jamf | CONNECT

How to Configure Jamf Connect with Google Cloud Identity

HCS TECHNOLOGY GROUP

Contents

Preface

The purpose of this guide is to provide a workflow for Mac administrators to deploy Jamf Connect using Google Cloud Identity as the Identity Provider (IdP). This guide will cover a myriad of topics such as installing, customizing, and deploying Jamf Connect with Google Cloud Identity.

Items required to follow along with this guide:

- Administrative access to your Google Cloud Admin Console. https://console.cloud.google.com
- Administrative access to your Google Workspace Admin Console. https://admin.google.com
- Jamf Connect - Download a trial here: http://jamf.it/JCDownload
- Administrative access to your Jamf Pro server.
- Administrative access to your Apple Business Manager/Apple School Manager portal.
- JC_Google_Files - These are sample files that we use in the guide.
  Download them here: https://hcsonline.com/images/Apps/JC_Google_Files.zip

There are six Google Workspace plans that are supported by Jamf Connect:

- Business Plus
- Enterprise
- Education Fundamentals
- Education Standard
- Teaching and Learning Upgrade
- Education Plus

You must have one of the above plans to following along with this guide. The above plans include LDAP client support which is required for password management.

NOTE:

- Google Workspace offers a free trial and it requires a credit card to sign up.
  https://cloud.google.com/free
- Jamf Connect 2.7 or later is required for password management with Google Workspace

Items not supported by Google Cloud Identity and Jamf Connect:

- Google Cloud identity supports OpenID Connect (OIDC)*. It does not support Resource Owner Password Grant (ROPG)** for password changes.
  Password changes are supported using a Google LDAP client certificate installed on Mac computers.
- Jamf connect cannot manage administrative and standard user roles with Google Cloud Identity.
- Jamf unlock is not supported by Google cloud identity.

This guide was written and tested using the following:

- Jamf Connect 2.17.0
- Jamf Connect Configuration app 2.17.0
- Jamf Pro Cloud Hosted Server 10.42.1
- Composer 10.42.1
- macOS Ventura 13.0.1 on a Mac computer with Apple silicon

Assumptions:

- Your Jamf Pro is linked to Apple Business Manager/Apple School Manager for Automated Device Enrollment and Volume Purchasing.
- 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:

- Erin McDonald
- Sean Rabbitt
- William Smith
- The HCS Team

*OpenID Connect (OIDC) is an open authentication protocol that works on top of the OAuth 2.0 framework.

**Resource Owner Password Grant (ROPG)—Authenticates the user's cloud username and password directly to your IdP's token endpoint. This authentication method is only used for password synchronization.

Section 1: Configure Google Cloud Identity

What You'll Need

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

Hardware and Software

Requirements for following along with this section:

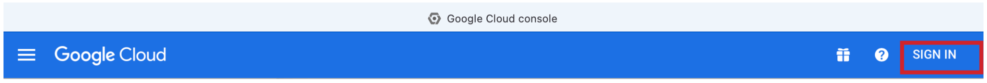
- A Mac with macOS 10.15.4 or later. This guide will use macOS 13.0.1
- Jamf Connect installer DMG. This guide will use version 2.17.0
- Administrative access to your Google Cloud Admin Console: https://console.cloud.google.com
- Administrative access to your Google Workspace Admin Console: https://admin.google.com

In this section we will configure configure Google Cloud Identity with the following items:

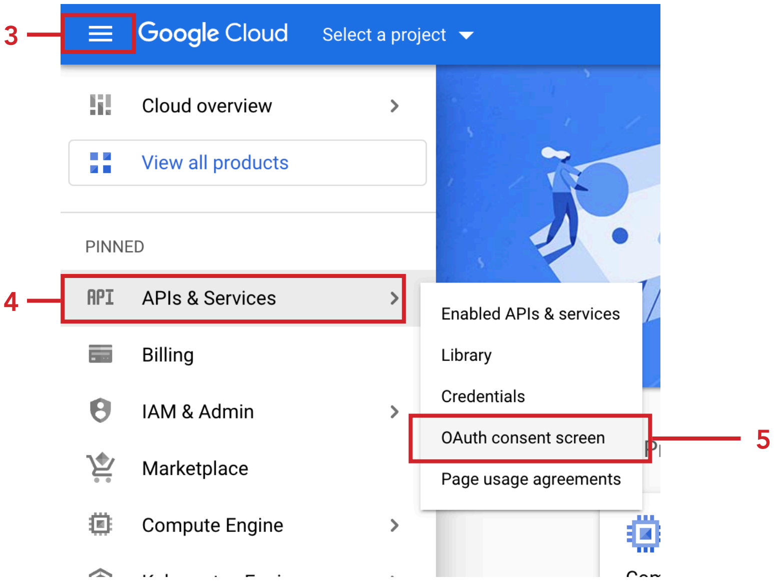
- A Project for Jamf Connect
- A LDAP Client
- A LDAP Keystore

Creating a Project for Jamf Connect:

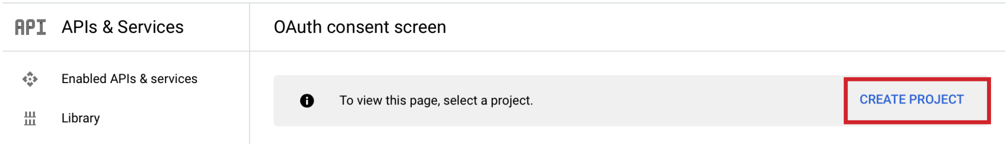
1. Using a web browser of your choosing, go to https://console.cloud.google.com
2. Sign in with your administrative credentials.



3. Click on the Navigation menu (≡).
4. Click APIs & Services
5. Click OAuth consent screen.



6. Click Create Project.



API APIs & Services

OAuth consent screen

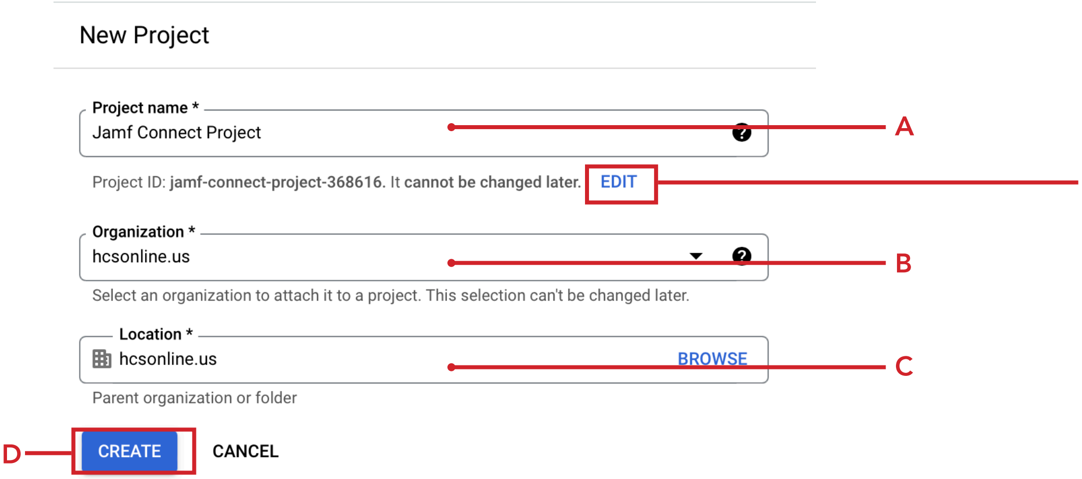
Enabled APIs & services

Library

To view this page, select a project.

CREATE PROJECT

7. Configure the following:
   A. Project Name: Jamf Connect Project
   B. Organization: Select your organization
   C. Location: Select your location
   D. Click Create



New Project

Project name *
Jamf Connect Project

Project ID: **jamf-connect-project-368616**. It **cannot be changed later.** EDIT

Organization *
hcsonline.us

Select an organization to attach it to a project. This selection can't be changed later.

Location *
hcsonline.us BROWSE

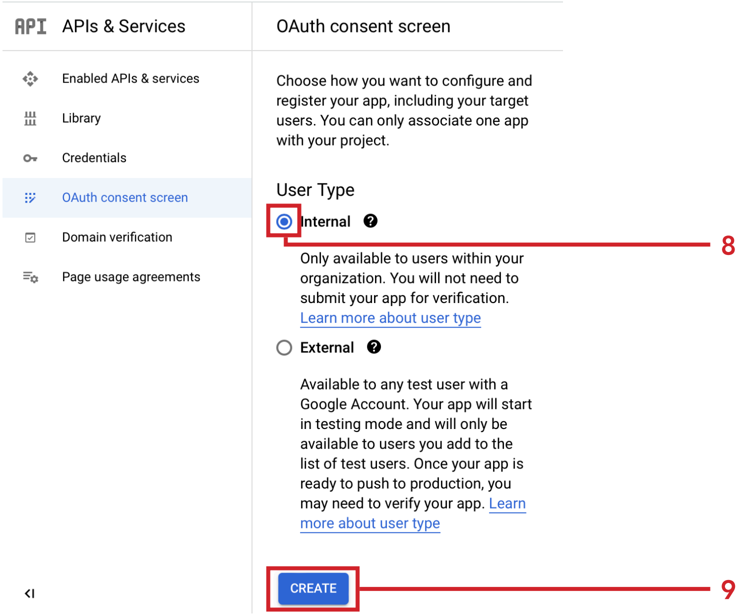
Parent organization or folder

CREATE CANCEL

*Optional:
Click Edit to
modify the
Project ID*

8. Select the radio button for Internal

9. Click Create.



API APIs & Services

OAuth consent screen

Enabled APIs & services

Library

Credentials

OAuth consent screen

Domain verification

Page usage agreements

Choose how you want to configure and register your app, including your target users. You can only associate one app with your project.

User Type

● Internal

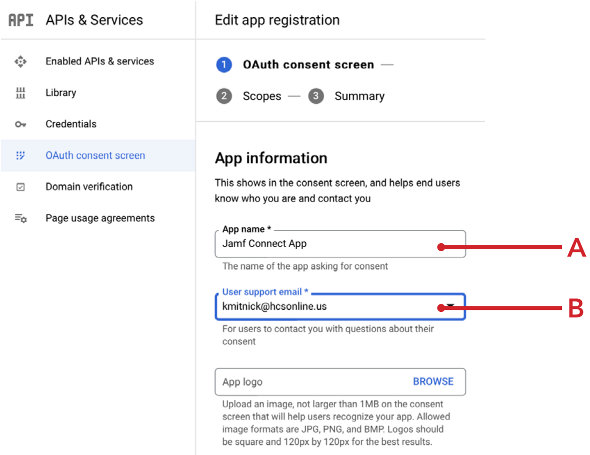
Only available to users within your organization. You will not need to submit your app for verification. Learn more about user type

○ External

Available to any test user with a Google Account. Your app will start in testing mode and will only be available to users you add to the list of test users. Once your app is ready to push to production, you may need to verify your app. Learn more about user type

CREATE

10. Configure the following:
    A. App Name: Jamf Connect App
    B. User support email: Select an email address from the dropdown menu
    C. Scroll down to the Developer contact information section



App information

This shows in the consent screen, and helps end users know who you are and contact you

App name *: Jamf Connect App

The name of the app asking for consent

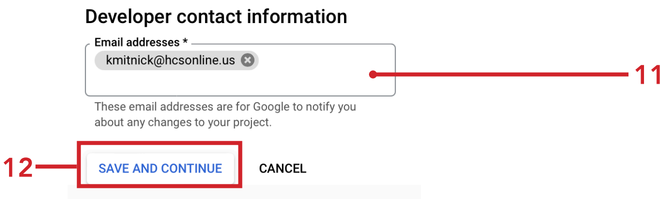
User support email *: kmitnick@hcsonline.us

For users to contact you with questions about their consent

App logo

Upload an image, not larger than 1MB on the consent screen that will help users recognize your app. Allowed image formats are JPG, PNG, and BMP. Logos should be square and 120px by 120px for the best results.

11. Add an email address.
12. Click Save and Continue.

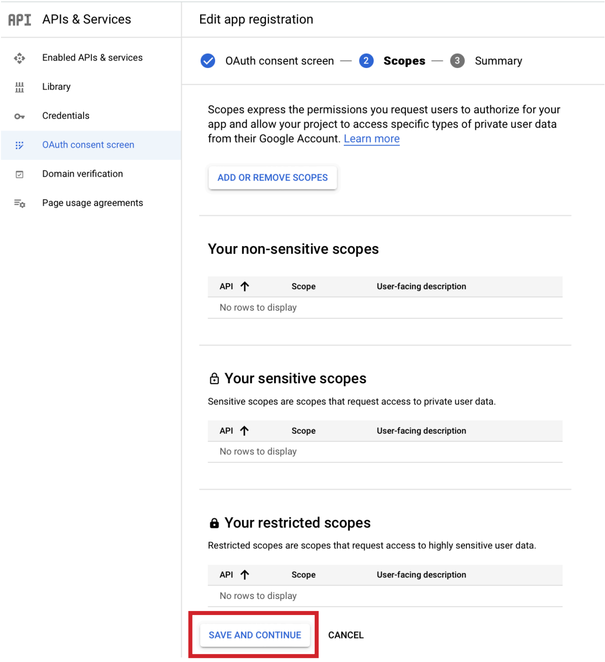


Developer contact information

Email addresses *: kmitnick@hcsonline.us

These email addresses are for Google to notify you about any changes to your project.

13. Click Save and Continue.



Scopes express the permissions you request users to authorize for your app and allow your project to access specific types of private user data from their Google Account. Learn more

Your non-sensitive scopes

API ↑	Scope	User-facing description
No rows to display		

Your sensitive scopes

Sensitive scopes are scopes that request access to private user data.

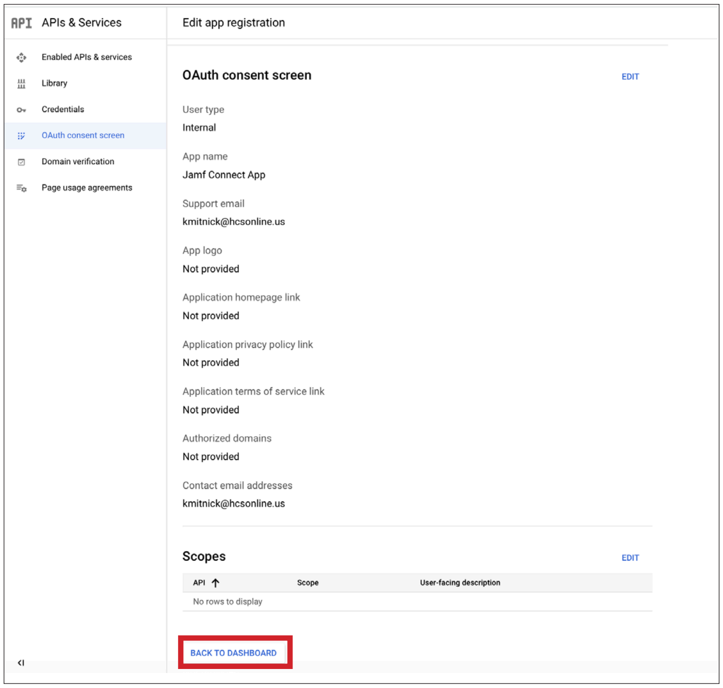
API ↑	Scope	User-facing description
No rows to display		

Your restricted scopes

Restricted scopes are scopes that request access to highly sensitive user data.

API ↑	Scope	User-facing description
No rows to display		

14. Click Back to Dashboard.



API APIs & Services

- Enabled APIs & services
- Library
- Credentials
- OAuth consent screen
- Domain verification
- Page usage agreements

Edit app registration

OAuth consent screen EDIT

User type
Internal

App name
Jamf Connect App

Support email
kmitnick@hcsonline.us

App logo
Not provided

Application homepage link
Not provided

Application privacy policy link
Not provided

Application terms of service link
Not provided

Authorized domains
Not provided

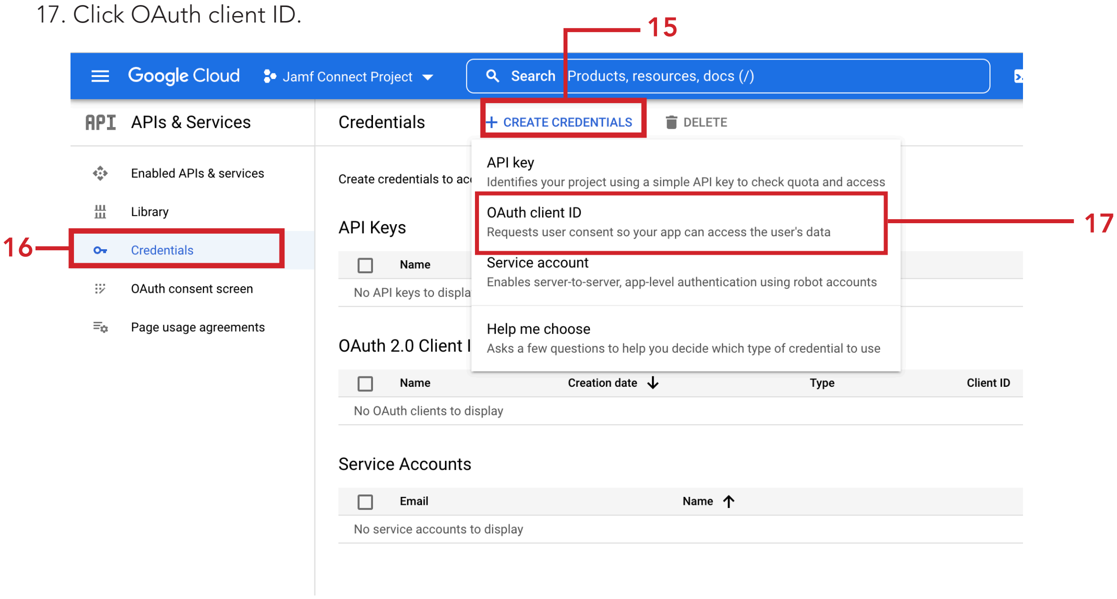
Contact email addresses
kmitnick@hcsonline.us

Scopes EDIT

API ↑	Scope	User-facing description
No rows to display		

BACK TO DASHBOARD

15. Click Credentials.
16. Click Create Credentials
17. Click OAuth client ID.



Google Cloud   Jamf Connect Project   Search Products, resources, docs (/)

API APIs & Services

- Enabled APIs & services
- Library
- Credentials
- OAuth consent screen
- Page usage agreements

Credentials   + CREATE CREDENTIALS   DELETE

Create credentials to ac

API key
Identifies your project using a simple API key to check quota and access

OAuth client ID
Requests user consent so your app can access the user's data

Service account
Enables server-to-server, app-level authentication using robot accounts

Help me choose
Asks a few questions to help you decide which type of credential to use

API Keys

□	Name
No API keys to displa	

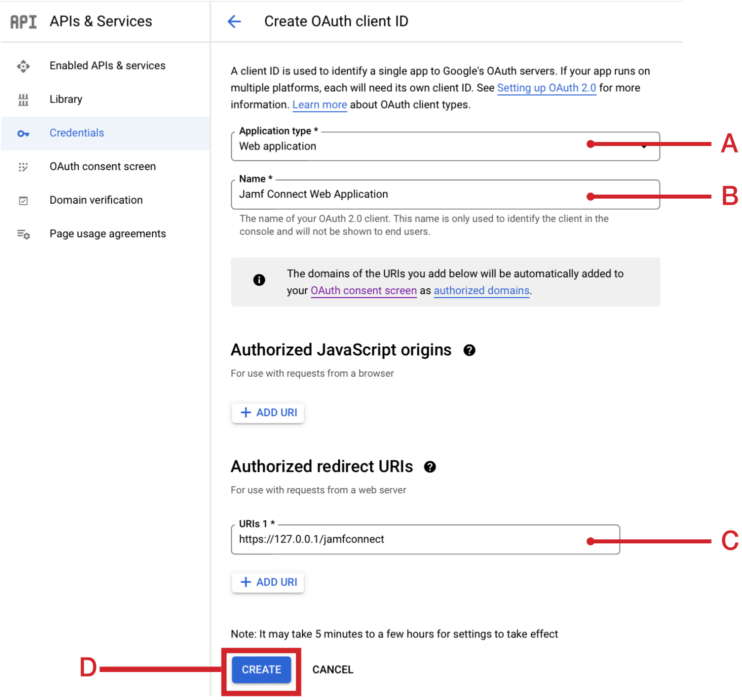
OAuth 2.0 Client I

□	Name	Creation date ↓	Type	Client ID
No OAuth clients to display				

Service Accounts

□	Email	Name ↑
No service accounts to display		

18. Configure the following:
    A. Select Web Application from Application type menu
    B. Enter Jamf Connect Web Application
    C. Authorized redirect URIs: Click the Add URI button then enter: https://127.0.0.1/jamfconnect
    D. Click Create.



Create OAuth client ID

A client ID is used to identify a single app to Google's OAuth servers. If your app runs on multiple platforms, each will need its own client ID. See Setting up OAuth 2.0 for more information. Learn more about OAuth client types.

Application type *
Web application

Name *
Jamf Connect Web Application

The name of your OAuth 2.0 client. This name is only used to identify the client in the console and will not be shown to end users.

The domains of the URIs you add below will be automatically added to your OAuth consent screen as authorized domains.

Authorized JavaScript origins

For use with requests from a browser

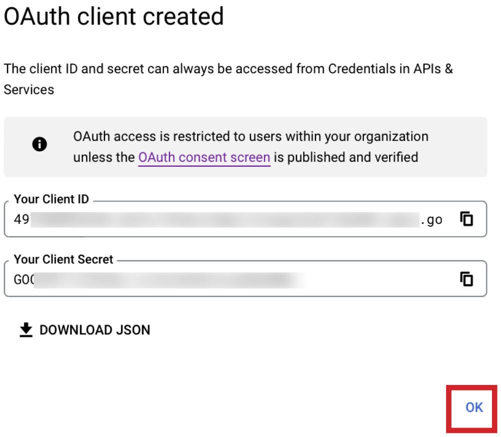
Authorized redirect URIs

For use with requests from a web server

URIs 1 *
https://127.0.0.1/jamfconnect

Note: It may take 5 minutes to a few hours for settings to take effect

19. At the OAuth client created window, copy the Your Client ID and Your Client Secret to a plain text document. We will need this information later in the guide. You can also download the JSON file for safe keeping. Click OK when done.



OAuth client created

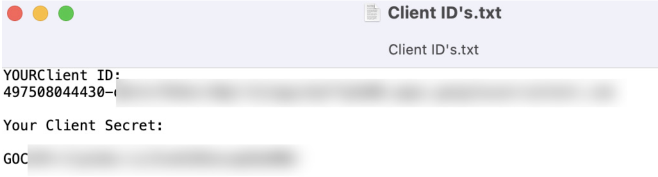
The client ID and secret can always be accessed from Credentials in APIs & Services

OAuth access is restricted to users within your organization unless the OAuth consent screen is published and verified

Your Client ID
49[redacted].go

Your Client Secret
GO([redacted]

20. Save the ID's to the Desktop. Provide a name of your choosing. This guide will use Client ID's.txt as the file name.

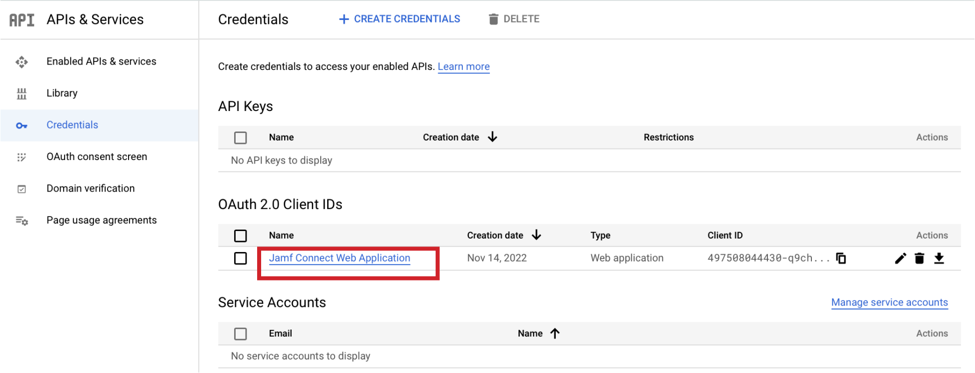


```
YOURClient ID:
497508044430-[redacted]

Your Client Secret:

GOC[redacted]
```

21. In the OAuth 2.0 Client IDs section, confirm the Jamf Connect Web Application was created. Sign out of https://console.cloud.google.com



Create credentials to access your enabled APIs. Learn more

API Keys

□	Name	Creation date ↓	Restrictions	Actions
No API keys to display				

OAuth 2.0 Client IDs

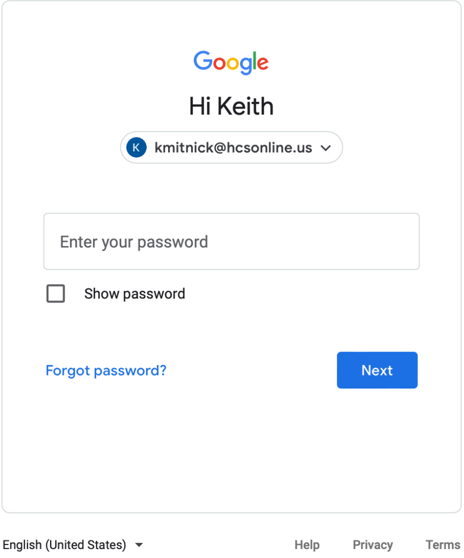
□	Name	Creation date ↓	Type	Client ID	Actions
□	Jamf Connect Web Application	Nov 14, 2022	Web application	497508044430-q9ch...	

Service Accounts — Manage service accounts

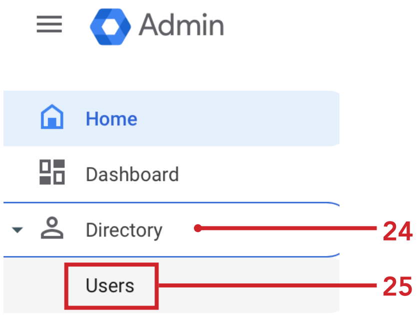
□	Email	Name ↑	Actions
No service accounts to display			

22. We are going to create a LDAP Client for Jamf Connect. In a web browser, go to: https://admin.google.com

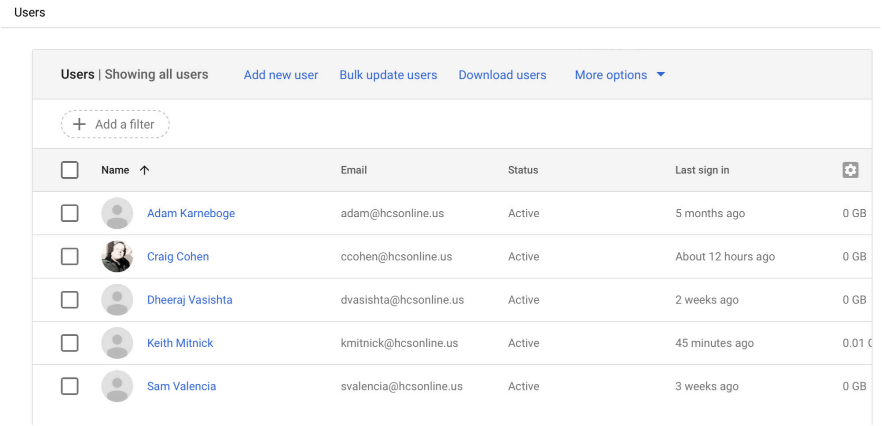
23. Sign in with your administrative credentials.



24. From the side bar, click Directory
25. Click Users.



26. Confirm the you have at least two users that you can use for testing with Jamf Connect.

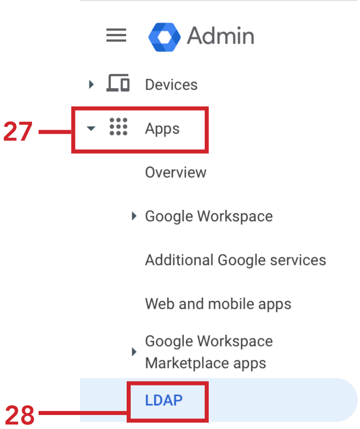

Users

Users | Showing all users   Add new user   Bulk update users   Download users   More options ▾

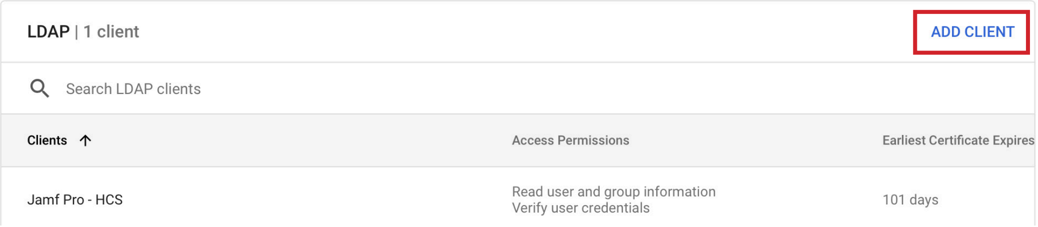
+ Add a filter

□	Name ↑	Email	Status	Last sign in	
□	Adam Karneboge	adam@hcsonline.us	Active	5 months ago	0 GB
□	Craig Cohen	ccohen@hcsonline.us	Active	About 12 hours ago	0 GB
□	Dheeraj Vasishta	dvasishta@hcsonline.us	Active	2 weeks ago	0 GB
□	Keith Mitnick	kmitnick@hcsonline.us	Active	45 minutes ago	0.01
□	Sam Valencia	svalencia@hcsonline.us	Active	3 weeks ago	0 GB

27. From the side bar, click Apps
28. Click LDAP.



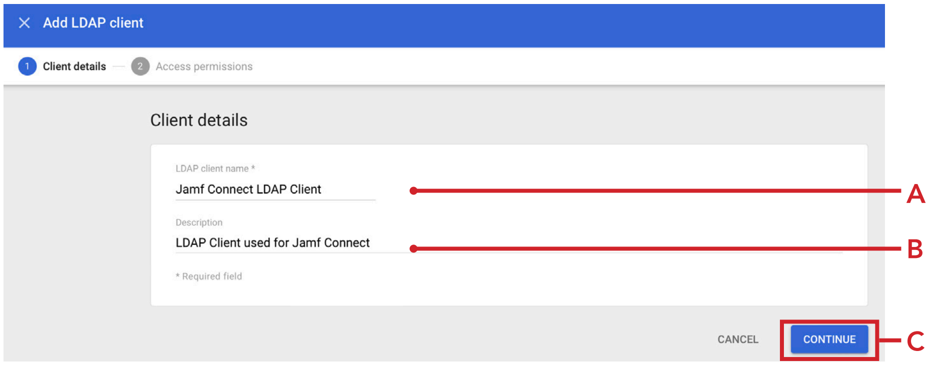
29. Click Add Client.



LDAP | 1 client

Clients ↑	Access Permissions	Earliest Certificate Expires
Jamf Pro - HCS	Read user and group information Verify user credentials	101 days

30. Enter the following:
    A. LDAP client name: Jamf Connect LDAP Client
    B. Description: LDAP client used for Jamf Connect
    C. Click Continue



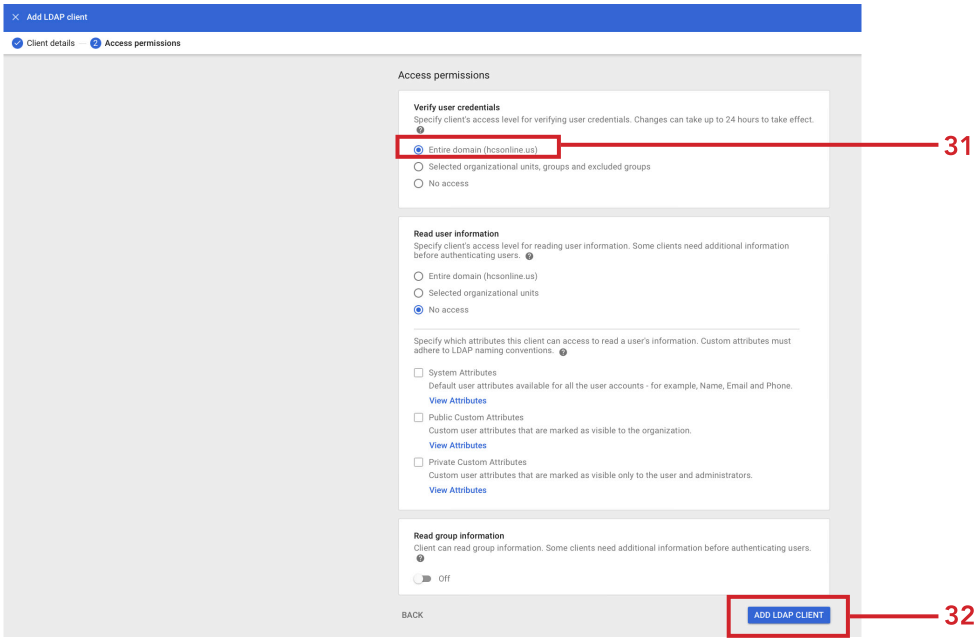
Client details

LDAP client name *: Jamf Connect LDAP Client

Description: LDAP Client used for Jamf Connect

* Required field

31. Select the radio button for Entire domain.
32. Click Add LDAP Client.
    NOTE: We are setting full permissions for the simplicity of this guide. Please select the permissions required by your organization.



Access permissions

Verify user credentials
Specify client's access level for verifying user credentials. Changes can take up to 24 hours to take effect.

● Entire domain (hcsonline.us)
○ Selected organizational units, groups and excluded groups
○ No access

Read user information
Specify client's access level for reading user information. Some clients need additional information before authenticating users.

○ Entire domain (hcsonline.us)
○ Selected organizational units
● No access

Specify which attributes this client can access to read a user's information. Custom attributes must adhere to LDAP naming conventions.

□ System Attributes
Default user attributes available for all the user accounts - for example, Name, Email and Phone.
View Attributes

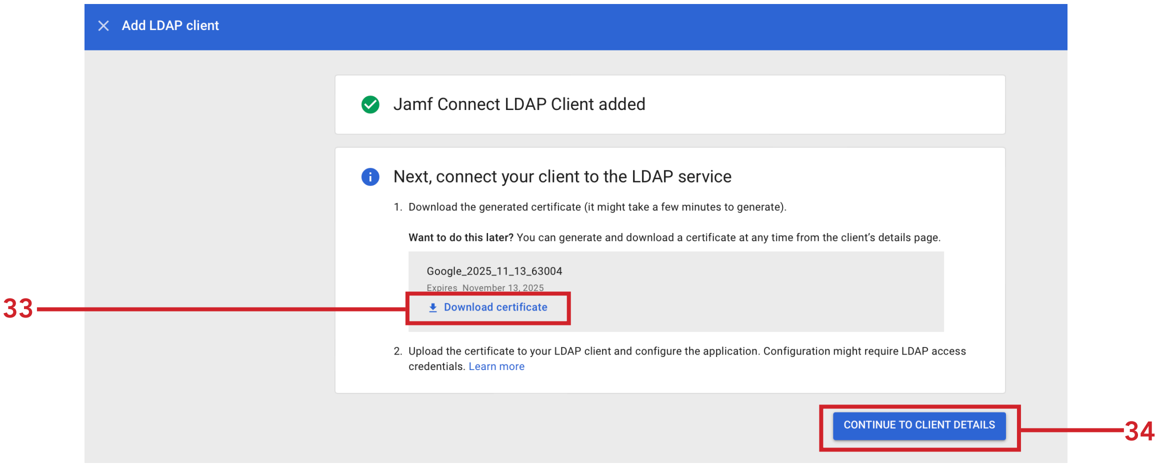
□ Public Custom Attributes
Custom user attributes that are marked as visible to the organization.
View Attributes

□ Private Custom Attributes
Custom user attributes that are marked as visible only to the user and administrators.
View Attributes

Read group information
Client can read group information. Some clients need additional information before authenticating users.

Off

33. Click Download certificate. The certificate will be used in the next section of this guide.
34. Click Continue to Client Details.



Add LDAP client

Jamf Connect LDAP Client added

Next, connect your client to the LDAP service

1. Download the generated certificate (it might take a few minutes to generate).

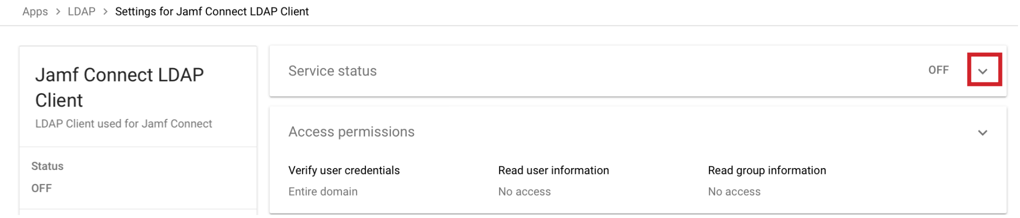
Want to do this later? You can generate and download a certificate at any time from the client's details page.

Google_2025_11_13_63004
Expires November 13, 2025
Download certificate

2. Upload the certificate to your LDAP client and configure the application. Configuration might require LDAP access credentials. Learn more

CONTINUE TO CLIENT DETAILS

35. Expand Service Status by clicking the arrow next to Off.



Apps > LDAP > Settings for Jamf Connect LDAP Client

Jamf Connect LDAP Client

LDAP Client used for Jamf Connect

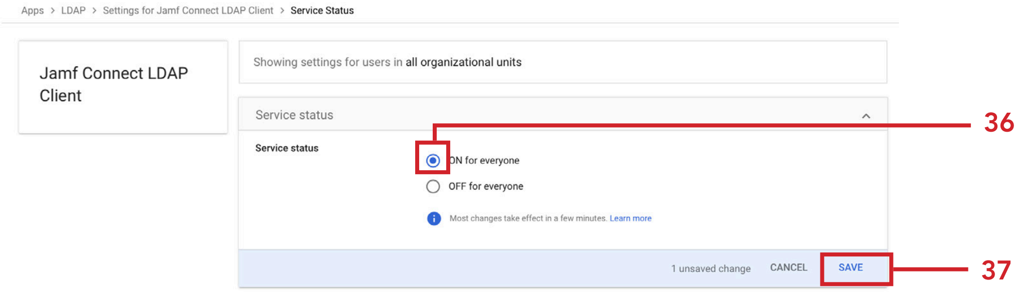
Status
OFF

Service status OFF

Access permissions

Verify user credentials	Read user information	Read group information
Entire domain	No access	No access

36. Select the radio button for On for everyone.
37. Click Save



Apps > LDAP > Settings for Jamf Connect LDAP Client > Service Status

Jamf Connect LDAP Client

Showing settings for users in all organizational units

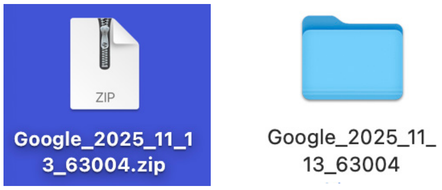
Service status

Service status
● ON for everyone
○ OFF for everyone

Most changes take effect in a few minutes. Learn more

1 unsaved change CANCEL SAVE

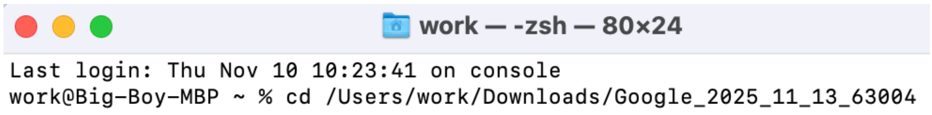
38. Log out of https://admin.google.com
39. Next we are going to create a LDAP Keystore.Go to your Downloads folder and double-click on the Google Certificate that we downloaded in step 23 of this section. The name will be similar to Google_2025_11_13_63004.zip. Once unzipped, there will be a folder with a similar name in your downloads folder.



40. Open Terminal from /Applications/Utilities/.

41. We need to change the current working directory in the Terminal. Enter cd then drag the unzipped Google folder into the terminal window so it copies the exact path to the folder. It will look similar to the picture below.

```
cd /Users/<Home>/Downloads/Google_2025_11_13_63004
```

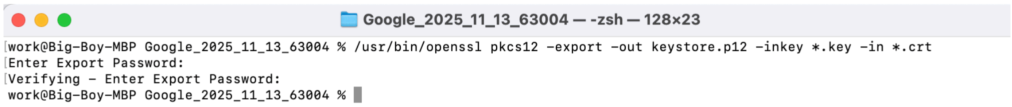


```
Last login: Thu Nov 10 10:23:41 on console
work@Big-Boy-MBP ~ % cd /Users/work/Downloads/Google_2025_11_13_63004
```

42. Enter the following command:

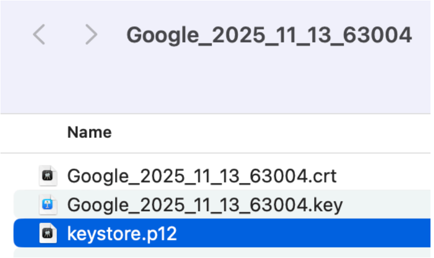
```
/usr/bin/openssl pkcs12 -export -out keystore.p12 -inkey *.key -in *.crt
```

You will be prompted to enter an Export Password and to verify it. For simplicity, this guide will use 1234. NOTE: Pick a more secure password in a production environment.



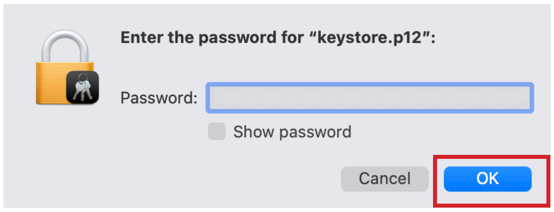
```
work@Big-Boy-MBP Google_2025_11_13_63004 % /usr/bin/openssl pkcs12 -export -out keystore.p12 -inkey *.key -in *.crt
Enter Export Password:
Verifying - Enter Export Password:
work@Big-Boy-MBP Google_2025_11_13_63004 %
```

43. A file named keystore.p12 will be created in the same folder as the Google certs located in your Downloads folder. The name of the folder will be similar to this Google_2025_11_13_63004. Double-Click the keystore.p12 file.

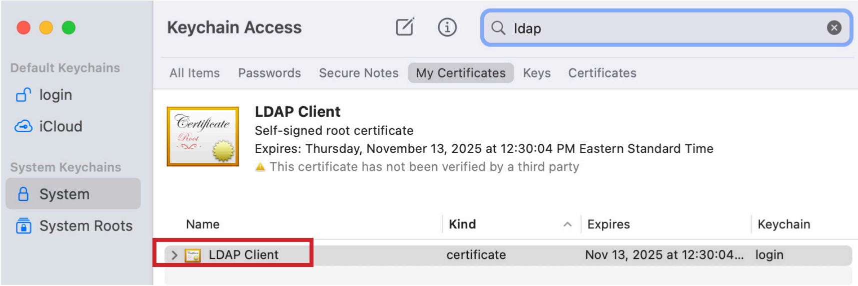


Google_2025_11_13_63004.crt
Google_2025_11_13_63004.key
keystore.p12

44. Enter the password that you created when exporting the certificate. Click OK.


Enter the password for "keystore.p12":

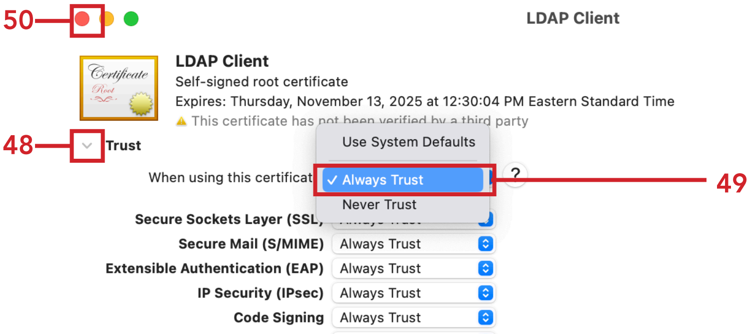
45. Keychain Access will open automatically. In the search bar, enter ldap.
46. Confirm System under System Keychains is selected and My Certificates is selected.
47. Double-click on the LDAP Client certificate.



LDAP Client
Self-signed root certificate
Expires: Thursday, November 13, 2025 at 12:30:04 PM Eastern Standard Time
⚠ This certificate has not been verified by a third party

Name	Kind	Expires	Keychain
LDAP Client	certificate	Nov 13, 2025 at 12:30:04...	login

48. Click Expand (>) for Trust to view the settings.
49. From the menu, select Always Trust.
50. Close this window.

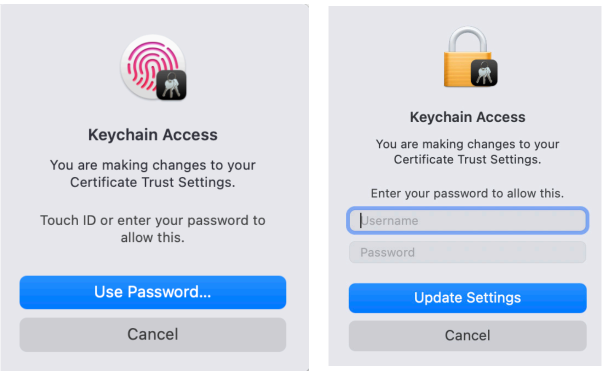


LDAP Client
Self-signed root certificate
Expires: Thursday, November 13, 2025 at 12:30:04 PM Eastern Standard Time
⚠ This certificate has not been verified by a third party

When using this certificat

Secure Sockets Layer (SSL)	Always Trust
Secure Mail (S/MIME)	Always Trust
Extensible Authentication (EAP)	Always Trust
IP Security (IPsec)	Always Trust
Code Signing	Always Trust

51. At the prompt, enter your credentials or use your Touch ID to Update the settings.



Keychain Access

You are making changes to your Certificate Trust Settings.

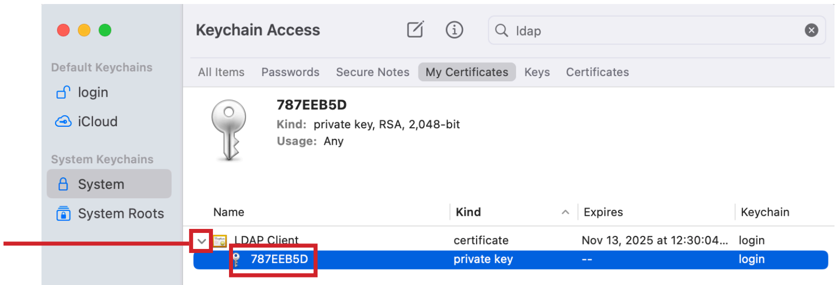
Touch ID or enter your password to allow this.

Keychain Access

You are making changes to your Certificate Trust Settings.

Enter your password to allow this.

52. Expand (>) the LDAP Client certificate so you can see the private key. Double-Click on the private key.



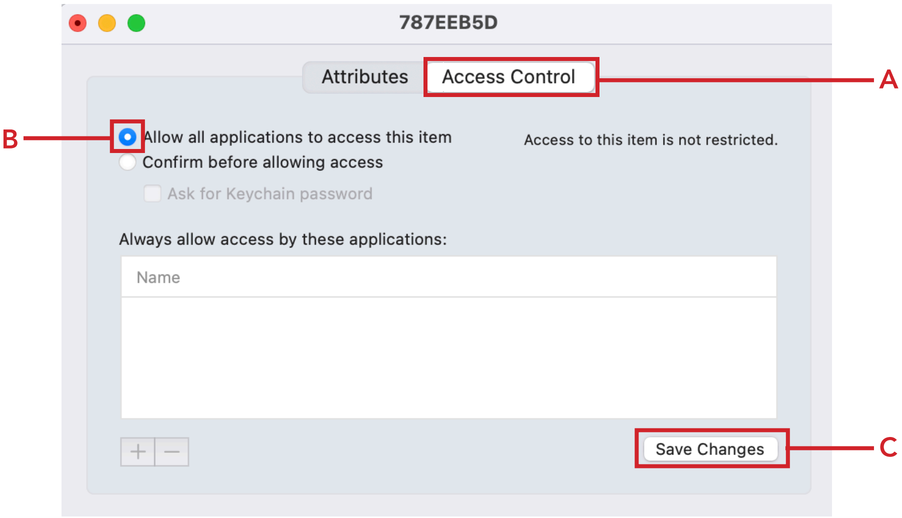
787EEB5D
Kind: private key, RSA, 2,048-bit
Usage: Any

Name	Kind	Expires	Keychain
LDAP Client	certificate	Nov 13, 2025 at 12:30:04...	login
787EEB5D	private key	--	login

Expand LDAP Client to view the private key

53. Configure the following:

A. Click Access Control
B. Select the radio button for Allow all applications to access this item
C. Save Changes

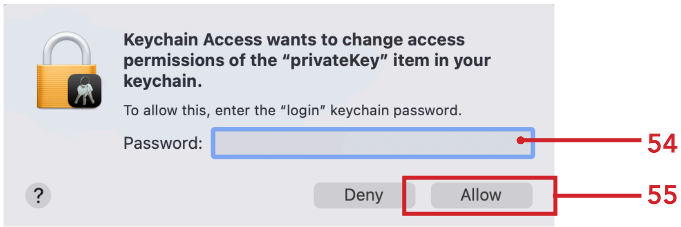


● Allow all applications to access this item
○ Confirm before allowing access
□ Ask for Keychain password

Access to this item is not restricted.

Always allow access by these applications:

54. Enter your administrative credentials
55. Click Allow.

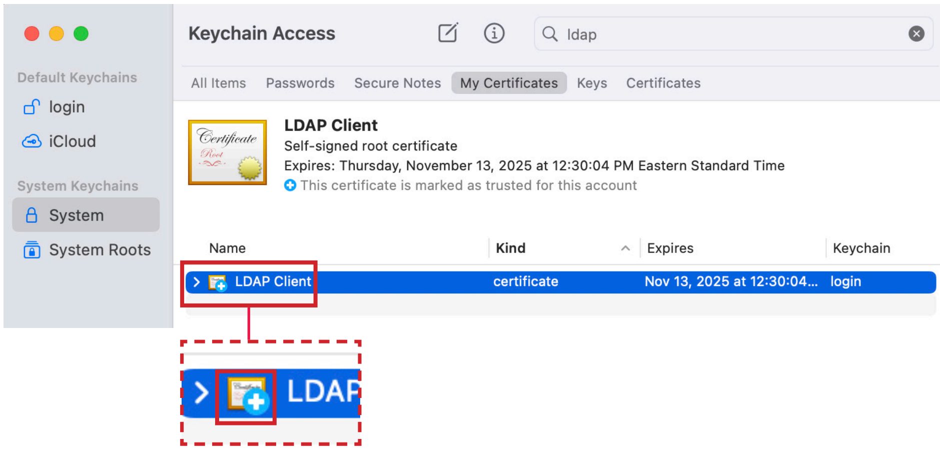


Keychain Access wants to change access permissions of the “privateKey” item in your keychain.

To allow this, enter the “login” keychain password.

Password:

56. Confirm that the LDAP Client certificate now shows as trusted (a blue + appears on the icon.)
57. Quit Keychain Access when done.



LDAP Client
Self-signed root certificate
Expires: Thursday, November 13, 2025 at 12:30:04 PM Eastern Standard Time
This certificate is marked as trusted for this account

Name	Kind	Expires	Keychain
LDAP Client	certificate	Nov 13, 2025 at 12:30:04...	login

In the next section we will use the Jamf Connect Configuration app to test connectivity to Google Cloud Identity.

This completes this section.

Section 2:
Authenticate to Google Cloud Identity using the Jamf Connect Configuration App

What You'll Need

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

Hardware and Software

Requirements for following along with this section:

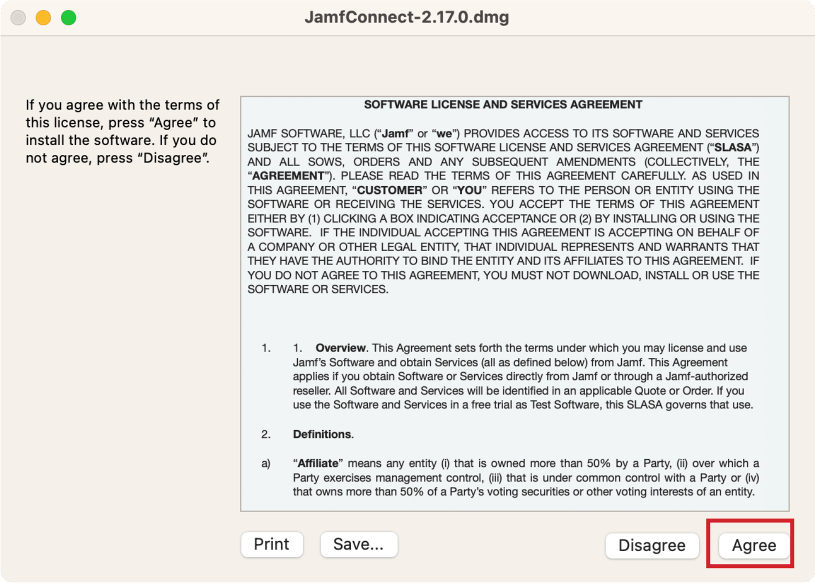
- A Mac with macOS 10.15.4 or later. This guide will use macOS 13.0.1.
- Jamf Connect installer DMG. This guide will use version 2.17.0.
- Google Cloud Identity Client ID and Client Secret.

