jamf | CONNECT

Using Jamf Connect with G Suite Cloud Identity

HCS TECHNOLOGY GROUP

Contents

With so much of today's workforce accessing resources remotely, organizations may have a need to provide account management in the form of an Identity Provider (IdP). One such provider is Google, which has a service called Cloud Identity (https://cloud.google.com/identity). Jamf Connect is a platform that allows provisioning of users using credentials from their Identity Provider and allows those credentials to stay in sync. There are three components to Jamf Connect:

- Jamf Connect Login: Allows administrators to manage authentication at the macOS login window.
- Jamf Connect Verify: Specific to use with Microsoft Azure AD & PingFederate. An app that appears in the menu bar to assist in keeping every user's local account password in sync with their IdP account password.
- Jamf Connect Sync: Specific to use with Okta. An app that appears in the menu bar to assist in keeping every user's local account password in sync with their IdP account password.

This guide shows you how to configure, deploy, and use Jamf Connect Login, leveraging Google as the Cloud Identity Provider.

Benefits of a cloud identity provider:

- Allow access outside of a local authentication server
- Centralize security management
- Create efficiency for the end user with a single set of credentials
- Reduce IT overhead by decreasing the number of password reset requests

The following was used for this guide:

- 2016 MacBook Pro
- macOS Catalina 10.15.4
- Jamf Pro 10.20.1
- Google Cloud Identity Premium
- Jamf Connect 1.19.1
  You can download Jamf Connect as a 30 day trial, available here:
  https://www.jamf.com/request-trial/jamf-connect/

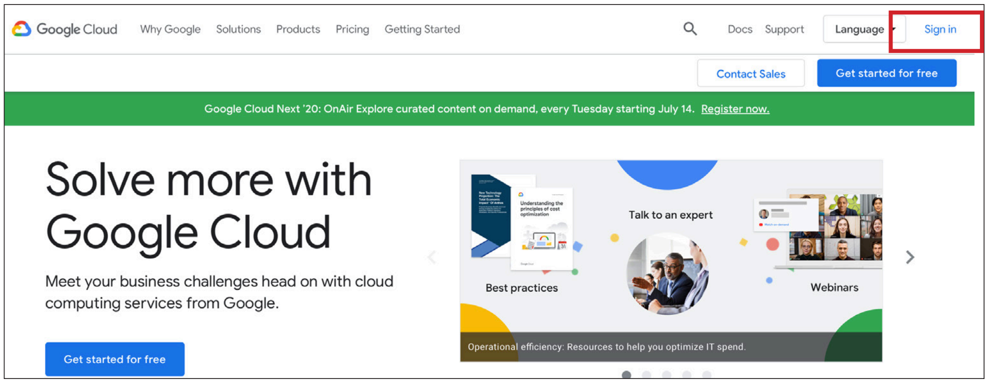
These blog posts may be helpful when configuring the various Jamf Connect integrations:

- https://travellingtechguy.eu/?s=jamf+connect
- https://travellingtechguy.eu/jamf-connect-login-and-google-cloud-identity/

Section 1: Create OAuth Client ID Credentials

In this section, you will sign in to a Google Developers account to create OAuth credentials. These credentials will allow the integration to occur between Google and Jamf Connect.

1. Navigate to https://console.cloud.google.com/ and click Sign In.



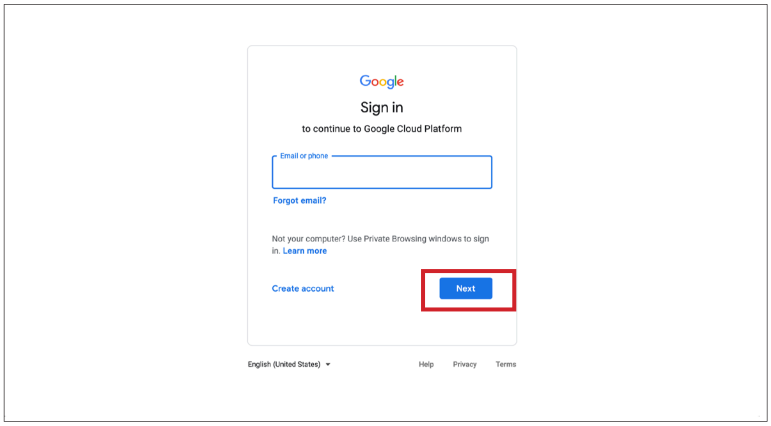
Google Cloud Next '20: OnAir Explore curated content on demand, every Tuesday starting July 14. Register now.

Solve more with Google Cloud

Meet your business challenges head on with cloud computing services from Google.

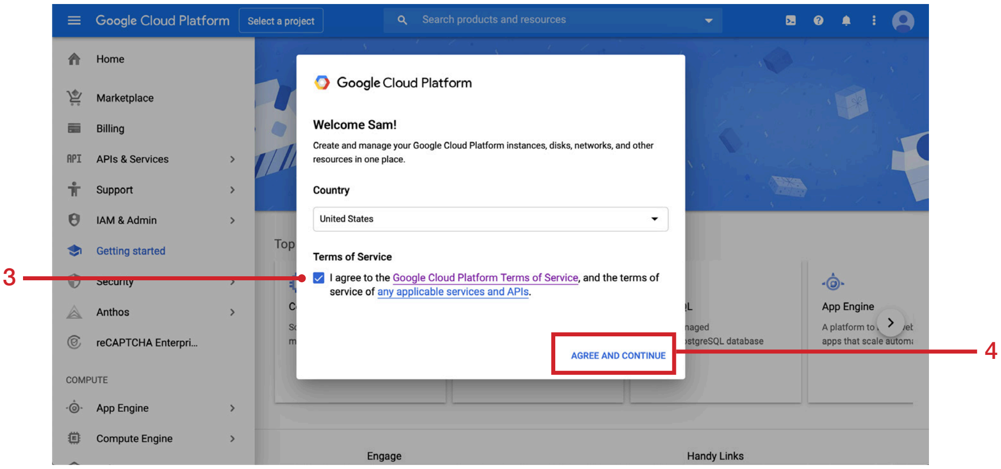
Operational efficiency: Resources to help you optimize IT spend.

2. Enter credentials for your Google Admin account and click Next.



Not your computer? Use Private Browsing windows to sign in. Learn more

3. If you are prompted to agree to the terms of service, carefully read the terms and select the checkbox to agree.
4. Click Agree and Continue.



Google Cloud Platform

Welcome Sam!

Create and manage your Google Cloud Platform instances, disks, networks, and other resources in one place.

Country

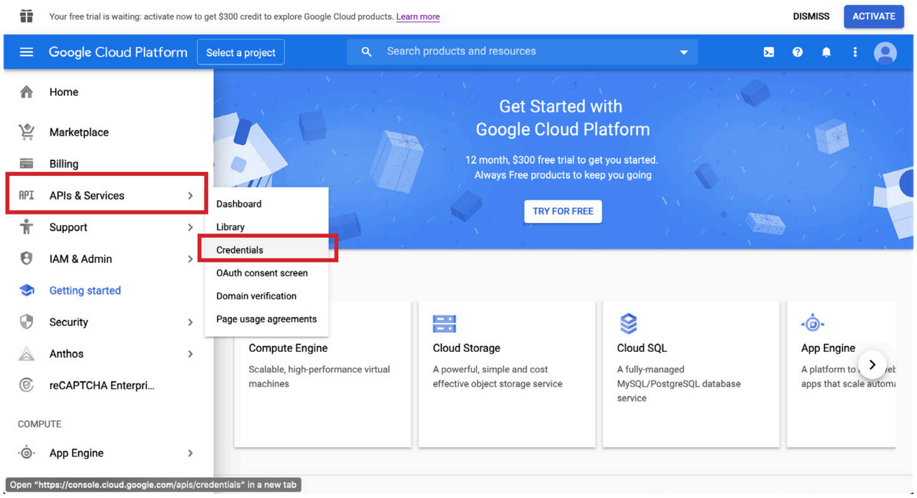
United States

Terms of Service

☑ I agree to the Google Cloud Platform Terms of Service, and the terms of service of any applicable services and APIs.

AGREE AND CONTINUE

5. Navigate to API & Services and choose Credentials from the sub menu.



Your free trial is waiting: activate now to get $300 credit to explore Google Cloud products. Learn more

12 month, $300 free trial to get you started.
Always Free products to keep you going

Scalable, high-performance virtual machines

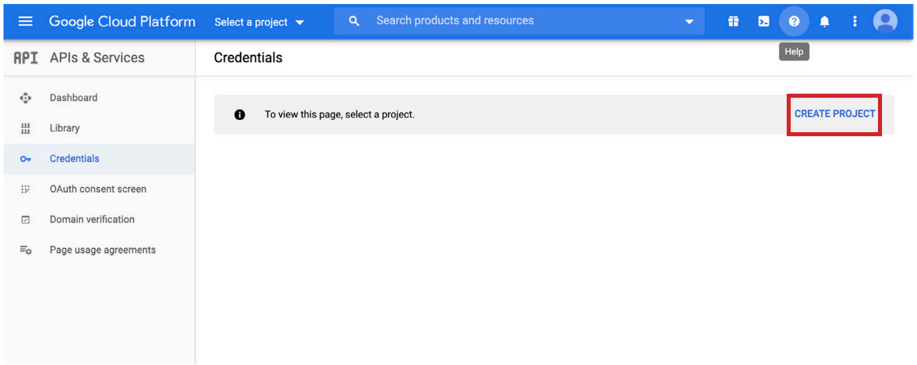
A powerful, simple and cost effective object storage service

A fully-managed MySQL/PostgreSQL database service

A platform to ... apps that scale automa...

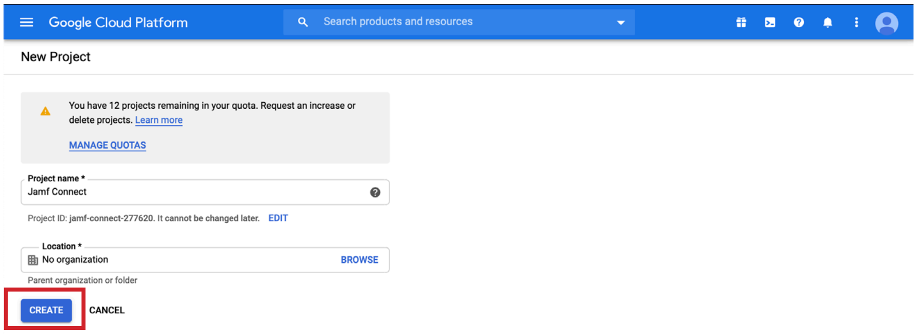
Open "https://console.cloud.google.com/apis/credentials" in a new tab

6. If you have not created a project before, in the upper-right corner, click Create Project.
NOTE: If you already have projects, please proceed to step 13.



To view this page, select a project.

7. Provide a project name and click Create. This guide uses **Jamf Connect** as an example.
NOTE: It may take a few moments for the project to create.



You have 12 projects remaining in your quota. Request an increase or delete projects. Learn more

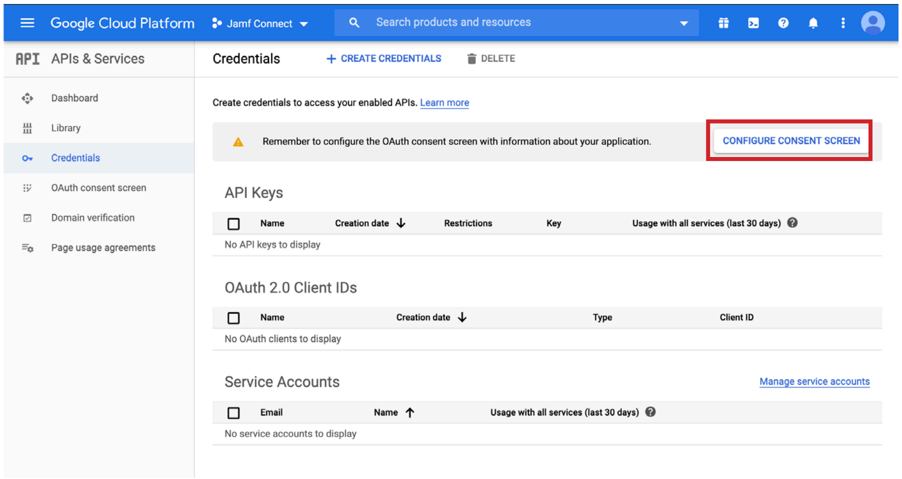
Project name *
Jamf Connect

Project ID: jamf-connect-277620. It cannot be changed later. EDIT

Location *
No organization

Parent organization or folder

8. Click the button to Configure Consent Screen.



Create credentials to access your enabled APIs. Learn more

Remember to configure the OAuth consent screen with information about your application.

API Keys

Name	Creation date ↓	Restrictions	Key	Usage with all services (last 30 days)

No API keys to display

OAuth 2.0 Client IDs

Name	Creation date ↓	Type	Client ID

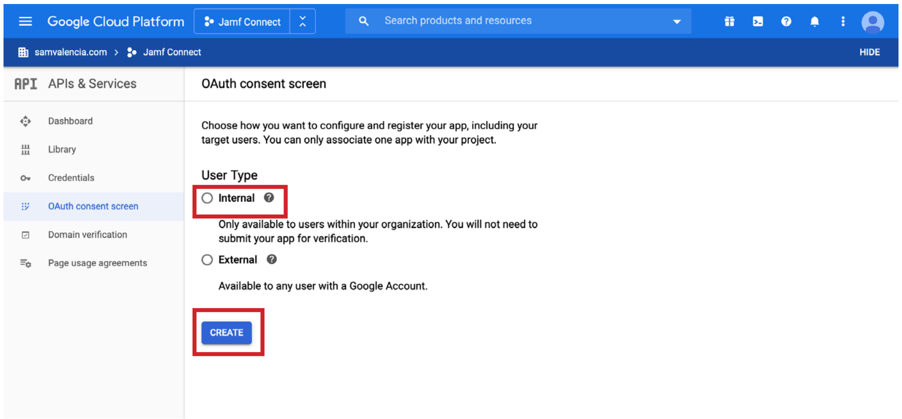
No OAuth clients to display

Service Accounts

Email	Name ↑	Usage with all services (last 30 days)

No service accounts to display

9. At the OAuth Consent Screen, select Internal and click Create.



OAuth consent screen

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

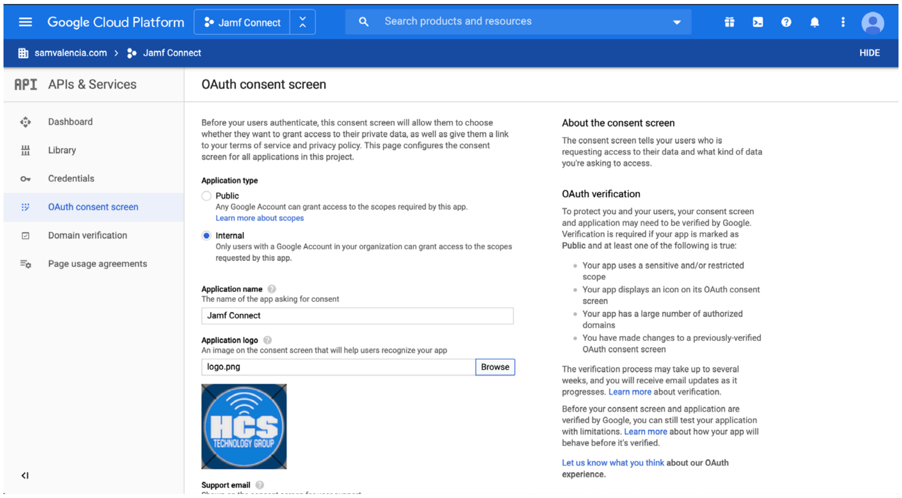
○ Internal

Only available to users within your organization. You will not need to submit your app for verification.

