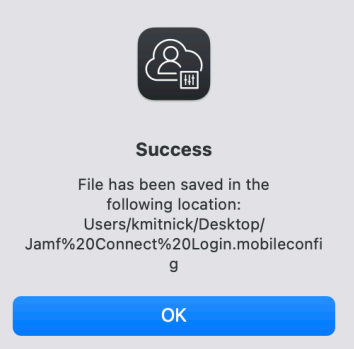
14. Configure the following:
    A. Select the radio button for Jamf Connect Login.
    B. Select the radio button for Configuration Profile
    C. Organization Name: Enter your organizations name. This guide will use HCS.
    D. Payload Name: Jamf Connect Login
    E. Payload Description: Jamf Connect Login
    F. Leave everything else at their default settings
    G. Click Save.



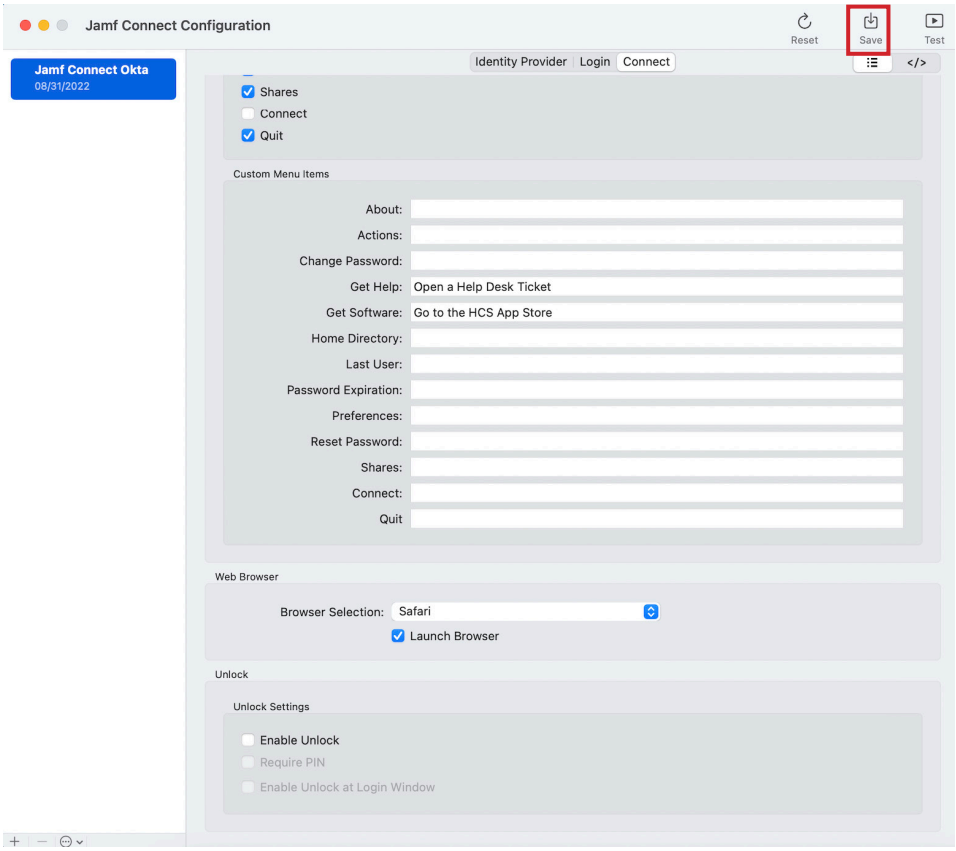
15. Configure the following:
    A. Save As: Jamf Connect Login
    B. Where: Desktop
    C. Click Save.



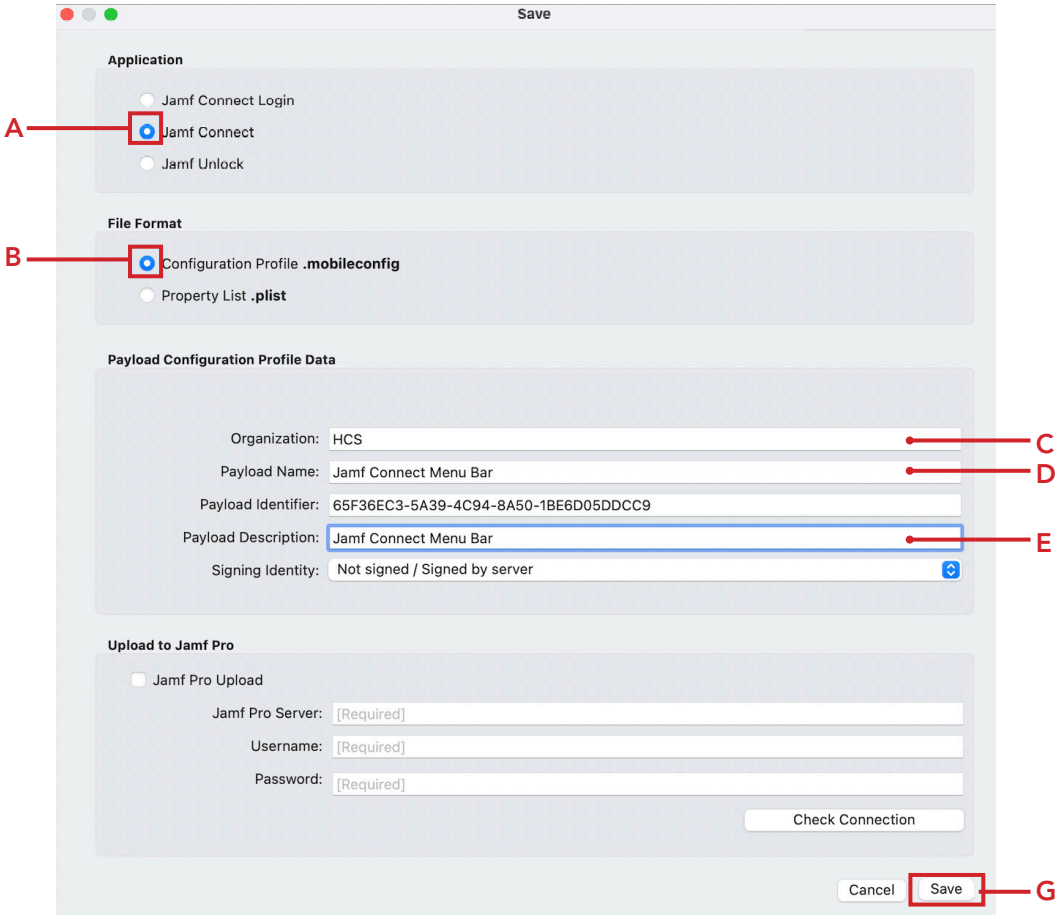
16. Click OK at this message.



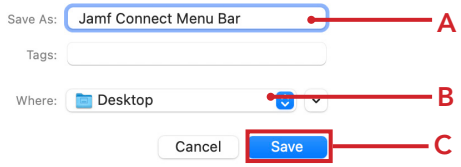
17. Click Save.



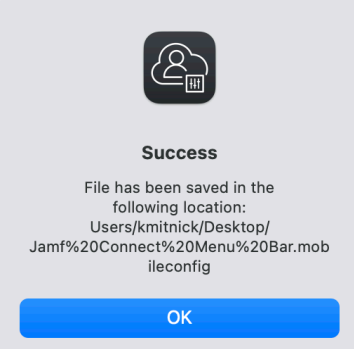
18. Configure the following:
    A. Select the radio button for Jamf Connect.
    B. Select the radio button for Configuration Profile
    C. Organization Name: Enter your organizations name. This guide will use HCS.
    D. Payload Name: Jamf Connect Menu Bar
    E. Payload Description: Jamf Connect Menu Bar
    F. Leave everything else at their default settings
    G. Click Save.



19. Configure the following:
    A. Save As: Jamf Connect Menu Bar
    B. Where: Desktop
    C. Click Save.



20. Click OK at this message.



21. Confirm that you have 2 configuration profiles saved on your Desktop.

In the next section we will install the two configuration profiles we just created along with Jamf Connect. Best practice is to always test your configuration profiles by manually installing the configuration profiles and Jamf Connect on a Mac manually. Once everything is working as expected, we can transfer all the items to the Jamf Pro server and test deploying Jamf Connect from Jamf Pro.

This completes this section.

Section 6: Manually Installing Jamf Connect on a Mac Computer

In this section we will install the two configuration profiles we created in section 5 along with Jamf Connect. Best practice is to always test your configuration profiles by manually installing the configuration profiles and Jamf Connect on a Mac Computer. Once everything is working as expected, we can transfer all the items to the Jamf Pro server. We will also test a Login Window and Menu Bar script to make sure all is working as expected.

Requirements for following along with this section:

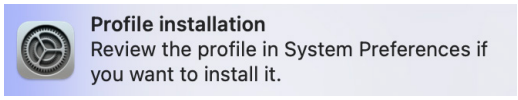
- A Mac Computer running 10.15.4 or later.
- Jamf Connect Installer version 2.14.0
- jamfconnecbranding.pkg - We created this in section 4.
- Okta login credentials for admin and standard user accounts.
- Login Window and Menu Bar Scripts (Optional)

NOTE: Login Window and Menu bar scripts are included with the sample files for this guide. If needed, get them here: https://hcsonline.com/images/Apps/JC_Okta_Files.zip

Before we install the Jamf Connect application, the configuration profiles need to be installed first. If you install Jamf Connect before installing the configuration profiles, it will have no configuration settings and will fail.

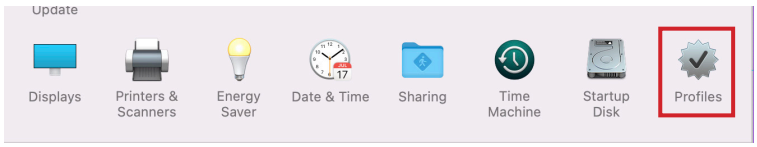
1. Double Click the Jamf Connect Login.mobileconfig profile.

2. Confirm a notification appears to ask you to review the profile.

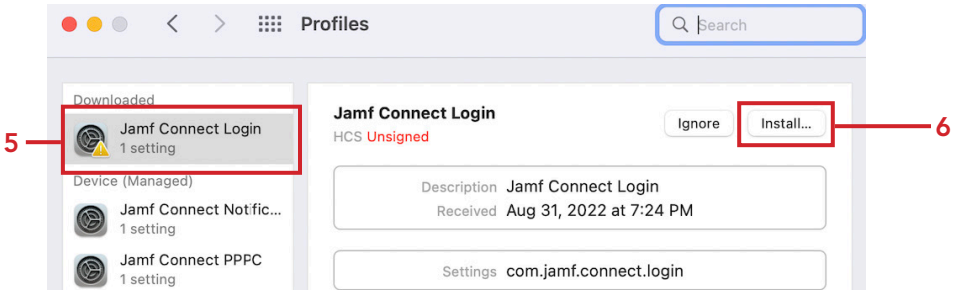


3. Open System Preferences.

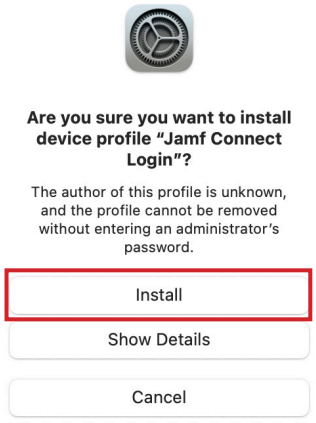
4. Click Profiles.



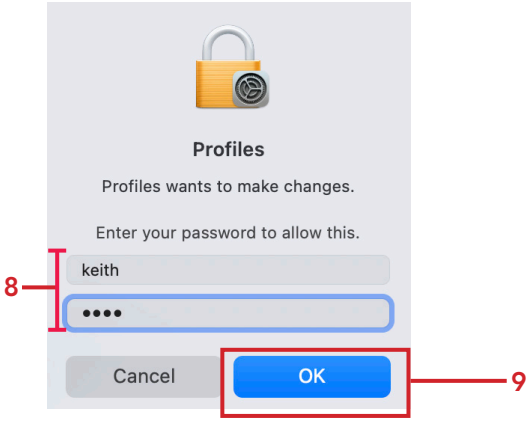
5. Click the Jamf Connect Login profile.
6. Click Install.



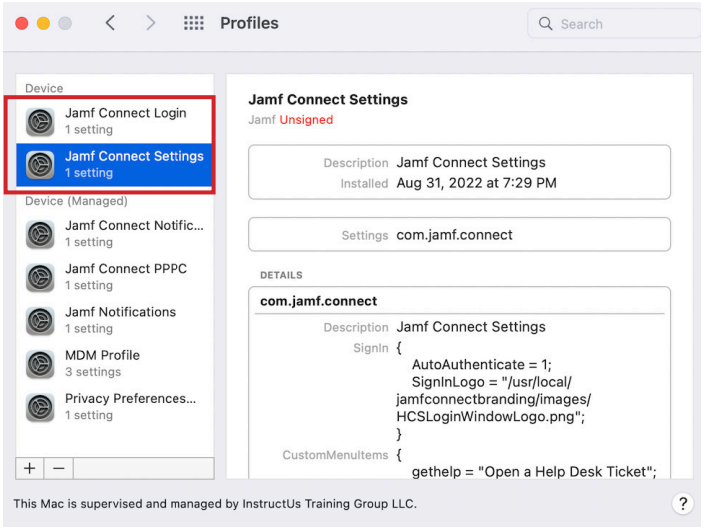
7. Click Install.



8. Enter your Admin credentials.
9. Click OK.

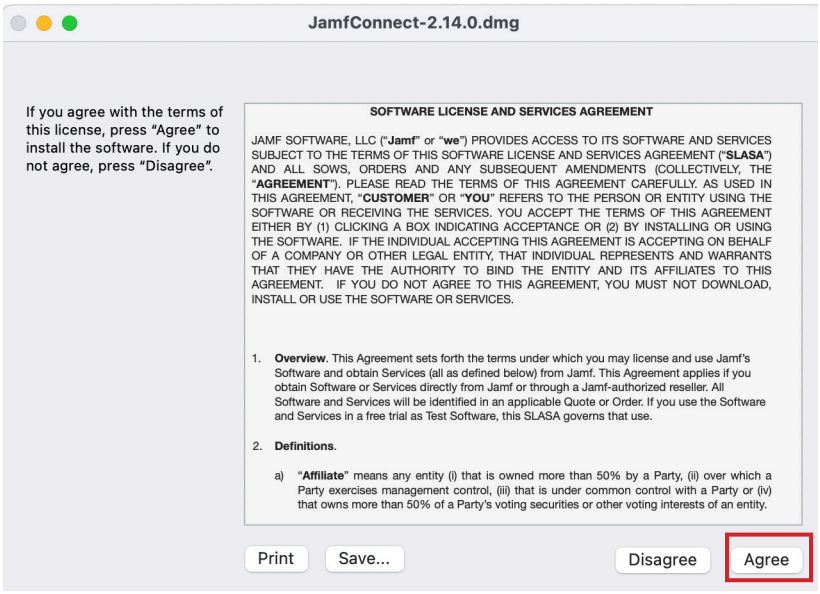


10. Follow steps 1 -7 to install the Jamf Connect Menu Bar.mobileconfig profile. Once done, you will end up with both configuration profiles as shown below.
    NOTE: The Jamf Connect Menu Bar profile will show up as Jamf Connect Settings.

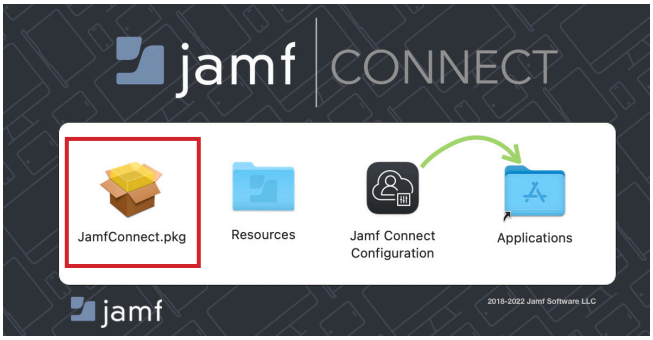


11. Open the Jamf Connect-2.14.0.dmg.

12. Click Agree.



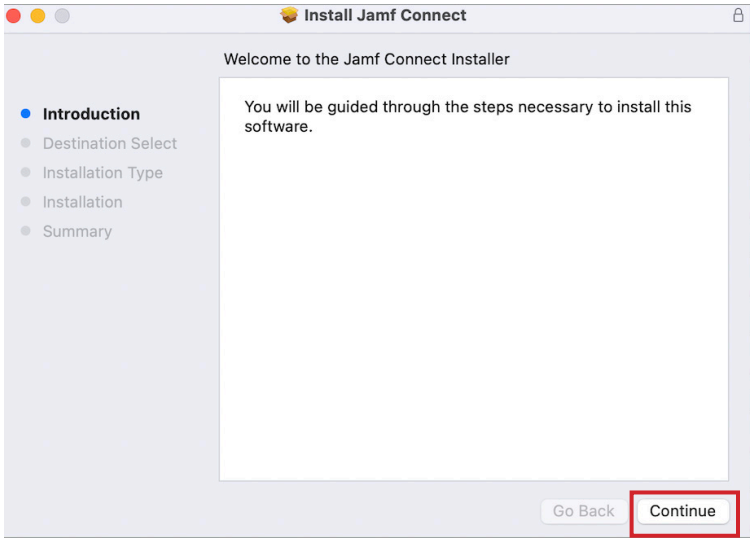
13. Drag the JamfConnect.pkg file to the Desktop. We will need to upload this to the Jamf Pro server later in this section.



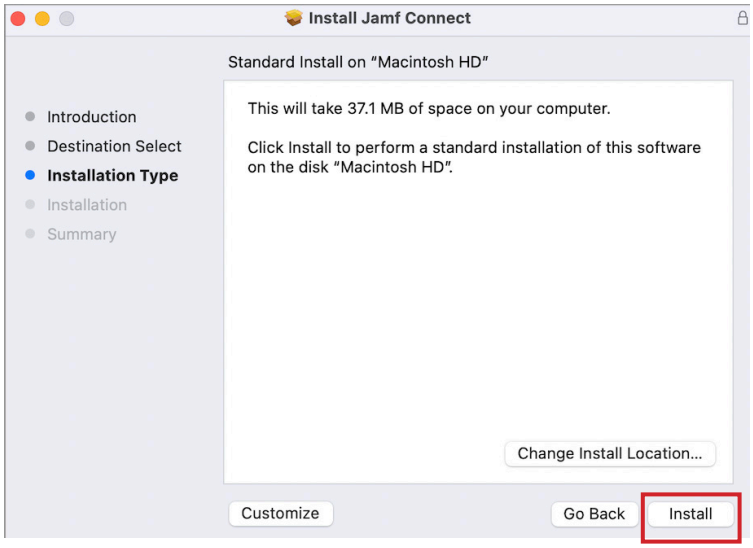
14. Open the Resources folder and drag the JamfConnectLaunnchAgent.pkg to the Desktop. We will need to upload this to the Jamf Pro server later in this section.

15. Double click the JamfConnect.pkg file on the Desktop.

16. Click Continue.

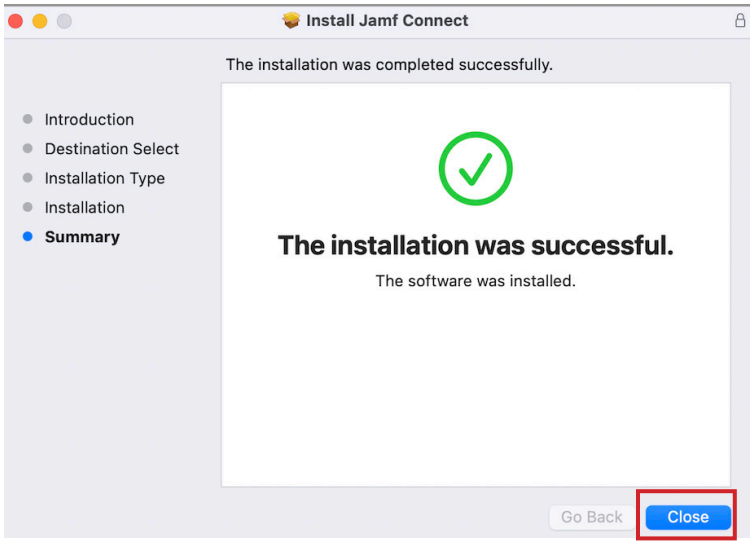


17. Click Install.



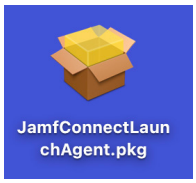
18. Enter your admin credentials then click Install Software

19. Click Close.

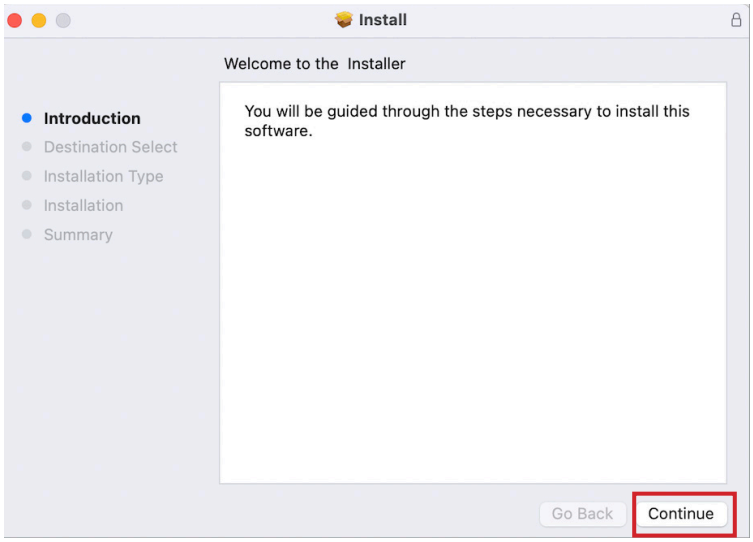


20. Close the Jamf Connect Sign In window.

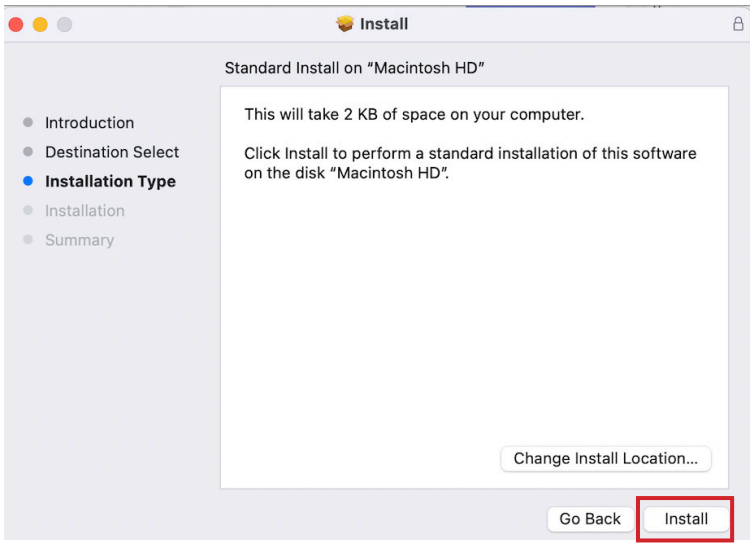
21. Double click the JamfConnectLaunchAgent.pkg file on the Desktop.
NOTE: This package will install a launch agent that will start Jamf Connect on startup.



22. Click Continue.

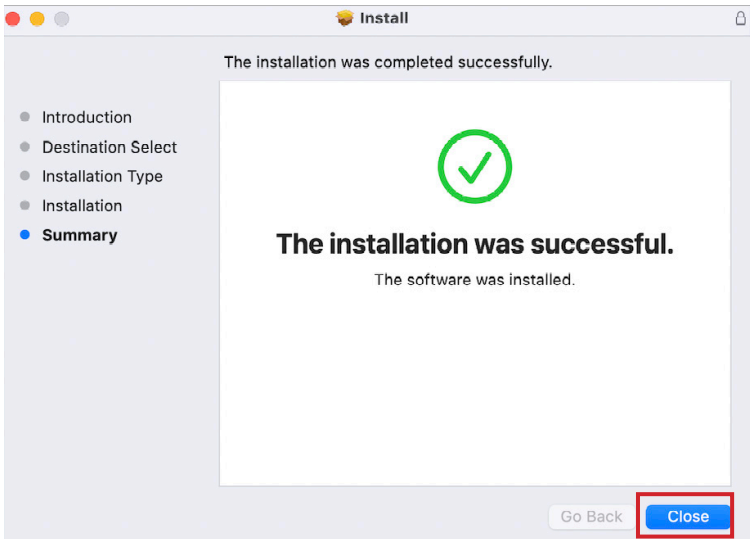


23. Click Install.



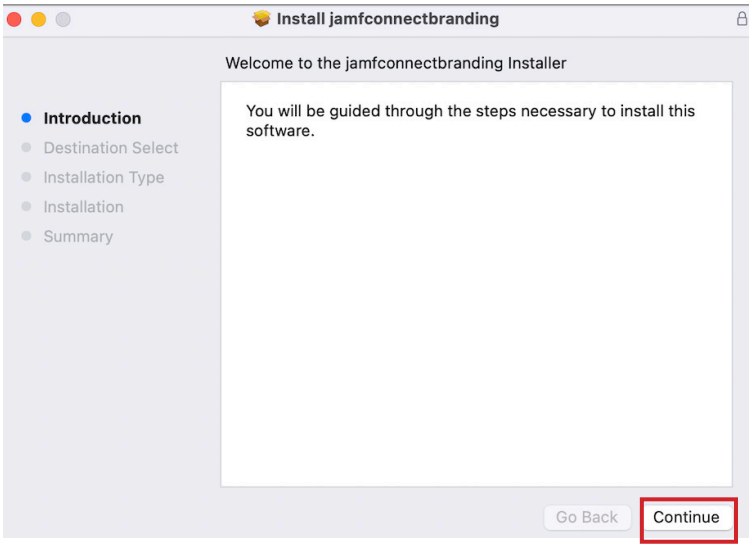
24. Enter your admin credentials then click Install Software.

25. Click Close.

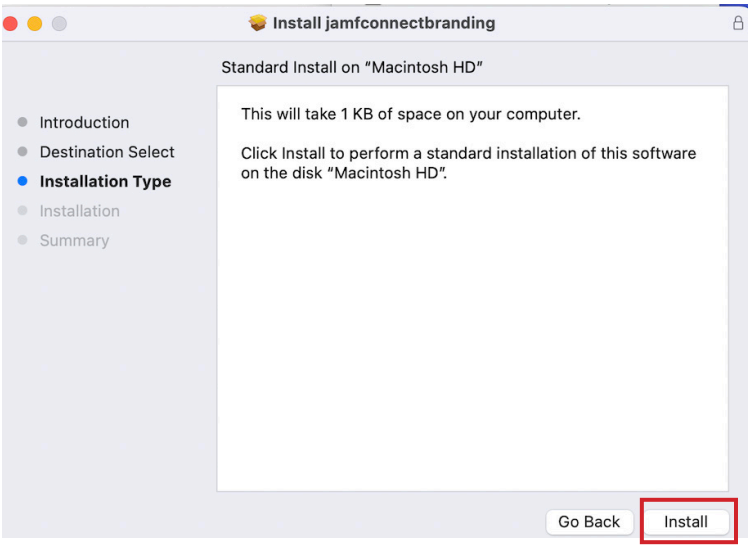


26. Double Click the jamfconnectbranding.pkg that we created in section 4 of this guide. This package should be on your Desktop and includes the images and scripts to customize Jamf Connect.

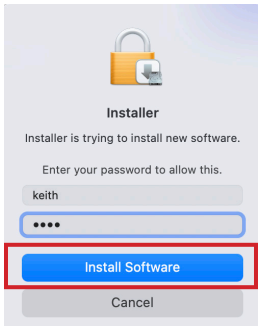
27. Click Continue.



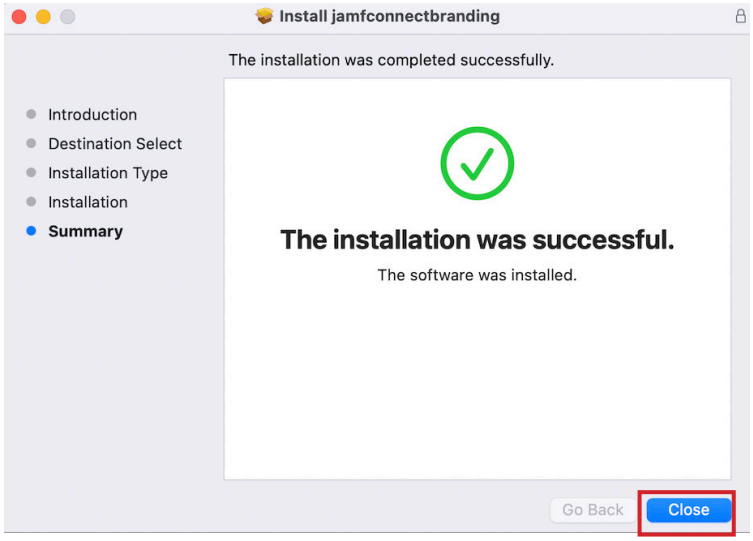
28. Click Install.



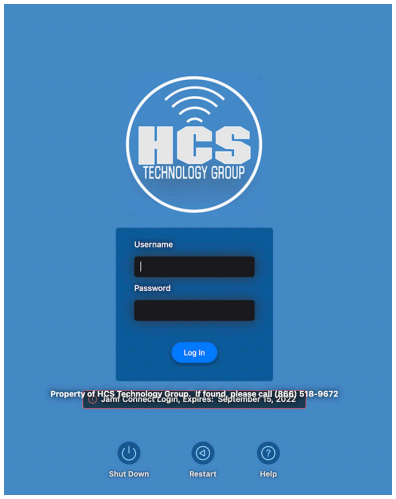
29. Enter your admin credentials then click Install Software.



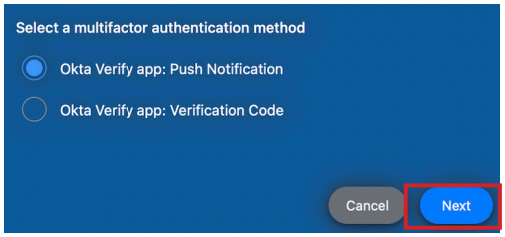
30. Click Close.



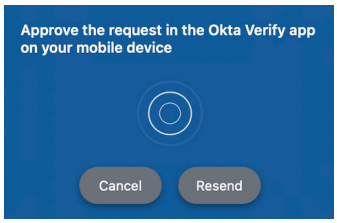
31. Logout of your Mac computer. If all went well, you should be greeted with the Jamf Connect Login Window. Enter your Okta credentials and click Log In.
NOTE: We did not add the Jamf Connect License so the login window will show as a Trial Version. We will add the Jamf Connect License in a later section. Also notice the branded logo, solid blue background, and the Wi-Fi icon all appear at the Login Window. Our customizations are working!



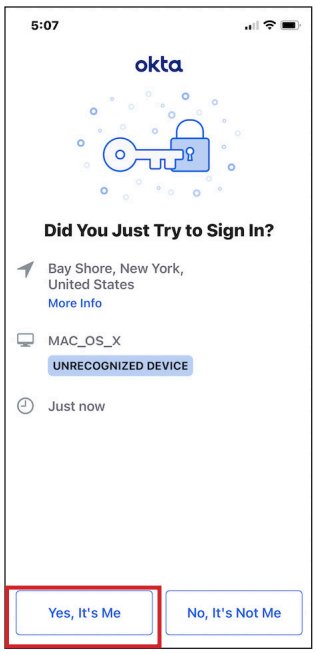
32. Click your MFA authentication method. This guide will use a Push Notification. Click Next.



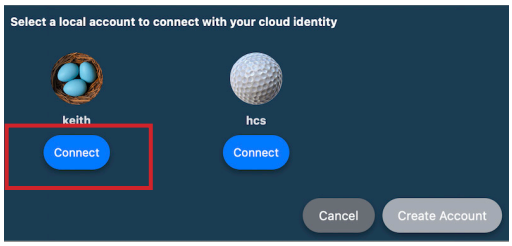
33. You will be prompted with the message below and a notification will be sent to your phone.



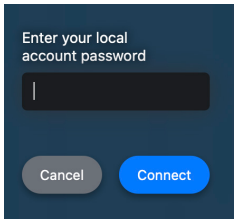
34. You will get the message below on your phone, Tap Yes, It's Me.



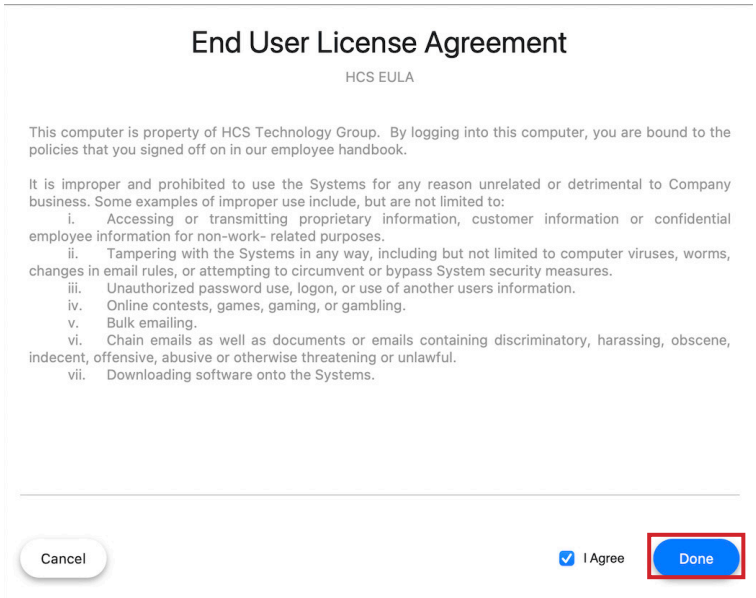
35. If you have an existing account on your Mac Computer that you want to link to your Okta credentials, click it at the window below. You also have the option to create a new account on the Mac by clicking the Create Account button. This guide will choose the existing keith account.
    NOTE: If you click an existing account at the window below and that account is a mobile account, It can be converted to a local user account if you clicked "Convert existing mobile accounts to local users " in your Jamf Connect Login settings.



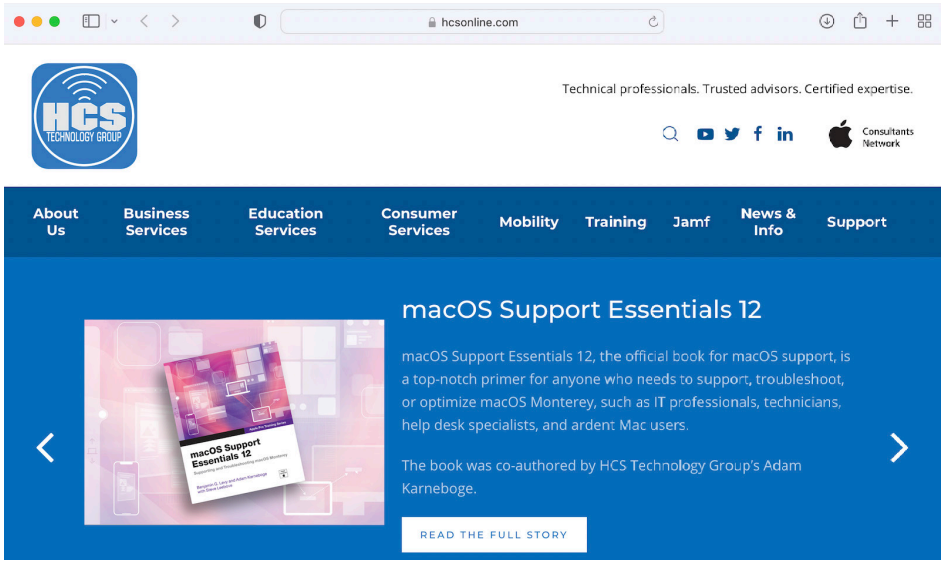
36. You will be prompted for the password of the LOCAL Mac account. In this case, the keith account. Enter your password and click Connect.
    NOTE: Do not enter your Okta password at this screen. This is your LOCAL Mac account password. Once entered, it will be synced to your Okta password and you will use your Okta password going forward to log in to your Mac Computer.