In this lesson we will configure the Jamf Connect Configuration App to use Google Cloud Identity with a few basic settings. Jamf Connect authenticates to Google using OIDC. Google does NOT support ROPG so password changes will require an LDAP certificate. This section will show you how easy it is to test connectivity to Google using the Jamf Connect Configuration App.

NOTE: Google does NOT support Jamf Unlock or role based management of user accounts created with Jamf Connect.

1. Double click the JamfConnect-2.17.0 dmg.

2. Click Agree.



If you agree with the terms of this license, press "Agree" to install the software. If you do not agree, press "Disagree".

SOFTWARE LICENSE AND SERVICES AGREEMENT

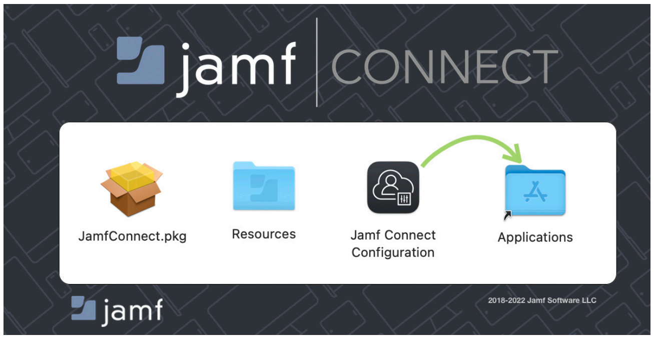
JAMF SOFTWARE, LLC ("**Jamf**" or "**we**") PROVIDES ACCESS TO ITS SOFTWARE AND SERVICES SUBJECT TO THE TERMS OF THIS SOFTWARE LICENSE AND SERVICES AGREEMENT ("**SLASA**") AND ALL SOWS, ORDERS AND ANY SUBSEQUENT AMENDMENTS (COLLECTIVELY, THE "**AGREEMENT**"). PLEASE READ THE TERMS OF THIS AGREEMENT CAREFULLY. AS USED IN THIS AGREEMENT, "**CUSTOMER**" OR "**YOU**" REFERS TO THE PERSON OR ENTITY USING THE SOFTWARE OR RECEIVING THE SERVICES. YOU ACCEPT THE TERMS OF THIS AGREEMENT EITHER BY (1) CLICKING A BOX INDICATING ACCEPTANCE OR (2) BY INSTALLING OR USING THE SOFTWARE. IF THE INDIVIDUAL ACCEPTING THIS AGREEMENT IS ACCEPTING ON BEHALF OF A COMPANY OR OTHER LEGAL ENTITY, THAT INDIVIDUAL REPRESENTS AND WARRANTS THAT THEY HAVE THE AUTHORITY TO BIND THE ENTITY AND ITS AFFILIATES TO THIS AGREEMENT. IF YOU DO NOT AGREE TO THIS AGREEMENT, YOU MUST NOT DOWNLOAD, INSTALL OR USE THE SOFTWARE OR SERVICES.

1. 1. **Overview**. This Agreement sets forth the terms under which you may license and use Jamf's Software and obtain Services (all as defined below) from Jamf. This Agreement applies if you obtain Software or Services directly from Jamf or through a Jamf-authorized reseller. All Software and Services will be identified in an applicable Quote or Order. If you use the Software and Services in a free trial as Test Software, this SLASA governs that use.

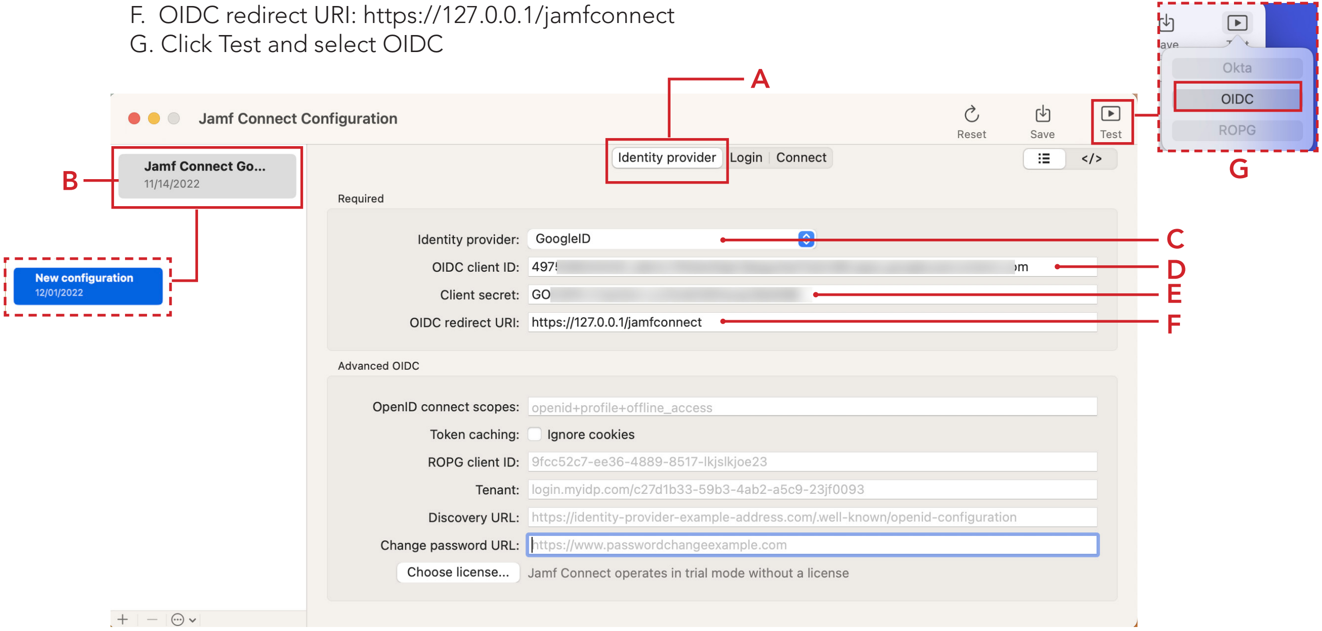
2. **Definitions**.

a) "**Affiliate**" means any entity (i) that is owned more than 50% by a Party, (ii) over which a Party exercises management control, (iii) that is under common control with a Party or (iv) that owns more than 50% of a Party's voting securities or other voting interests of an entity.

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



4. Configure the following:
    - A. Click Identity Provider
    - B. Select New Configuration and rename the configuration: Jamf Connect Google
    - C. Identity Provider: GoogleID
    - D. OIDC Client ID: Paste in your client ID that you copied in section 1 of this guide.
    - E. Client Secret: Paste in your client secret that you copied in section 1 of this guide.
    - F. OIDC redirect URI: https://127.0.0.1/jamfconnect
    - G. Click Test and select OIDC



Required

Identity provider: GoogleID

OIDC client ID: 497[redacted]om

Client secret: GO[redacted]

OIDC redirect URI: https://127.0.0.1/jamfconnect

Advanced OIDC

OpenID connect scopes: openid+profile+offline_access

Token caching: □ Ignore cookies

ROPG client ID: 9fcc52c7-ee36-4889-8517-lkjslkjoe23

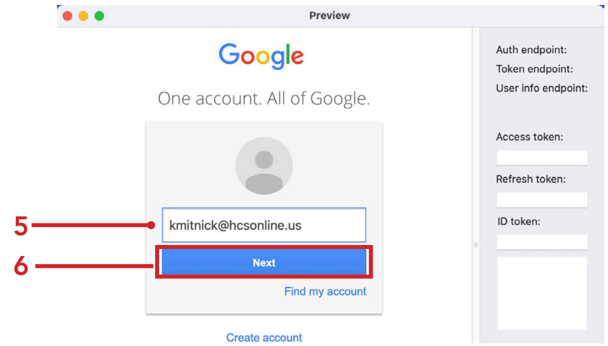
Tenant: login.myidp.com/c27d1b33-59b3-4ab2-a5c9-23jf0093

Discovery URL: https://identity-provider-example-address.com/.well-known/openid-configuration

Change password URL: https://www.passwordchangeexample.com

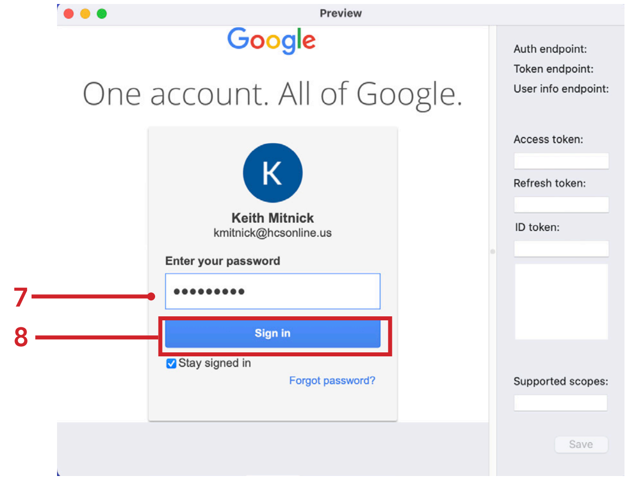
Jamf Connect operates in trial mode without a license

5. Enter your Google account name
6. Click Next.



kmitnick@hcsonline.us

7. Enter your Google account password
8. Click Sign In.



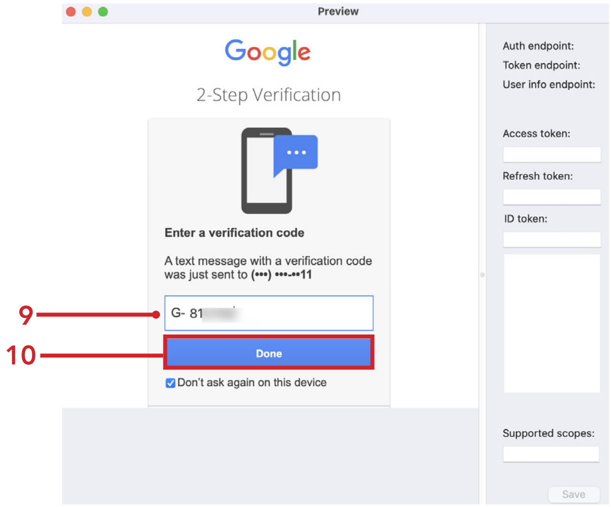
Keith Mitnick
kmitnick@hcsonline.us

Enter your password

•••••••••

☑ Stay signed in

9. If you have MFA enabled, enter the code
10. Click Done.



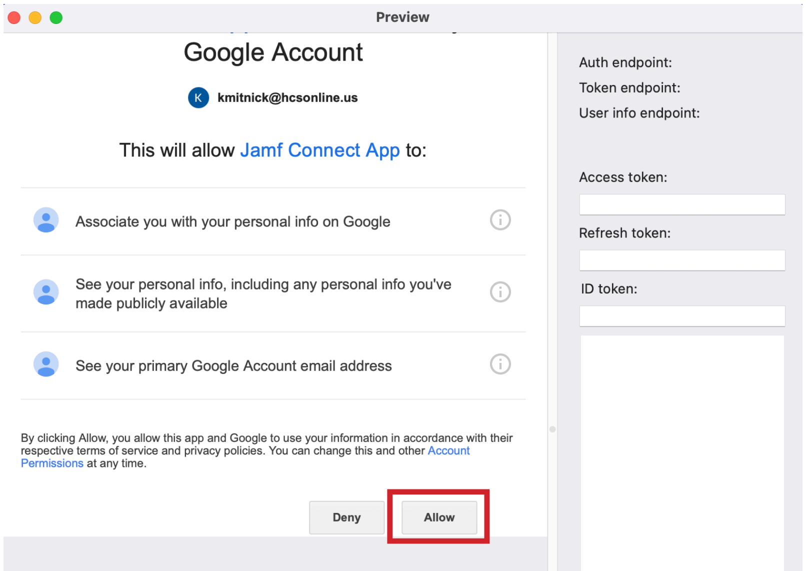
Enter a verification code

A text message with a verification code was just sent to (•••) •••-••11

G- 81[redacted]

☑ Don't ask again on this device

11. Click Allow.



Preview

Google Account

kmitnick@hcsonline.us

This will allow Jamf Connect App to:

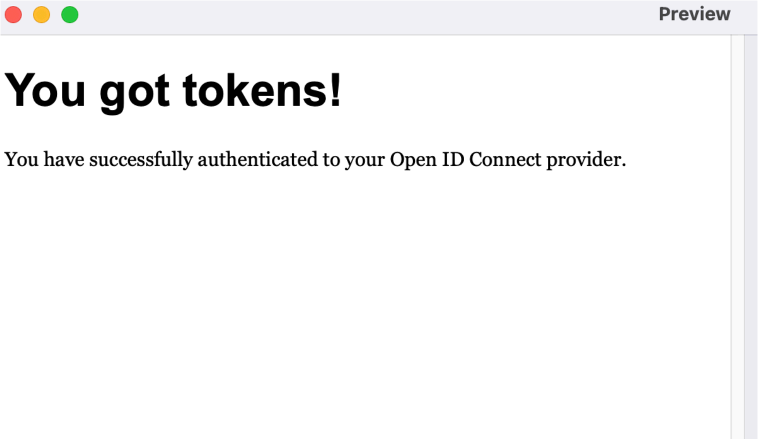
Associate you with your personal info on Google

See your personal info, including any personal info you've made publicly available

See your primary Google Account email address

By clicking Allow, you allow this app and Google to use your information in accordance with their respective terms of service and privacy policies. You can change this and other Account Permissions at any time.

12. If authentication was successful, you will see the message below. Close the window. That is all you need to configure Google Cloud Identity with Jamf Connect for basic authentication settings. Close the window.



Preview

You got tokens!

You have successfully authenticated to your Open ID Connect provider.

In the next section we will create a code signing certificate using the Jamf Pro Server.

This completes this section.

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

What You'll Need

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

Hardware and Software

Requirements for following along with this section:

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

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

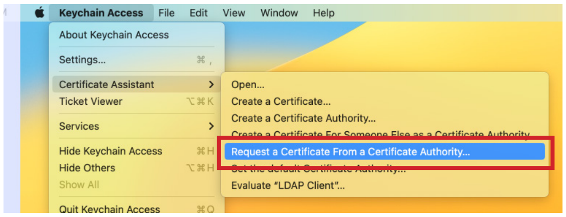
Why do we need a code signing certificate?
In order to deploy a package using a PreStage enrollment in Jamf Pro, the package must be signed. In the next section of this guide, we will create a custom package with images and scripts that will be used to customize the look of Jamf Connect. This package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

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

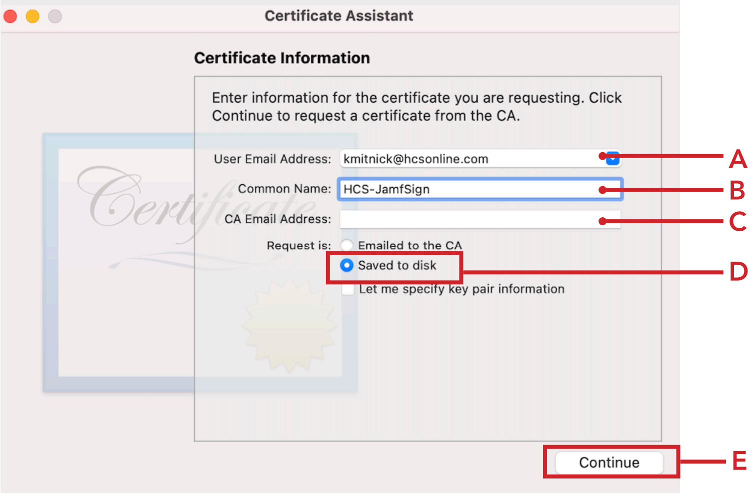
1. Open Keychain Access located in /Applications/Utilities.

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.



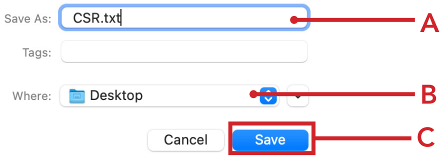
Certificate Assistant

Certificate Information

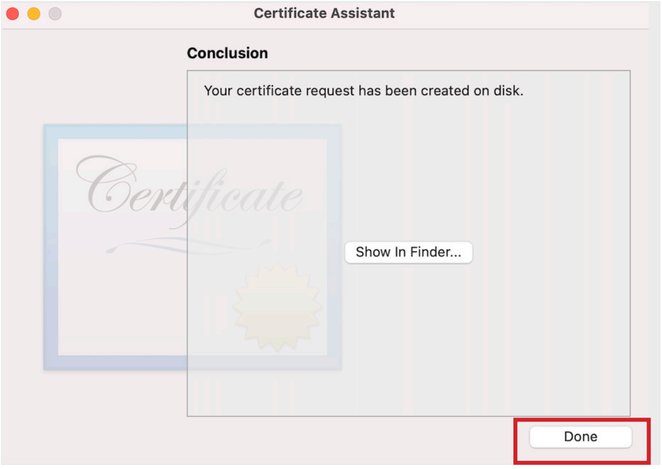
Enter information for the certificate you are requesting. Click Continue to request a certificate from the CA.

User Email Address: kmitnick@hcsonline.com
Common Name: HCS-JamfSign
CA Email Address:
Request is: ○ Emailed to the CA
● Saved to disk
□ Let me specify key pair information

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



5. Click Done.

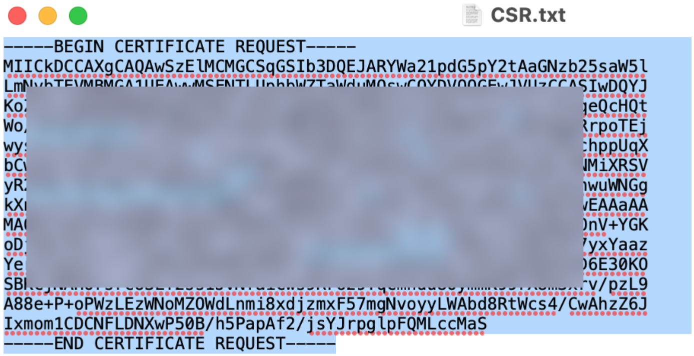


Conclusion

Your certificate request has been created on disk.

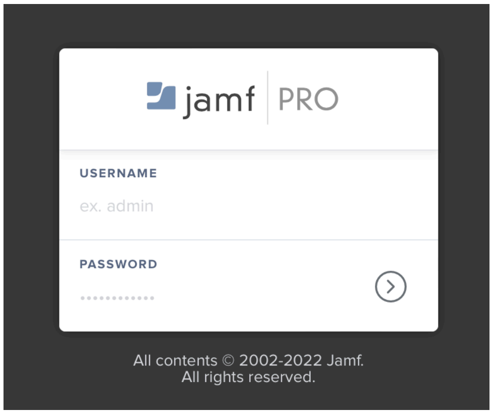
6. Open the CSR.txt file on your desktop with a text editor.

7. Copy the entire CSR text.



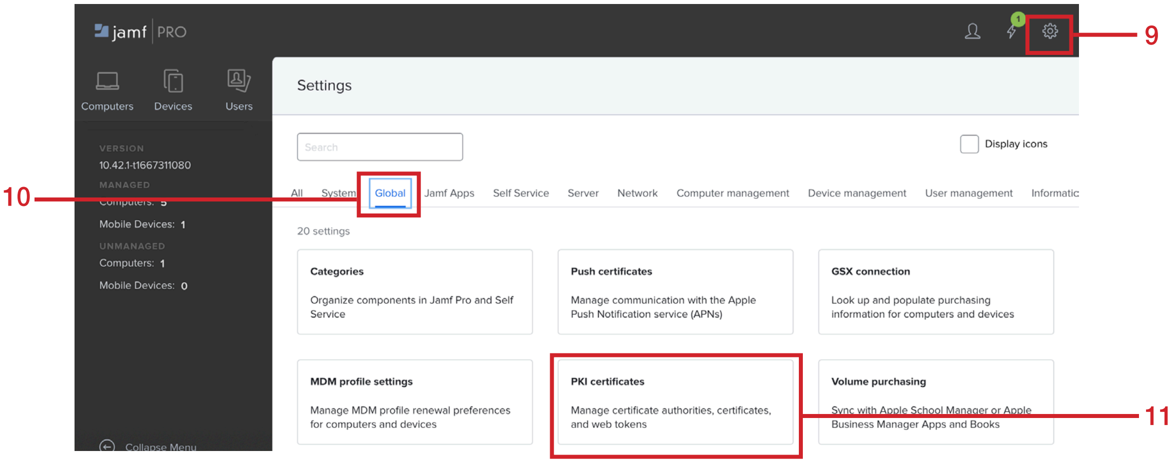
```
-----BEGIN CERTIFICATE REQUEST-----
MIICkDCCAXgCAQAwSzElMCMGCSqGSIb3DQEJARYWa21pdG5pY2tAaGNzb25saW5l
[redacted]
A88e+P+oPWzLEzWNoMZOWdLnmi8xdjzmxF57mgNvoyyLWAbd8RtWcs4/CwAhzZ6J
Ixmom1CDCNFLDNXwP50B/h5PapAf2/jsYJrpglpFQMLccMaS
-----END CERTIFICATE REQUEST-----
```

8. Log into your Jamf Pro Server.



All contents © 2002-2022 Jamf.
All rights reserved.

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



VERSION
10.42.1-t1667311080
MANAGED
Computers: 5
Mobile Devices: 1
UNMANAGED
Computers: 1
Mobile Devices: 0

20 settings

Categories
Organize components in Jamf Pro and Self Service

Push certificates
Manage communication with the Apple Push Notification service (APNs)

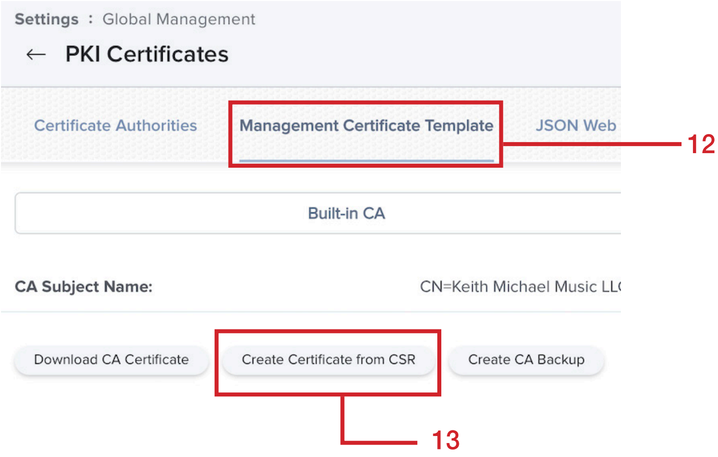
GSX connection
Look up and populate purchasing information for computers and devices

MDM profile settings
Manage MDM profile renewal preferences for computers and devices

PKI certificates
Manage certificate authorities, certificates, and web tokens

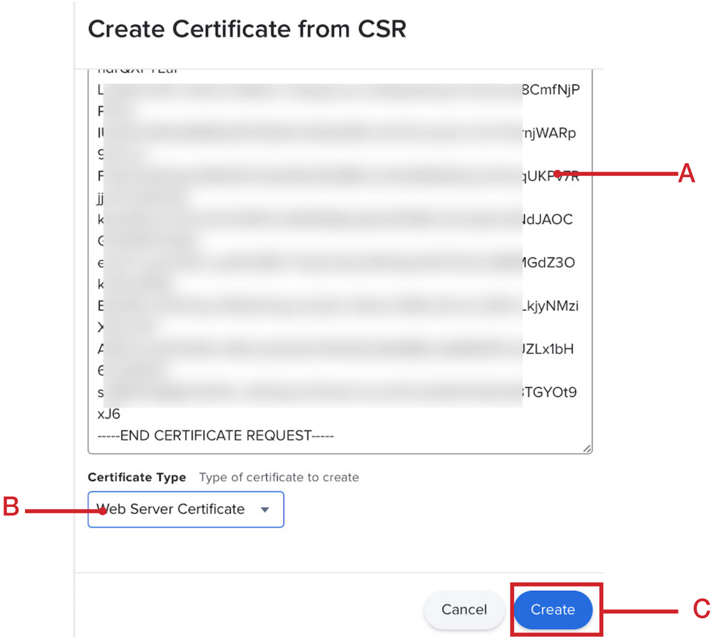
Volume purchasing
Sync with Apple School Manager or Apple Business Manager Apps and Books

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



CA Subject Name: CN=Keith Michael Music LL

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.



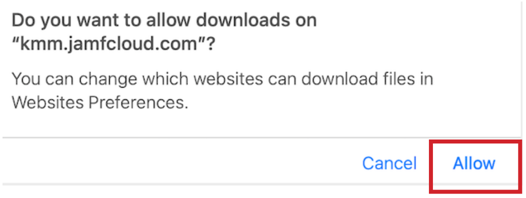
Create Certificate from CSR

```
[redacted]
8CmfNjP
njWARp
qUKPV7R
NdJAOC
MGdZ3O
LkjyNMzi
JZLx1bH
TGYOt9
xJ6
-----END CERTIFICATE REQUEST-----
```

Certificate Type Type of certificate to create

Web Server Certificate ▾

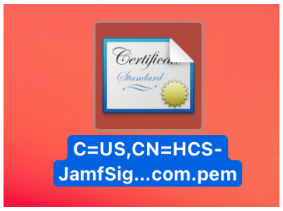
15. Click Allow.
    NOTE: After downloading the file your web browser may need to be refreshed to properly display things in Jamf Pro.



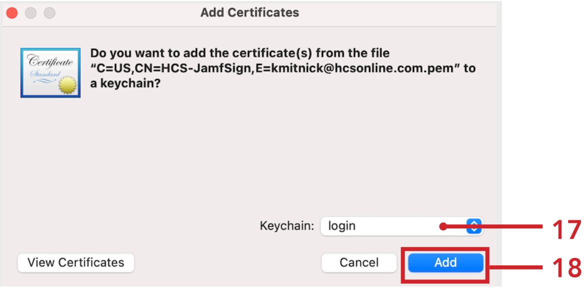
Do you want to allow downloads on "kmm.jamfcloud.com"?

You can change which websites can download files in Websites Preferences.

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



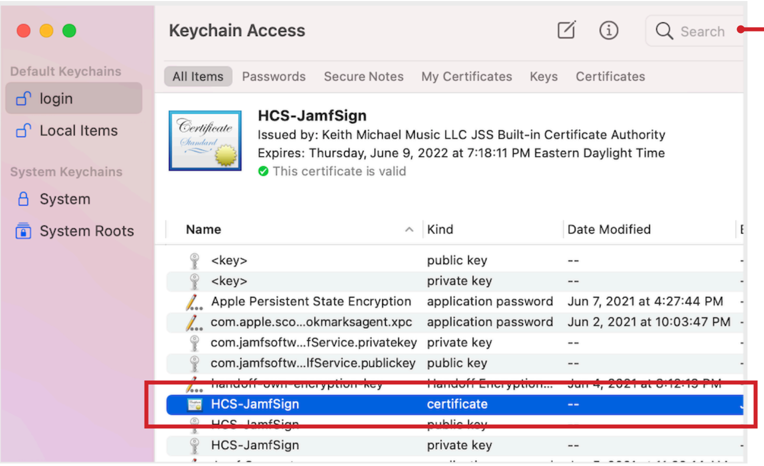
17. From the Keychain menu, select login.
18. Click Add.



Do you want to add the certificate(s) from the file "C=US,CN=HCS-JamfSign,E=kmitnick@hcsonline.com.pem" to a keychain?

Keychain: login

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.

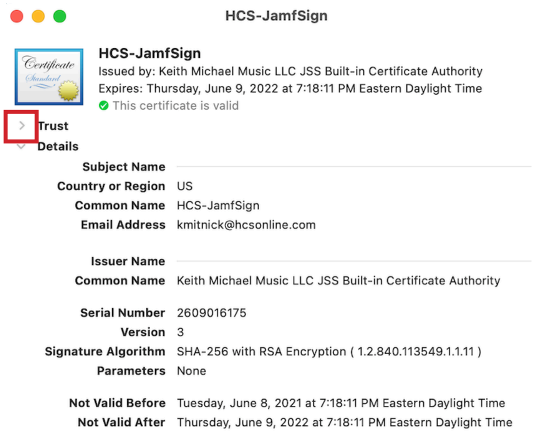


HCS-JamfSign
Issued by: Keith Michael Music LLC JSS Built-in Certificate Authority
Expires: Thursday, June 9, 2022 at 7:18:11 PM Eastern Daylight Time
✓ This certificate is valid

Name	Kind	Date Modified
<key>	public key	--
<key>	private key	--
Apple Persistent State Encryption	application password	Jun 7, 2021 at 4:27:44 PM
com.apple.sco...okmarksagent.xpc	application password	Jun 2, 2021 at 10:03:47 PM
com.jamfsoftw...fService.privatekey	private key	--
com.jamfsoftw...lfService.publickey	public key	--
handoff-own-encryption-key	Handoff Encryption...	Jun 4, 2021 at 8:12:13 PM
HCS-JamfSign	certificate	--
HCS-JamfSign	public key	--
HCS-JamfSign	private key	--

You may use search to look for the correct certificate

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



HCS-JamfSign
Issued by: Keith Michael Music LLC JSS Built-in Certificate Authority
Expires: Thursday, June 9, 2022 at 7:18:11 PM Eastern Daylight Time
✓ This certificate is valid

> Trust
⌄ Details

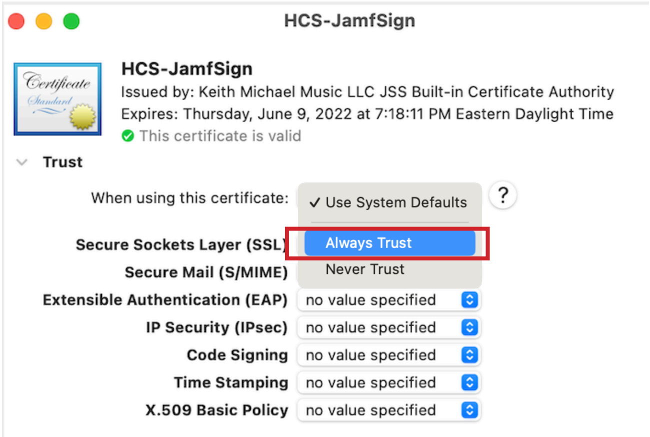
Subject Name
Country or Region US
Common Name HCS-JamfSign
Email Address kmitnick@hcsonline.com

Issuer Name
Common Name Keith Michael Music LLC JSS Built-in Certificate Authority

Serial Number 2609016175
Version 3
Signature Algorithm SHA-256 with RSA Encryption (1.2.840.113549.1.1.11)
Parameters None

Not Valid Before Tuesday, June 8, 2021 at 7:18:11 PM Eastern Daylight Time
Not Valid After Thursday, June 9, 2022 at 7:18:11 PM Eastern Daylight Time

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



HCS-JamfSign

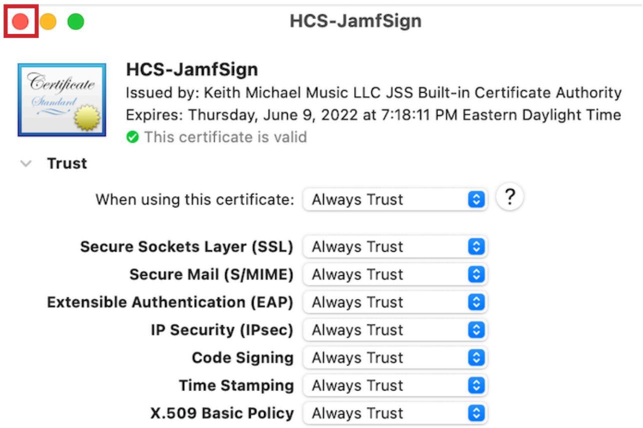
HCS-JamfSign
Issued by: Keith Michael Music LLC JSS Built-in Certificate Authority
Expires: Thursday, June 9, 2022 at 7:18:11 PM Eastern Daylight Time
This certificate is valid

Trust

When using this certificate: ✓ Use System Defaults / Always Trust / Never Trust

Secure Sockets Layer (SSL)
Secure Mail (S/MIME)
Extensible Authentication (EAP): no value specified
IP Security (IPsec): no value specified
Code Signing: no value specified
Time Stamping: no value specified
X.509 Basic Policy: no value specified

22. Close the window.



HCS-JamfSign

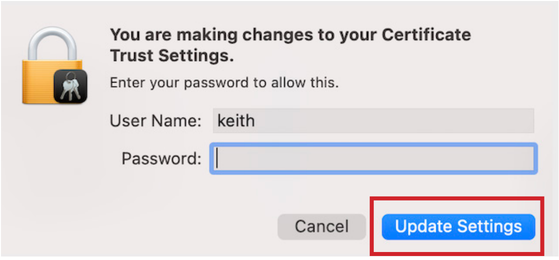
HCS-JamfSign
Issued by: Keith Michael Music LLC JSS Built-in Certificate Authority
Expires: Thursday, June 9, 2022 at 7:18:11 PM Eastern Daylight Time
This certificate is valid

Trust

When using this certificate: Always Trust

Secure Sockets Layer (SSL): Always Trust
Secure Mail (S/MIME): Always Trust
Extensible Authentication (EAP): Always Trust
IP Security (IPsec): Always Trust
Code Signing: Always Trust
Time Stamping: Always Trust
X.509 Basic Policy: Always Trust

23. Enter your admin credentials and click Update Settings.



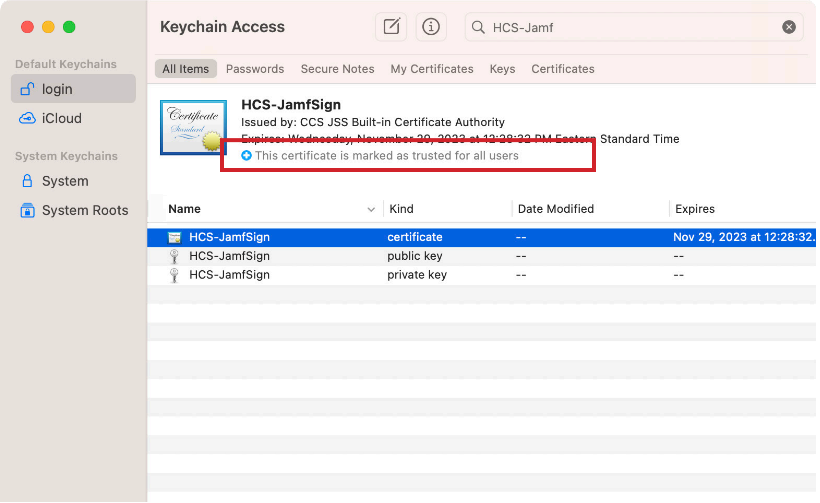
You are making changes to your Certificate Trust Settings.

Enter your password to allow this.

User Name: keith

Password:

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



HCS-JamfSign
Issued by: CCS JSS Built-in Certificate Authority
Expires: Wednesday, November 29, 2023 at 12:28:32 PM Eastern Standard Time
This certificate is marked as trusted for all users

Name	Kind	Date Modified	Expires
HCS-JamfSign	certificate	--	Nov 29, 2023 at 12:28:32.
HCS-JamfSign	public key	--	--
HCS-JamfSign	private key	--	--

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

What You'll Need

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

Hardware and Software

Requirements for following along with this section:

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

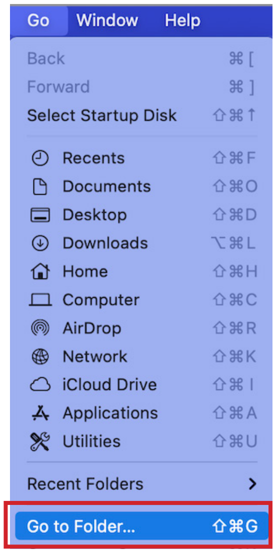
In this section we will create a folder structure for branding images, and scripts. Once the structure is created, we will add our branding images, Login Window scripts, and Menu bar scripts to the corresponding folders then use Composer to set permissions and create a package to deploy to all computers. 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: 16 x 16 pixels
- Login logo: 250 x 250 pixels
- Sign in Logo 449 x 131 pixels

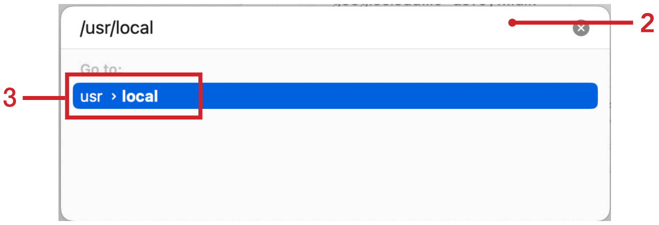
NOTE: This guide will use Composer for packaging. You can get Composer from your assets in your Jamf account located at https://id.jamf.com

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

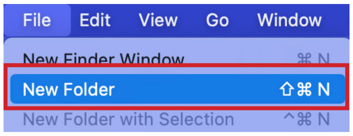


2. Enter the following path: /usr/local

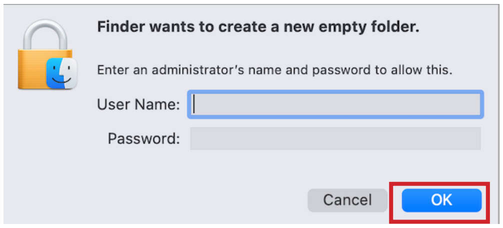
3. Click usr > local or hit Enter.



4. Create a New Folder.



5. Enter your Admin credentials then click OK.



Finder wants to create a new empty folder.

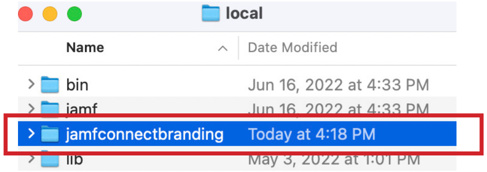
Enter an administrator's name and password to allow this.

User Name:

Password:

6. Name the folder jamfconnectbranding.

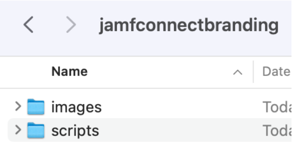
7. Open the jamfconnectbranding folder.



local

Name	Date Modified
bin	Jun 16, 2022 at 4:33 PM
jamf	Jun 16, 2022 at 4:33 PM
jamfconnectbranding	Today at 4:18 PM
lib	May 3, 2022 at 1:01 PM

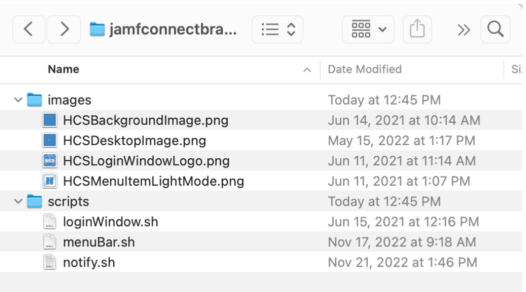
8. Follow steps 3 and 4 to create two folders within the jamfconnectbranding folder:
   - images
   - scripts



jamfconnectbranding

Name	Date
images	Toda
scripts	Toda

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.



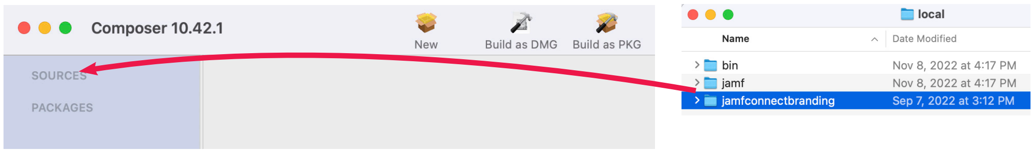
jamfconnectbra...

Name	Date Modified	Si
images	Today at 12:45 PM	
HCSBackgroundImage.png	Jun 14, 2021 at 10:14 AM	
HCSDesktopImage.png	May 15, 2022 at 1:17 PM	
HCSLoginWindowLogo.png	Jun 11, 2021 at 11:14 AM	
HCSMenuItemLightMode.png	Jun 11, 2021 at 1:07 PM	
scripts	Today at 12:45 PM	
loginWindow.sh	Jun 15, 2021 at 12:16 PM	
menuBar.sh	Nov 17, 2022 at 9:18 AM	
notify.sh	Nov 21, 2022 at 1:46 PM	

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

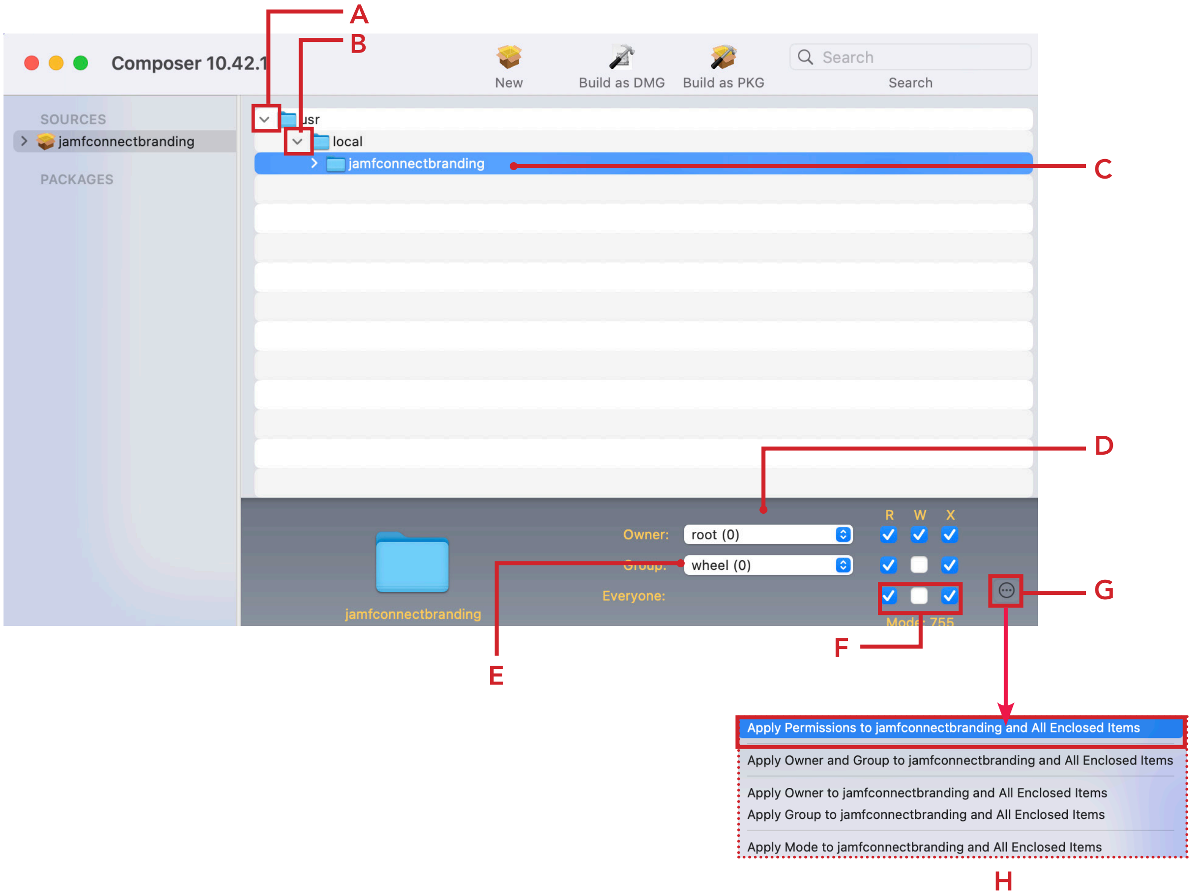
Composer

11. Click Cancel at the make a Snapshot message.
12. Drag the jamfconnectbranding folder to Sources.



Name	Date Modified
bin	Nov 8, 2022 at 4:17 PM
jamf	Nov 8, 2022 at 4:17 PM
jamfconnectbranding	Sep 7, 2022 at 3:12 PM

13. 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.



Owner: root (0)

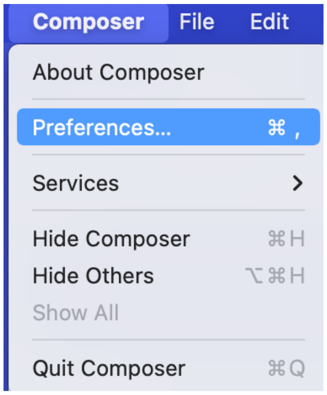
Group: wheel (0)

Everyone:

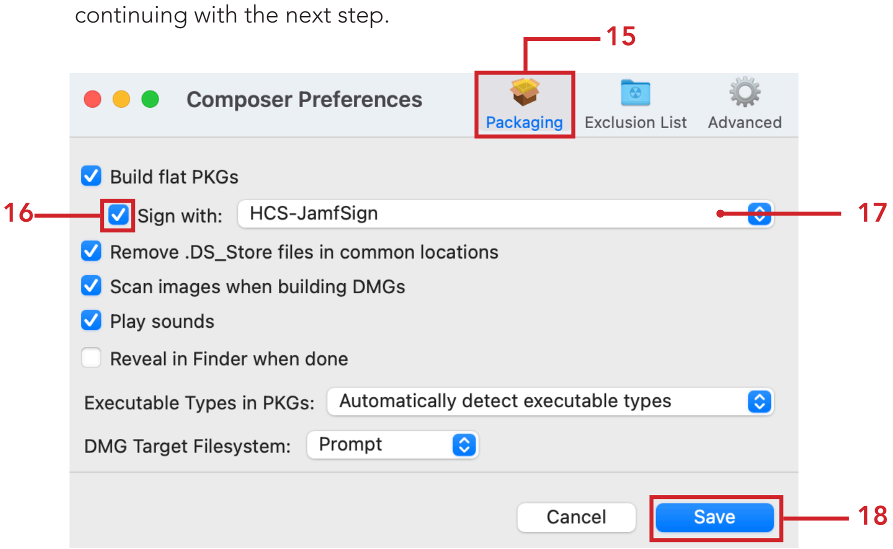
Mode: 755

Apply Permissions to jamfconnectbranding and All Enclosed Items
Apply Owner and Group to jamfconnectbranding and All Enclosed Items
Apply Owner to jamfconnectbranding and All Enclosed Items
Apply Group to jamfconnectbranding and All Enclosed Items
Apply Mode to jamfconnectbranding and All Enclosed Items

14. Click the Composer menu then select Preferences.

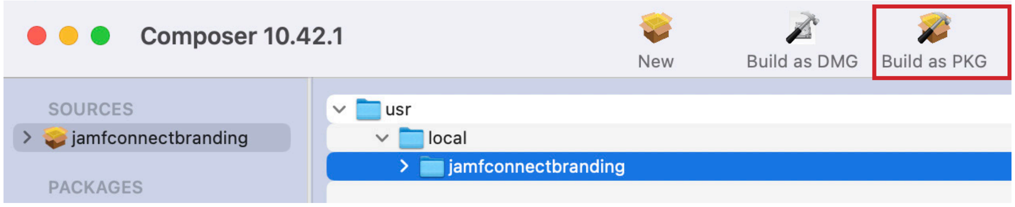


15. Click Packaging.
16. Select the checkbox for Sign with.
17. From the menu, select your signing certificate.
18. Click Save.
NOTE: We need to sign this package if we want to use it in a PreStage enrollment in Jamf Pro. If you don't have a code signing certificate, refer to section 3 of this guide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

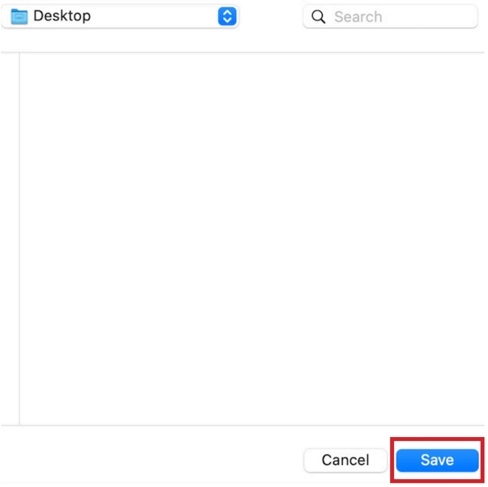


☑ Build flat PKGs
☑ Sign with: HCS-JamfSign
☑ Remove .DS_Store files in common locations
☑ Scan images when building DMGs
☑ Play sounds
☐ Reveal in Finder when done
Executable Types in PKGs: Automatically detect executable types
DMG Target Filesystem: Prompt

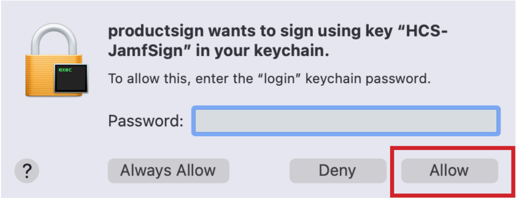
19. Confirm your settings.
20. Click Build as PKG.



21. Save the package to your Desktop.



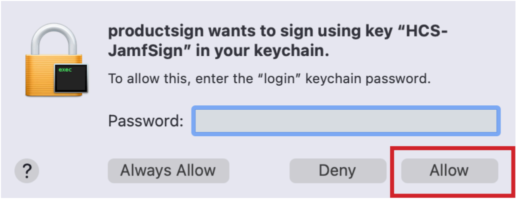
22. Enter your Admin password to sign the package.
23. Click Allow. You will see this message twice.


productsign wants to sign using key "HCS-JamfSign" in your keychain.

To allow this, enter the "login" keychain password.

Password:

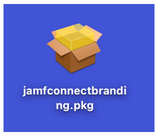
24. Enter your Admin password to sign the package.
25. Click Allow.


productsign wants to sign using key "HCS-JamfSign" in your keychain.

To allow this, enter the "login" keychain password.

Password:

26. 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

What You'll Need

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

Hardware and Software

Requirements for following along with this section:

- A Mac with macOS 10.15.4 or later.
- Jamf Connect Configuration App 2.17.0.
- Google Cloud Identity Client ID and Client Secret.

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.

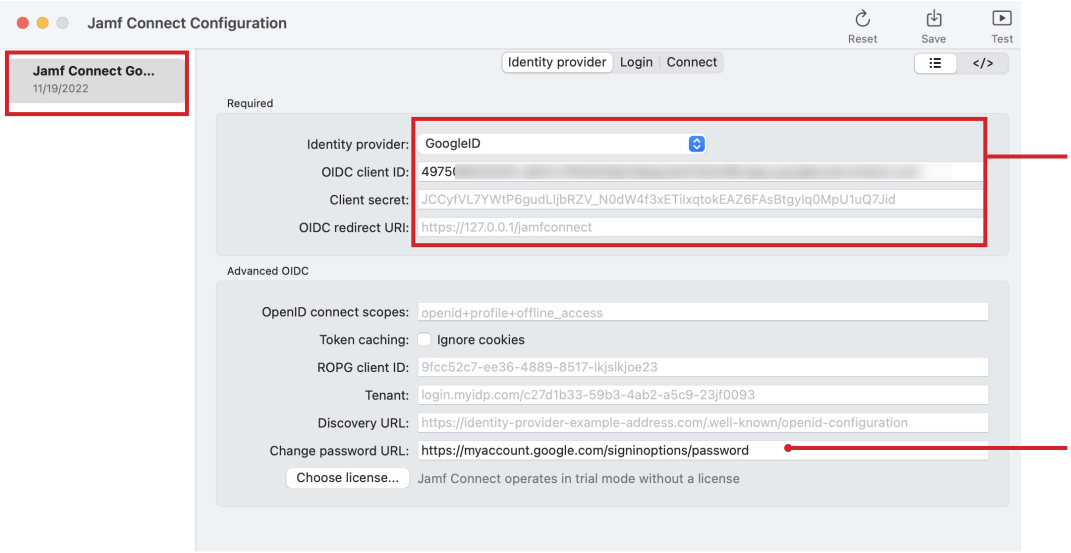
https://docs.jamf.com/jamf-connect/documentation/Jamf_Connect_Documentation.html

1. Open the Jamf Connect Configuration App.

Jamf Connect
Configuration

2. In section two of this guide, we created a configuration named Jamf Connect Google. Select that configuration then click Identity Provider. It should only have the following configured:
    - Identity Provider: GoogleID
    - OIDC Client ID: Your client ID should be entered here
    - Client Secret: Your client secret should be entered here
    - OIDC Redirect URI: https://127.0.0.1/jamfconnect

3. Add this to Change password URL:
   https://myaccount.google.com/signinoptions/password
   NOTE: We are adding the URL above so we can change the password using the Jamf Connect menu bar.