○ External

Available to any user with a Google Account.

10. Provide an Application Name and, if desired, a logo. The remaining items may be configured to your liking but are not required to save.



OAuth consent screen

Before your users authenticate, this consent screen will allow them to choose whether they want to grant access to their private data, as well as give them a link to your terms of service and privacy policy. This page configures the consent screen for all applications in this project.

Application type

○ Public
Any Google Account can grant access to the scopes required by this app.
Learn more about scopes

● Internal
Only users with a Google Account in your organization can grant access to the scopes requested by this app.

Application name
The name of the app asking for consent
Jamf Connect

Application logo
An image on the consent screen that will help users recognize your app
logo.png

Support email

About the consent screen

The consent screen tells your users who is requesting access to their data and what kind of data you're asking to access.

OAuth verification

To protect you and your users, your consent screen and application may need to be verified by Google. Verification is required if your app is marked as **Public** and at least one of the following is true:

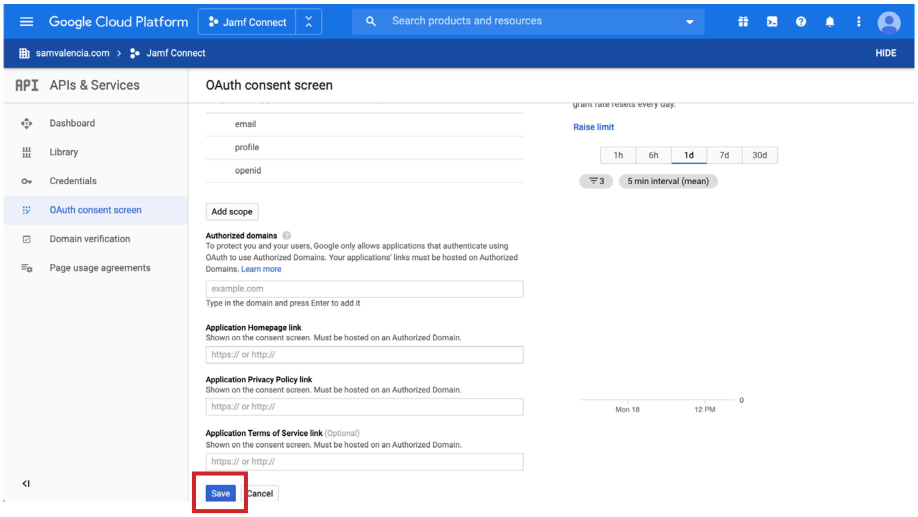
- Your app uses a sensitive and/or restricted scope
- Your app displays an icon on its OAuth consent screen
- Your app has a large number of authorized domains
- You have made changes to a previously-verified OAuth consent screen

The verification process may take up to several weeks, and you will receive email updates as it progresses. Learn more about verification.

Before your consent screen and application are verified by Google, you can still test your application with limitations. Learn more about how your app will behave before it's verified.

Let us know what you think about our OAuth experience.

11. Scroll down and click Save.



Google Cloud Platform · Jamf Connect · Search products and resources

samvalencia.com > Jamf Connect · HIDE

APIs & Services: Dashboard, Library, Credentials, OAuth consent screen, Domain verification, Page usage agreements

OAuth consent screen

email

profile

openid

Add scope

Authorized domains
To protect you and your users, Google only allows applications that authenticate using OAuth to use Authorized Domains. Your applications' links must be hosted on Authorized Domains. Learn more

example.com
Type in the domain and press Enter to add it

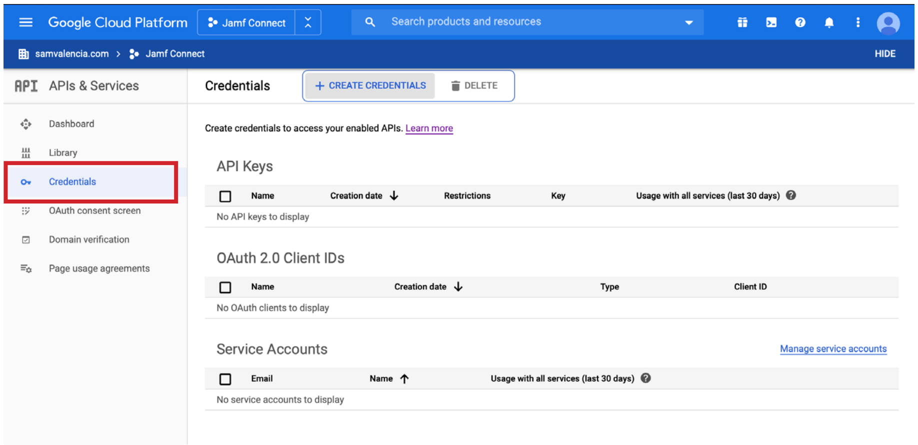
Application Homepage link
Shown on the consent screen. Must be hosted on an Authorized Domain.
https:// or http://

Application Privacy Policy link
Shown on the consent screen. Must be hosted on an Authorized Domain.
https:// or http://

Application Terms of Service link (Optional)
Shown on the consent screen. Must be hosted on an Authorized Domain.
https:// or http://

Save · Cancel

12. In the sidebar, click Credentials.



Google Cloud Platform · Jamf Connect · Search products and resources

samvalencia.com > Jamf Connect · HIDE

APIs & Services: Dashboard, Library, Credentials, OAuth consent screen, Domain verification, Page usage agreements

Credentials · + CREATE CREDENTIALS · DELETE

Create credentials to access your enabled APIs. Learn more

API Keys

☐	Name	Creation date ↓	Restrictions	Key	Usage with all services (last 30 days)

No API keys to display

OAuth 2.0 Client IDs

☐	Name	Creation date ↓	Type	Client ID

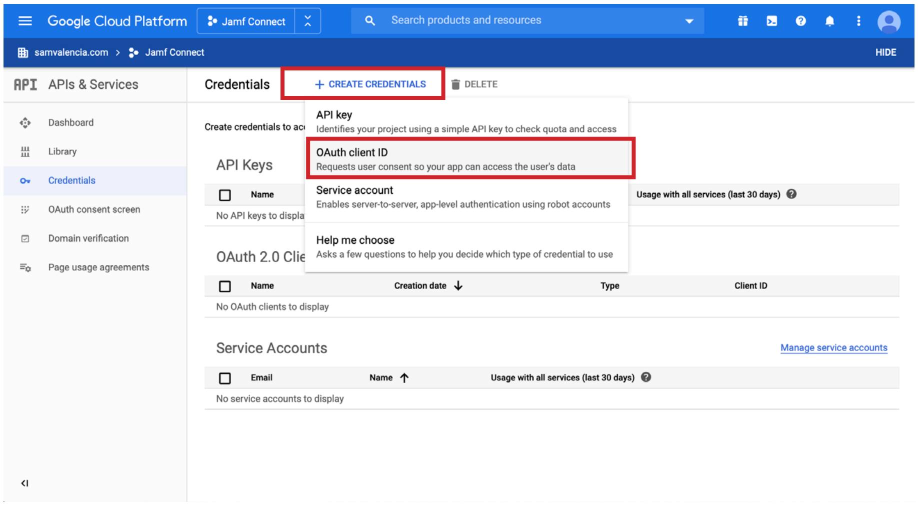
No OAuth clients to display

Service Accounts · Manage service accounts

☐	Email	Name ↑	Usage with all services (last 30 days)

No service accounts to display

13. Click Create Credentials and choose OAuth Client ID.



Google Cloud Platform · Jamf Connect · Search products and resources

samvalencia.com > Jamf Connect · HIDE

Credentials · + CREATE CREDENTIALS · DELETE

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

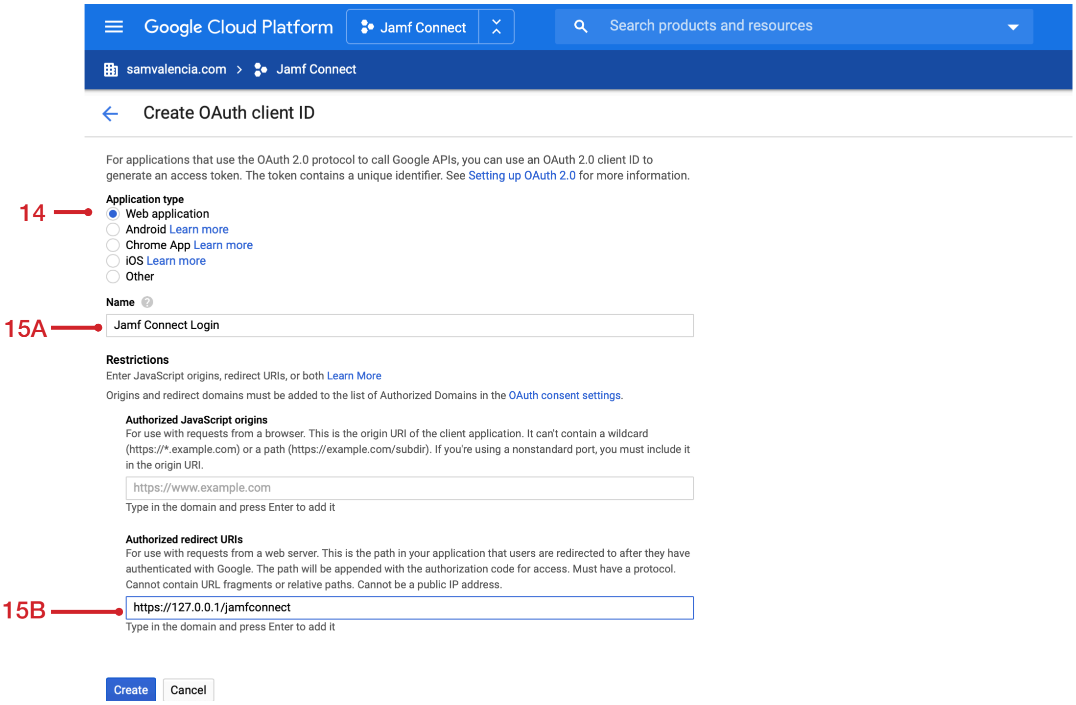
Service account
Enables server-to-server, app-level authentication using robot accounts

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

14. For Application type, select "Web application."
15. Enter the following information:

    A. Name: **Jamf Connect Login**
    B. Authorized redirect URLs: **https://127.0.0.1/jamfconnect**

    NOTE: This URI is a recommended value. However, any valid URI may be used, as long as it matches the URI in your Jamf Connect Login configuration profile (created in section 4).



Create OAuth client ID

For applications that use the OAuth 2.0 protocol to call Google APIs, you can use an OAuth 2.0 client ID to generate an access token. The token contains a unique identifier. See Setting up OAuth 2.0 for more information.

Application type
● Web application
○ Android Learn more
○ Chrome App Learn more
○ iOS Learn more
○ Other

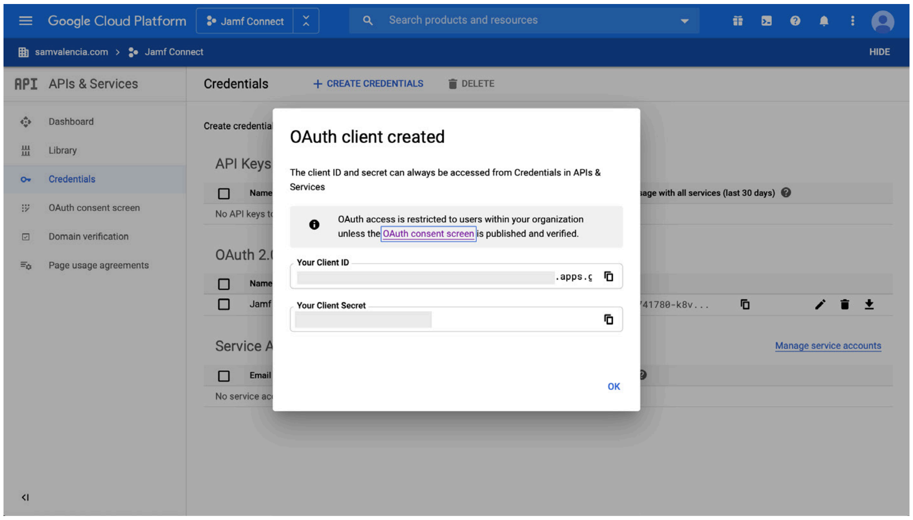
Name
Jamf Connect Login

Restrictions
Enter JavaScript origins, redirect URIs, or both Learn More
Origins and redirect domains must be added to the list of Authorized Domains in the OAuth consent settings.

Authorized JavaScript origins
For use with requests from a browser. This is the origin URI of the client application. It can't contain a wildcard (https://*.example.com) or a path (https://example.com/subdir). If you're using a nonstandard port, you must include it in the origin URI.
https://www.example.com
Type in the domain and press Enter to add it

Authorized redirect URIs
For use with requests from a web server. This is the path in your application that users are redirected to after they have authenticated with Google. The path will be appended with the authorization code for access. Must have a protocol. Cannot contain URL fragments or relative paths. Cannot be a public IP address.
https://127.0.0.1/jamfconnect
Type in the domain and press Enter to add it

16. Click Create.
17. Copy the values for Your Client ID and Your Client Secret as you will need them in a later section.