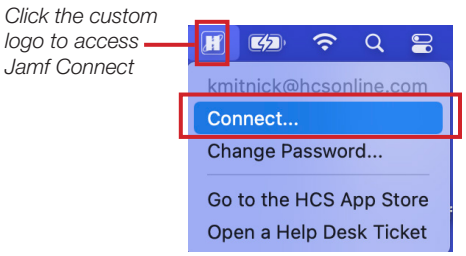
37. We configured the EULA in our Jamf Connect Login profile so we are prompted with the EULA. click I Agree, then click Done.



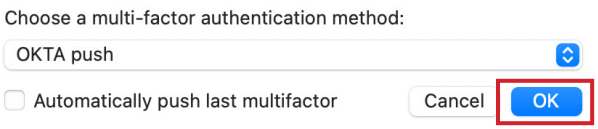
38. We configured a login script in our Jamf Connect Login settings. This guide uses a script to open Safari and go to https://hcsonline.com. Our login script is working!



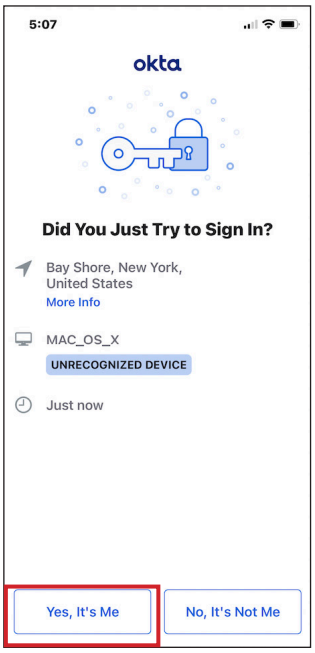
39. We configured a Menu Bar script in our Jamf Connect Menu Bar settings. This script will run when a successful connection is made to Okta. Re-Connect to Okta by clicking the Jamf Connect Menu Bar icon, which should be customized to your branded logo if you followed along with this guide, and click Connect.



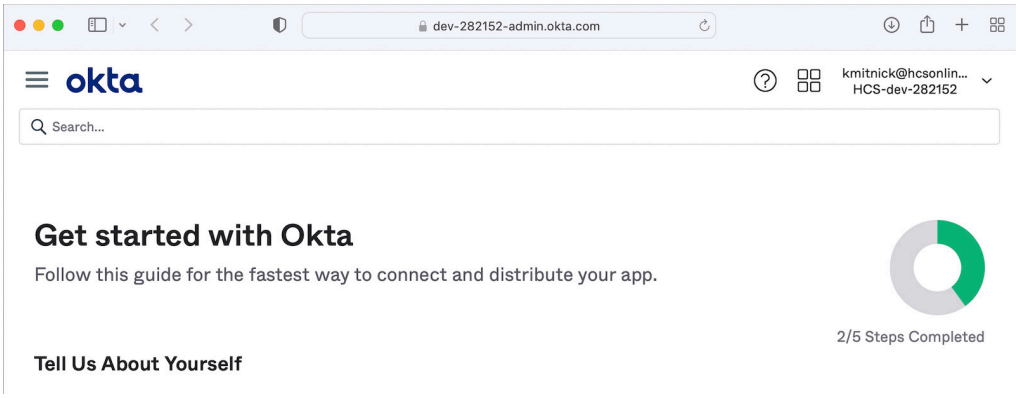
40. At the message below, click OK.



41. You will get the message below on your phone, Tap Yes, It's Me.



42. If the connection was successful, Safari will open and will sign you into your Okta user account. Our Menu Bar script is working!



In the next section we will transfer all the required Jamf Connect files and installers to a Jamf Pro server so we can deploy Jamf Connect via Jamf Pro.

This completes this section.

Section 7: Configure Jamf Pro to Deploy Jamf Connect

In this section we will upload all the required installation packages for Jamf Connect, create configuration profiles with the settings for Jamf Connect, and create a PreStage enrollment to deploy Jamf Connect via Automated Device Enrollment.

Requirements for following along with this section:

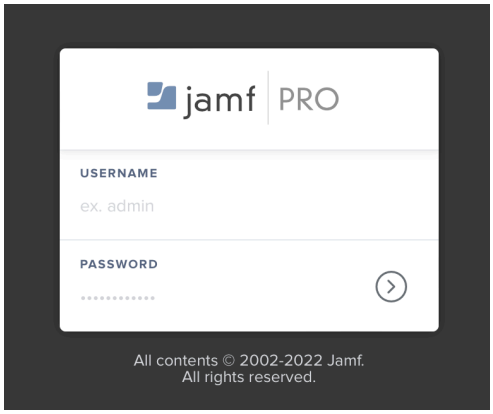
- A Mac Computer running 10.15.4 or later.
- Jamf Connect Configuration App
- Jamf Connect Installer version 2.14.0
- Jamf Connect Launch Agent Installer
- jamfconnecbranding.pkg - We created this in section 4.
- Jamf Connect License - Get this from https://id.jamf.com

If you followed along with this guide from the beginning, you should have three packages on your Desktop:

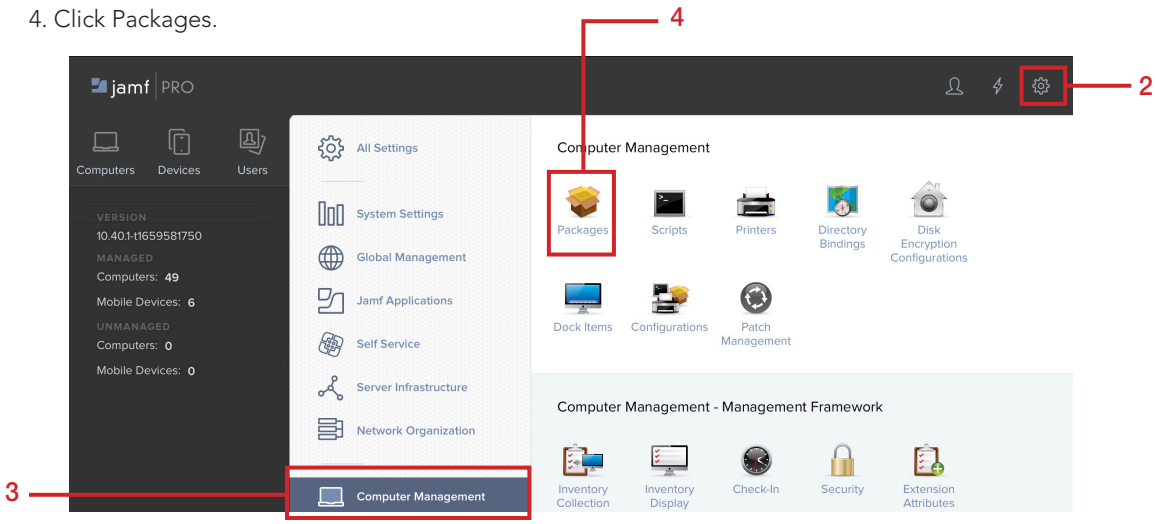
- JamfConnect.pkg
- JamfconnectLaunchAgent.pkg
- jamfconnectbranding.pkg

Make sure you have those packages before continuing with this section. You will need to upload them to your Jamf Pro server.

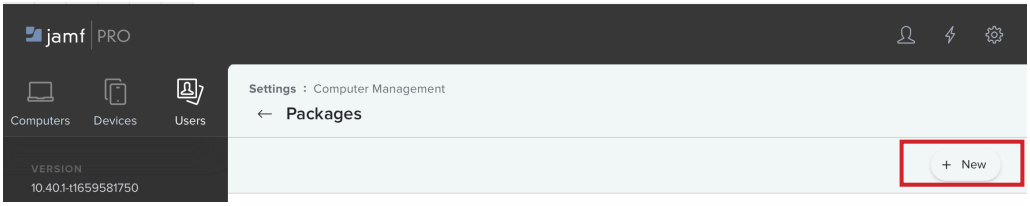
1. Using a web browser of your choice, Log in to your Jamf Pro server.



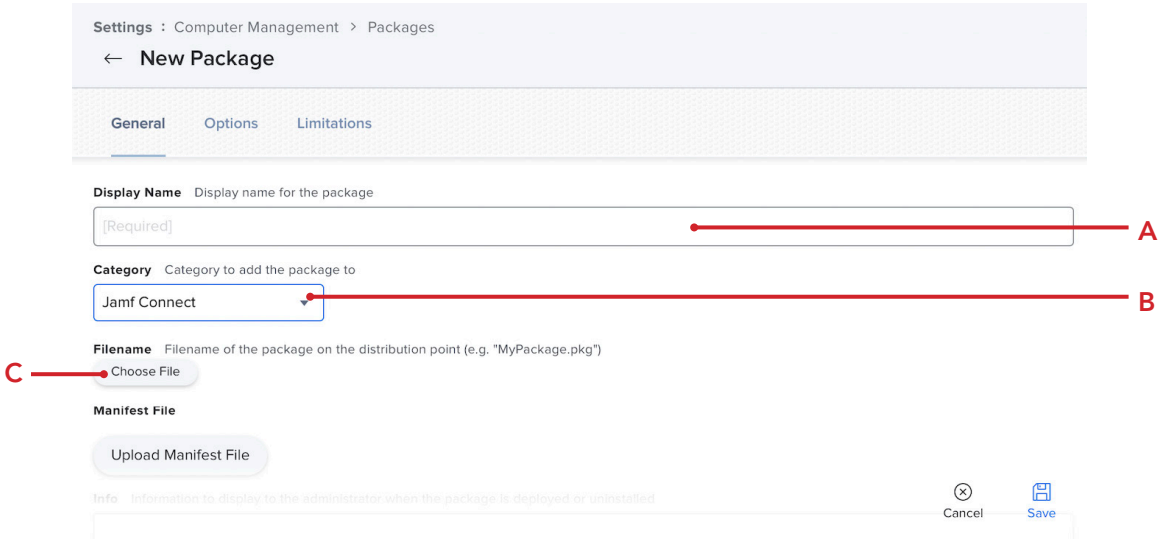
2. Click Settings (⚙) in the upper-right corner.
3. Click Computer Management.
4. Click Packages.



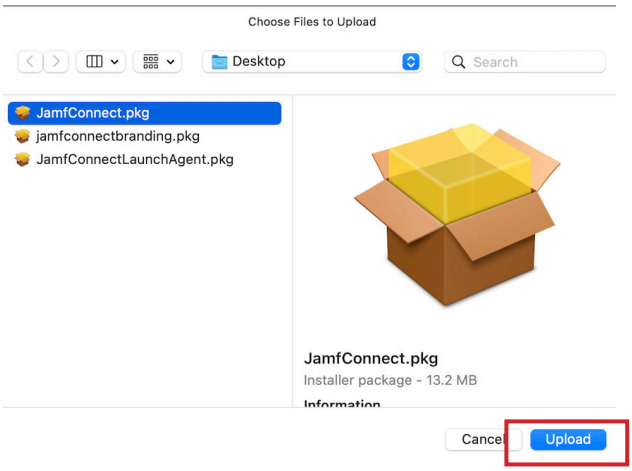
5. Click New.



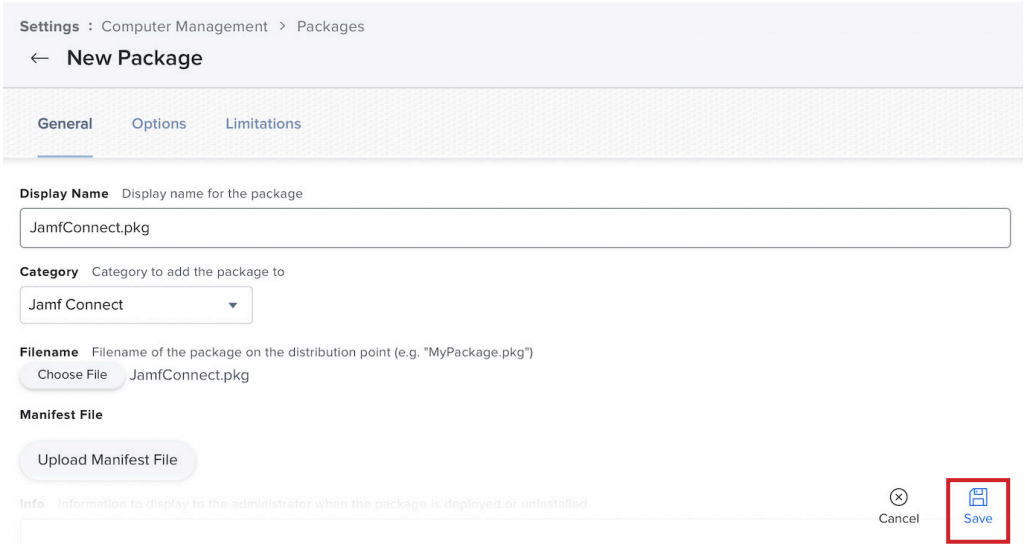
6. Enter the following:
   A. Display Name: Leave this blank. It will auto populate once we click the package.
   B. Category: This guide will use Jamf Connect
   C. Click Choose File



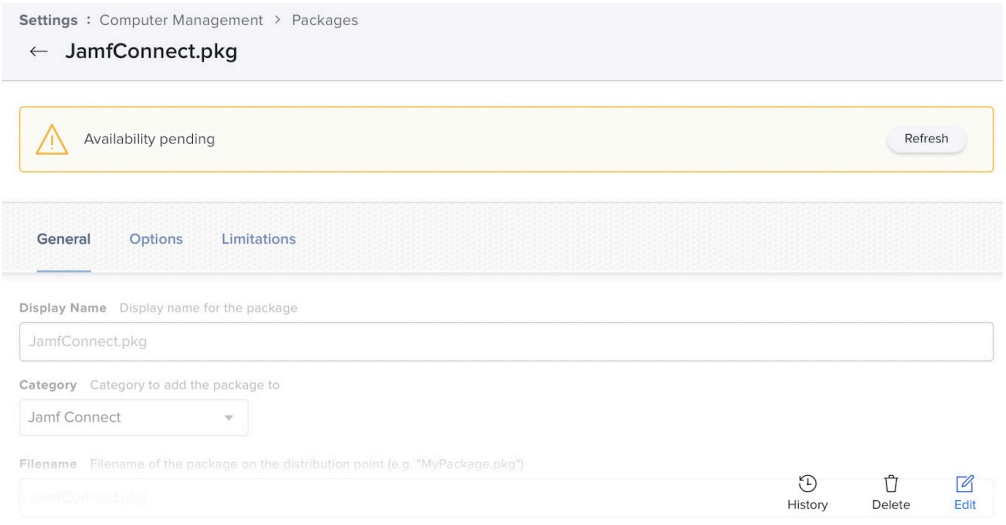
7. Navigate to your Desktop and choose the JamfConnect.pkg then click Upload.



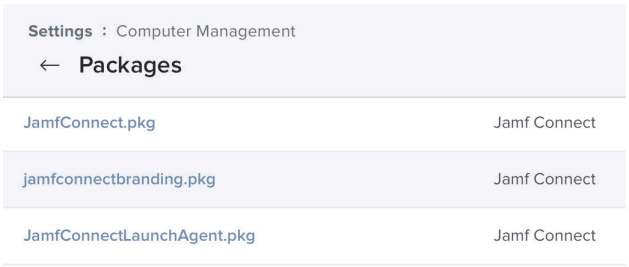
8. Click Save to start the upload of the package.



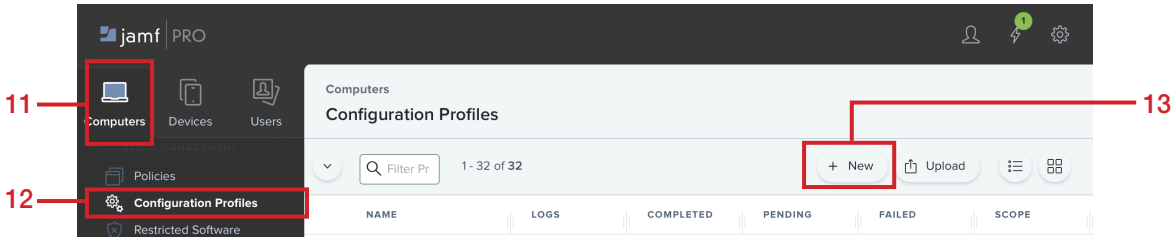
9. The package was successfully uploaded. Follow steps 4 -7 to upload the JamfconnectLaunchAgent.pkg and jamfconnectbranding.pkg.



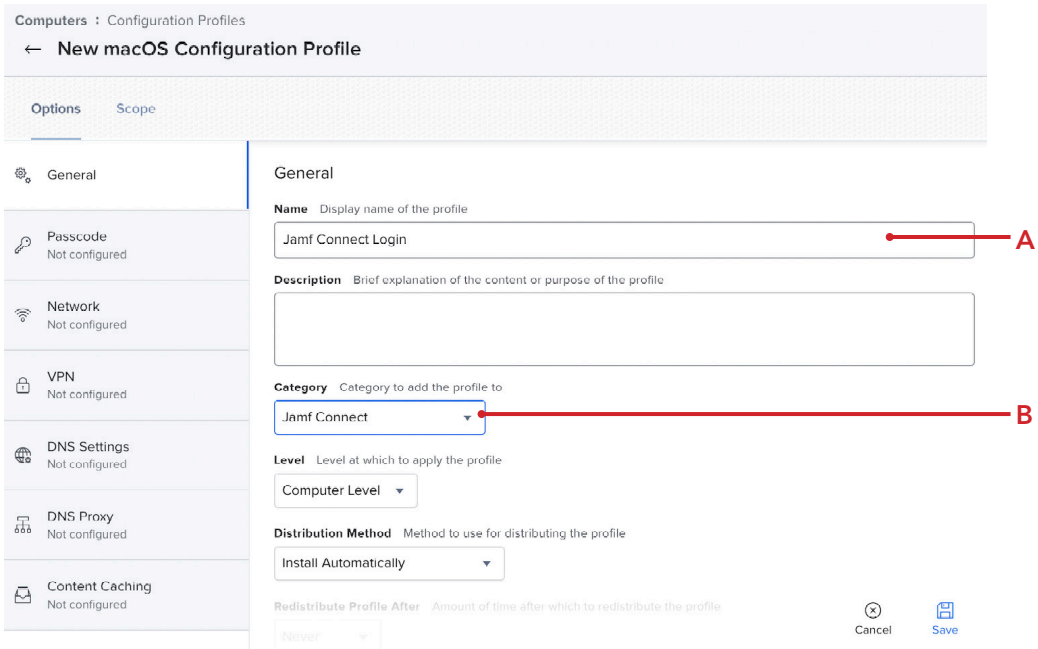
10. Confirm all three packages are uploaded to your Jamf Pro server.



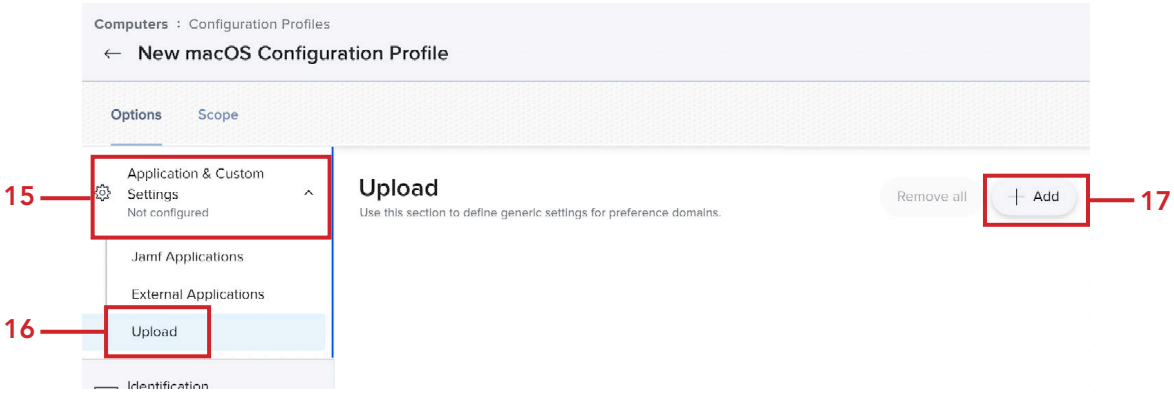
11. Click Computers.
12. Click Configuration Profiles.
13. Click New.



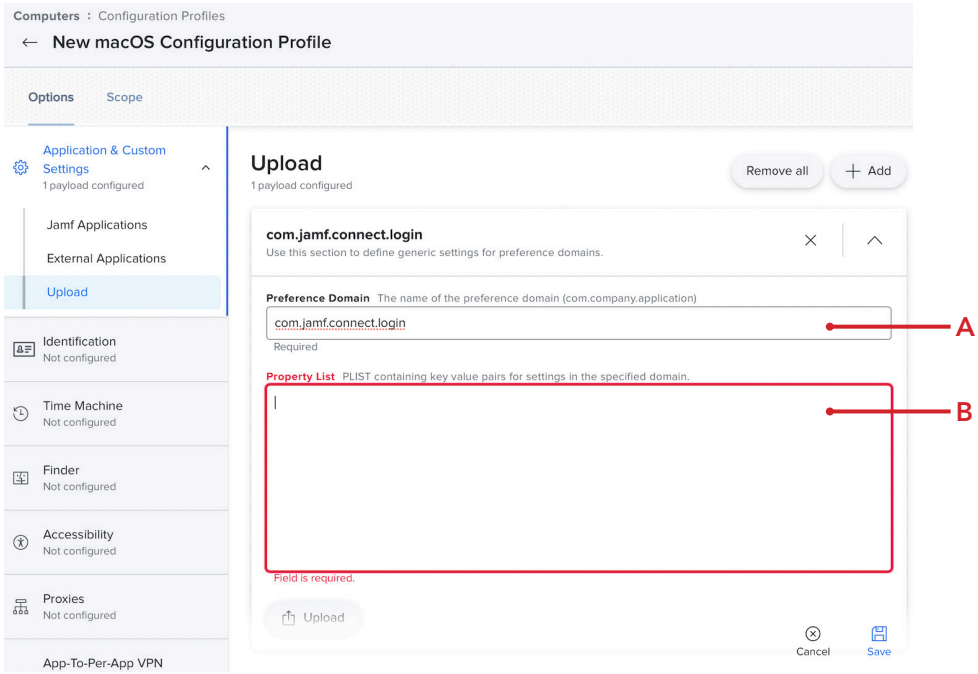
14. Click the General Payload, then enter the following:
    A. Name: Jamf Connect Login
    B. Category: This guide will use Jamf Connect



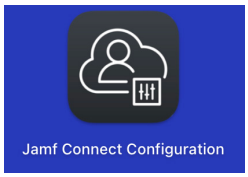
15. Expand the Application & Custom Settings payload.
16. Click Upload.
17. Click Add.



18. Enter the following:
    A. Preference Domain: com.jamf.connect.login
    B. Property List: We will copy this from the Jamf Connect Configuration App in the next step.

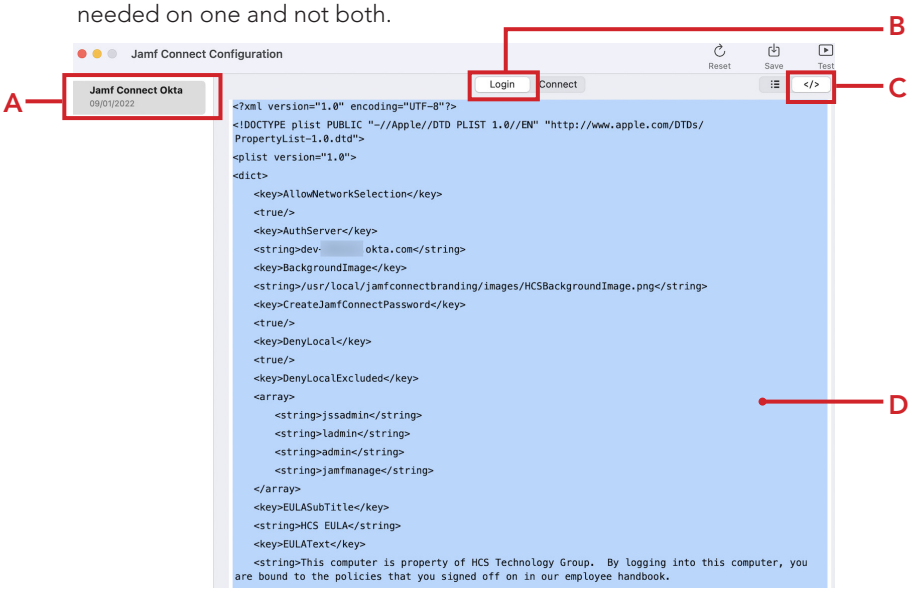


19. Open the Jamf Connect Configuration App.

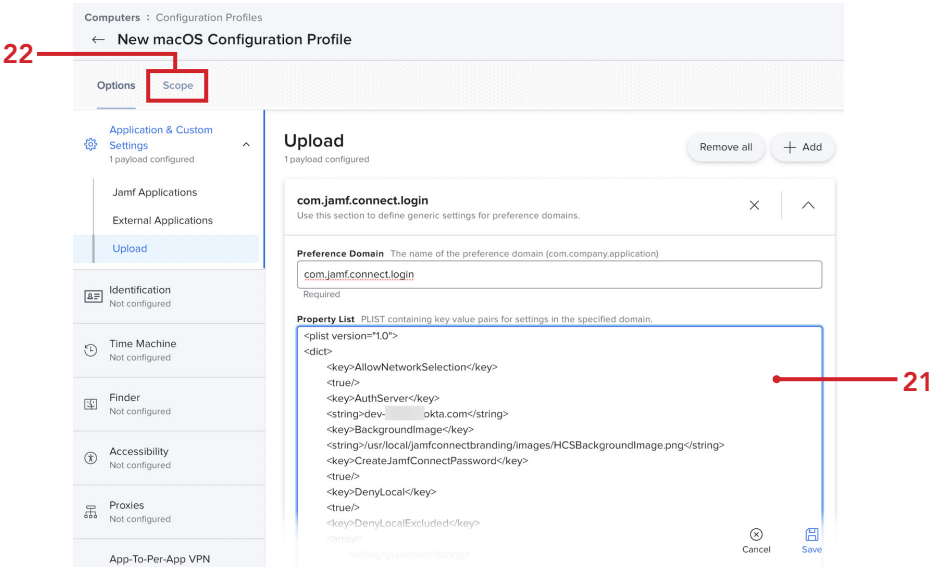


20. Follow the steps:
    A. Click Jamf Connect Okta.
    B. Click the Login tab.
    C. Click the XML tag icon. < / >
    D. Select all the XML and copy it.

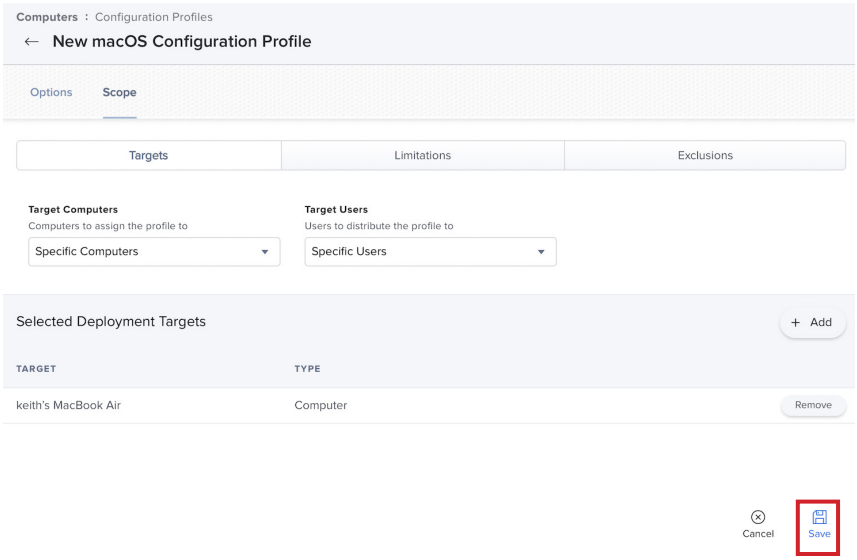
    NOTE: Best practice is to copy the XML data and create new configuration profiles in Jamf Pro for the Login and Connect settings. There have been issues in the past with uploading configuration profiles created in the Jamf Connect Configuration App to Jamf Pro. During the upload process, key value pairs can be stripped out of the configuration profile. To avoid those issues, we always start with fresh profiles using the XML data. It's also best practice to create individual configuration profiles for Login and Connect. Makes life easier when changes are needed on one and not both.



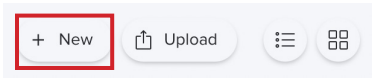
21. Switch back to the Jamf Pro server and paste the XML in the Property List section. Inspect the beginning and end of the pasted XML and remove any spaces from the beginning and the end if necessary.
22. Click Scope.



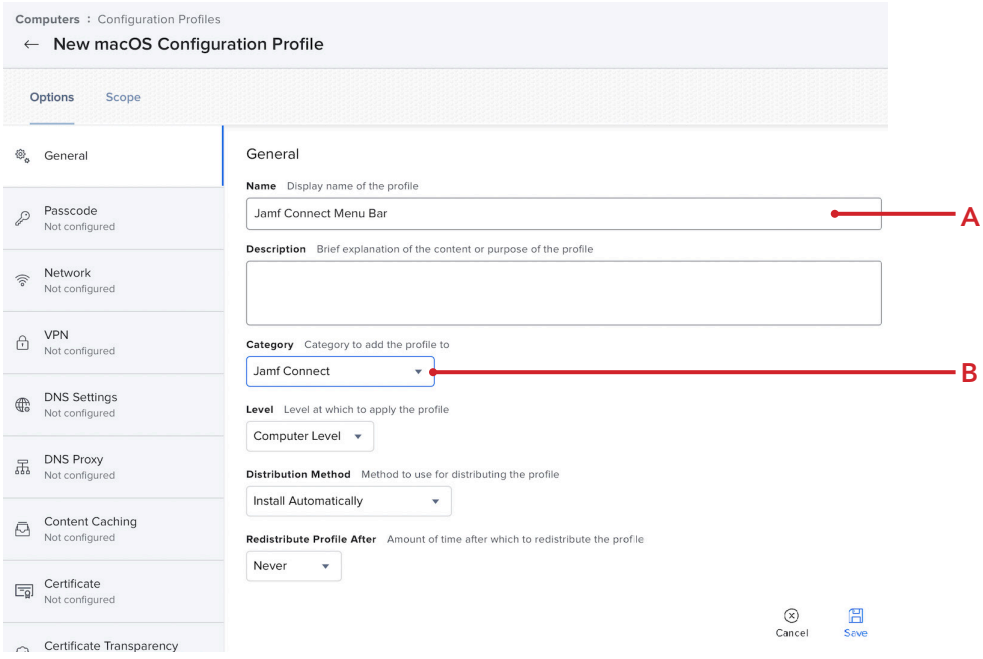
23. Scope to your needs. This guide will scope to a test Mac Computer.
24. Click Save.



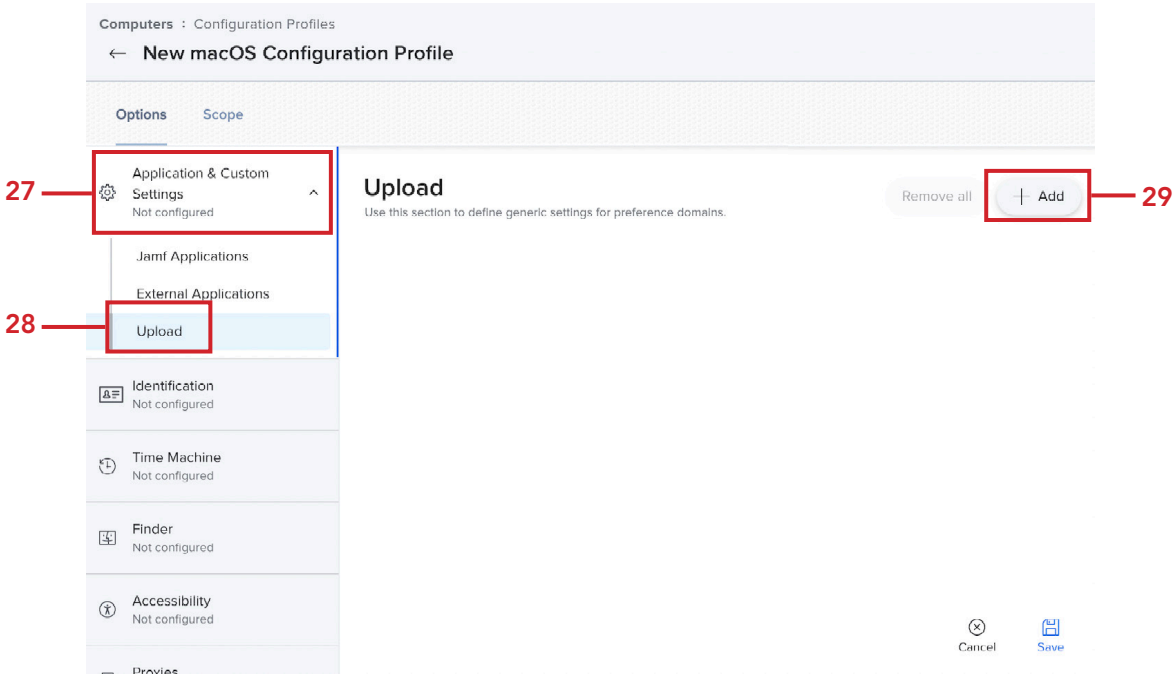
25. Create another Configuration Profile. Click New.