Required

Identity provider: GoogleID
OIDC client ID: 4975[redacted]
Client secret: JCCyfVL7YWtP6gudLljbRZV_N0dW4f3xETilxqtokEAZ6FAsBtgylq0MpU1uQ7Jid
OIDC redirect URI: https://127.0.0.1/jamfconnect

Advanced OIDC

OpenID connect scopes: openid+profile+offline_access
Token caching: □ Ignore cookies
ROPG client ID: 9fcc52c7-ee36-4889-8517-lkjslkjoe23
Tenant: login.myidp.com/c27d1b33-59b3-4ab2-a5c9-23jf0093
Discovery URL: https://identity-provider-example-address.com/.well-known/openid-configuration
Change password URL: https://myaccount.google.com/signinoptions/password
Choose license... Jamf Connect operates in trial mode without a license

Confirm these settings

3

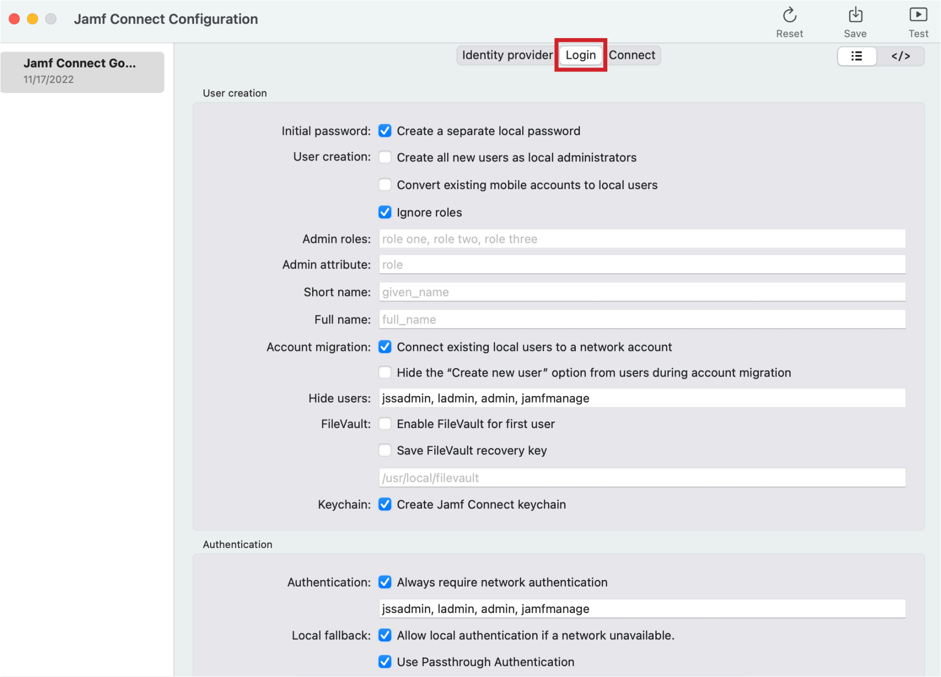
4. Click Login. This has many options and we will not cover all of them in this guide however, We will discuss some of them briefly. Configure these settings to your needs.

User Creation

- Initial Password: Create a separate local password This is required when using Google Cloud Identity as your IDP as Google does NOT support ROPG. It uses LDAP for passwords so Jamf Connect cannot pass along the password.
- Create all new users as local administrators Enable this if you want all users to be created as admins when they log in with their Google credentials.
- Convert existing mobile accounts to local users Enable this if you want to migrate your mobile accounts to local Mac accounts.
- Ignore roles Google Cloud Identity does NOT support this feature but you need to select the checkbox so the local user account is not demoted to a standard account if they are already an admin on the Mac.
- Account Migration Enable this if your users already have a local account on the Mac and they want to link it to their Google login. This will avoid the user having two separate accounts when they log in with their Google credentials. It adds an alias to their existing user account on the Mac with the Google username.
- Hide the “Create New User” option from users during account migration Enable 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, we recommend handling FileVault using your Jamf Pro server and allow the key to be escrowed back to the Jamf pro server.
- Keychain Enable this to create the Jamf Connect Keychain.

Authentication

- Authentication Select the checkbox for "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 Enable this 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.
- Use Passthrough Authentication Enable this to avoid having to enter your password multiple times on startup or a restart of your Mac. If you have FileVault enabled, you will need to enter your password twice if this is enabled instead of three times if FileVault is not enabled.



User creation

Initial password: ☑ Create a separate local password

User creation: □ Create all new users as local administrators

□ Convert existing mobile accounts to local users

☑ Ignore roles

Admin roles: role one, role two, role three

Admin attribute: role

Short name: given_name

Full name: full_name

Account migration: ☑ Connect existing local users to a network account

□ Hide the “Create new user” option from users during account migration

Hide users: jssadmin, ladmin, admin, jamfmanage

FileVault: □ Enable FileVault for first user

□ Save FileVault recovery key

/usr/local/filevault

Keychain: ☑ Create Jamf Connect keychain

Authentication

Authentication: ☑ Always require network authentication

jssadmin, ladmin, admin, jamfmanage

Local fallback: ☑ Allow local authentication if a network unavailable.

☑ Use Passthrough Authentication

5. Continue from Step 4.

Appearance (Optional)

- **Internet** Enable this 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** Enable this if you want to hide these buttons at the Login Window.

Help section (Optional)

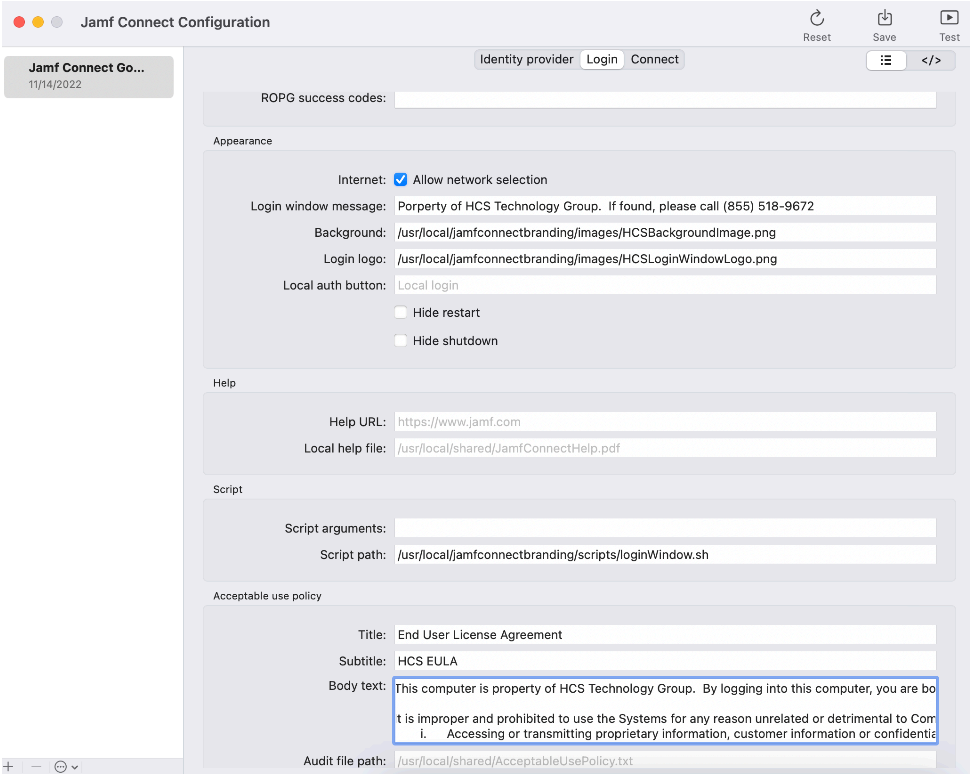
- **Help URL** URL to a help page of your choosing.
- **Local Help File** You can create a custom help file that lives in the same location on all Macs.

Script section (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.
- **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.



ROPG success codes:

Appearance

Internet: ☑ Allow network selection

Login window message: Porperty of HCS Technology Group. If found, please call (855) 518-9672

Background: /usr/local/jamfconnectbranding/images/HCSBackgroundImage.png

Login logo: /usr/local/jamfconnectbranding/images/HCSLoginWindowLogo.png

Local auth button: Local login

☐ Hide restart

☐ Hide shutdown

Help

Help URL: https://www.jamf.com

Local help file: /usr/local/shared/JamfConnectHelp.pdf

Script

Script arguments:

Script path: /usr/local/jamfconnectbranding/scripts/loginWindow.sh

Acceptable use policy

Title: End User License Agreement

Subtitle: HCS EULA

Body text: This computer is property of HCS Technology Group. By logging into this computer, you are bo

t is improper and prohibited to use the Systems for any reason unrelated or detrimental to Com
i. Accessing or transmitting proprietary information, customer information or confidentia

Audit file path: /usr/local/shared/AcceptableUsePolicy.txt

6. Click Connect tab.

Authentication

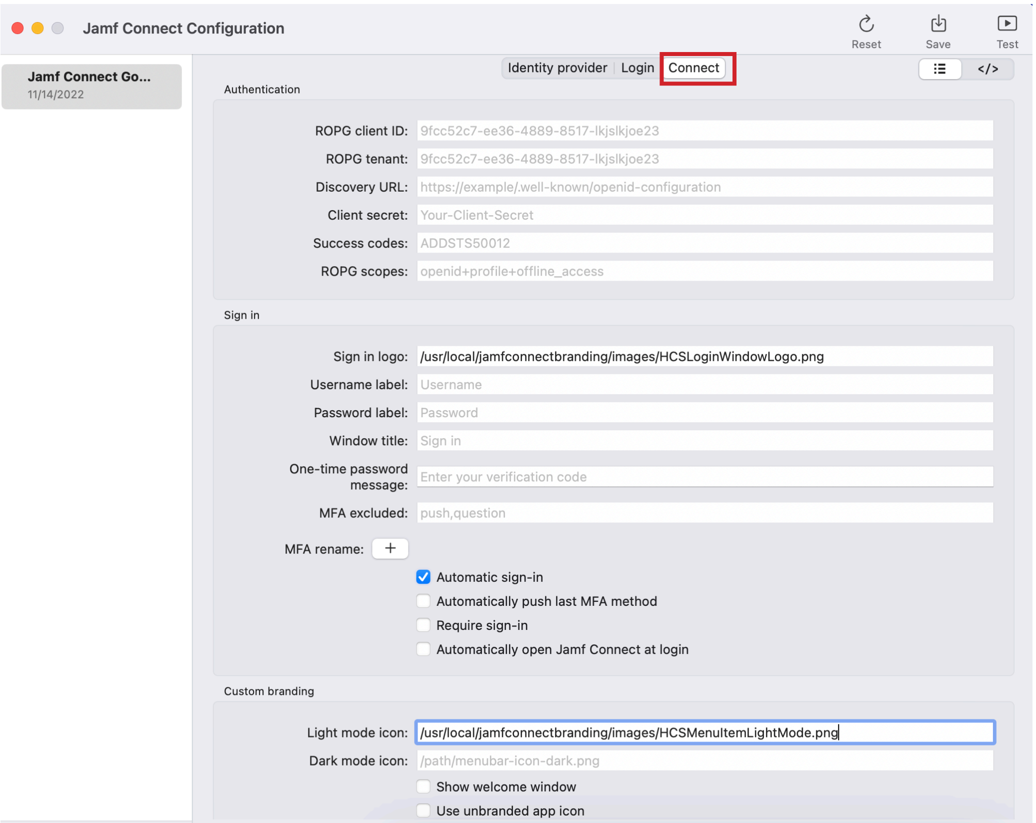
- ROPG is not supported by Google Cloud Identity.

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** Select the checkbox to enable Jamf Connect to automatically sign in using your stored credential 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** We recommend selecting then deselcting the check 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 (see graphic on side.) 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.



Authentication

ROPG client ID: 9fcc52c7-ee36-4889-8517-lkjslkjoe23

ROPG tenant: 9fcc52c7-ee36-4889-8517-lkjslkjoe23

Discovery URL: https://example/.well-known/openid-configuration

Client secret: Your-Client-Secret

Success codes: ADDSTS50012

ROPG scopes: openid+profile+offline_access

Sign in

Sign in logo: /usr/local/jamfconnectbranding/images/HCSLoginWindowLogo.png

Username label: Username

Password label: Password

Window title: Sign in

One-time password message: Enter your verification code

MFA excluded: push,question

MFA rename: +

☑ Automatic sign-in

□ Automatically push last MFA method

□ Require sign-in

□ Automatically open Jamf Connect at login

Custom branding

Light mode icon: /usr/local/jamfconnectbranding/images/HCSMenuItemLightMode.png

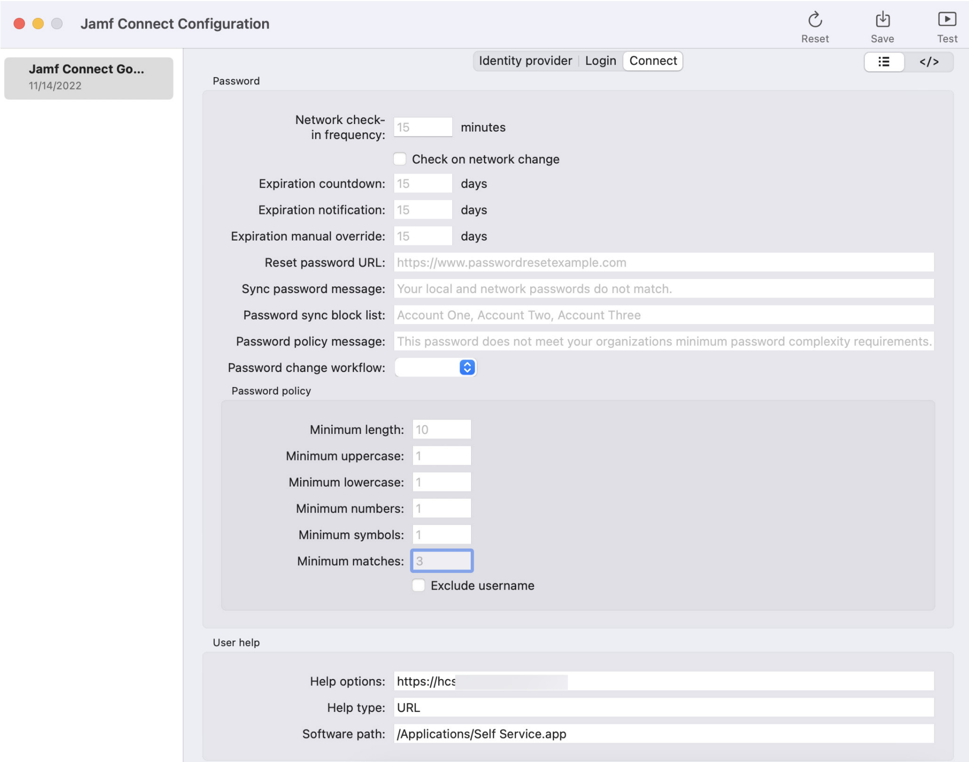
Dark mode icon: /path/menubar-icon-dark.png

□ Show welcome window

□ Use unbranded app icon

7. **Password** (Optional)
   - Network Check-in Frequency By default, Jamf Connect will check every 60 minutes to see if the Google 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 or 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.



Password

Network check-in frequency:	15 minutes
	□ Check on network change
Expiration countdown:	15 days
Expiration notification:	15 days
Expiration manual override:	15 days
Reset password URL:	https://www.passwordresetexample.com
Sync password message:	Your local and network passwords do not match.
Password sync block list:	Account One, Account Two, Account Three
Password policy message:	This password does not meet your organizations minimum password complexity requirements.
Password change workflow:	

Password policy

Minimum length:	10
Minimum uppercase:	1
Minimum lowercase:	1
Minimum numbers:	1
Minimum symbols:	1
Minimum matches:	3
	□ Exclude username

User help

Help options:	https://hcs[redacted]
Help type:	URL
Software path:	/Applications/Self Service.app

8. Continue from step 7:

Scripting (Optional).

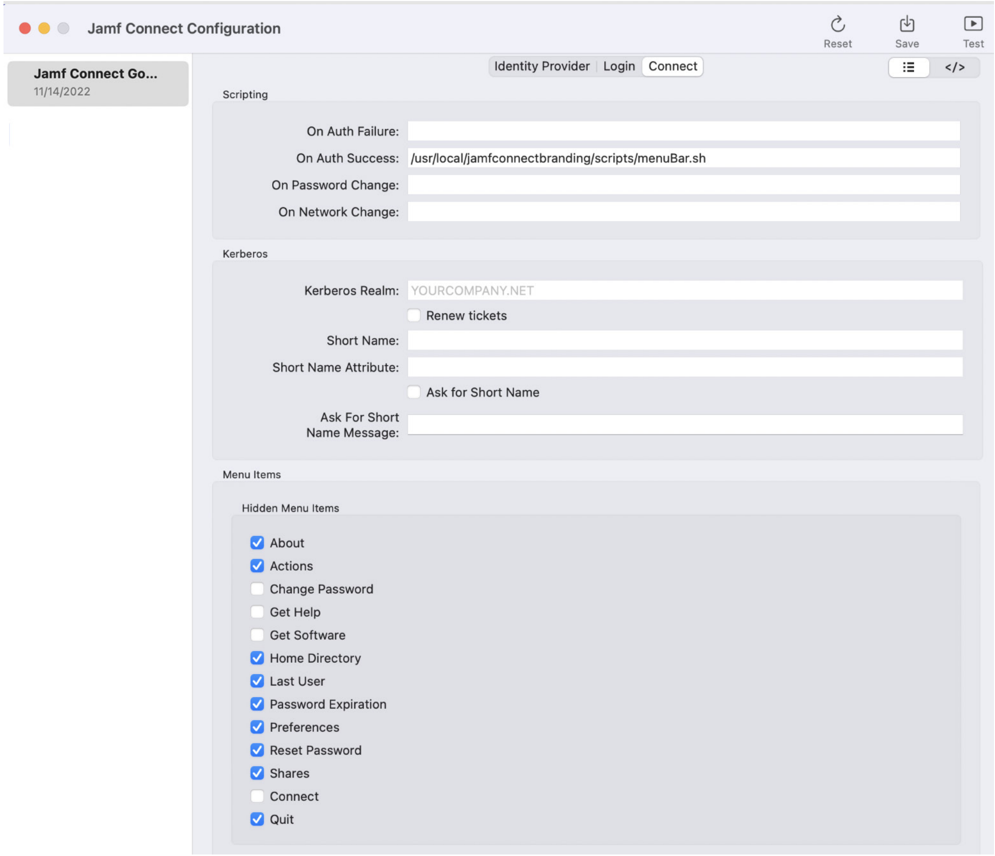
- You can add the path to a script in each field listed. For example, if you wanted to run a script on a successful Authentication, enter the path to the script you want to run in the field. See the path in the On Auth Success field in the picture below.

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.



Scripting

On Auth Failure:
On Auth Success: /usr/local/jamfconnectbranding/scripts/menuBar.sh
On Password Change:
On Network Change:

Kerberos

Kerberos Realm: YOURCOMPANY.NET
□ Renew tickets
Short Name:
Short Name Attribute:
□ Ask for Short Name
Ask For Short Name Message:

Menu Items

Hidden Menu Items

☑ About
☑ Actions
□ Change Password
□ Get Help
□ Get Software
☑ Home Directory
☑ Last User
☑ Password Expiration
☑ Preferences
☑ Reset Password
☑ Shares
□ Connect
☑ Quit

9. Continue from Step 8.

   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 7.

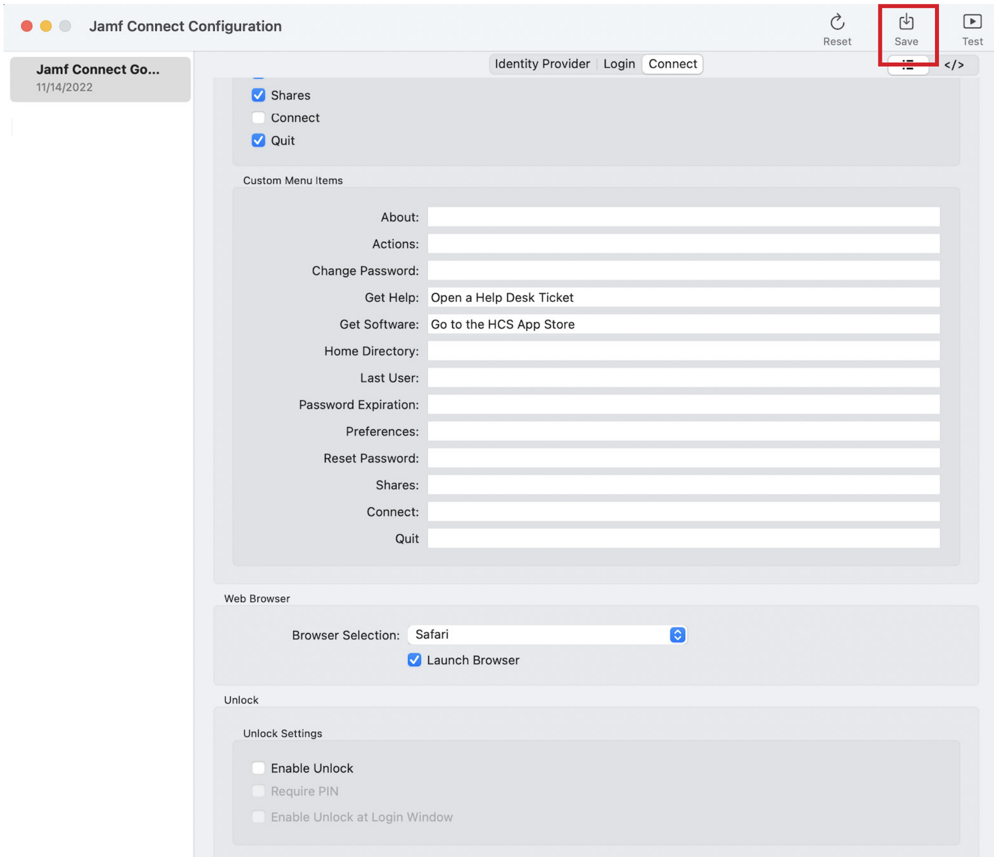
   Web Browser (Optional)

   - 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.

10. Click Save.



☑ Shares
☐ Connect
☑ Quit

Custom Menu Items

About:
Actions:
Change Password:
Get Help: Open a Help Desk Ticket
Get Software: Go to the HCS App Store
Home Directory:
Last User:
Password Expiration:
Preferences:
Reset Password:
Shares:
Connect:
Quit

Web Browser

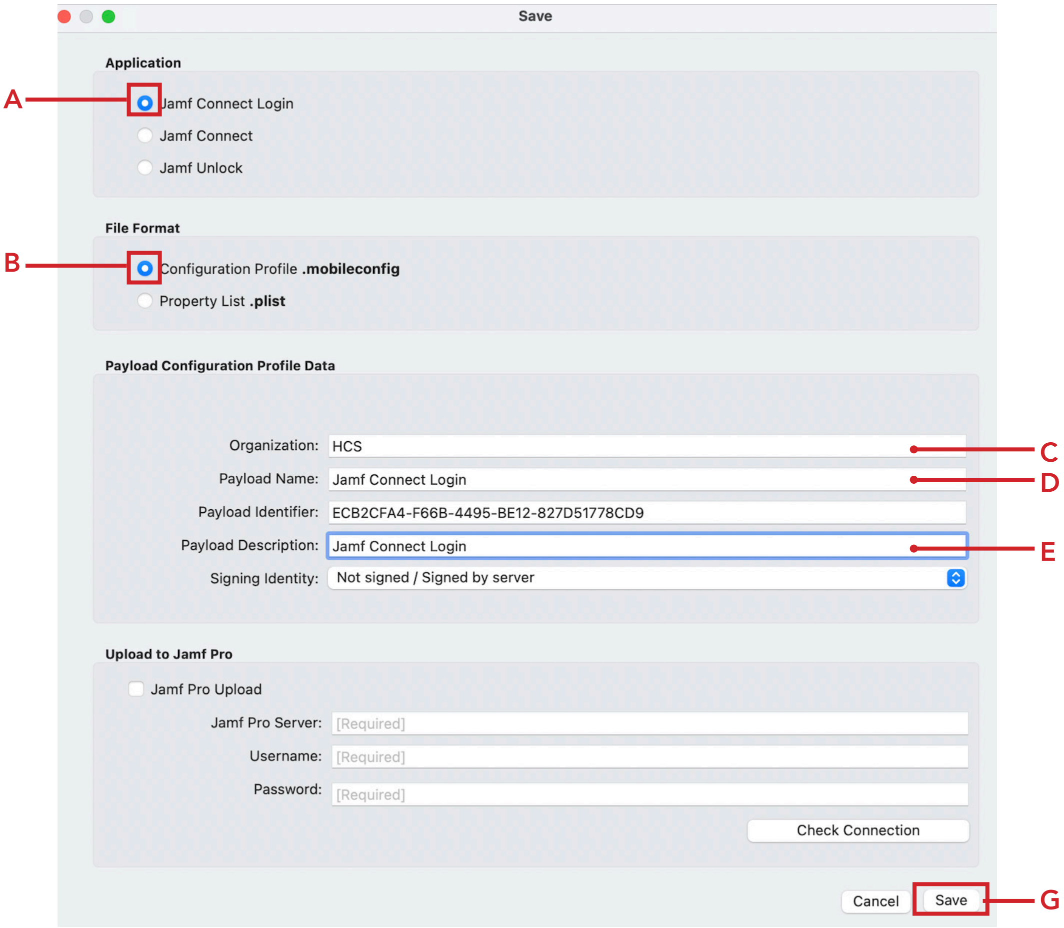
Browser Selection: Safari
☑ Launch Browser

Unlock

Unlock Settings

☐ Enable Unlock
☐ Require PIN
☐ Enable Unlock at Login Window

11. 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.



Save

Application

● Jamf Connect Login
○ Jamf Connect
○ Jamf Unlock

File Format

● Configuration Profile **.mobileconfig**
○ Property List **.plist**

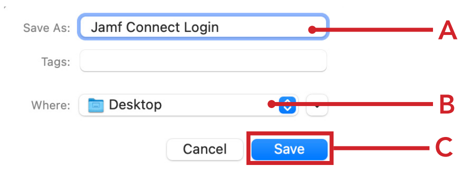
Payload Configuration Profile Data

Organization: HCS
Payload Name: Jamf Connect Login
Payload Identifier: ECB2CFA4-F66B-4495-BE12-827D51778CD9
Payload Description: Jamf Connect Login
Signing Identity: Not signed / Signed by server

Upload to Jamf Pro

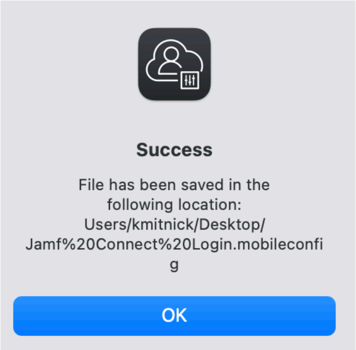
□ Jamf Pro Upload
Jamf Pro Server: [Required]
Username: [Required]
Password: [Required]

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



Save As: Jamf Connect Login
Tags:
Where: Desktop

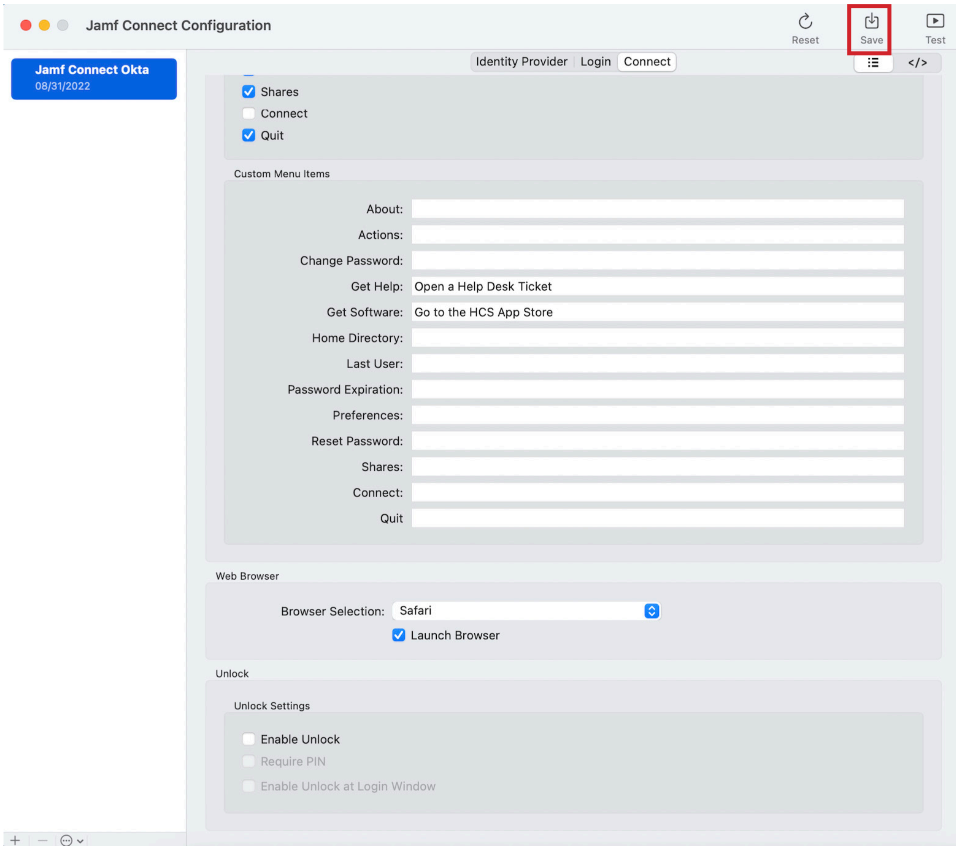
13. Click OK at this message.



Success

File has been saved in the following location: Users/kmitnick/Desktop/Jamf%20Connect%20Login.mobileconfig

14. Click Save.



☑ Shares
□ Connect
☑ Quit

Custom Menu Items

About:
Actions:
Change Password:
Get Help: Open a Help Desk Ticket
Get Software: Go to the HCS App Store
Home Directory:
Last User:
Password Expiration:
Preferences:
Reset Password:
Shares:
Connect:
Quit

Web Browser

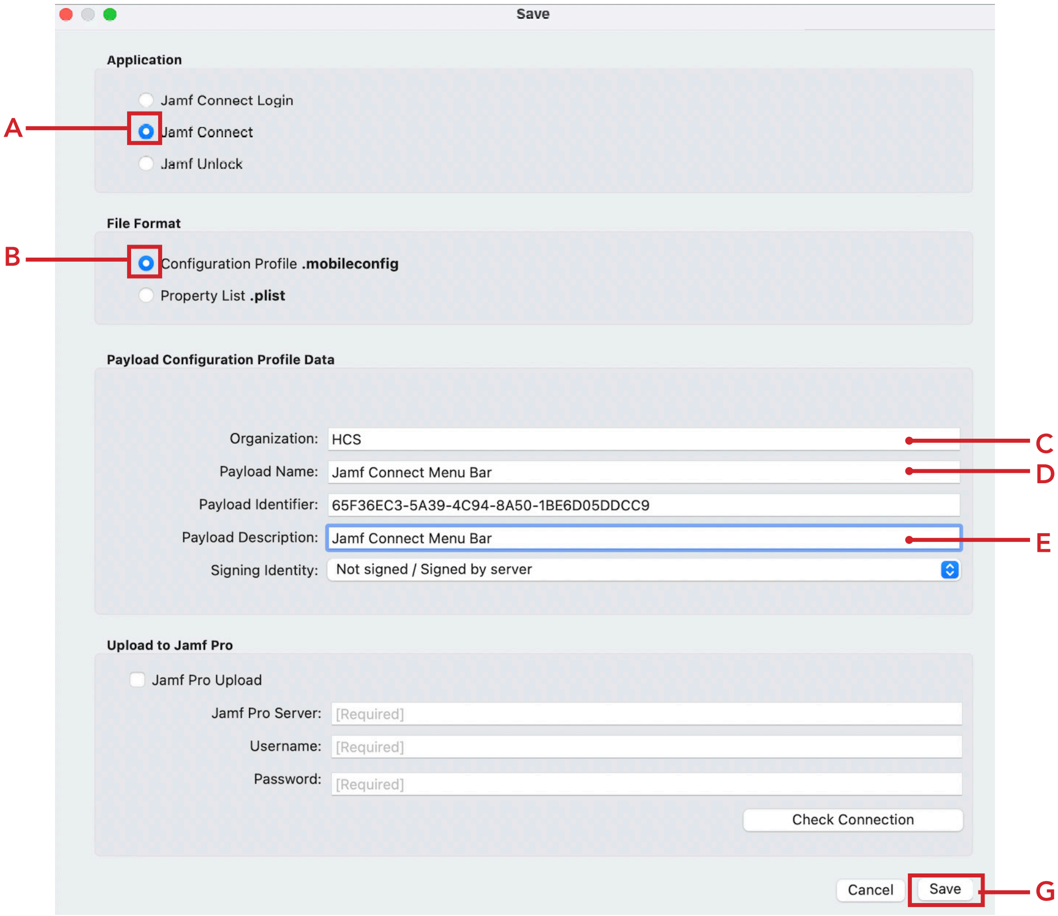
Browser Selection: Safari
☑ Launch Browser

Unlock

Unlock Settings

□ Enable Unlock
□ Require PIN
□ Enable Unlock at Login Window

15. 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.



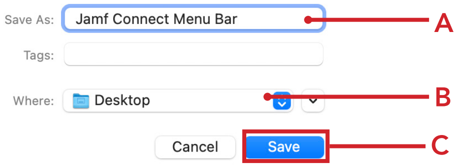
Application
○ Jamf Connect Login
● Jamf Connect
○ Jamf Unlock

File Format
● Configuration Profile **.mobileconfig**
○ Property List **.plist**

Payload Configuration Profile Data
Organization: HCS
Payload Name: Jamf Connect Menu Bar
Payload Identifier: 65F36EC3-5A39-4C94-8A50-1BE6D05DDCC9
Payload Description: Jamf Connect Menu Bar
Signing Identity: Not signed / Signed by server

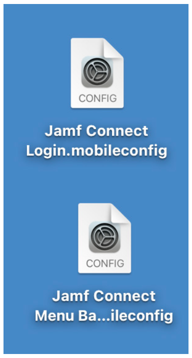
Upload to Jamf Pro
□ Jamf Pro Upload
Jamf Pro Server: [Required]
Username: [Required]
Password: [Required]

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



Save As: Jamf Connect Menu Bar
Tags:
Where: Desktop

17. Confirm that you have two configuration profiles saved on your Desktop.


CONFIG
Jamf Connect Login.mobileconfig
CONFIG
Jamf Connect Menu Ba...ileconfig

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. Once everything is working as expected, we can transfer all the items to the Jamf Pro server.

This completes this section.

Section 6: Manually Installing Jamf Connect on a Mac

What You'll Need

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

Hardware and Software

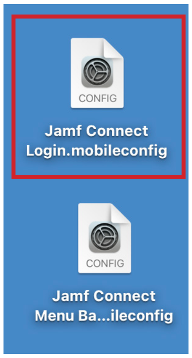
Requirements for following along with this section:

- A Mac with macOS 10.15.4 or later.
- Jamf Connect Installer version 2.17.0
- jamfconnecbranding.pkg - We created this in Section 4.
- Google Login Credentials
- Login Window and Menu Bar Scripts (Optional)

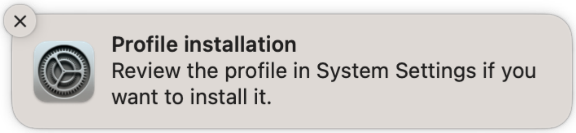
In this section we will install the two configuration profiles we created in Section 5 along with Jamf Connect. Best practice is to always test your configuration profiles by manually installing the configuration profiles and Jamf Connect on a Mac. Once everything is working as expected, we can transfer 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.

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.


CONFIG
Jamf Connect Login.mobileconfig
CONFIG
Jamf Connect Menu Ba...ileconfig

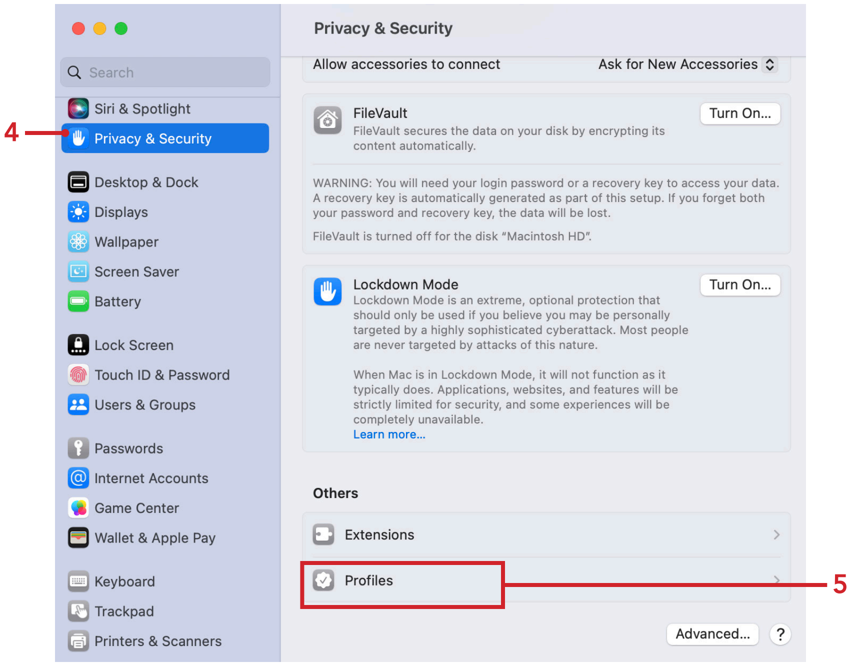
2. Confirm a notification appears to ask you to review the profile.



Profile installation
Review the profile in System Settings if you want to install it.

3. Open System Settings.

4. Click Privacy & Security.
5. Click Profiles



Privacy & Security

Allow accessories to connect — Ask for New Accessories

FileVault
FileVault secures the data on your disk by encrypting its content automatically.

WARNING: You will need your login password or a recovery key to access your data. A recovery key is automatically generated as part of this setup. If you forget both your password and recovery key, the data will be lost.

FileVault is turned off for the disk "Macintosh HD".

Lockdown Mode
Lockdown Mode is an extreme, optional protection that should only be used if you believe you may be personally targeted by a highly sophisticated cyberattack. Most people are never targeted by attacks of this nature.

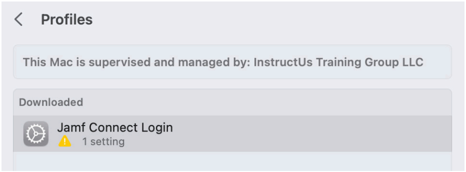
When Mac is in Lockdown Mode, it will not function as it typically does. Applications, websites, and features will be strictly limited for security, and some experiences will be completely unavailable.
Learn more...

Others

Extensions

Profiles

6. Double-click the Jamf Connect Login profile.



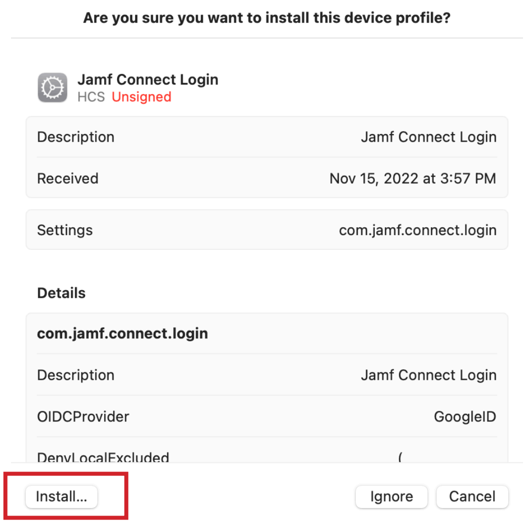
Profiles

This Mac is supervised and managed by: InstructUs Training Group LLC

Downloaded

Jamf Connect Login
⚠ 1 setting

7. Click Install



Are you sure you want to install this device profile?

Jamf Connect Login
HCS Unsigned

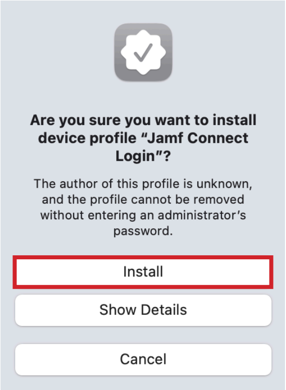
Description	Jamf Connect Login
Received	Nov 15, 2022 at 3:57 PM
Settings	com.jamf.connect.login

Details

com.jamf.connect.login

Description	Jamf Connect Login
OIDCProvider	GoogleID
DenyLocalExcluded	(

8. Click Install

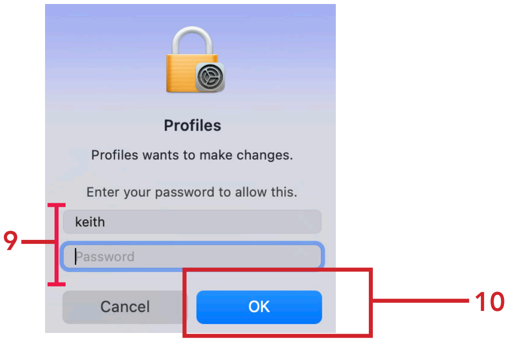


Are you sure you want to install device profile "Jamf Connect Login"?

The author of this profile is unknown, and the profile cannot be removed without entering an administrator's password.

9. Enter your administrative credentials.

10. Click OK.



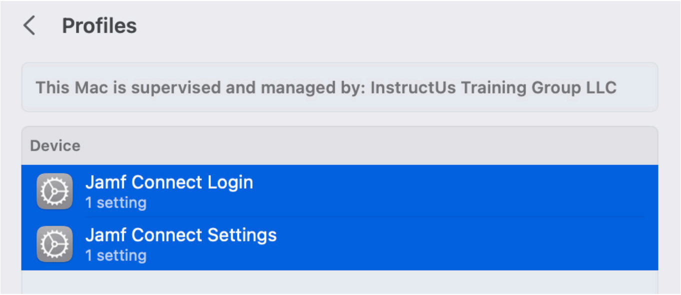
Profiles

Profiles wants to make changes.

Enter your password to allow this.

keith

11. Follow steps 1-10 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.



Profiles

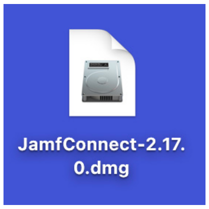
This Mac is supervised and managed by: InstructUs Training Group LLC

Device

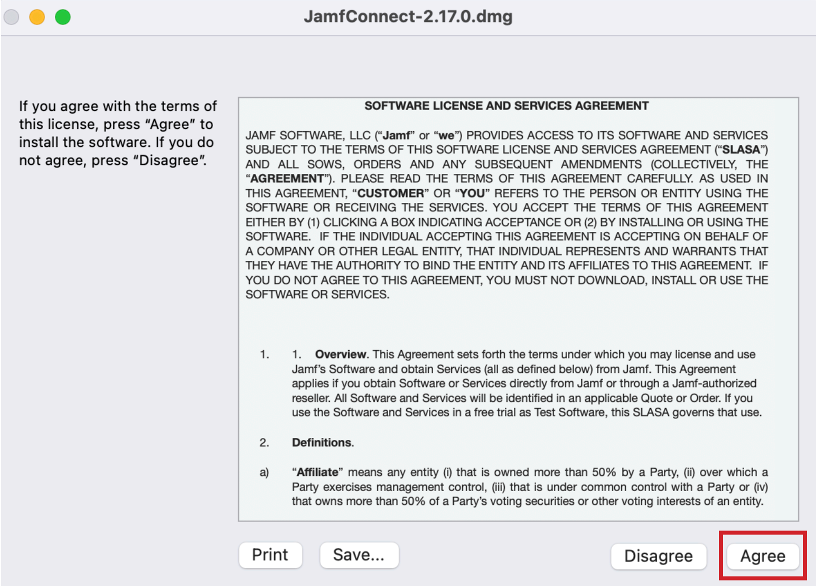
Jamf Connect Login
1 setting

Jamf Connect Settings
1 setting

12. Open the Jamf Connect-2.17.0.dmg.



13. Click Agree.



If you agree with the terms of this license, press “Agree” to install the software. If you do not agree, press “Disagree”.

SOFTWARE LICENSE AND SERVICES AGREEMENT

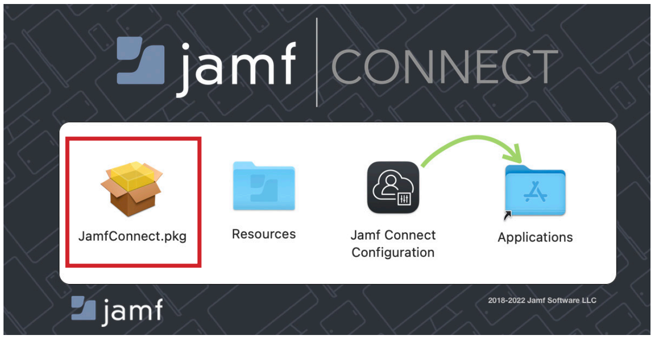
JAMF SOFTWARE, LLC (“**Jamf**” or “**we**”) PROVIDES ACCESS TO ITS SOFTWARE AND SERVICES SUBJECT TO THE TERMS OF THIS SOFTWARE LICENSE AND SERVICES AGREEMENT (“**SLASA**”) AND ALL SOWS, ORDERS AND ANY SUBSEQUENT AMENDMENTS (COLLECTIVELY, THE “**AGREEMENT**”). PLEASE READ THE TERMS OF THIS AGREEMENT CAREFULLY. AS USED IN THIS AGREEMENT, “**CUSTOMER**” OR “**YOU**” REFERS TO THE PERSON OR ENTITY USING THE SOFTWARE OR RECEIVING THE SERVICES. YOU ACCEPT THE TERMS OF THIS AGREEMENT EITHER BY (1) CLICKING A BOX INDICATING ACCEPTANCE OR (2) BY INSTALLING OR USING THE SOFTWARE. IF THE INDIVIDUAL ACCEPTING THIS AGREEMENT IS ACCEPTING ON BEHALF OF A COMPANY OR OTHER LEGAL ENTITY, THAT INDIVIDUAL REPRESENTS AND WARRANTS THAT THEY HAVE THE AUTHORITY TO BIND THE ENTITY AND ITS AFFILIATES TO THIS AGREEMENT. IF YOU DO NOT AGREE TO THIS AGREEMENT, YOU MUST NOT DOWNLOAD, INSTALL OR USE THE SOFTWARE OR SERVICES.

1. 1. **Overview**. This Agreement sets forth the terms under which you may license and use Jamf’s Software and obtain Services (all as defined below) from Jamf. This Agreement applies if you obtain Software or Services directly from Jamf or through a Jamf-authorized reseller. All Software and Services will be identified in an applicable Quote or Order. If you use the Software and Services in a free trial as Test Software, this SLASA governs that use.

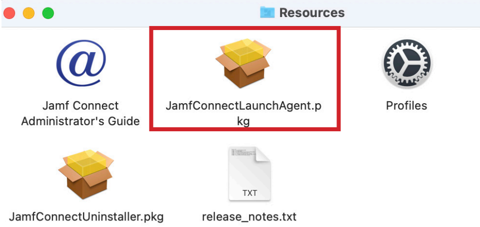
2. **Definitions**.

a) “**Affiliate**” means any entity (i) that is owned more than 50% by a Party, (ii) over which a Party exercises management control, (iii) that is under common control with a Party or (iv) that owns more than 50% of a Party’s voting securities or other voting interests of an entity.

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

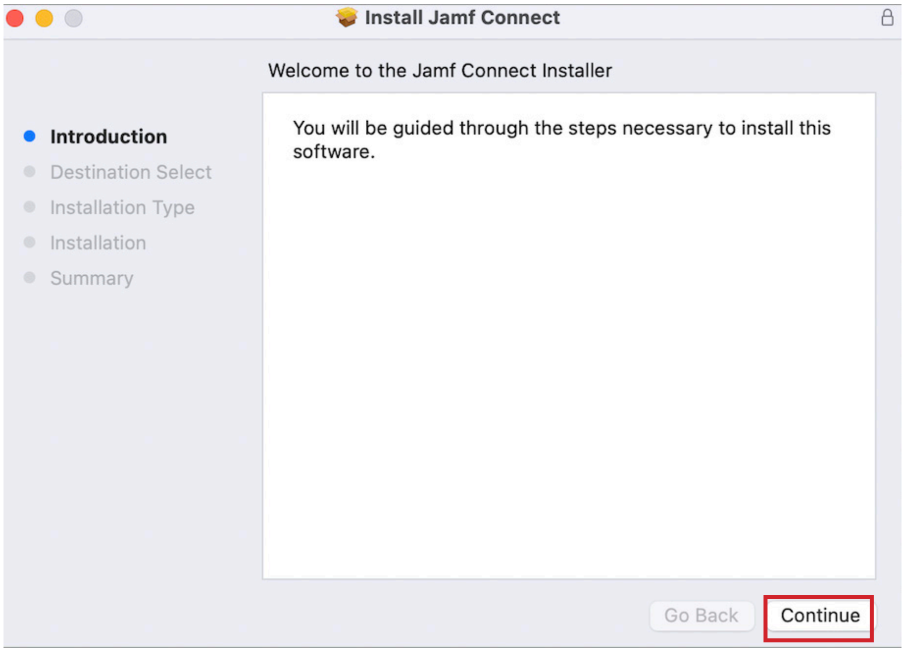


15. Open the Resources folder and drag the JamfConnectLaunnchAgent.pkg to the Desktop. We will need to upload this to the Jamf Pro server later in this section.


Resources
Jamf Connect Administrator's Guide
JamfConnectLaunchAgent.pkg
Profiles
JamfConnectUninstaller.pkg
TXT
release_notes.txt

16. Double-click the JamfConnect.pkg file on the Desktop.

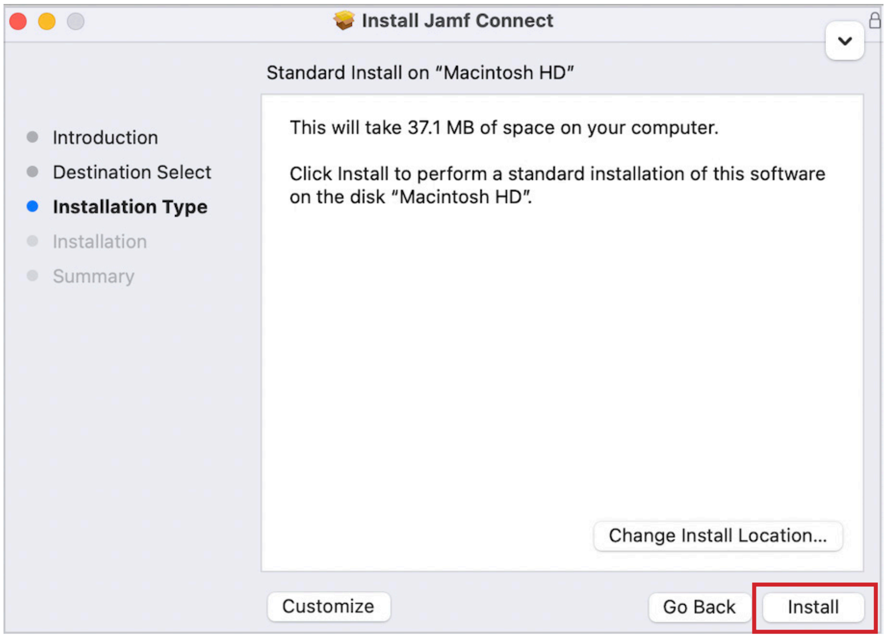
17. Click Continue.