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
[redacted].apps.g

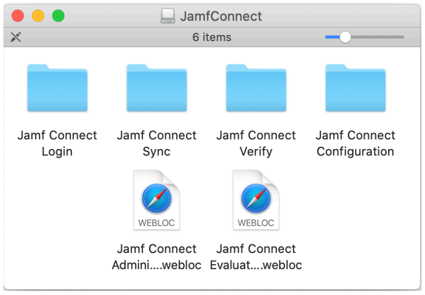
Your Client Secret
[redacted]

18. Click OK. It may be helpful to remain logged in as you may need to reference this information for later sections.

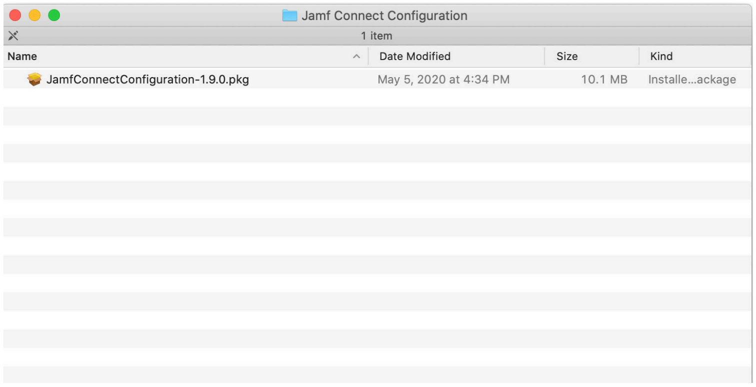
Section 2: Jamf Connect Configuration

You can install Jamf Connect Configuration on an administrative Mac computer to configure settings for Jamf Connect apps. However, in this guide you will only use the built-in test feature to test configuration settings with your IdP.

1. Download Jamf Connect: https://files.jamfconnect.com/JamfConnect.dmg.
2. Open the disk image file that you downloaded (with the filename suffix .dmg) and navigate to the Jamf Connect Configuration folder in the disk image.

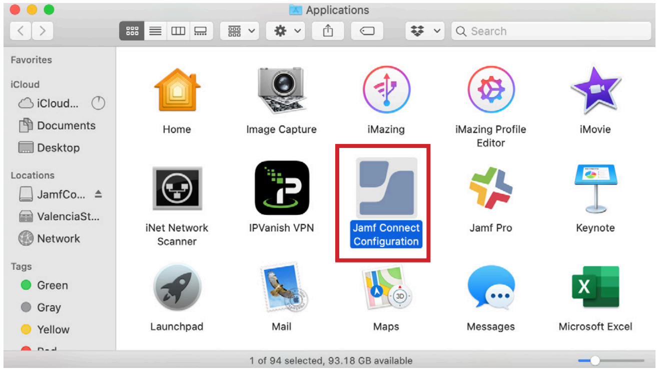

JamfConnect
6 items
Jamf Connect Login
Jamf Connect Sync
Jamf Connect Verify
Jamf Connect Configuration
WEBLOC
Jamf Connect Admini....webloc
WEBLOC
Jamf Connect Evaluat....webloc

3. Double click the package to open the installer (at the time this guide was written the package name was JamfConnectConfiguration-1.9.0.pkg).

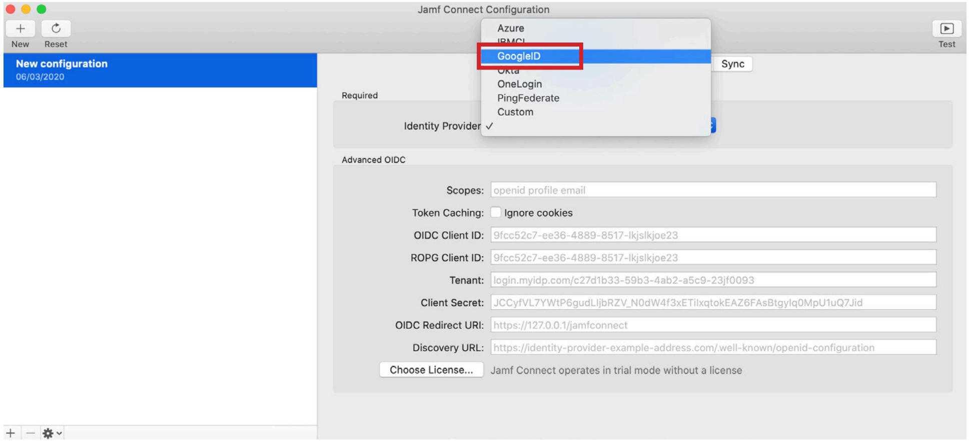


Name	Date Modified	Size	Kind
JamfConnectConfiguration-1.9.0.pkg	May 5, 2020 at 4:34 PM	10.1 MB	Installe...ackage

4. Proceed with the installation steps
5. Open your Applications folder.
6. Open Jamf Connect Configuration.



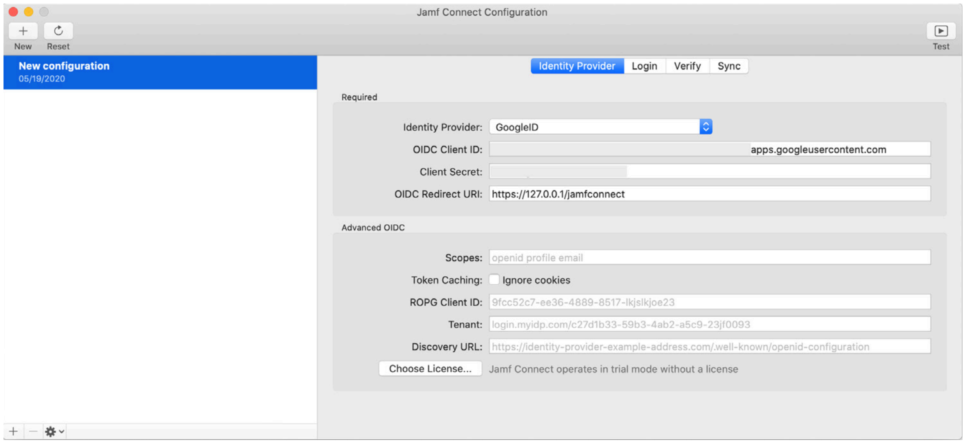
7. From the Identity Provider menu, choose GoogleID.



Identity Provider ✓

Scopes: openid profile email
Token Caching: □ Ignore cookies
OIDC Client ID: 9fcc52c7-ee36-4889-8517-lkjslkjoe23
ROPG Client ID: 9fcc52c7-ee36-4889-8517-lkjslkjoe23
Tenant: login.myidp.com/c27d1b33-59b3-4ab2-a5c9-23jf0093
Client Secret: JCCyfVL7YWtP6gudLljbRZV_N0dW4f3xETilxqtokEAZ6FAsBtgylq0MpU1uQ7Jid
OIDC Redirect URI: https://127.0.0.1/jamfconnect
Discovery URL: https://identity-provider-example-address.com/.well-known/openid-configuration
Jamf Connect operates in trial mode without a license

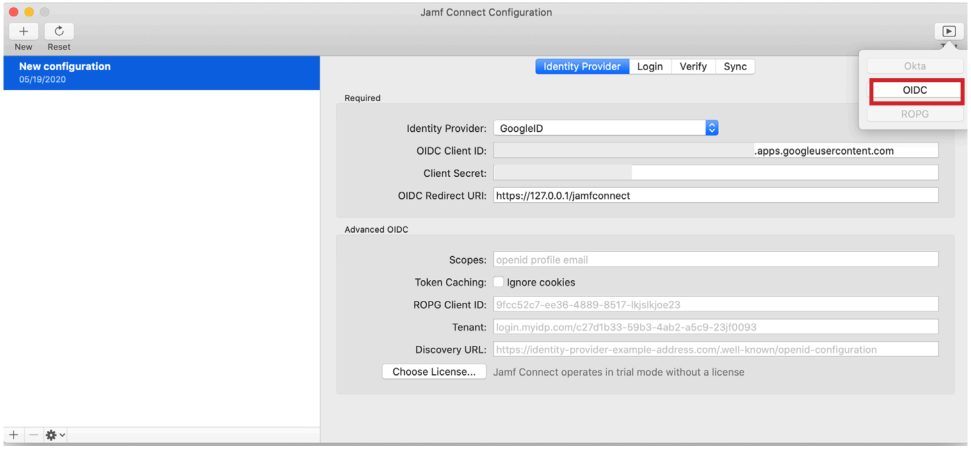
8. Populate OIDC Client ID, Client Secret, and OIDC Redirect URL from steps 15 through 18 in Section 1.
NOTE: You can configure Advanced OpenID Connect settings that allow for values like tenant and client secret. Depending on the environment, you may wish to configure these settings but they are not required for this test environment.



Identity Provider: GoogleID
OIDC Client ID: apps.googleusercontent.com
Client Secret:
OIDC Redirect URI: https://127.0.0.1/jamfconnect

Scopes: openid profile email
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
Jamf Connect operates in trial mode without a license

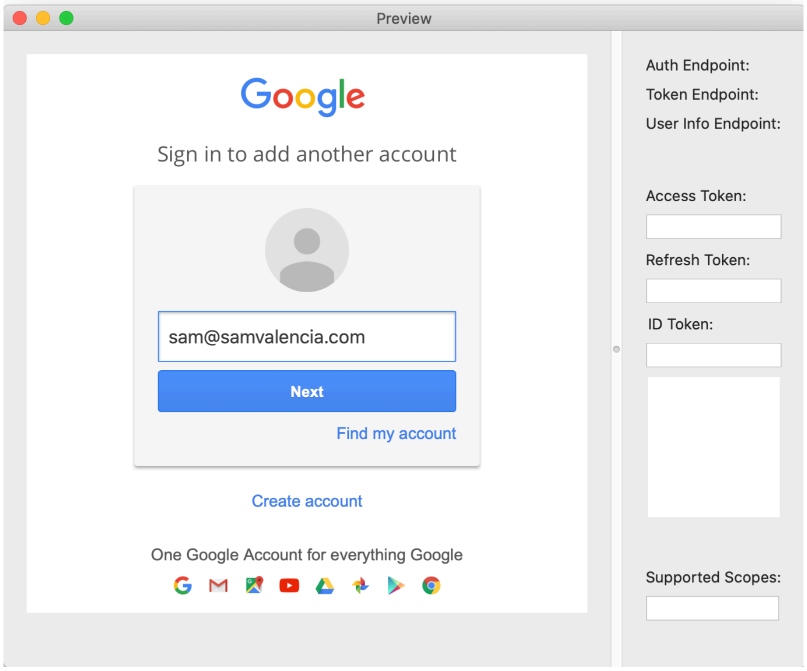
9. In the upper-right corner, click Test (looks like a triangle in a rounded square) and select OIDC to test the parameters you just entered.



Identity Provider: GoogleID
OIDC Client ID: .apps.googleusercontent.com
Client Secret:
OIDC Redirect URI: https://127.0.0.1/jamfconnect

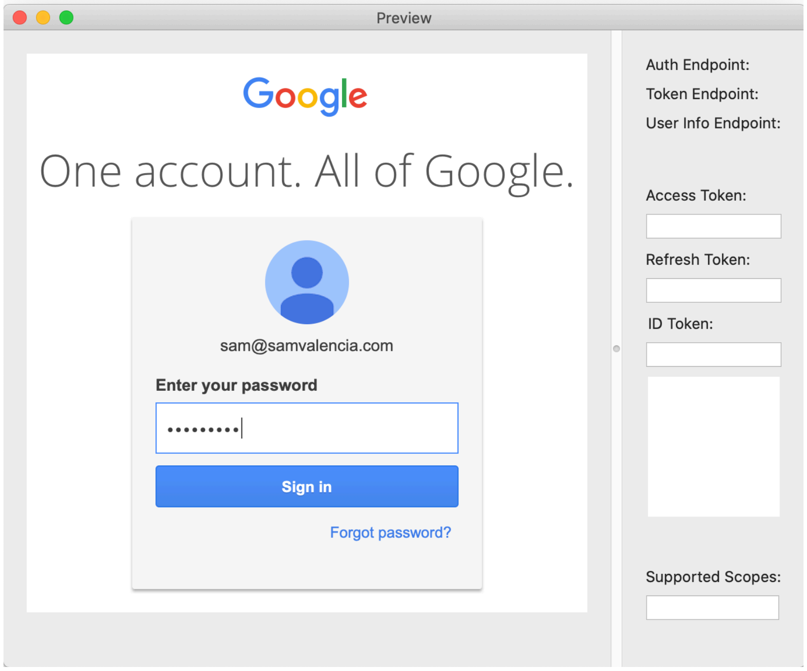
Scopes: openid profile email
Token Caching: □ Ignore cookies
ROPG Client ID: 9fcc52c7-ee36-4889-8517-lkjslkjoe23
Tenant: login.myidp.com/c27d1b33-59b3-4ab2-a5c9-23jf0093
Discovery URL: https://identity-provider-example-address.com/.well-known/openid-configuration
Jamf Connect operates in trial mode without a license

10. Enter an email address in your G Suite domain.
    NOTE: Ensure you have a Google Cloud Identity license assigned to this account.

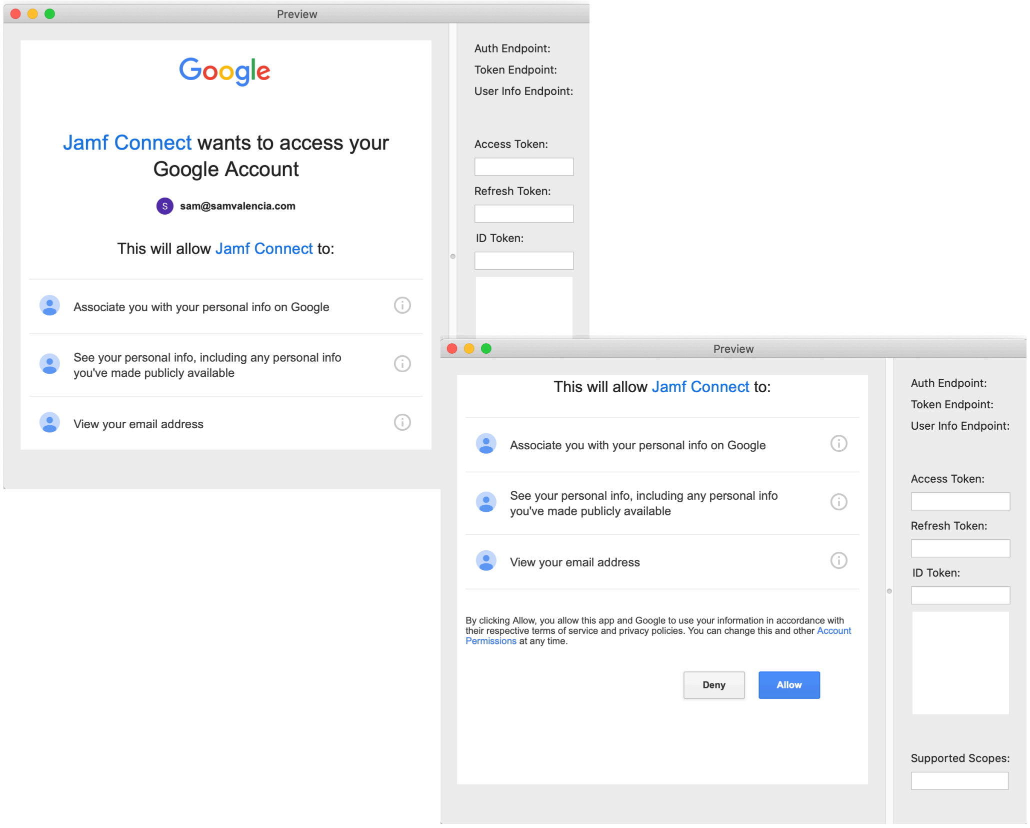


sam@samvalencia.com

11. Enter the password and click "Sign in."



12. Note the capabilities you are allowing and click Allow.



Jamf Connect wants to access your Google Account

sam@samvalencia.com

This will allow Jamf Connect to:

- Associate you with your personal info on Google
- See your personal info, including any personal info you've made publicly available
- View your email address

Auth Endpoint:
Token Endpoint:
User Info Endpoint:

Access Token:

Refresh Token:

ID Token:

This will allow Jamf Connect to:

- Associate you with your personal info on Google
- See your personal info, including any personal info you've made publicly available
- View your 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.