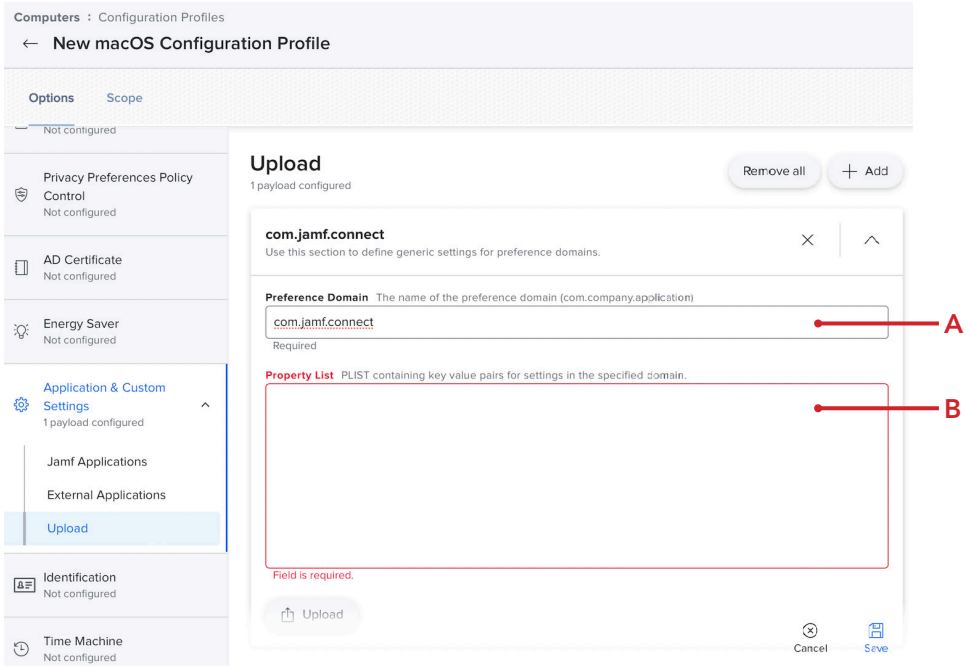
26. Click the General Payload, then enter the following:
    A. Name: Jamf Connect Menu Bar
    B. Category: This guide will use Jamf Connect



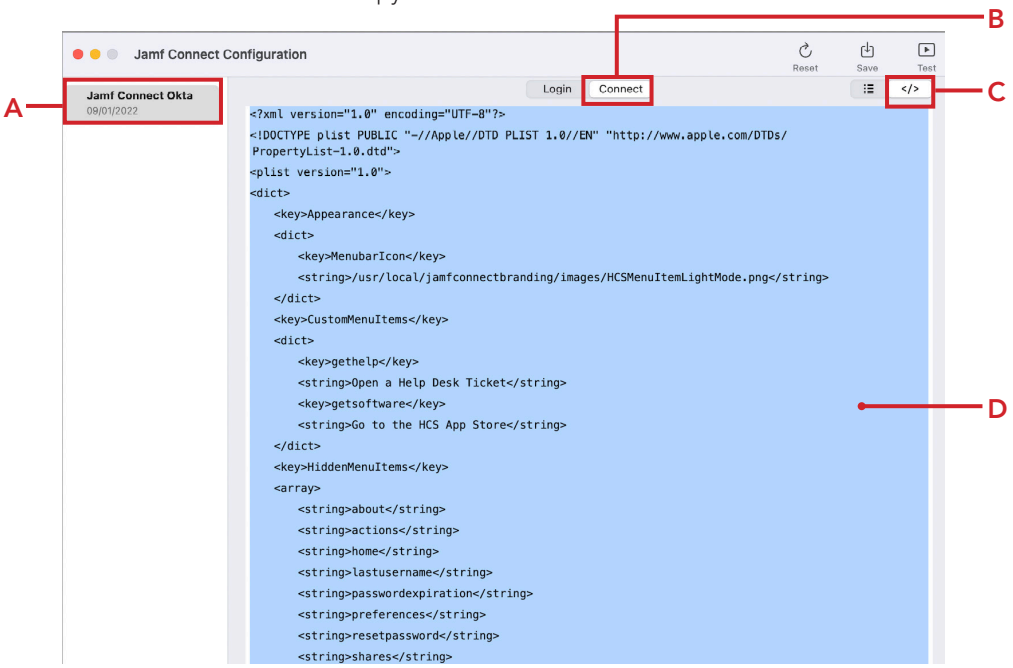
27. Expand the Application & Custom Settings payload.
28. Click Upload.
29. Click Add.



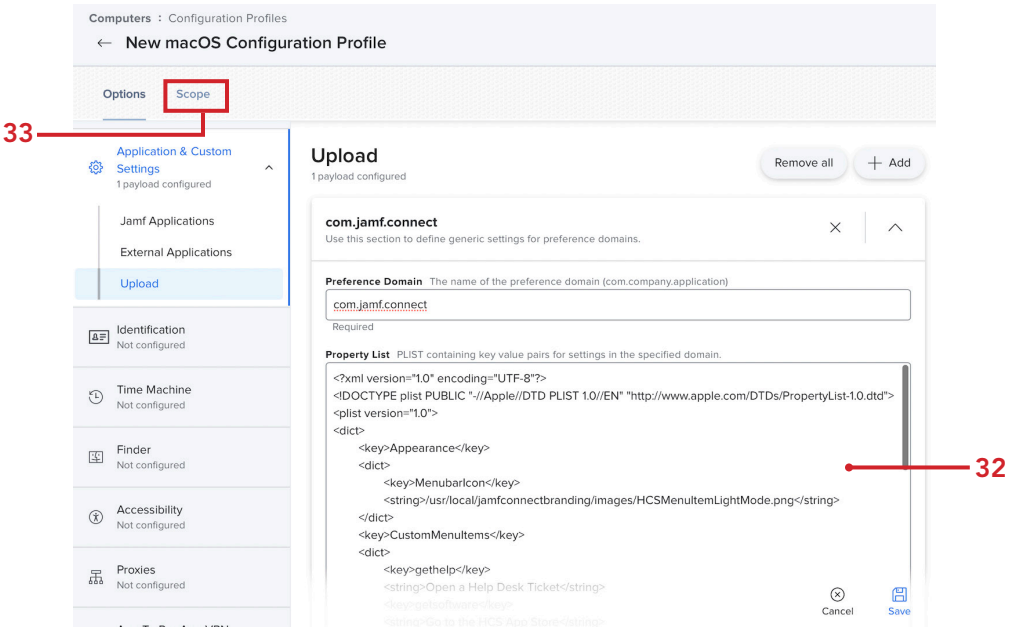
30. Enter the following:
    A. Preference Domain: com.jamf.connect
    B. Property List: We will copy this from the Jamf Connect Configuration App in the next step.



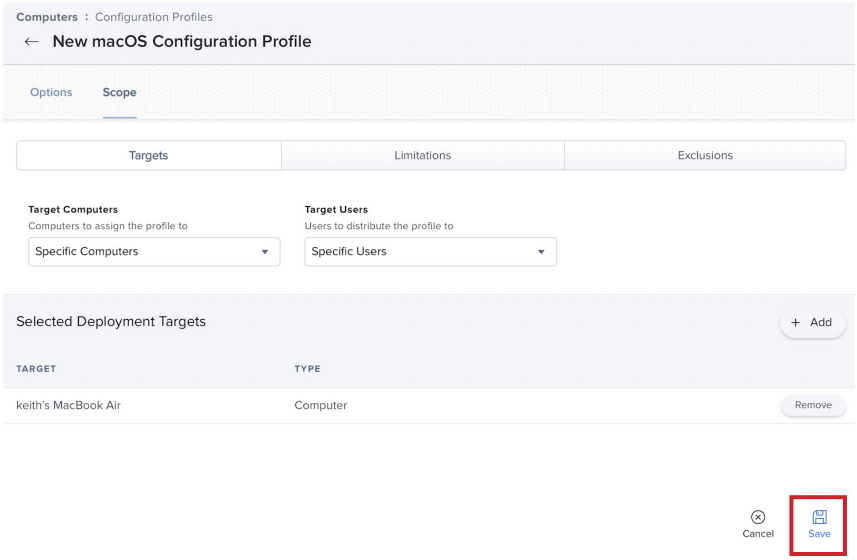
31. Follow the steps:
    A. Click Jamf Connect Okta.
    B. Click Connect.
    C. Click the XML tag icon. < / >
    D. Select all the XML and copy it.



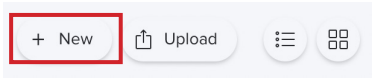
32. Switch back to the Jamf Pro server and paste the XML in the Property List section. Inspect the beginning and end of the pasted XML and remove any spaces from the beginning and the end if necessary.
33. Click Scope.



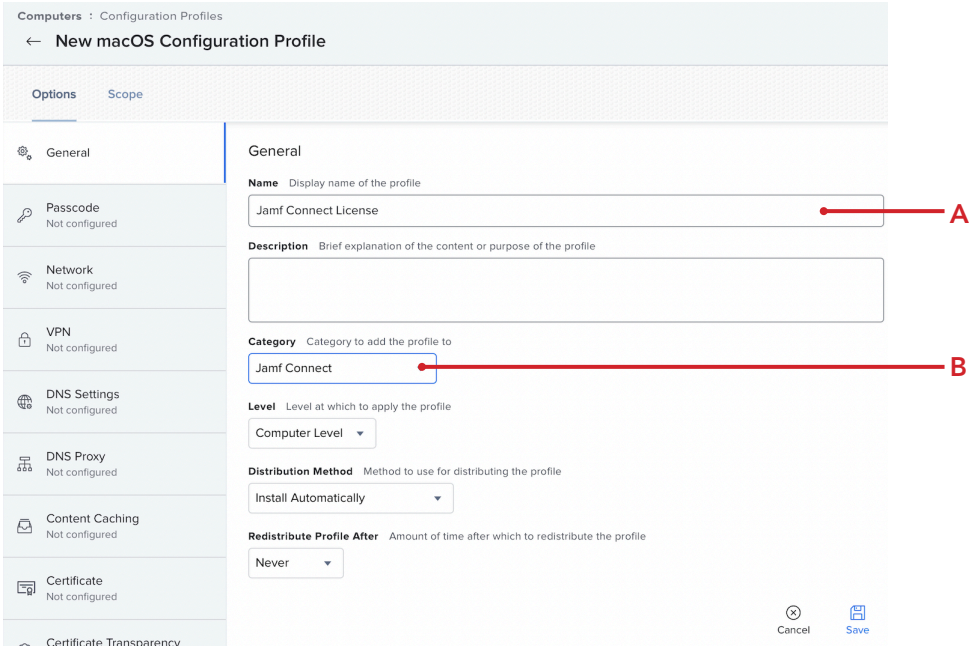
34. Scope to your needs. This guide will scope to a test Mac Computer.
35. Click Save.



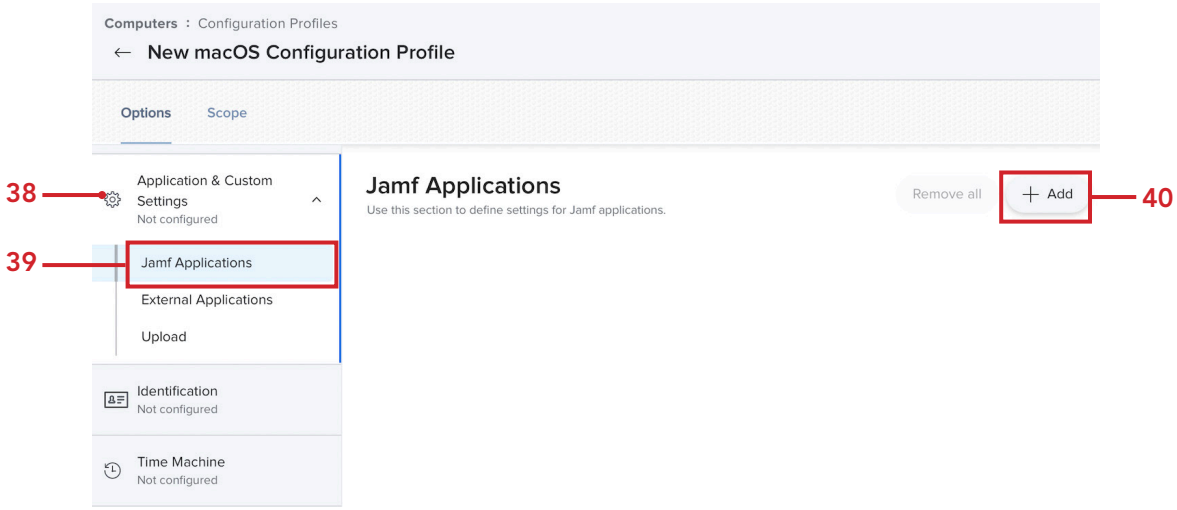
36. Create another Configuration Profile. Click New.



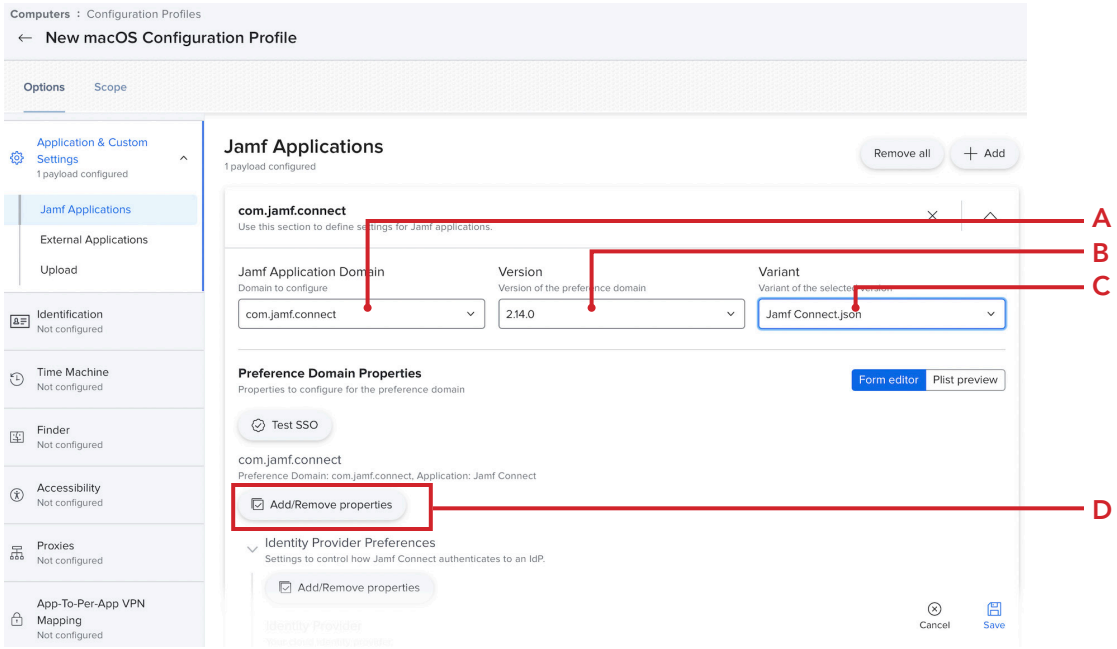
37. Click the General Payload, then enter the following:
    A. Name: Jamf Connect License
    B. Category: This guide will use Jamf Connect



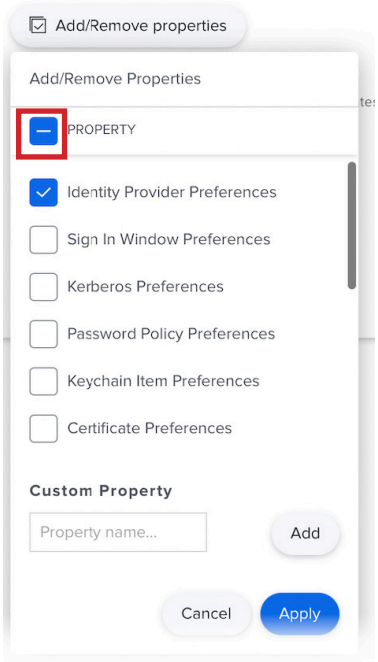
38. Click the Application & Custom Settings to expand the payload.
39. Click Jamf Applications.
40. Click Add.



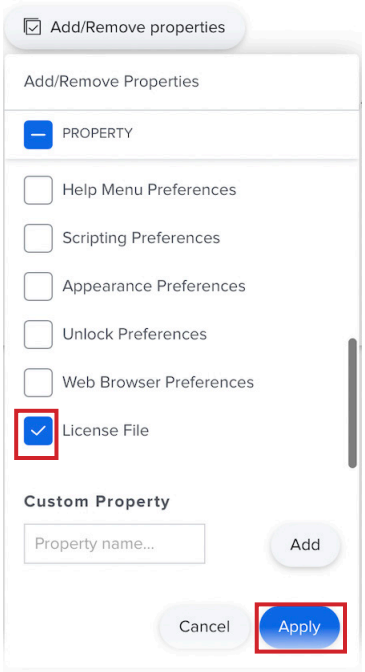
41. Configure the following:
    A. Jamf Application Domain: com.jamf.connect
    B. Version: 2.14.0 (or the latest version available)
    C. Variant: Jamf Connect json
    D. Click the first Add/Remove properties button



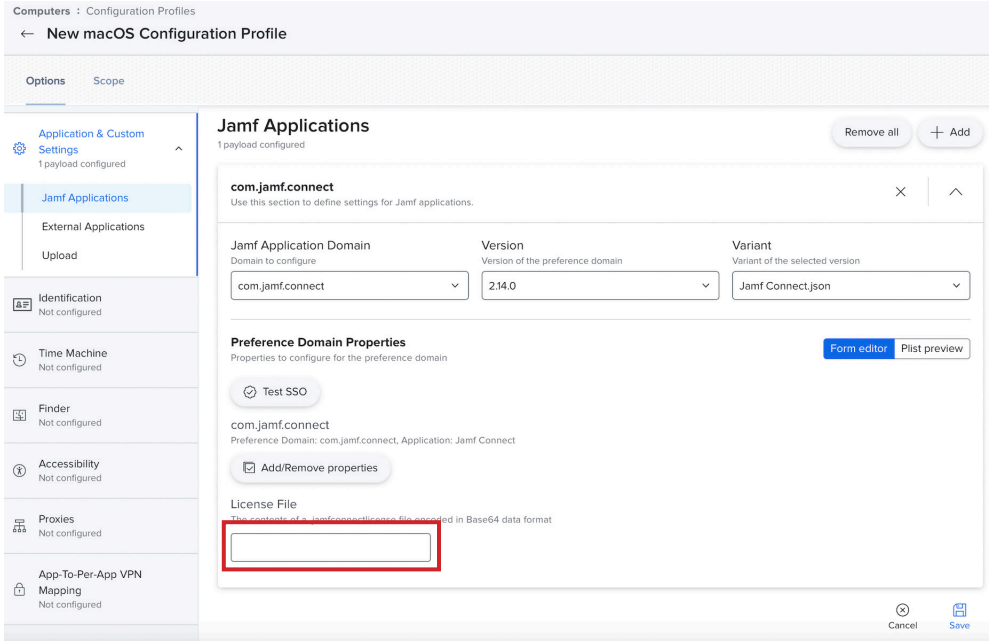
42. Deselect the checkbox for Property twice to clear it's contents.



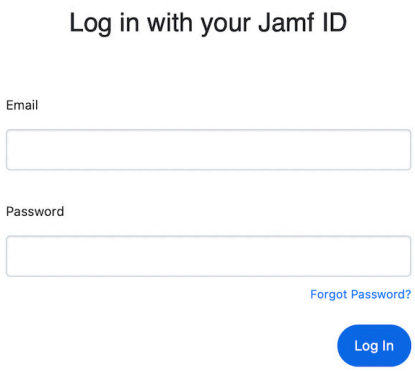
43. Scroll down to the bottom and Select the checkbox for License File. Confirm nothing else is selected. Click Apply.



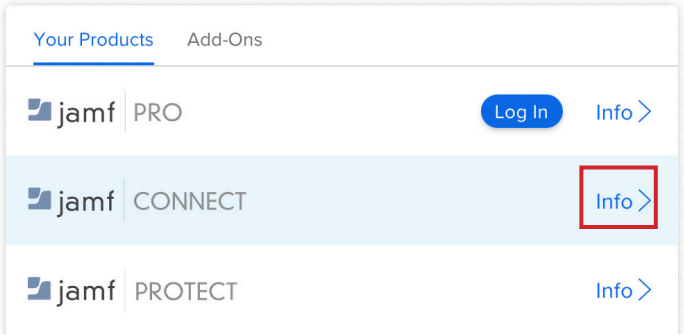
44. Confirm a field for License File appears. We need to get our Jamf Connect License in the next step.



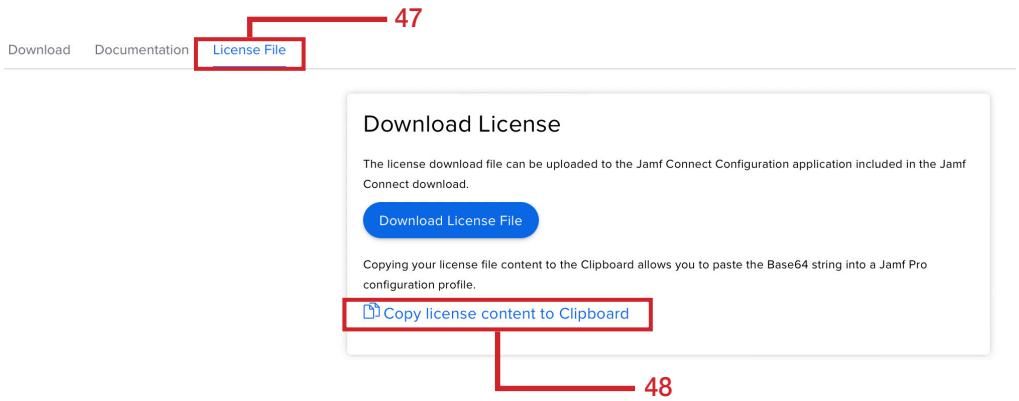
45. Open another web bowser window and go to https://id.jamf.com and login with your Jamf ID that has access to all of your assets.



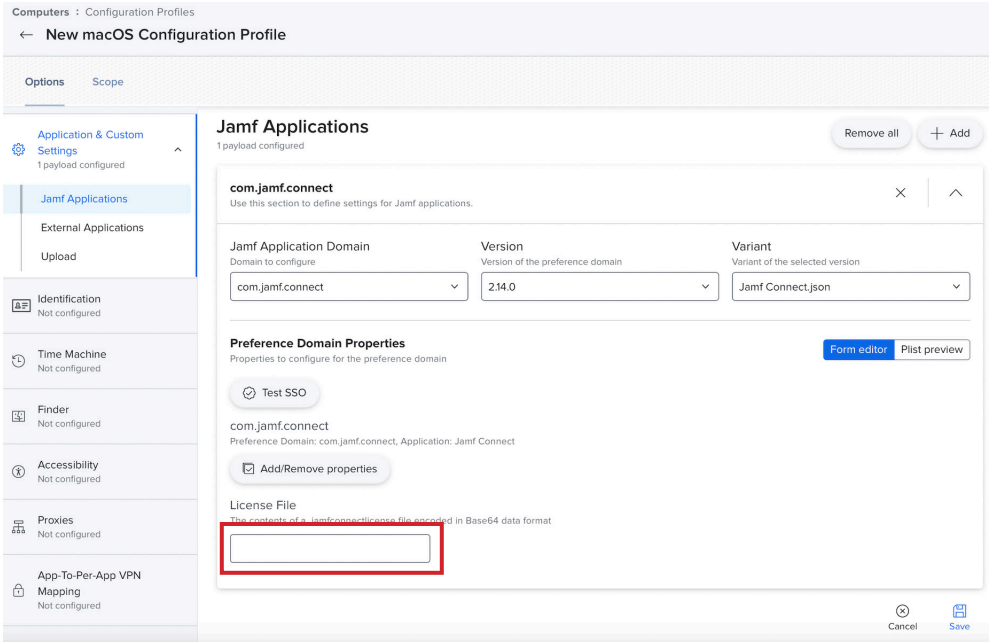
46. Click Jamf Connect from the Product list and click Info.



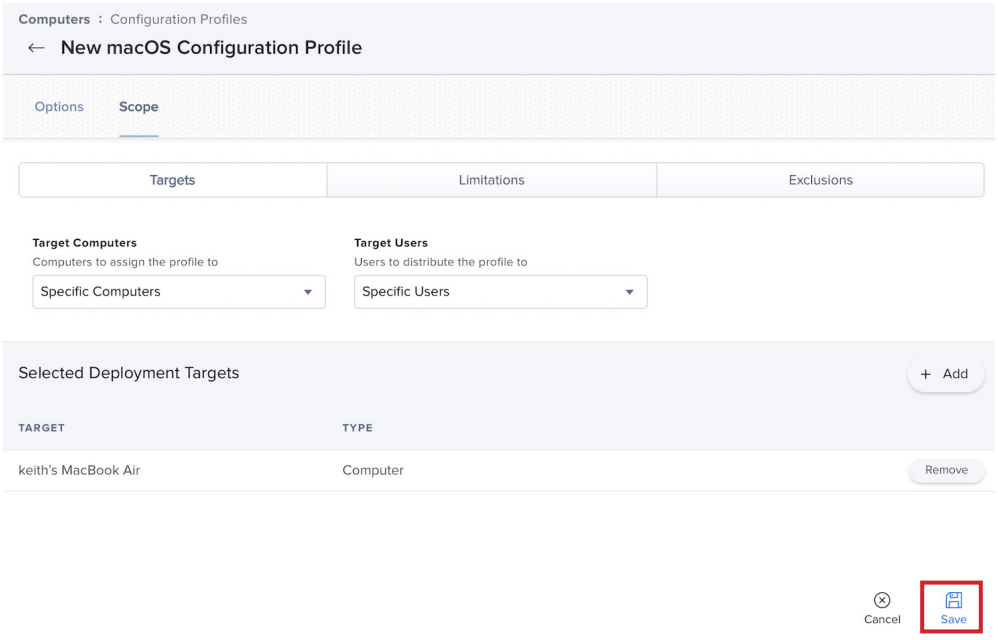
47. Click License File.
48. Click Copy license content to Clipboard.



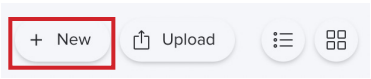
49. Switch back to the Jamf Pro server and paste the license in the License File field. Make sure there are no leading or trailing spaces after you paste it in. Click Scope.



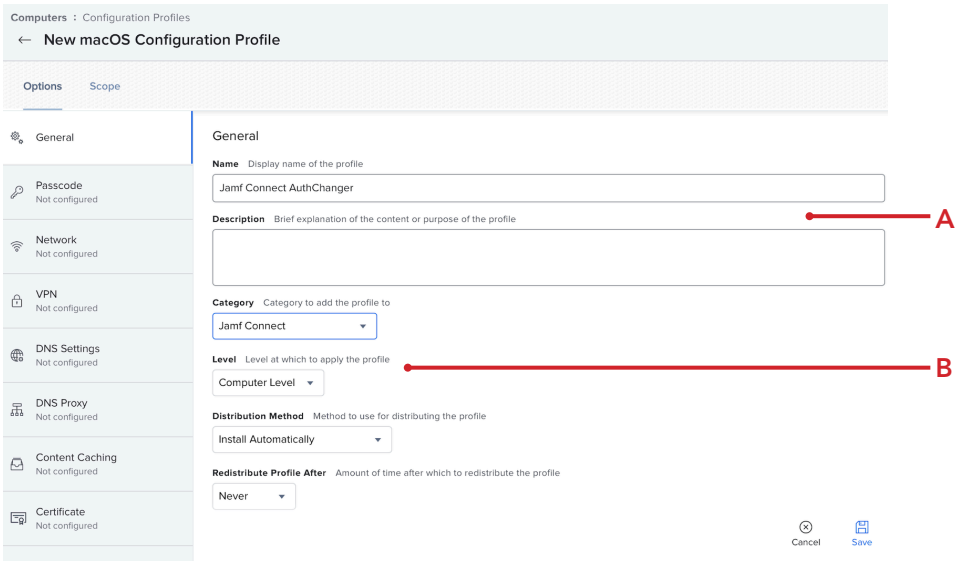
50. Scope to your needs. This guide will scope to a test Mac Computer. Click Save.
NOTE: We create the license file this way so when it's time to renew your Jamf Connect license, all you need to do is edit the configuration profile with the new license information. This makes it much easier than embedding the license file with the Login and Connect profiles.



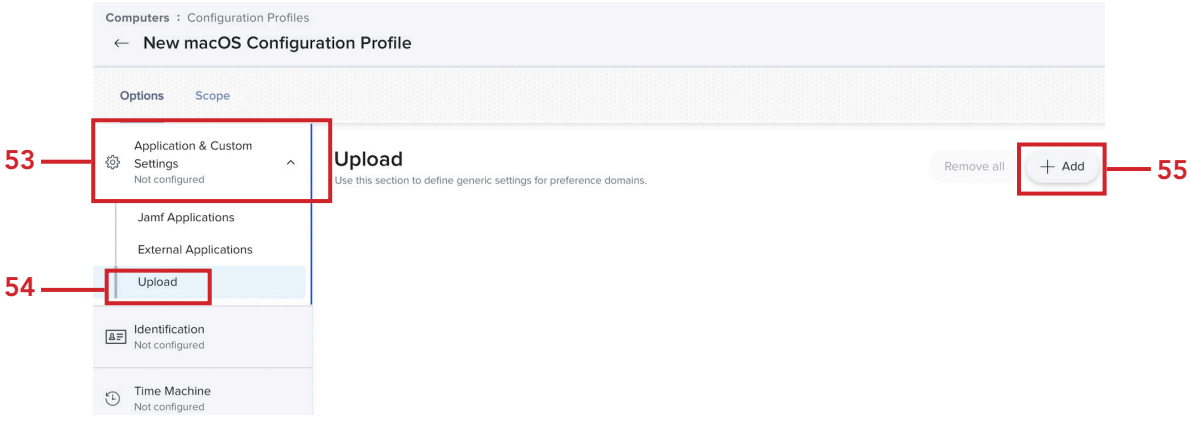
51. Create another Configuration Profile. Click New.



52. Click the General Payload, then enter the following:
    A. Name: Jamf Connect AuthChanger
    B. Category: This guide will use Jamf Connect
    NOTE: This configuration profile will ensure Jamf Connect is always enabled as the default login window. There are times when a macOS update can change the login window back to the default macOS login window. This profile will prevent that from happening.

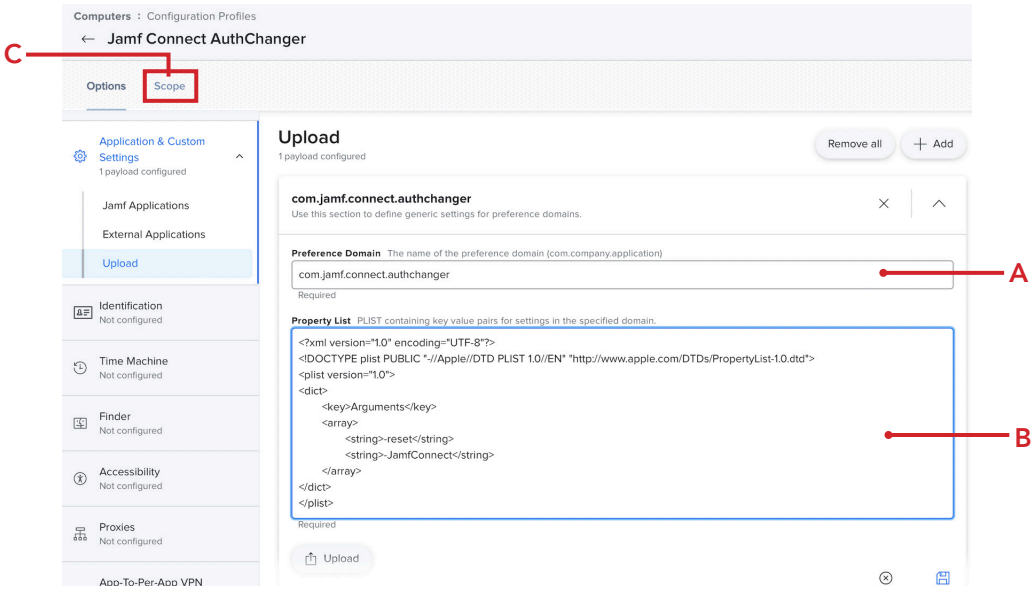


53. Expand the Application & Custom Settings payload.
54. Click Upload.
55. Click Add.

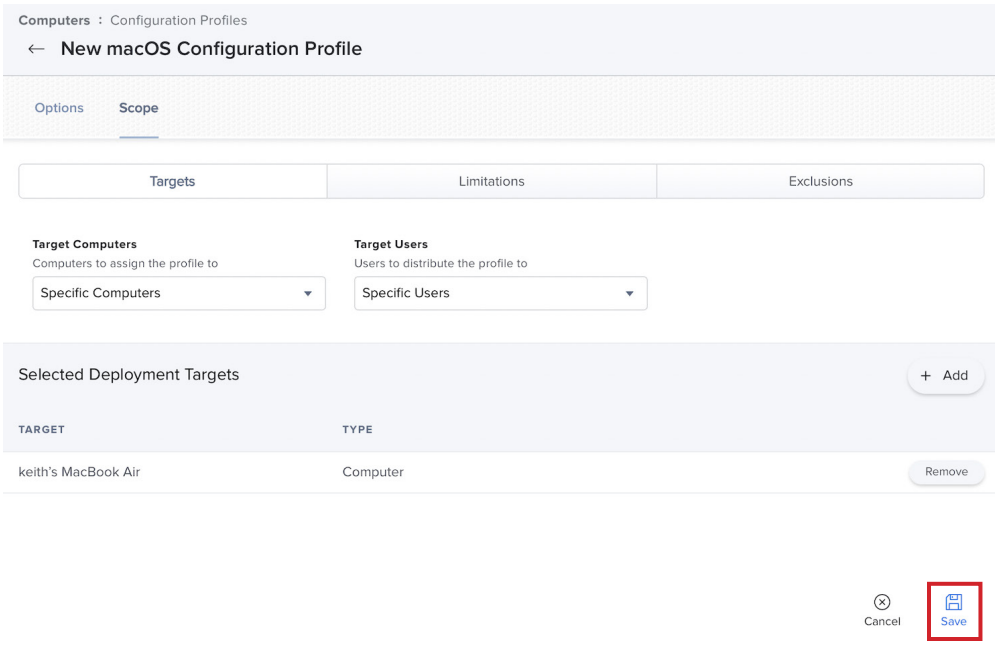


56. Enter the following:
    A. Preference Domain: com.jamf.connect.authchanger
    B. Property List: Copy the XML below and paste in the Property List field
    C. Click Scope

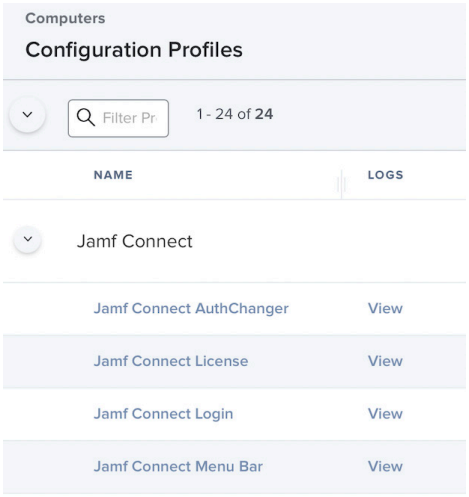
```
<?xml version="1.0" encoding="UTF-8"?>
<!DOCTYPE plist PUBLIC "-//Apple//DTD PLIST 1.0//EN" "http://www.apple.com/DTDs/PropertyList-1.0.dtd">
<plist version="1.0">
<dict>
        <key>Arguments</key>
        <array>
                <string>-reset</string>
                <string>-JamfConnect</string>
        </array>
</dict>
</plist>
```



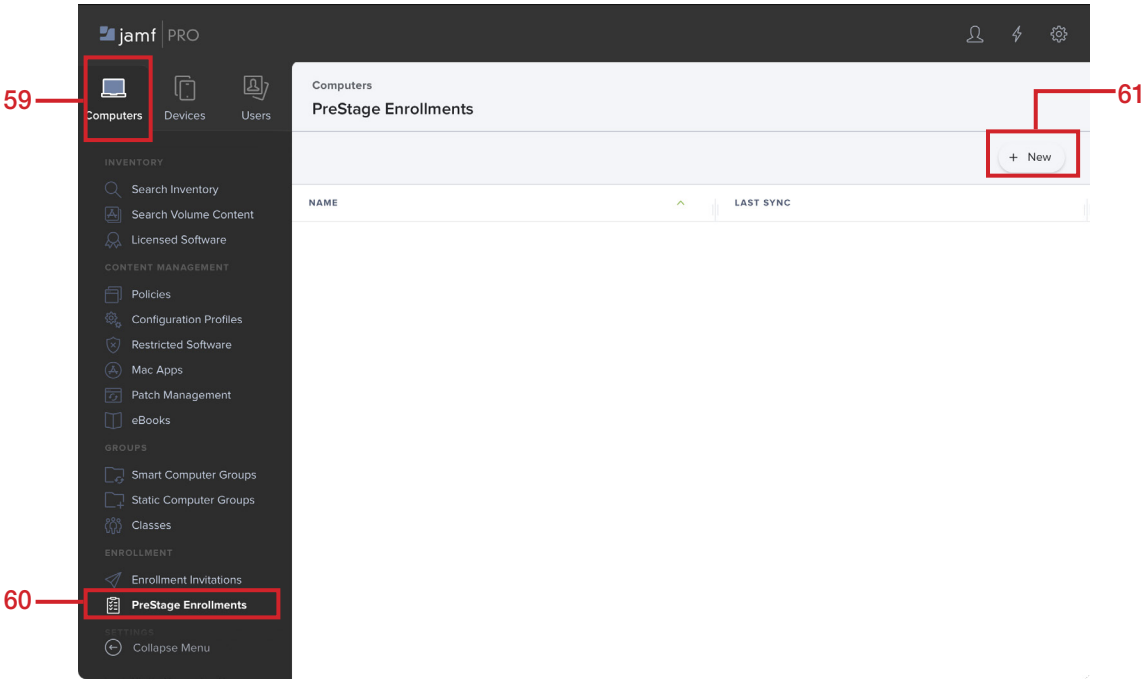
57. Scope to your needs. This guide will scope to a test Mac Computer. Click Save.