Welcome to the Jamf Connect Installer

You will be guided through the steps necessary to install this software.

18. Click Install.



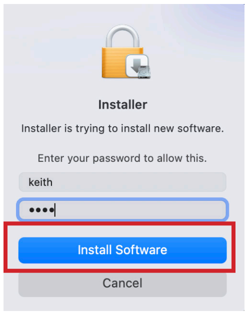
Install Jamf Connect

Standard Install on "Macintosh HD"

This will take 37.1 MB of space on your computer.

Click Install to perform a standard installation of this software on the disk "Macintosh HD".

19. Enter your admin credentials then click Install Software



Installer

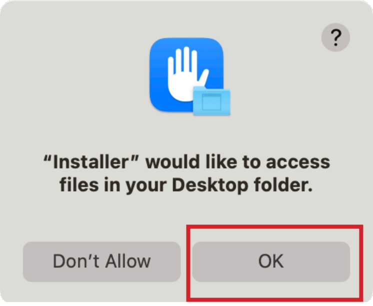
Installer is trying to install new software.

Enter your password to allow this.

keith

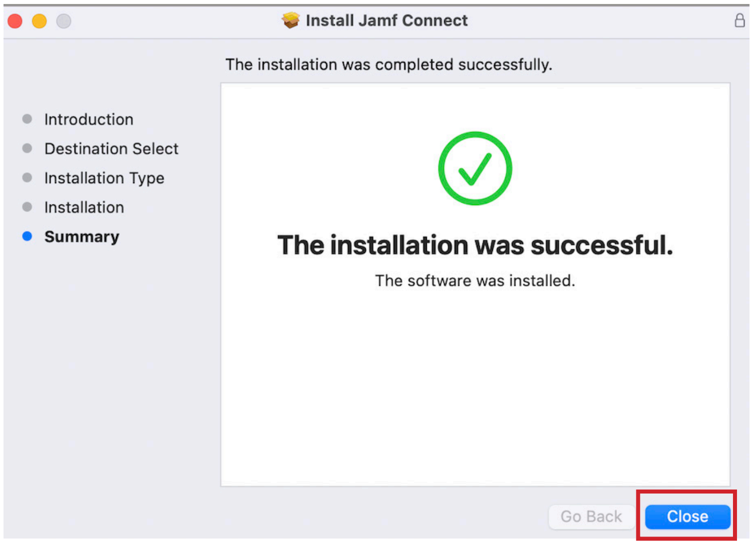
••••

20. Click OK.



"Installer" would like to access files in your Desktop folder.

21. Click Close.



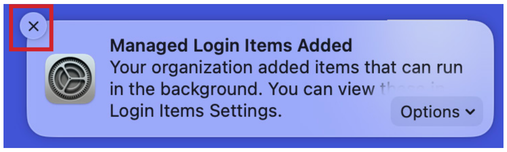
Install Jamf Connect

The installation was completed successfully.

The installation was successful.

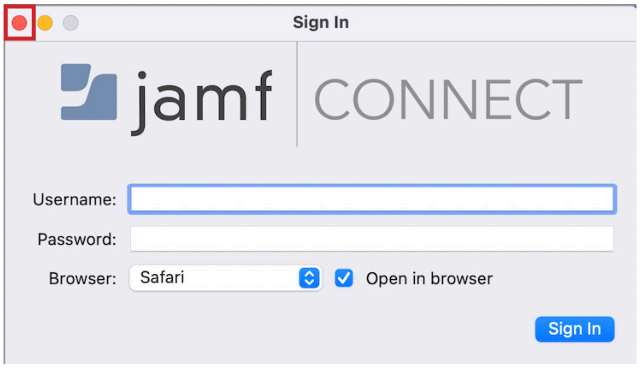
The software was installed.

22. Close the notfication.***



Managed Login Items Added
Your organization added items that can run in the background. You can view them in Login Items Settings.

23. Close the Jamf Connect Sign In window.



Sign In

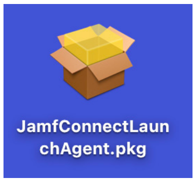
Username:

Password:

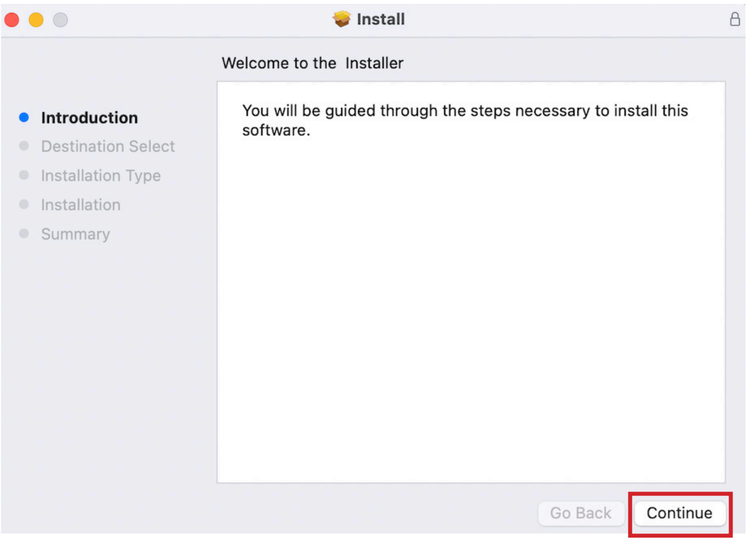
Browser: Safari ☑ Open in browser

***You can learn more about managing Background Tasks with this technical article: https://hcsonline.com/support/white-papers/manage-background-tasks-with-jamf-pro

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



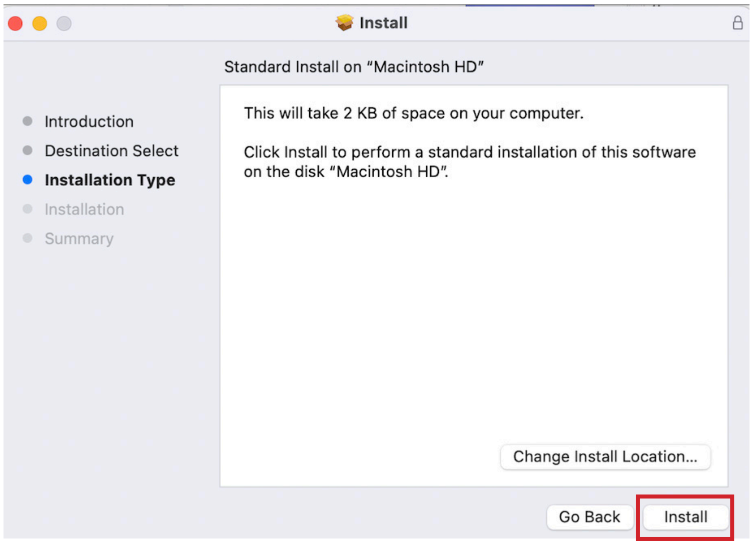
25. Click Continue.



Welcome to the Installer

You will be guided through the steps necessary to install this software.

26. Click Install.

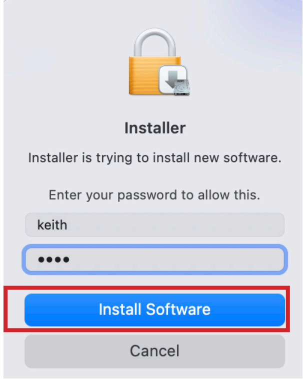


Standard Install on "Macintosh HD"

This will take 2 KB of space on your computer.

Click Install to perform a standard installation of this software on the disk "Macintosh HD".

27. Enter your admin credentials then click Install Software.



Installer

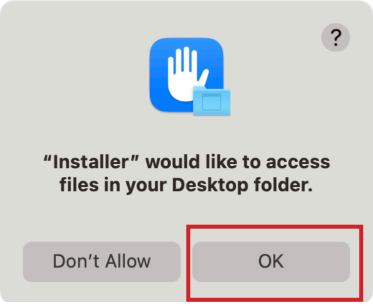
Installer is trying to install new software.

Enter your password to allow this.

keith

••••

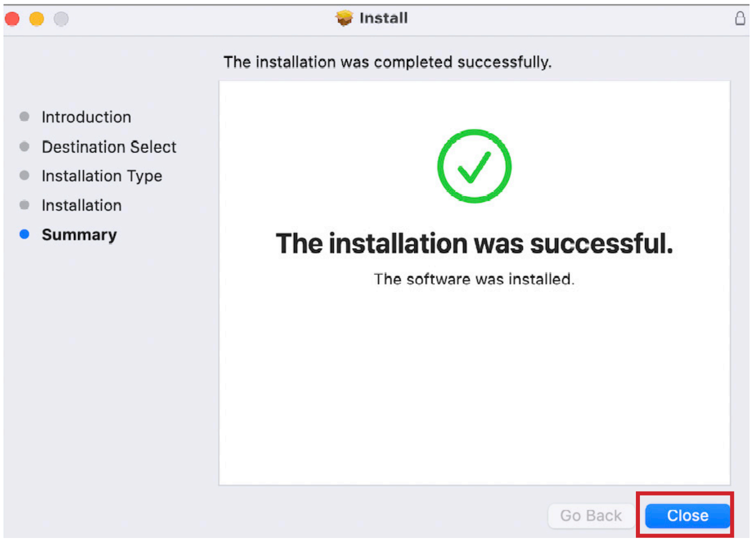
28. Click OK.



“Installer” would like to access files in your Desktop folder.

29. Click Close.

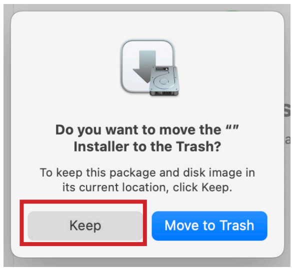
NOTE: After installation, it may ask for you to Keep or Move to Trash. Click Keep. We will need it for later.



The installation was completed successfully.

The installation was successful.

The software was installed.

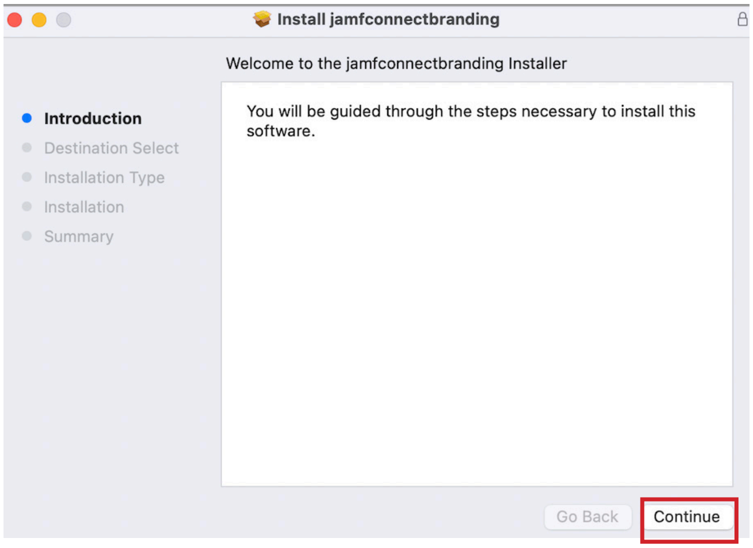


Do you want to move the “” Installer to the Trash?

To keep this package and disk image in its current location, click Keep.

30. 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.

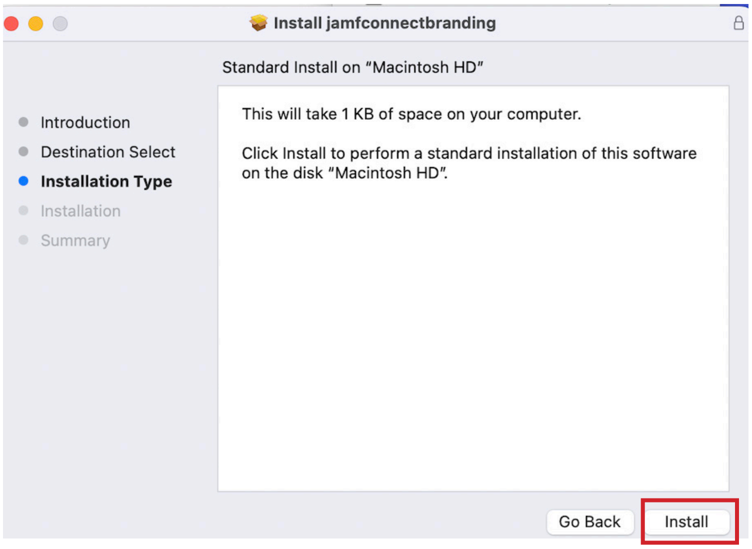
31. Click Continue.



Welcome to the jamfconnectbranding Installer

You will be guided through the steps necessary to install this software.

32. Click Install.

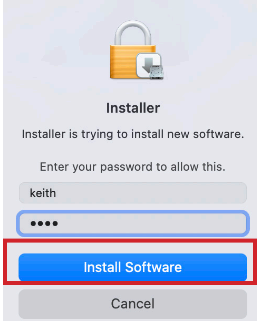


Standard Install on “Macintosh HD”

This will take 1 KB of space on your computer.

Click Install to perform a standard installation of this software on the disk “Macintosh HD”.

33. Enter your admin credentials then click Install Software.



Installer

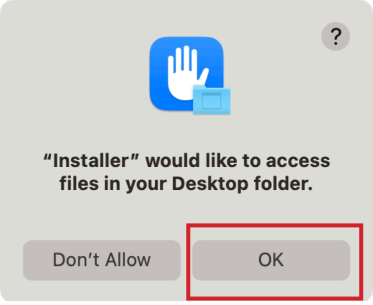
Installer is trying to install new software.

Enter your password to allow this.

keith

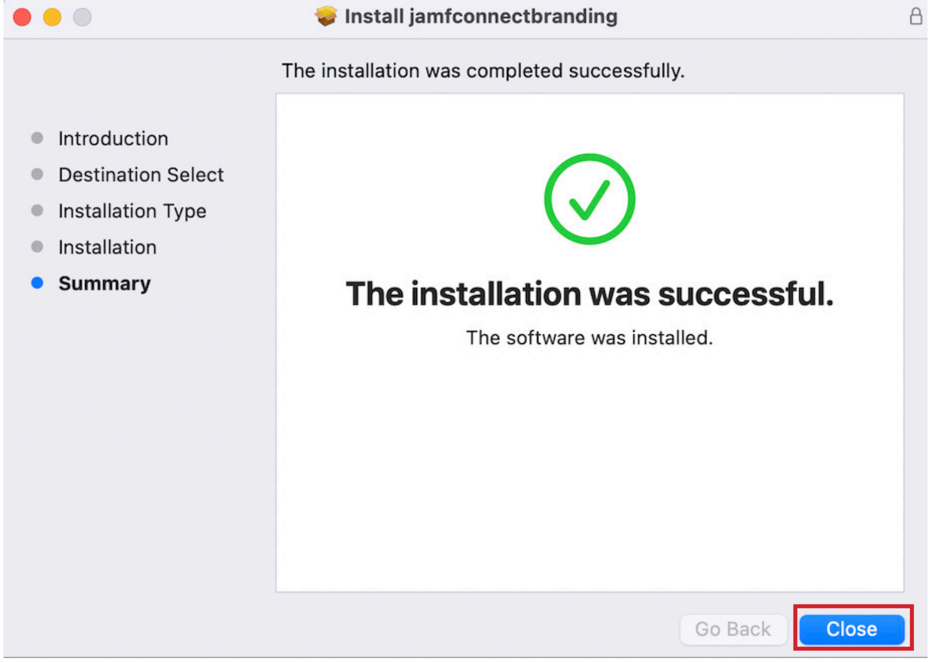
••••

34. Click OK.



“Installer” would like to access files in your Desktop folder.

35. Click Close.



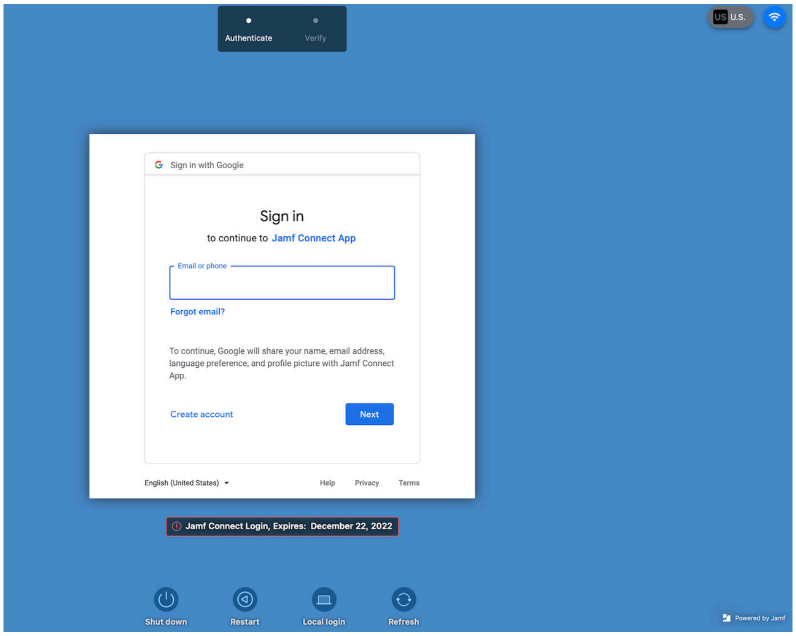
Install jamfconnectbranding

The installation was completed successfully.

The installation was successful.

The software was installed.

36. Logout of your Mac. If all went well, you should be greeted with the Jamf Connect Login Window. Enter your Google username and click Next.
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!



Sign in

to continue to Jamf Connect App

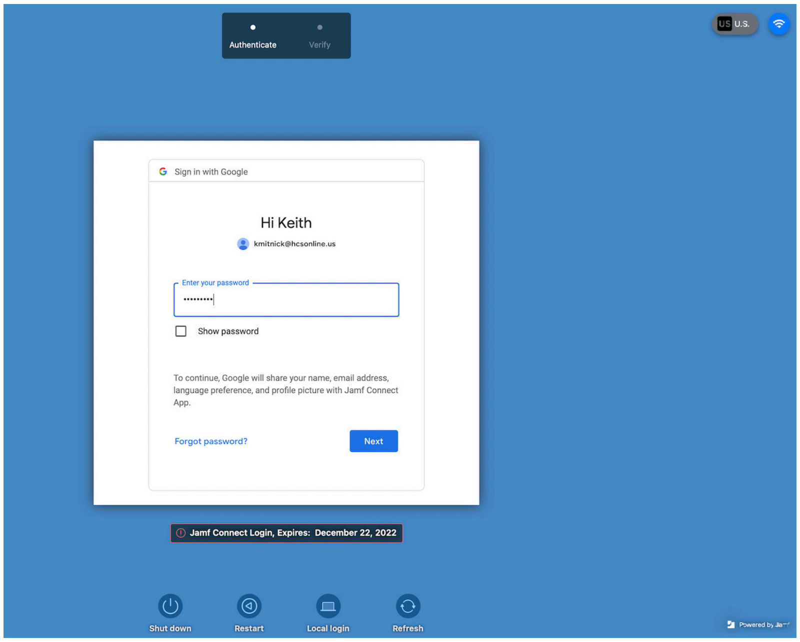
Email or phone

Forgot email?

To continue, Google will share your name, email address, language preference, and profile picture with Jamf Connect App.

Jamf Connect Login, Expires: December 22, 2022

37. Enter your Google password and click Next.



Hi Keith

kmitnick@hcsonline.us

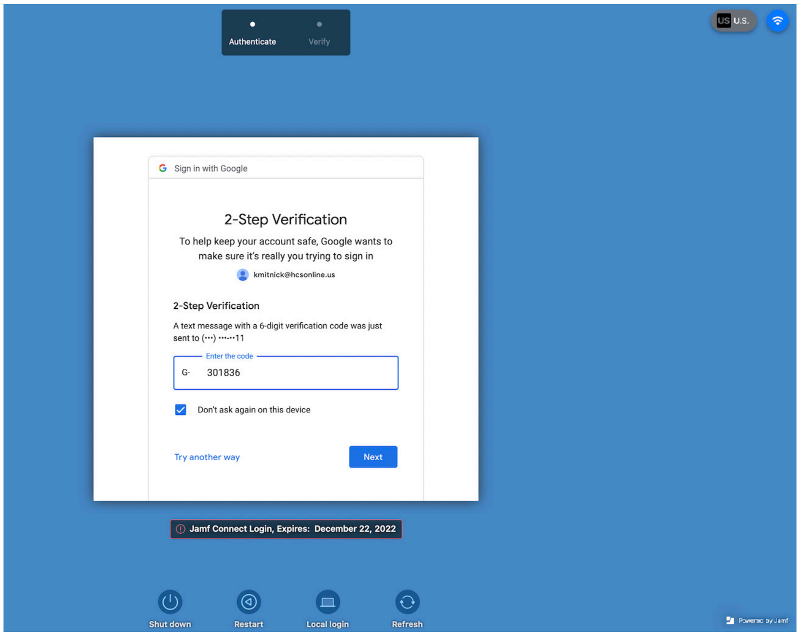
Enter your password: ••••••••••

□ Show password

To continue, Google will share your name, email address, language preference, and profile picture with Jamf Connect App.

Jamf Connect Login, Expires: December 22, 2022

38. If you have MFA enabled, Enter the code that was sent to you by Google and click Next.



Sign in with Google

2-Step Verification

To help keep your account safe, Google wants to make sure it's really you trying to sign in

kmitnick@hcsonline.us

2-Step Verification

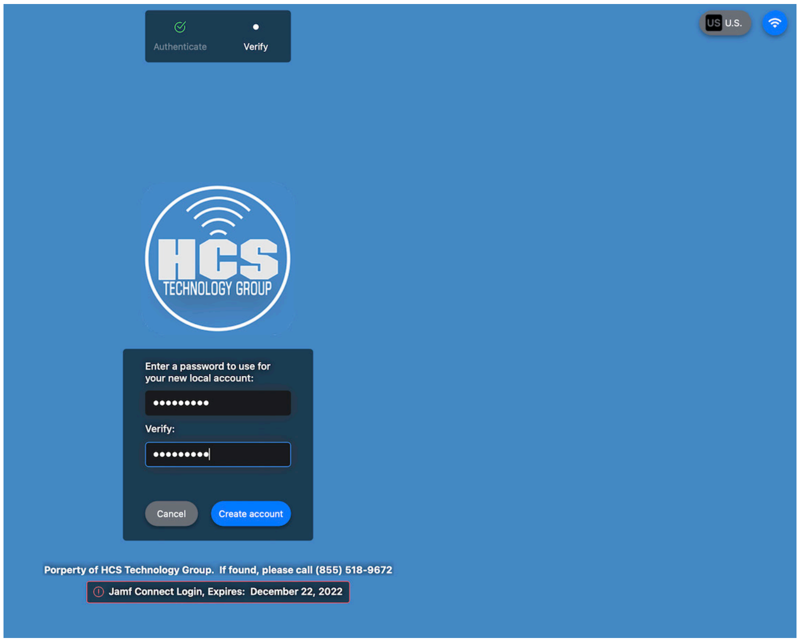
A text message with a 6-digit verification code was just sent to (•••) •••-••11

Enter the code: G- 301836

☑ Don't ask again on this device

Jamf Connect Login, Expires: December 22, 2022

39. Enter a password to use for your new local account then click Create account. NOTE: We recommend using the same password as your Google account password. Click Create account.



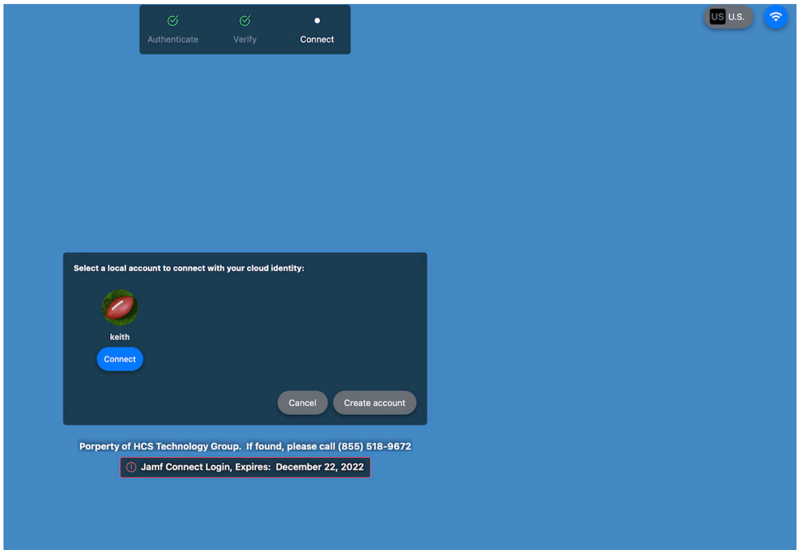
Enter a password to use for your new local account: •••••••••

Verify: •••••••••

Porperty of HCS Technology Group. If found, please call (855) 518-9672

Jamf Connect Login, Expires: December 22, 2022

40. If you have an existing account on your Mac that you want to link to your Google account credentials, select it at the window below. You also have the option to create a new account on the Mac by selecting the Create Account button. This guide will choose the existing keith account.
NOTE: If you select 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 selected "Convert existing mobile accounts to local users " in your Jamf Connect Login settings.

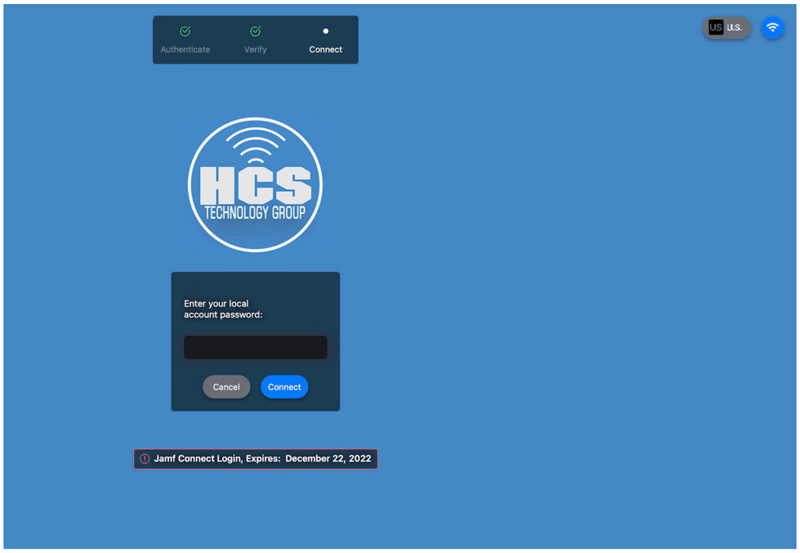


Select a local account to connect with your cloud identity:

Porperty of HCS Technology Group. If found, please call (855) 518-9672

Jamf Connect Login, Expires: December 22, 2022

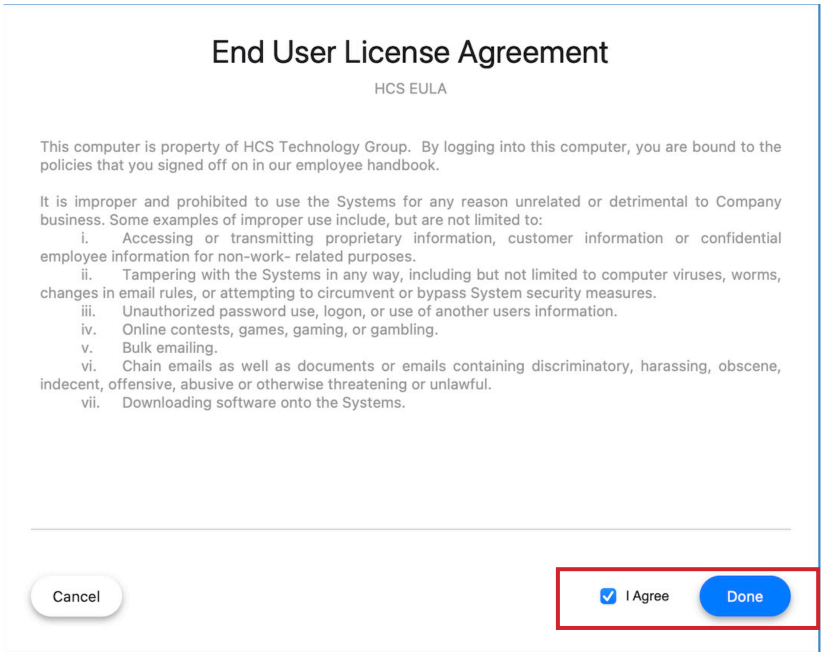
41. You will be prompted for the password of the LOCAL Mac account. In this case, the keith account. Enter your password and click Connect.
NOTE: Do not enter your Google password at this screen. This is your LOCAL Mac account password. Once entered, it will be synced to your Google password and you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



Enter your local account password:

Jamf Connect Login, Expires: December 22, 2022

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



End User License Agreement

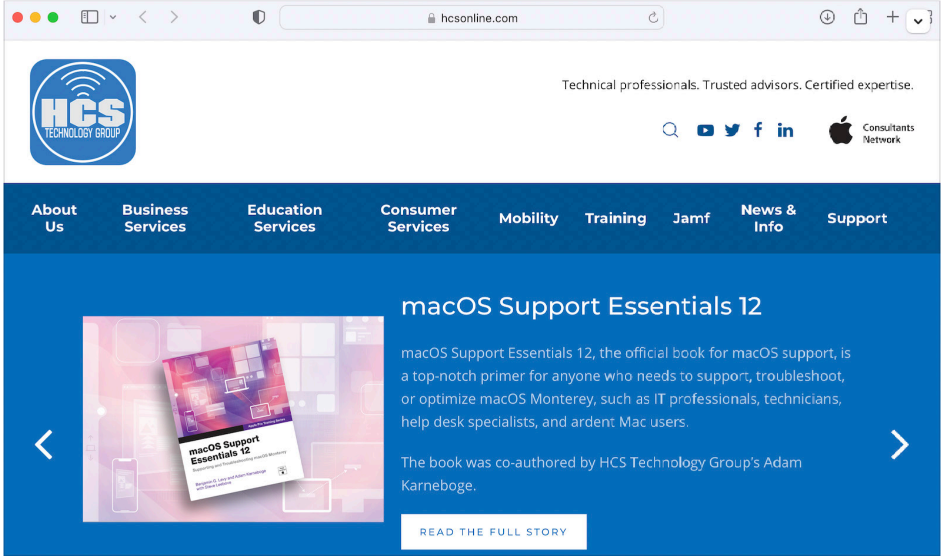
HCS EULA

This computer is property of HCS Technology Group. By logging into this computer, you are bound to the policies that you signed off on in our employee handbook.

It is improper and prohibited to use the Systems for any reason unrelated or detrimental to Company business. Some examples of improper use include, but are not limited to:

i. Accessing or transmitting proprietary information, customer information or confidential employee information for non-work- related purposes.
ii. Tampering with the Systems in any way, including but not limited to computer viruses, worms, changes in email rules, or attempting to circumvent or bypass System security measures.
iii. Unauthorized password use, logon, or use of another users information.
iv. Online contests, games, gaming, or gambling.
v. Bulk emailing.
vi. Chain emails as well as documents or emails containing discriminatory, harassing, obscene, indecent, offensive, abusive or otherwise threatening or unlawful.
vii. Downloading software onto the Systems.

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



Technical professionals. Trusted advisors. Certified expertise.

macOS Support Essentials 12

macOS Support Essentials 12, the official book for macOS support, is a top-notch primer for anyone who needs to support, troubleshoot, or optimize macOS Monterey, such as IT professionals, technicians, help desk specialists, and ardent Mac users.

The book was co-authored by HCS Technology Group's Adam Karneboge.

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

What You'll Need

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

Hardware and Software

Requirements for following along with this section:

- A Mac with macOS 10.15.4 or later.
- Jamf Connect Configuration App 2.17.0.
- Jamf Connect Installer version 2.17.0.
- Jamf Connect Launch Agent Installer.
- jamfconnecbranding.pkg - We created this in section 4.
- Jamf Connect License - Get this from https://id.jamf.com.

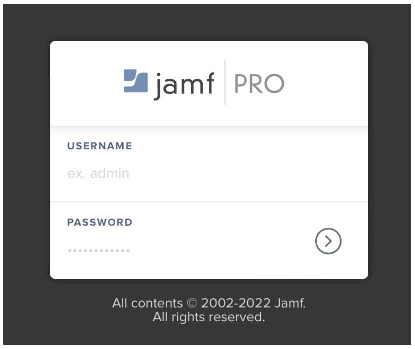
In this section we will upload all the required installation packages for Jamf Connect, create configuration profiles with the settings for Jamf Connect, and create a PreStage enrollment to deploy Jamf Connect via Automated Device Enrollment.

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

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

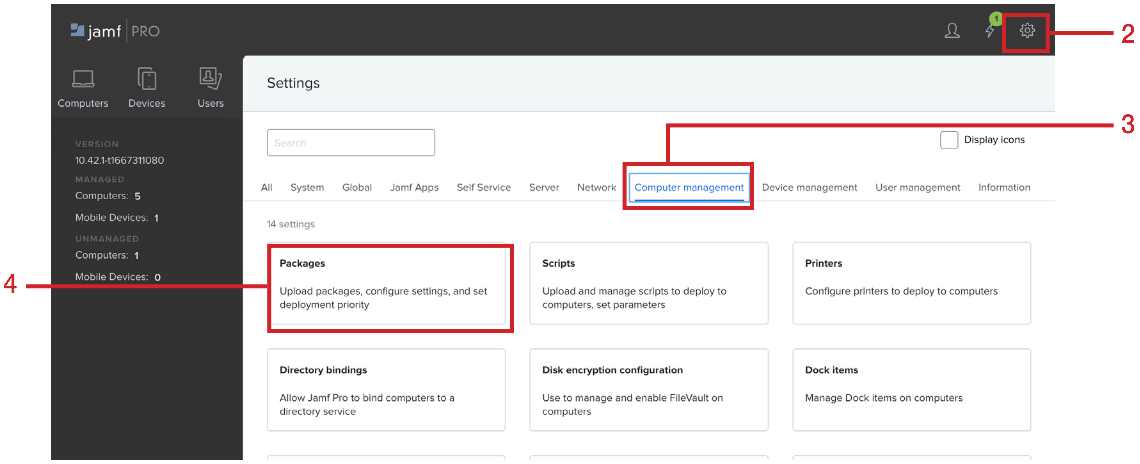
Make sure you have those packages before continuing with this section. You will need to upload them to your Jamf Pro server.

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



All contents © 2002-2022 Jamf.
All rights reserved.

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



VERSION
10.42.1-t1667311080
MANAGED
Computers: 5
Mobile Devices: 1
UNMANAGED
Computers: 1
Mobile Devices: 0

14 settings

Packages
Upload packages, configure settings, and set deployment priority

Scripts
Upload and manage scripts to deploy to computers, set parameters

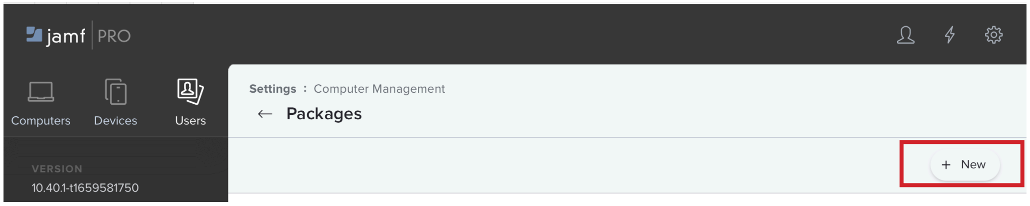
Printers
Configure printers to deploy to computers

Directory bindings
Allow Jamf Pro to bind computers to a directory service

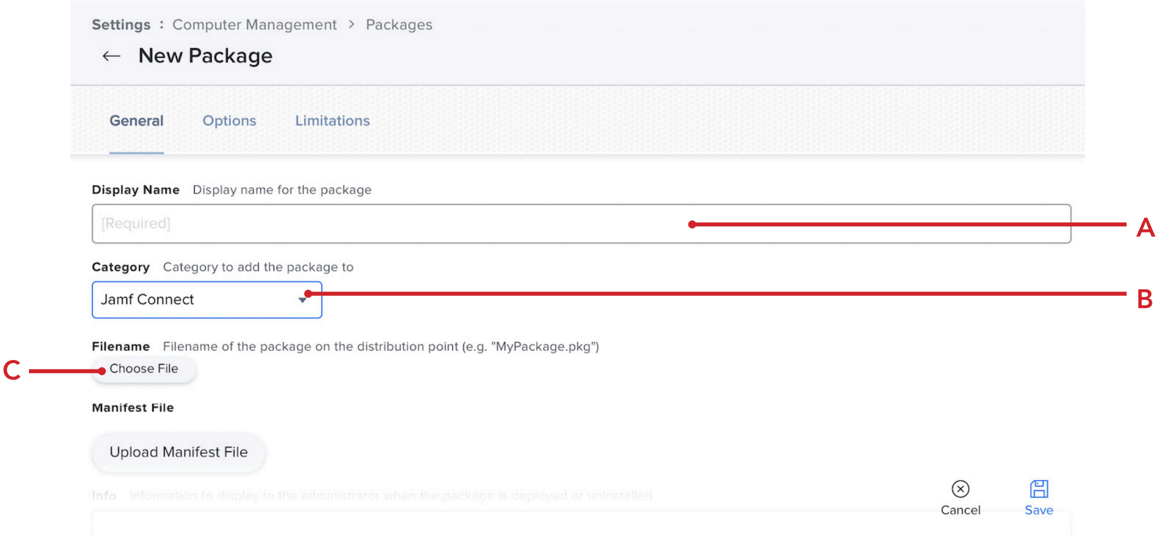
Disk encryption configuration
Use to manage and enable FileVault on computers

Dock items
Manage Dock items on computers

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


Settings : Computer Management > Packages

New Package

Display Name Display name for the package
[Required]

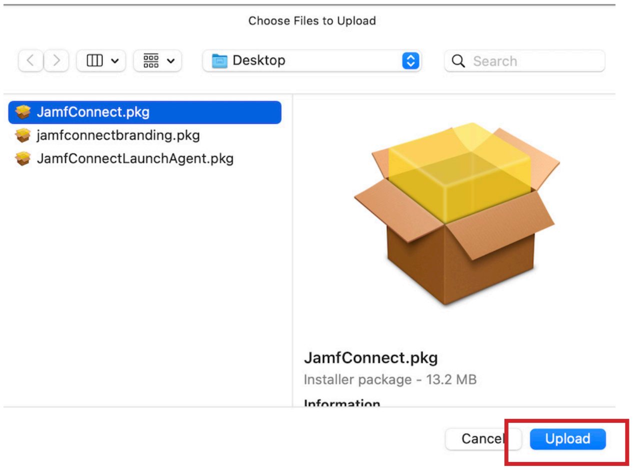
Category Category to add the package to
Jamf Connect

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

Manifest File

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

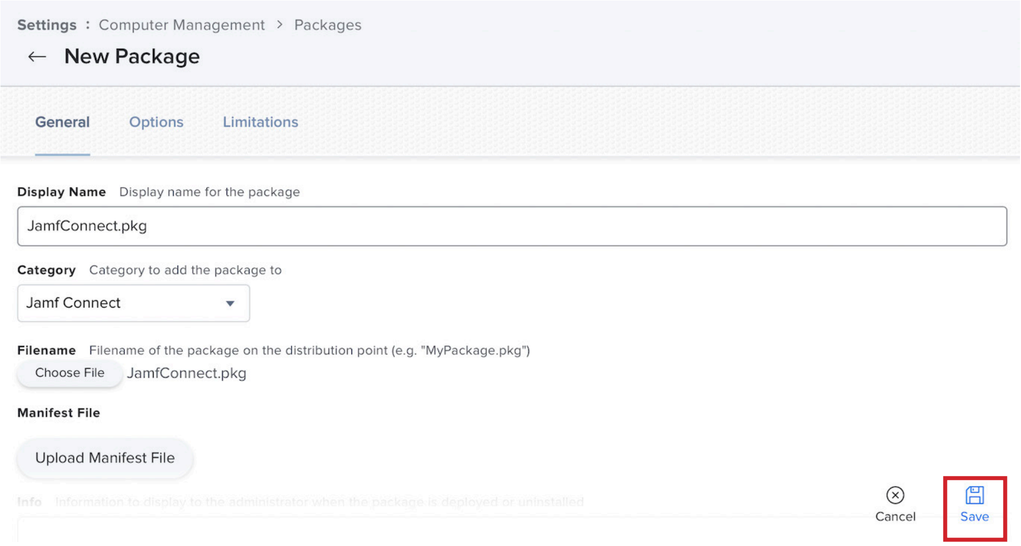
7. Navigate to your Desktop and choose the JamfConnect.pkg then click Upload.


Choose Files to Upload

JamfConnect.pkg
jamfconnectbranding.pkg
JamfConnectLaunchAgent.pkg

JamfConnect.pkg
Installer package - 13.2 MB
Information

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



Settings : Computer Management > Packages

← New Package

General | Options | Limitations

Display Name Display name for the package

JamfConnect.pkg

Category Category to add the package to

Jamf Connect

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

Choose File JamfConnect.pkg

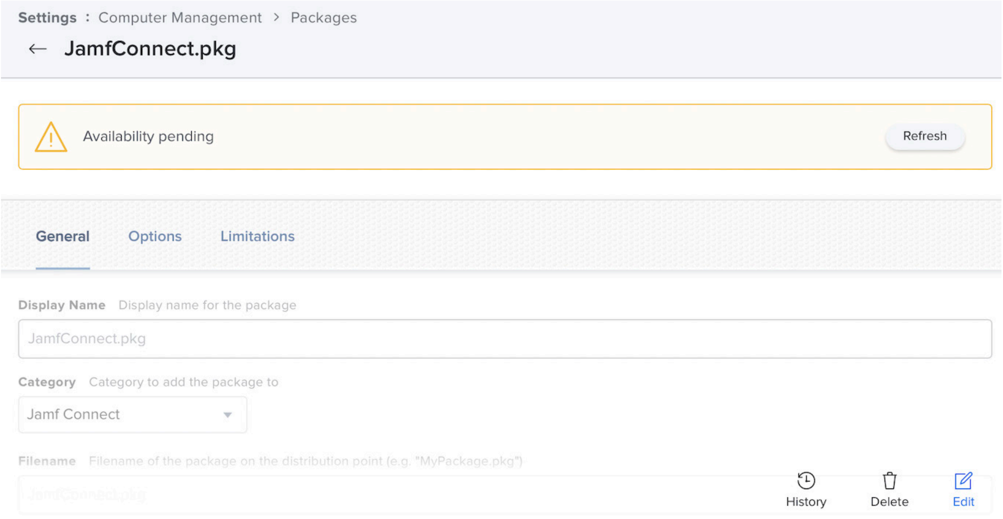
Manifest File

Upload Manifest File

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

Cancel | Save

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



Settings : Computer Management > Packages

← JamfConnect.pkg

Availability pending | Refresh

General | Options | Limitations

Display Name Display name for the package

JamfConnect.pkg

Category Category to add the package to

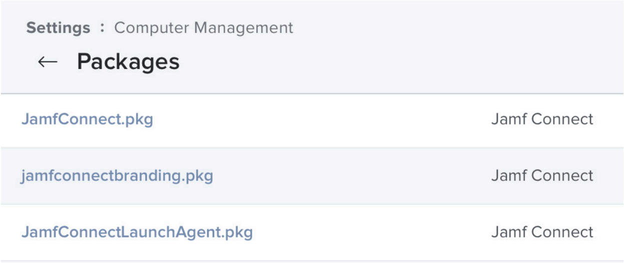
Jamf Connect

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

JamfConnect.pkg

History | Delete | Edit

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

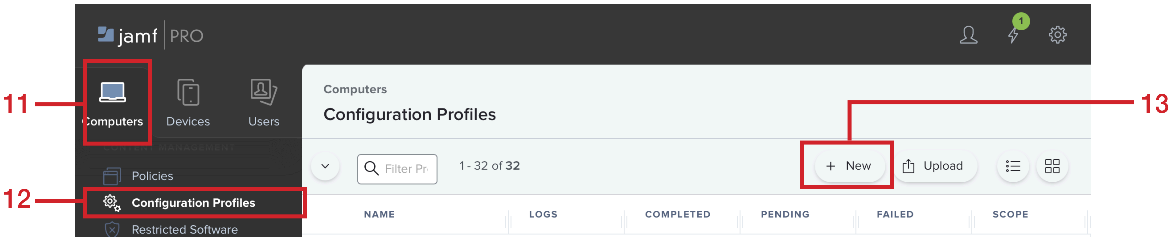


Settings : Computer Management

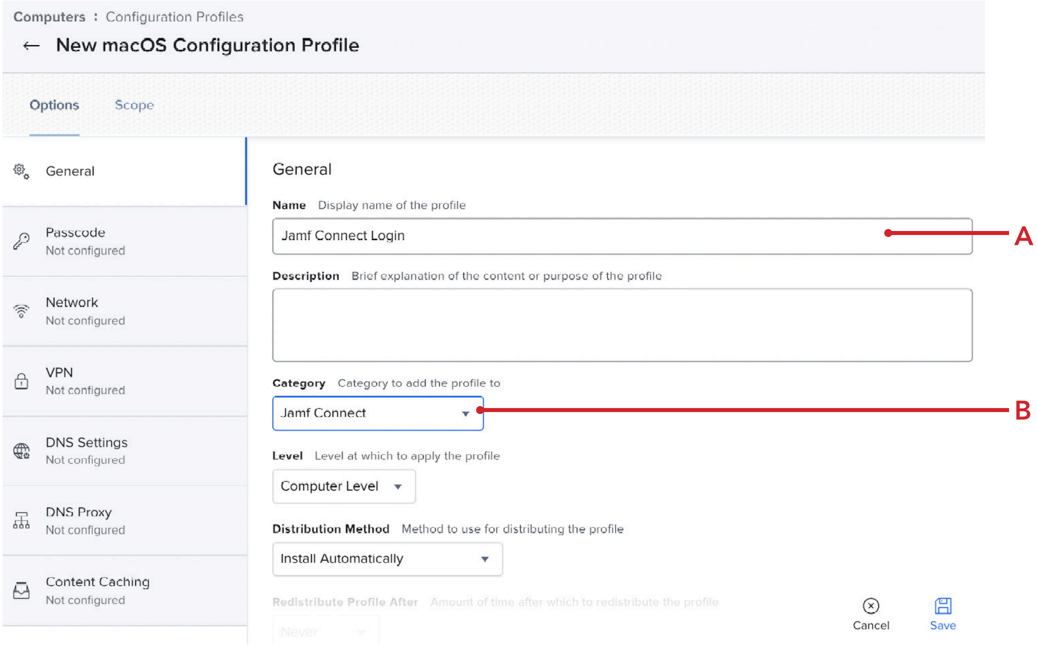
← Packages

JamfConnect.pkg	Jamf Connect
jamfconnectbranding.pkg	Jamf Connect
JamfConnectLaunchAgent.pkg	Jamf Connect

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



General

Name Display name of the profile
Jamf Connect Login

Description Brief explanation of the content or purpose of the profile

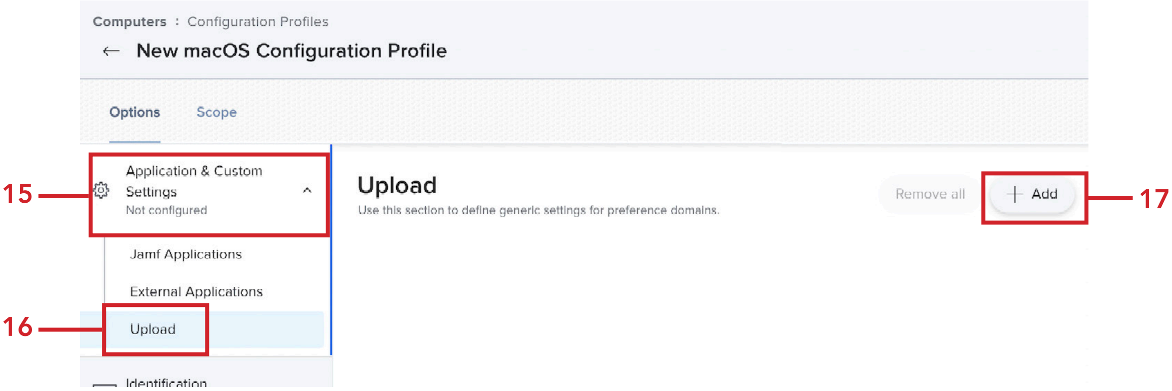
Category Category to add the profile to
Jamf Connect

Level Level at which to apply the profile
Computer Level

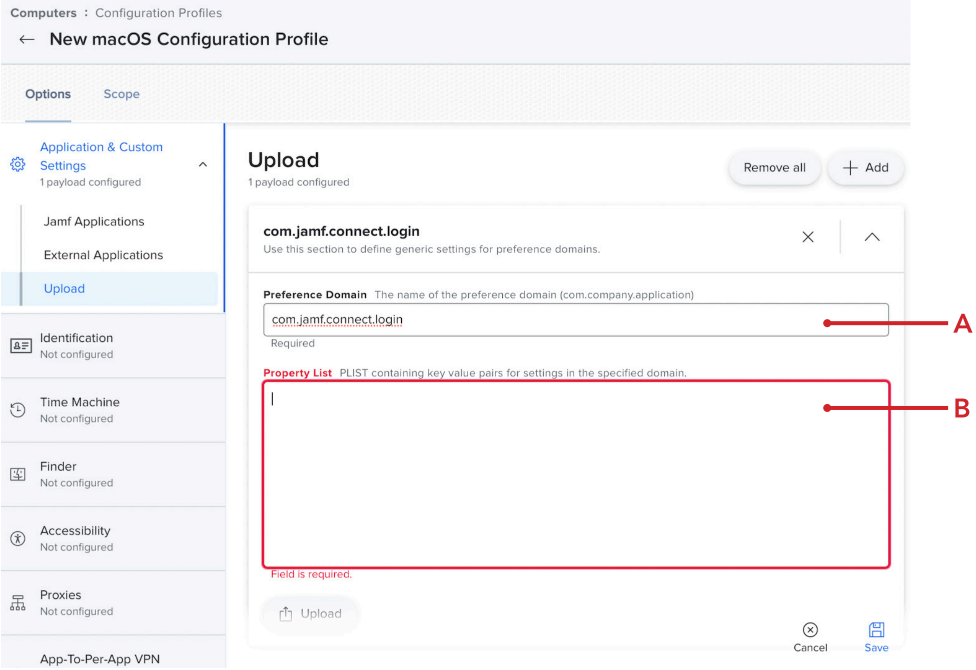
Distribution Method Method to use for distributing the profile
Install Automatically

Redistribute Profile After Amount of time after which to redistribute the profile
Never

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

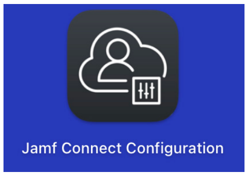

Computers : Configuration Profiles
← New macOS Configuration Profile
Options
Scope
Application & Custom Settings
Not configured
Jamf Applications
External Applications
Upload
Identification
Upload
Use this section to define generic settings for preference domains.
Remove all
+ Add
15
16
17

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.