Auth Endpoint:
Token Endpoint:
User Info Endpoint:

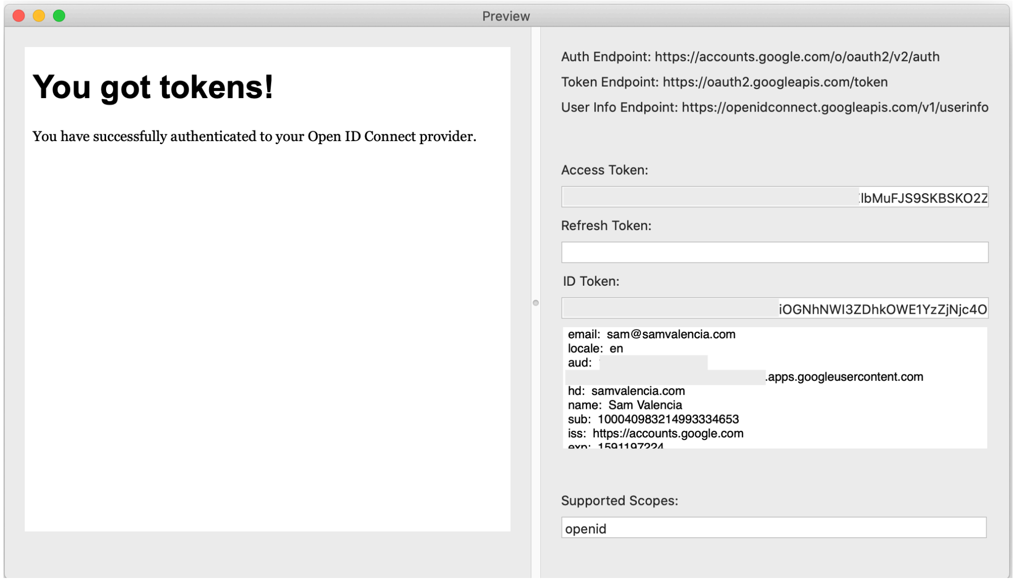
Access Token:

Refresh Token:

ID Token:

Supported Scopes:

13. Confirm that a message appears that you have successfully authenticated to your Open ID Connect provider. You are now ready to configure Jamf Connect Login.



You got tokens!

You have successfully authenticated to your Open ID Connect provider.

Auth Endpoint: https://accounts.google.com/o/oauth2/v2/auth

Token Endpoint: https://oauth2.googleapis.com/token

User Info Endpoint: https://openidconnect.googleapis.com/v1/userinfo

Access Token:

[redacted]lbMuFJS9SKBSKO2Z

Refresh Token:

ID Token:

[redacted]iOGNhNWI3ZDhkOWE1YzZjNjc4O

```
email:  sam@samvalencia.com
locale:  en
aud:  [redacted]
.apps.googleusercontent.com
hd:  samvalencia.com
name:  Sam Valencia
sub:  100040983214993334653
iss:  https://accounts.google.com
exp:  1591197224
```

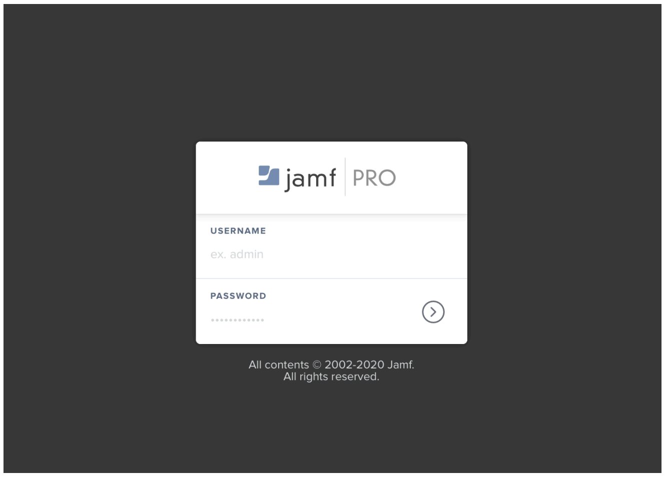
Supported Scopes:

openid

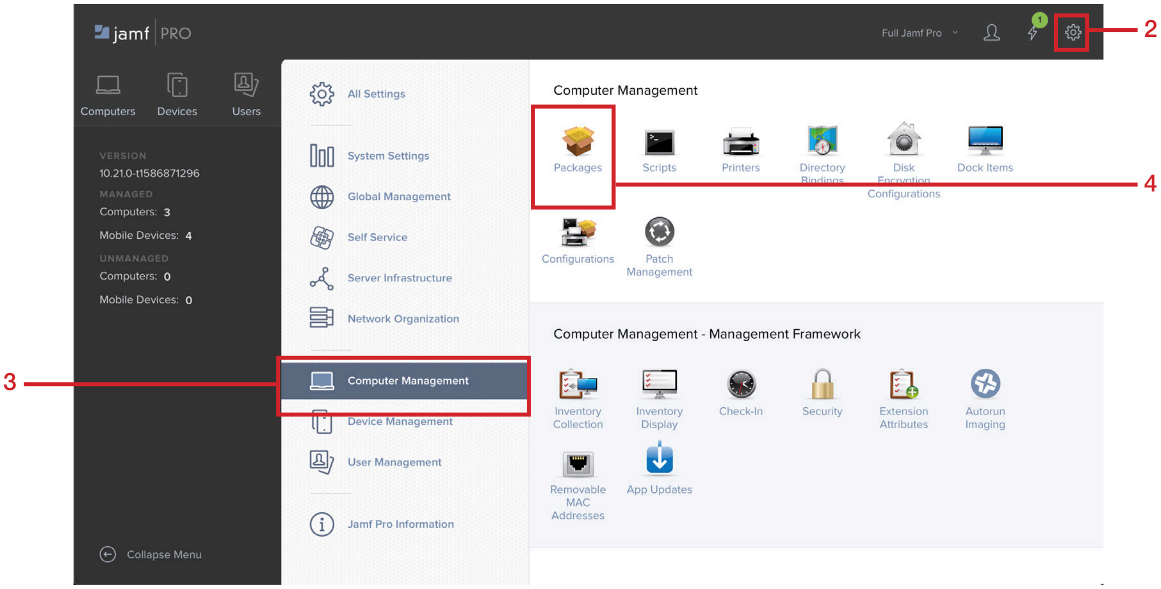
Section 3: Upload Jamf Connect Login Package & Create Configuration Profile

The computers using Jamf Connect will require the package to be installed. This section will detail uploading the Jamf Connection package for eventual deployment.

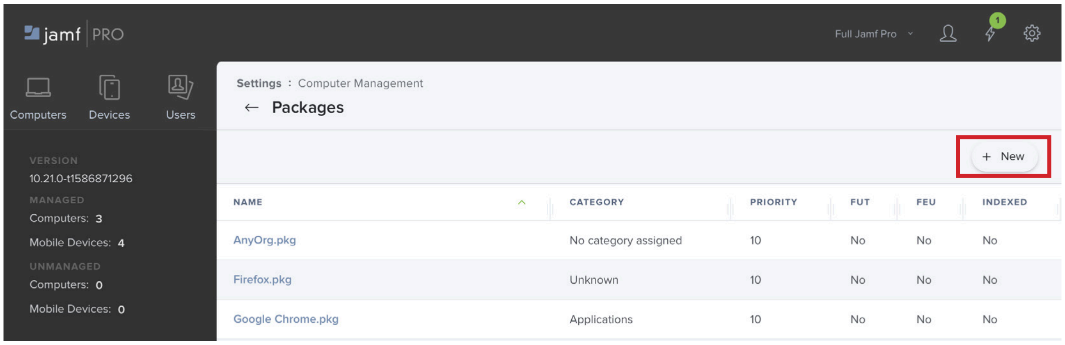
1. Log in to your Jamf Pro.



2. In the upper-right corner, click Settings.
3. Click Computer Management.
4. Click Packages.



5. In the upper-right corner, click New.



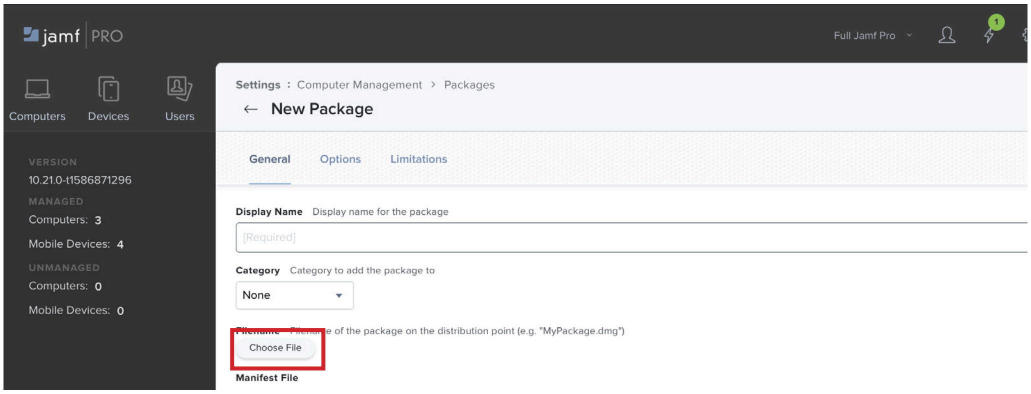
Settings : Computer Management

Packages

VERSION
10.21.0-t1586871296
MANAGED
Computers: 3
Mobile Devices: 4
UNMANAGED
Computers: 0
Mobile Devices: 0

NAME	CATEGORY	PRIORITY	FUT	FEU	INDEXED
AnyOrg.pkg	No category assigned	10	No	No	No
Firefox.pkg	Unknown	10	No	No	No
Google Chrome.pkg	Applications	10	No	No	No

6. Click Choose File.



Settings : Computer Management > Packages

New Package

VERSION
10.21.0-t1586871296
MANAGED
Computers: 3
Mobile Devices: 4
UNMANAGED
Computers: 0
Mobile Devices: 0

Display Name Display name for the package
[Required]

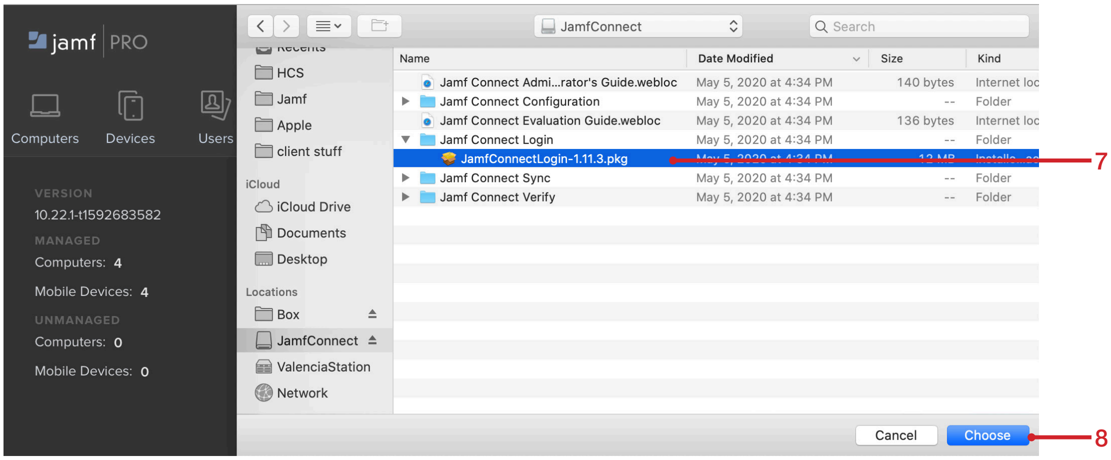
Category Category to add the package to
None

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

Manifest File

7. Navigate to the Jamf Connect folder that you downloaded in section 2 and select the JamfConnectLogin package (at the time this guide was written the package name was JamfConnectLogin-1.11.3.pkg) in the Jamf Connect Login folder.

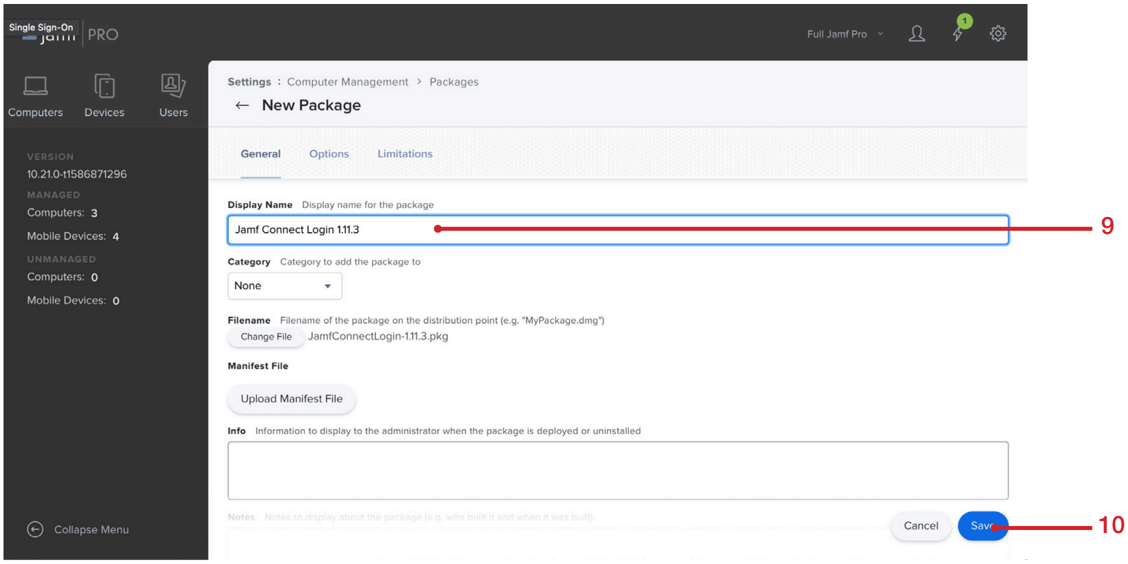
8. Click Choose.