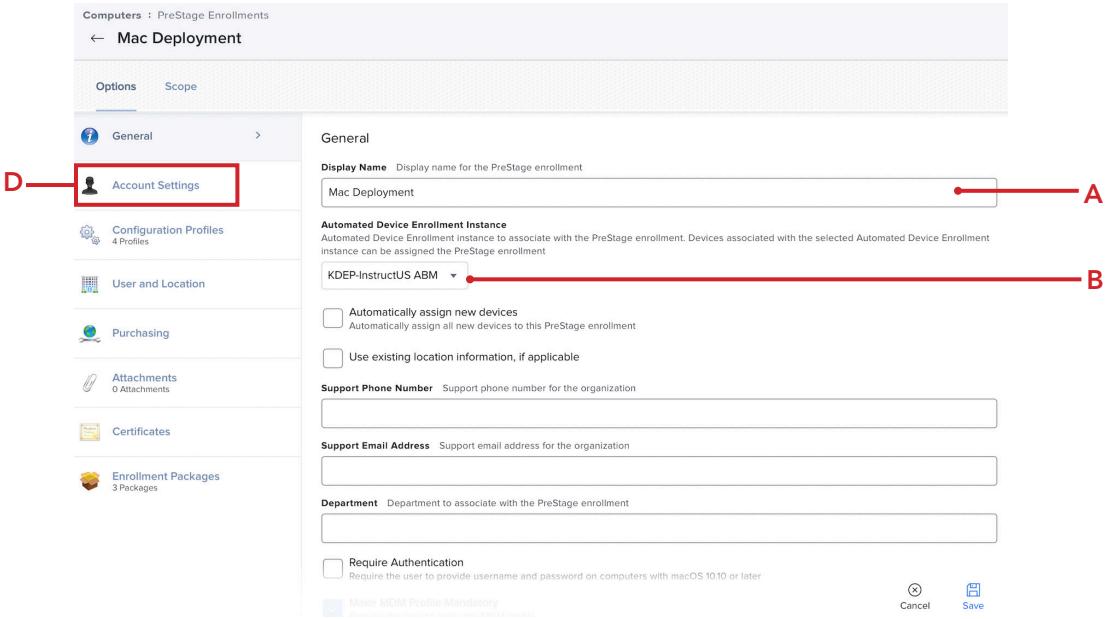
58. Confirm you have the four configuration profiles shown below.



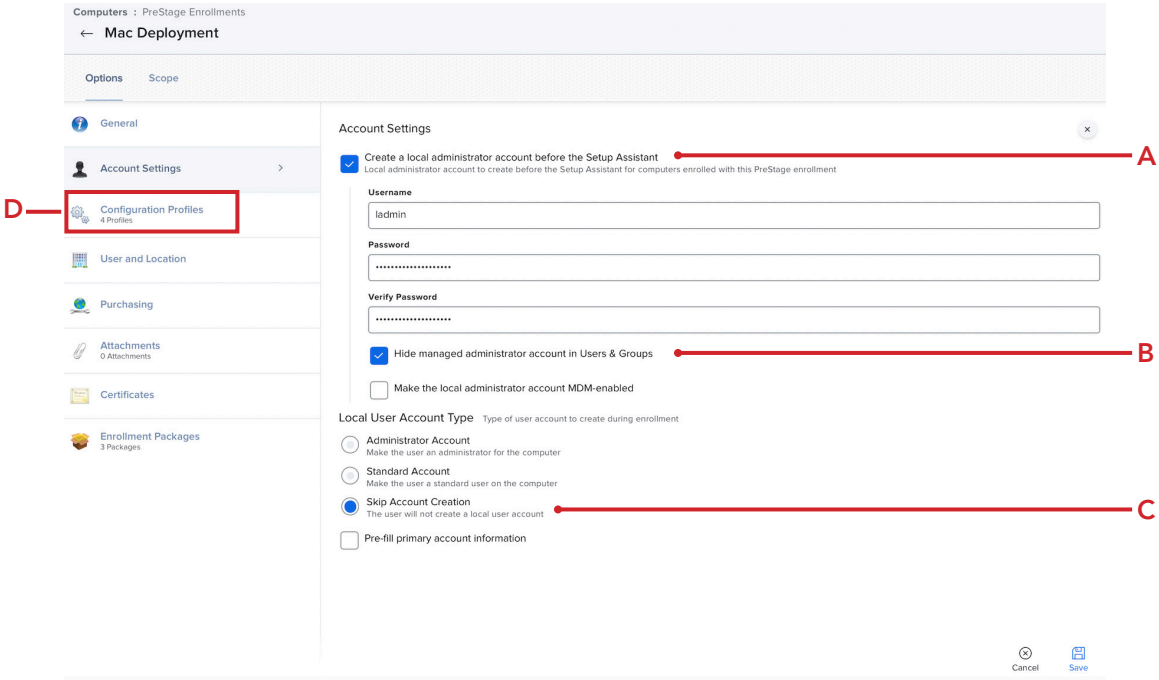
59. Click Computers
60. Click PreStage Enrollments.
61. Click New



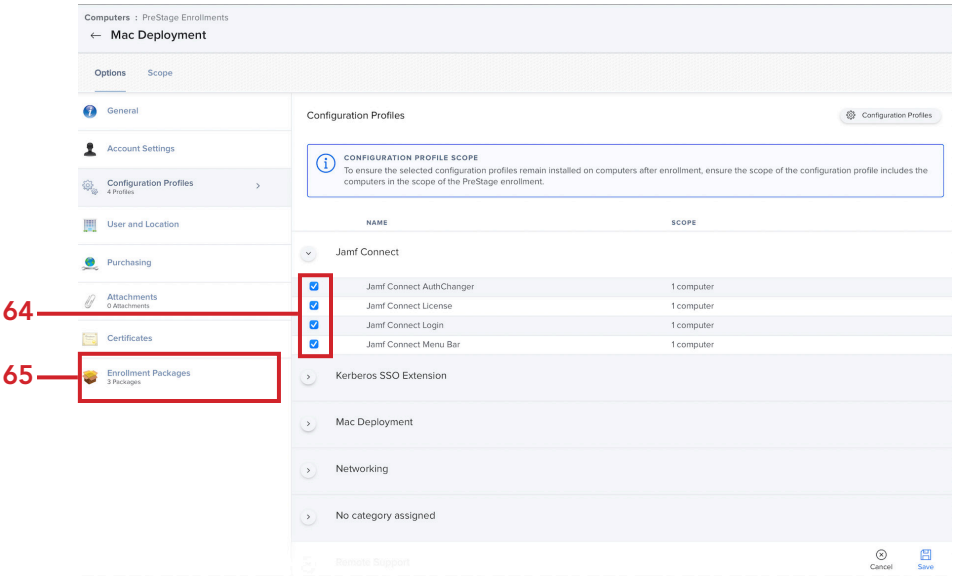
62. Click the General Payload, then enter the following:
    A. Display Name: Mac Deployment
    B. Automated Device Enrollment Instance: Click your instance. This guide will use KDEP-InstructUS ABM
    C. Configure the rest of the General section to your needs.
    D. Click the Account Settings payload.



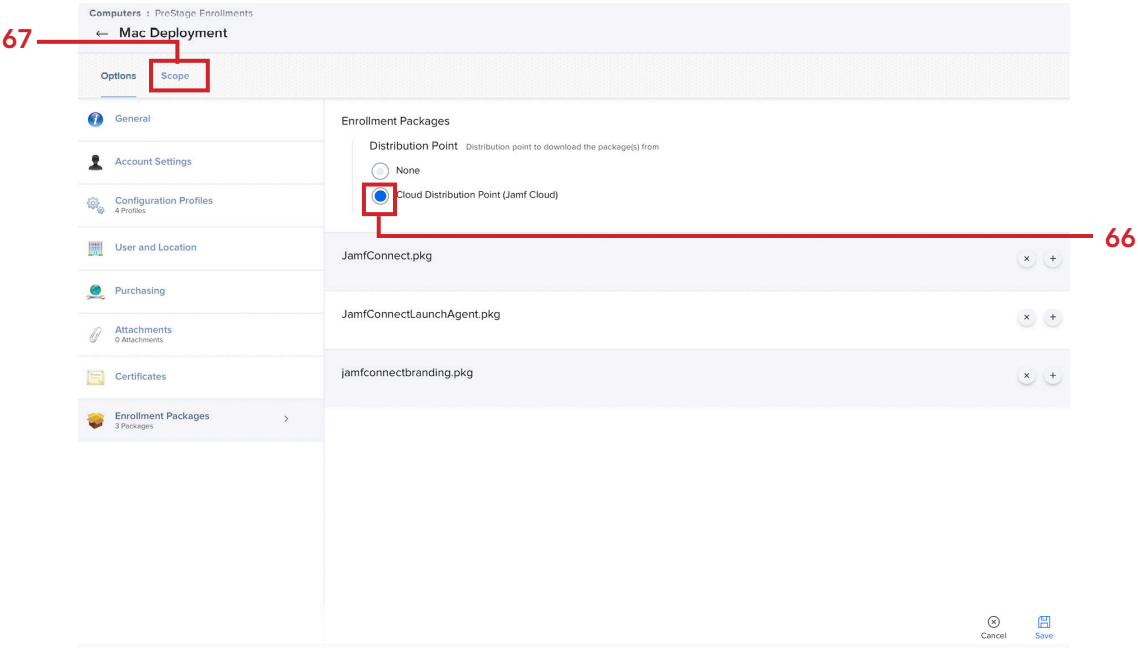
63. Configure the following:
    A. Create a local administrator account before the setup Assistant. Enable this if needed. This guide will enable it.
    B. Select the checkbox for Hide managed administrator account in Users & Groups
    C. Local User Account Type: Select the radio button for Skip Account Creation
    D. Click the Configuration Profiles payload



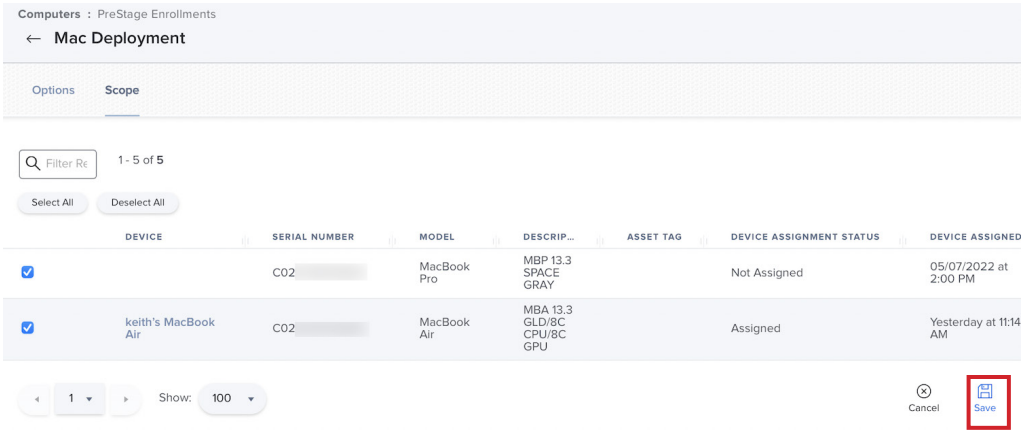
64. Select the checkboxes for the four Jamf Connect configuration profiles
65. Click the Enrollment Packages payload.



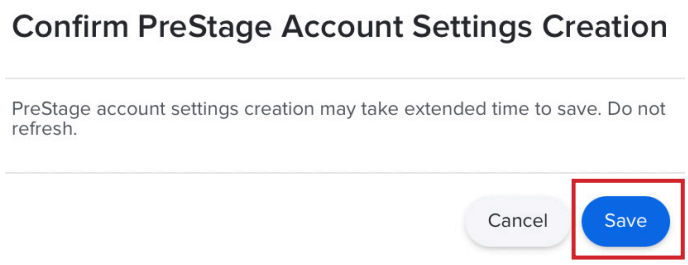
66. Add the three packages shown below and Select the radio button for the Cloud Distribution Point (Jamf Cloud) radio button.
67. Click Scope.



68. Scope to your needs then click Save.



69. Click Save.



In the next section we will deploy a Mac Computer using the PreStage enrollment created in this section and confirm Jamf Connect is working as expected.

This completes this section.

Section 8: Installing Jamf Connect on a Mac Computer with Jamf Pro

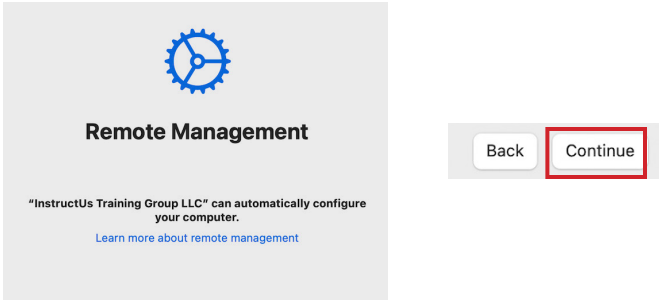
In this section we will deploy a Mac computer using the PreStage enrollment created in section 7 and confirm Jamf Connect is installed with all of our customized settings.

Requirements for following along with this section:

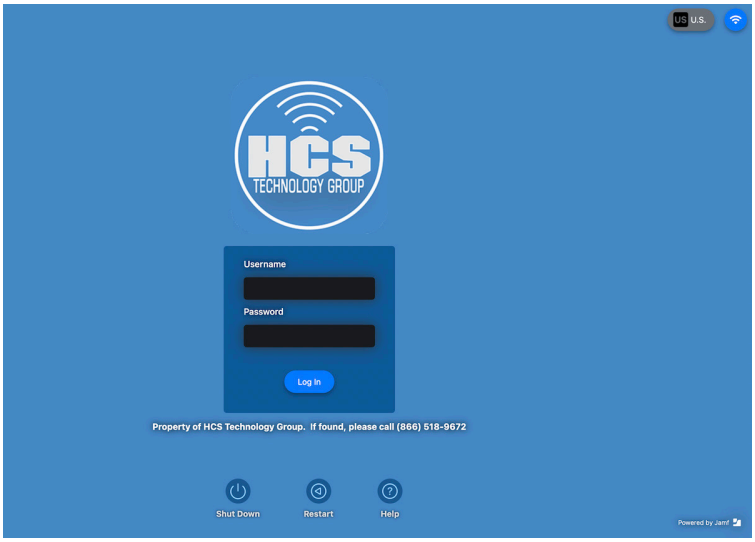
- A Mac computer that's brand new in the box or an old Mac computer that was erased and has a new macOS installed (10.15.4 or later). The Mac computer must be enrolled in Apple Business or School Manager and assigned to your PreStage in Jamf Pro. This is required for Automated Device Enrollment using a Jamf Pro PreStage.
- Okta login credentials. We recommend using a NON admin account when logging in at the Jamf Connect Login window to see how role based account creation works. This will create the user on the Mac computer as a standard user which is their role in Okta.

NOTE: This section will NOT walk through all the setup assistant screens as this would be different in every environment based on the settings you used for your PreStage. We will start at the Remote management screen so please follow the on screen instructions that come before the Remote Management screen.

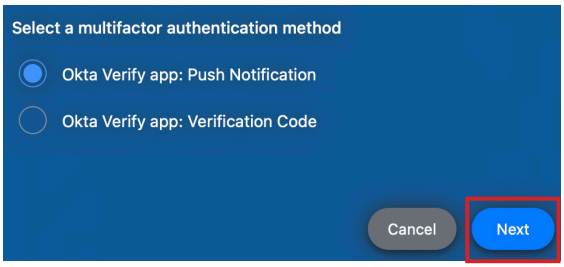
1. At the Remote Management screen, click Continue.



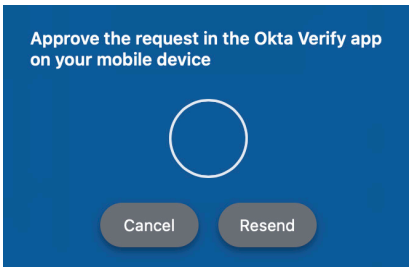
2. After setup assistant is completed, Confirm a customized Jamf Connect Login window. The background is blue, the Wi-Fi logo is visible, Corporate Logo appears, the Login Window message is shown, and the Jamf Connect License has been applied which removed the trial verbiage from the login window. All of our customizations are working. We recommend using a non-admin account when logging in at the Jamf Connect Login window to see how role based account creation works. This will create the user on the Mac Computer as a standard user which is their role in Okta.
   Enter your Okta Username and Password then click Log In.



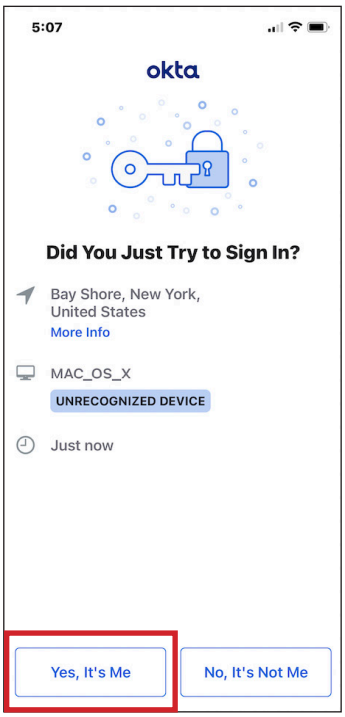
3. Select your MFA authentication method. This guide will use a Push Notification. Click Next.



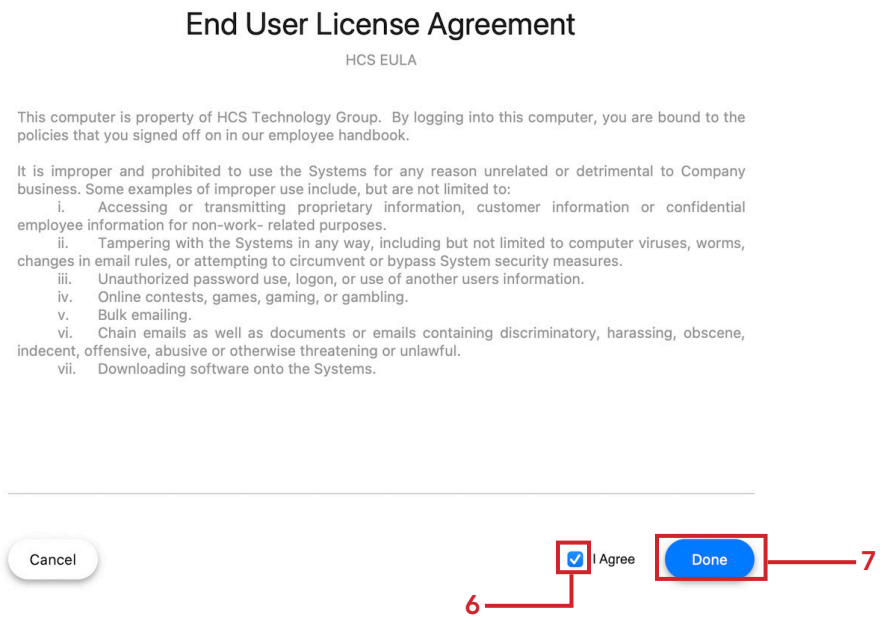
4. You will be prompted with the message below and a notification will be sent to your phone.



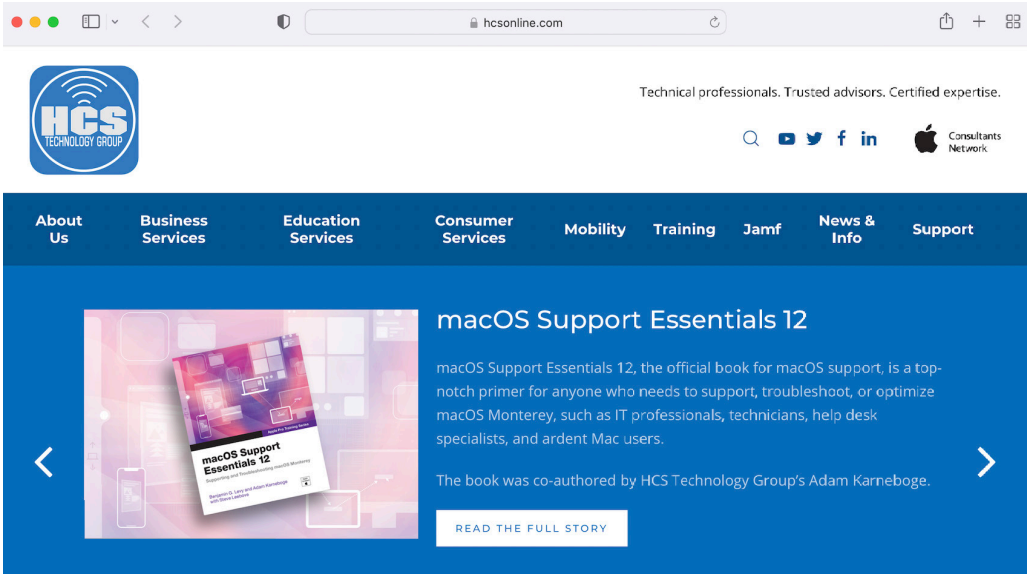
5. Confirm you received a notification on your phone, Tap Yes, It's Me.



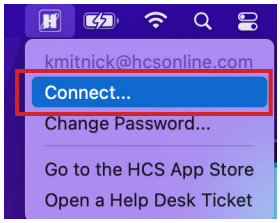
6. Select the checkbox for I Agree.
7. Click Done.



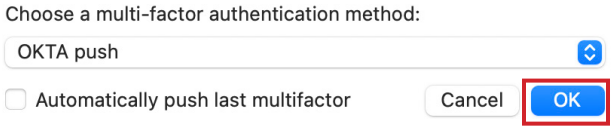
8. Confirm the login script is working. Once logged in, Safari will open and go to: https://hcsonline.com This is using the login script we configured in section 5.



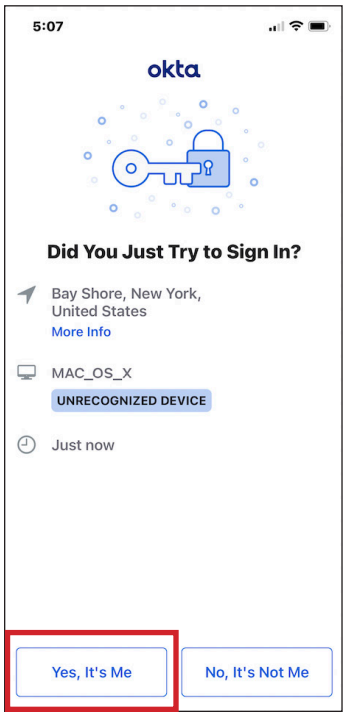
9. Confirm the custom Menu Bar icon is there and the connection script we created is working. Reconnect to Okta by selecting the Jamf Connect Menu Bar icon, which should be customized to your branded logo if you followed along with this guide. Click Connect.



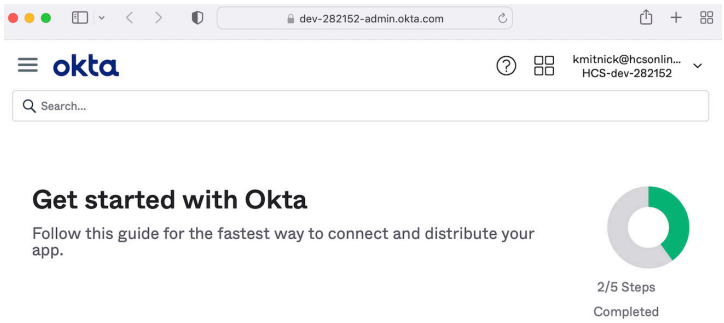
10. Click OK.



11. Confirm you received a notification on your phone, Tap Yes, It's Me.

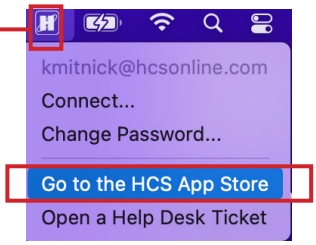


12. If the connection was successful, Safari will open and will sign you into your Okta user account. Our Menu Bar script is working!

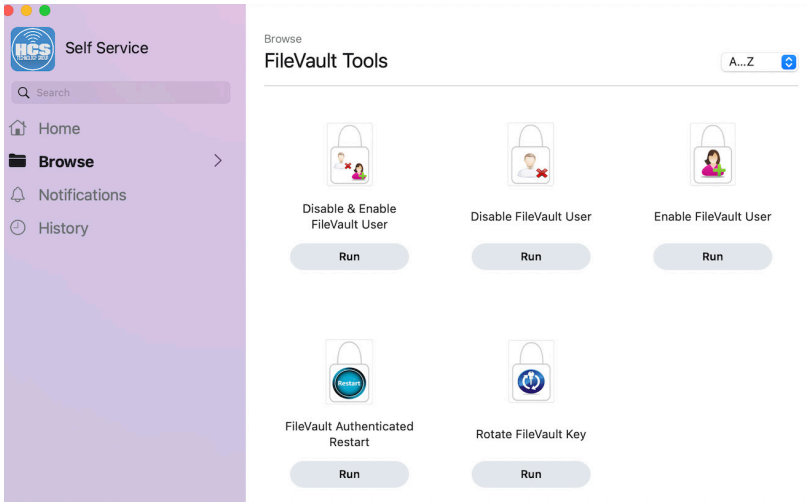


13. Confirm the customized menu items are working. Click the Jamf Connect Menu Bar icon and select Go to the HCS App Store.

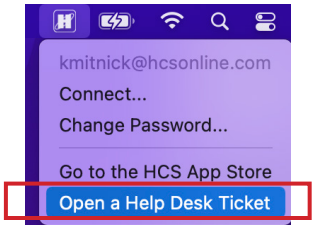
Click the custom logo to access Jamf Connect



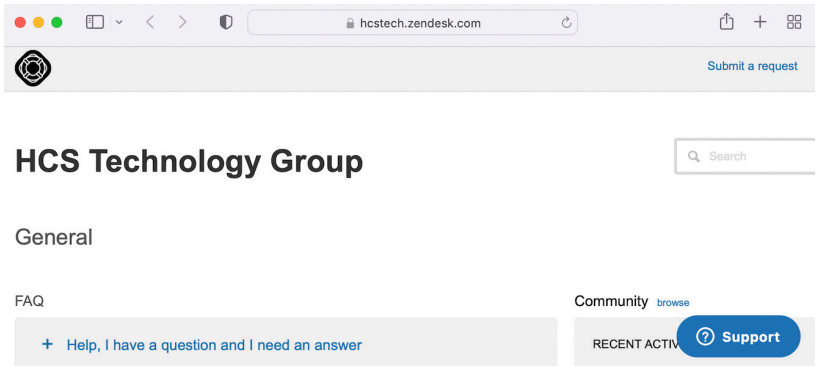
14. The Self Service application will open.



15. Confirm the customized menu items are working. Click the Jamf Connect Menu Bar icon and select Open a Help Desk Ticket.



16. Safari will open and go to: https://hcstech.zendesk.com/hc/en-us



NOTE: If you want to check the role of the user that you just logged in as, Open System Preferences and select Users & Groups. Select your user account and it will be listed as either an Admin or Standard user based on the role assigned to your account in Okta.

The next section is optional. We will discuss configuring Jamf Connect Notify which is a screen that can display a progress bar, customized text, and images during Automated Device Enrollment.

This completes this section.

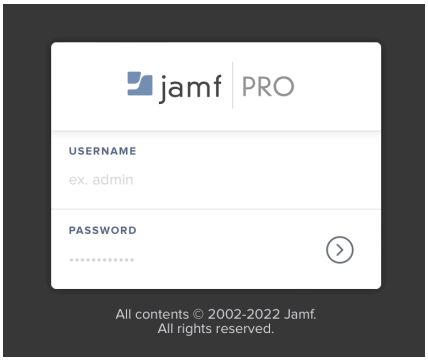
Section 9: Configure Jamf Connect Notify

This section is optional and assumes you followed the guide from the beginning. Items discussed in this section build upon other sections in this guide. In this section we will discuss configuring Jamf Connect Notify which is a screen that can display a progress bar, customized text, and images during Automated Device Enrollment. This allows an organization to install required applications when the user logs in for the first time. The entire screen is taken over by Notify allowing the installation process to complete before the Mac computer can be used by the user.

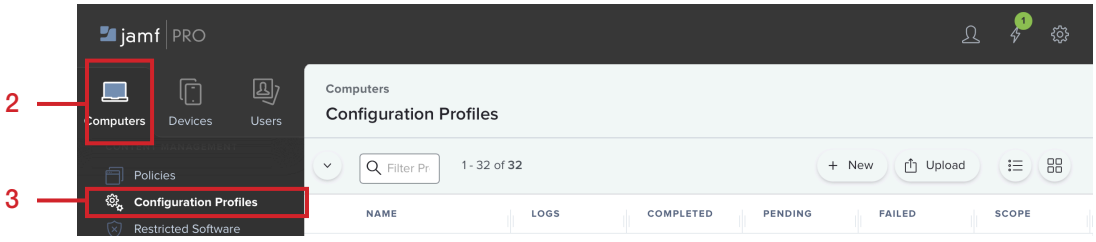
Requirements for following along with this section:

- A Mac computer that's brand new in the box or an old Mac computer that was erased and has a new macOS installed (10.15.4 or later). The Mac computer must be enrolled in Apple Business or School Manager and assigned to your PreStage in Jamf Pro. This is required for Automated Device Enrollment using a Jamf Pro PreStage.
- The notify.sh script is provided in the download files for this guide. This script assumes you have two polices created to install Firefox and Google chrome using a custom trigger for each policy. Firefox is using the custom trigger named: InstallFirefox and Google Chrome is using the custom trigger named: InstallGoogleChrome. Please edit this script to install items to your needs before continuing with this section.
- Administrative access to your Jamf Pro server.
- Okta login credentials. We recommend using a non-admin account when logging in at the Jamf Connect Login window to see how role based account creation works. This will create the user on the Mac computer as a standard user which is their role in Okta.

1. Using a web browser of your choice, Log in to your Jamf Pro server.

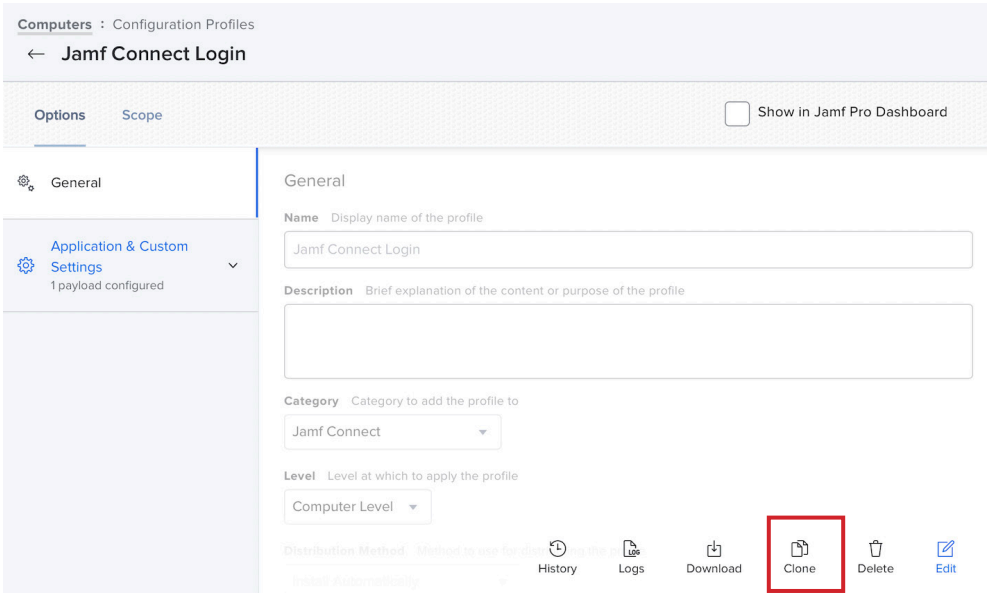


2. Click Computers.
3. Click Configuration Profiles.

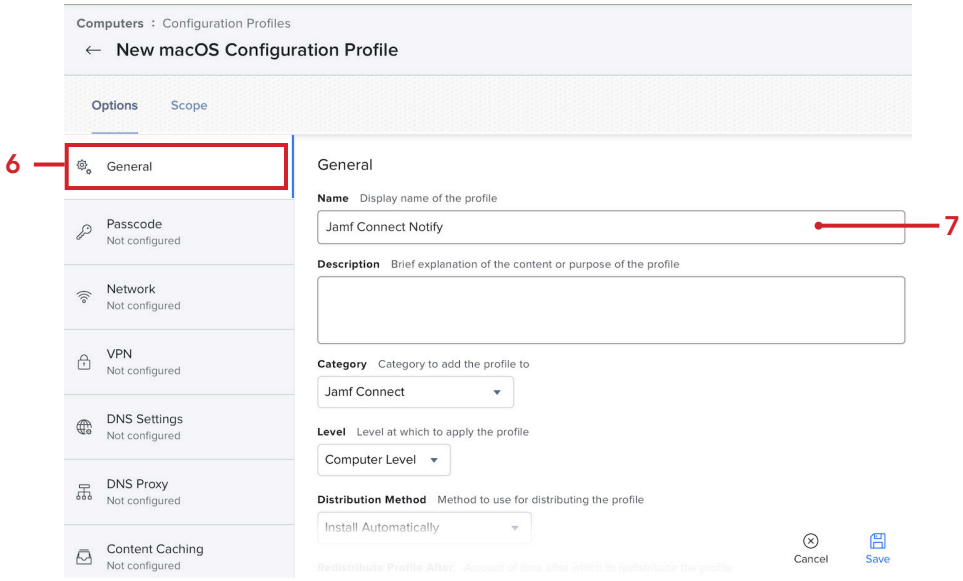


4. Select the Jamf Connect Login configuration profile.

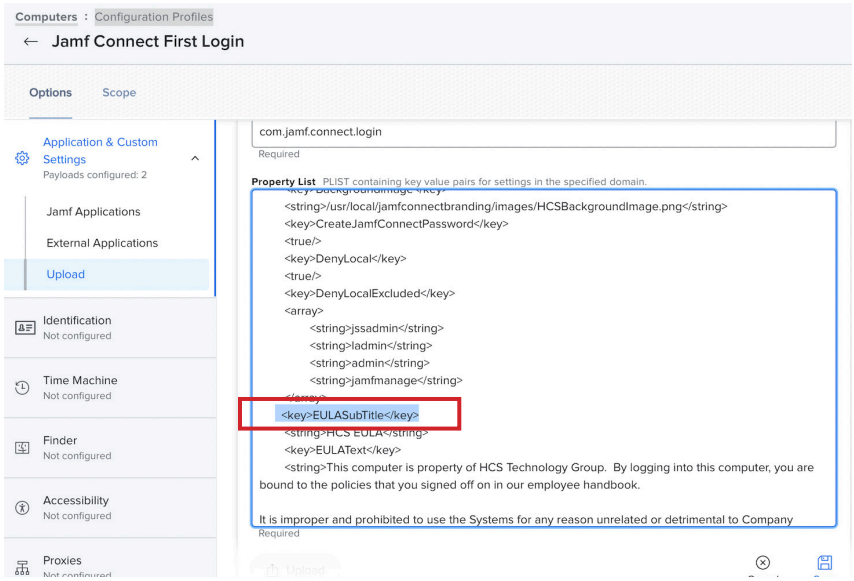
5. Click Clone.
   NOTE: We are cloning this to create a second configuration profile named Jamf Connect First Login that will include the Notify string and the EULA. This is required to use Notify during an Automated Device Enrollment. This profile will be removed after Notify has ran once and will be replaced by another profile named Jamf Connect Login which will stop Notify and the EULA from running at every login.