Computers : Configuration Profiles
← New macOS Configuration Profile
Options
Scope
Application & Custom Settings
1 payload configured
Jamf Applications
External Applications
Upload
Identification
Not configured
Time Machine
Not configured
Finder
Not configured
Accessibility
Not configured
Proxies
Not configured
App-To-Per-App VPN
Upload
1 payload configured
Remove all
+ Add
com.jamf.connect.login
Use this section to define generic settings for preference domains.
Preference Domain The name of the preference domain (com.company.application)
Required
Property List PLIST containing key value pairs for settings in the specified domain.
Field is required.
Upload
Cancel
Save
A
B

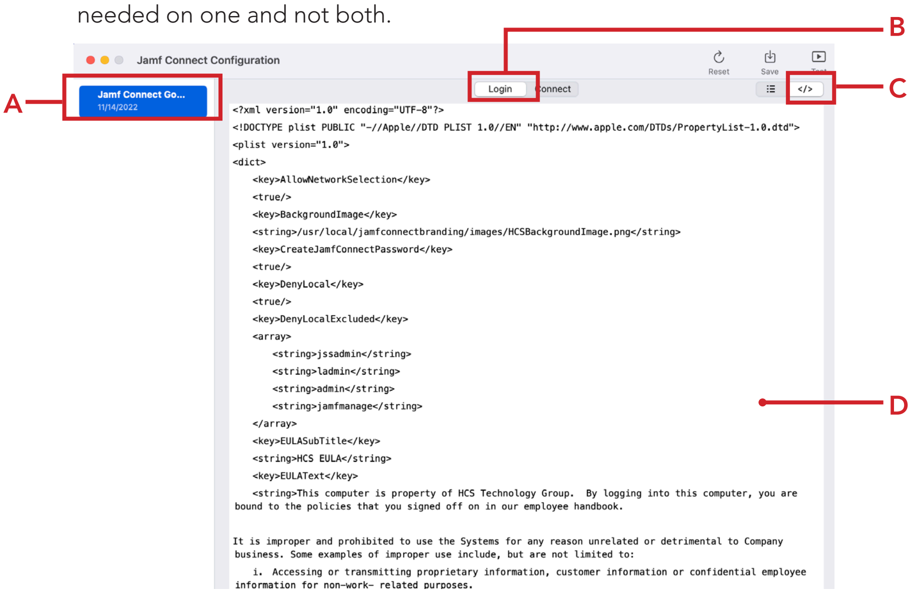
Preference Domain: com.jamf.connect.login

19. Open the Jamf Connect Configuration App.



20. Follow the steps:
    A. Click Jamf Connect Google.
    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. Make life easier when changes are needed on one and not both.

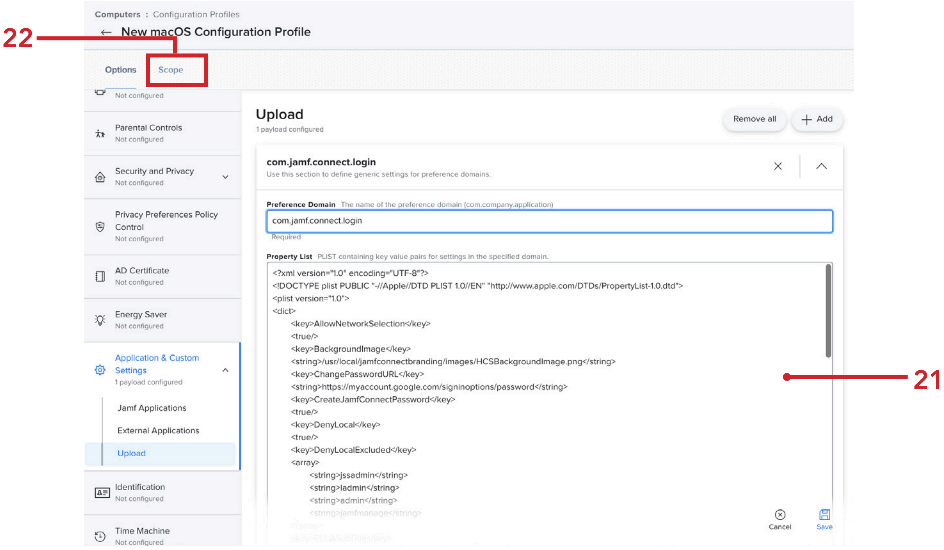


```
<?xml version="1.0" encoding="UTF-8"?>
<!DOCTYPE plist PUBLIC "-//Apple//DTD PLIST 1.0//EN" "http://www.apple.com/DTDs/PropertyList-1.0.dtd">
<plist version="1.0">
<dict>
    <key>AllowNetworkSelection</key>
    <true/>
    <key>BackgroundImage</key>
    <string>/usr/local/jamfconnectbranding/images/HCSBackgroundImage.png</string>
    <key>CreateJamfConnectPassword</key>
    <true/>
    <key>DenyLocal</key>
    <true/>
    <key>DenyLocalExcluded</key>
    <array>
        <string>jssadmin</string>
        <string>ladmin</string>
        <string>admin</string>
        <string>jamfmanage</string>
    </array>
    <key>EULASubTitle</key>
    <string>HCS EULA</string>
    <key>EULAText</key>
    <string>This computer is property of HCS Technology Group.  By logging into this computer, you are
bound to the policies that you signed off on in our employee handbook.


It is improper and prohibited to use the Systems for any reason unrelated or detrimental to Company
business. Some examples of improper use include, but are not limited to:
    i.  Accessing or transmitting proprietary information, customer information or confidential employee
information for non-work- related purposes.
```

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.

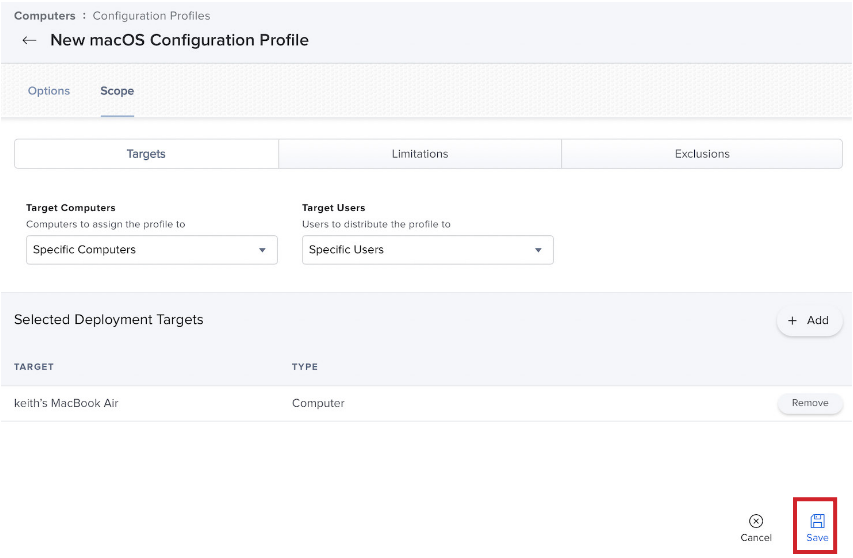
22. Click Scope.



Preference Domain: com.jamf.connect.login

```
<?xml version="1.0" encoding="UTF-8"?>
<!DOCTYPE plist PUBLIC "-//Apple//DTD PLIST 1.0//EN" "http://www.apple.com/DTDs/PropertyList-1.0.dtd">
<plist version="1.0">
<dict>
    <key>AllowNetworkSelection</key>
    <true/>
    <key>BackgroundImage</key>
    <string>/usr/local/jamfconnectbranding/images/HCSBackgroundImage.png</string>
    <key>ChangePasswordURL</key>
    <string>https://myaccount.google.com/signinoptions/password</string>
    <key>CreateJamfConnectPassword</key>
    <true/>
    <key>DenyLocal</key>
    <true/>
    <key>DenyLocalExcluded</key>
    <array>
        <string>jssadmin</string>
        <string>ladmin</string>
        <string>admin</string>
        <string>jamfmanage</string>
    </array>
    <key>EULASubTitle</key>
```

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



Computers : Configuration Profiles
← New macOS Configuration Profile
Options
Scope
Targets
Limitations
Exclusions
+ Add
Remove
Cancel
Save

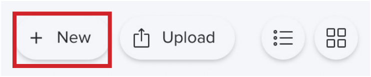
Target Computers Computers to assign the profile to: Specific Computers

Target Users Users to distribute the profile to: Specific Users

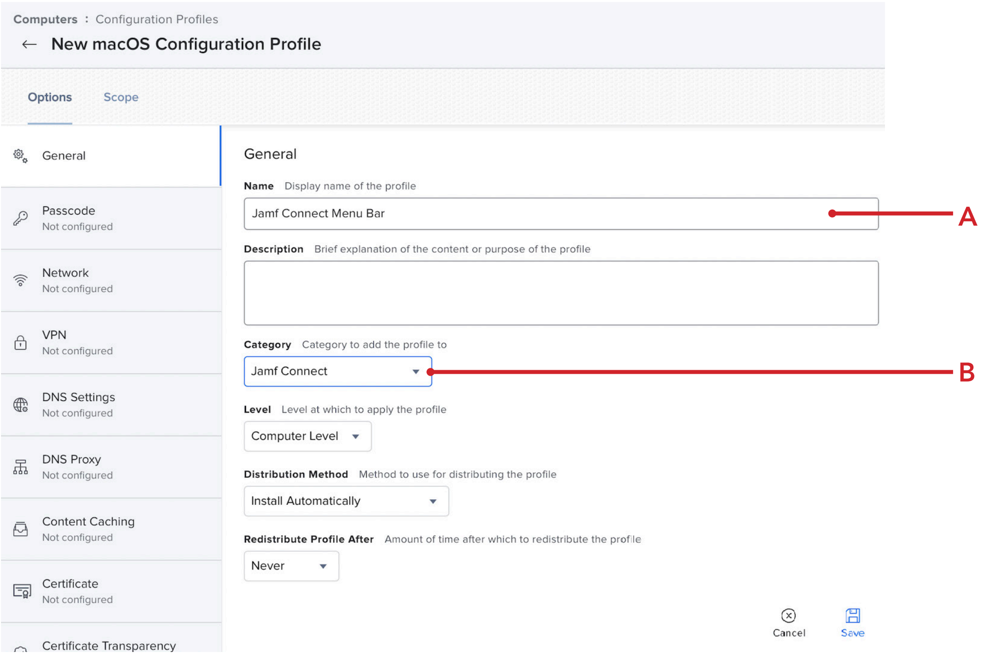
Selected Deployment Targets

TARGET	TYPE
keith's MacBook Air	Computer

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



General

Name Display name of the profile: Jamf Connect Menu Bar

Description Brief explanation of the content or purpose of the profile

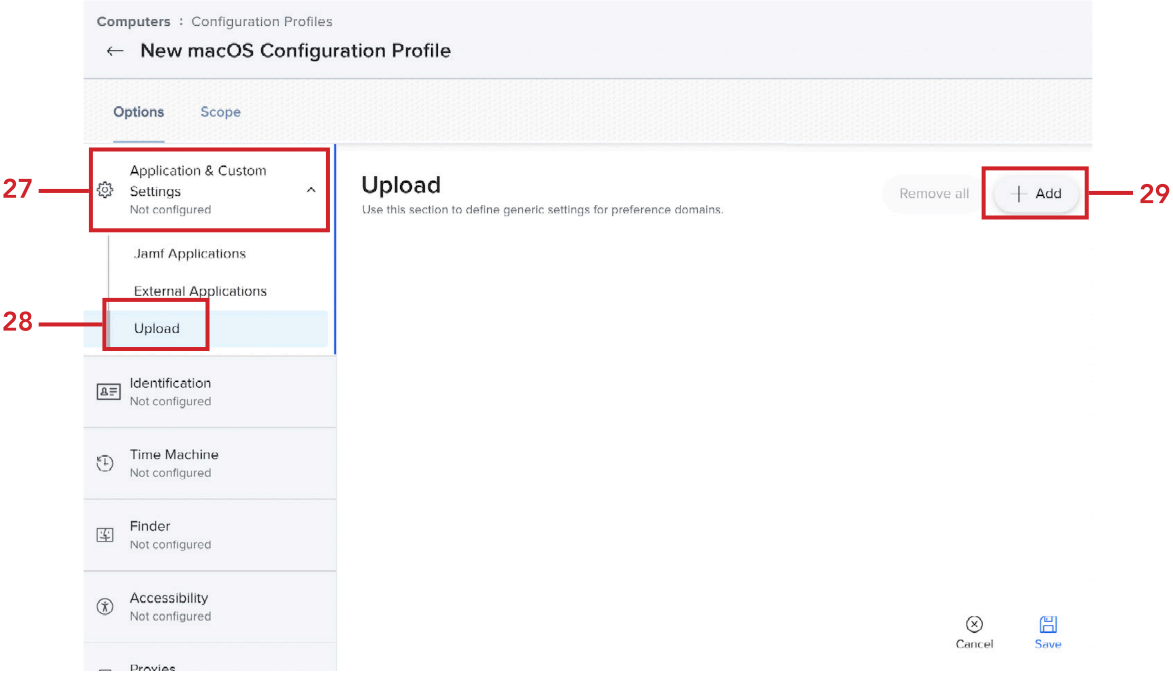
Category Category to add the profile to: Jamf Connect

Level Level at which to apply the profile: Computer Level

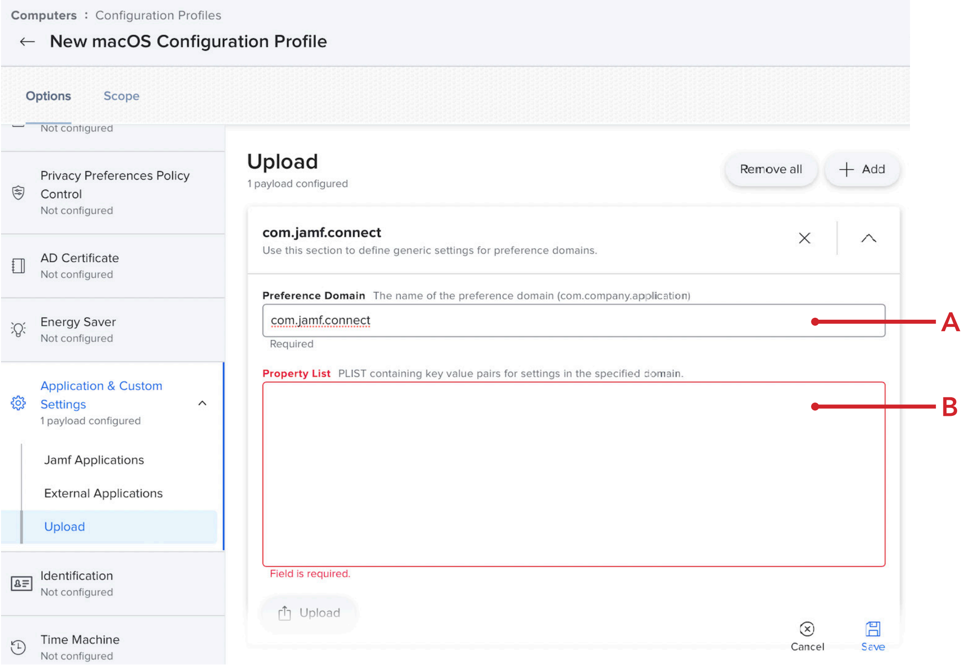
Distribution Method Method to use for distributing the profile: Install Automatically

Redistribute Profile After Amount of time after which to redistribute the profile: Never

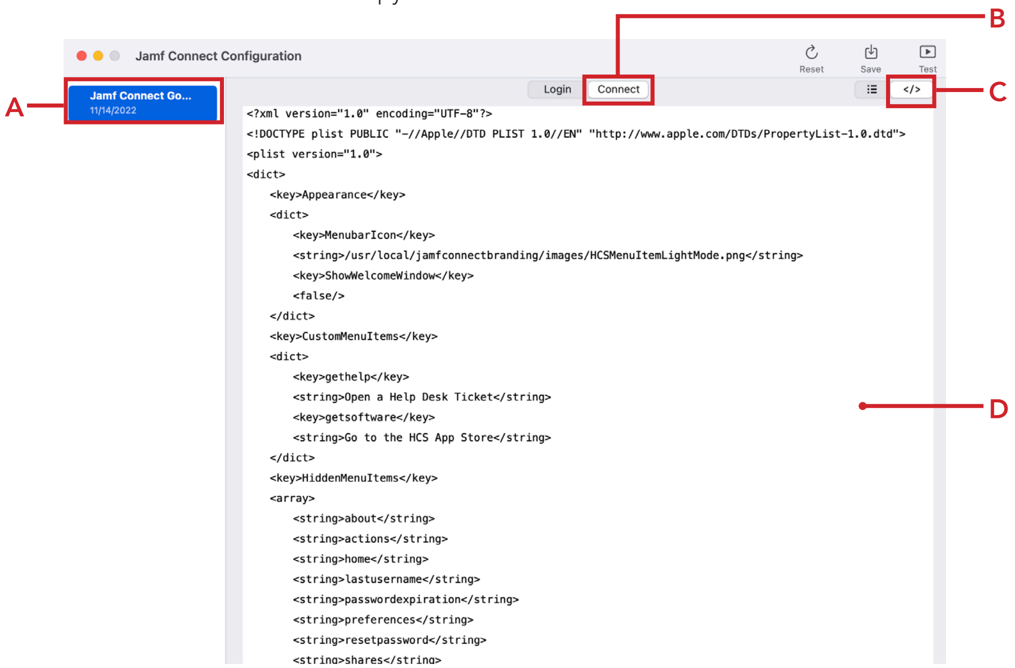
27. Expand the Application & Custom Settings payload.
28. Click Upload.
29. Click Add.



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.


Computers : Configuration Profiles
New macOS Configuration Profile
Options
Scope
Not configured
Privacy Preferences Policy Control
Not configured
AD Certificate
Not configured
Energy Saver
Not configured
Application & Custom Settings
1 payload configured
Jamf Applications
External Applications
Upload
Identification
Not configured
Time Machine
Not configured
Upload
1 payload configured
Remove all
Add
com.jamf.connect
Use this section to define generic settings for preference domains.
Preference Domain The name of the preference domain (com.company.application)
com.jamf.connect
Required
A
Property List PLIST containing key value pairs for settings in the specified domain.
B
Field is required.
Upload
Cancel
Save

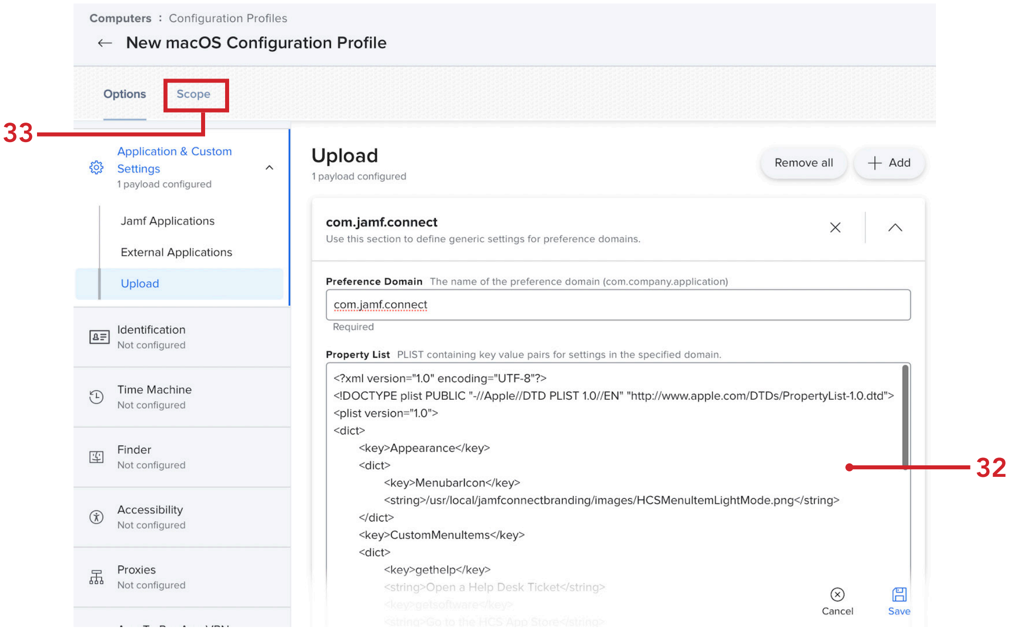
31. Follow the steps:
    A. Click Jamf Connect Google.
    B. Click Connect.
    C. Click the XML tag icon. < / >
    D. Select all the XML and copy it.



```
<?xml version="1.0" encoding="UTF-8"?>
<!DOCTYPE plist PUBLIC "-//Apple//DTD PLIST 1.0//EN" "http://www.apple.com/DTDs/PropertyList-1.0.dtd">
<plist version="1.0">
<dict>
    <key>Appearance</key>
    <dict>
        <key>MenubarIcon</key>
        <string>/usr/local/jamfconnectbranding/images/HCSMenuItemLightMode.png</string>
        <key>ShowWelcomeWindow</key>
        <false/>
    </dict>
    <key>CustomMenuItems</key>
    <dict>
        <key>gethelp</key>
        <string>Open a Help Desk Ticket</string>
        <key>getsoftware</key>
        <string>Go to the HCS App Store</string>
    </dict>
    <key>HiddenMenuItems</key>
    <array>
        <string>about</string>
        <string>actions</string>
        <string>home</string>
        <string>lastusername</string>
        <string>passwordexpiration</string>
        <string>preferences</string>
        <string>resetpassword</string>
        <string>shares</string>
```

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.



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

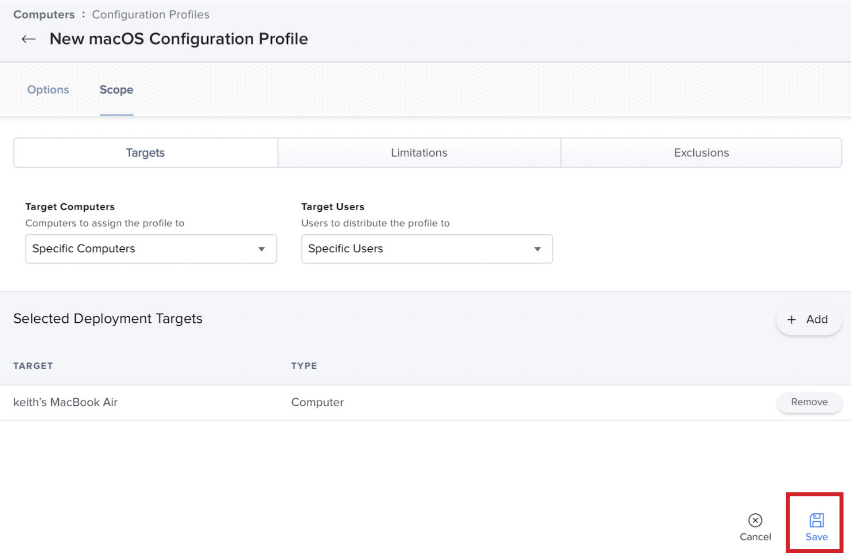
com.jamf.connect

Required

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

```
<?xml version="1.0" encoding="UTF-8"?>
<!DOCTYPE plist PUBLIC "-//Apple//DTD PLIST 1.0//EN" "http://www.apple.com/DTDs/PropertyList-1.0.dtd">
<plist version="1.0">
<dict>
    <key>Appearance</key>
    <dict>
        <key>MenubarIcon</key>
        <string>/usr/local/jamfconnectbranding/images/HCSMenuItemLightMode.png</string>
    </dict>
    <key>CustomMenuItems</key>
    <dict>
        <key>gethelp</key>
        <string>Open a Help Desk Ticket</string>
        <key>getsoftware</key>
        <string>Go to the HCS App Store</string>
```

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



Computers : Configuration Profiles

New macOS Configuration Profile

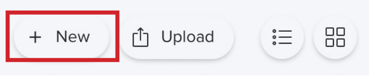
Target Computers
Computers to assign the profile to
Specific Computers

Target Users
Users to distribute the profile to
Specific Users

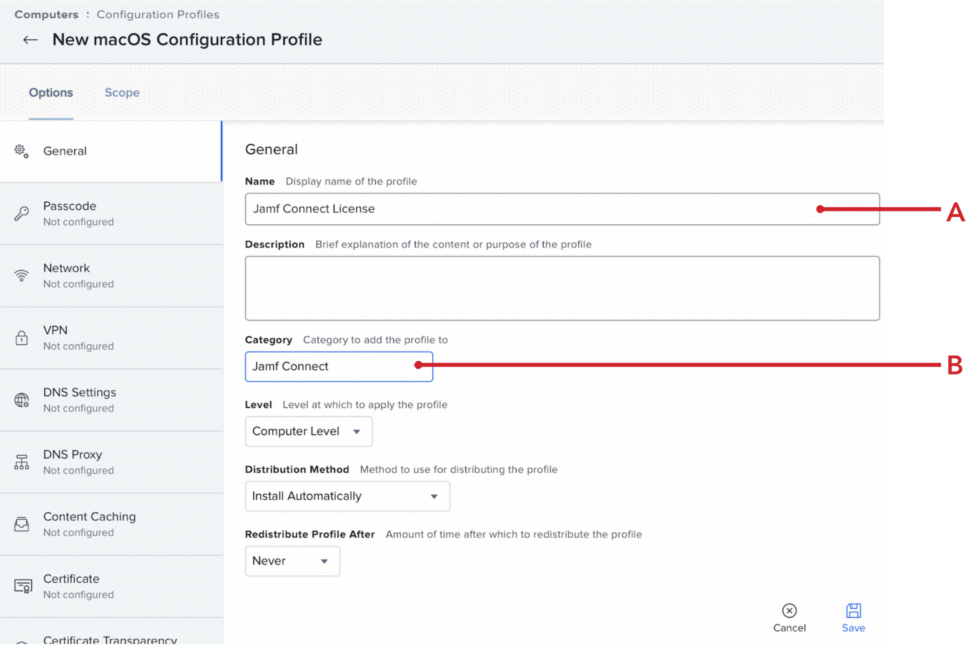
Selected Deployment Targets

TARGET	TYPE
keith's MacBook Air	Computer

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



Computers : Configuration Profiles

New macOS Configuration Profile

General

Name Display name of the profile
Jamf Connect License

Description Brief explanation of the content or purpose of the profile

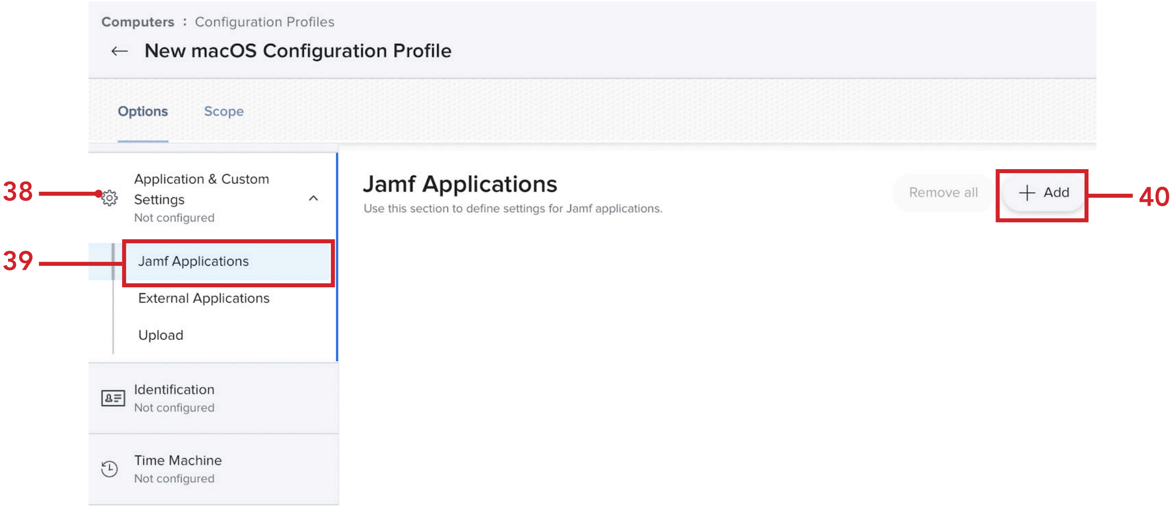
Category Category to add the profile to
Jamf Connect

Level Level at which to apply the profile
Computer Level

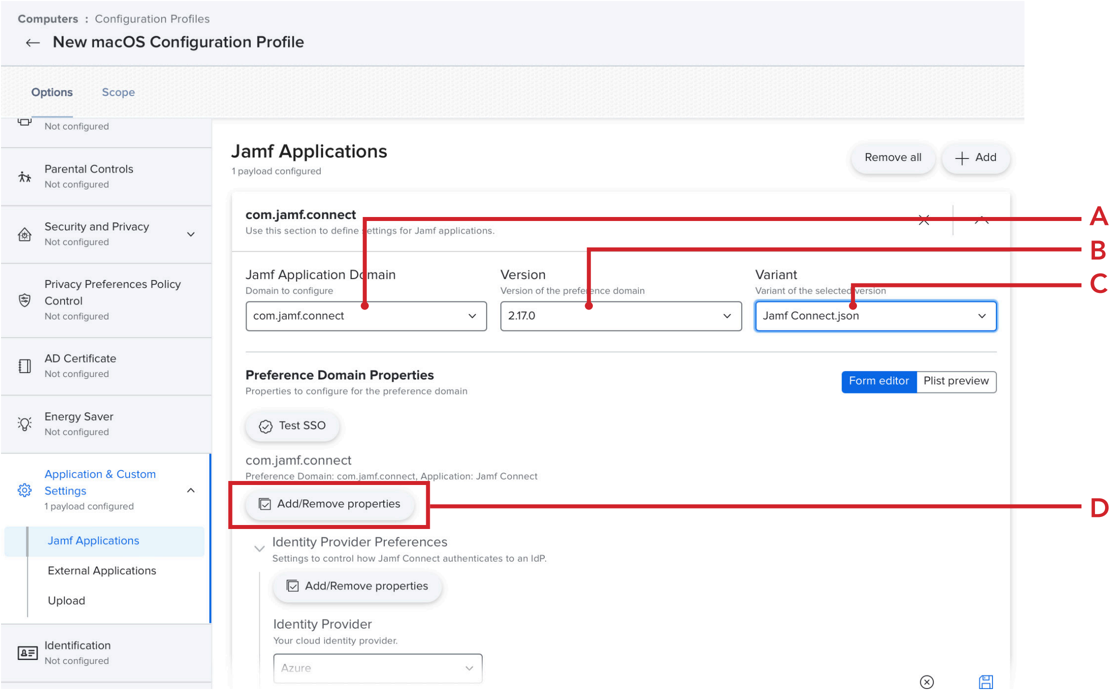
Distribution Method Method to use for distributing the profile
Install Automatically

Redistribute Profile After Amount of time after which to redistribute the profile
Never

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: 2.17.0 (or the latest version available)
    C. Variant: Jamf Connect json
    D. Click the first Add/Remove properties button



Jamf Application Domain
Domain to configure
com.jamf.connect

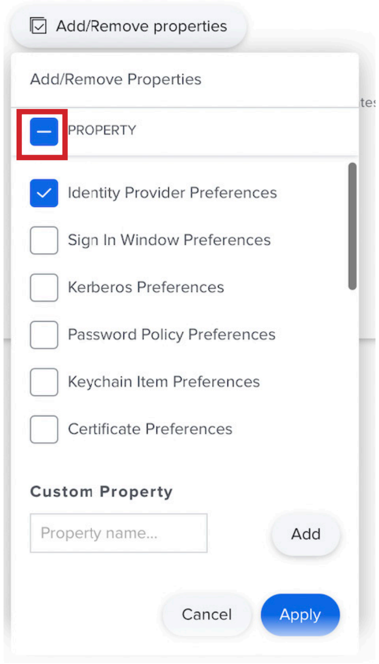
Version
Version of the preference domain
2.17.0

Variant
Variant of the selected version
Jamf Connect.json

com.jamf.connect
Preference Domain: com.jamf.connect, Application: Jamf Connect

Identity Provider
Your cloud identity provider.
Azure

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



Add/Remove properties

Add/Remove Properties

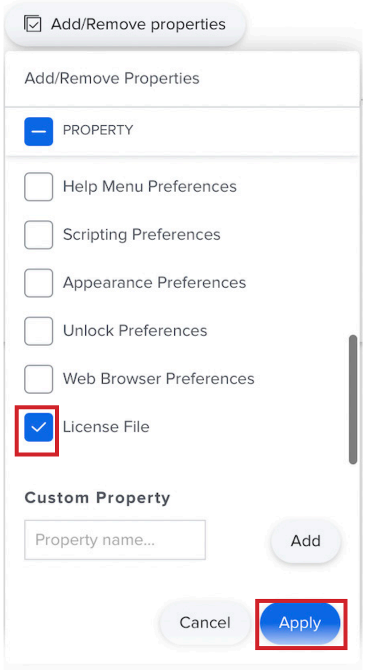
▣ PROPERTY

☑ Identity Provider Preferences
□ Sign In Window Preferences
□ Kerberos Preferences
□ Password Policy Preferences
□ Keychain Item Preferences
□ Certificate Preferences

Custom Property

Property name...

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



Add/Remove properties

Add/Remove Properties

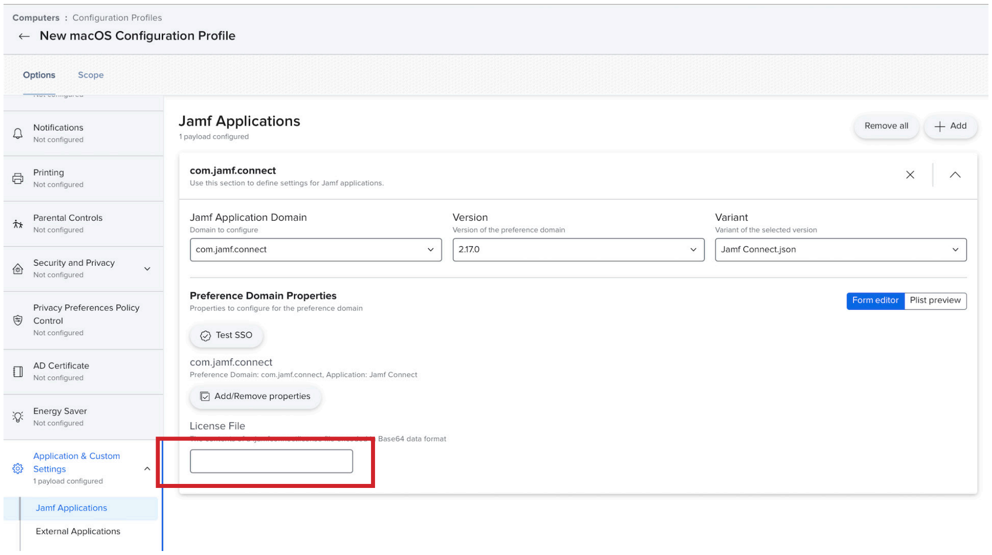
▣ PROPERTY

□ Help Menu Preferences
□ Scripting Preferences
□ Appearance Preferences
□ Unlock Preferences
□ Web Browser Preferences
☑ License File

Custom Property

Property name...

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



Computers : Configuration Profiles

← New macOS Configuration Profile

Jamf Applications
1 payload configured

com.jamf.connect
Use this section to define settings for Jamf applications.

Jamf Application Domain
Domain to configure
com.jamf.connect

Version
Version of the preference domain
2.17.0

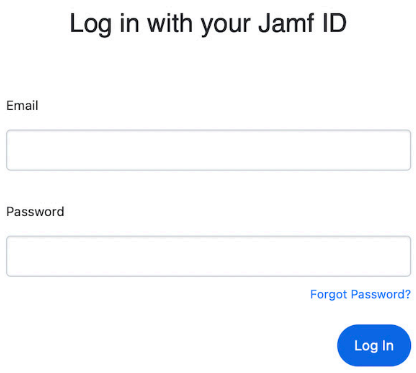
Variant
Variant of the selected version
Jamf Connect.json

Preference Domain Properties
Properties to configure for the preference domain

com.jamf.connect
Preference Domain: com.jamf.connect, Application: Jamf Connect

License File
Base64 data format

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.

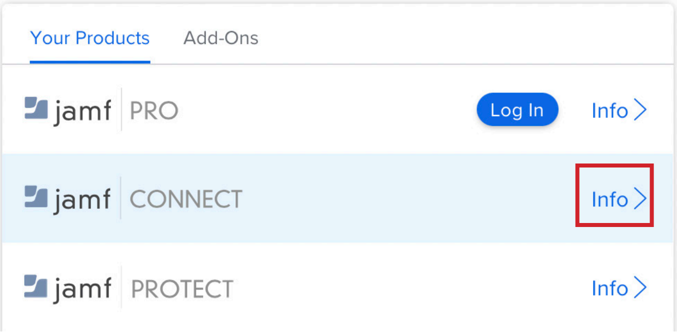


Log in with your Jamf ID

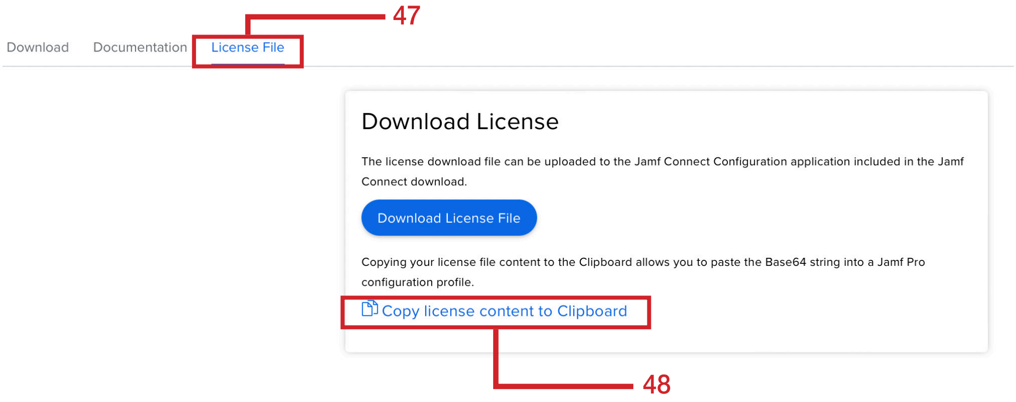
Email

Password

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



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

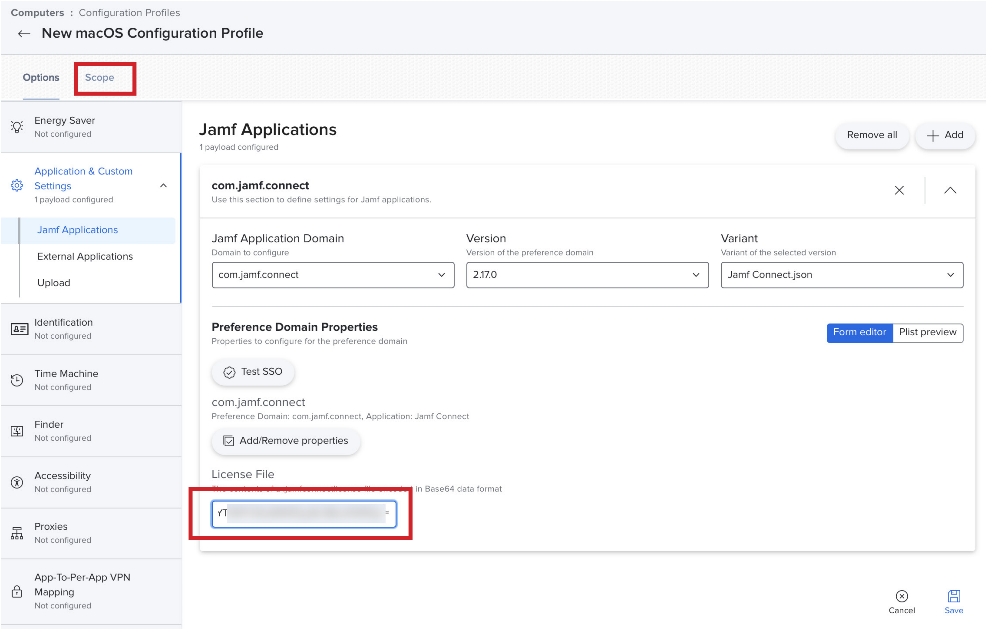


Download License

The license download file can be uploaded to the Jamf Connect Configuration application included in the Jamf Connect download.

Copying your license file content to the Clipboard allows you to paste the Base64 string into a Jamf Pro configuration profile.

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.
50. Click Scope.



Computers : Configuration Profiles

← New macOS Configuration Profile

Jamf Applications

1 payload configured

com.jamf.connect

Use this section to define settings for Jamf applications.

Jamf Application Domain: com.jamf.connect (Domain to configure)

Version: 2.17.0 (Version of the preference domain)

Variant: Jamf Connect.json (Variant of the selected version)

Preference Domain Properties

Properties to configure for the preference domain

com.jamf.connect

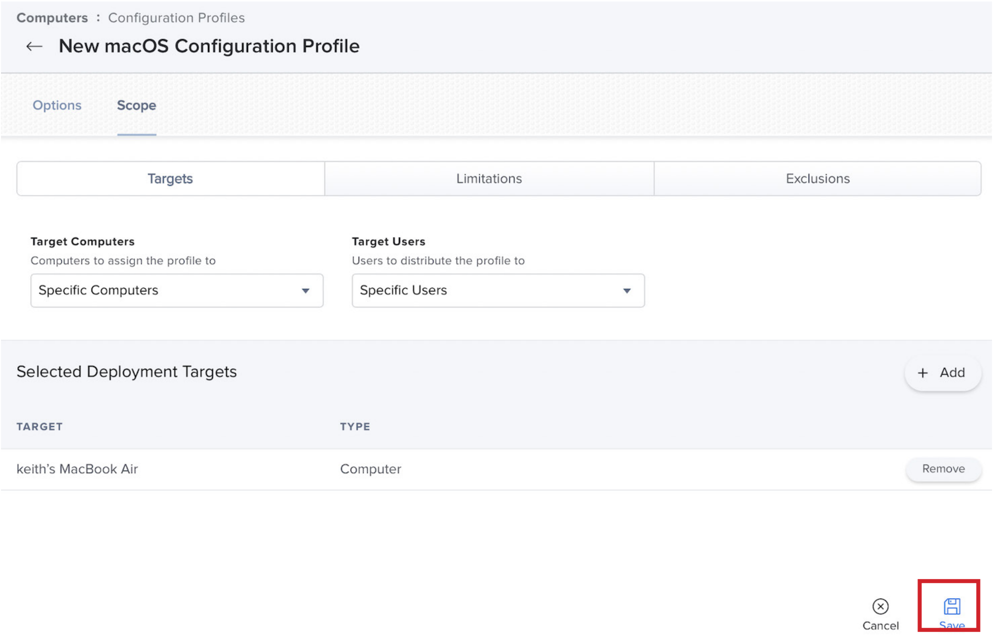
Preference Domain: com.jamf.connect, Application: Jamf Connect

License File

The contents of a jamfconnect license file encoded in Base64 data format

YT[redacted]=

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



Computers : Configuration Profiles

← New macOS Configuration Profile

Target Computers

Computers to assign the profile to

Specific Computers

Target Users

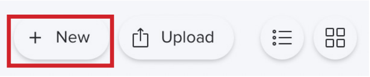
Users to distribute the profile to

Specific Users

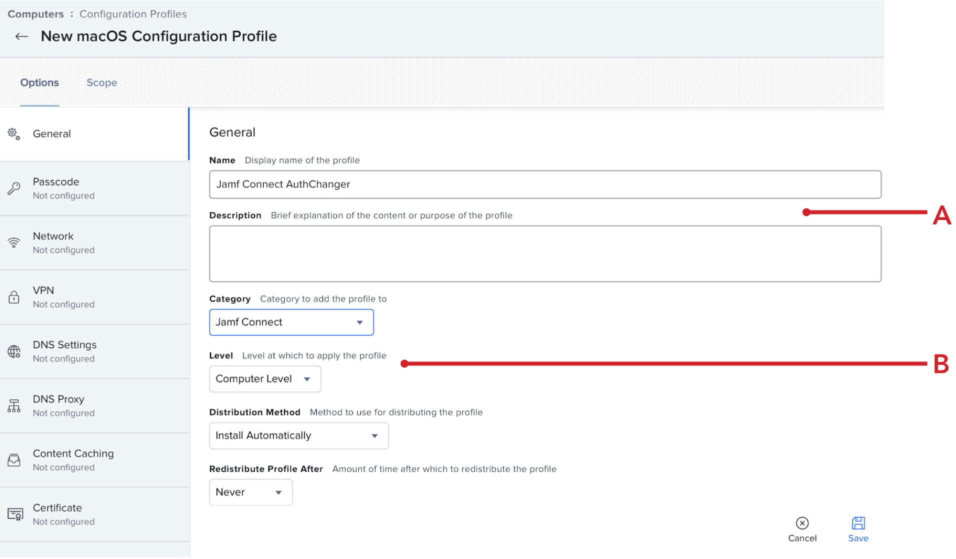
Selected Deployment Targets

TARGET	TYPE
keith's MacBook Air	Computer

52. Create another Configuration Profile. Click New.



53. 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.


Computers : Configuration Profiles

New macOS Configuration Profile

Options | Scope

General

Name Display name of the profile: Jamf Connect AuthChanger

Description Brief explanation of the content or purpose of the profile

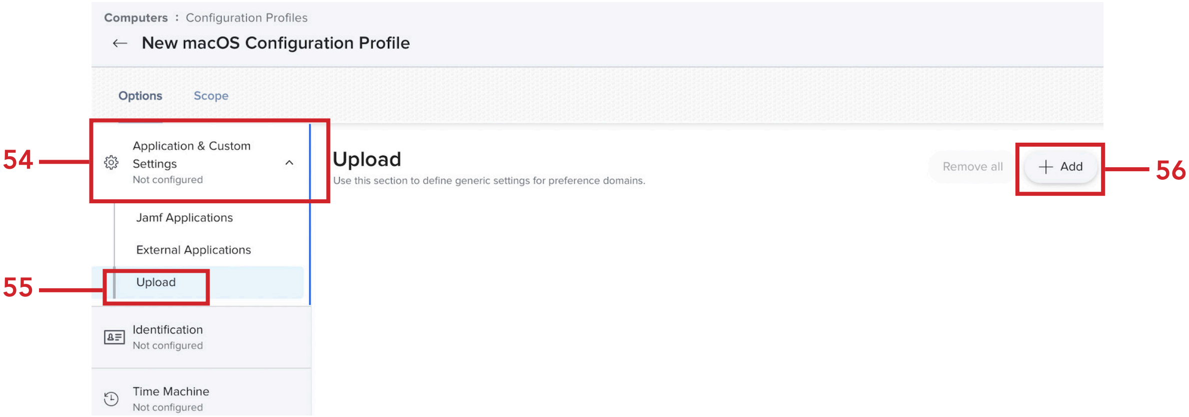
Category Category to add the profile to: Jamf Connect

Level Level at which to apply the profile: Computer Level

Distribution Method Method to use for distributing the profile: Install Automatically

Redistribute Profile After Amount of time after which to redistribute the profile: Never

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


Computers : Configuration Profiles

New macOS Configuration Profile

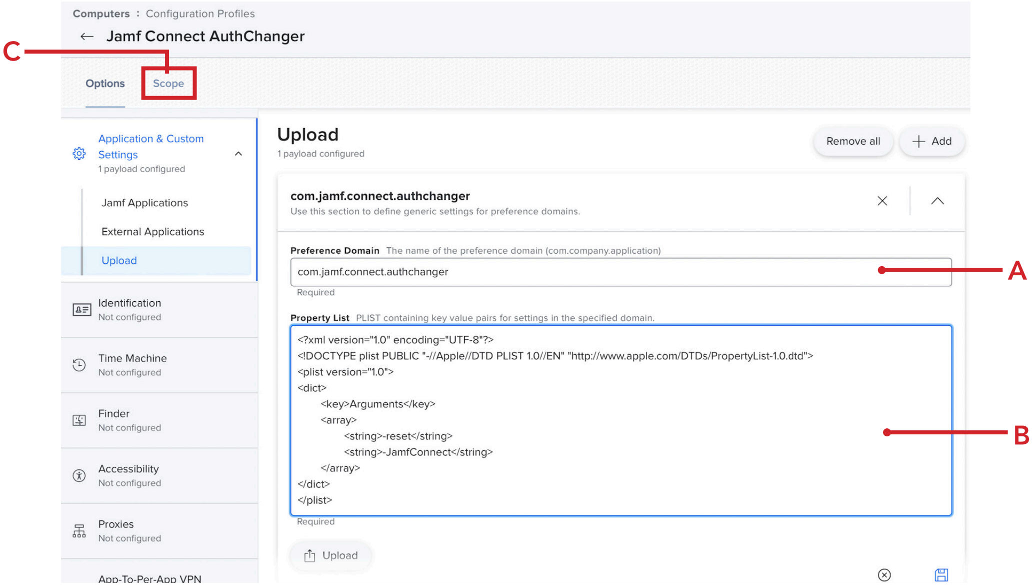
Options | Scope

Upload

Use this section to define generic settings for preference domains.