VERSION
10.22.1-t1592683582
MANAGED
Computers: 4
Mobile Devices: 4
UNMANAGED
Computers: 0
Mobile Devices: 0

Name	Date Modified	Size	Kind
Jamf Connect Admi...rator's Guide.webloc	May 5, 2020 at 4:34 PM	140 bytes	Internet loc
Jamf Connect Configuration	May 5, 2020 at 4:34 PM	--	Folder
Jamf Connect Evaluation Guide.webloc	May 5, 2020 at 4:34 PM	136 bytes	Internet loc
Jamf Connect Login	May 5, 2020 at 4:34 PM	--	Folder
JamfConnectLogin-1.11.3.pkg	May 5, 2020 at 4:34 PM	12 MB	Installe...ge
Jamf Connect Sync	May 5, 2020 at 4:34 PM	--	Folder
Jamf Connect Verify	May 5, 2020 at 4:34 PM	--	Folder

9. In the Display Name field, replace the existing name with **Jamf Connect Login**, followed by the version number. This guide uses Jamf Connect Login 1.11.3 as an example.
10. Optional: Click the Category menu and choose an appropriate category. This guide uses None.
11. Optional: In the Info and Notes fields, enter the information that your organization has standardized on entering for those fields. For simplicity, this guide leaves these fields blank.
12. Click Save.



Display Name Display name for the package

Jamf Connect Login 1.11.3

Category Category to add the package to

None

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

Change File JamfConnectLogin-1.11.3.pkg

Manifest File

Upload Manifest File

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

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

Section 4: Configure Jamf Connect Login

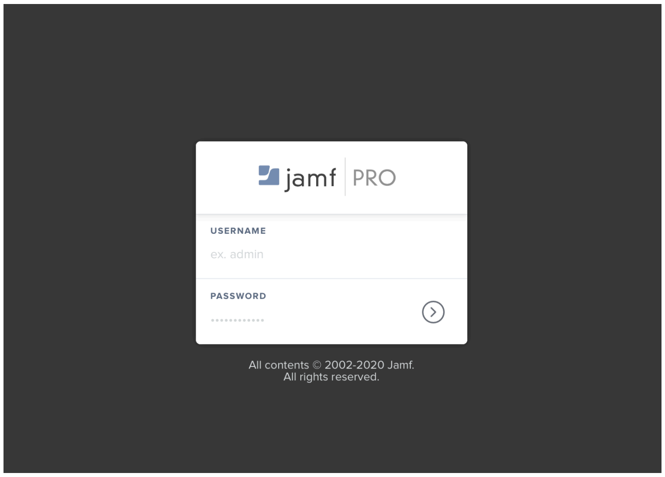
As of Jamf Pro 10.18, the Custom Settings payload in Computer Configuration Profiles was updated to Applications & Custom Settings. That new payload contains settings available for Jamf Connect Login, Sync, and Verify. Although you could use the Jamf Connect Configuration used in Section 2 to configure these settings, export the settings, then upload the settings to Jamf Pro, using the Applications & Custom Settings payload is a more straightforward and flexible process.

The following values are required for Jamf Connect Sync to work with Google as an IdP:

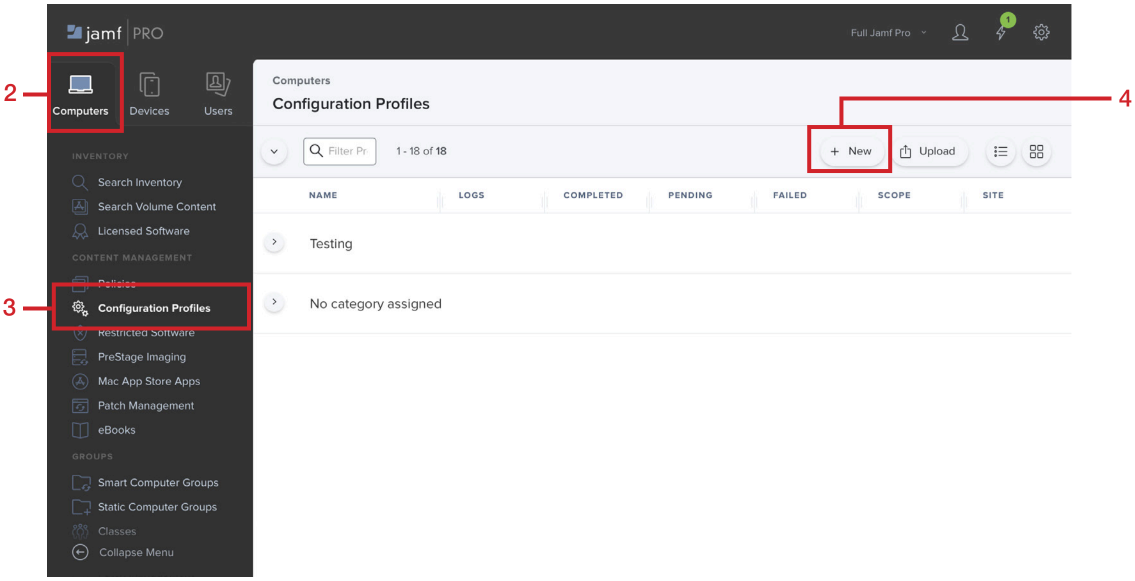
- Identity Provider
- Client ID
- Redirect URI
- Client Secret
- Create a Separate Local Password (must be set to True)

In this section you will use the Applications & Custom Settings payload to configure Jamf Connect Login.

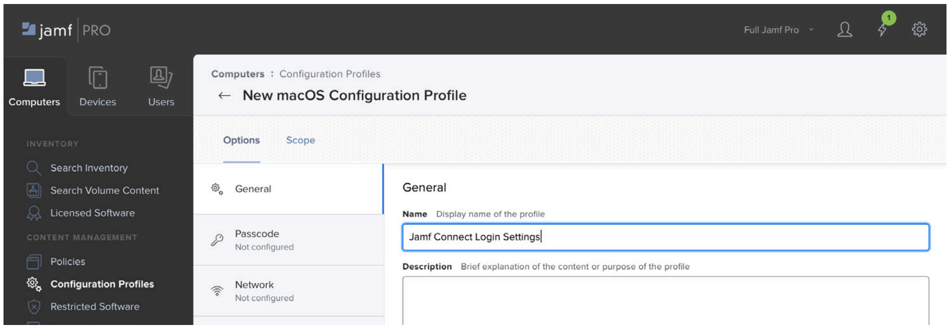
1. Log in to your Jamf Pro.



2. Click Computers.
3. Click Configuration Profiles.
4. Click New.



5. In the Name field, enter **Jamf Connect Login Settings**.



General

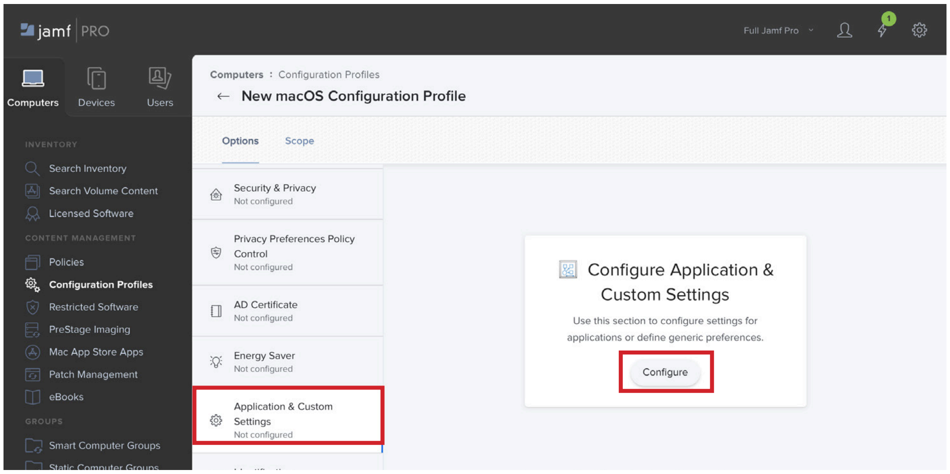
Name Display name of the profile

Jamf Connect Login Settings

Description Brief explanation of the content or purpose of the profile

6. Scroll to the Application & Custom Settings payload and select it.

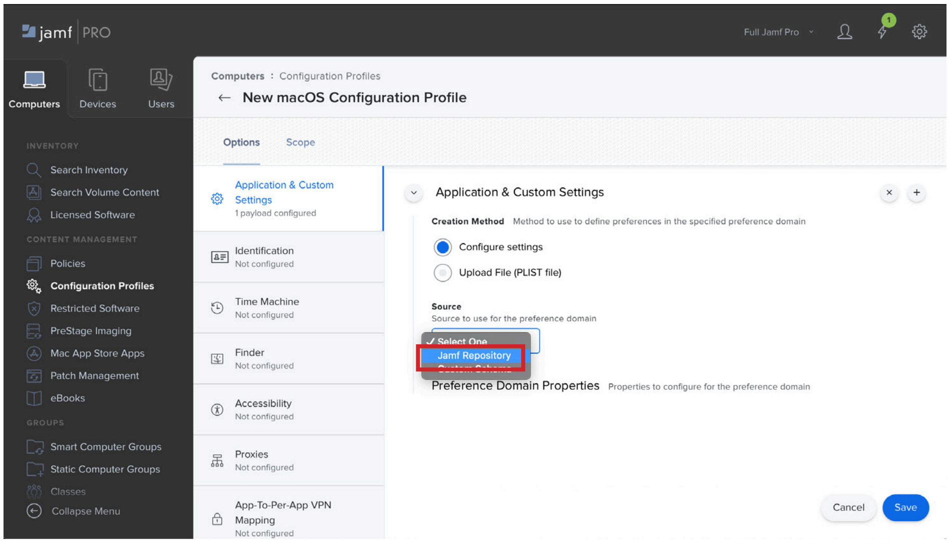
7. Click Configure.



Configure Application & Custom Settings

Use this section to configure settings for applications or define generic preferences.

8. Click the Source menu and choose Jamf Repository.



Application & Custom Settings

Creation Method Method to use to define preferences in the specified preference domain

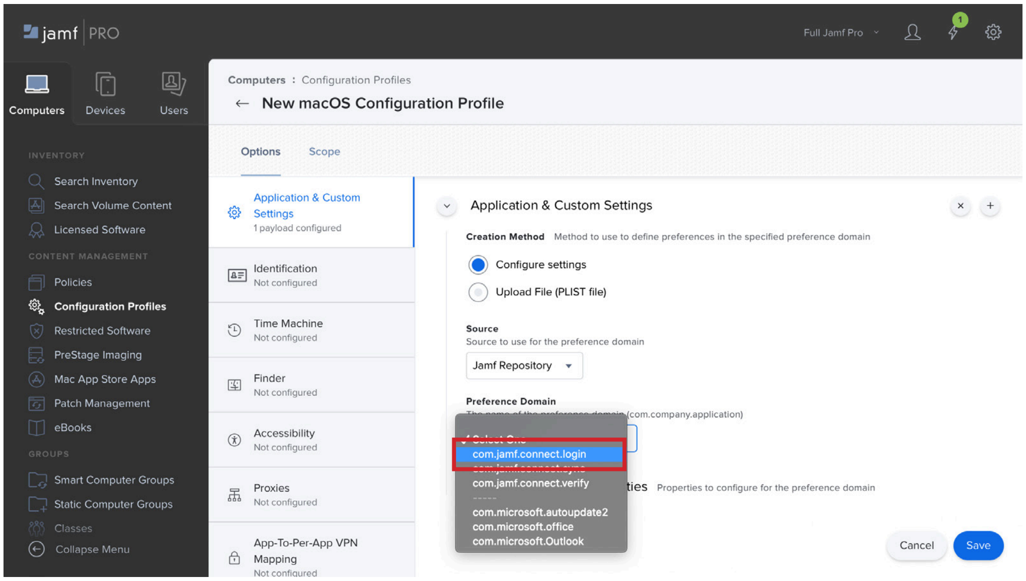
● Configure settings

○ Upload File (PLIST file)

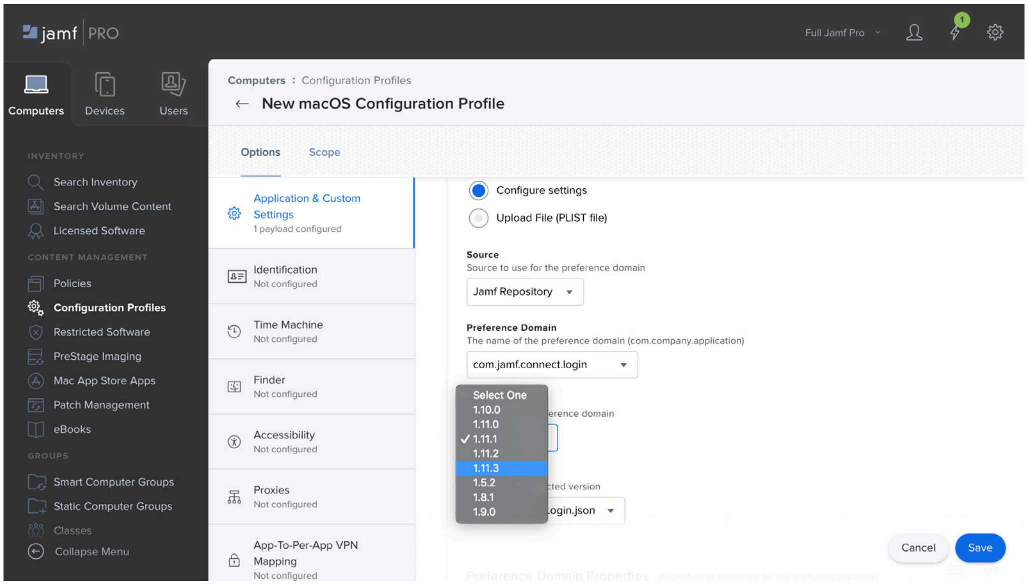
Source Source to use for the preference domain