6. Click the General payload.
7. Change the name to Jamf Connect First Login.



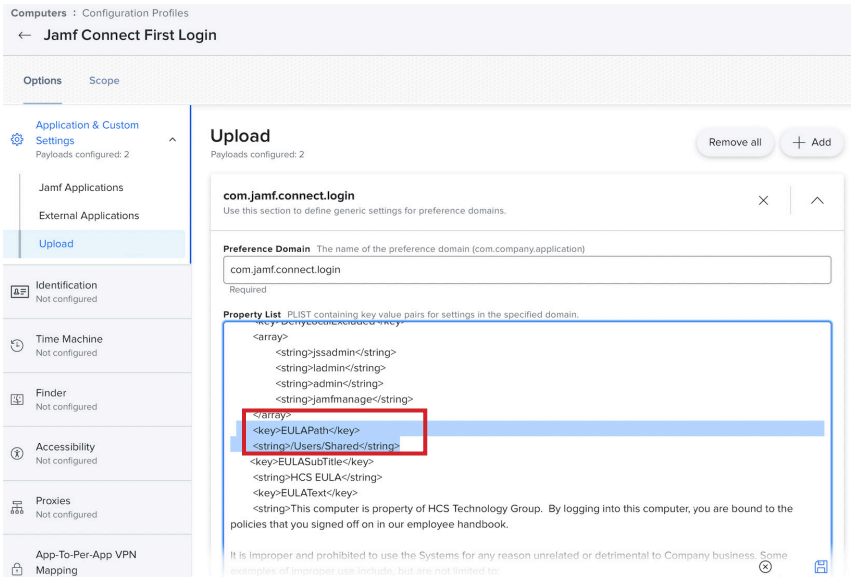
8. Scroll down in the Property List section until you find the key named EULASubTitle as shown below.



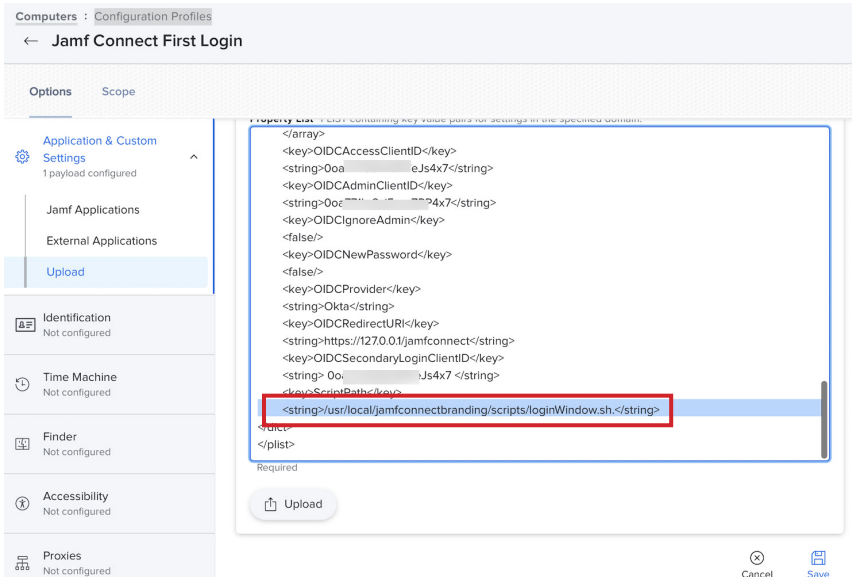
9. Add the XML listed below above the EULASubTitle key.

```
<key>EULAPath</key>
<string>/Users/Shared</string>
```

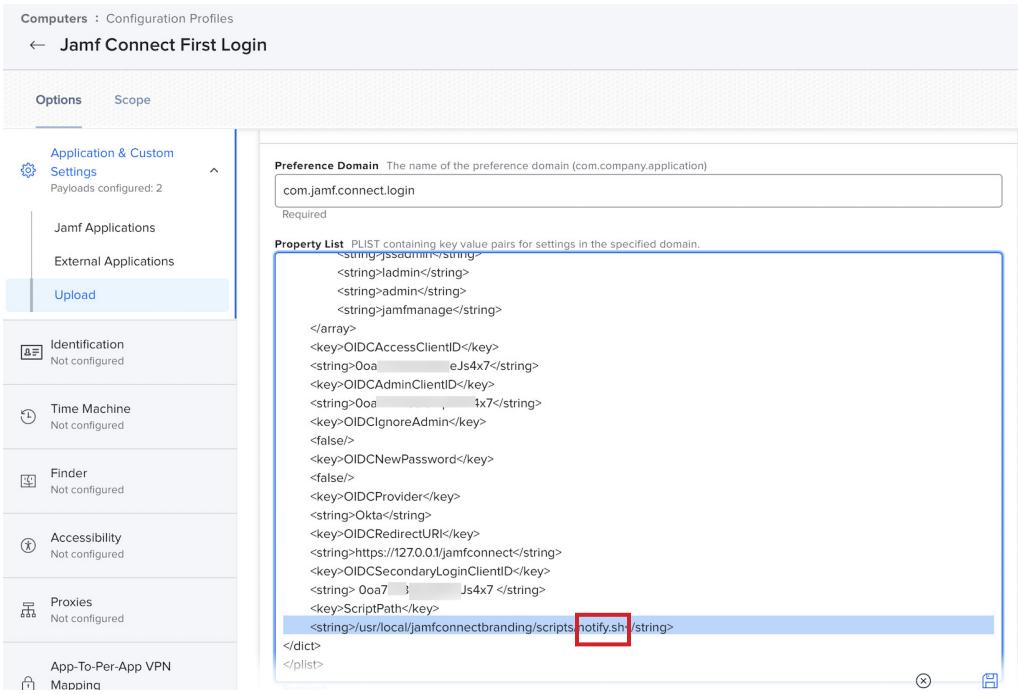
NOTE: We are doing this to record the user accepting the EULA. The acceptance is saved in a file located at /Users/Shared. This file is created automatically by Jamf Connect.



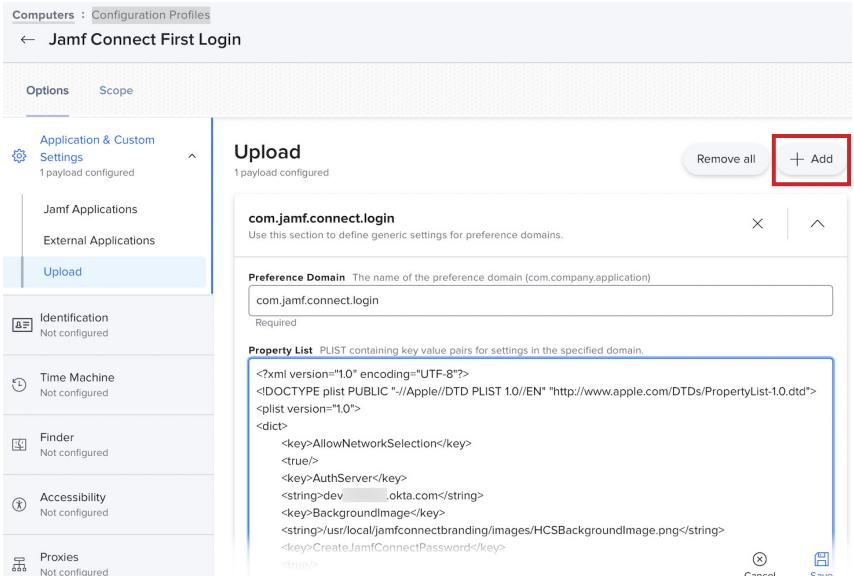
10. Scroll down to the bottom of the Property List section and select the key shown below.



11. Remove loginWindow.sh from the string and replace it with notify.sh. This will allow us to run Notify on first login



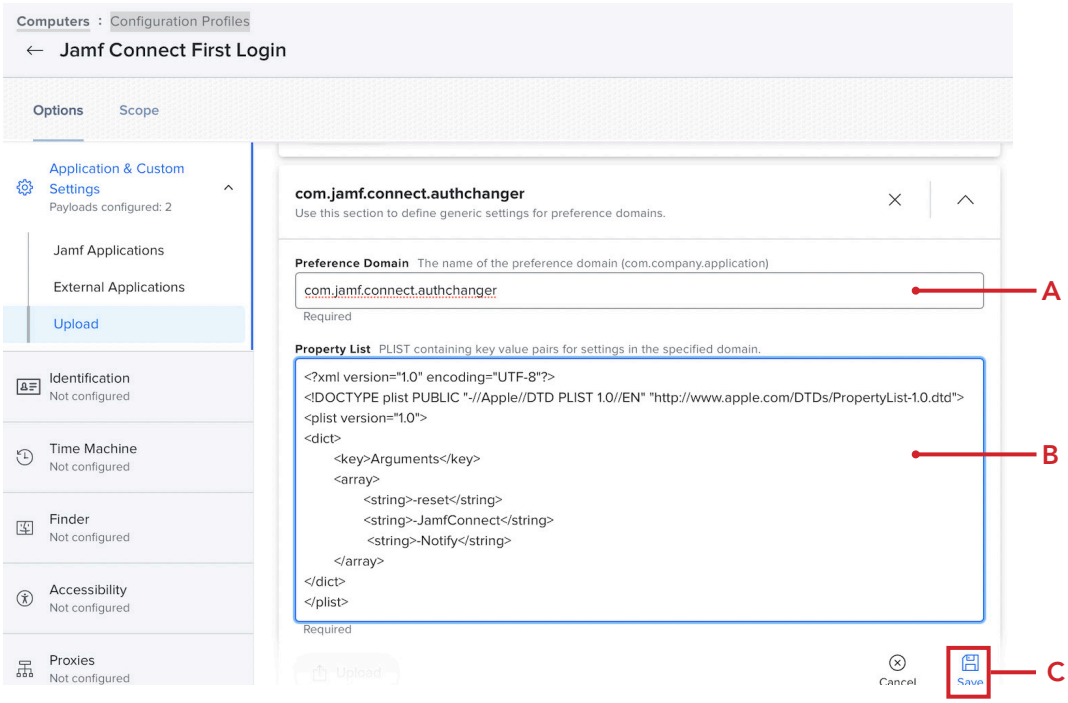
12. Scroll up and click Add to create an additional payload.



13. Scroll down to the newly created payload and enter the following:
    A. Preference Domain: com.jamf.connect.authchanger
    B. Property List: Paste in the XML below.
    C. Click Save.

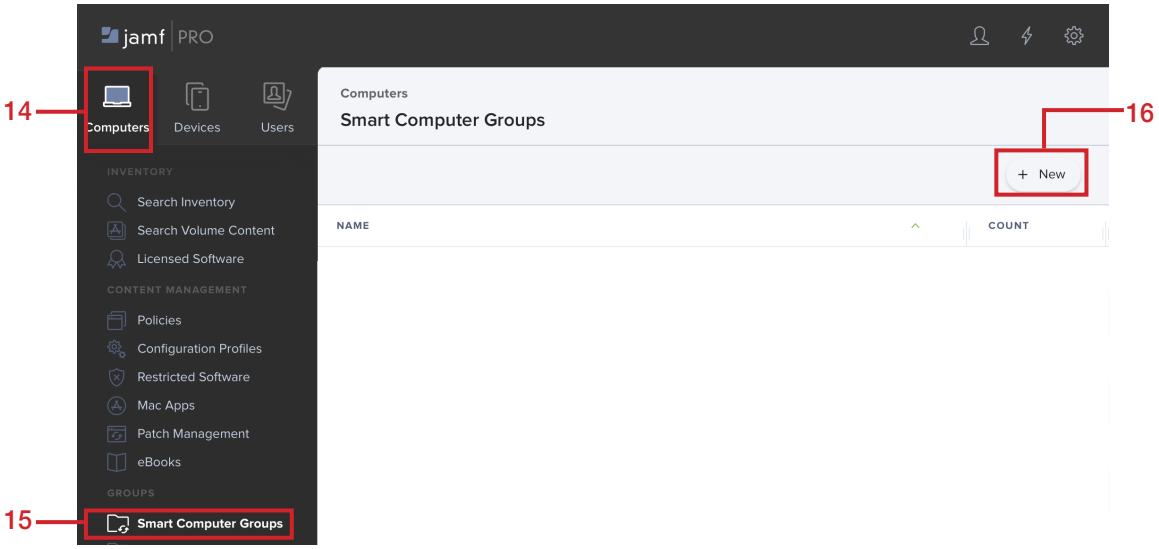
```
<?xml version="1.0" encoding="UTF-8"?>
<!DOCTYPE plist PUBLIC "-//Apple//DTD PLIST 1.0//EN" "http://www.apple.com/DTDs/
PropertyList-1.0.dtd">
<plist version="1.0">
<dict>
     <key>Arguments</key>
     <array>
             <string>-reset</string>
             <string>-JamfConnect</string>
     <string>-Notify</string>
     </array>
</dict>
</plist>
```

NOTE: This payload will allow us to run Notify on first login and will ensure Jamf Connect is the default login window during first login.

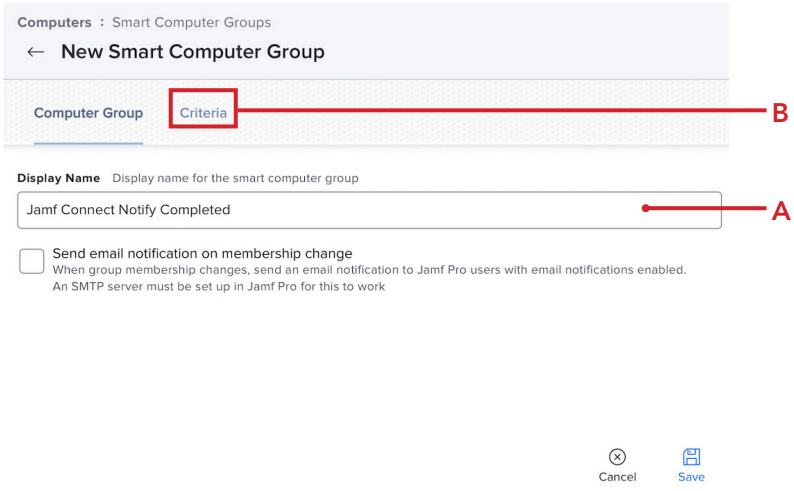


14. Click Computers
15. Click Smart Computer Groups.
16. Click New.

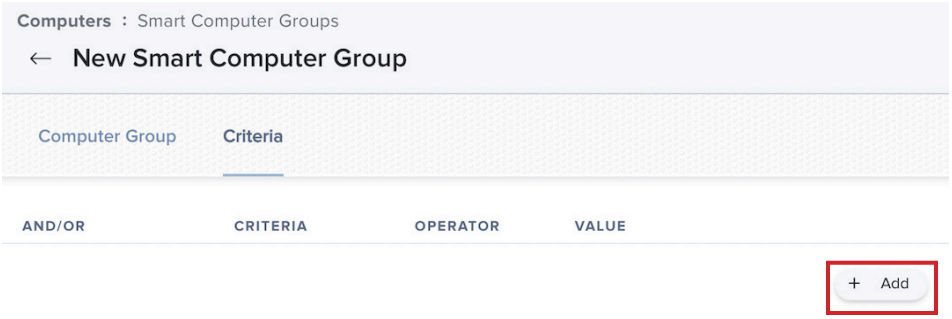
NOTE: We are creating a smart group to find a file named com.jamf.connect.InitialRunDone.pkg which gets created at the end of the notify.sh script. This will let us know that Notify has ran and will allow us to use this criteria in a smart group. Notify and the EULA only need to run once and we need a way to remove the Jamf Connect Login configuration profile so it does not run at every login.



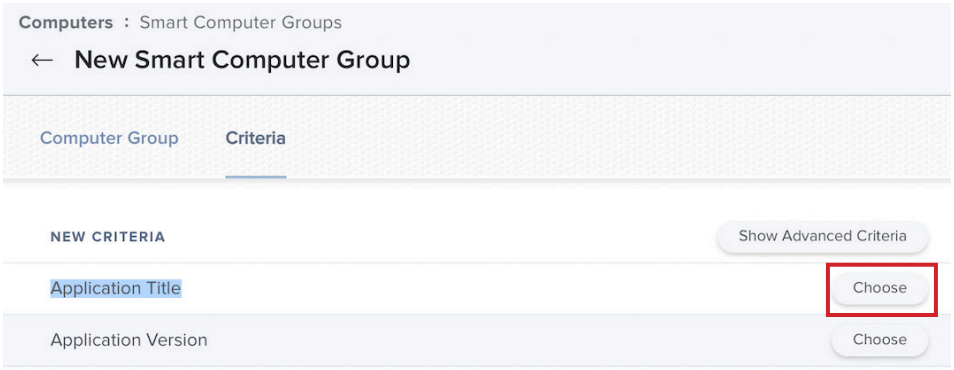
17. Enter the following:
    A. Display Name: Jamf Connect Notify Completed
    B. Click Criteria



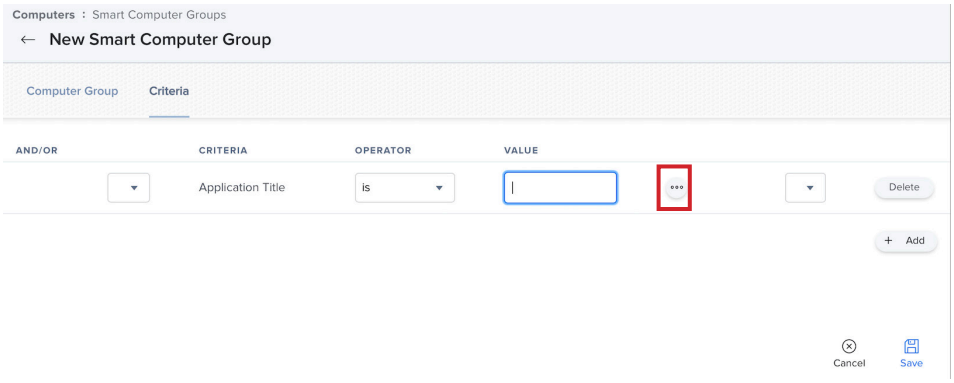
18. Click Add.



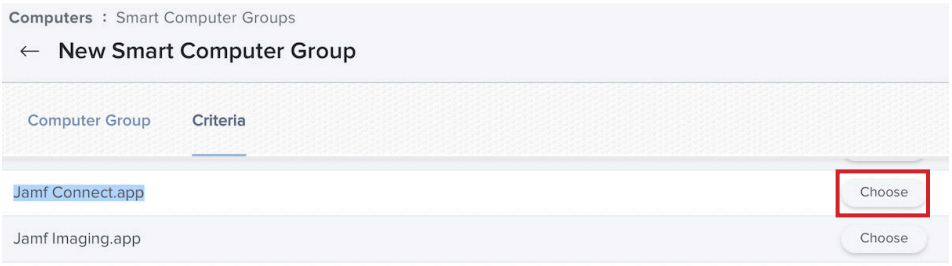
19. For Application Title, click Choose.



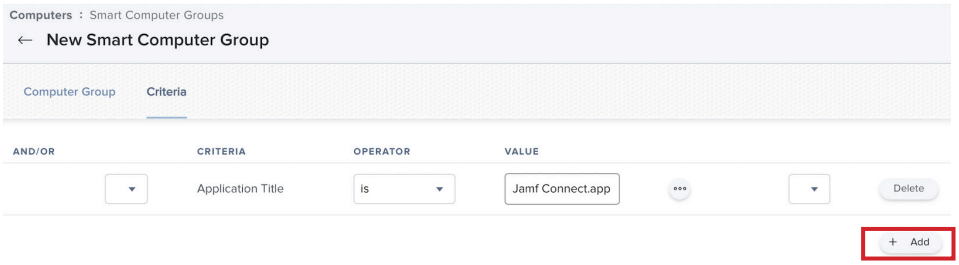
20. Click Choices (⋯).



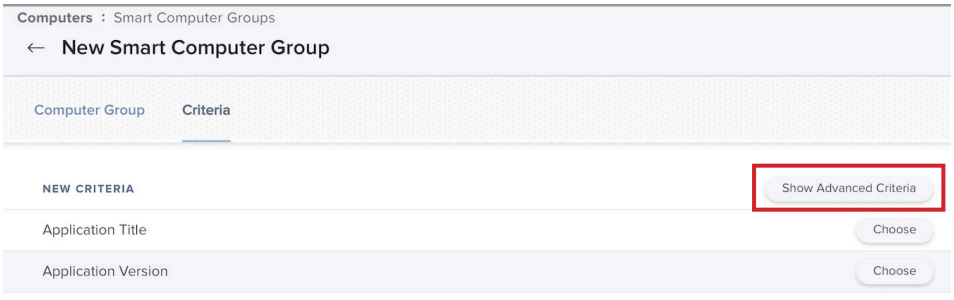
21. Scroll down until you find Jamf Connect.app, then click Choose.



22. Click Add.



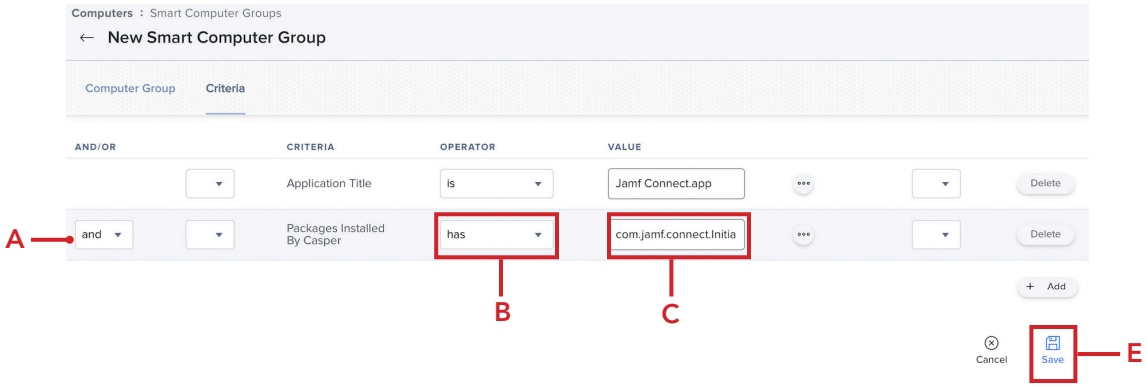
23. Click the Show Advanced Criteria button.



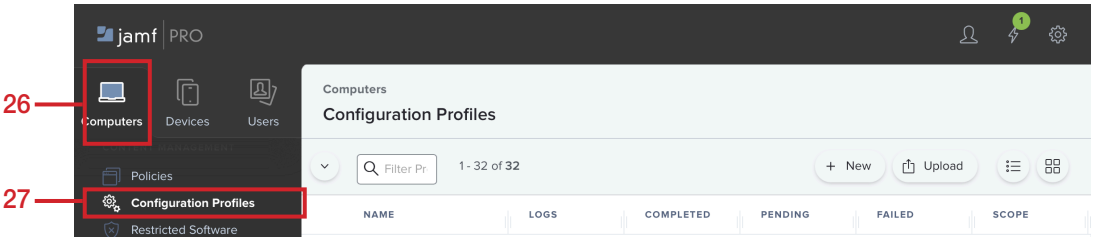
24. Scroll down to find Packages Installed By Casper then click Choose.

25. Configure the following:
    A. AND/OR: Make sure "and" is selected
    B. OPERATOR: has
    C. VALUE: com.jamf.connect.InitialRunDone.pkg
    D. Confirm your settings look like what is shown in the picture below
    E. Click Save

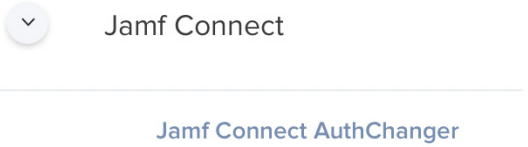
    NOTE: com.jamf.connect.InitialRunDone.pkg is case sensitive.



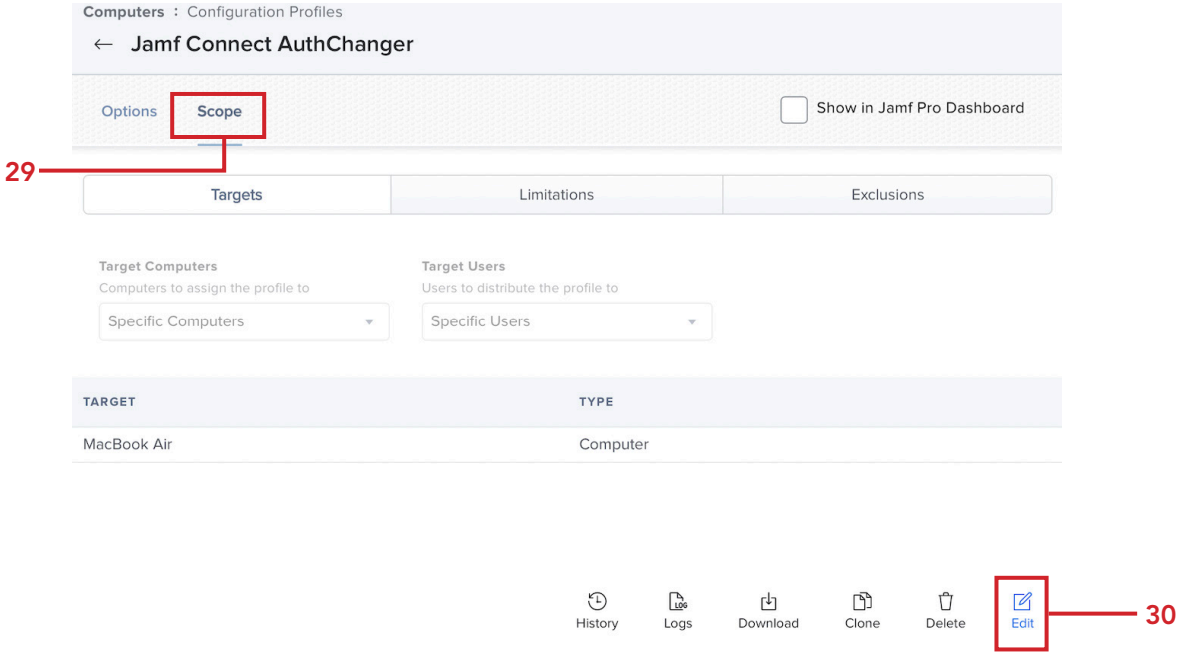
26. Click Computers.
27. Click Configuration Profiles.



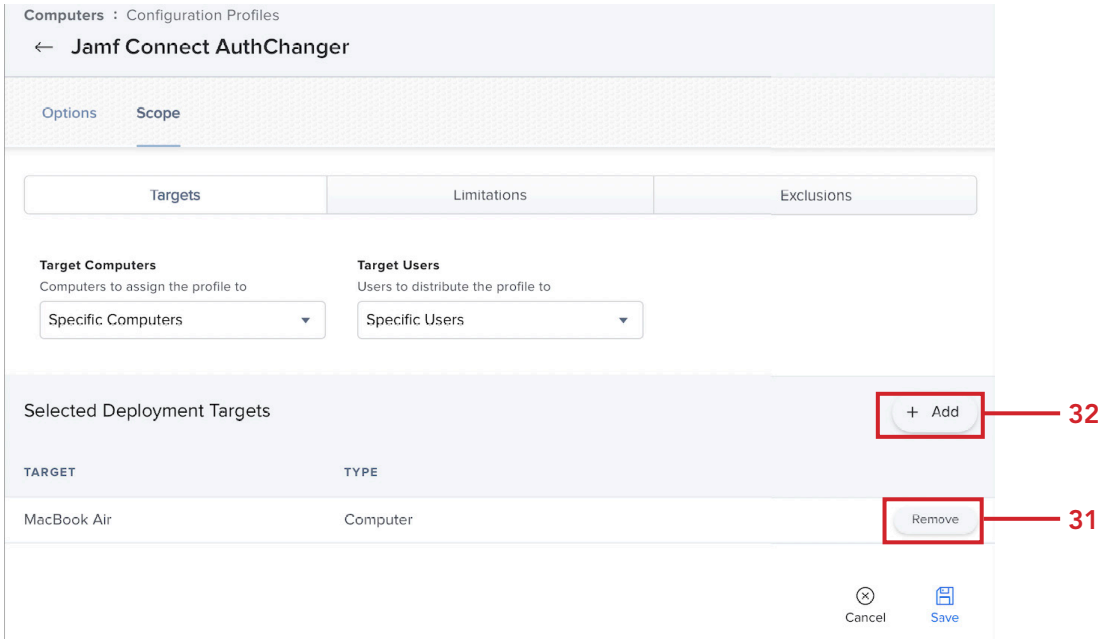
28. Click the Jamf Connect AuthChanger configuration profile.



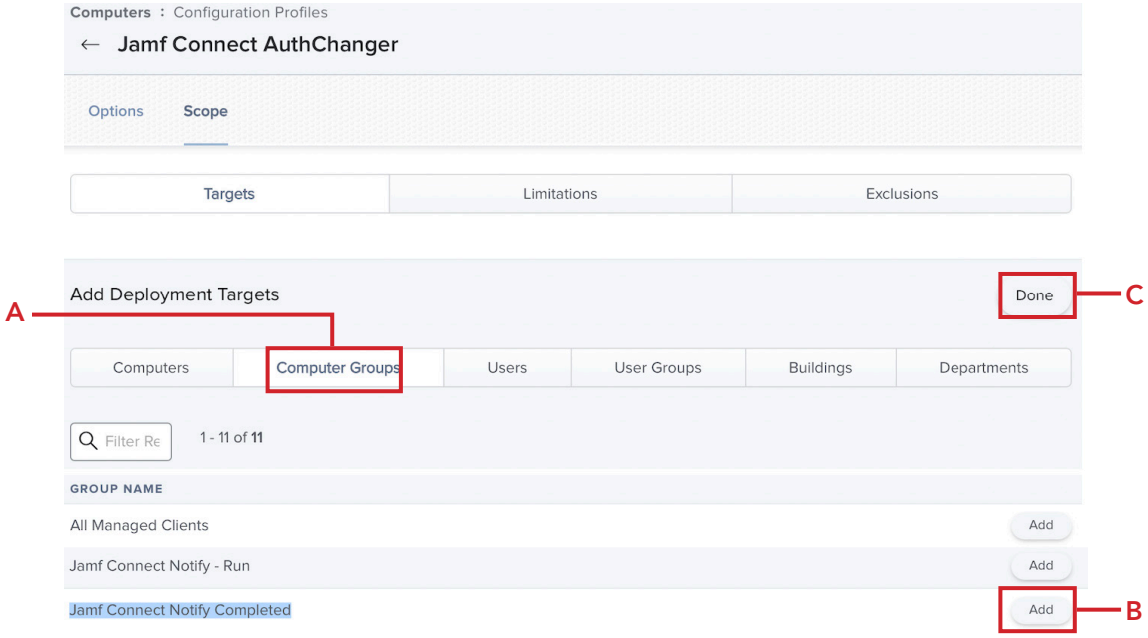
29. Click Scope
30. Click Edit.



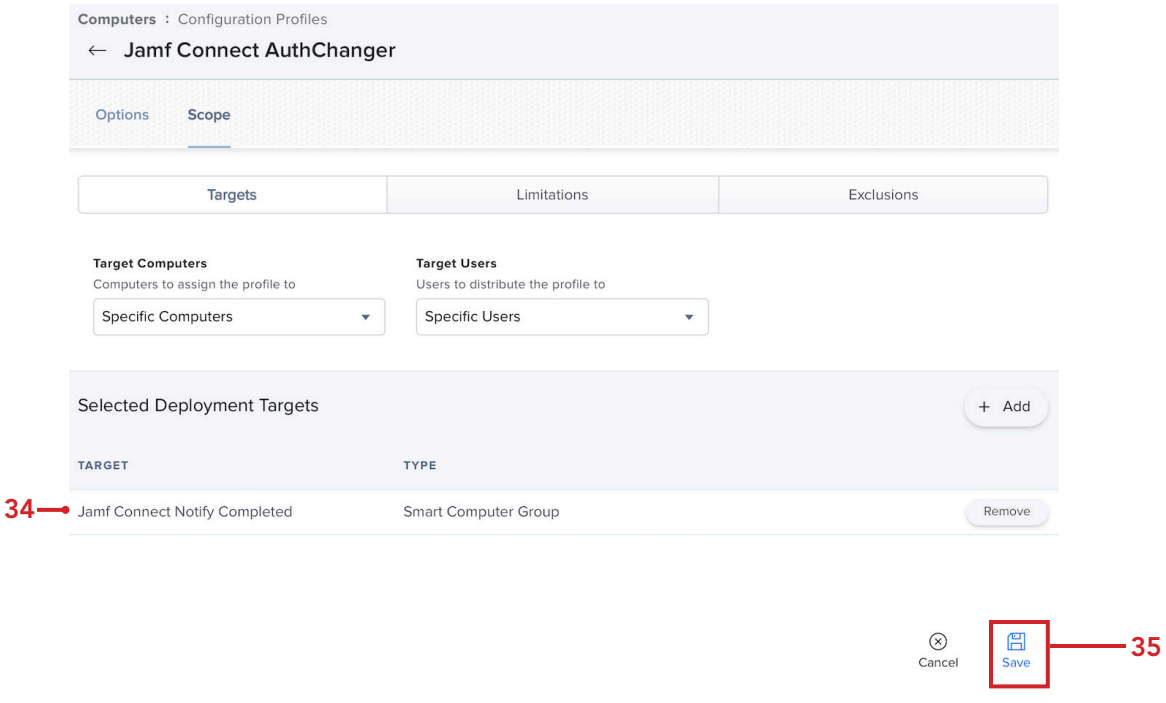
31. Remove any previously scoped devices by clicking Remove.
32. Click Add.