57. 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>
```



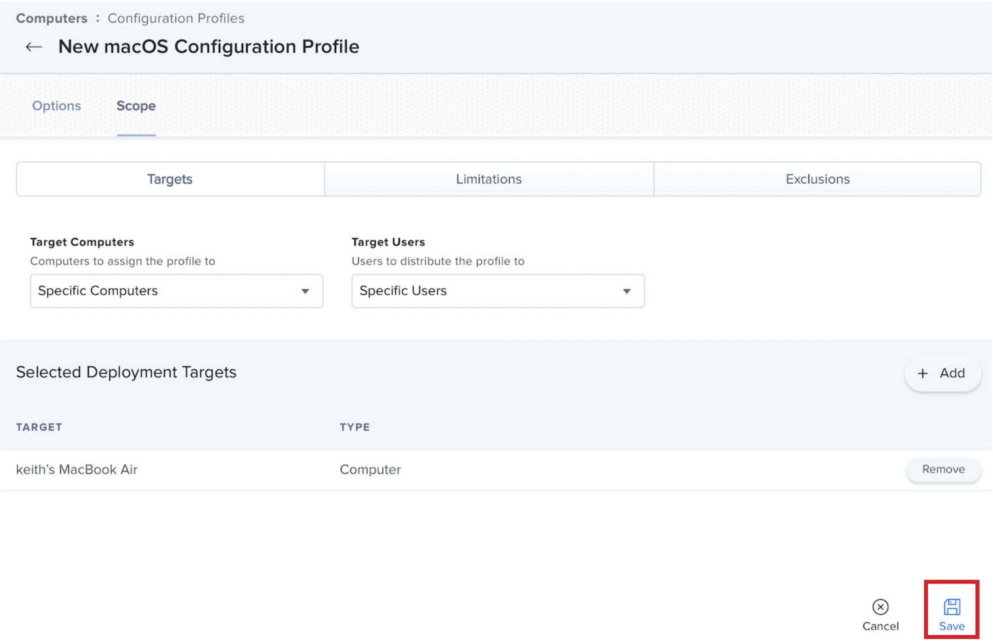
Preference Domain The name of the preference domain (com.company.application)

com.jamf.connect.authchanger

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

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

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

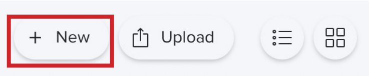

Computers : Configuration Profiles
New macOS Configuration Profile
Options
Scope
Targets
Limitations
Exclusions
Selected Deployment Targets
Add
Remove
Cancel
Save

Target Computers
Computers to assign the profile to
Specific Computers

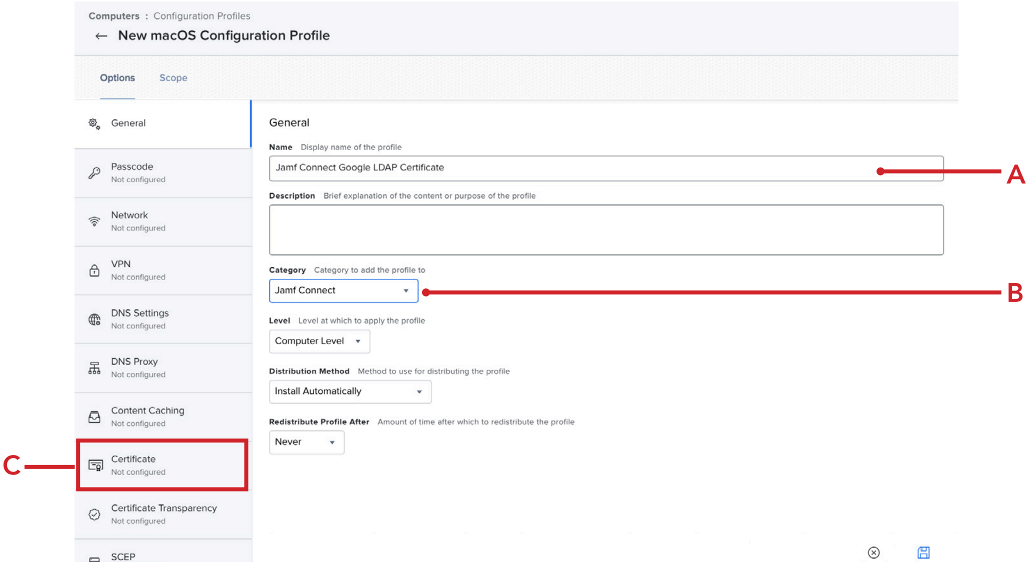
Target Users
Users to distribute the profile to
Specific Users

TARGET	TYPE
keith's MacBook Air	Computer

59. Create another Configuration Profile. Click New.



60. Click the General Payload, then enter the following:
   A. Name: Jamf Connect Google LDAP Certificate
   B. Category: This guide will use Jamf Connect
   C. Select the Certificate payload.



General

Name Display name of the profile: Jamf Connect Google LDAP Certificate

Description Brief explanation of the content or purpose of the profile

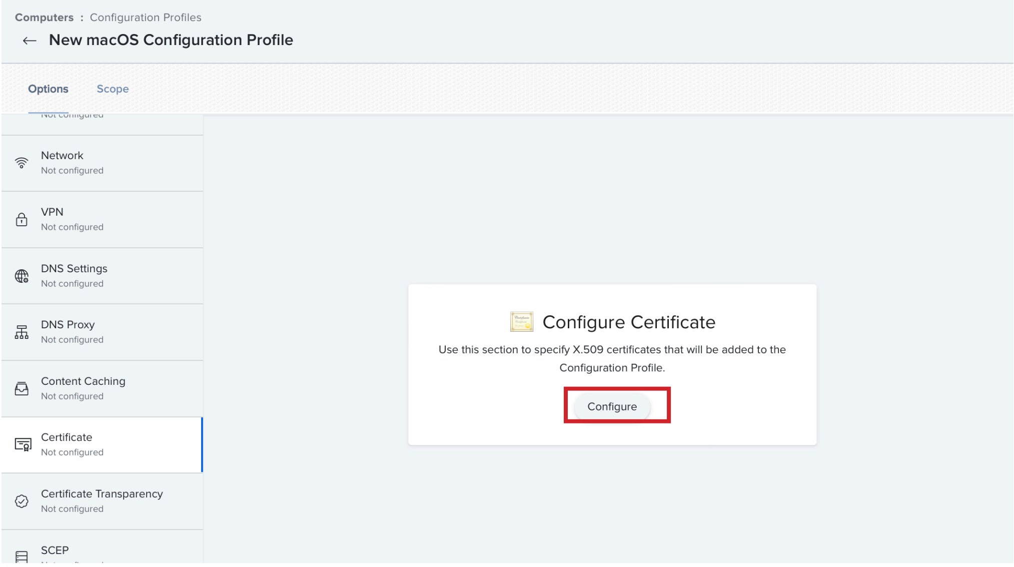
Category Category to add the profile to: Jamf Connect

Level Level at which to apply the profile: Computer Level

Distribution Method Method to use for distributing the profile: Install Automatically

Redistribute Profile After Amount of time after which to redistribute the profile: Never

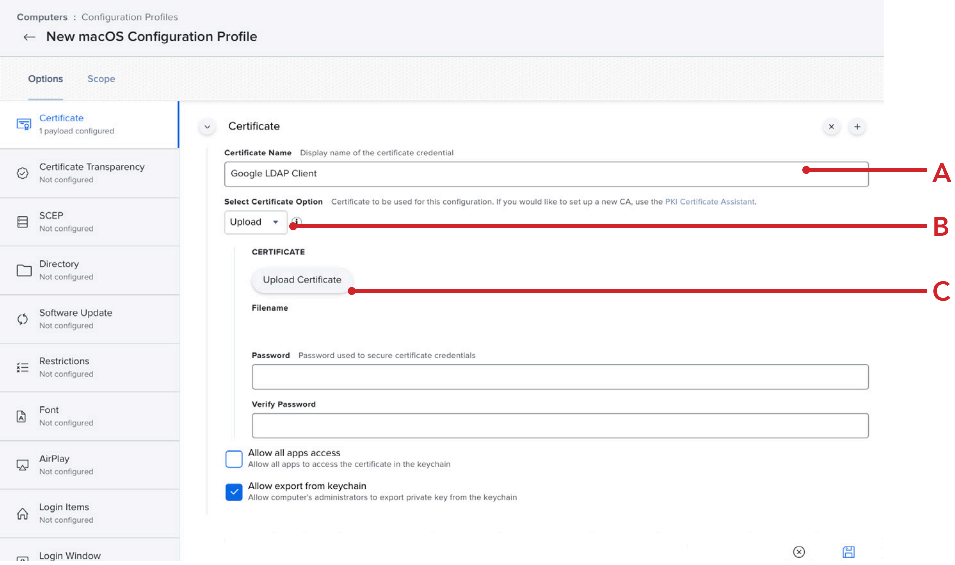
61. Click Configure. NOTE: Google Cloud Identity requires an LDAP certificate in order to log in using Jamf Connect.



Configure Certificate

Use this section to specify X.509 certificates that will be added to the Configuration Profile.

62. Enter the following:
    A. Certificate Name: Google LDAP Client
    B. Select Certificate Option: Select Upload
    C. Certificate: Click Upload Certificate



Certificate Name Display name of the certificate credential

Google LDAP Client

Select Certificate Option Certificate to be used for this configuration. If you would like to set up a new CA, use the PKI Certificate Assistant.

Upload ▾

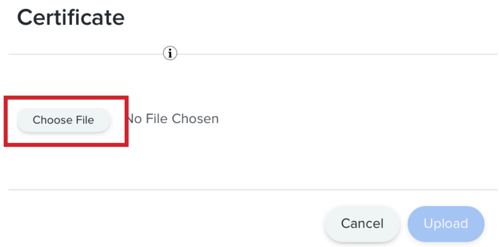
Password Password used to secure certificate credentials

Verify Password

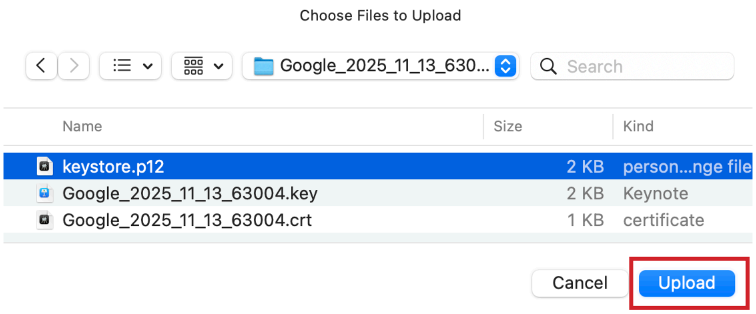
☐ Allow all apps access
Allow all apps to access the certificate in the keychain

☑ Allow export from keychain
Allow computer's administrators to export private key from the keychain

63. Click Choose File.

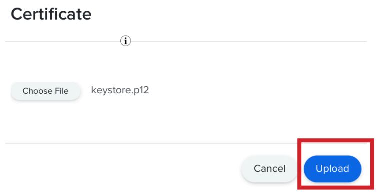


64. Navigate to the keystore.p12 file that we created in section one of this guide. Click Upload.



Name	Size	Kind
keystore.p12	2 KB	person...nge file
Google_2025_11_13_63004.key	2 KB	Keynote
Google_2025_11_13_63004.crt	1 KB	certificate

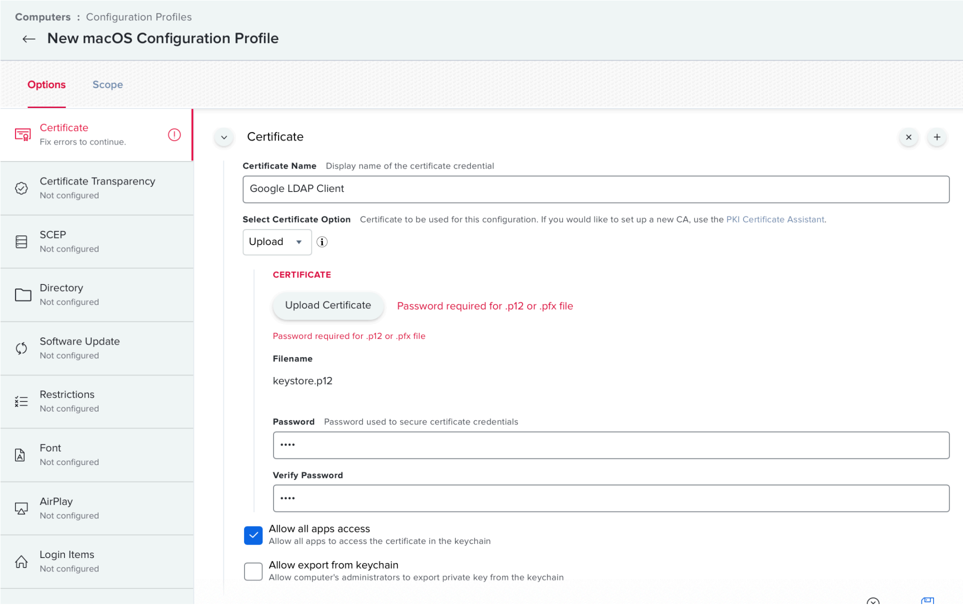
65. Click Upload.



Certificate

Choose File keystore.p12

66. Enter the following:
    A. Enter the password that you used when you created the keystore.p12 file. This guide will use 1234
    B. Verify Password: Enter in the same password to verify it.
    C. Enable Allow all apps access.
    D. Disable Allow export from keychain.
    E. Click Scope.



Computers : Configuration Profiles

New macOS Configuration Profile

Certificate

Certificate Name Display name of the certificate credential

Google LDAP Client

Select Certificate Option Certificate to be used for this configuration. If you would like to set up a new CA, use the PKI Certificate Assistant.

Upload

CERTIFICATE

Upload Certificate Password required for .p12 or .pfx file

Password required for .p12 or .pfx file

Filename

keystore.p12

Password Password used to secure certificate credentials

••••

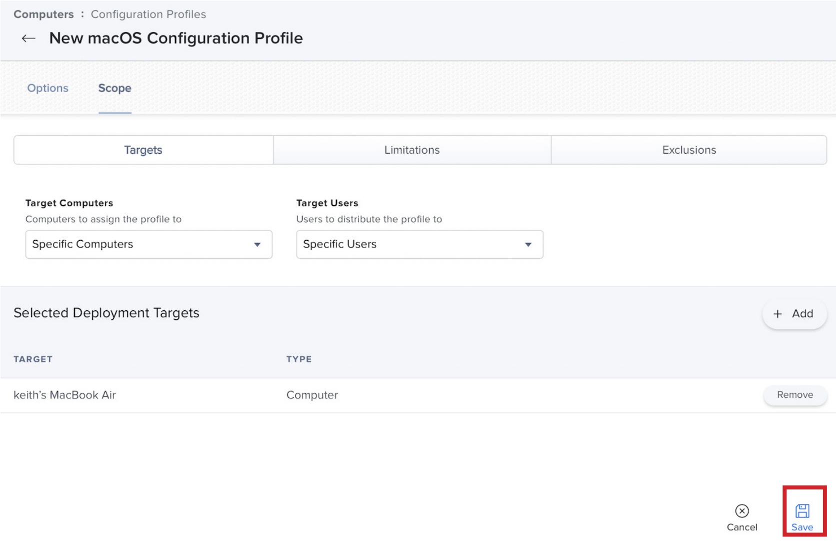
Verify Password

••••

☑ Allow all apps access
Allow all apps to access the certificate in the keychain

☐ Allow export from keychain
Allow computer's administrators to export private key from the keychain

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



Computers : Configuration Profiles

New macOS Configuration Profile

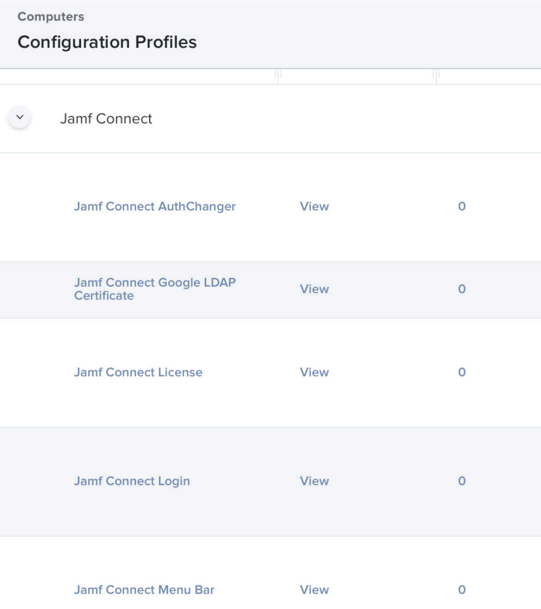
Target Computers
Computers to assign the profile to
Specific Computers

Target Users
Users to distribute the profile to
Specific Users

Selected Deployment Targets

TARGET	TYPE
keith's MacBook Air	Computer

68. Confirm you have the five configuration profiles shown below.



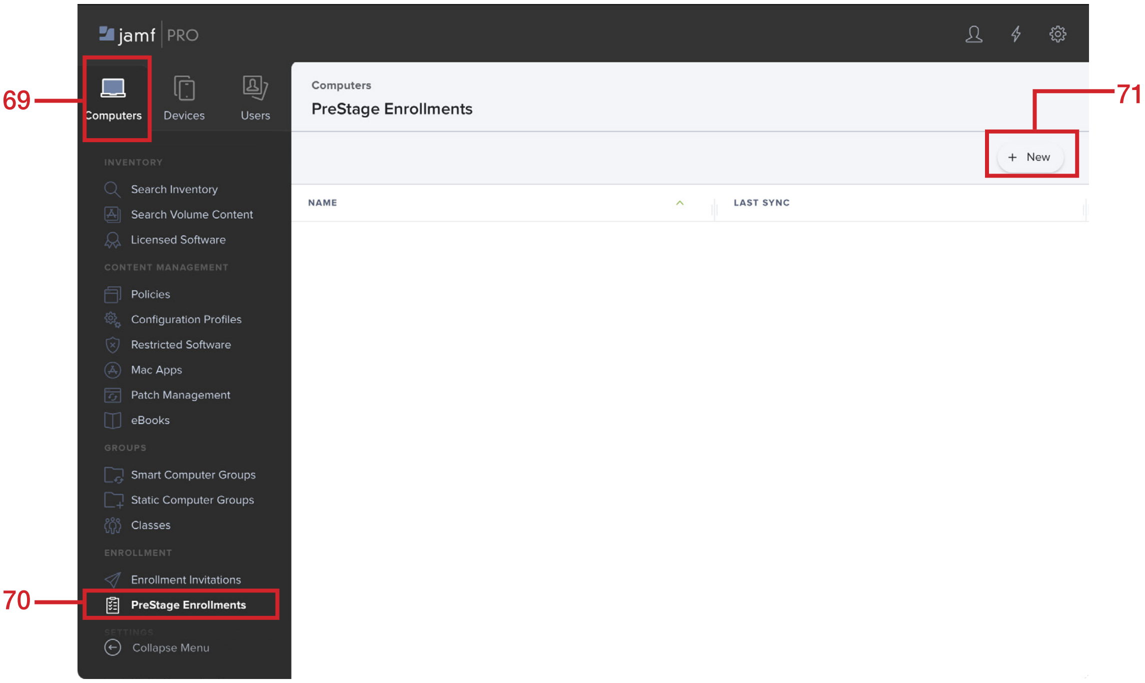
Computers

Configuration Profiles

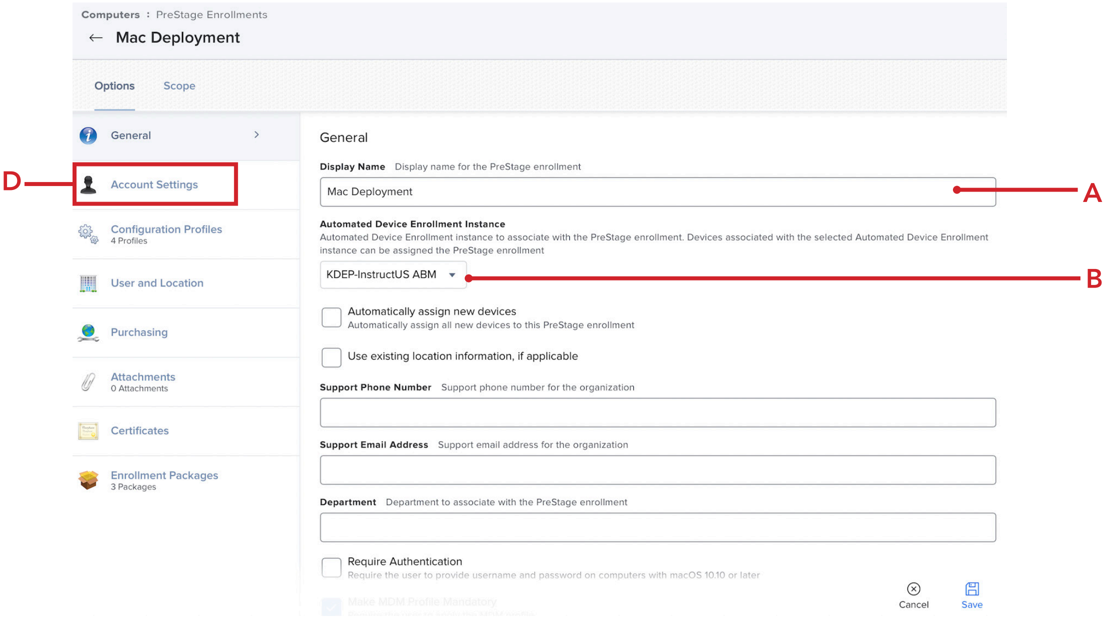
Jamf Connect

Jamf Connect AuthChanger	View	0
Jamf Connect Google LDAP Certificate	View	0
Jamf Connect License	View	0
Jamf Connect Login	View	0
Jamf Connect Menu Bar	View	0

69. Click Computers
70. Click PreStage Enrollments.
71. Click New



72. 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.



Computers : PreStage Enrollments

← Mac Deployment

Options | Scope

- General ›
- Account Settings
- Configuration Profiles
  4 Profiles
- User and Location
- Purchasing
- Attachments
  0 Attachments
- Certificates
- Enrollment Packages
  3 Packages

General

Display Name Display name for the PreStage enrollment

Mac Deployment

Automated Device Enrollment Instance
Automated Device Enrollment instance to associate with the PreStage enrollment. Devices associated with the selected Automated Device Enrollment instance can be assigned the PreStage enrollment

KDEP-InstructUS ABM

□ Automatically assign new devices
Automatically assign all new devices to this PreStage enrollment

□ Use existing location information, if applicable

Support Phone Number Support phone number for the organization

Support Email Address Support email address for the organization

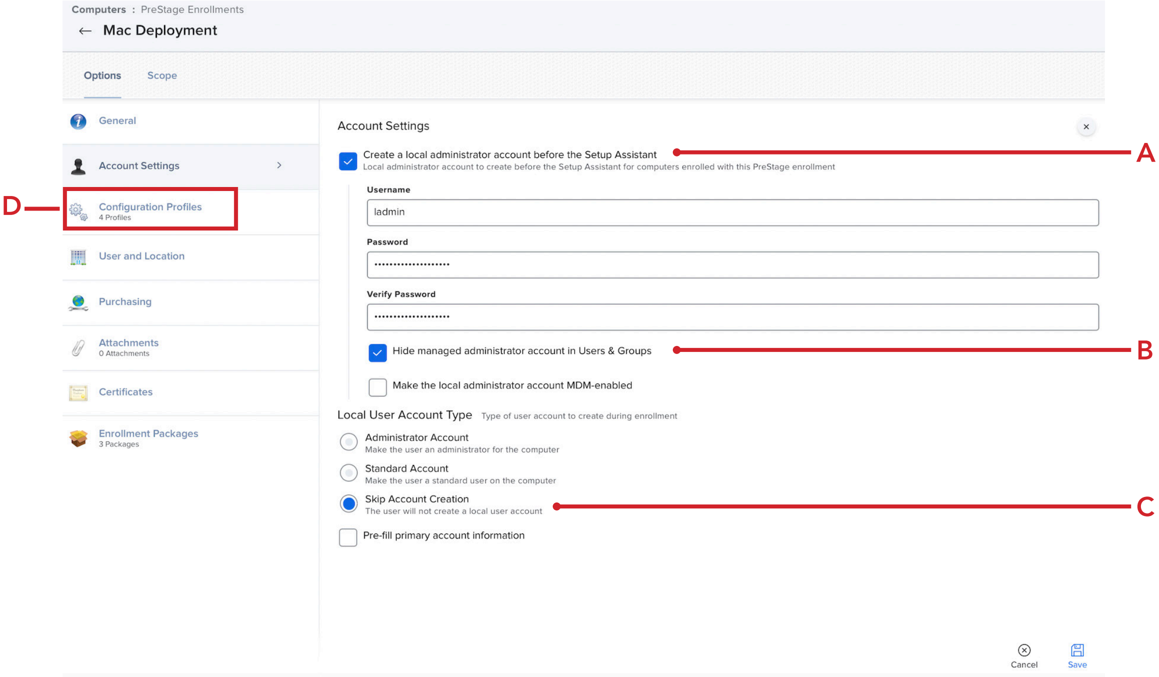
Department Department to associate with the PreStage enrollment

□ Require Authentication
Require the user to provide username and password on computers with macOS 10.10 or later

Make MDM Profile Mandatory

Cancel | Save

73. 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



Computers : PreStage Enrollments

← Mac Deployment

Options | Scope

- General
- Account Settings ›
- Configuration Profiles
  4 Profiles
- User and Location
- Purchasing
- Attachments
  0 Attachments
- Certificates
- Enrollment Packages
  3 Packages

Account Settings ×

☑ Create a local administrator account before the Setup Assistant
Local administrator account to create before the Setup Assistant for computers enrolled with this PreStage enrollment

Username
ladmin

Password
••••••••••••••••••••

Verify Password
••••••••••••••••••••

☑ Hide managed administrator account in Users & Groups

□ Make the local administrator account MDM-enabled

Local User Account Type Type of user account to create during enrollment

○ Administrator Account
Make the user an administrator for the computer

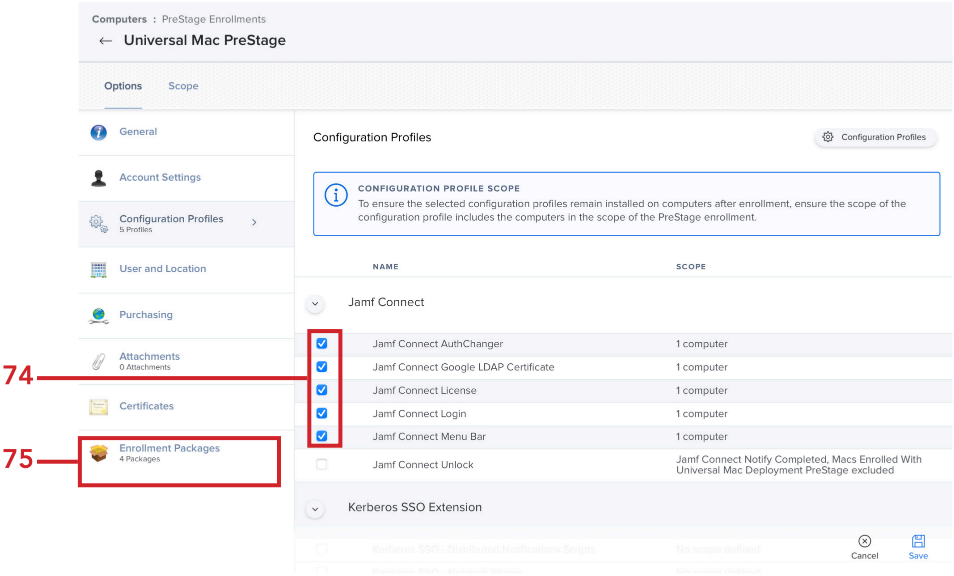
○ Standard Account
Make the user a standard user on the computer

● Skip Account Creation
The user will not create a local user account

□ Pre-fill primary account information

Cancel | Save

74. Select the checkboxes for the four Jamf Connect configuration profiles
75. Click the Enrollment Packages payload.



Configuration Profiles

CONFIGURATION PROFILE SCOPE
To ensure the selected configuration profiles remain installed on computers after enrollment, ensure the scope of the configuration profile includes the computers in the scope of the PreStage enrollment.

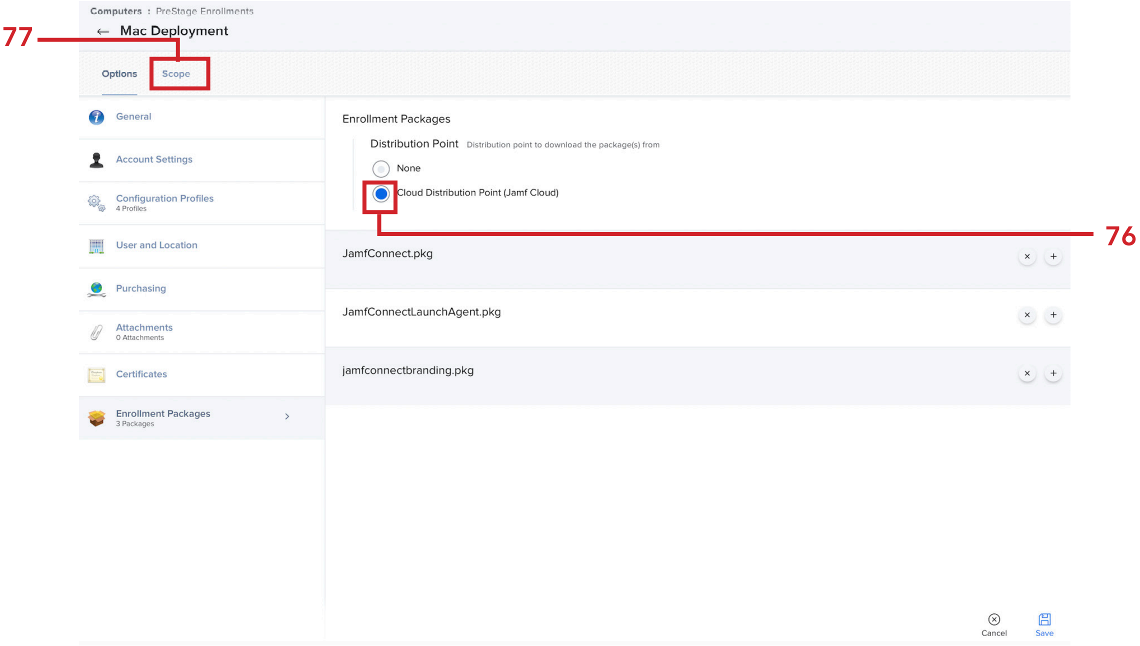
Jamf Connect

	NAME	SCOPE
☑	Jamf Connect AuthChanger	1 computer
☑	Jamf Connect Google LDAP Certificate	1 computer
☑	Jamf Connect License	1 computer
☑	Jamf Connect Login	1 computer
☑	Jamf Connect Menu Bar	1 computer
□	Jamf Connect Unlock	Jamf Connect Notify Completed, Macs Enrolled With Universal Mac Deployment PreStage excluded

Kerberos SSO Extension

□	Kerberos SSO - Distributed Notifications Scripts	No scope defined
□	Kerberos SSO - Network Shares	No scope defined

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



Enrollment Packages

Distribution Point Distribution point to download the package(s) from

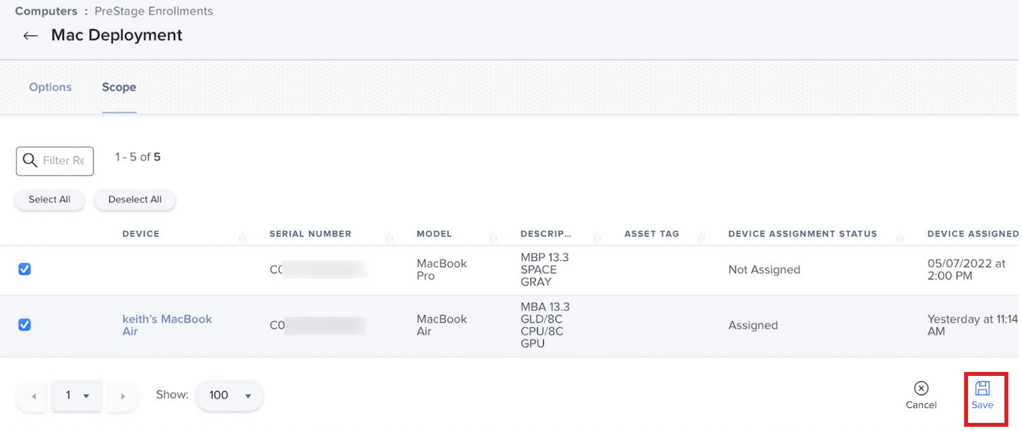
○ None
● Cloud Distribution Point (Jamf Cloud)

JamfConnect.pkg

JamfConnectLaunchAgent.pkg

jamfconnectbranding.pkg

78. Scope to your needs then click Save.



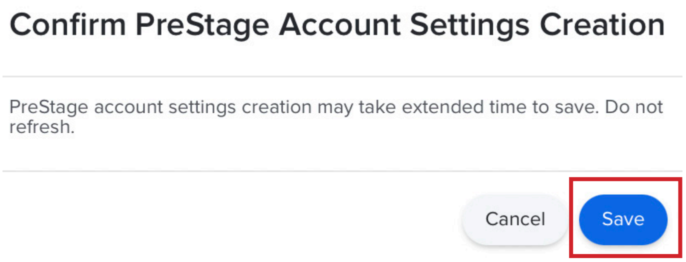
Computers : PreStage Enrollments

← Mac Deployment

1 - 5 of 5

	DEVICE	SERIAL NUMBER	MODEL	DESCRIP...	ASSET TAG	DEVICE ASSIGNMENT STATUS	DEVICE ASSIGNED
☑		CC[redacted]	MacBook Pro	MBP 13.3 SPACE GRAY		Not Assigned	05/07/2022 at 2:00 PM
☑	keith's MacBook Air	CO[redacted]	MacBook Air	MBA 13.3 GLD/8C CPU/8C GPU		Assigned	Yesterday at 11:14 AM

79. Click Save.



Confirm PreStage Account Settings Creation

PreStage account settings creation may take extended time to save. Do not refresh.

In the next section we will deploy a Mac 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 with Jamf Pro

What You'll Need

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

Hardware and Software

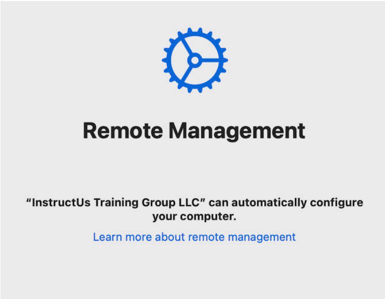
Requirements for following along with this section:

- A Mac that's brand new in the box or an old Mac that is at Setup Assistant (10.15.4 or later). The Mac must be enrolled in Apple Business Manager or Apple School Manager and assigned to your PreStage in Jamf Pro. This is required for Automated Device Enrollment scoped in a PreStage.
- Google login credentials.

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.

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

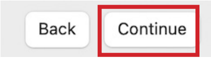
1. At the Remote Management screen, click Continue.



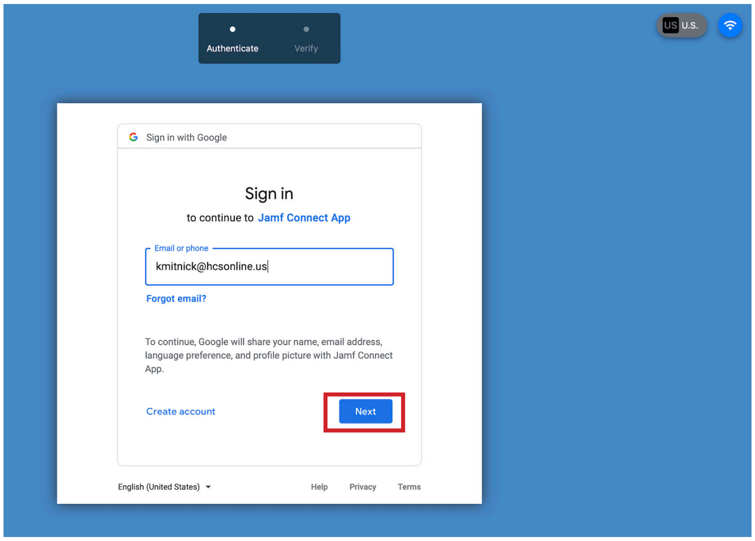
Remote Management

"InstructUs Training Group LLC" can automatically configure your computer.

Learn more about remote management



2. After setup assistant is completed, You're presented with a customized Jamf Connect Login window. The background is blue, the Wi-Fi logo is visible, 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. Enter your Google Email address then click Next.



Sign in

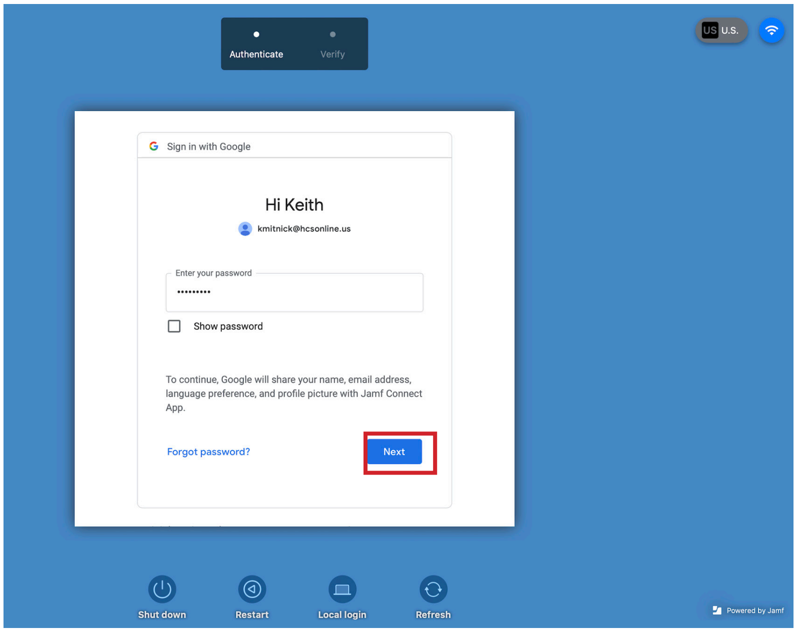
to continue to Jamf Connect App

Email or phone: kmitnick@hcsonline.us

Forgot email?

To continue, Google will share your name, email address, language preference, and profile picture with Jamf Connect App.

3. Enter your Google password then click Next.



Hi Keith

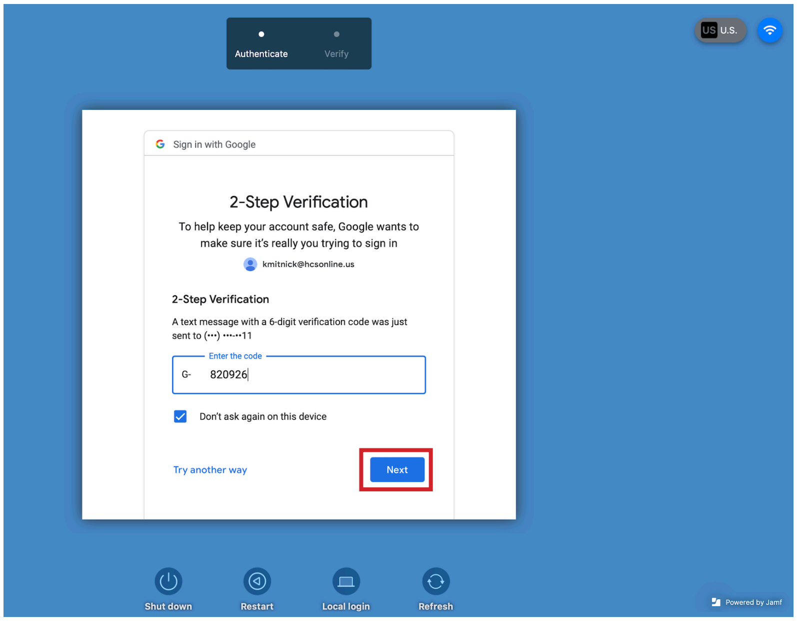
kmitnick@hcsonline.us

Enter your password: •••••••••

□ Show password

To continue, Google will share your name, email address, language preference, and profile picture with Jamf Connect App.

4. You will be prompted with the 2-Step Verification message below and a code will be sent to your phone. Enter the code and click Next.



2-Step Verification

To help keep your account safe, Google wants to make sure it's really you trying to sign in

kmitnick@hcsonline.us

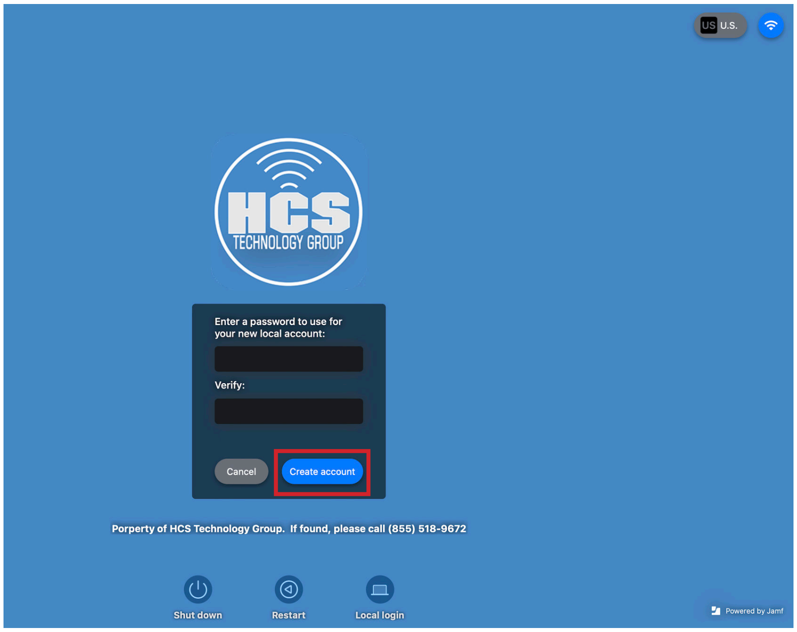
2-Step Verification

A text message with a 6-digit verification code was just sent to (•••) •••-••11

Enter the code: G- 820926

☑ Don't ask again on this device

5. Enter a password that you want to use for your new local account. We recommend using the same password as your Google account password to keep things in sync. Click Create account.

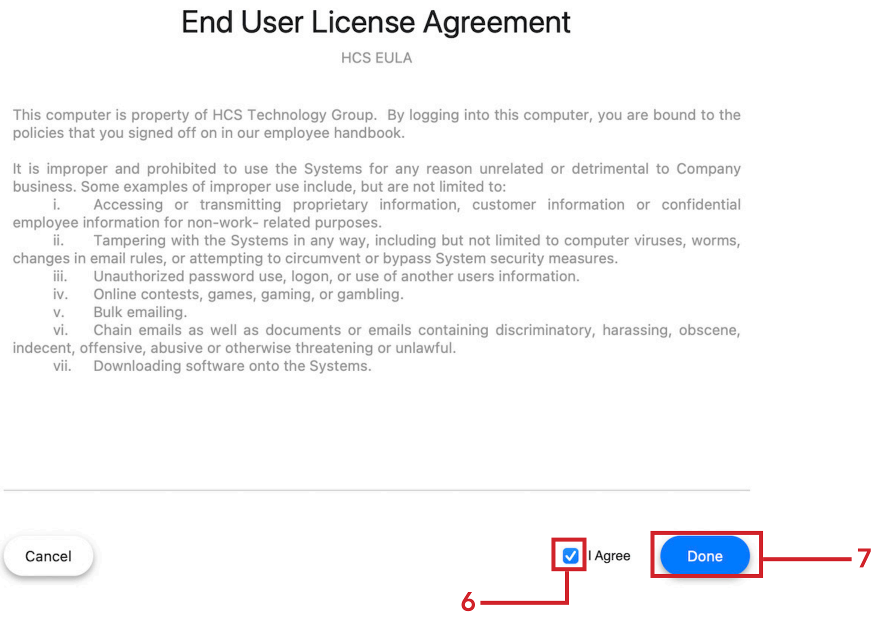


Enter a password to use for your new local account:

Verify:

Porperty of HCS Technology Group. If found, please call (855) 518-9672

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



End User License Agreement

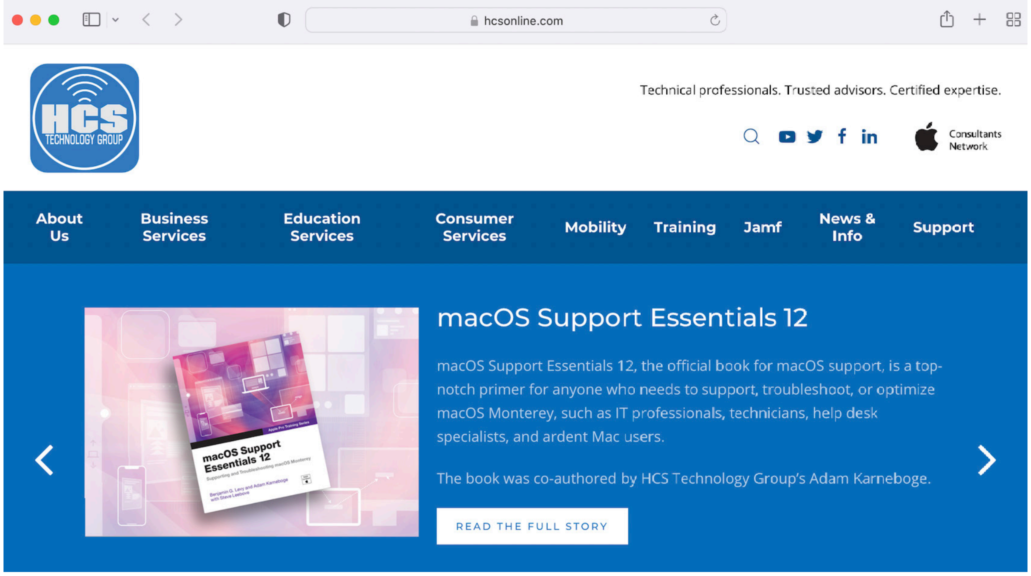
HCS EULA

This computer is property of HCS Technology Group. By logging into this computer, you are bound to the policies that you signed off on in our employee handbook.

It is improper and prohibited to use the Systems for any reason unrelated or detrimental to Company business. Some examples of improper use include, but are not limited to:

i. Accessing or transmitting proprietary information, customer information or confidential employee information for non-work- related purposes.
ii. Tampering with the Systems in any way, including but not limited to computer viruses, worms, changes in email rules, or attempting to circumvent or bypass System security measures.
iii. Unauthorized password use, logon, or use of another users information.
iv. Online contests, games, gaming, or gambling.
v. Bulk emailing.
vi. Chain emails as well as documents or emails containing discriminatory, harassing, obscene, indecent, offensive, abusive or otherwise threatening or unlawful.
vii. Downloading software onto the Systems.

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.



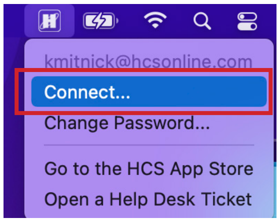
Technical professionals. Trusted advisors. Certified expertise.

macOS Support Essentials 12

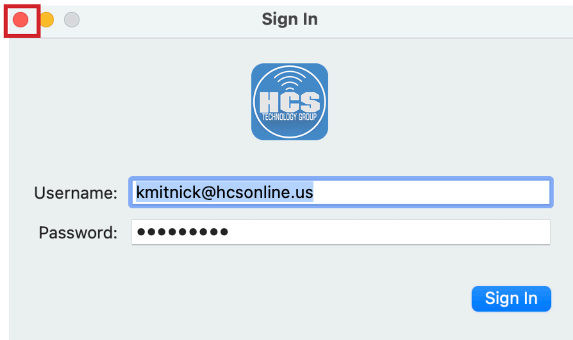
macOS Support Essentials 12, the official book for macOS support, is a top-notch primer for anyone who needs to support, troubleshoot, or optimize macOS Monterey, such as IT professionals, technicians, help desk specialists, and ardent Mac users.

The book was co-authored by HCS Technology Group's Adam Karneboge.

9. Reconnect to Google Cloud Identity by selecting the Jamf Connect Menu Bar icon, which should be customized to your branded logo if you followed along with this guide, and select Connect.



10. Confirm the customized logo shows up at the Sign In window. Close this window.

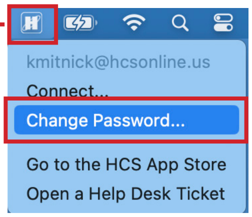


Username: kmitnick@hcsonline.us

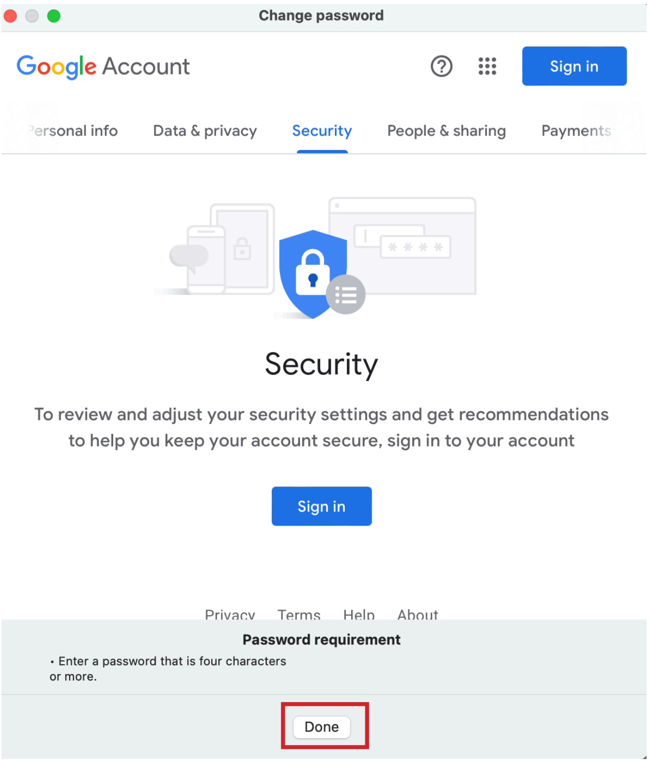
Password: •••••••••

11. Click the Jamf Connect Menu Bar icon and select Change Password.

Click the custom logo to access Jamf Connect



12. Confirm the Google Cloud Identity window shows up in the change password window. We will not change the password at this time. Click Done to close this window.



Security

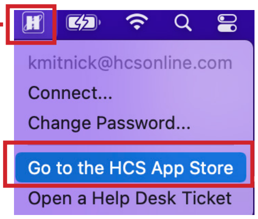
To review and adjust your security settings and get recommendations to help you keep your account secure, sign in to your account

Password requirement

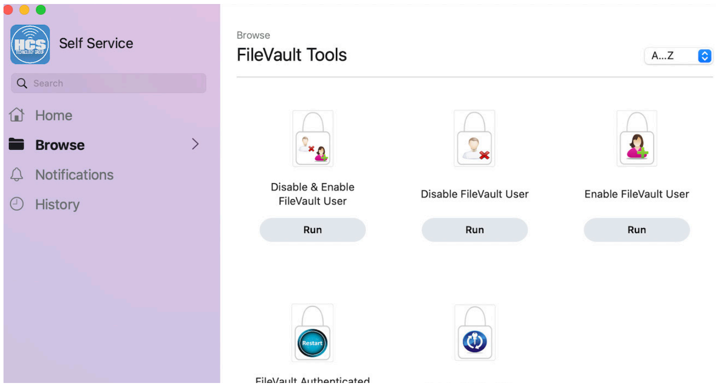
- Enter a password that is four characters or more.

13. Click Jamf Connect from the Menu bar and select Go to the HCS App Store.

Click the custom logo to access Jamf Connect

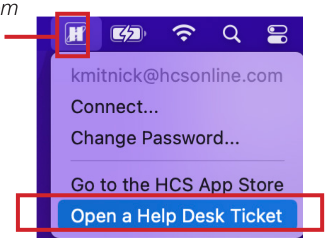


14. The Self Service application will open. Quit the Self Service application.

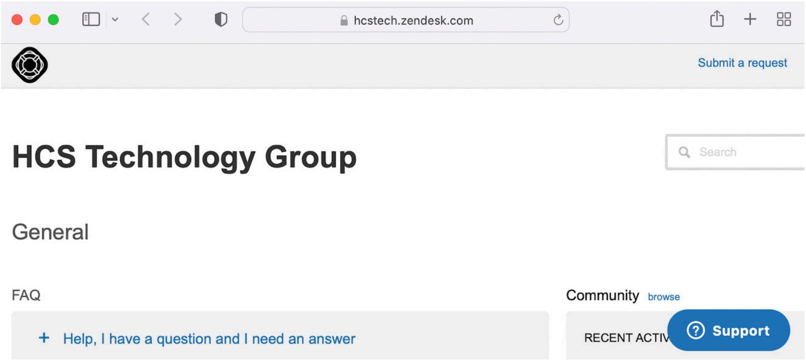


15. Click the Jamf Connect Menu Bar icon and select Open a Help Desk Ticket. NOTE: you will only see this if you entered information for User help (Please see Section 5, Step 7, **User help** on page 37.)

Click the custom logo to access Jamf Connect



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



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

What You'll Need

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

Hardware and Software

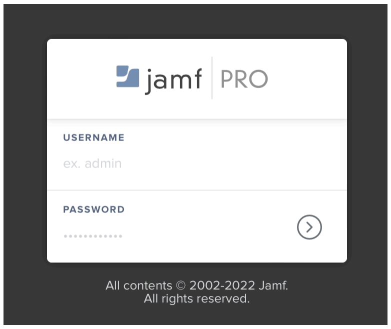
Requirements for following along with this section:

- A Mac that's brand new in the box or an old Mac that is at Setup Assistant (10.15.4 or later). The Mac must be enrolled in Apple Business Manager or Apple School Manager and assigned to your PreStage in Jamf Pro. This is required for Automated Device Enrollment scoped in a 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.
- Google login credentials.

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.

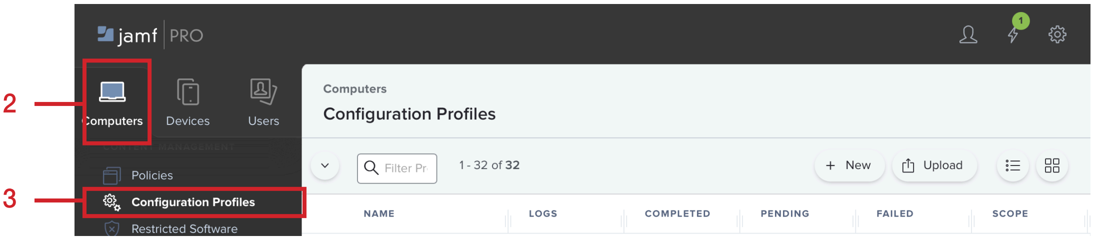
In this section we will discuss configuring Jamf Connect Notify which is a screen that can display a progress bar, customized text, and images during Automated Device Enrollment. This allows an organization to install required applications when the user logs in for the first time. The entire screen is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

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

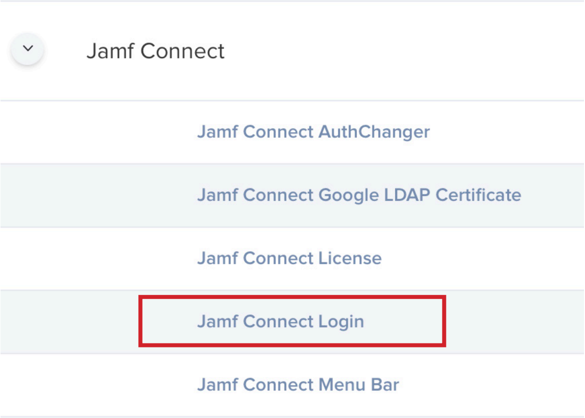


All contents © 2002-2022 Jamf.
All rights reserved.

2. Click Computers.
3. Click Configuration Profiles.



4. Select the Jamf Connect Login configuration profile.

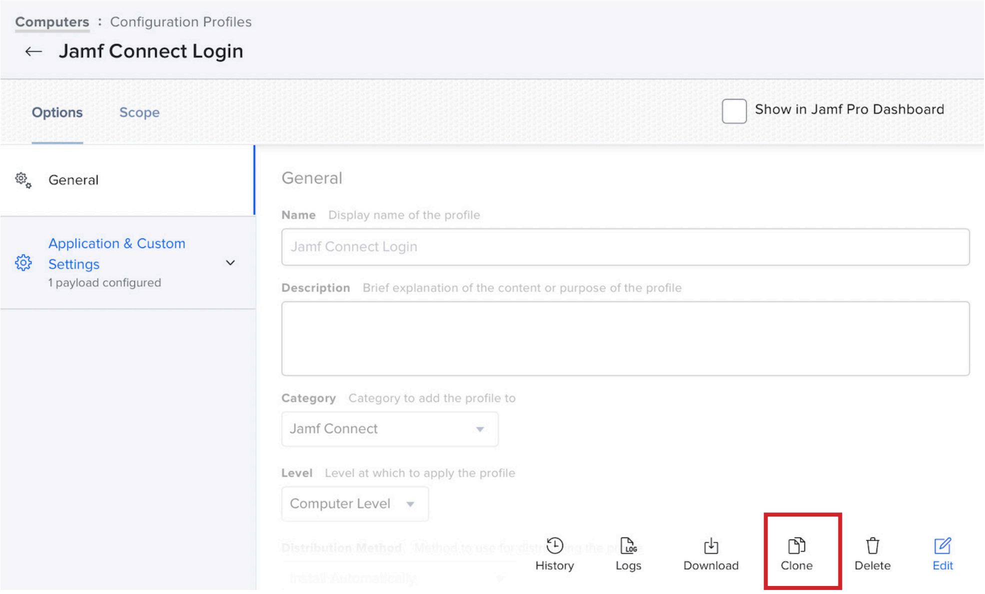


Jamf Connect

- Jamf Connect AuthChanger
- Jamf Connect Google LDAP Certificate
- Jamf Connect License
- Jamf Connect Login
- Jamf Connect Menu Bar

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.



Computers : Configuration Profiles

← Jamf Connect Login

Options Scope □ Show in Jamf Pro Dashboard

General

Application & Custom Settings
1 payload configured

General

Name Display name of the profile

Jamf Connect Login

Description Brief explanation of the content or purpose of the profile

Category Category to add the profile to

Jamf Connect

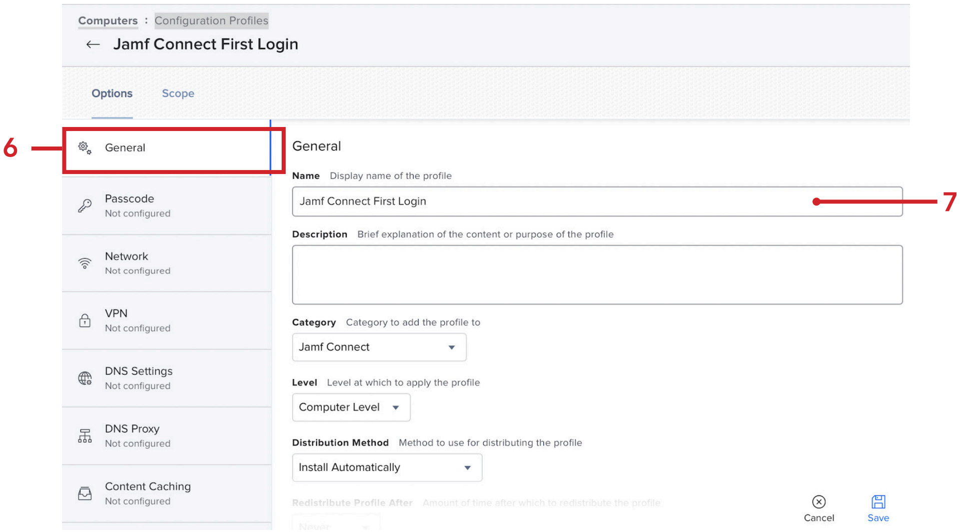
Level Level at which to apply the profile

Computer Level

Distribution Method Method to use for distributing the profile

Install Automatically

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



Jamf Connect First Login

General

Name Display name of the profile: Jamf Connect First Login

Description Brief explanation of the content or purpose of the profile

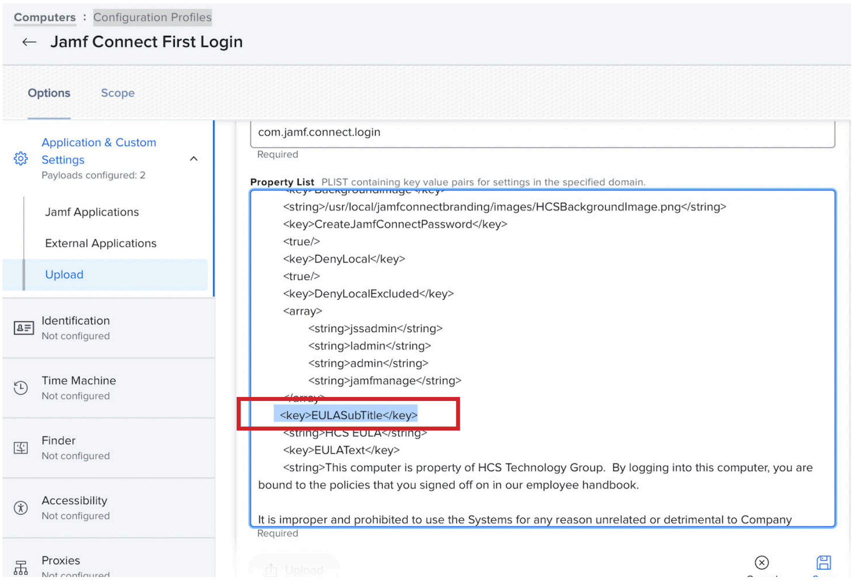
Category Category to add the profile to: Jamf Connect

Level Level at which to apply the profile: Computer Level

Distribution Method Method to use for distributing the profile: Install Automatically

Redistribute Profile After Amount of time after which to redistribute the profile: Never

8. Scroll down to Application & Custom Settings. Click Upload.
9. Scroll down in the Property List section until you find the key named EULASubTitle as shown below.



Jamf Connect First Login

com.jamf.connect.login

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

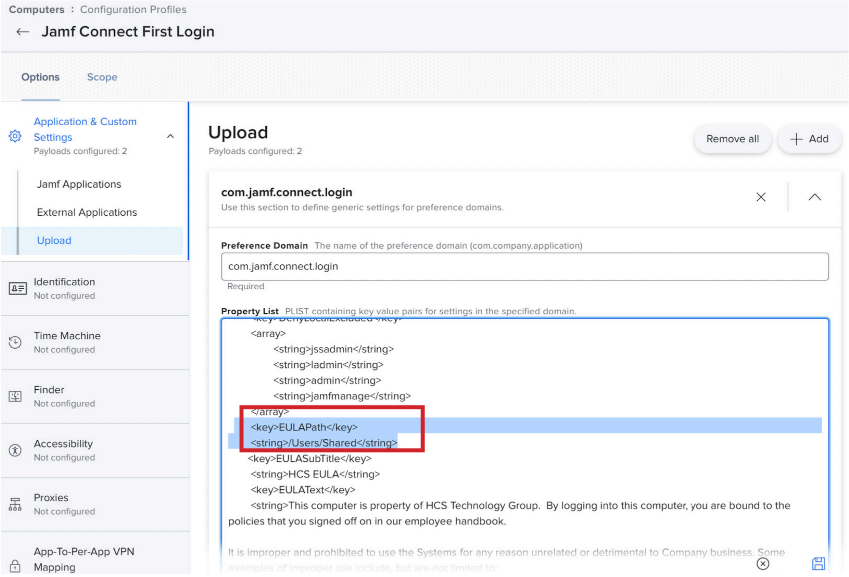
```
    <key>BackgroundImage</key>
    <string>/usr/local/jamfconnectbranding/images/HCSBackgroundImage.png</string>
    <key>CreateJamfConnectPassword</key>
    <true/>
    <key>DenyLocal</key>
    <true/>
    <key>DenyLocalExcluded</key>
    <array>
        <string>jssadmin</string>
        <string>ladmin</string>
        <string>admin</string>
        <string>jamfmanage</string>
    </array>
    <key>EULASubTitle</key>
    <string>HCS EULA</string>
    <key>EULAText</key>
    <string>This computer is property of HCS Technology Group.  By logging into this computer, you are
bound to the policies that you signed off on in our employee handbook.