Preference Domain Properties Properties to configure for the preference domain

9. Click the Preference Domain menu that appears, and choose com.jamf.connect.login.

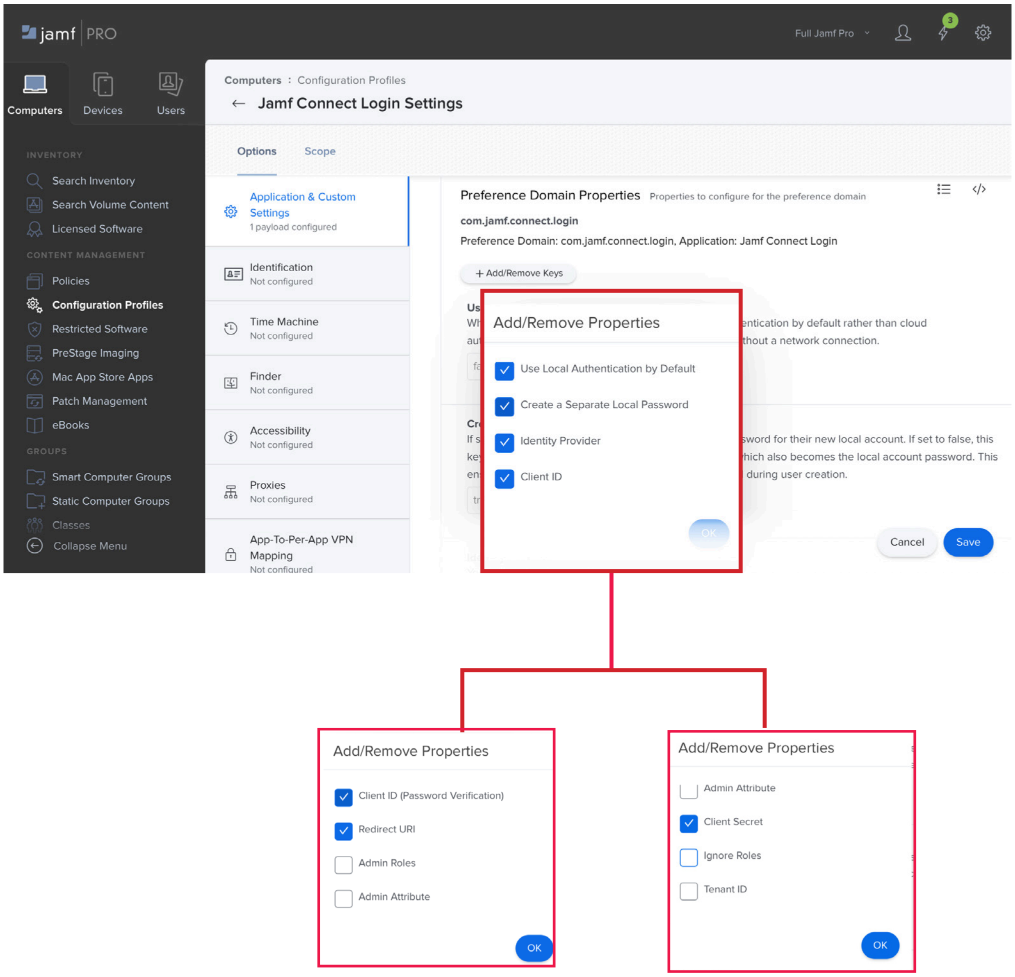


8. Click the Version menu that appears and choose the version that you uploaded. This guide uses 1.11.3 as an example.



9. Leave the Variant menu at its default value, (There are no options besides JSON.)

10. Click Add/Remove Keys.
    IMPORTANT NOTE: Deselect all unnecessary keys, because leaving them in can result in settings that cause errors during authentication.
11. Deselect all keys except the following:
    - Use Local Authentication by Default
    - Create a Separate Local Password
    - Identity Provider
    - Client ID
    - Client ID (Password Verification)
    - Redirect URI
    - Client Secret



Preference Domain Properties Properties to configure for the preference domain

com.jamf.connect.login

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

Add/Remove Properties

☑ Use Local Authentication by Default
☑ Create a Separate Local Password
☑ Identity Provider
☑ Client ID

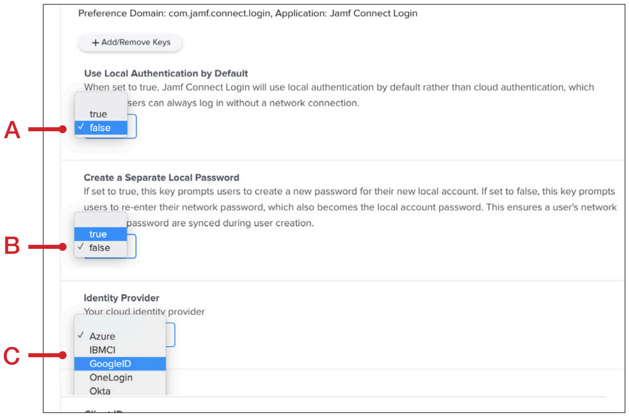
Add/Remove Properties

☑ Client ID (Password Verification)
☑ Redirect URI
☐ Admin Roles
☐ Admin Attribute

Add/Remove Properties

☐ Admin Attribute
☑ Client Secret
☐ Ignore Roles
☐ Tenant ID

12. For Preference Domain Properties, configure the following settings with the following values:
    A. Use Local Authentication by Default: false (a value of *true* allows a user to log in, even without a network connection)
    B. Create a Separate Local Password: true (This ensures each user's local password is synced with their network password)
    C. Identity Provider: GoogleID
    D. Client ID: Enter the Client ID from the Google Cloud instance that you created in section 1
    E. Client ID (Password Verification): Since credentials are stored in the same tenant, enter the Client ID from above again
    F. Redirect URI: **https://127.0.0.1/jamfconnect**
    G. Client Secret: Enter the Client Secret from the Google Cloud instance that you created in section 1



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

+ Add/Remove Keys

Use Local Authentication by Default
When set to true, Jamf Connect Login will use local authentication by default rather than cloud authentication, which sers can always log in without a network connection.

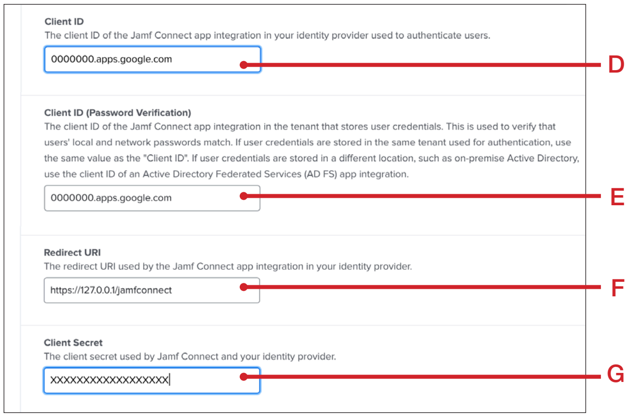
true
✓ false

Create a Separate Local Password
If set to true, this key prompts users to create a new password for their new local account. If set to false, this key prompts users to re-enter their network password, which also becomes the local account password. This ensures a user's network password are synced during user creation.

true
✓ false

Identity Provider
Your cloud identity provider

✓ Azure
IBMCI
GoogleID
OneLogin
Okta



Client ID
The client ID of the Jamf Connect app integration in your identity provider used to authenticate users.

0000000.apps.google.com

Client ID (Password Verification)
The client ID of the Jamf Connect app integration in the tenant that stores user credentials. This is used to verify that users' local and network passwords match. If user credentials are stored in the same tenant used for authentication, use the same value as the "Client ID". If user credentials are stored in a different location, such as on-premise Active Directory, use the client ID of an Active Directory Federated Services (AD FS) app integration.

0000000.apps.google.com

Redirect URI
The redirect URI used by the Jamf Connect app integration in your identity provider.

https://127.0.0.1/jamfconnect

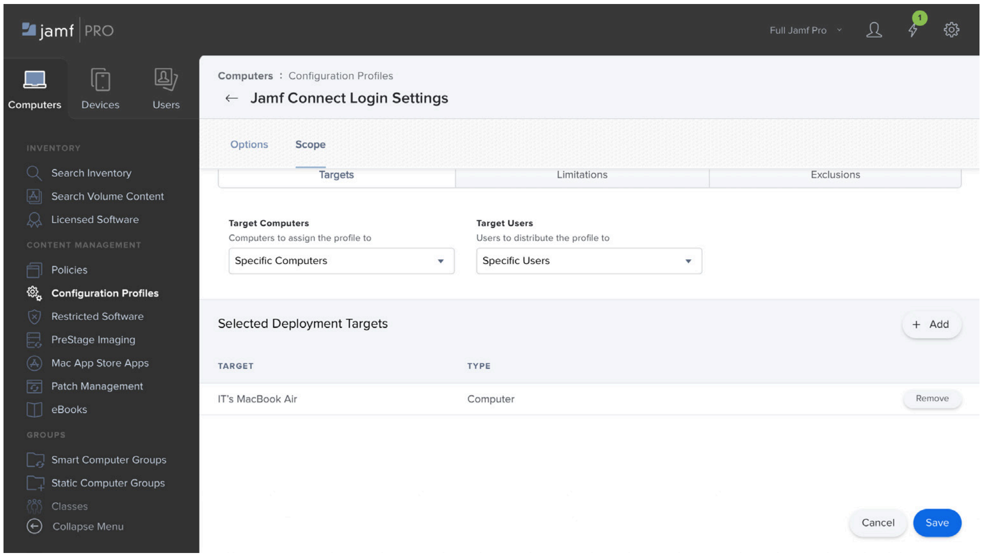
Client Secret
The client secret used by Jamf Connect and your identity provider.

xxxxxxxxxxxxxxxxxx

There are many different settings in this payload. Some are not relevant to Google (They are meant for other IdPs). The following settings are not relevant to using Google as an IdP:

- Allow Local Fallback - Allow local authentication if a network is unavailable
- Create Admin Users - If set to true, all users are created as local administrators. NOTE: Admin Roles is a feature not currently supported with Google ID: https://docs.jamf.com/jamf-connect/1.19.0/administrator-guide/
- Users with local authentication privileges - Specify users (ie. An IT administrator account) that are allowed to bypass network authentication.
- License File - If you purchase licenses for Jamf Connect, you can enter a license file here. We recommend that you distirbute the license with a separate configuration profile.
- Connect existing local accounts to a network account - This can be useful if there are already local accounts on the computer.
- Local Accounts prohibited from network account creation - These accounts would be excluded from the Jamf Connect migration menu.
- Login Logo - A company logo that would appear during password validation or local password creation. This file must be stored locally on the computer so consider a separate policy to deploy the image. This can be used with Google but is beyond the scope of this guide.
- Allow Network Selection - Allow users to select their network at the login window.
- Help URL/Icon/File - Methods to allow users to find assistance if they cannot login.
- Audit Filepath/EULA Text/EULA Title/EULA Subtitle - Entries to incorporate an End User License Agreement.
- Enable FileVault - Setting this as *true* will enable FileVault for the first user that logs in.
- Save FileVault Recovery Key - Stores the FileVault recovery key in /var/db/NoMADFDE on the local computer.
- Set Recovery Key Filepath - Specify a custom directory for the recovery key.

13. Click Scope and scope this configuration profile to your desired target computers.
    NOTE: It is recommended to scope to test computers first, to test functionality.



Jamf Connect Login Settings

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
IT's MacBook Air	Computer

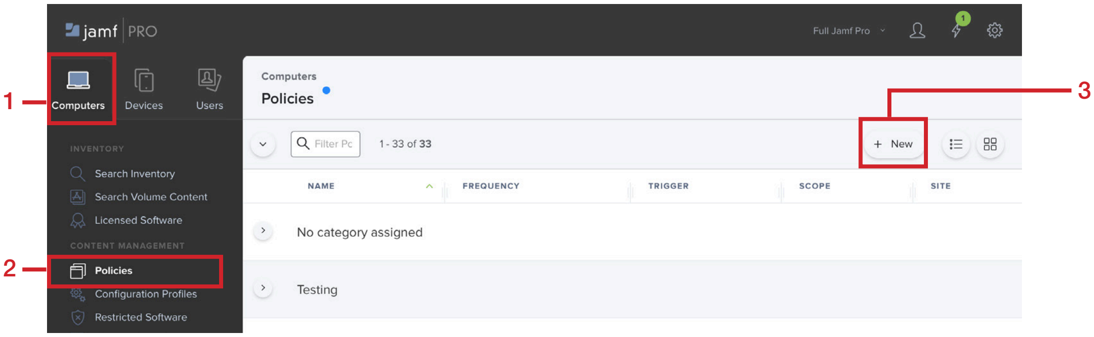
Section 5: Deploy Jamf Connect Login

You can deploy Jamf Connect Login to computers that have already been configured with local accounts, as well as to computers prior to unboxing. Your method of deployment will depend on the status of your fleet.

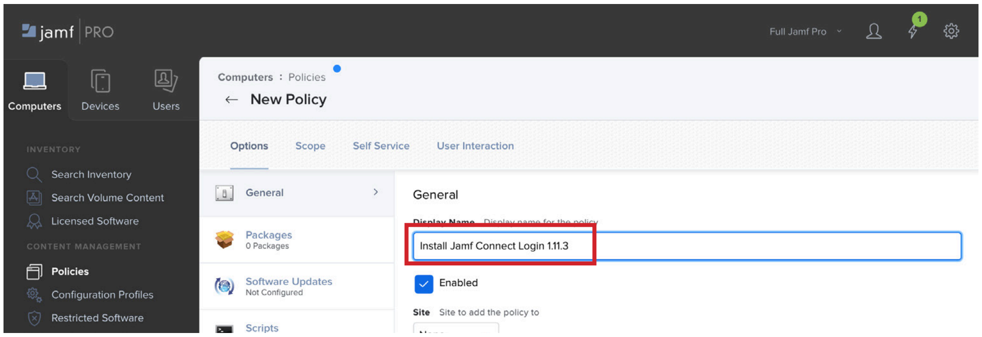
Option A:

In this option, you will configure Jamf Connect Login to deploy to computers with existing local users.