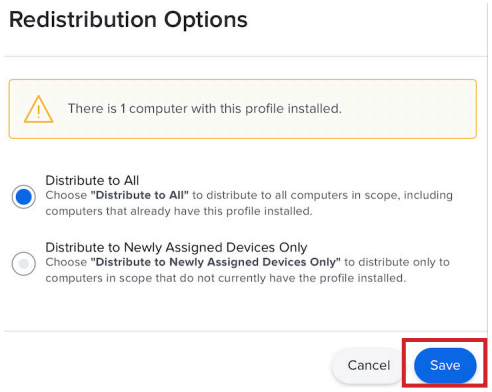
33. Follow these steps:
    A. Click Computer Groups
    B. Click Add for the Jamf Connect Notify Completed group.
    C. Click Done



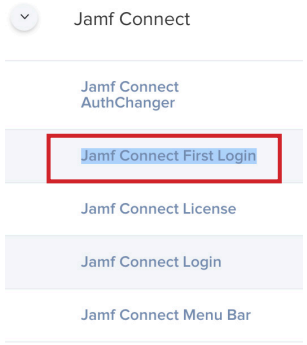
34. Confirm the Jamf Connect Notify Completed group is listed.
35. Click Save.
    NOTE: This will ensure that only Mac Computers that completed installing Jamf Connect and ran Notify will get this profile. This profile does NOT include the Notify string and will ensure Jamf Connect is the default Login Window on the Mac Computer.



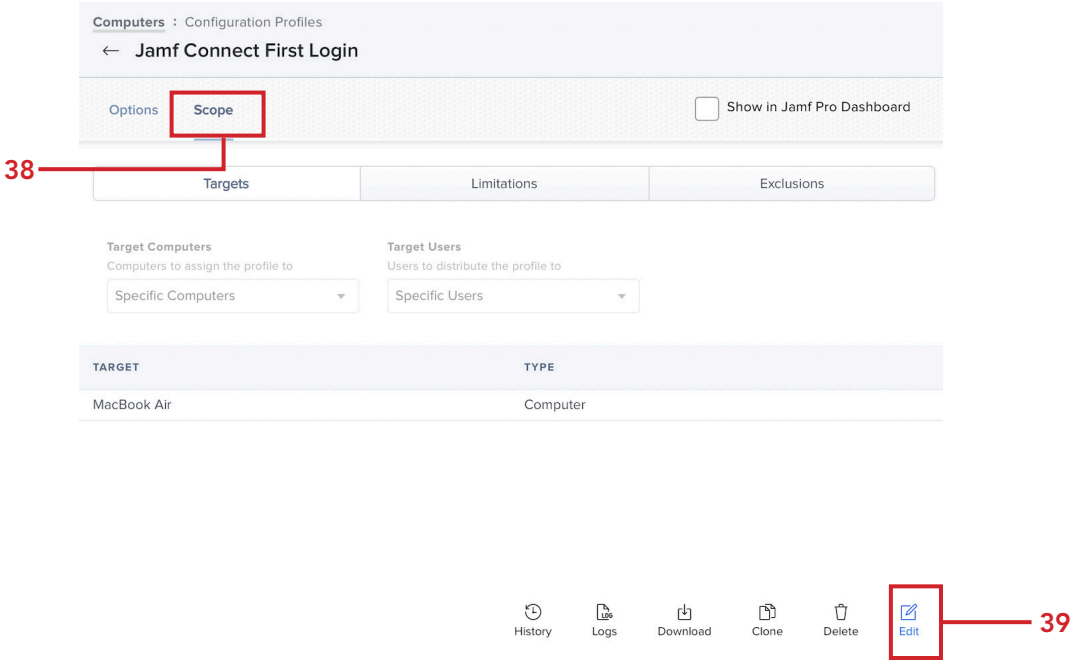
36. Confirm a message appears on how to redistribute the profile, pick what works best for you. This guide will choose distribute to all. Click Save.



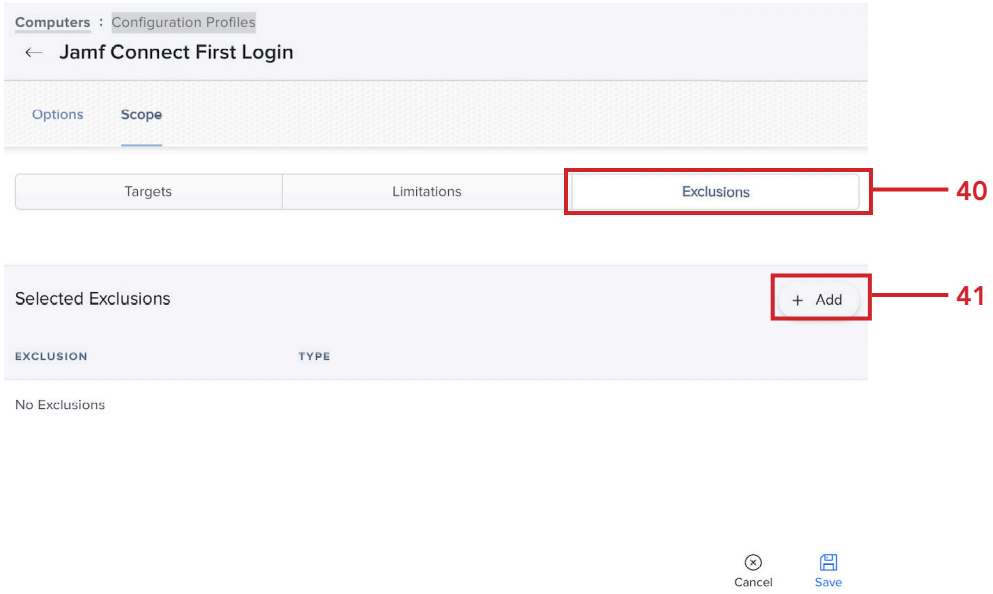
37. Click the Jamf Connect First Login configuration profile.



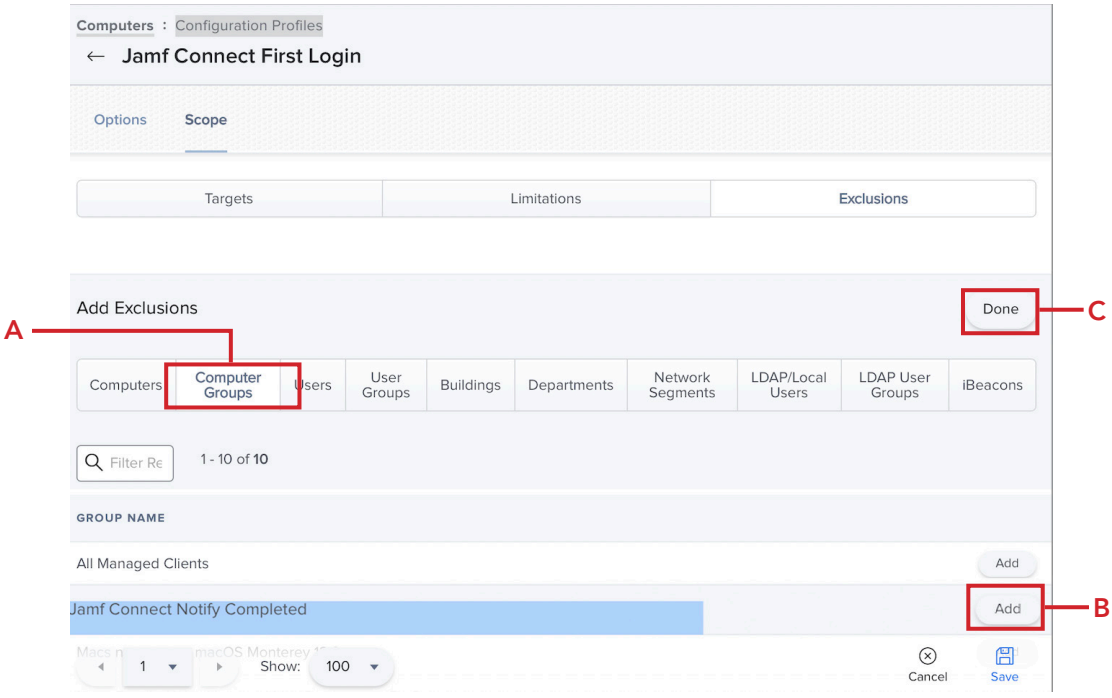
38. Click Scope.
39. Click Edit.



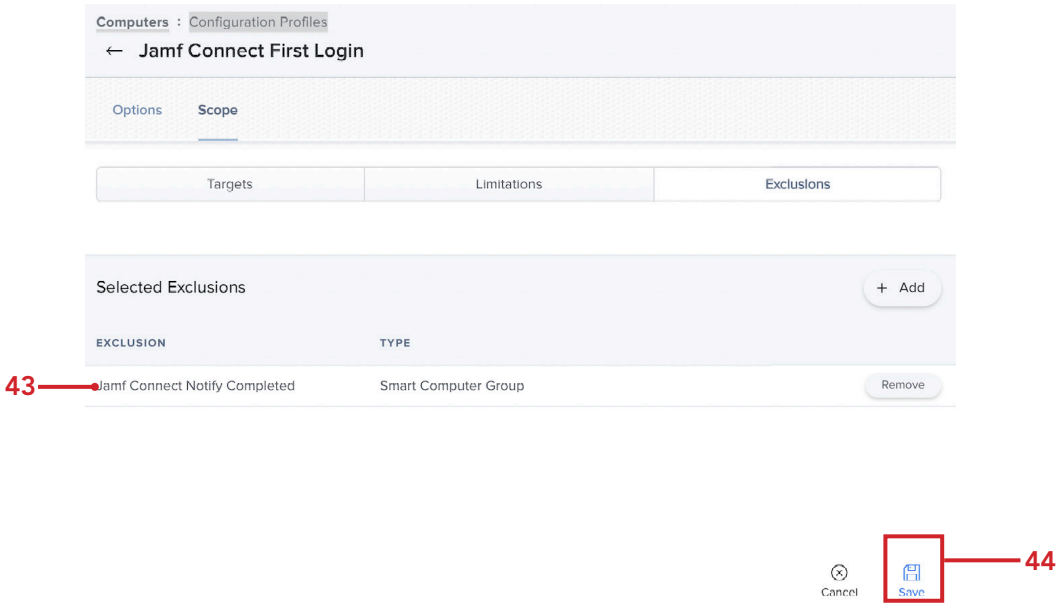
40. Click Exclusions.
41. Click Add.



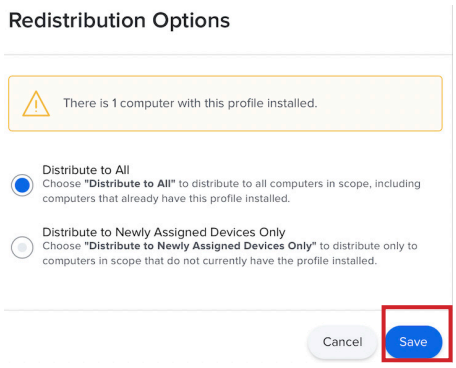
42. Follow these steps:
    A. Click the Computer Groups tab
    B. Add the Jamf Connect Notify Completed group.
    C. Click Done



43. Confirm the Jamf Connect Notify Completed group is listed.
44. Click Save.
    NOTE: This will ensure that the Jamf Connect First Login profile gets removed from a Mac Computer once Jamf Connect has been installed and Notify has run. This will stop Notify and the EULA from running at every login to your Mac computer.

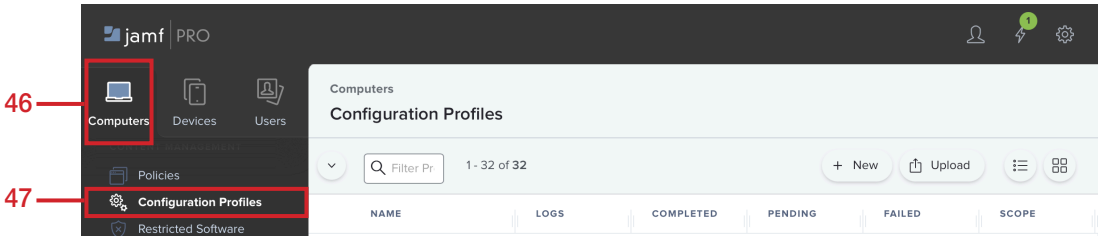


45. Confirm a message appears on how to redistribute the profile, pick what works best for you. This guide will choose distribute to all. Click Save.

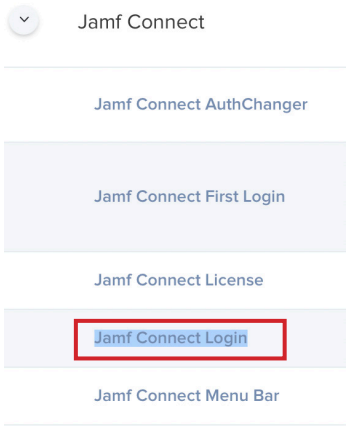


Let's edit the Jamf Connect Login configuration profile to remove the EULA. The EULA was originally part of this profile when created in section 5 of this guide.

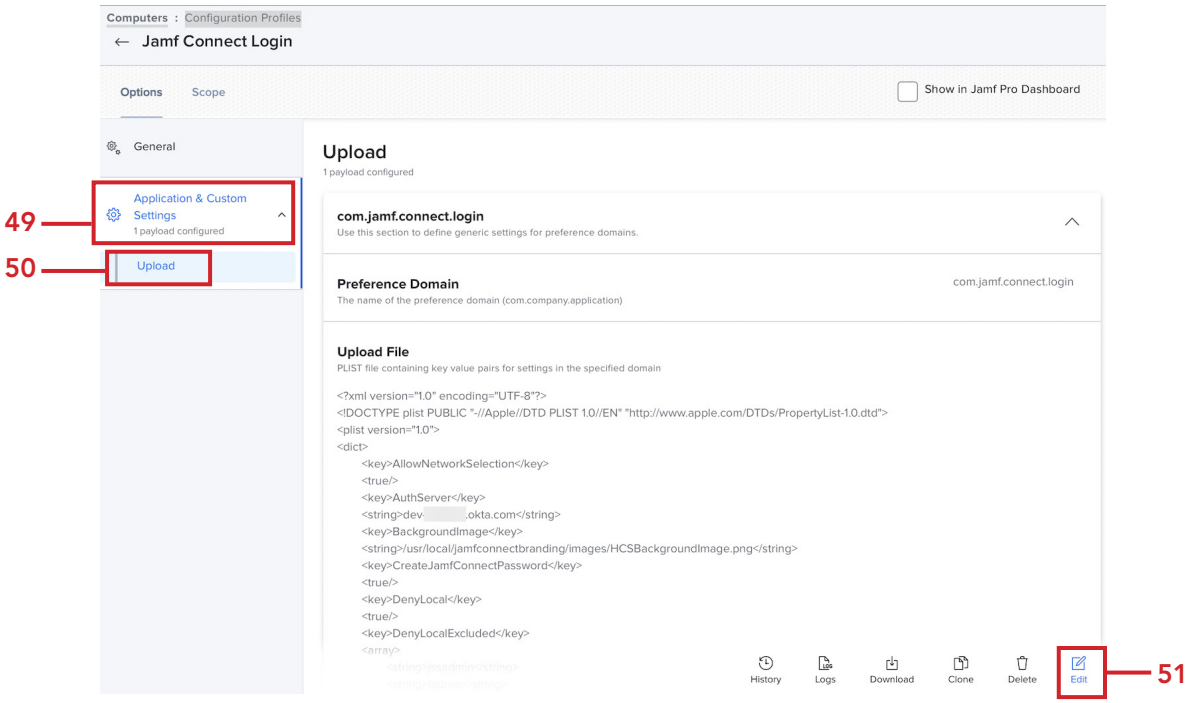
46. Click Computers.
47. Click Configuration Profiles.



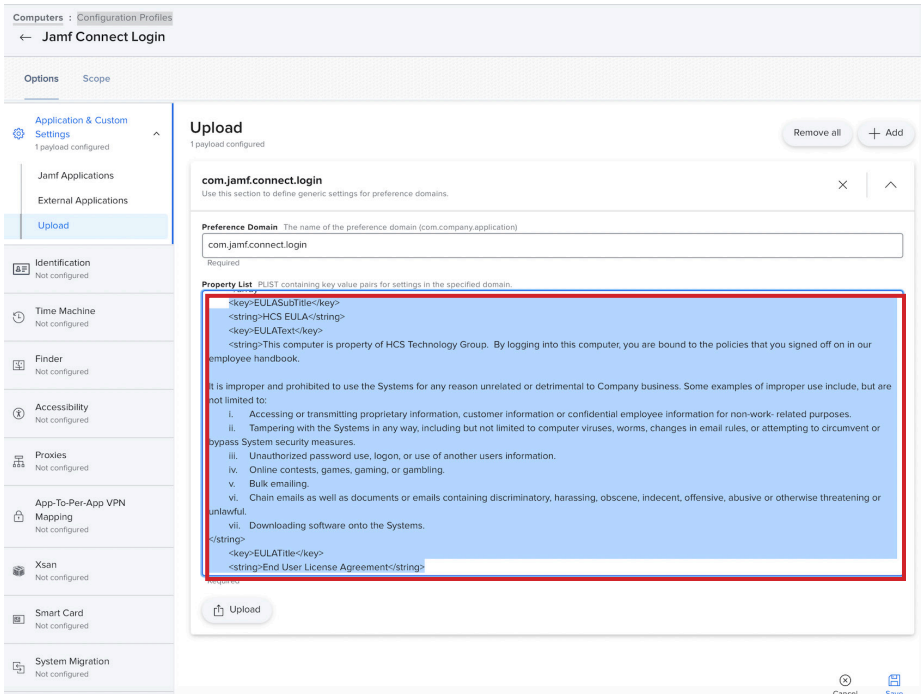
48. Click the Jamf Connect Login configuration profile.



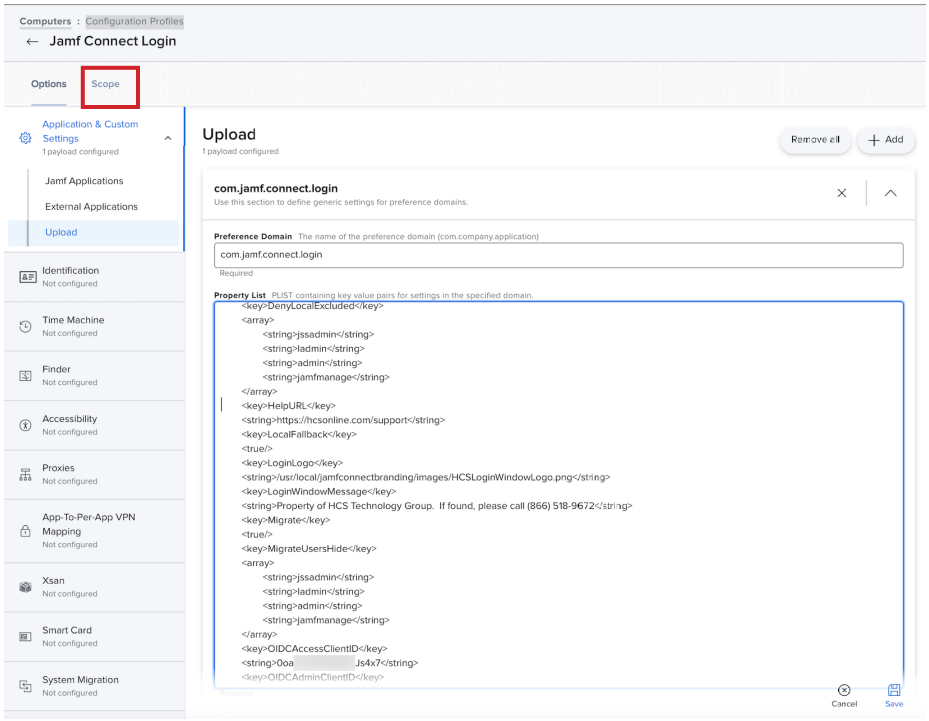
49. Expand the Application & Custom Settings payload.
50. Click Upload,
51. Click Edit.



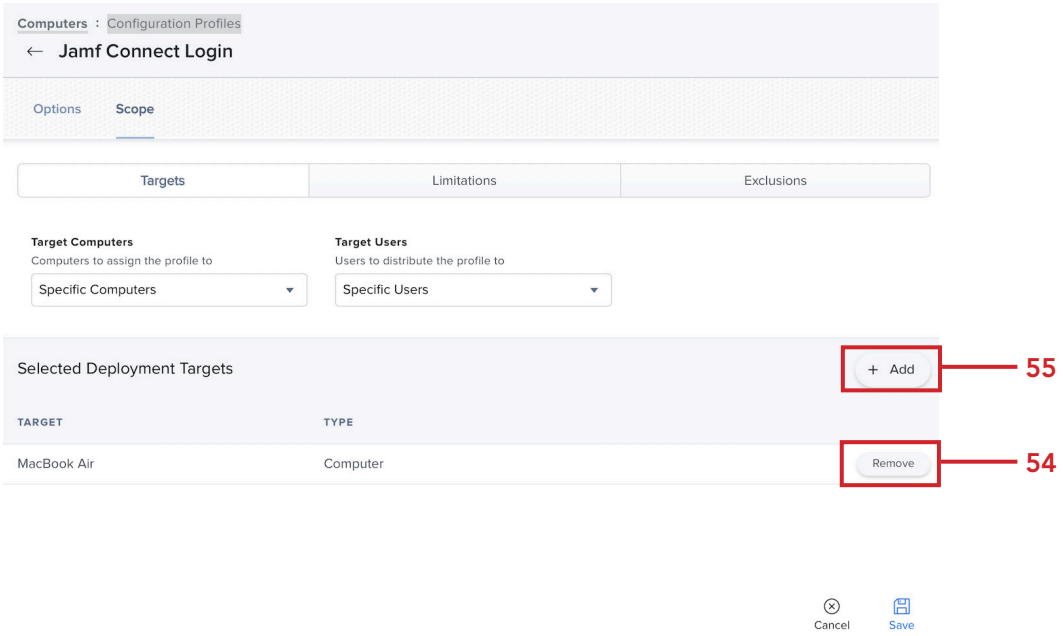
52. In the Property List section, Select everything between the EULASubTitle key and the End User License Agreement key and delete it. This will remove the EULA from this configuration profile as we no longer need it.



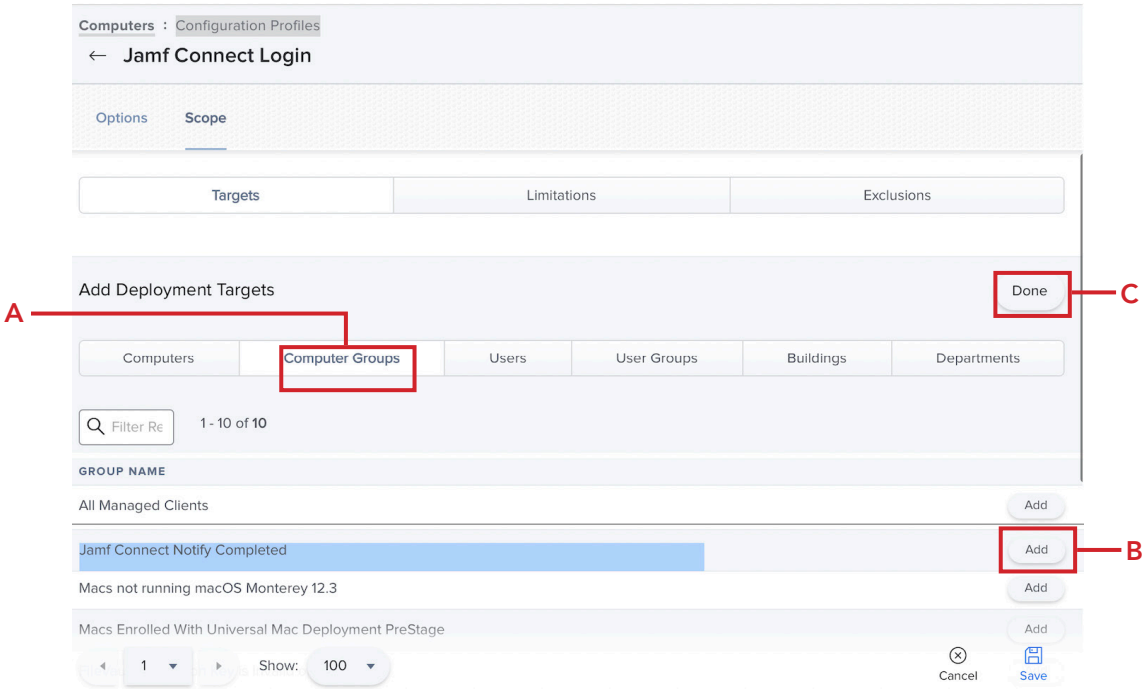
53. Confirm the EULA keys are gone, then click Scope.



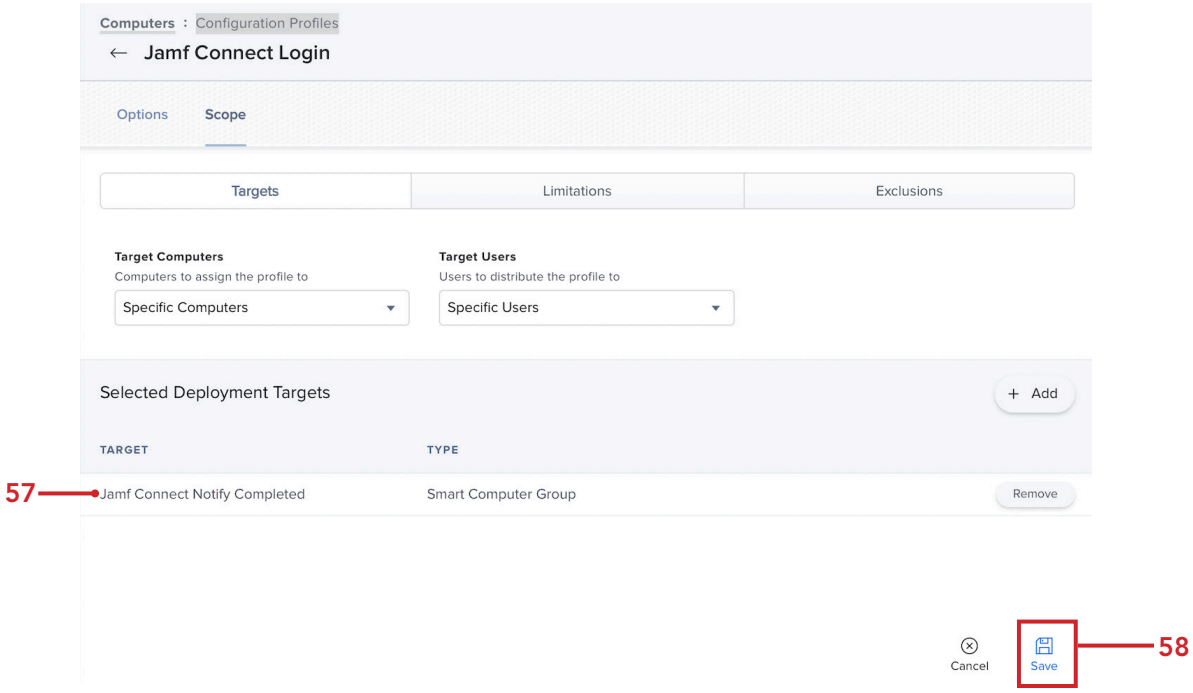
54. Remove any previously scoped devices.
55. Click Add.



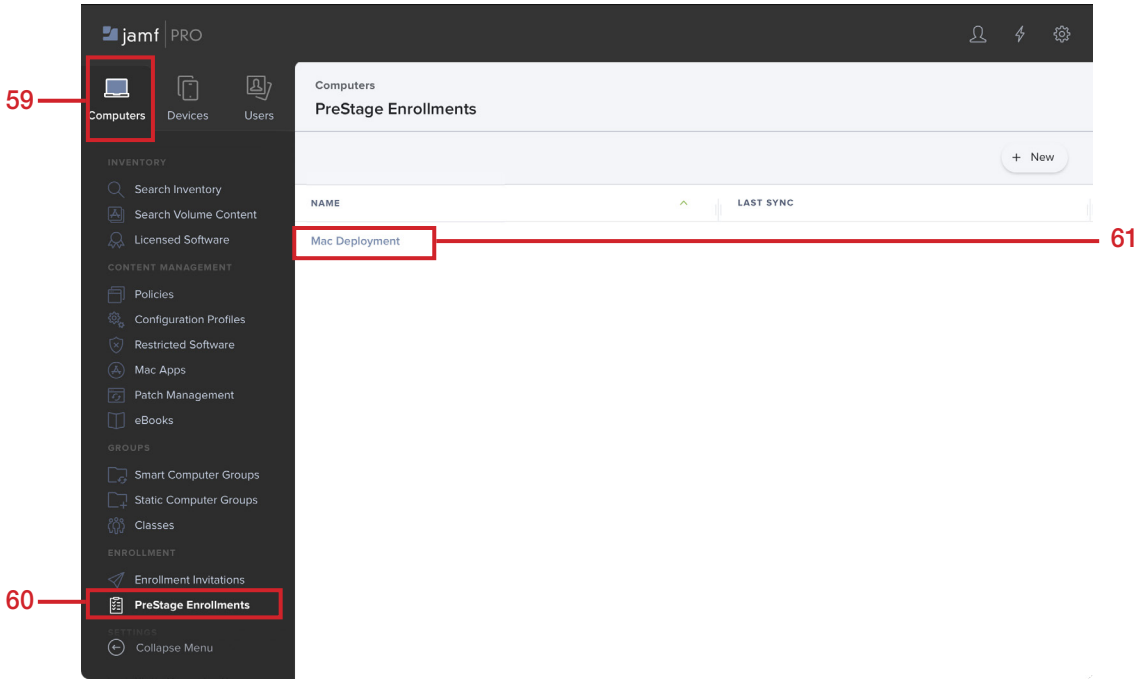
56. Follow these steps:
    A. Click Computer Groups
    B. Add the Jamf Connect Notify Completed group.
    C. Click Done



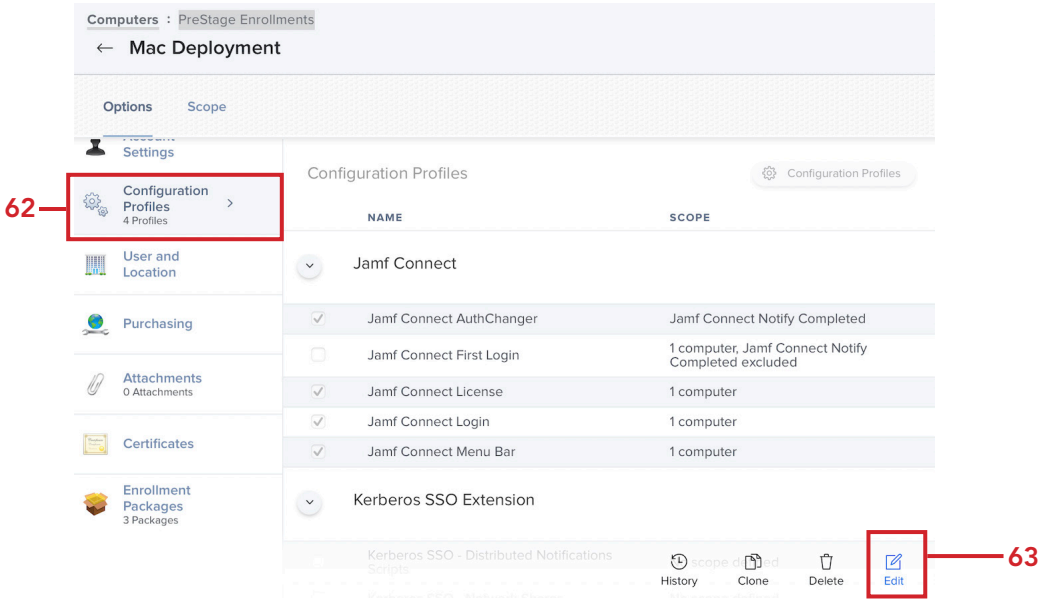
57. Confirm the Jamf Connect Notify Completed group was added
58. Click Save.



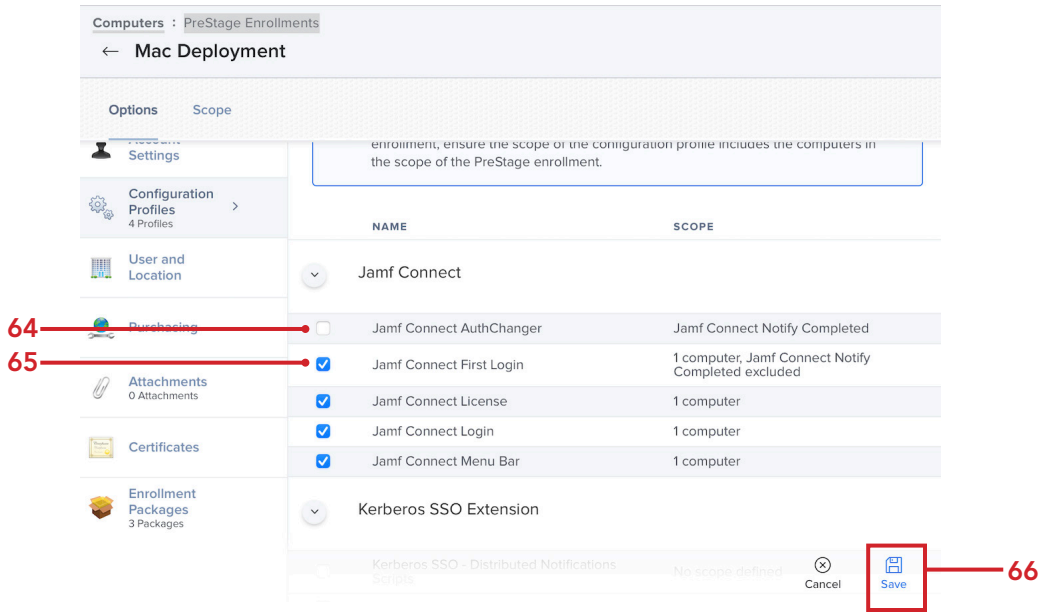
59. Click Computers
60. Click PreStage Enrollments.
61. Click on your PreStage. This guide will use the Mac Deployment PreStage.