It is improper and prohibited to use the Systems for any reason unrelated or detrimental to Company
```

10. 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.



com.jamf.connect.login

Use this section to define generic settings for preference domains.

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

com.jamf.connect.login

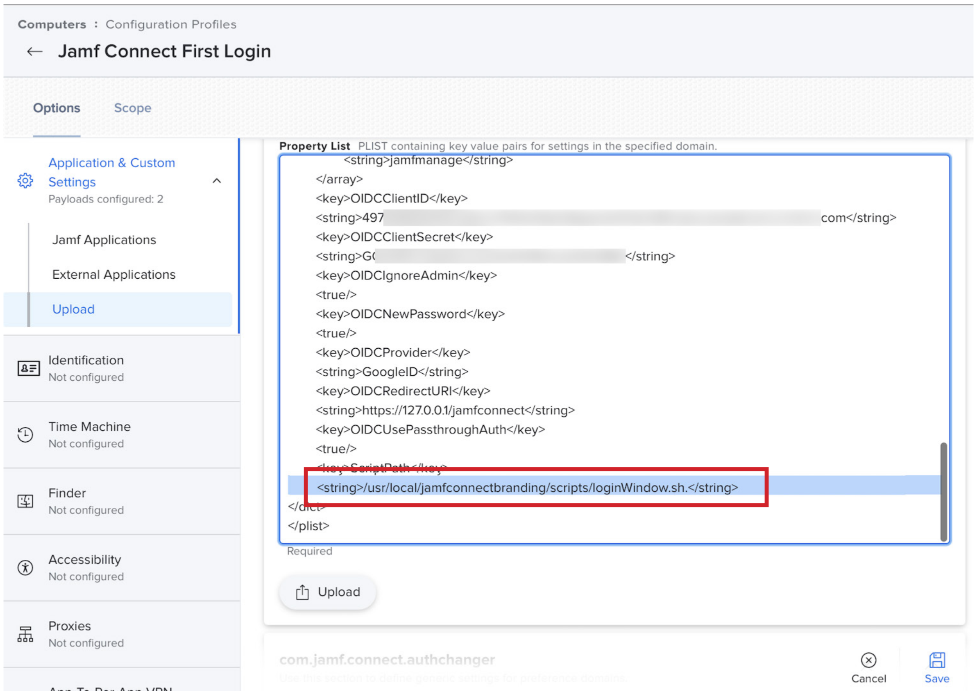
Required

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

```
    <key>DenyLocalExcluded</key>
    <array>
          <string>jssadmin</string>
          <string>ladmin</string>
          <string>admin</string>
          <string>jamfmanage</string>
    </array>
    <key>EULAPath</key>
    <string>/Users/Shared</string>
   <key>EULASubTitle</key>
    <string>HCS EULA</string>
    <key>EULAText</key>
    <string>This computer is property of HCS Technology Group.  By logging into this computer, you are bound to the
policies that you signed off on in our employee handbook.

It is improper and prohibited to use the Systems for any reason unrelated or detrimental to Company business. Some
examples of improper use include, but are not limited to:
```

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

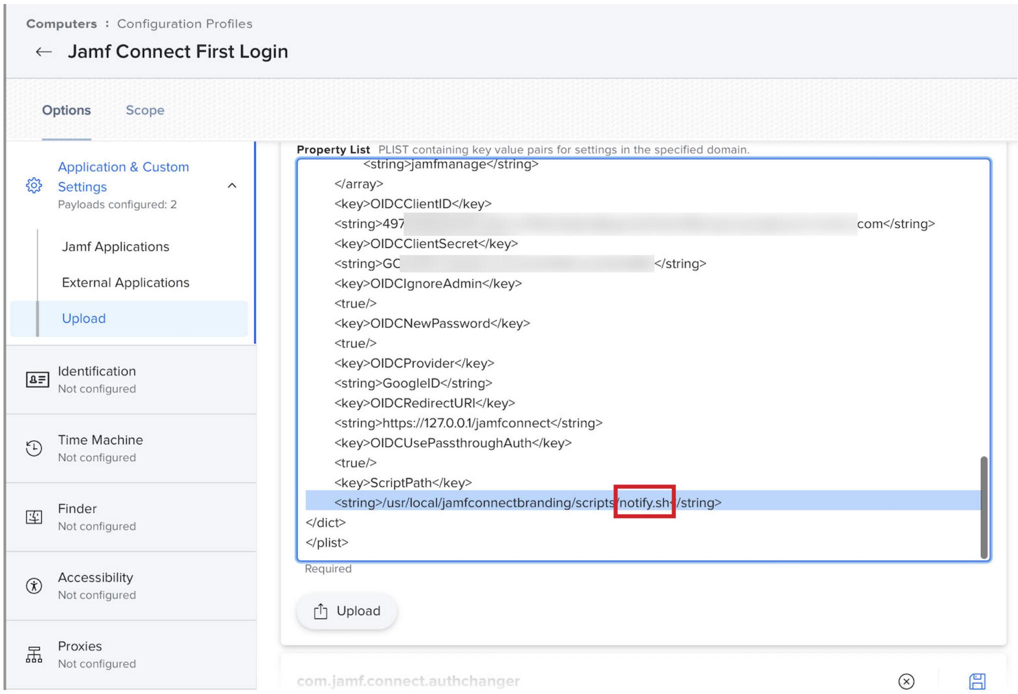


Property List PLIST containing key value pairs for settings in the specified domain.

```
          <string>jamfmanage</string>
    </array>
    <key>OIDCClientID</key>
    <string>497[redacted]com</string>
    <key>OIDCClientSecret</key>
    <string>G[redacted]</string>
    <key>OIDCIgnoreAdmin</key>
    <true/>
    <key>OIDCNewPassword</key>
    <true/>
    <key>OIDCProvider</key>
    <string>GoogleID</string>
    <key>OIDCRedirectURI</key>
    <string>https://127.0.0.1/jamfconnect</string>
    <key>OIDCUsePassthroughAuth</key>
    <true/>
    <key>ScriptPath</key>
    <string>/usr/local/jamfconnectbranding/scripts/loginWindow.sh.</string>
</dict>
</plist>
```

Required

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

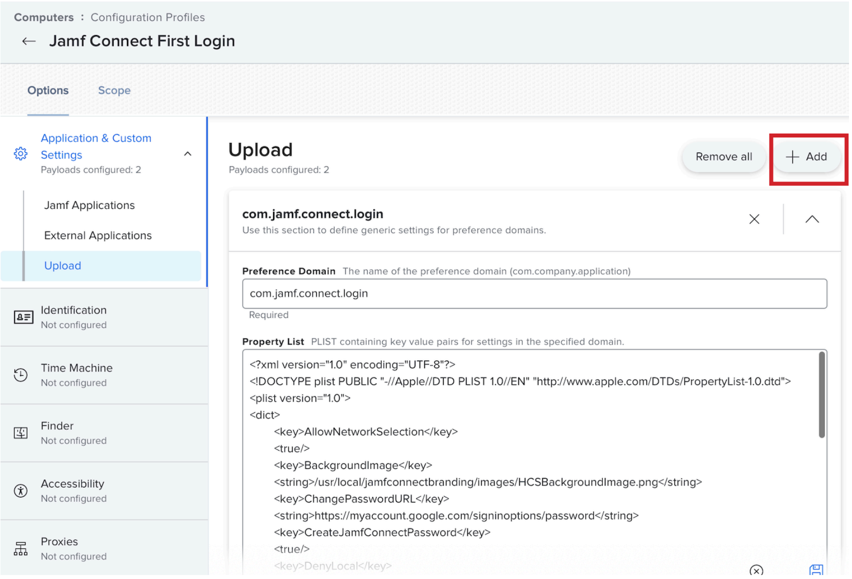


Property List PLIST containing key value pairs for settings in the specified domain.

```
        <string>jamfmanage</string>
    </array>
    <key>OIDCClientID</key>
    <string>497[redacted]com</string>
    <key>OIDCClientSecret</key>
    <string>GC[redacted]</string>
    <key>OIDCIgnoreAdmin</key>
    <true/>
    <key>OIDCNewPassword</key>
    <true/>
    <key>OIDCProvider</key>
    <string>GoogleID</string>
    <key>OIDCRedirectURI</key>
    <string>https://127.0.0.1/jamfconnect</string>
    <key>OIDCUsePassthroughAuth</key>
    <true/>
    <key>ScriptPath</key>
    <string>/usr/local/jamfconnectbranding/scripts/notify.sh</string>
</dict>
</plist>
```

Required

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



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

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

com.jamf.connect.login

Required

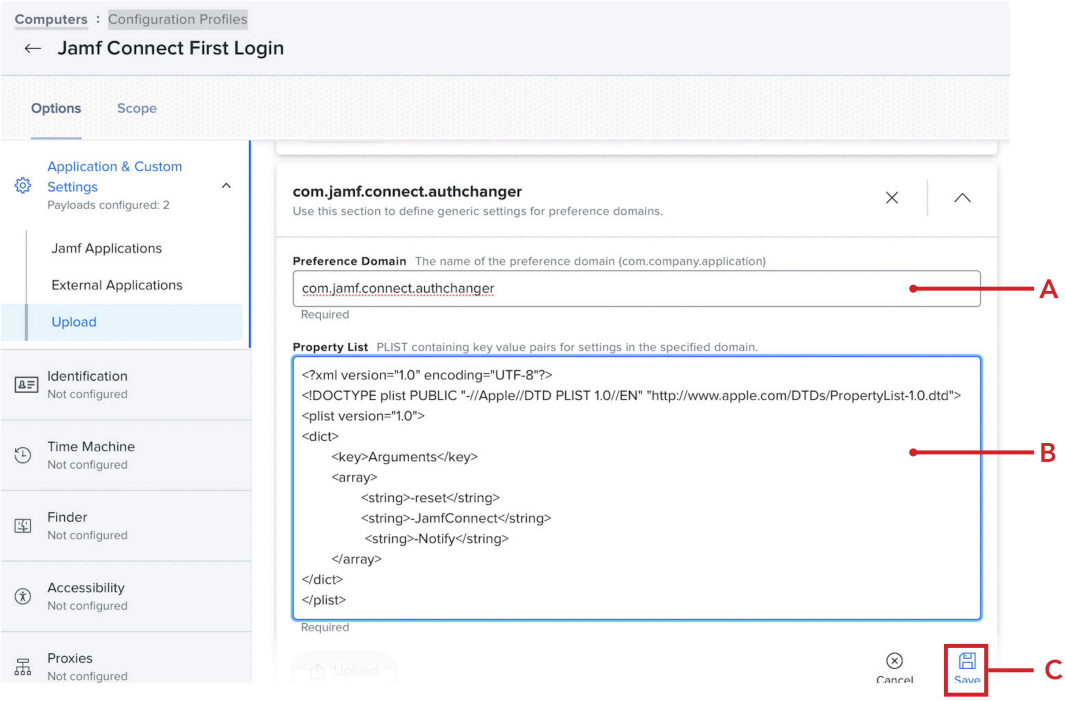
Property List PLIST containing key value pairs for settings in the specified domain.

```
<?xml version="1.0" encoding="UTF-8"?>
<!DOCTYPE plist PUBLIC "-//Apple//DTD PLIST 1.0//EN" "http://www.apple.com/DTDs/PropertyList-1.0.dtd">
<plist version="1.0">
<dict>
    <key>AllowNetworkSelection</key>
    <true/>
    <key>BackgroundImage</key>
    <string>/usr/local/jamfconnectbranding/images/HCSBackgroundImage.png</string>
    <key>ChangePasswordURL</key>
    <string>https://myaccount.google.com/signinoptions/password</string>
    <key>CreateJamfConnectPassword</key>
    <true/>
    <key>DenyLocal</key>
```

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.



Computers : Configuration Profiles

Jamf Connect First Login

Options Scope

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

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

com.jamf.connect.authchanger

Required

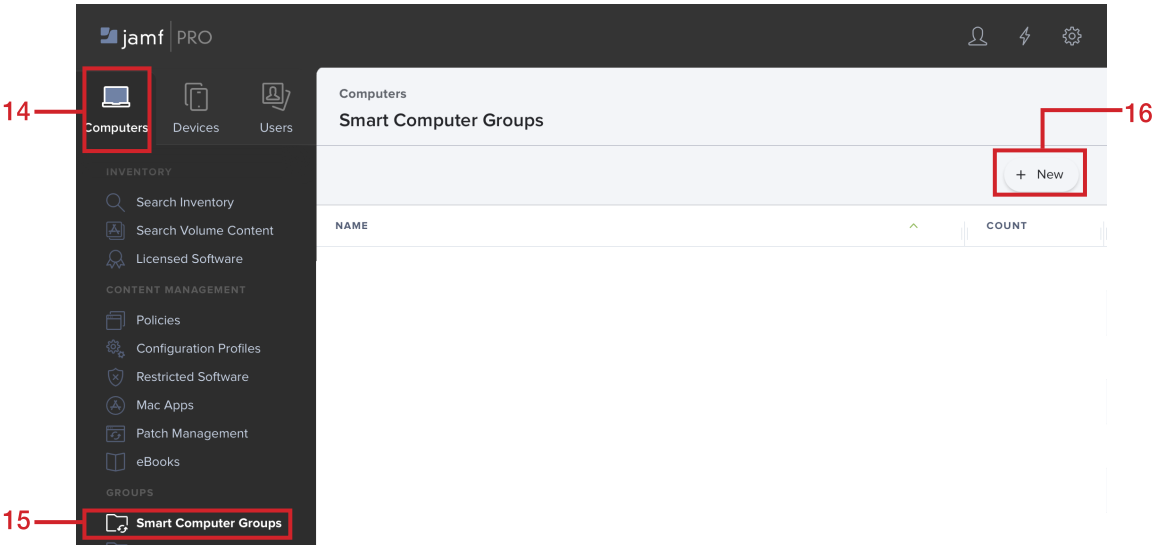
Property List PLIST containing key value pairs for settings in the specified domain.

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

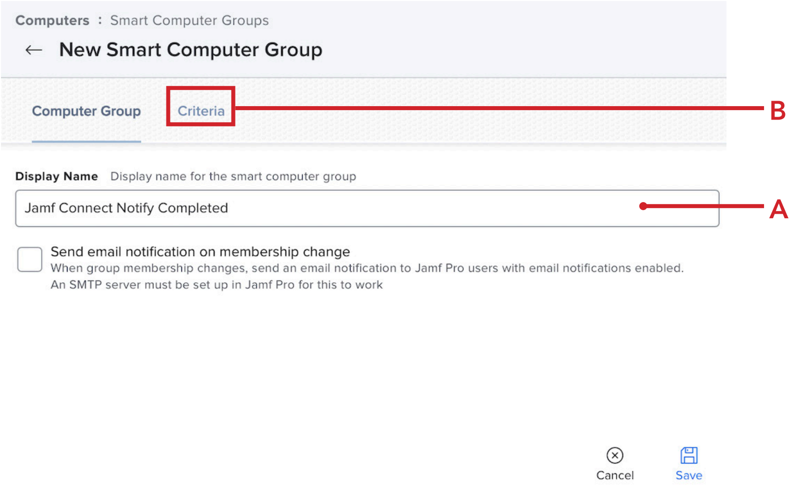
Required

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

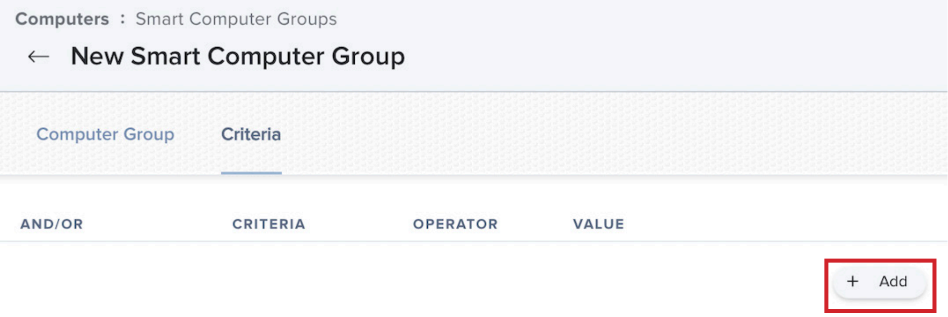


Display Name Display name for the smart computer group

Jamf Connect Notify Completed

□ Send email notification on membership change
When group membership changes, send an email notification to Jamf Pro users with email notifications enabled.
An SMTP server must be set up in Jamf Pro for this to work

18. Click Add.



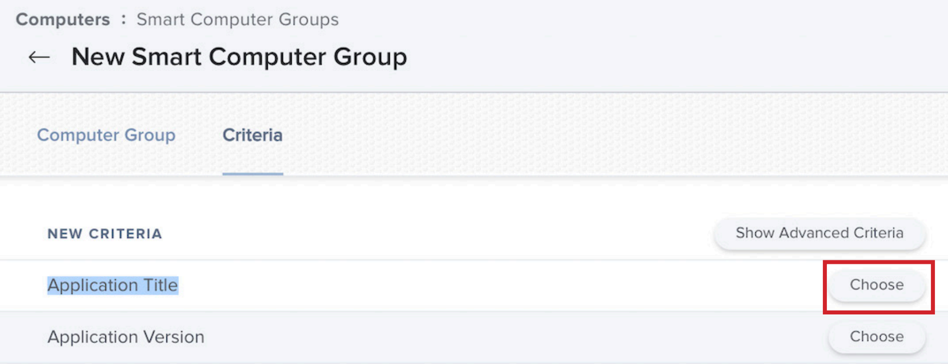
Computers : Smart Computer Groups

← New Smart Computer Group

Computer Group Criteria

AND/OR	CRITERIA	OPERATOR	VALUE

19. For Application Title, click Choose.



Computers : Smart Computer Groups

← New Smart Computer Group

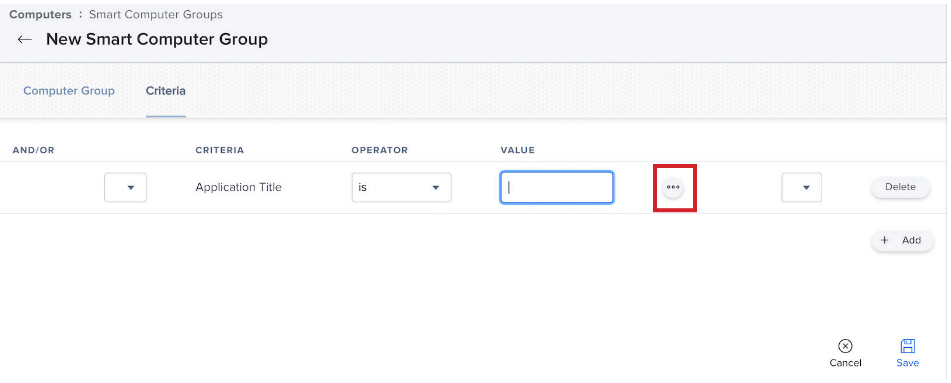
Computer Group Criteria

NEW CRITERIA

Application Title

Application Version

20. Click Choices (⋯).



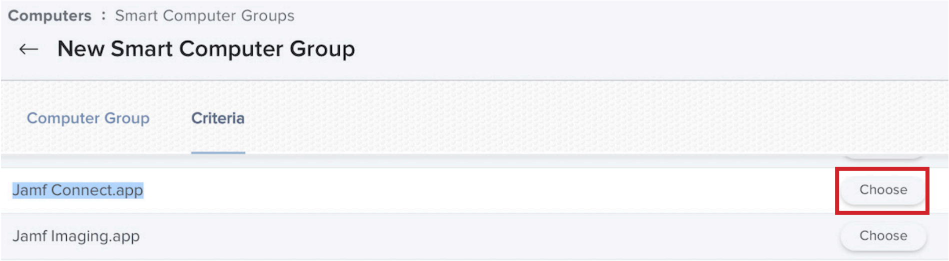
Computers : Smart Computer Groups

← New Smart Computer Group

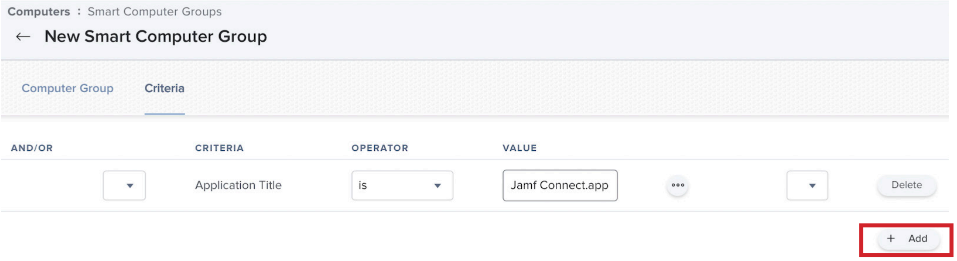
Computer Group Criteria

AND/OR	CRITERIA	OPERATOR	VALUE
▾	Application Title	is ▾	

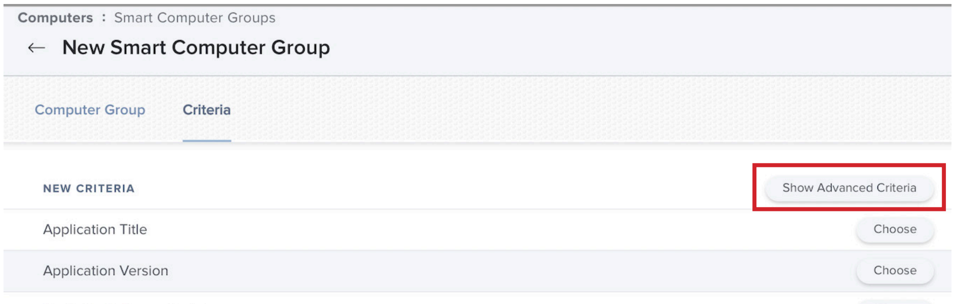
21. Scroll down until you find Jamf Connect.app, then click Choose.



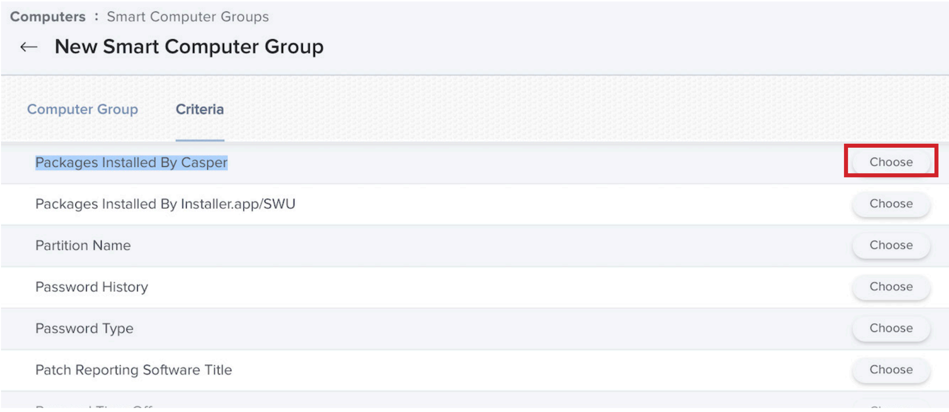
22. Click Add.



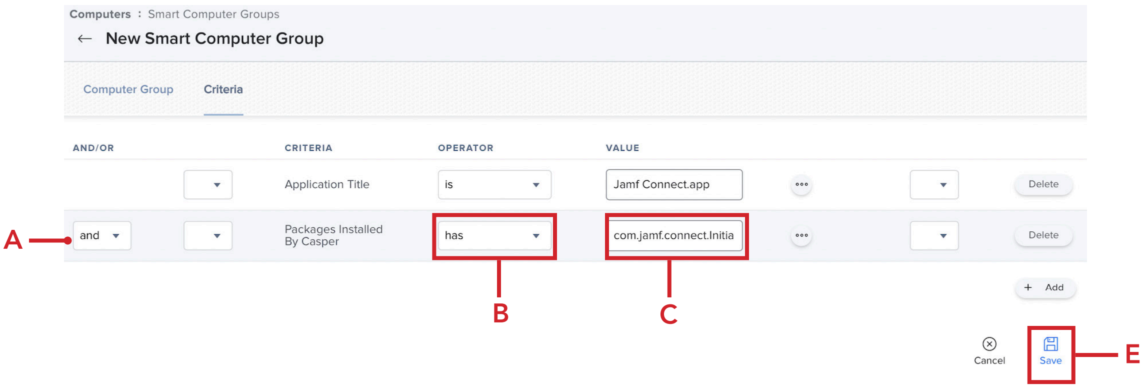
23. Click the Show Advanced Criteria button.



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


Computers : Smart Computer Groups
← New Smart Computer Group
Computer Group
Criteria
Packages Installed By Casper
Choose
Packages Installed By Installer.app/SWU
Choose
Partition Name
Choose
Password History
Choose
Password Type
Choose
Patch Reporting Software Title
Choose

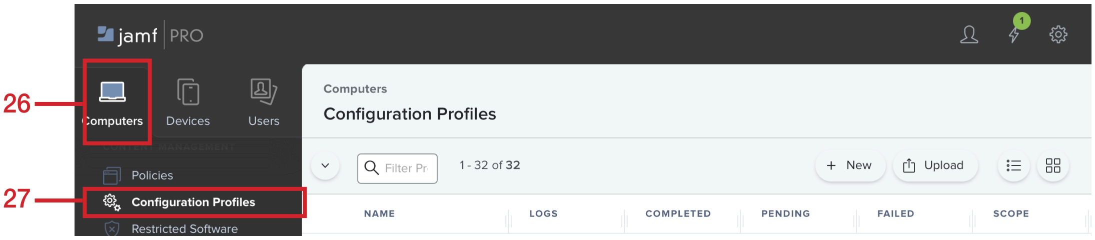
25. Configure the following:
    A. AND/OR: Make sure "and" is selected
    B. OPERATOR: has
    C. VALUE: com.jamf.connect.InitialRunDone.pkg
    D. Confirm your settings look like what is shown in the picture below
    E. Click Save
    NOTE: com.jamf.connect.InitialRunDone.pkg is case sensitive.



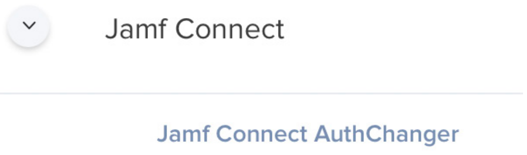
AND/OR		CRITERIA	OPERATOR	VALUE
		Application Title	is	Jamf Connect.app
and		Packages Installed By Casper	has	com.jamf.connect.Initia

26. Click Computers.

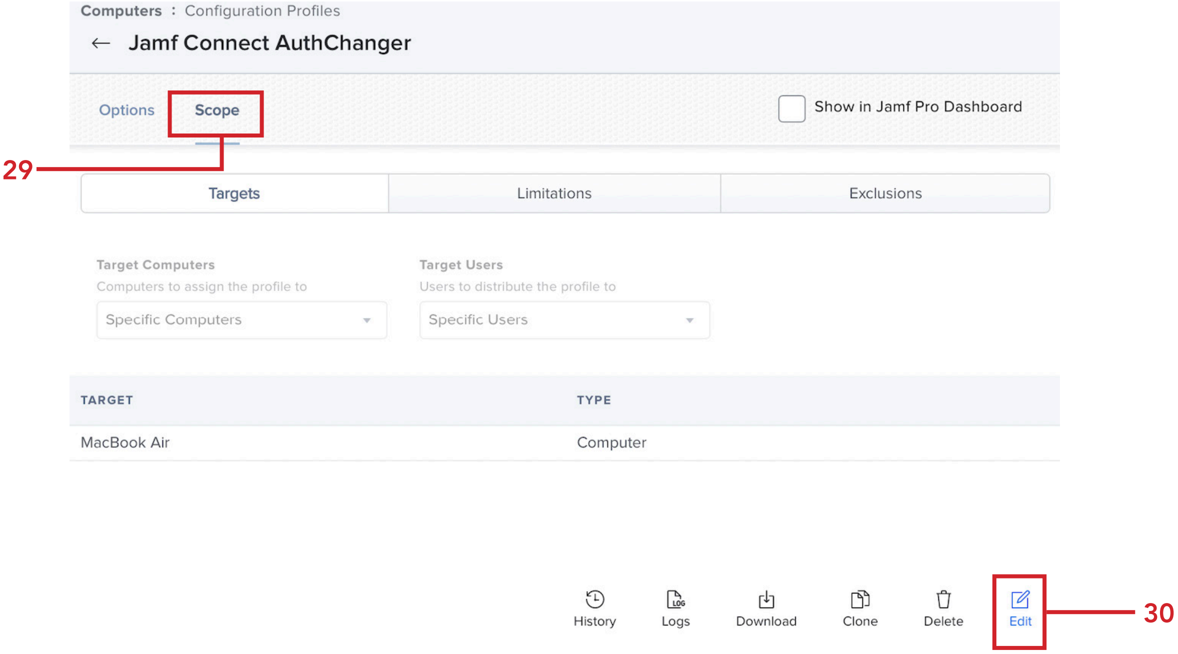
27. Click Configuration Profiles.



28. Click the Jamf Connect AuthChanger configuration profile.



29. Click Scope
30. Click Edit.



Computers : Configuration Profiles

← Jamf Connect AuthChanger

Options | Scope | □ Show in Jamf Pro Dashboard

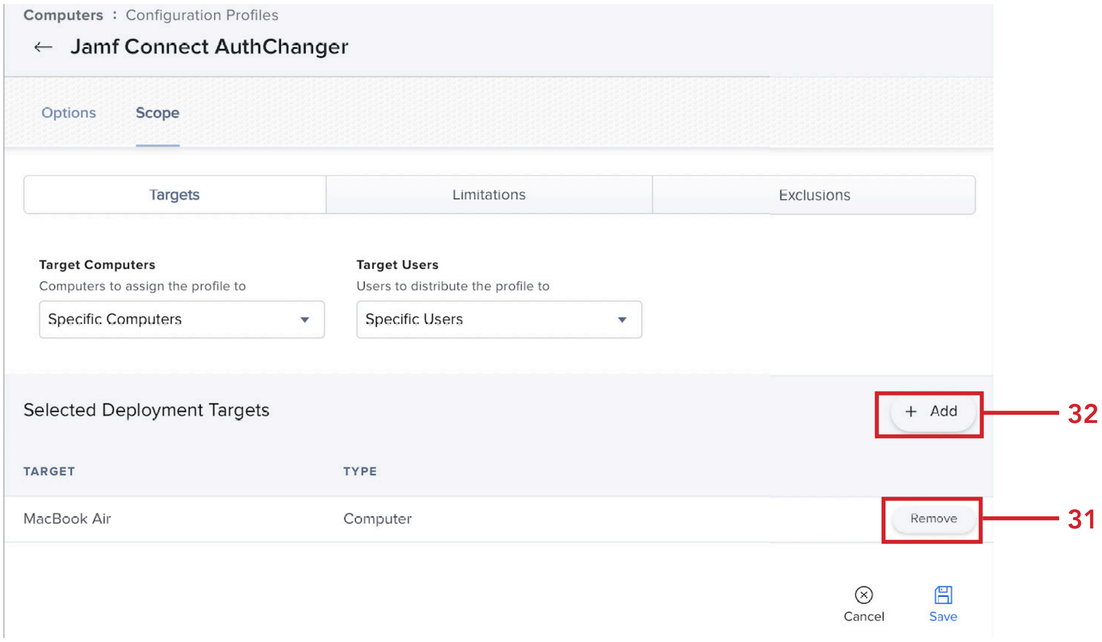
Targets | Limitations | Exclusions

Target Computers
Computers to assign the profile to
Specific Computers

Target Users
Users to distribute the profile to
Specific Users

TARGET	TYPE
MacBook Air	Computer

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



Computers : Configuration Profiles

← Jamf Connect AuthChanger

Options | Scope

Targets | Limitations | Exclusions

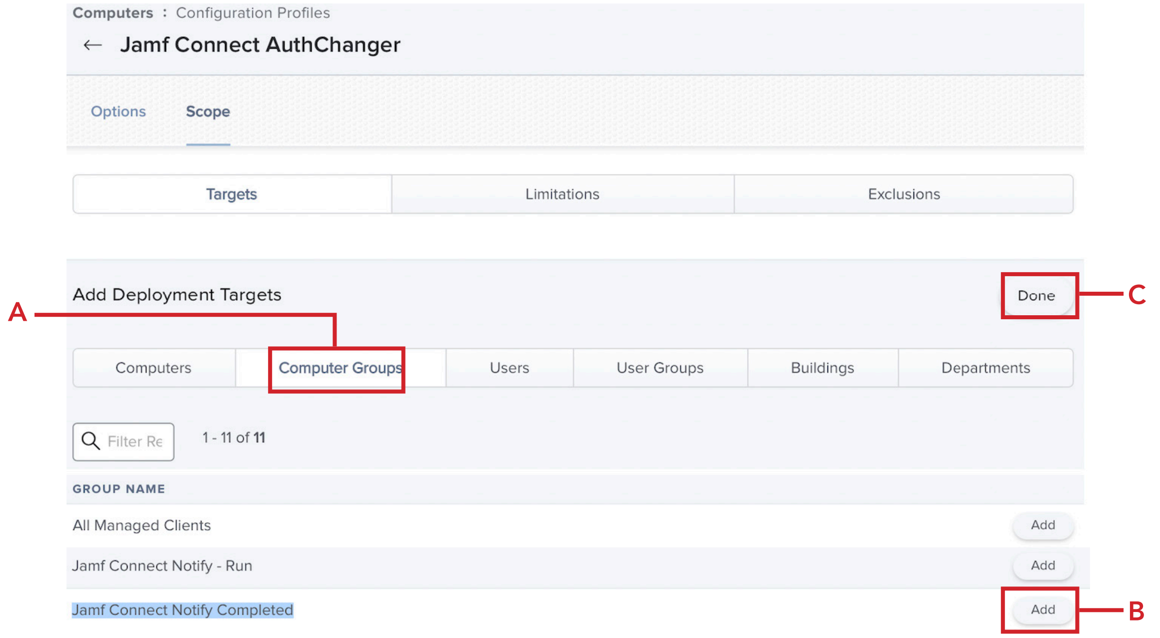
Target Computers
Computers to assign the profile to
Specific Computers

Target Users
Users to distribute the profile to
Specific Users

Selected Deployment Targets

TARGET	TYPE	
MacBook Air	Computer	Remove

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



Computers : Configuration Profiles

← Jamf Connect AuthChanger

Options Scope

Targets | Limitations | Exclusions

Add Deployment Targets

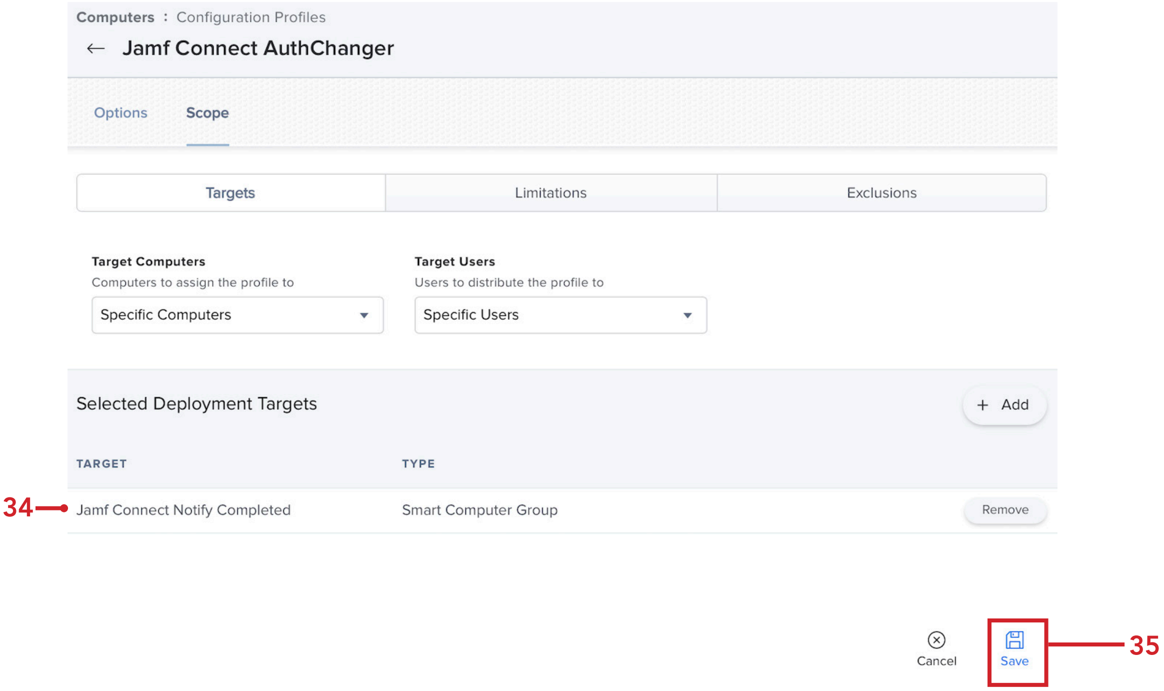
Computers | Computer Groups | Users | User Groups | Buildings | Departments

Filter Re 1 - 11 of 11

GROUP NAME	
All Managed Clients	Add
Jamf Connect Notify - Run	Add
Jamf Connect Notify Completed	Add

34. Confirm the Jamf Connect Notify Completed group is listed.

35. Click Save.
    NOTE: This will ensure that only Macs 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.



Computers : Configuration Profiles

← Jamf Connect AuthChanger

Options Scope

Targets | Limitations | Exclusions

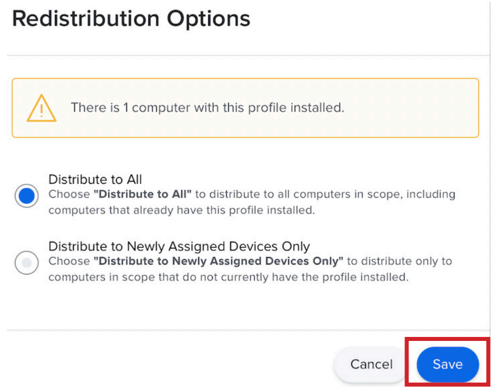
Target Computers
Computers to assign the profile to
Specific Computers

Target Users
Users to distribute the profile to
Specific Users

Selected Deployment Targets

TARGET	TYPE	
Jamf Connect Notify Completed	Smart Computer Group	Remove

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.



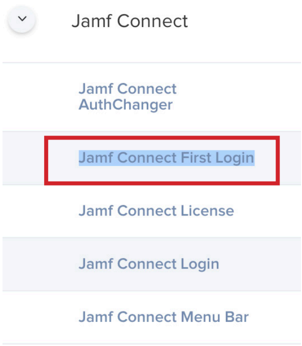
Redistribution Options

There is 1 computer with this profile installed.

● Distribute to All
Choose **"Distribute to All"** to distribute to all computers in scope, including computers that already have this profile installed.

○ Distribute to Newly Assigned Devices Only
Choose **"Distribute to Newly Assigned Devices Only"** to distribute only to computers in scope that do not currently have the profile installed.

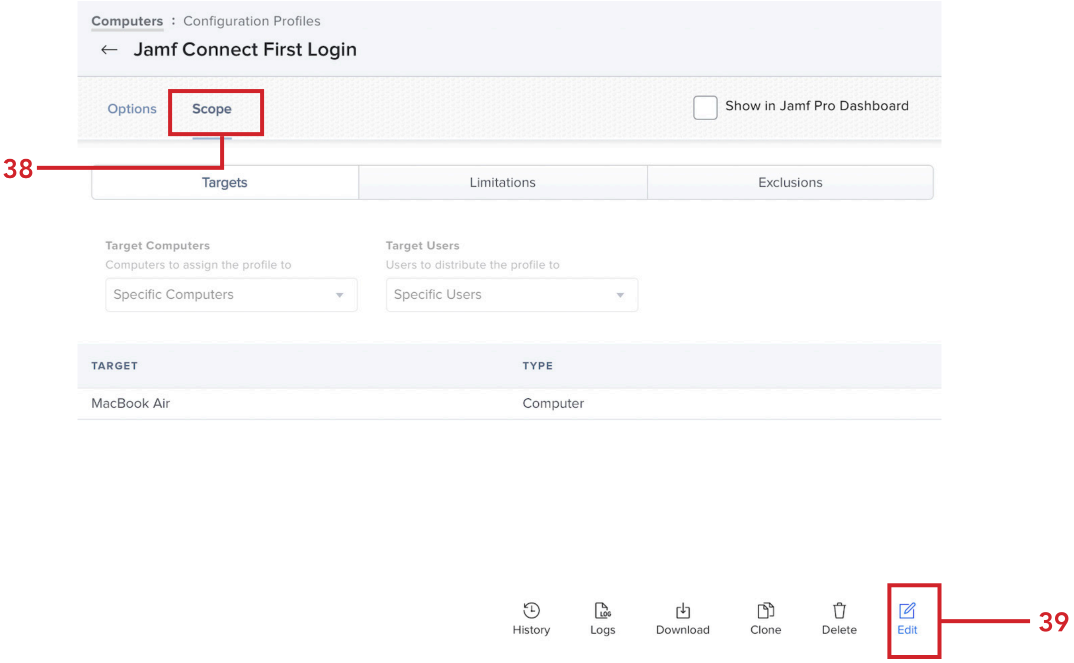
37. Click the Jamf Connect First Login configuration profile.



Jamf Connect

- Jamf Connect AuthChanger
- Jamf Connect First Login
- Jamf Connect License
- Jamf Connect Login
- Jamf Connect Menu Bar

38. Click Scope.
39. Click Edit.



Computers : Configuration Profiles

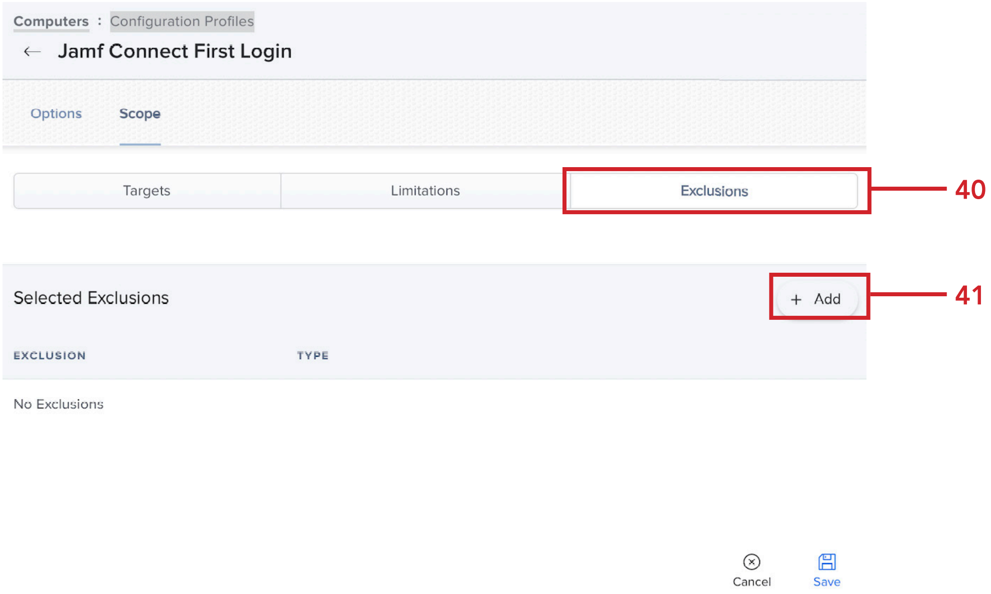
← Jamf Connect First Login

Target Computers
Computers to assign the profile to
Specific Computers

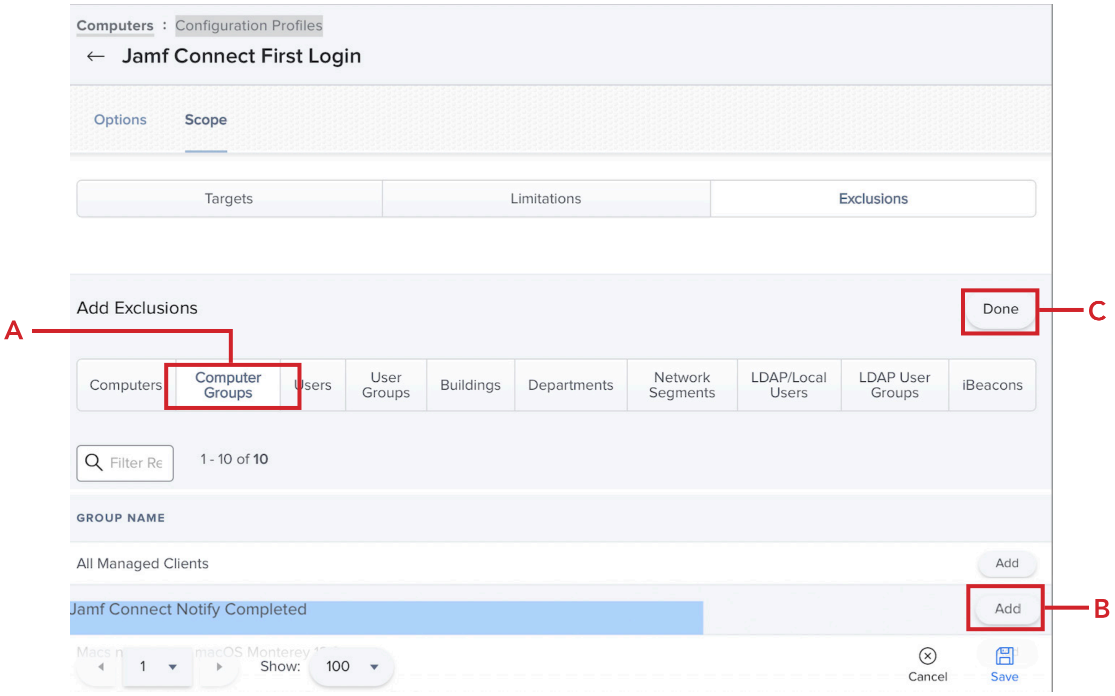
Target Users
Users to distribute the profile to
Specific Users

TARGET	TYPE
MacBook Air	Computer

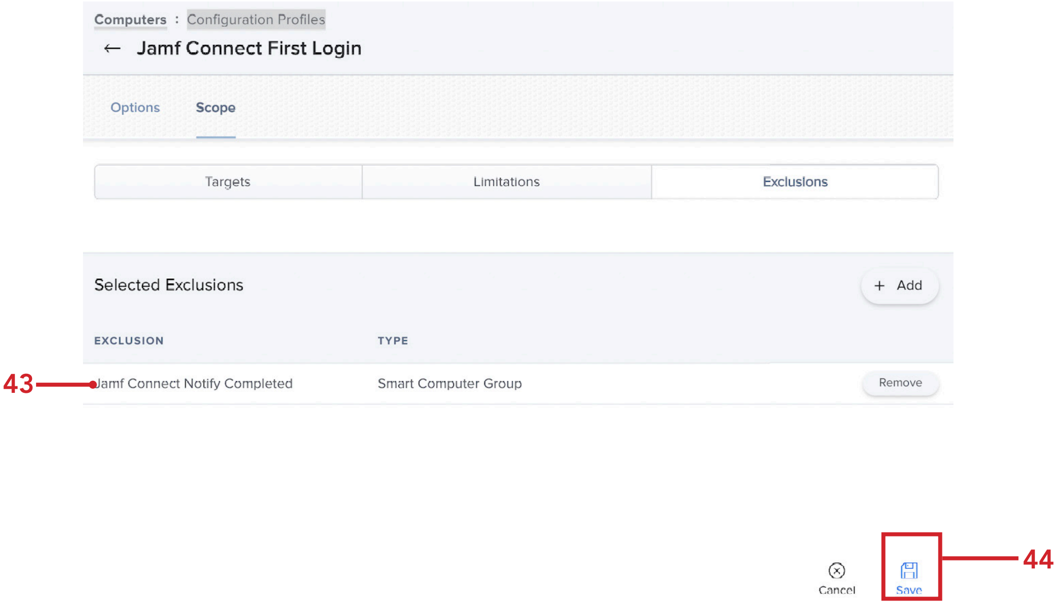
40. Click Exclusions.
41. Click Add.



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



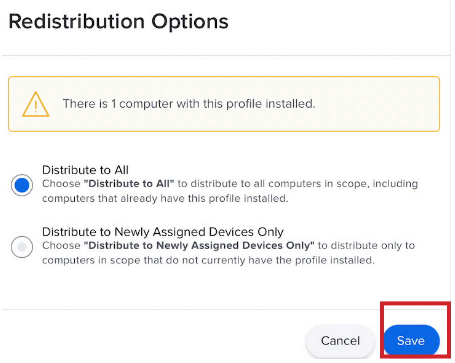
43. Confirm the Jamf Connect Notify Completed group is listed.
44. Click Save.
    NOTE: This will ensure that the Jamf Connect First Login profile gets removed from a Mac Computer once Jamf Connect has been installed and Notify has run. This will stop Notify and the EULA from running at every login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



Selected Exclusions

EXCLUSION	TYPE
Jamf Connect Notify Completed	Smart Computer Group

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.



Redistribution Options

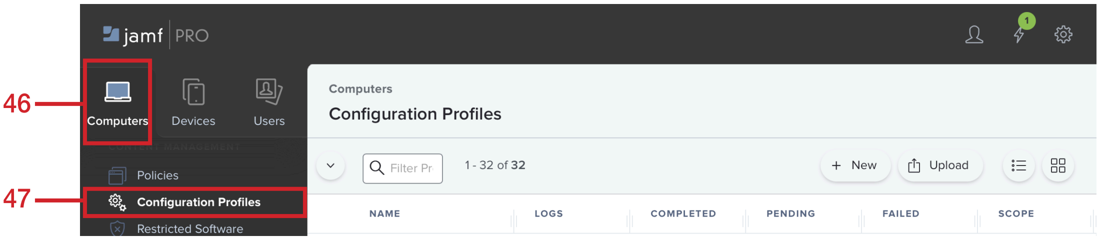
There is 1 computer with this profile installed.

● Distribute to All
Choose **"Distribute to All"** to distribute to all computers in scope, including computers that already have this profile installed.

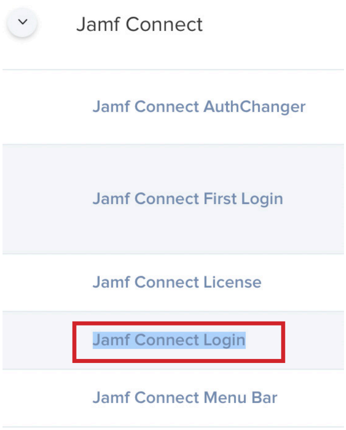
○ Distribute to Newly Assigned Devices Only
Choose **"Distribute to Newly Assigned Devices Only"** to distribute only to computers in scope that do not currently have the profile installed.

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.



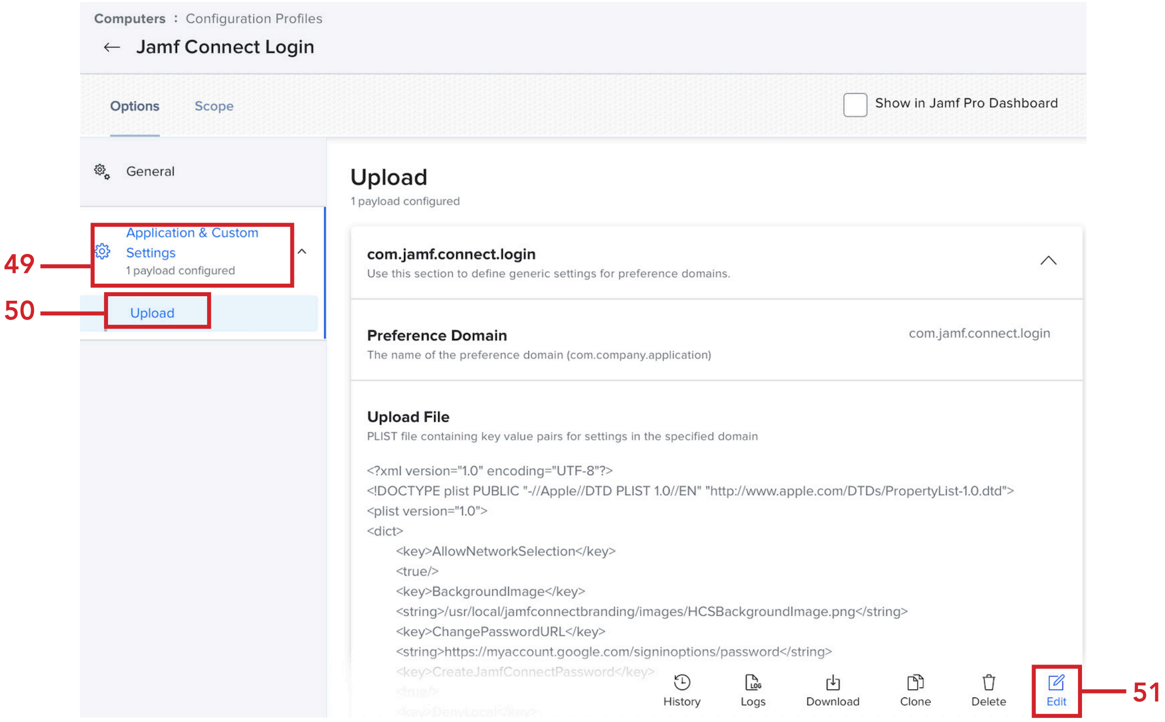
48. Click the Jamf Connect Login configuration profile.



49. Expand the Application & Custom Settings payload.

50. Click Upload,

51. Click Edit.



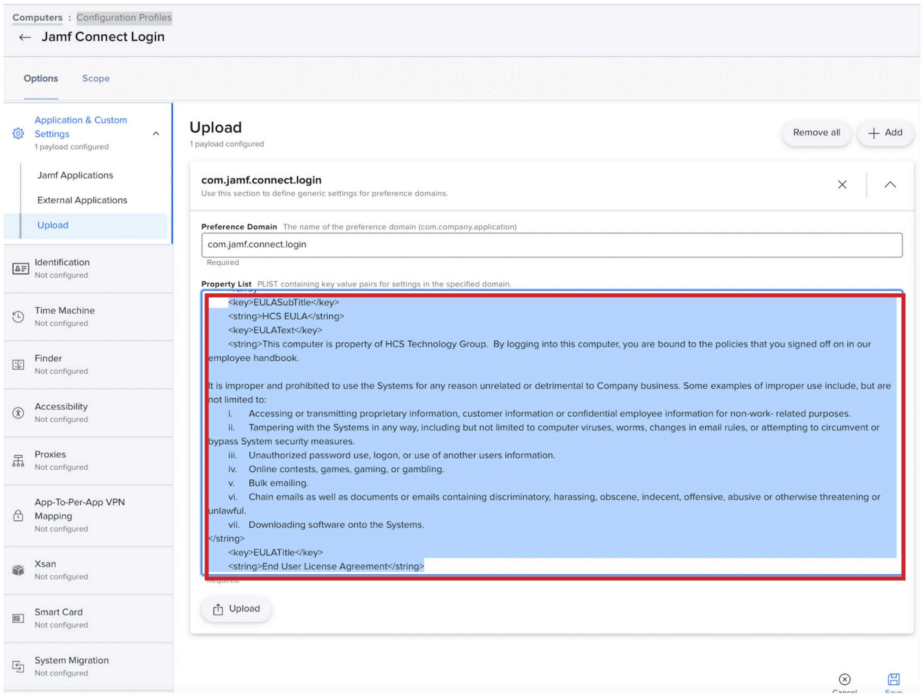
com.jamf.connect.login
Use this section to define generic settings for preference domains.

Preference Domain: com.jamf.connect.login
The name of the preference domain (com.company.application)

Upload File
PLIST file containing key value pairs for settings in the specified domain