1. Click Computers.
2. Click Policies.
3. Click New.



4. Enter **Install Jamf Connect Login** (followed by the version number) for the Display Name.

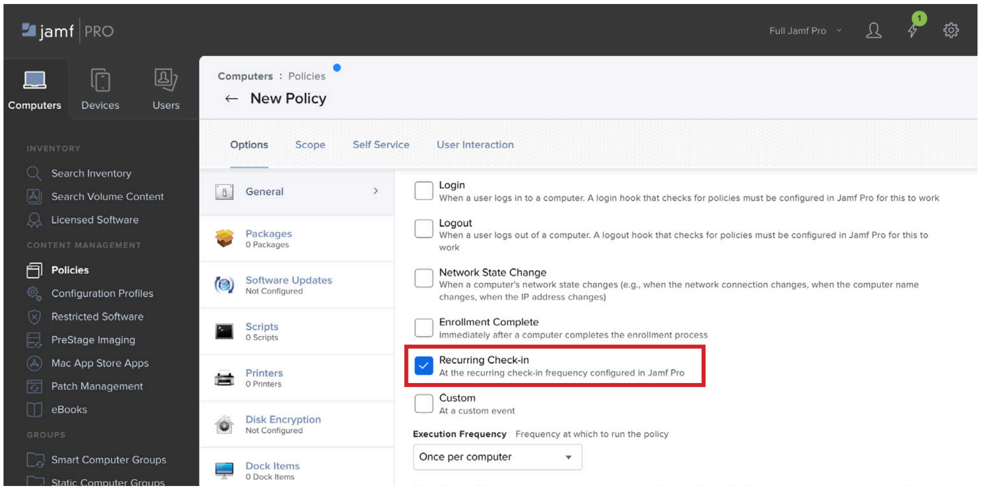


Display Name Display name for the policy
Install Jamf Connect Login 1.11.3

☑ Enabled

Site Site to add the policy to

5. In the Trigger section, select the checkbox for Recurring Check-in.



☐ Login
When a user logs in to a computer. A login hook that checks for policies must be configured in Jamf Pro for this to work

☐ Logout
When a user logs out of a computer. A logout hook that checks for policies must be configured in Jamf Pro for this to work

☐ Network State Change
When a computer's network state changes (e.g., when the network connection changes, when the computer name changes, when the IP address changes)

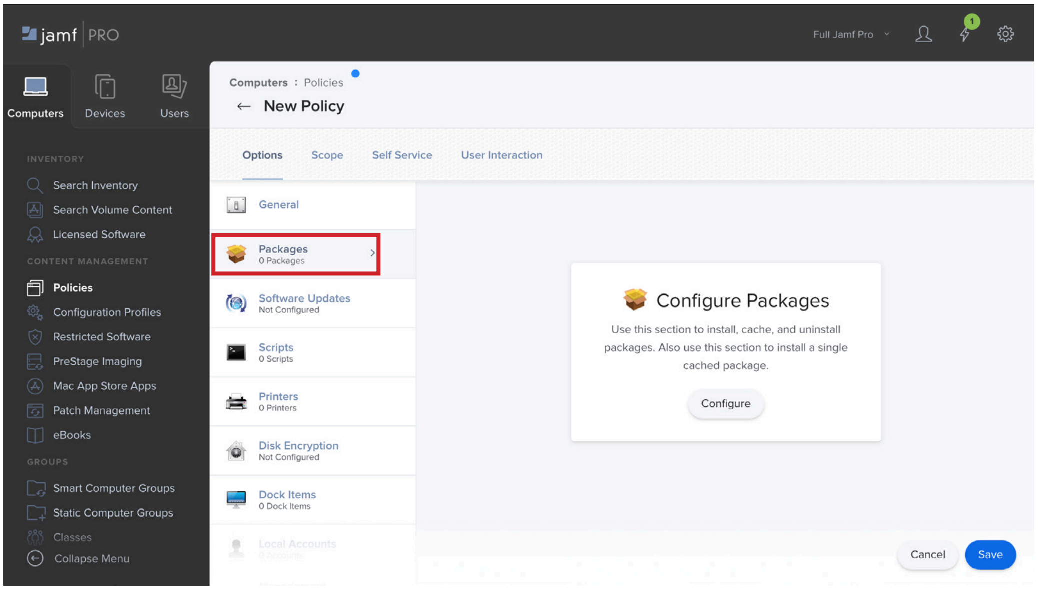
☐ Enrollment Complete
Immediately after a computer completes the enrollment process

☑ Recurring Check-in
At the recurring check-in frequency configured in Jamf Pro

☐ Custom
At a custom event

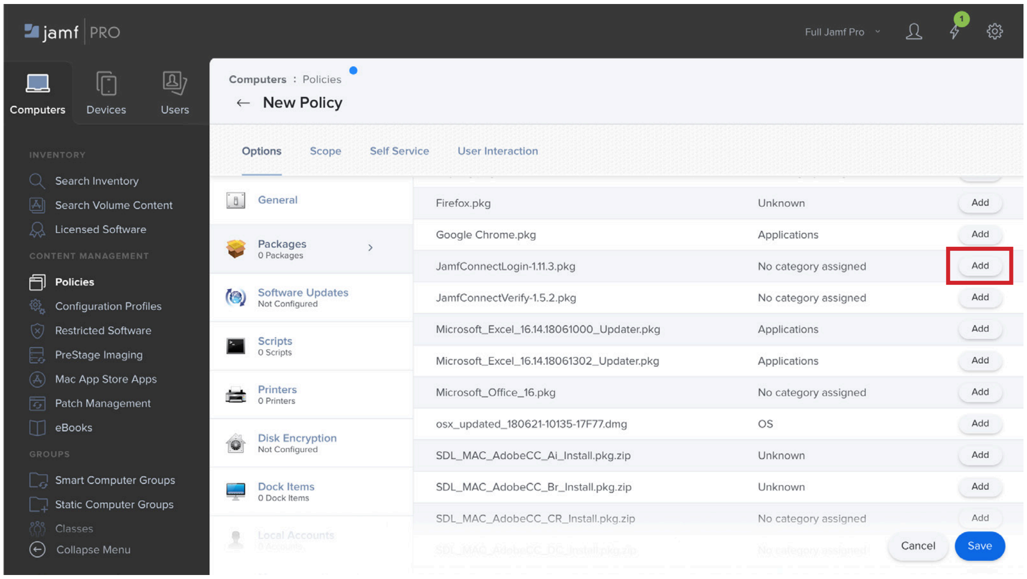
Execution Frequency Frequency at which to run the policy
Once per computer

6. Leave the Execution Frequency as "Once per Computer."
7. In the list of payloads, click Packages.



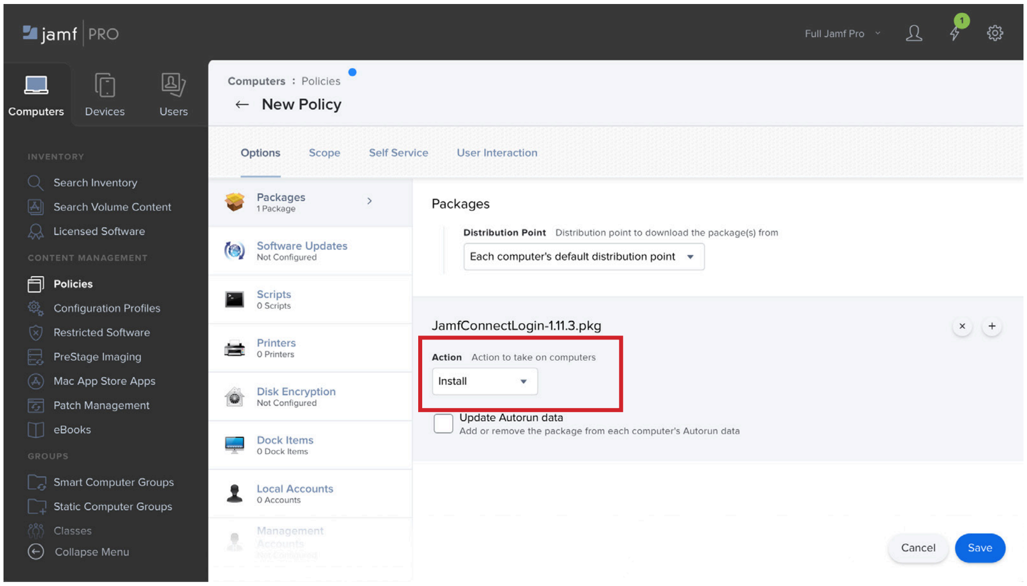
Use this section to install, cache, and uninstall packages. Also use this section to install a single cached package.

8. Click Configure.
9. Next to the package for Jamf Connect Login, click Add.



Firefox.pkg	Unknown	Add
Google Chrome.pkg	Applications	Add
JamfConnectLogin-1.11.3.pkg	No category assigned	Add
JamfConnectVerify-1.5.2.pkg	No category assigned	Add
Microsoft_Excel_16.14.18061000_Updater.pkg	Applications	Add
Microsoft_Excel_16.14.18061302_Updater.pkg	Applications	Add
Microsoft_Office_16.pkg	No category assigned	Add
osx_updated_180621-10135-17F77.dmg	OS	Add
SDL_MAC_AdobeCC_Ai_Install.pkg.zip	Unknown	Add
SDL_MAC_AdobeCC_Br_Install.pkg.zip	Unknown	Add
SDL_MAC_AdobeCC_CR_Install.pkg.zip	No category assigned	Add
SDL_MAC_AdobeCC_DC_Install.pkg.zip	No category assigned	

9. Leave the Action as Install.



Packages

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

Each computer's default distribution point

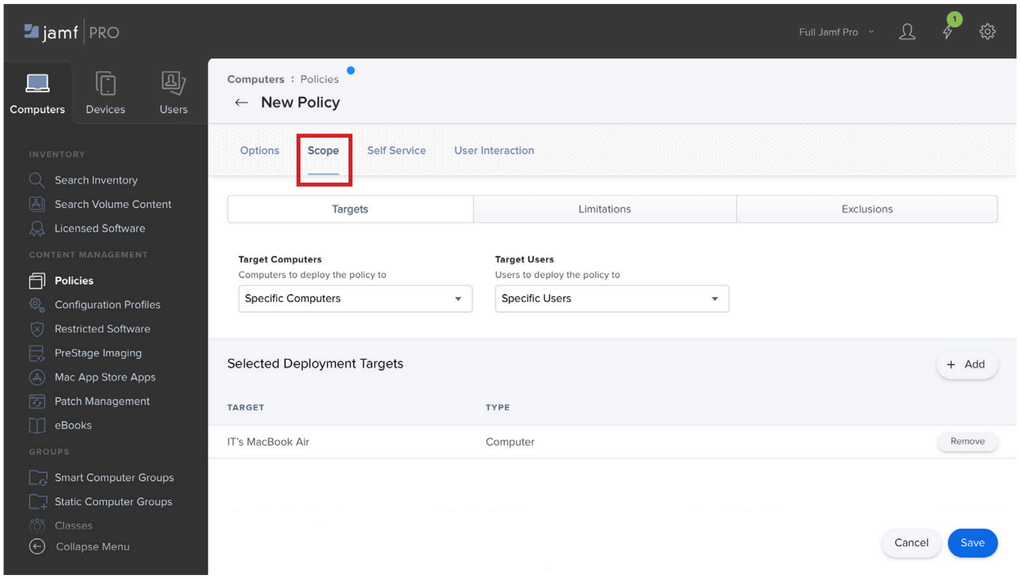
JamfConnectLogin-1.11.3.pkg

Action Action to take on computers

Install

□ Update Autorun data
Add or remove the package from each computer's Autorun data

10. Select Scope and add the target destination for computers that will use Jamf Connect.



Target Computers Computers to deploy the policy to

Specific Computers

Target Users Users to deploy the policy to

Specific Users

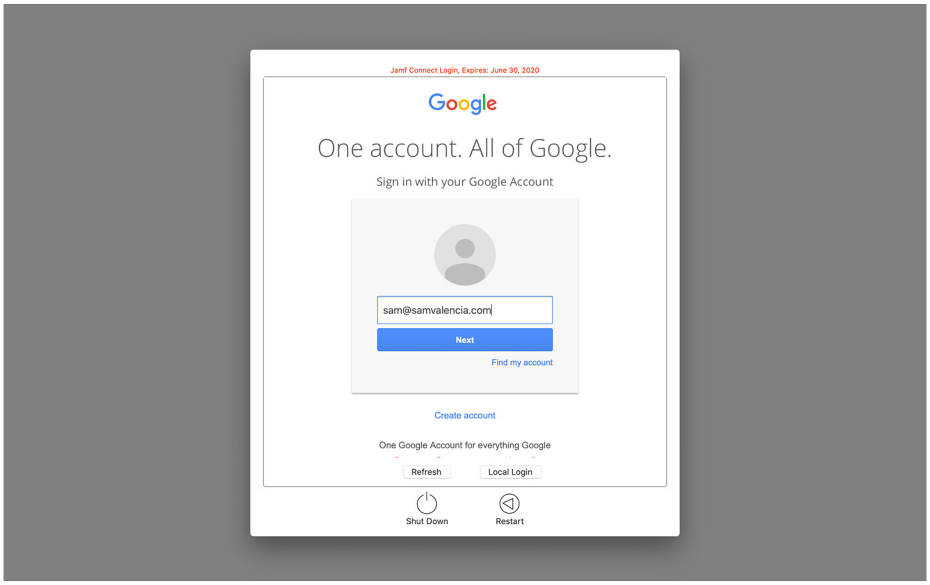
Selected Deployment Targets

TARGET	TYPE
IT's MacBook Air	Computer

11. Click Save.

Once the Jamf Connect Login package and configuration profile have been deployed, you are now ready to test authentication.

1. Turn on the target Mac computer.
2. Enter a user email address in your G Suite environment and click Next.



Jamf Connect Login, Expires: June 30, 2020

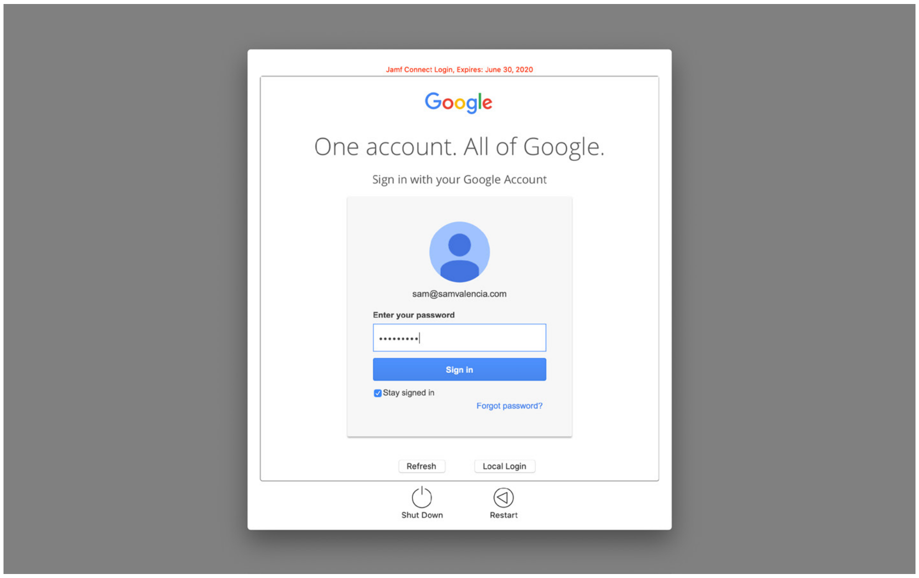
One account. All of Google.