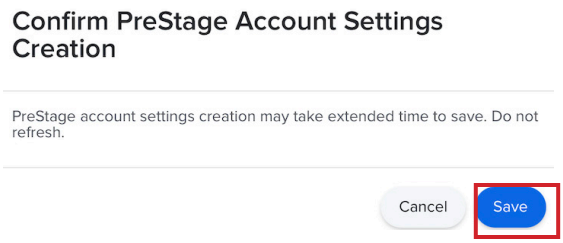
62. Select the Configuration Profiles payload
63. Click Edit.



64. Deselect the checkbox for Jamf Connect AuthChanger profile.
65. Select the checkbox for Jamf Connect First Login profile.
66. Click Save.



67. Click Save.



In the next section, we will deploy a Mac Computer via Automated Device Enrollment to see the Notify and EULA screens in action.

This completes this section.

Section 10: Deploying a Mac Computer with Jamf Connect Notify

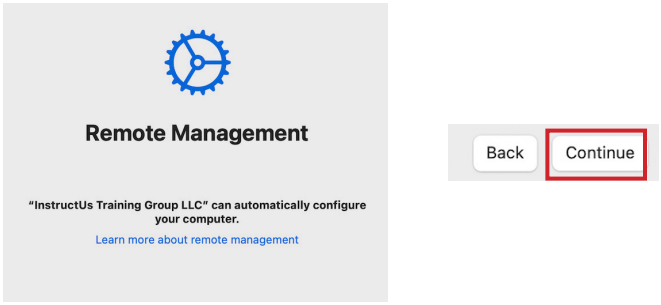
This section is optional and assumes you followed the guide from the beginning. Items discussed in this section build upon other sections in this guide. In this section we will deploy a Mac computer using the PreStage enrollment that we edited in section 9 and confirm Jamf Connect Notify runs after the first login. We will also confirm the Jamf Connect First Login Profile is no longer on the Mac computer after Notify runs and the AuthChanger profile is installed after Notify has completed.

Requirements for following along with this section:

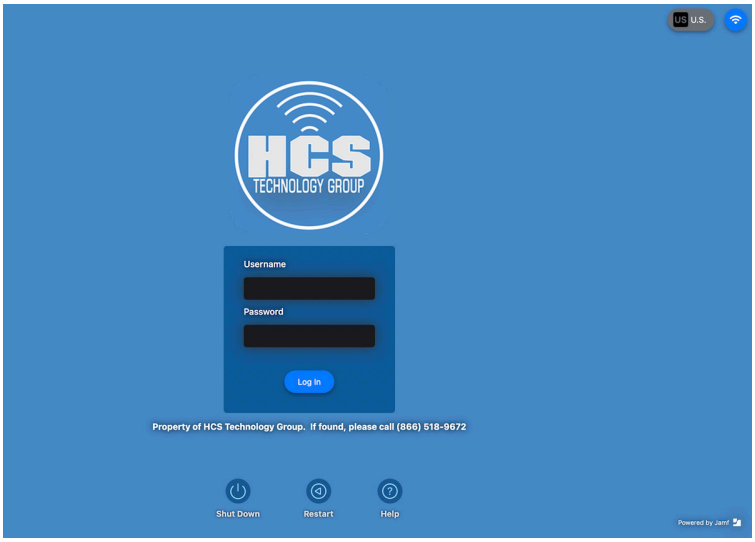
- A Mac computer that's brand new in the box or an old Mac computer that was erased and has a new macOS installed (10.15.4 or later). The Mac computer must be enrolled in Apple Business or School Manager and assigned to your PreStage in Jamf Pro. This is required for Automated Device Enrollment using a Jamf Pro PreStage.
- Okta login credentials. We recommend using a NON admin account when logging in at the Jamf Connect Login window to see how role based account creation works. This will create the user on the Mac computer as a standard user which is their role in Okta.

NOTE: This section will NOT walk through all the setup assistant screens as this would be different in every environment based on the settings you used for your PreStage. We will start at the Remote management screen so please follow the on screen instructions that come before the Remote Management screen.

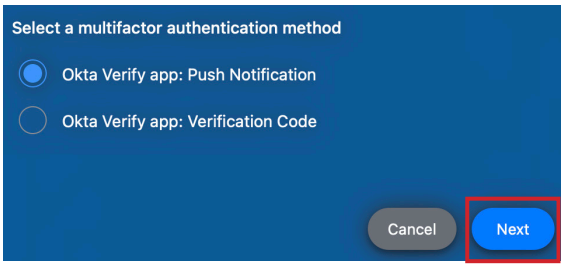
1. At the Remote Management screen, click Continue.



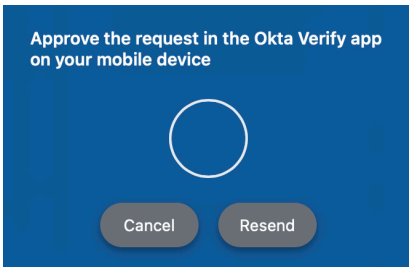
2. Enter your Okta Username and Password then click Log In.



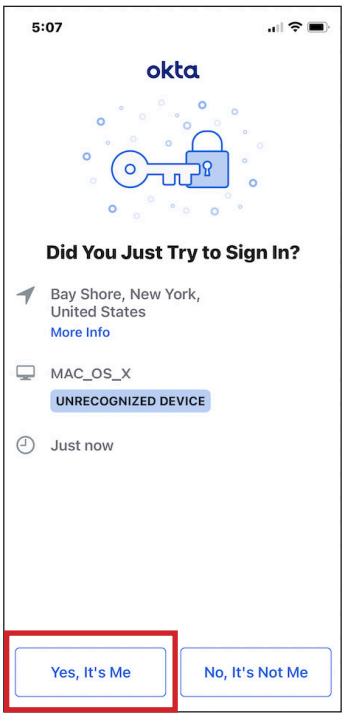
3. Select your MFA authentication method. This guide will use a Push Notification. Click Next.



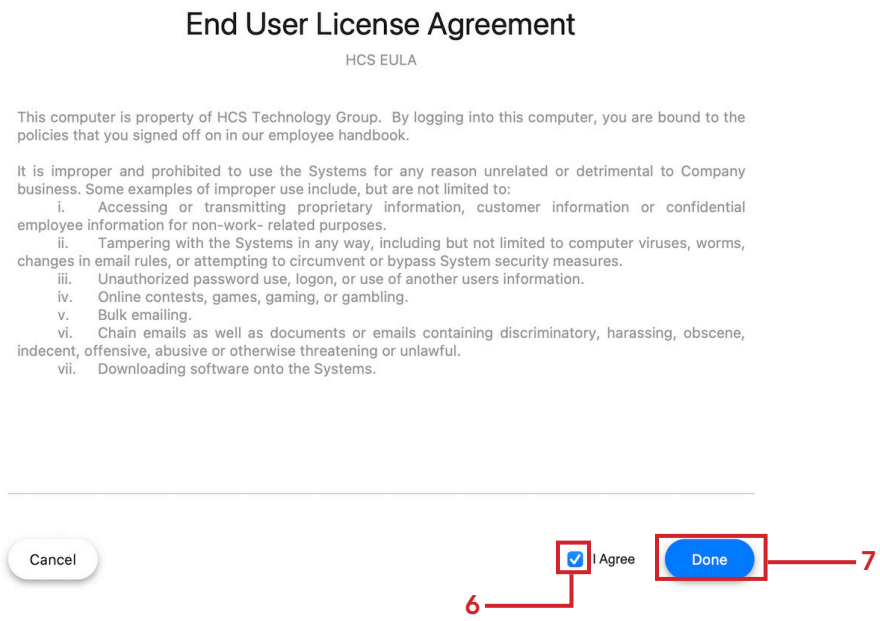
4. You will be prompted with the message below and a notification will be sent to your phone.



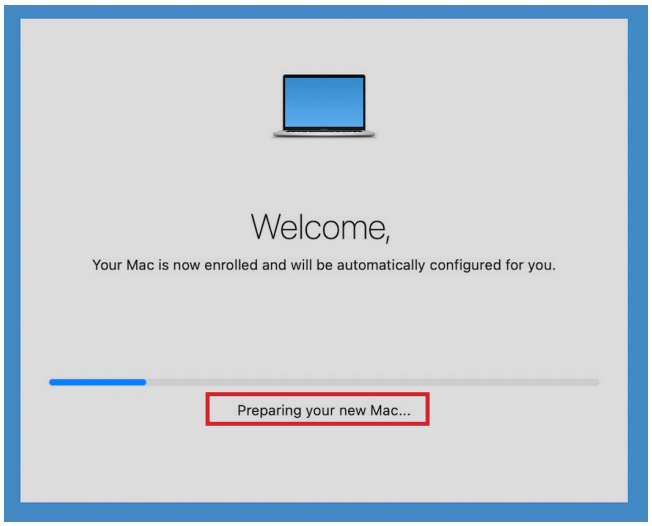
5. Confirm you received a notification on your phone, Tap Yes, It's Me.



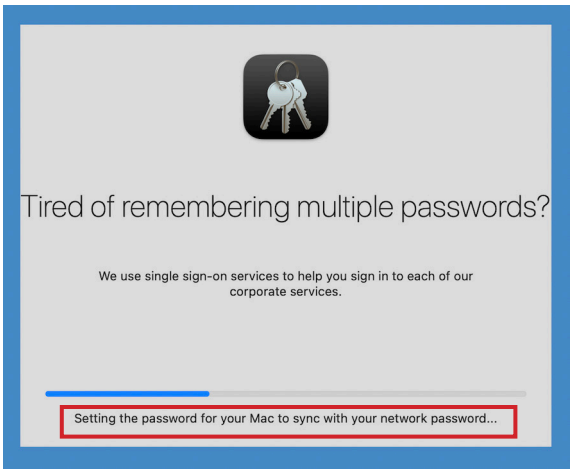
6. Select the checkbox for I Agree.
7. Click Done.



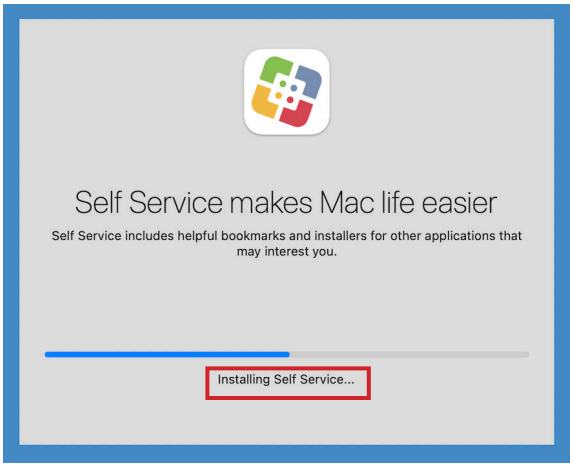
8. The Notify welcome screen will be displayed.



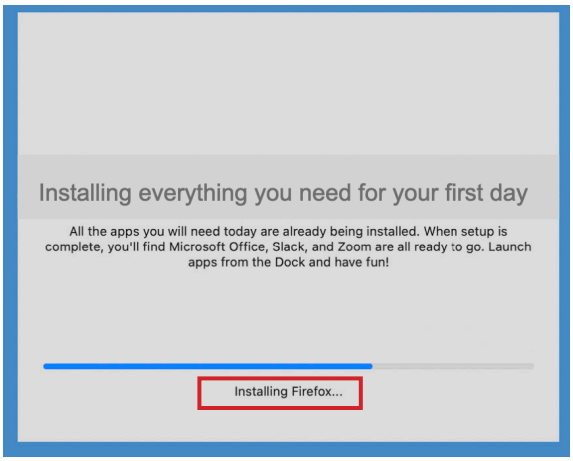
9. Notify will display different screens based on its progression.



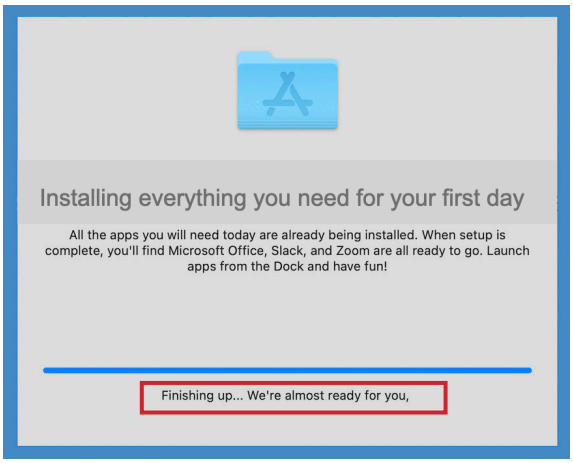
10. Notify will let you know when applications are being installed.



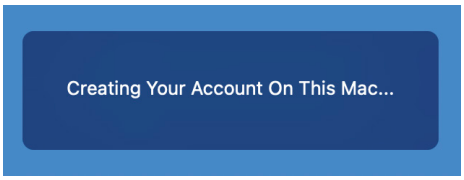
11. Another application being installed. You can add custom icons if needed.
NOTE: Customizing Notify is not covered in this guide.



12. Notify will let you know when it's finishing up the install.

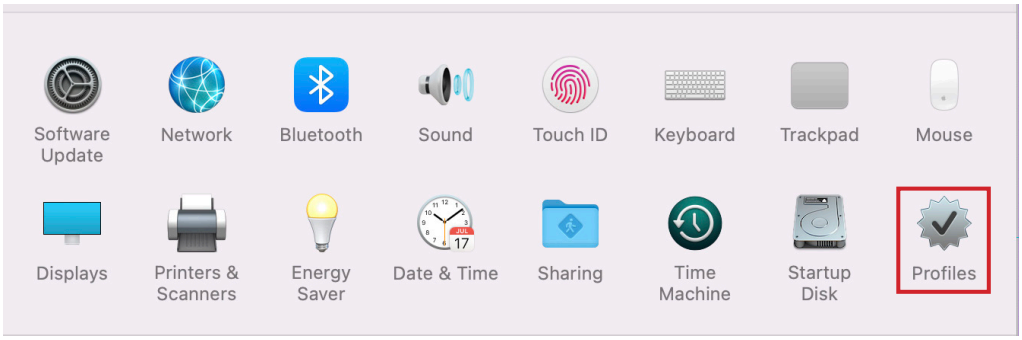


13. When Notify is done, Your account will be created on the Mac computer.

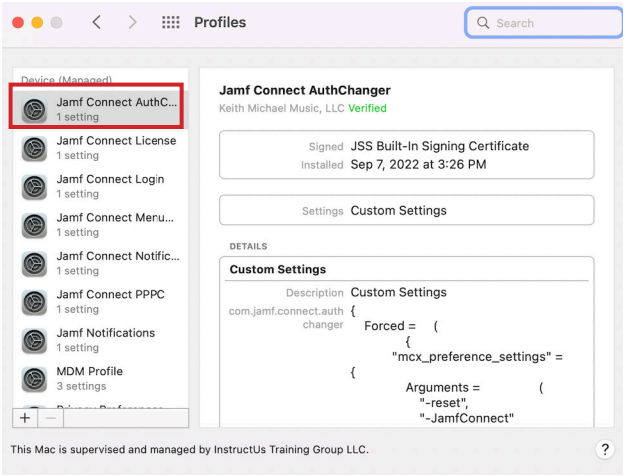


14. Open System Preferences.

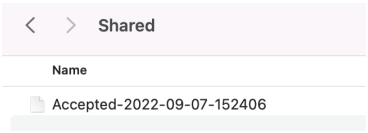
15. Click Profiles.



16. Confirm the Jamf Connect First Login profile is no longer installed and the Jamf Connect AuthChanger profile is installed. Quit system preferences when done.



18. Navigate to /Users/Shared. You will see a file similar to the file shown below. This is an audit file that got created when the EULA was accepted by the user that logged into the Mac computer. NOTE: You can create an extension attribute to search for a file that contains the word Accepted in the name. Once done, you can create a smart group to find all Mac computers that contain that file which means the EULA has been accepted by the user. This is great for reporting purposes.



If you want to be sure that Notify and the EULA will NOT run again, logout as the user then log back in to confirm all is working as expected.

In the next section we will cover configuring Jamf Unlock.

This completes this section.

Section 11: Configure Jamf Connect Unlock

This section is optional and assumes you followed the guide from the beginning. Items discussed in this section build upon other sections in this guide. In this section we will configure Jamf Unlock. Jamf Unlock is a mobile app that enables users to unlock their Mac computer without using a password. With Jamf Unlock, users complete a setup process to generate identity credentials (a certificate) on their mobile device and pair the device with their Mac computer. Once complete, users can use the app to authenticate in the following scenarios:

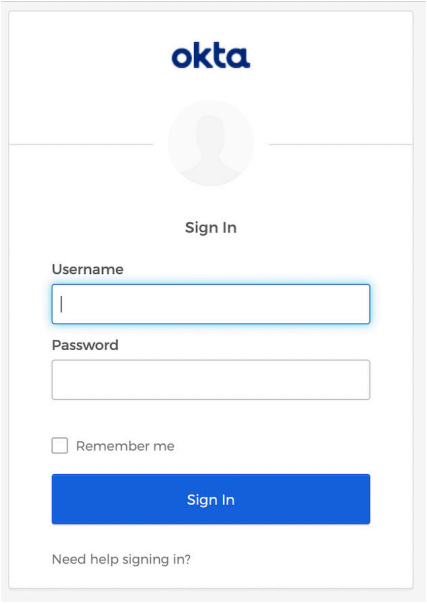
- Logging into a Mac computer - NOTE this only works at the default Mac computer's Login Screen and not the Jamf Connect Login screen. If using Jamf Connect at the login window, Jamf Unlock will only allow you to unlock your Mac computer from the lock screen.
- Changing settings in System Preferences
- Installing software updates
- Executing commands with root privileges using the sudo command

Requirements for following along with this section:

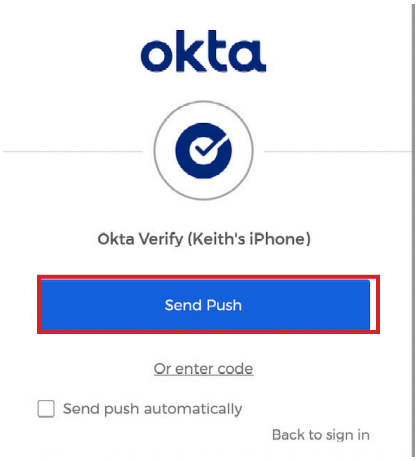
- A Mac computer managed in Jamf Pro running macOS 11 or later.
- An iOS 15 or iPadOS 15 device with a passcode and Face ID or Touch ID enabled.
- The Jamf Unlock app,Version 1.4.0 or later, and installed on your iOS device via Managed App Distribution from Jamf Pro.
- Jamf Connect version 2.14.0 or later.
- Admin access to your Mac Computer.
- Admin access to your Okta web portal.
- Admin access to your Jamf Pro server.

NOTE: This section assumes the Jamf Unlock app is already assigned to your Jamf Pro server from Apple Business / School Manager. This guide does not cover assigning apps from Apple Business / School Manager to Jamf Pro.

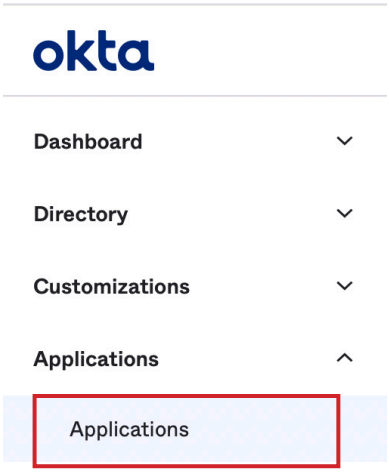
1. Using a web browser of your choosing, sign in to Okta using your admin credentials.



2. If prompted for MFA, select Send Push.

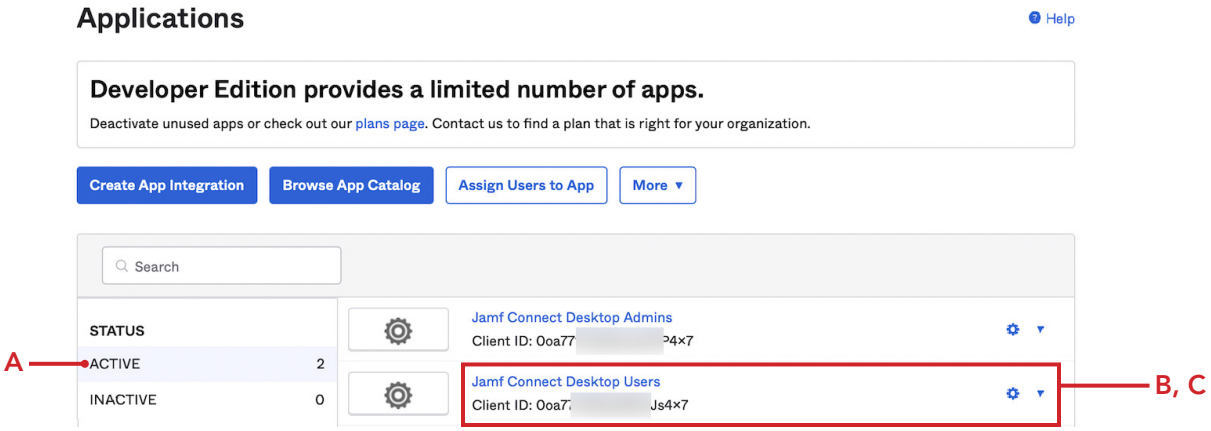


3. Expand Applications and click Applications.

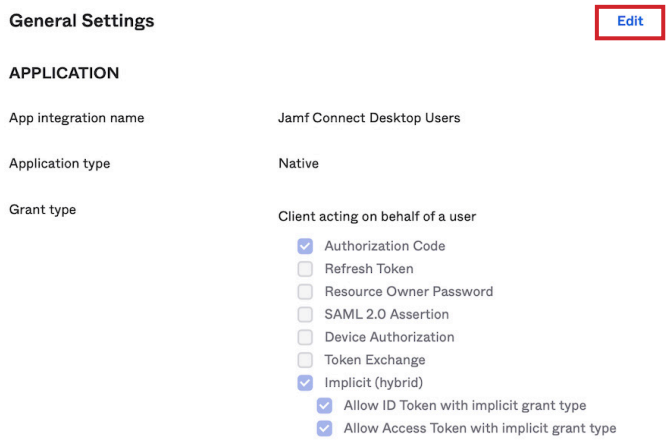


4. Follow these steps:
   A. Select ACTIVE
   B. Copy the Client ID for the Jamf Connect Desktop Users. Paste this into a text document and save it on your Desktop. We will need it later on in this section.
   C. Click on Jamf Connect Desktop Users. We need to modify this App Integration to include the Jamf Unlock URI.

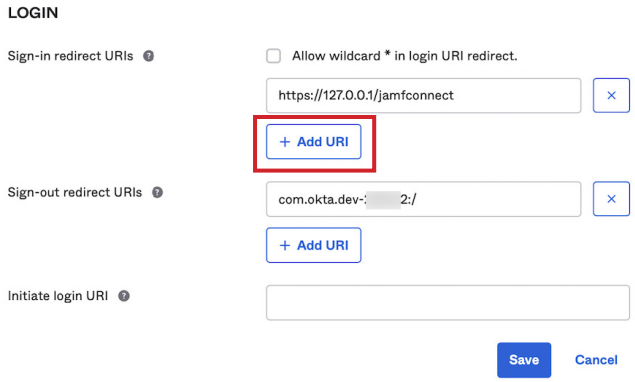
NOTE: If you did not follow this guide from the beginning, you will not have the Jamf Connect Desktop Users App Integration. Please refer to section 2 of this guide for more info on configuring an App Integration before you continue with this section.



5. In General Settings, select Edit.

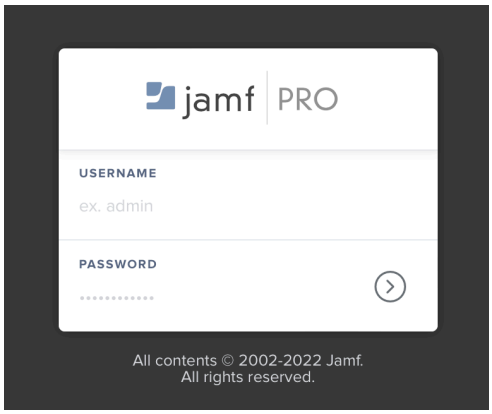


6. Go to LOGIN.
7. For Sign-in redirect URI, click Add URI.

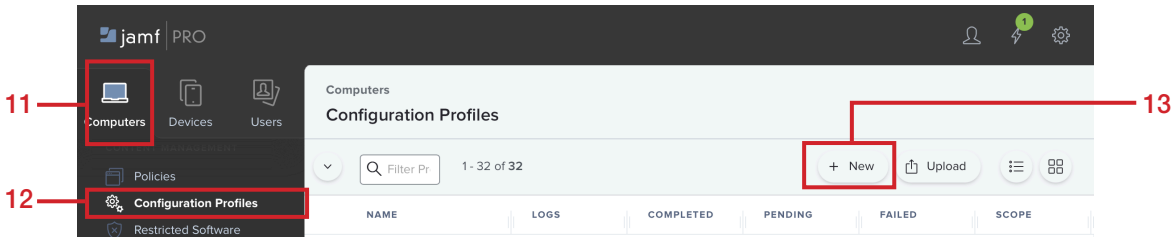


8. Enter the following URI: jamfunlock://callback/auth
   NOTE: The URI is case sensitive.
9. Click Save.

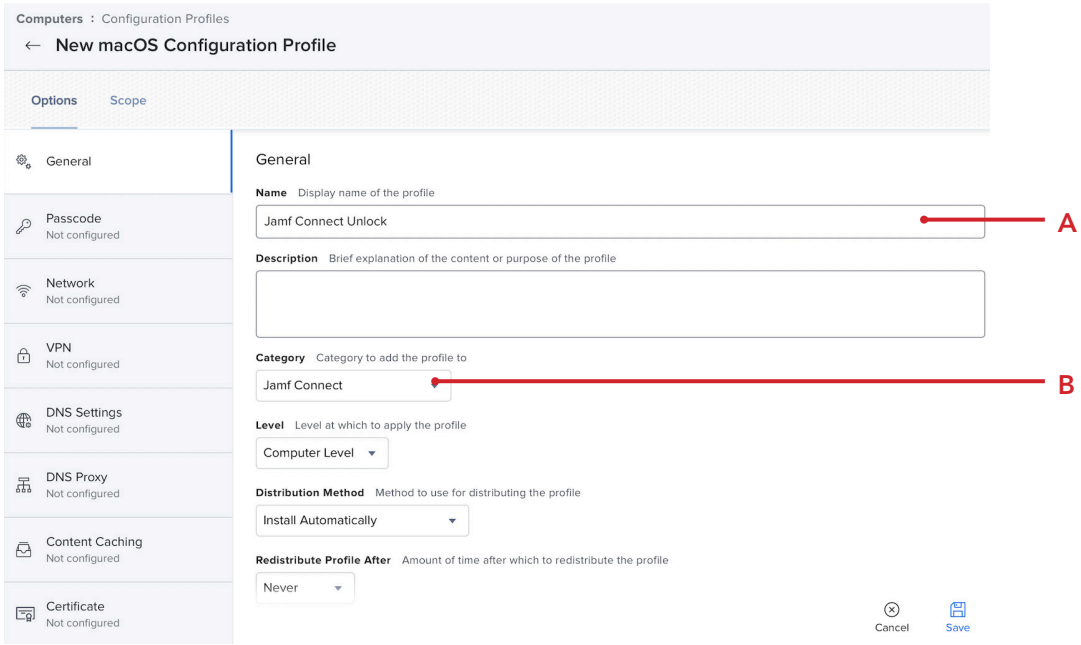
10. Log into your Jamf Pro server with admin credentials.



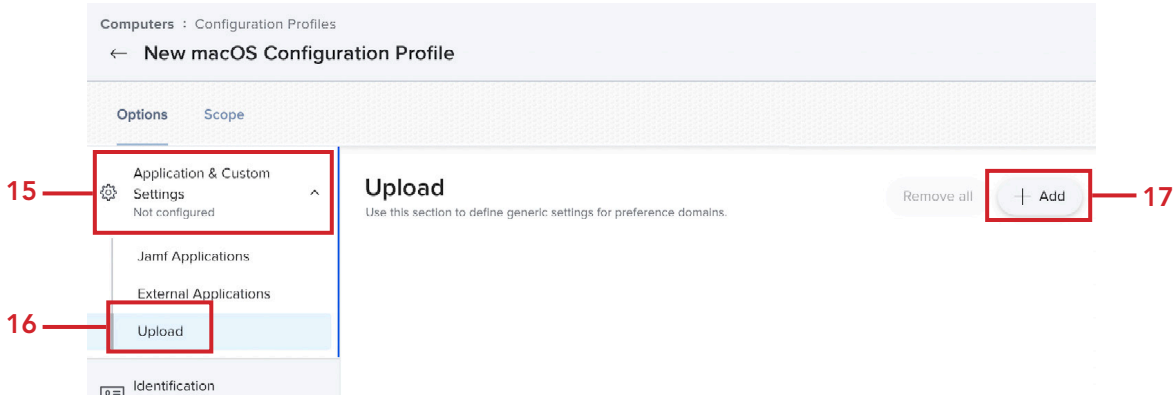
11. Click Computers.
12. Click Configuration Profiles.
13. Click New.



14. Select the General Payload and enter the following:
    A. Name: Jamf Connect Unlock
    B. Category: Jamf Connect (or a category that fits your needs)



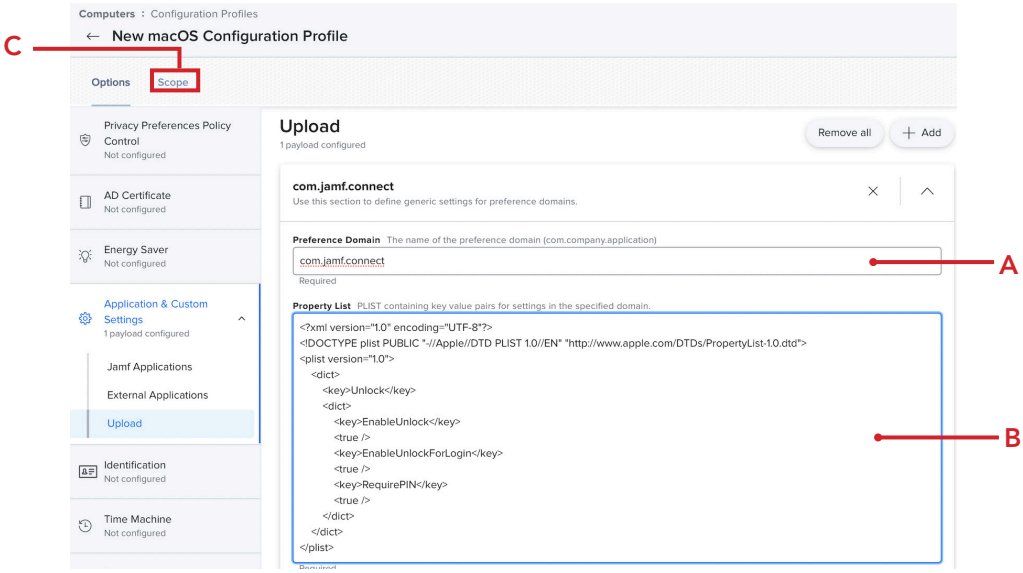
15. Click the Application & custom Settings Payload.
16. Click Upload.
17. Click Add.



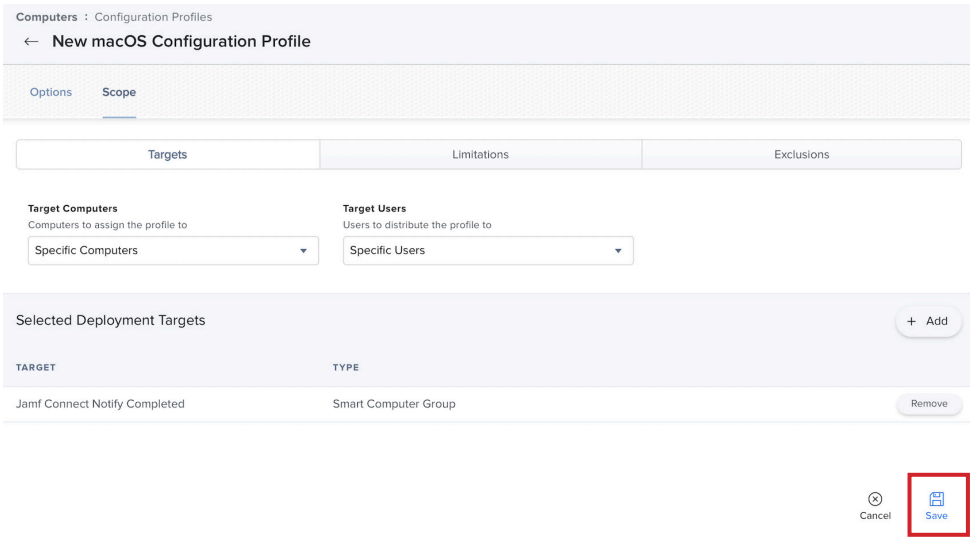
18. Enter the following:
    A. Preference Domain: com.jamf.connect
    B. Property List: Paste in the XML below
    C. Select Scope

    The XML below will enable Unlock in the Jamf connect menu bar, Enable log in for Mac Computers, and enable Require a PIN.

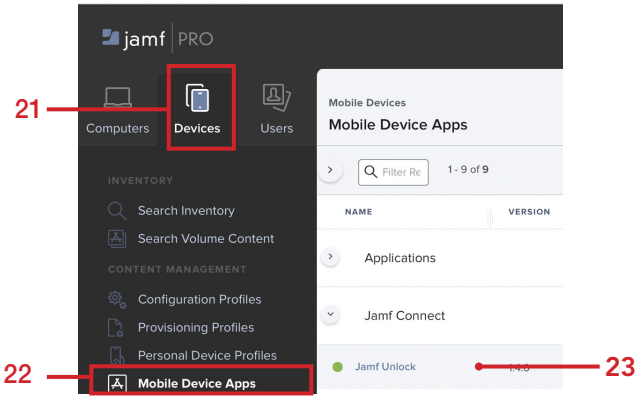
```
<?xml version="1.0" encoding="UTF-8"?>
<!DOCTYPE plist PUBLIC "-//Apple//DTD PLIST 1.0//EN" "http://www.apple.com/DTDs/
PropertyList-1.0.dtd">
<plist version="1.0">
  <dict>
    <key>Unlock</key>
    <dict>
      <key>EnableUnlock</key>
      <true />
      <key>EnableUnlockForLogin</key>
      <true />
      <key>RequirePIN</key>
      <true />
    </dict>
  </dict>
</plist>
```



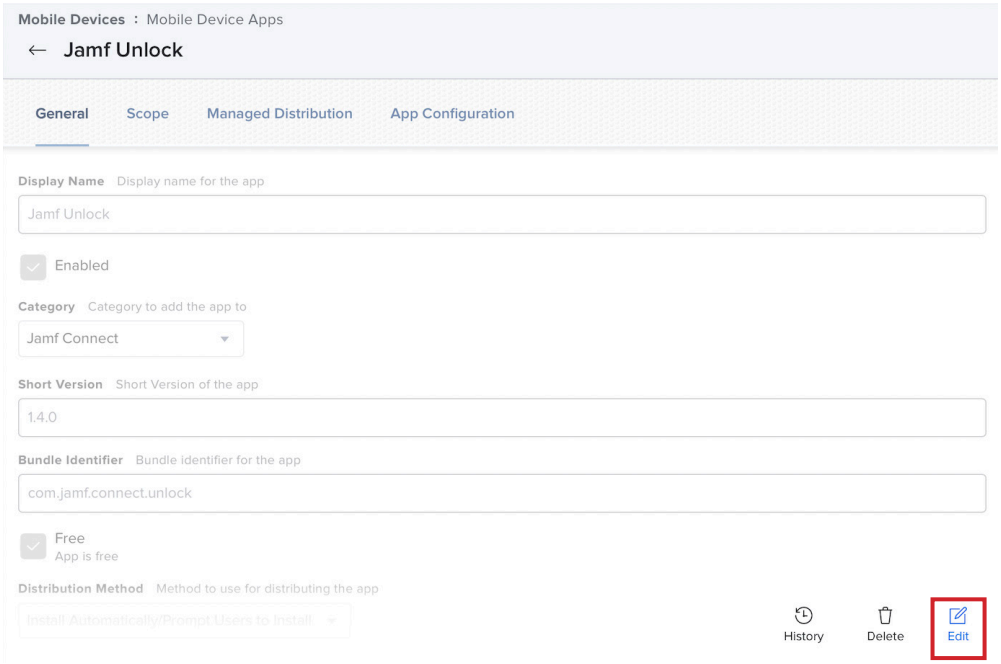
19. Scope to your needs. This guide will scope to a test Mac computer.
20. Click Save.