```
<?xml version="1.0" encoding="UTF-8"?>
<!DOCTYPE plist PUBLIC "-//Apple//DTD PLIST 1.0//EN" "http://www.apple.com/DTDs/PropertyList-1.0.dtd">
<plist version="1.0">
<dict>
	<key>AllowNetworkSelection</key>
	<true/>
	<key>BackgroundImage</key>
	<string>/usr/local/jamfconnectbranding/images/HCSBackgroundImage.png</string>
	<key>ChangePasswordURL</key>
	<string>https://myaccount.google.com/signinoptions/password</string>
	<key>CreateJamfConnectPassword</key>
	<true/>
	<key>DenyLocal</key>
```

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.



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

com.jamf.connect.login

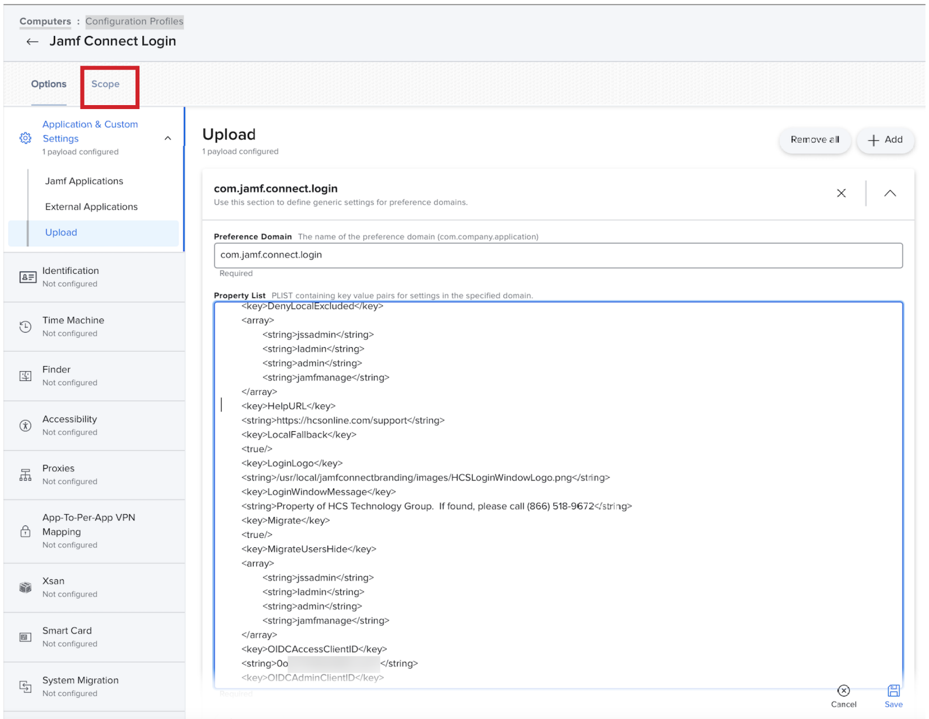
Required

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

```
	<key>EULASubTitle</key>
	<string>HCS EULA</string>
	<key>EULAText</key>
	<string>This computer is property of HCS Technology Group.  By logging into this computer, you are bound to the policies that you signed off on in our employee handbook.

It is improper and prohibited to use the Systems for any reason unrelated or detrimental to Company business. Some examples of improper use include, but are not limited to:
	i.	Accessing or transmitting proprietary information, customer information or confidential employee information for non-work- related purposes.
	ii.	Tampering with the Systems in any way, including but not limited to computer viruses, worms, changes in email rules, or attempting to circumvent or bypass System security measures.
	iii.	Unauthorized password use, logon, or use of another users information.
	iv.	Online contests, games, gaming, or gambling.
	v.	Bulk emailing.
	vi.	Chain emails as well as documents or emails containing discriminatory, harassing, obscene, indecent, offensive, abusive or otherwise threatening or unlawful.
	vii.	Downloading software onto the Systems.
</string>
	<key>EULATitle</key>
	<string>End User License Agreement</string>
```

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



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

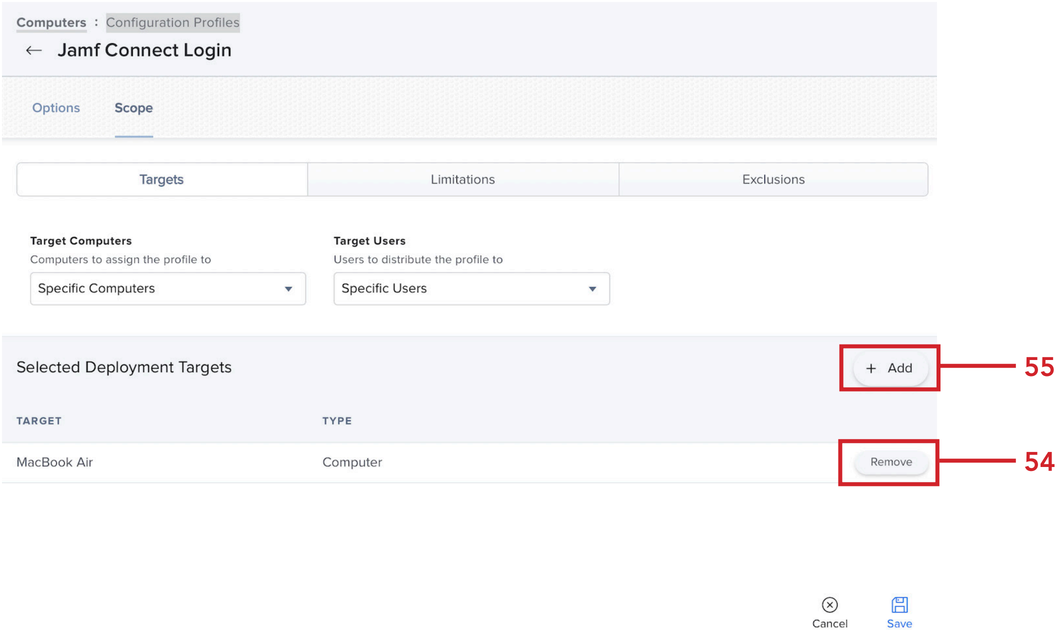
com.jamf.connect.login

Required

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

```
	<key>DenyLocalExcluded</key>
	<array>
		<string>jssadmin</string>
		<string>ladmin</string>
		<string>admin</string>
		<string>jamfmanage</string>
	</array>
	<key>HelpURL</key>
	<string>https://hcsonline.com/support</string>
	<key>LocalFallback</key>
	<true/>
	<key>LoginLogo</key>
	<string>/usr/local/jamfconnectbranding/images/HCSLoginWindowLogo.png</string>
	<key>LoginWindowMessage</key>
	<string>Property of HCS Technology Group.  If found, please call (866) 518-9672</string>
	<key>Migrate</key>
	<true/>
	<key>MigrateUsersHide</key>
	<array>
		<string>jssadmin</string>
		<string>ladmin</string>
		<string>admin</string>
		<string>jamfmanage</string>
	</array>
	<key>OIDCAccessClientID</key>
	<string>0o[redacted]</string>
	<key>OIDCAdminClientID</key>
```

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



Computers : Configuration Profiles

Jamf Connect Login

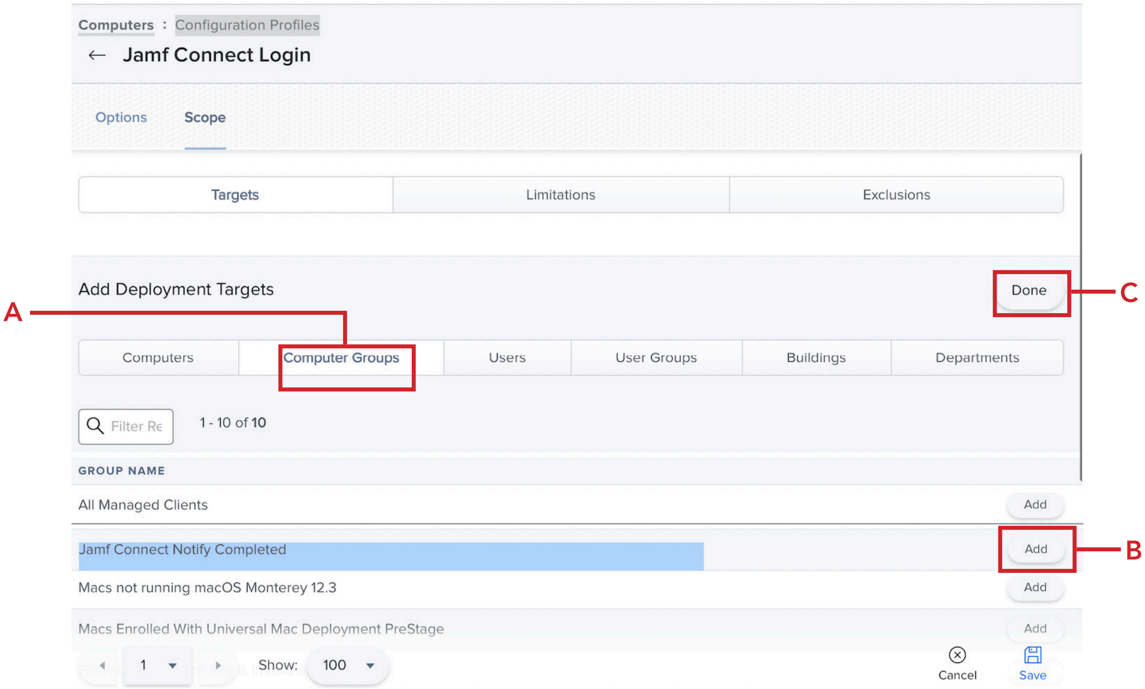
Target Computers
Computers to assign the profile to
Specific Computers

Target Users
Users to distribute the profile to
Specific Users

Selected Deployment Targets

TARGET	TYPE
MacBook Air	Computer

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



Computers : Configuration Profiles

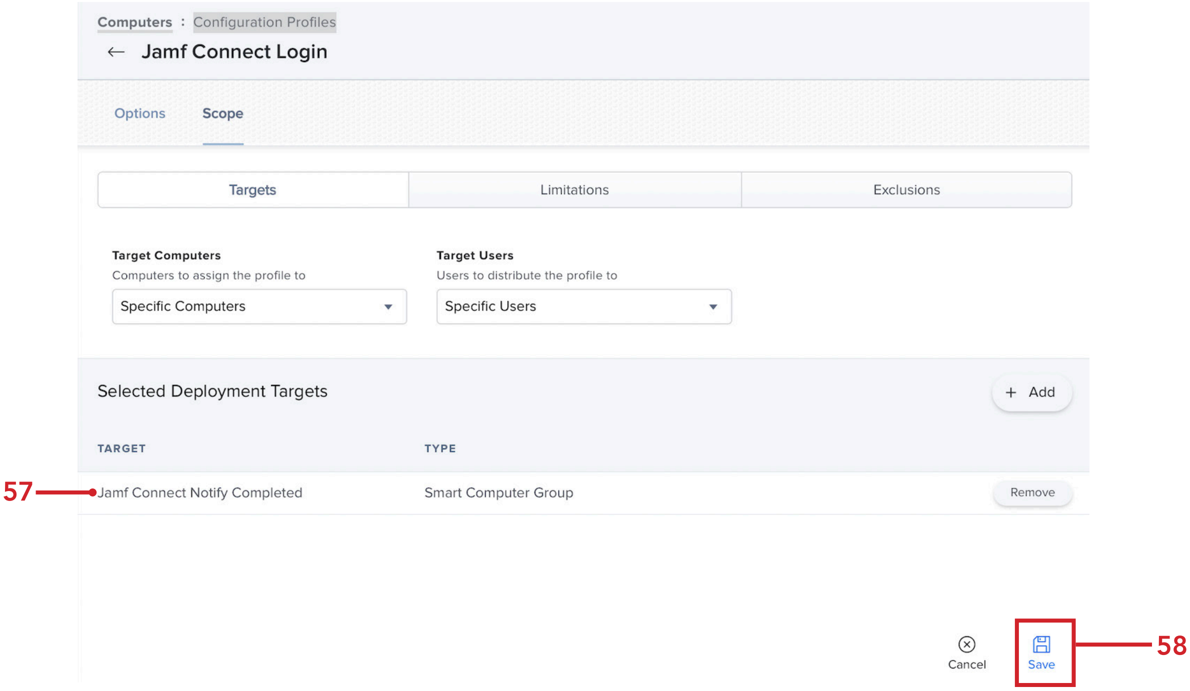
Jamf Connect Login

Add Deployment Targets

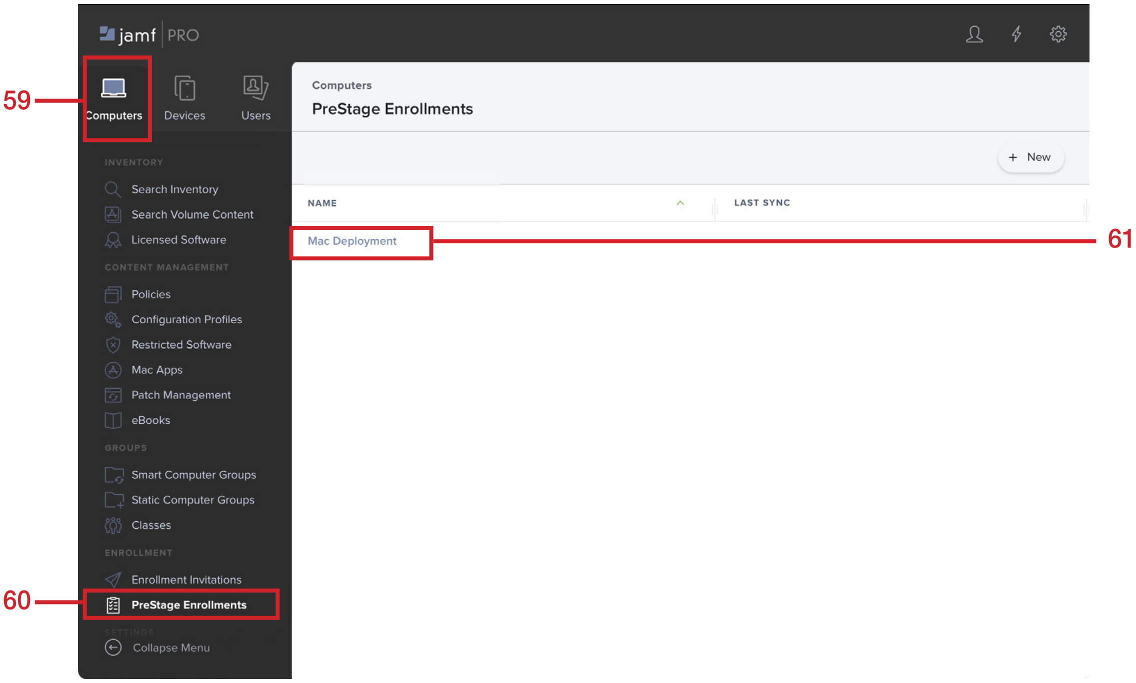
1 - 10 of 10

GROUP NAME	
All Managed Clients	Add
Jamf Connect Notify Completed	Add
Macs not running macOS Monterey 12.3	Add
Macs Enrolled With Universal Mac Deployment PreStage	Add

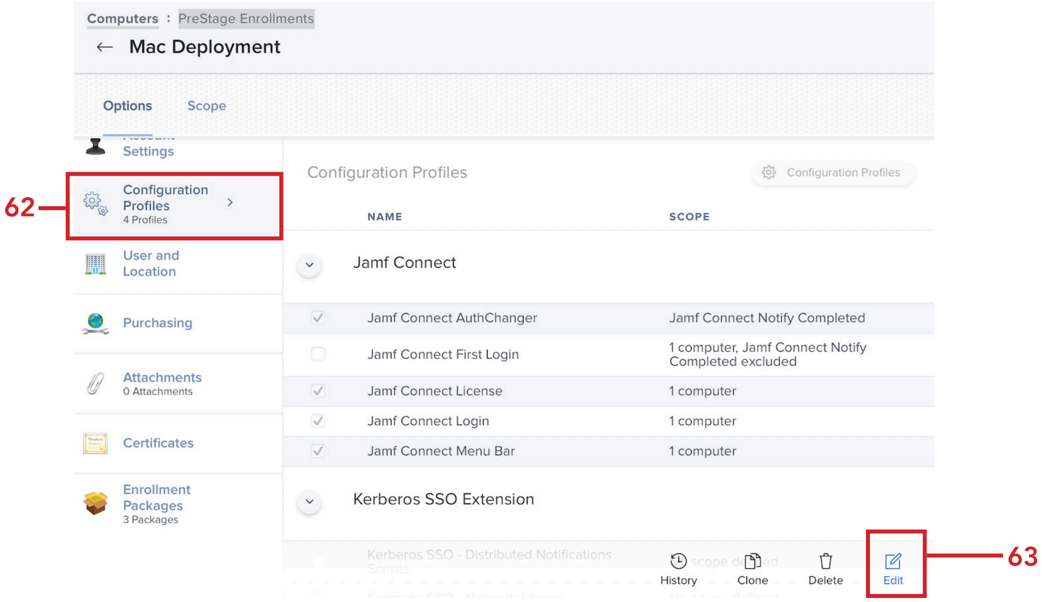
57. Confirm the Jamf Connect Notify Completed group was added
58. Click Save.



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

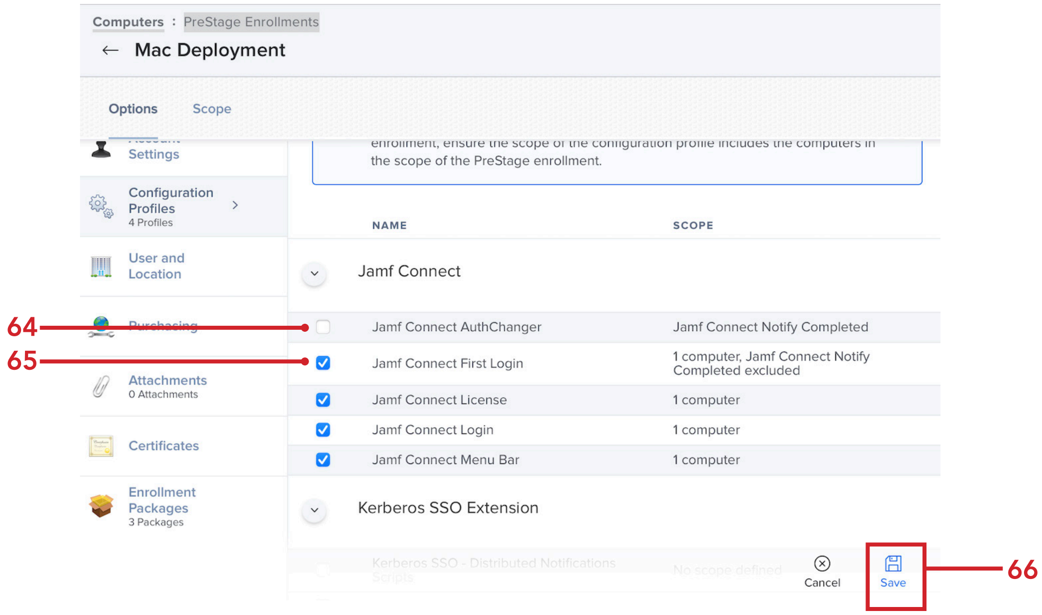


62. Select the Configuration Profiles payload
63. Click Edit.



	NAME	SCOPE
	Jamf Connect	
✓	Jamf Connect AuthChanger	Jamf Connect Notify Completed
□	Jamf Connect First Login	1 computer, Jamf Connect Notify Completed excluded
✓	Jamf Connect License	1 computer
✓	Jamf Connect Login	1 computer
✓	Jamf Connect Menu Bar	1 computer
	Kerberos SSO Extension	
	Kerberos SSO - Distributed Notifications Scripts	

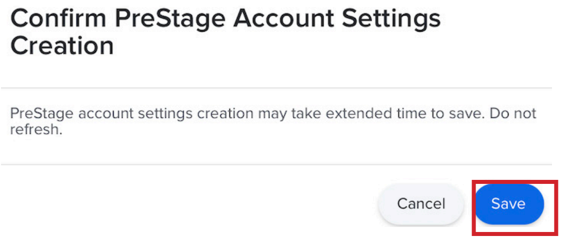
64. Deselect the checkbox for Jamf Connect AuthChanger profile.
65. Select the checkbox for Jamf Connect First Login profile.
66. Click Save.



enrollment, ensure the scope of the configuration profile includes the computers in the scope of the PreStage enrollment.

	NAME	SCOPE
	Jamf Connect	
□	Jamf Connect AuthChanger	Jamf Connect Notify Completed
☑	Jamf Connect First Login	1 computer, Jamf Connect Notify Completed excluded
☑	Jamf Connect License	1 computer
☑	Jamf Connect Login	1 computer
☑	Jamf Connect Menu Bar	1 computer
	Kerberos SSO Extension	
	Kerberos SSO - Distributed Notifications Scripts	No scope defined

67. Click Save.



Confirm PreStage Account Settings Creation

PreStage account settings creation may take extended time to save. Do not refresh.

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 with Jamf Connect Notify

What You’ll Need

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

Hardware and Software

Requirements for following along with this section:

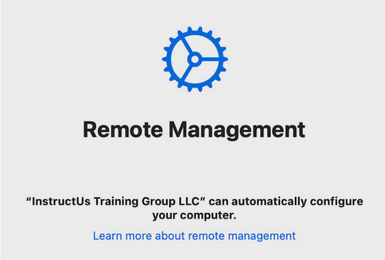
- A Mac that’s brand new in the box or an old Mac that is at Setup Assistant (10.15.4 or later). The Mac must be enrolled in Apple Business Manager or Apple School Manager and assigned to your PreStage in Jamf Pro. This is required for Automated Device Enrollment scoped in a PreStage.
- Google login credentials.

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.

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 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 not longer on the Mac after Notify runs and the AuthChanger profile is installed after Notify has completed.

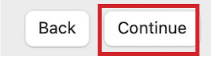
1. At the Remote Management screen, click Continue.



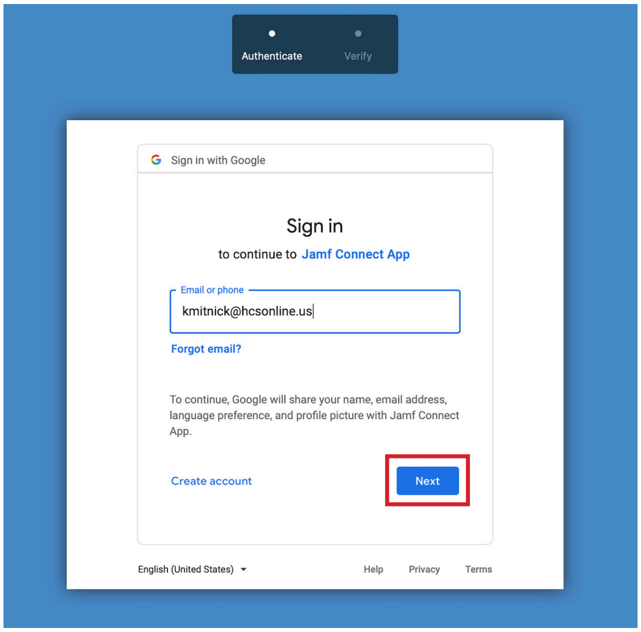
Remote Management

“InstructUs Training Group LLC” can automatically configure your computer.

Learn more about remote management



2. Enter your Google Email address then click Next.



Sign in

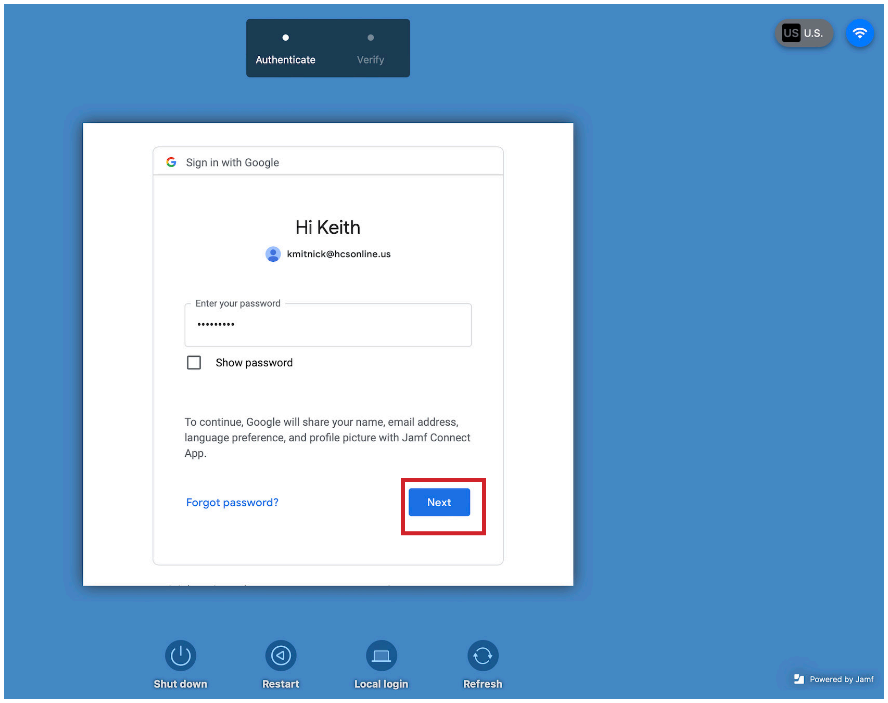
to continue to Jamf Connect App

Email or phone: kmitnick@hcsonline.us

Forgot email?

To continue, Google will share your name, email address, language preference, and profile picture with Jamf Connect App.

3. Enter your Google password then click Next.



Sign in with Google

Hi Keith

kmitnick@hcsonline.us

Enter your password

•••••••••

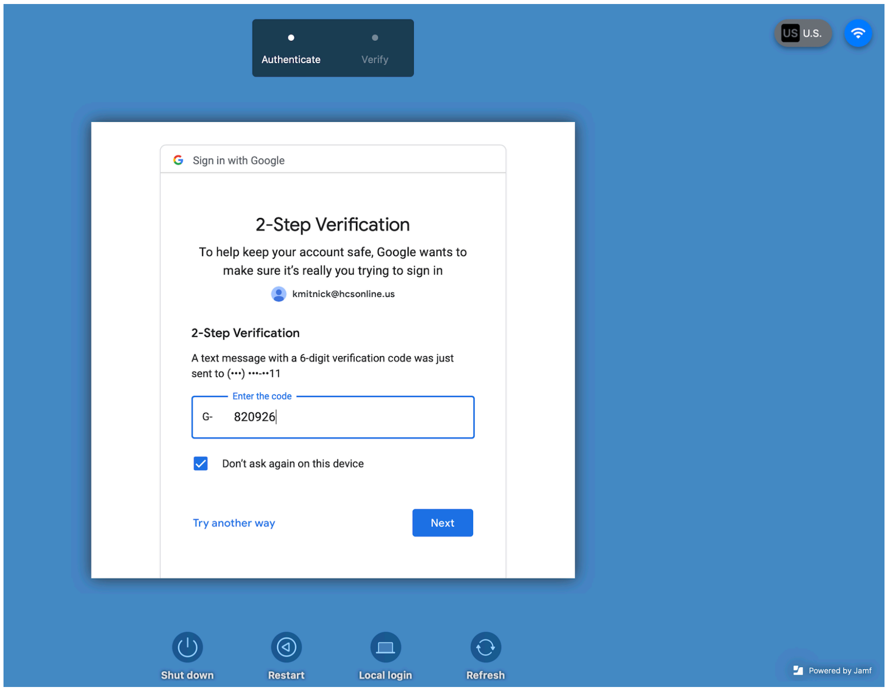
□ Show password

To continue, Google will share your name, email address, language preference, and profile picture with Jamf Connect App.

Forgot password?

Next

4. You will be prompted with the 2-Step Verification message below and a code will be sent to your phone. Enter the code and click Next.



Sign in with Google

2-Step Verification

To help keep your account safe, Google wants to make sure it's really you trying to sign in

kmitnick@hcsonline.us

2-Step Verification

A text message with a 6-digit verification code was just sent to (•••) •••-••11

Enter the code

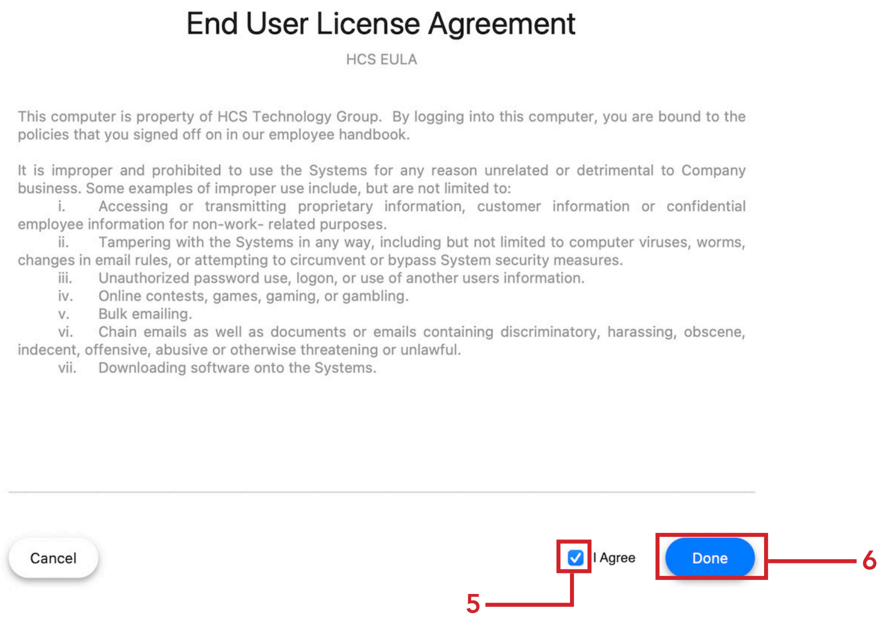
G- 820926

☑ Don't ask again on this device

Try another way

Next

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



End User License Agreement

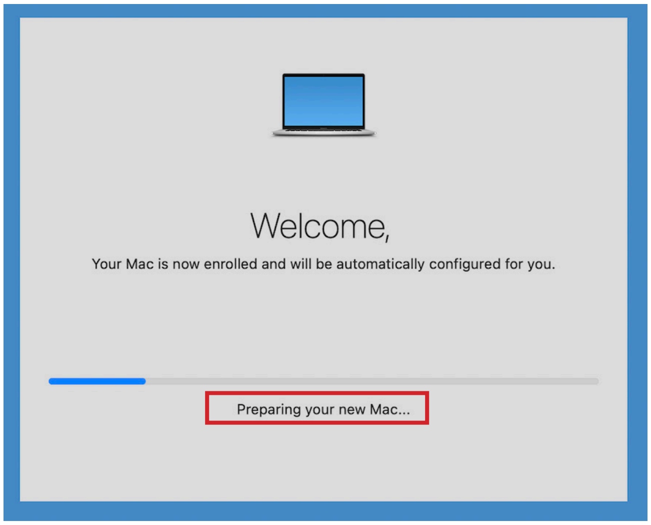
HCS EULA

This computer is property of HCS Technology Group. By logging into this computer, you are bound to the policies that you signed off on in our employee handbook.

It is improper and prohibited to use the Systems for any reason unrelated or detrimental to Company business. Some examples of improper use include, but are not limited to:

i. Accessing or transmitting proprietary information, customer information or confidential employee information for non-work- related purposes.
ii. Tampering with the Systems in any way, including but not limited to computer viruses, worms, changes in email rules, or attempting to circumvent or bypass System security measures.
iii. Unauthorized password use, logon, or use of another users information.
iv. Online contests, games, gaming, or gambling.
v. Bulk emailing.
vi. Chain emails as well as documents or emails containing discriminatory, harassing, obscene, indecent, offensive, abusive or otherwise threatening or unlawful.
vii. Downloading software onto the Systems.

7. The Notify welcome screen will be displayed.

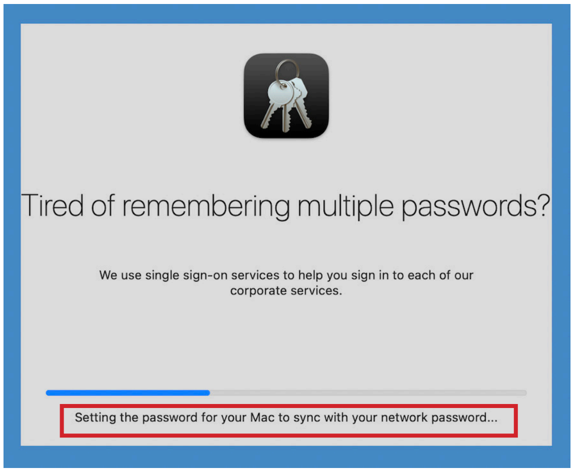


Welcome,

Your Mac is now enrolled and will be automatically configured for you.

Preparing your new Mac...

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

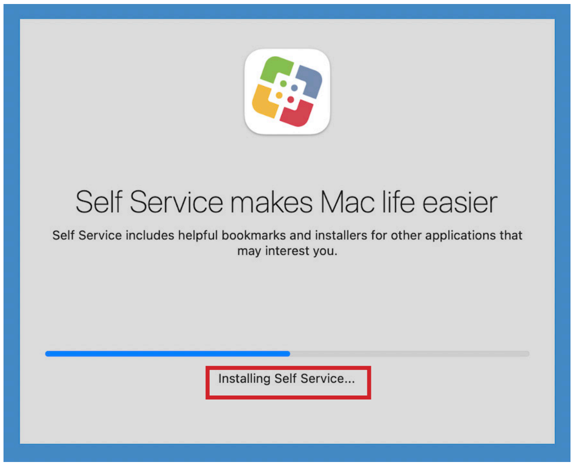


Tired of remembering multiple passwords?

We use single sign-on services to help you sign in to each of our corporate services.

Setting the password for your Mac to sync with your network password...

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

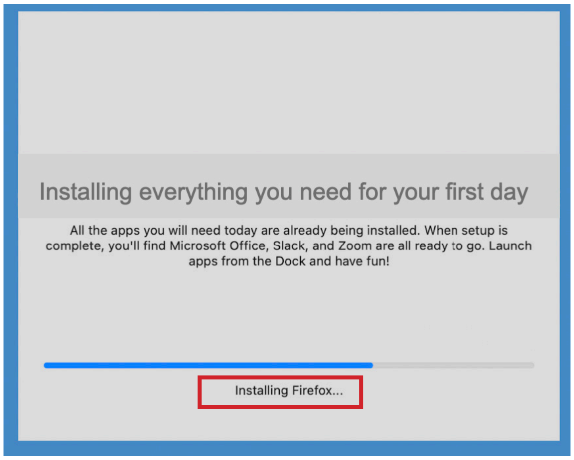


Self Service makes Mac life easier

Self Service includes helpful bookmarks and installers for other applications that may interest you.

Installing Self Service...

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

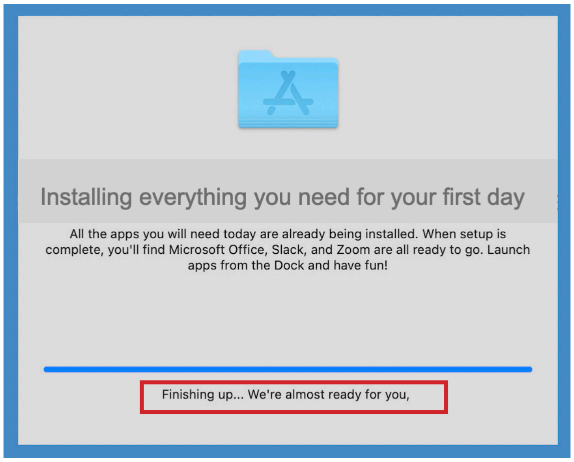


Installing everything you need for your first day

All the apps you will need today are already being installed. When setup is complete, you'll find Microsoft Office, Slack, and Zoom are all ready to go. Launch apps from the Dock and have fun!

Installing Firefox...

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

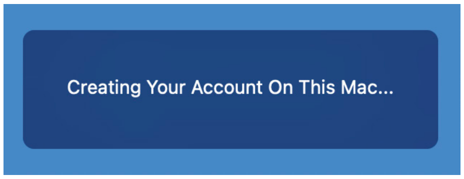


Installing everything you need for your first day

All the apps you will need today are already being installed. When setup is complete, you'll find Microsoft Office, Slack, and Zoom are all ready to go. Launch apps from the Dock and have fun!

Finishing up... We're almost ready for you,

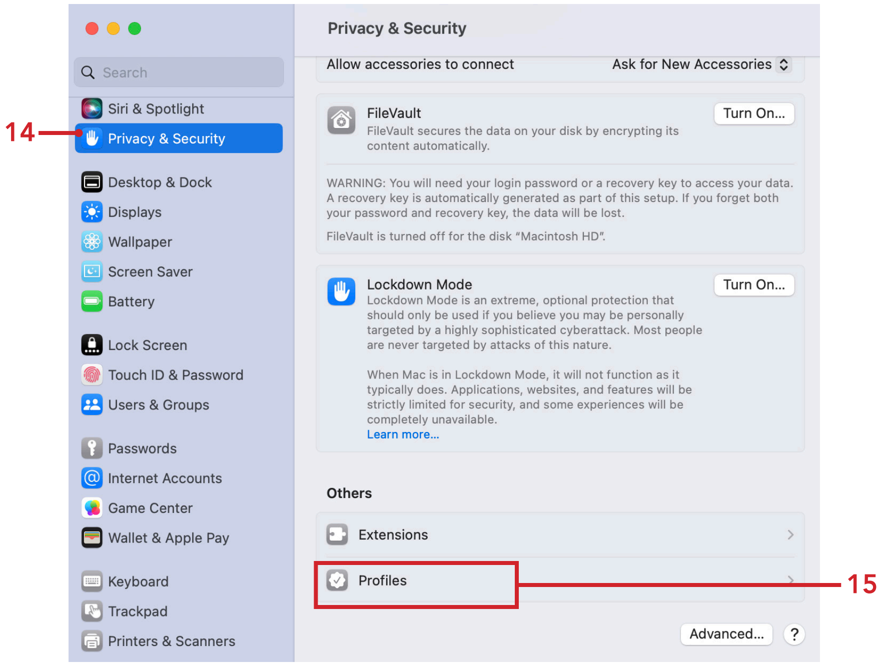
12. When Notify is done, Your account will be created on the Mac.



Creating Your Account On This Mac...

13. Open System Settings.

14. Click Privacy & Security.
15. Click Profiles



Privacy & Security

Allow accessories to connect — Ask for New Accessories

FileVault — Turn On...
FileVault secures the data on your disk by encrypting its content automatically.

WARNING: You will need your login password or a recovery key to access your data. A recovery key is automatically generated as part of this setup. If you forget both your password and recovery key, the data will be lost.

FileVault is turned off for the disk "Macintosh HD".

Lockdown Mode — Turn On...
Lockdown Mode is an extreme, optional protection that should only be used if you believe you may be personally targeted by a highly sophisticated cyberattack. Most people are never targeted by attacks of this nature.

When Mac is in Lockdown Mode, it will not function as it typically does. Applications, websites, and features will be strictly limited for security, and some experiences will be completely unavailable.
Learn more...

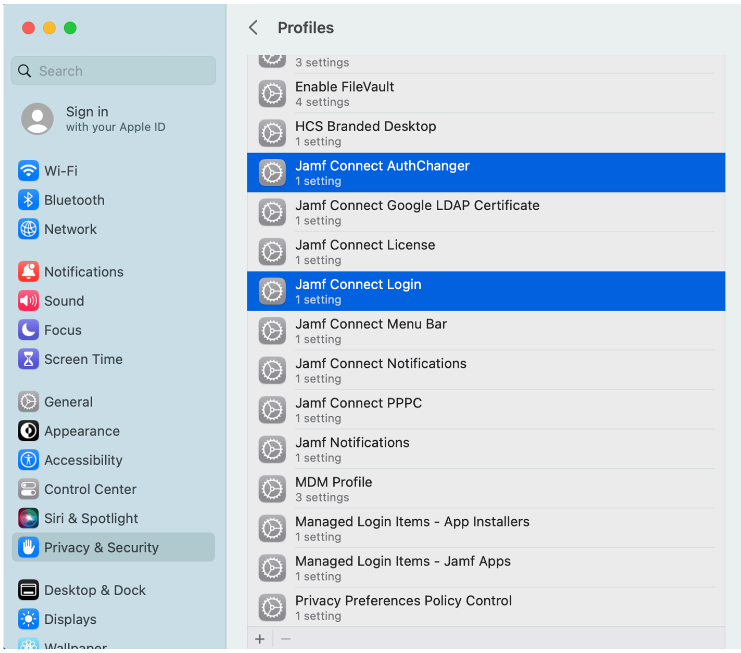
Others

Extensions

Profiles

Advanced... ?

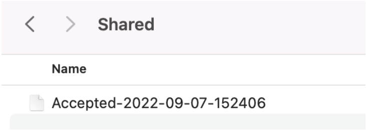
16. Confirm the Jamf Connect First Login profile is no longer installed and the Jamf Connect AuthChanger and Jamf Connect Login profile is installed. Quit System Settings when done.



Profiles

3 settings
Enable FileVault — 4 settings
HCS Branded Desktop — 1 setting
Jamf Connect AuthChanger — 1 setting
Jamf Connect Google LDAP Certificate — 1 setting
Jamf Connect License — 1 setting
Jamf Connect Login — 1 setting
Jamf Connect Menu Bar — 1 setting
Jamf Connect Notifications — 1 setting
Jamf Connect PPPC — 1 setting
Jamf Notifications — 1 setting
MDM Profile — 3 settings
Managed Login Items - App Installers — 1 setting
Managed Login Items - Jamf Apps — 1 setting
Privacy Preferences Policy Control — 1 setting

17. 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.
    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 that contain that file which means the EULA has been accepted by the user. This is great for reporting purposes.



Accepted-2022-09-07-152406

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.

This completes this guide.