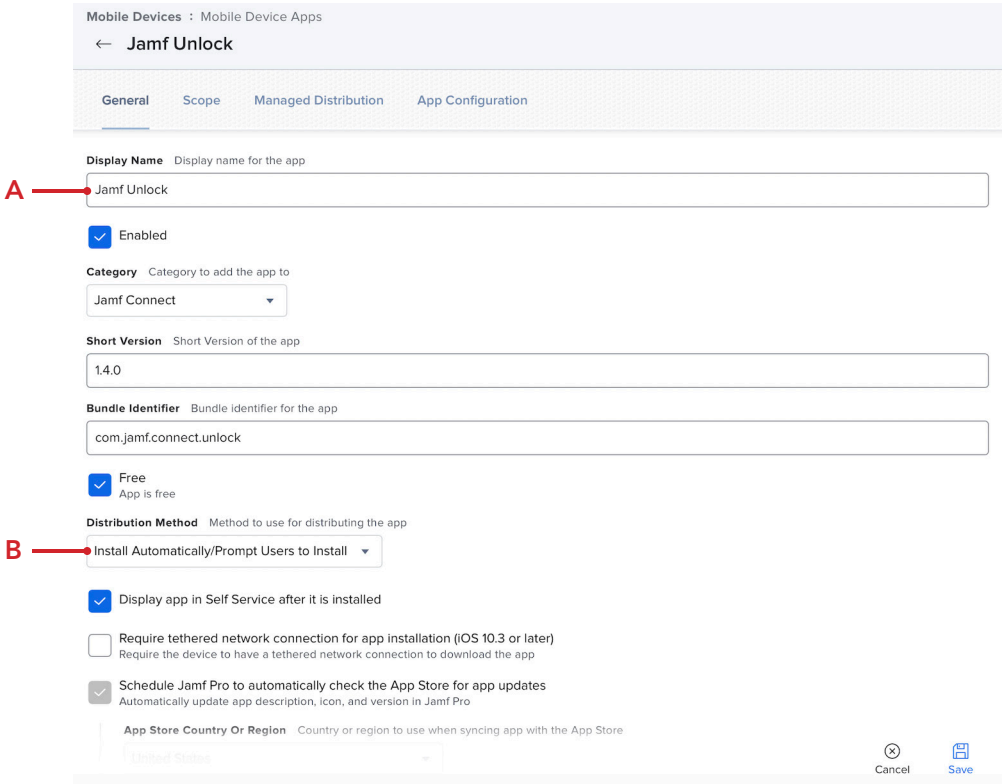
21. Click Devices.
22. Click Mobile Device Apps.
23. Select Jamf Unlock



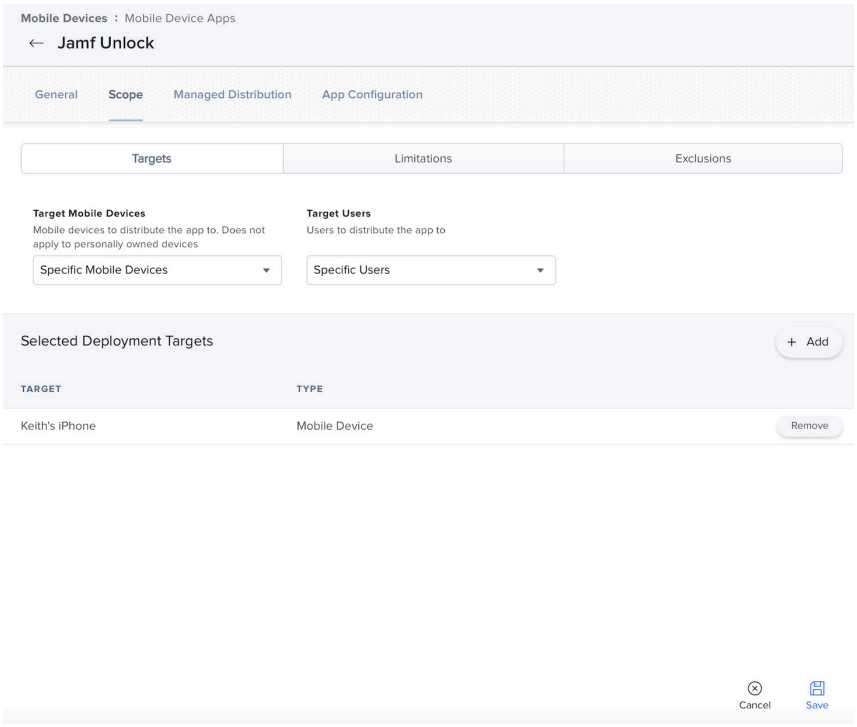
24. Click Edit.



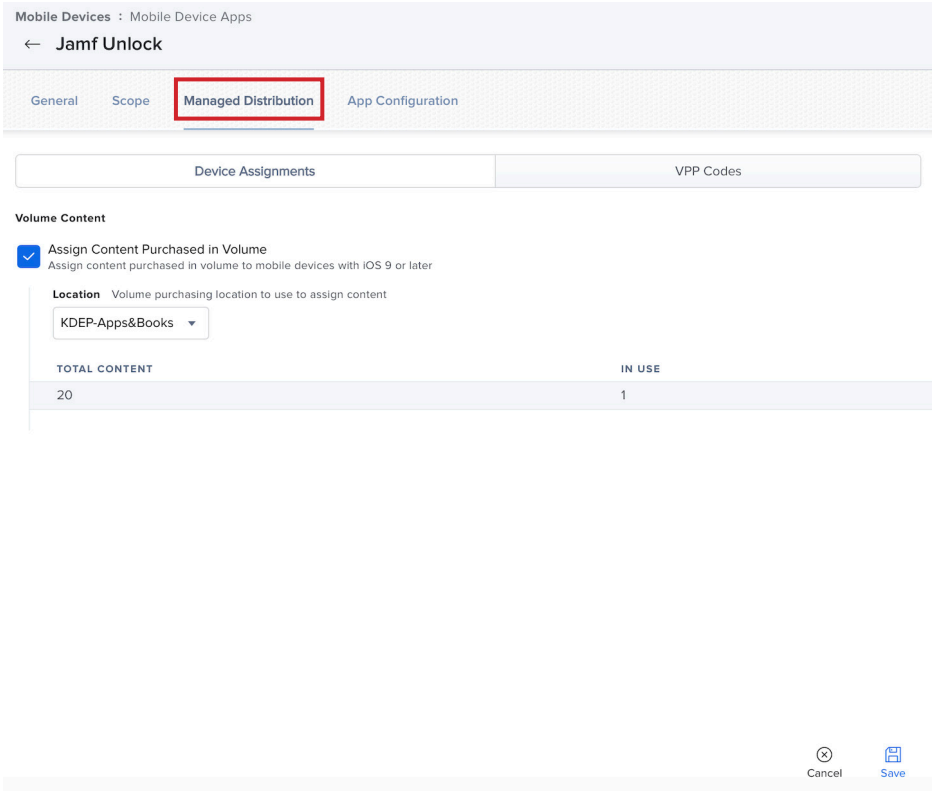
25. Configure the following:
    A. Select a category of your choosing. This guide will use Jamf Connect
    B. Set the distribution method to: Install Automatically/Prompt Users to Install
    C. Leave all other settings at their default values



26. Scope to your needs. This guide will scope to a test Mac computer.



27. Select Managed Distribution. Confirm Assign Content Purchased in Volume is enabled.



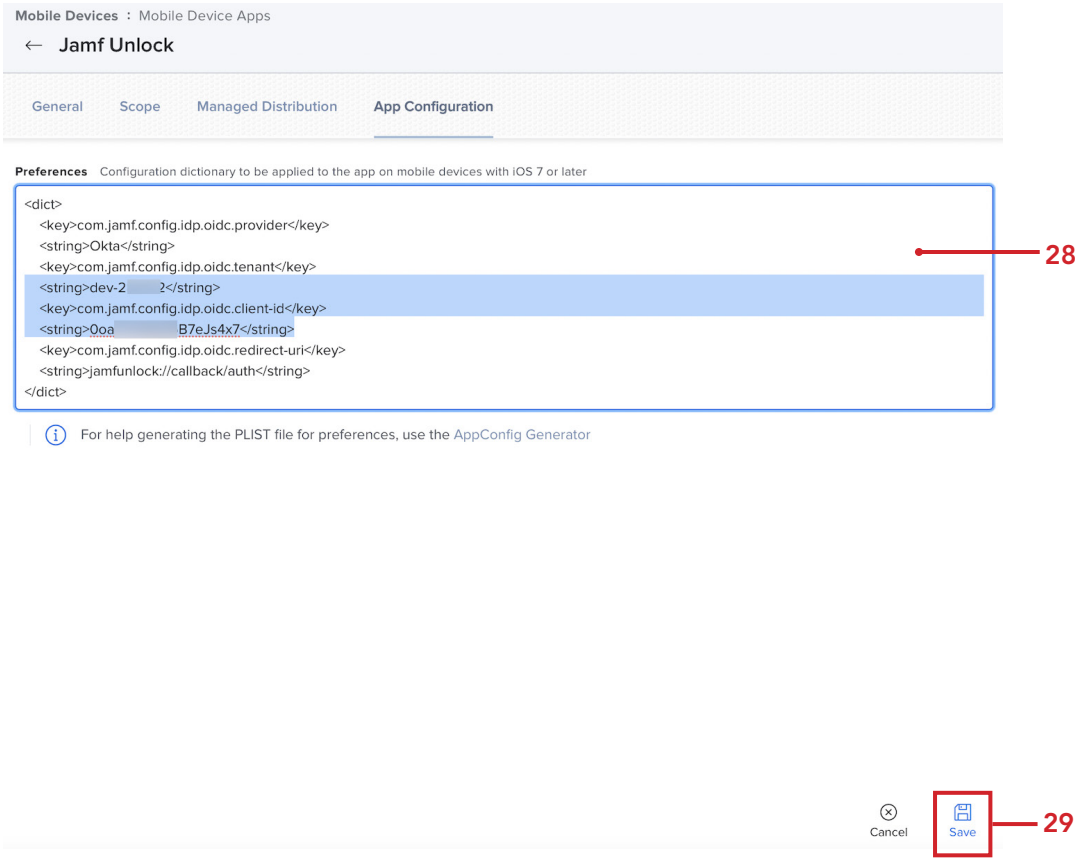
28. Select App Configuration. Using the XML below, replace the two strings that are in blue with the following:

    The first string is your Okta tenant-name. This should be entered with only the first part of your Okta URL. For example, If you Okta URL is https://mycompany.okta.com, all you need to enter is: mycompany - no other part of the URL is required.

    The second string is your App Integration client ID for the Jamf Connect Users App we created in step 4. You should have this saved to a text document on your desktop.

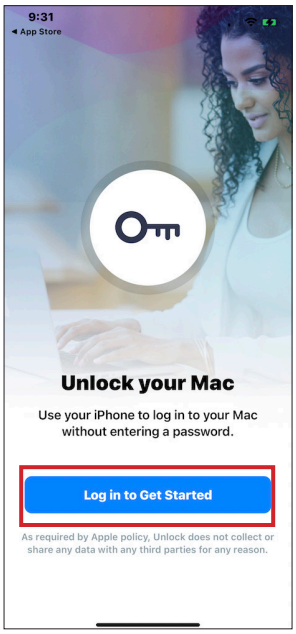
```
<dict>
  <key>com.jamf.config.idp.oidc.provider</key>
  <string>Okta</string>
  <key>com.jamf.config.idp.oidc.tenant</key>
  <string>YourTenantNameGoesHere</string>
  <key>com.jamf.config.idp.oidc.client-id</key>
  <string>YourAppIntergrationIDGoesHere</string>
  <key>com.jamf.config.idp.oidc.redirect-uri</key>
  <string>jamfunlock://callback/auth</string>
</dict>
```

29. Click Save.

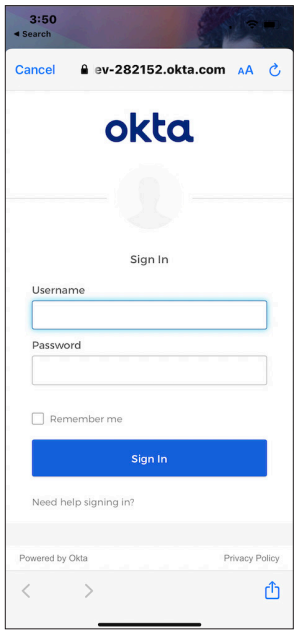


Let's switch to an iOS device. This guide will use an iPhone and we are assuming you already scoped the Jamf Unlock app to your iOS device.

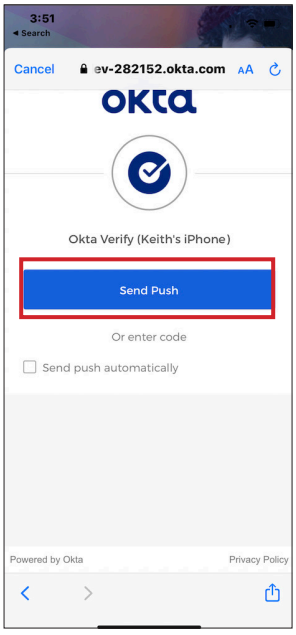
30. On your iPhone, open the Jamf Unlock app. Tap Log in to Get Started.



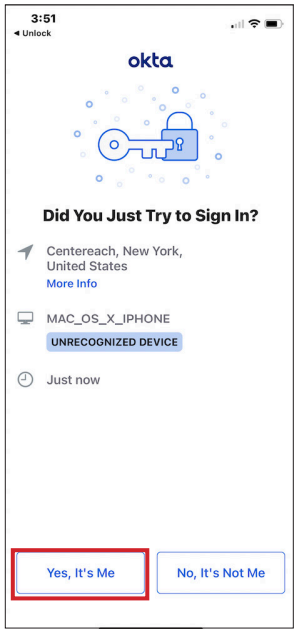
31. Enter your Okta credentials, tap Sign In.



32. Click Send Push.*

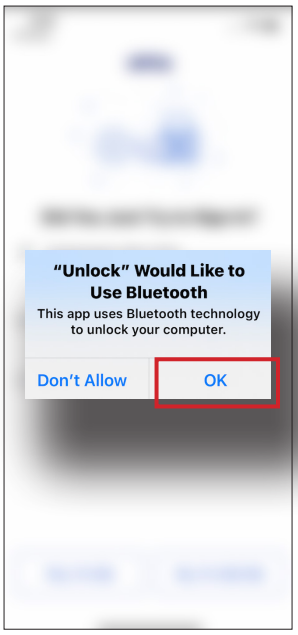


33. Tap Yes, Its Me.

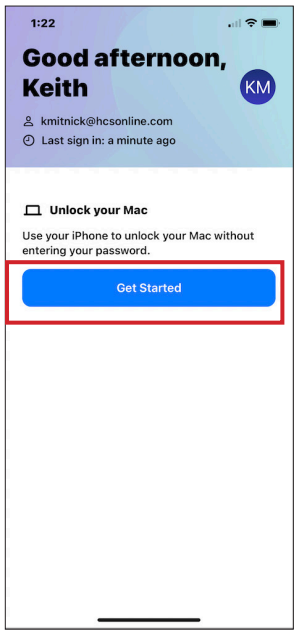


*Depending on how your MFA is configured, you may be challenged a second time with a screen that asks you to match numbers on another device. If you get prompted with that message, that means "Number Challenge for Okta Verify push" is enabled in Okta's Security section under the Multifactor tab. Reach out to your Okta admin or security team for more options. You may not be able to go forward with this section without having an additional device enrolled in Okta to handle the number matching message.

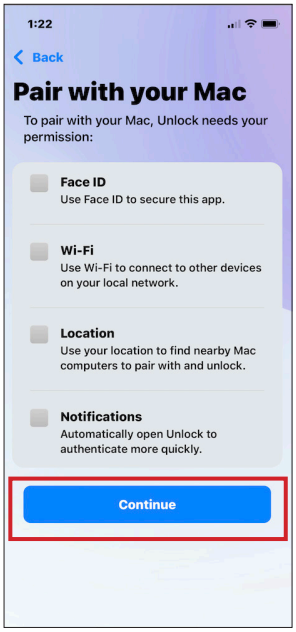
34. Tap OK at the Bluetooth message.



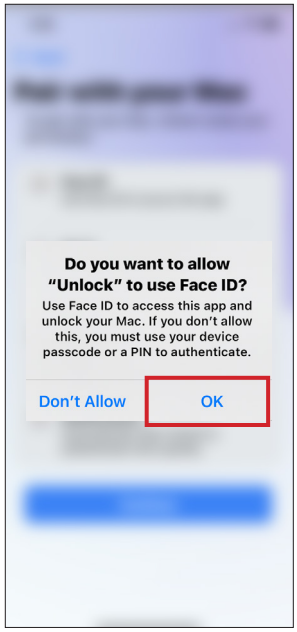
35. Tap Get Started..



36. Tap Continue

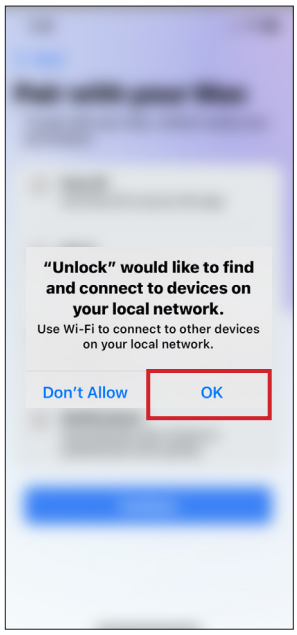


37. Tap OK.

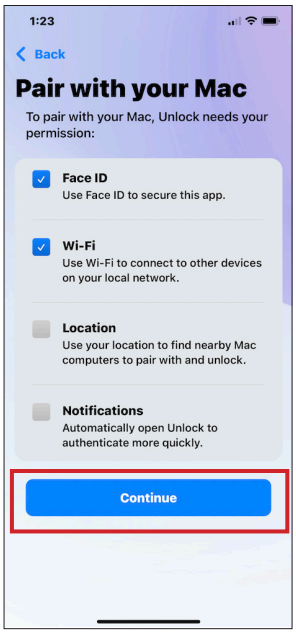


38. Tap Continue

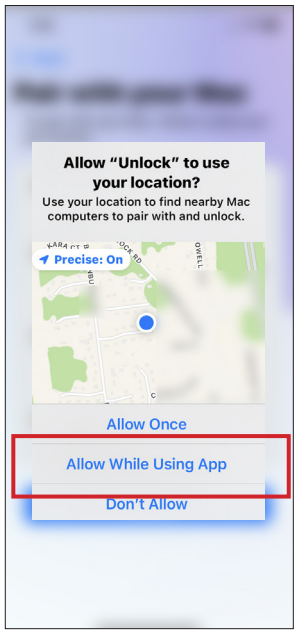
39. Tap OK.



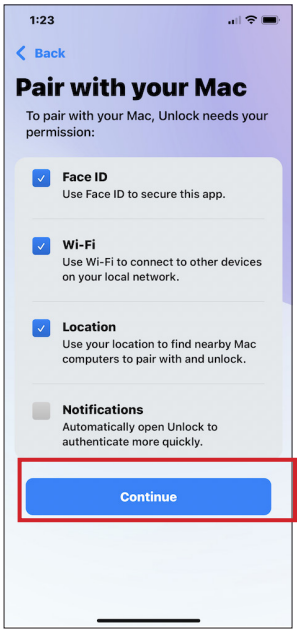
40. Tap Continue



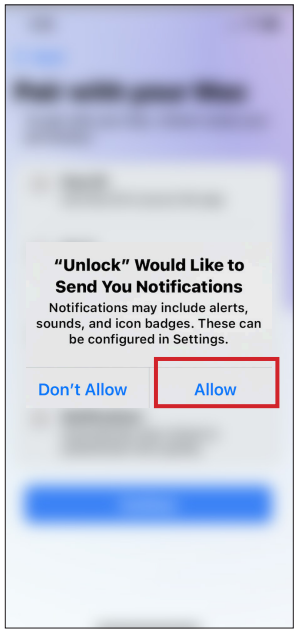
41. Make a selection that works for you. This guide will use Allow While Using App.



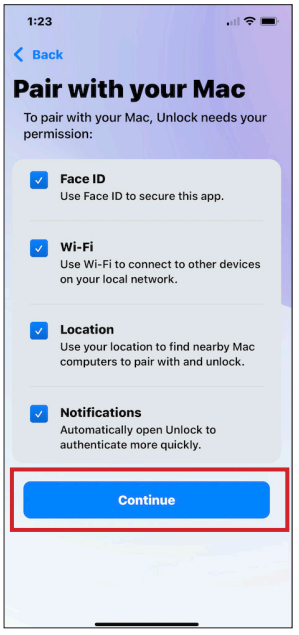
42. Tap Continue



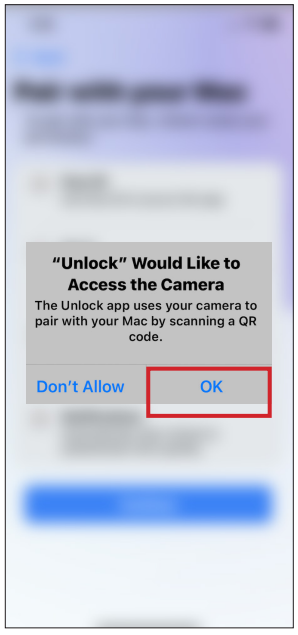
43. Tap OK.



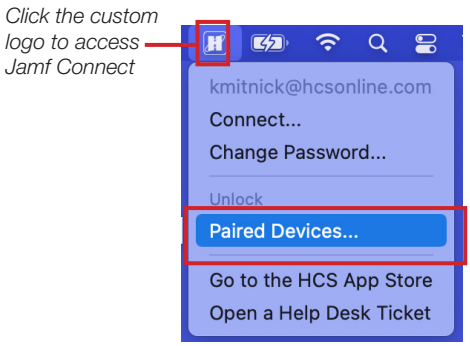
44. Tap Continue



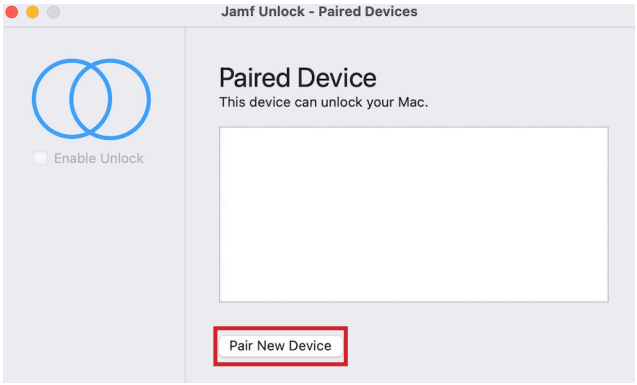
45. Tap OK.



46. Switch to your Mac computer. Select Jamf Connect from the Menu then select Paired Devices.

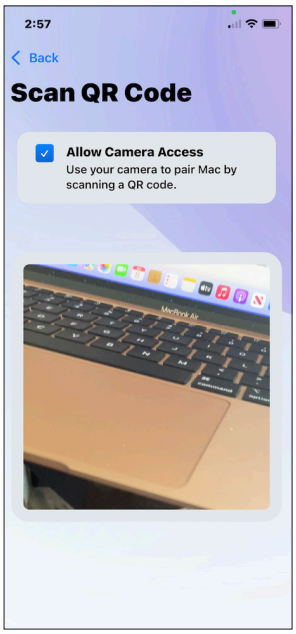


47. Click Pair New Device.



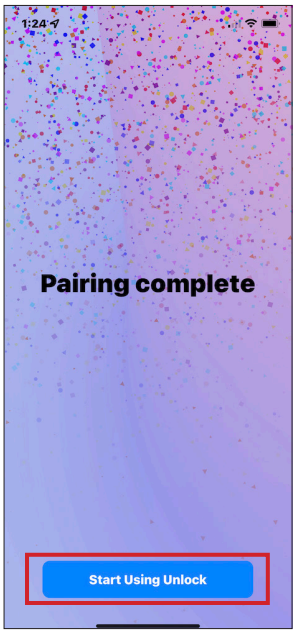
48. Confirm a QR code appears.

49. On your iPhone, line up the camera with your Mac computer to scan the QR code.



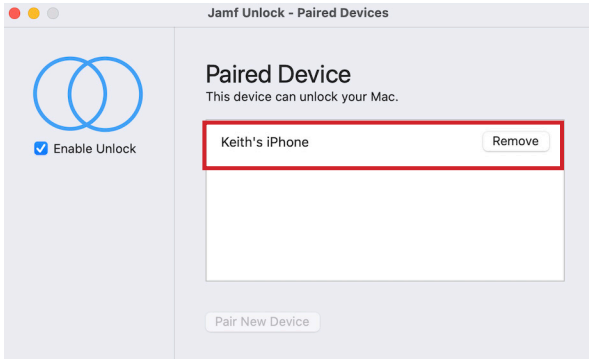
50. On your Mac computer, Click OK at the Bluetooth message.

51. On your iPhone, you will get a Pairing complete message. Tap Start Using Unlock.



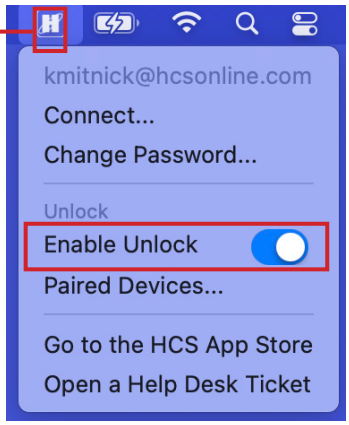
52. You can quit the Jamf Unlock app on your iPhone.

53. On your Mac, confirm the iPhone is paired.



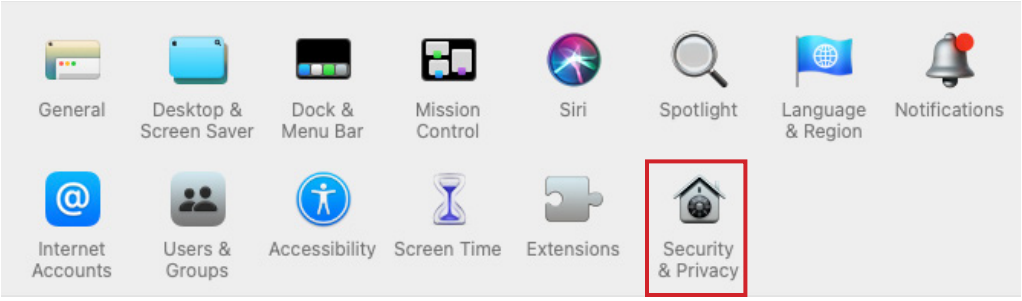
54. Select Jamf Connect from the Menu Bar, confirm Enable Unlock is now active.

Click the custom logo to access Jamf Connect

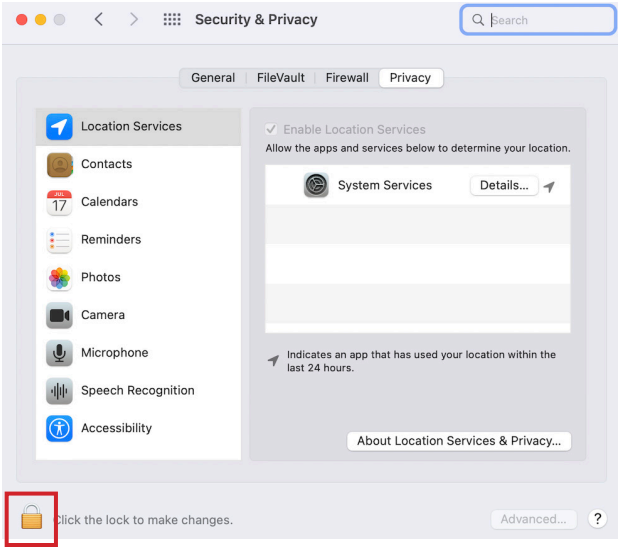


55. Let's test out Jamf Unlock on your Mac computer. Open System Preferences.

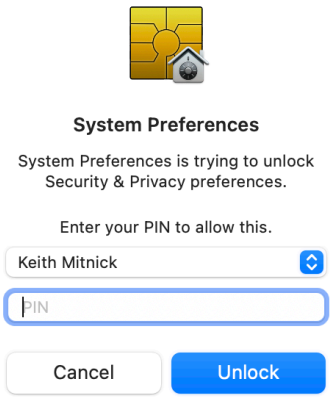
56. Click Security & Privacy.



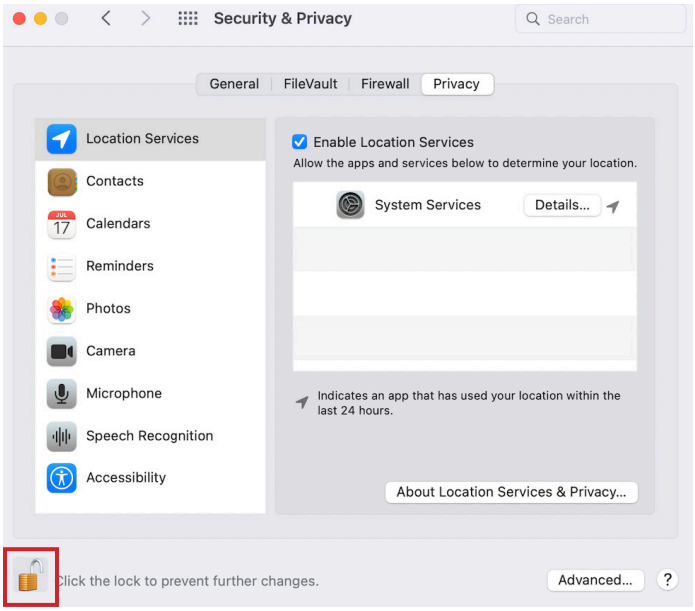
57. On the bottom-left, click the Lock to unlock the pane.



58. Confirm the password field say PIN.
59. Select the PIN field then press Enter on your keyboard.



60. You will get a Jamf Unlock alert on your phone and will be authenticated using Face ID. Confirm the pane has been unlocked. Quit System Preferences.



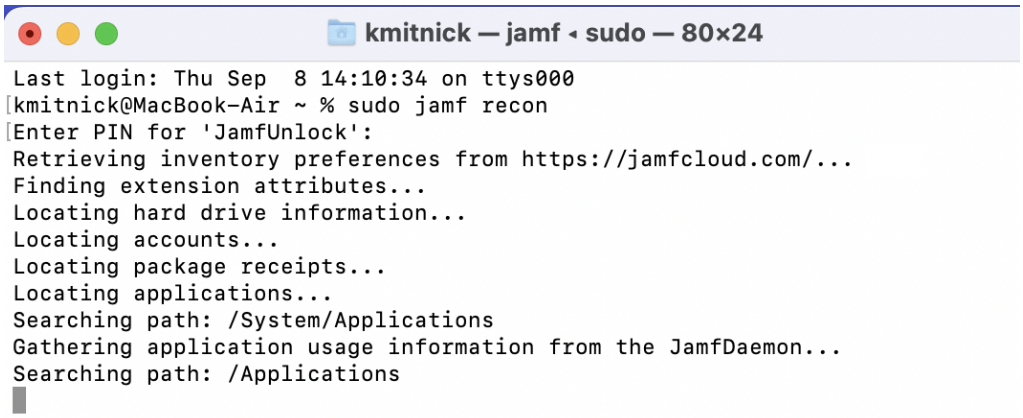
61. Open Terminal from /Applications/Utilities.

62. Enter the command:

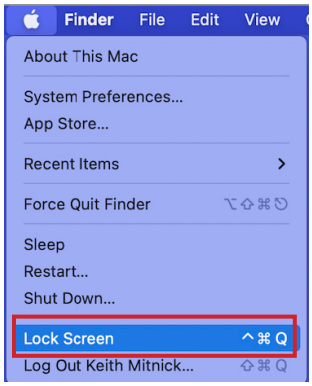
```
sudo jamf recon
```

When prompted to Enter PIN for JamfUnlock, press the Enter key on your keyboard.

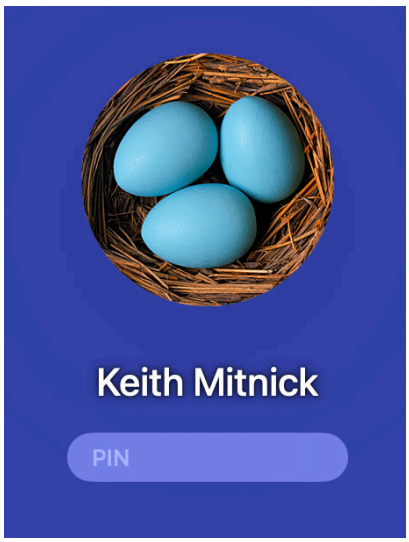
63. You will get a Jamf Unlock alert on your phone and will be authenticated using Face ID. Once done, the command starts to run.



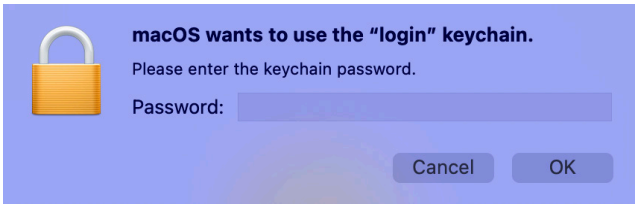
64. Click on the Apple Logo and select Lock Screen.



65. Confirm the password field say PIN.
66. Select the PIN field then press Enter on your keyboard.



67. If all went well, your Mac computer is now unlocked. If not, you may be presented with the screen below. This is currently a known issue. This message can happen one time, many times, or not at all. Just be aware you did not do anything wrong if you see this message.



This completes the guide.