Sign in with your Google Account

sam@samvalencia.com

One Google Account for everything Google

3. Enter the account password and click Sign In.



Jamf Connect Login, Expires: June 30, 2020

One account. All of Google.

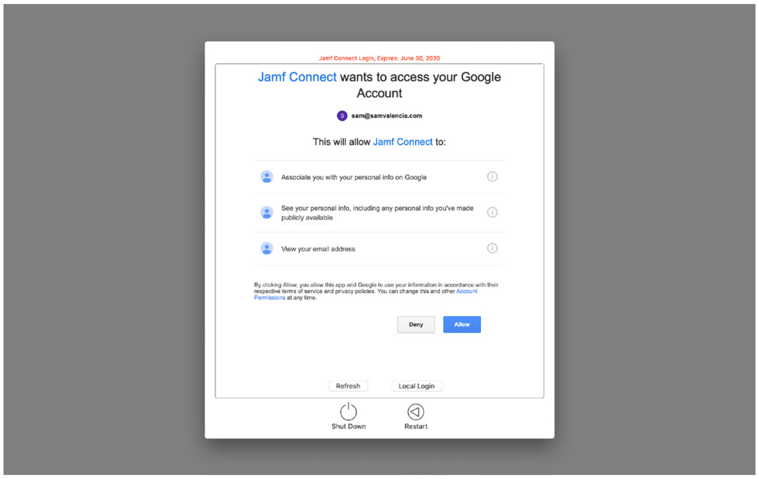
Sign in with your Google Account

sam@samvalencia.com

Enter your password: •••••••••

☑ Stay signed in

4. Confirm that Jamf Connect displays a message with information about what you will be allowing Jamf Connect to have access to.
5. Click Allow.



Jamf Connect Login, Expires: June 30, 2020

Jamf Connect wants to access your Google Account

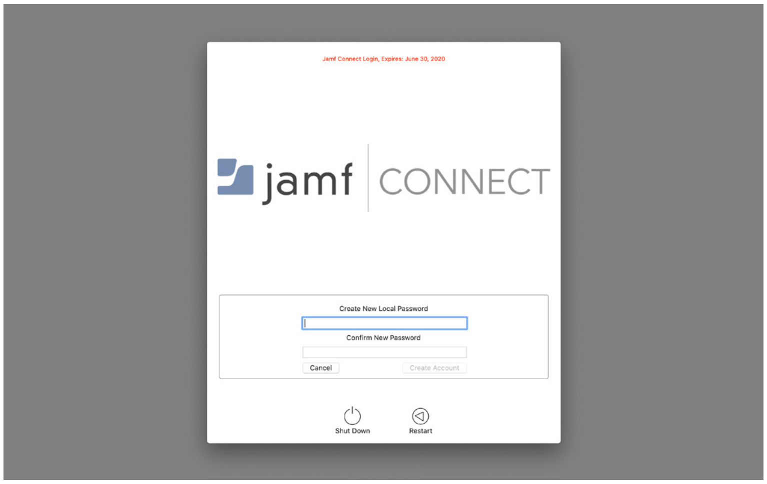
sam@samvalencia.com

This will allow Jamf Connect to:

- Associate you with your personal info on Google
- See your personal info, including any personal info you've made publicly available
- View your email address

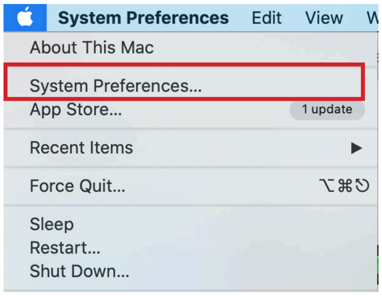
By clicking Allow, you allow this app and Google to use your information in accordance with their respective terms of service and privacy policies. You can change this and other Account Permissions at any time.

6. Enter and re-enter your G Suite password. Click Create Account.
   NOTE: Jamf Connect Login does NOT synchronize your Google password with the local account password after creation.

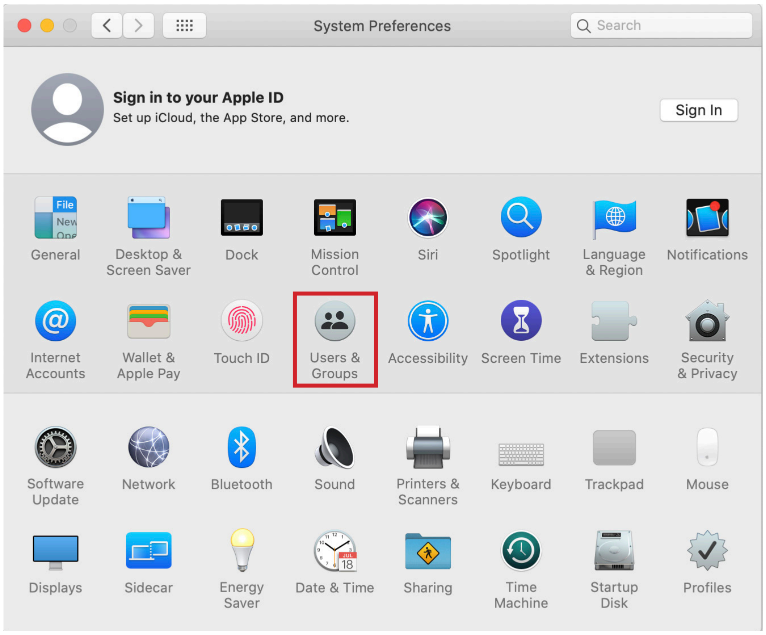


Jamf Connect Login, Expires: June 30, 2020

7. Once logged in, click the Apple menu and choose System Preferences.



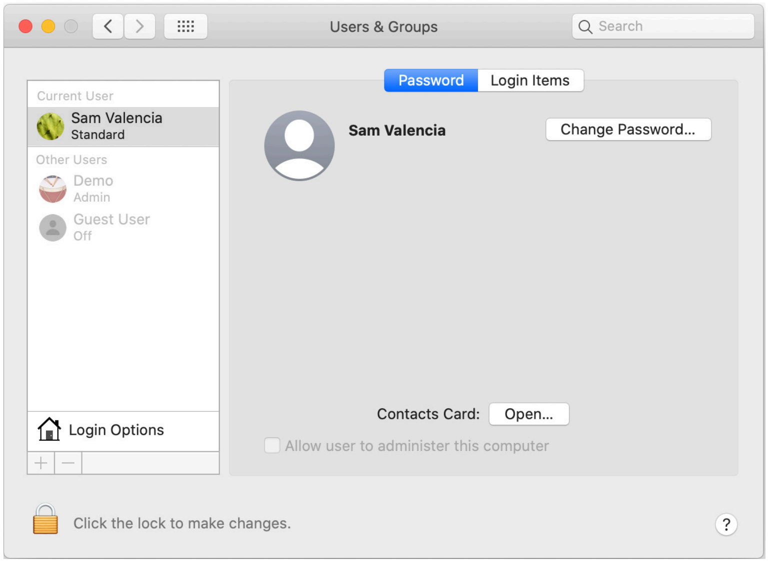
8. Click Users & Groups.



9. Select the newly-created account.

Note the following details:

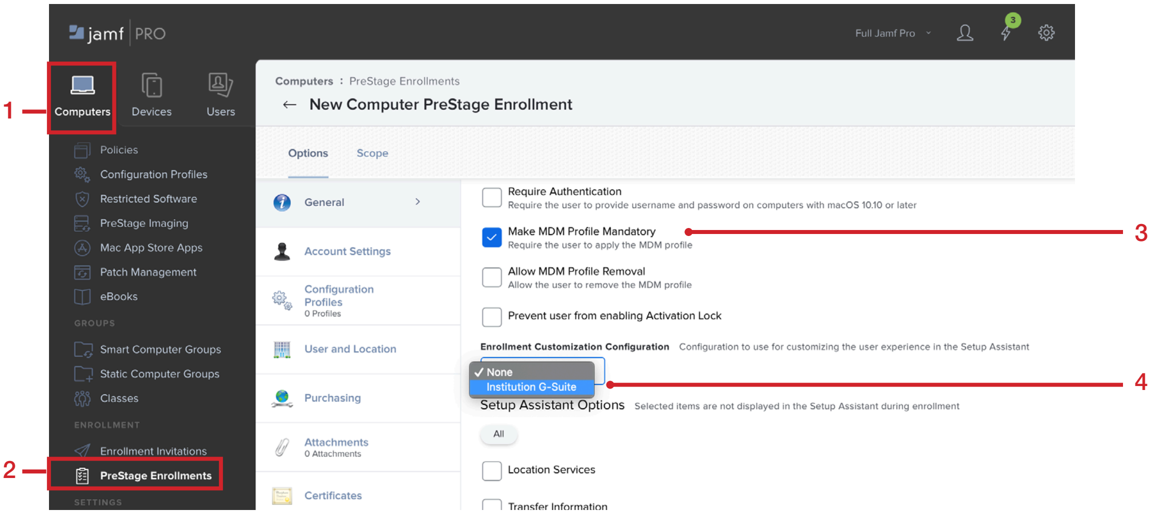
- The account created by this process is a Standard account. As of this writing, Admin Roles is a feature not currently supported with Google ID: https://docs.jamf.com/jamf-connect/1.19.0/administrator-guide/
- Standard accounts cannot enable FileVault
- Standard accounts can be promoted to admin.



Option B

Follow the steps in this option to deploy Jamf Connect Login to computers that are enrolled in Apple Business Manager and available in a PreStage scope. In order to perform these tasks, you need to integrate Jamf Pro with Google Secure LDAP. Follow our guide to learn more: https://hcsonline.com/support/white-papers/how-to-integrate-jamf-pro-with-google-secure-ldap-as-a-cloud-identity-provider

1. Click Computers.
2. Click PreStage Enrollments.
3. In the General pane, confirm that the "Make MDM Profile Mandatory" option is selected.
4. Click the Enrollment Customization Configuration menu then choose your Google LDAP configuration (created separately).



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

☑ Make MDM Profile Mandatory
Require the user to apply the MDM profile

□ Allow MDM Profile Removal
Allow the user to remove the MDM profile

□ Prevent user from enabling Activation Lock

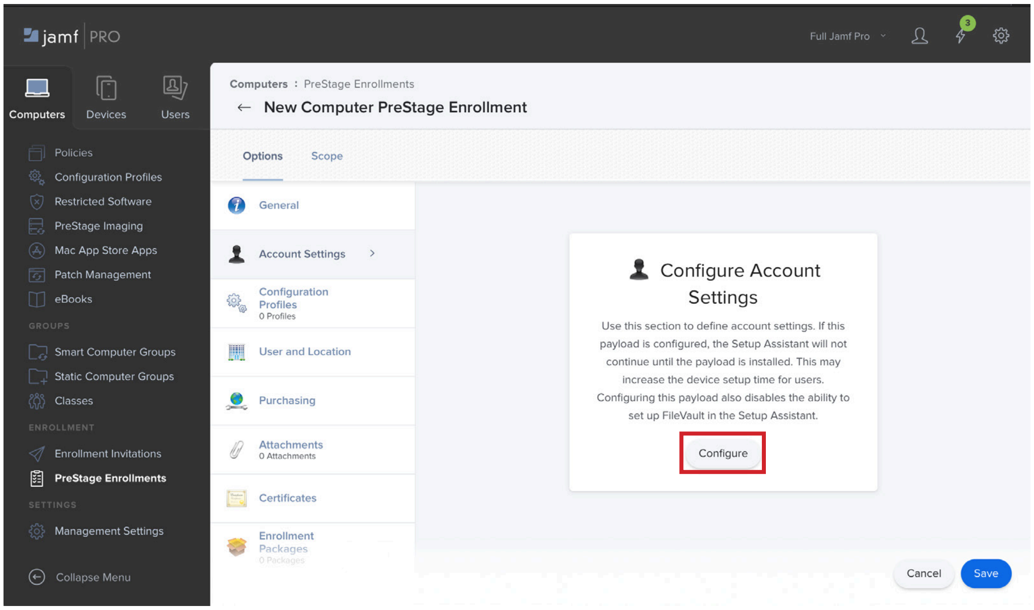
Enrollment Customization Configuration Configuration to use for customizing the user experience in the Setup Assistant

Setup Assistant Options Selected items are not displayed in the Setup Assistant during enrollment

□ Location Services

□ Transfer Information

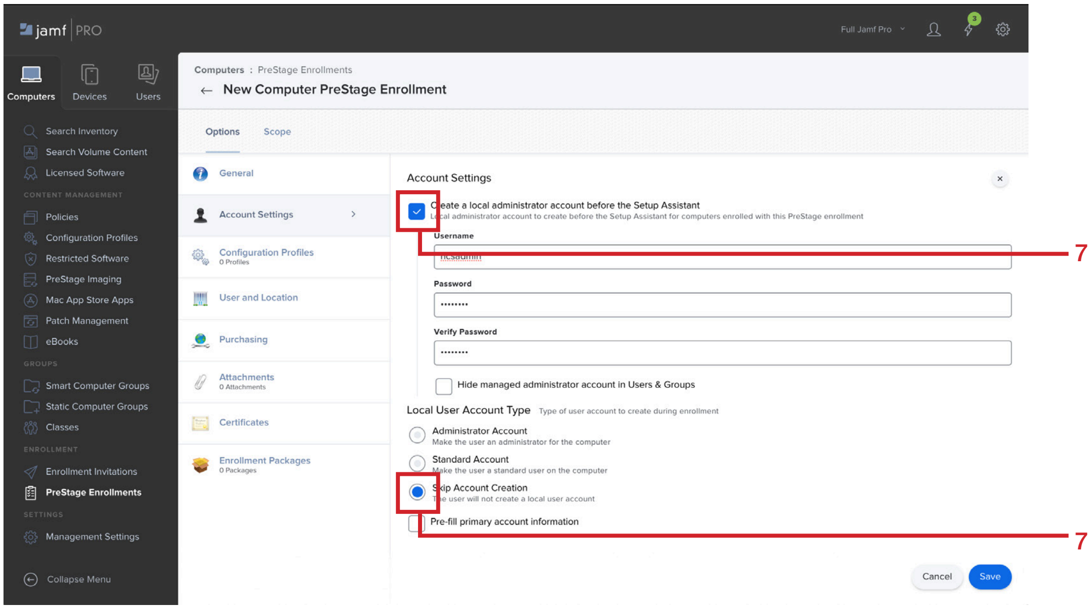
5. Select which options you would like to appear during Setup Assistant.
6. Click Account Settings and click Configure.



Configure Account Settings

Use this section to define account settings. If this payload is configured, the Setup Assistant will not continue until the payload is installed. This may increase the device setup time for users. Configuring this payload also disables the ability to set up FileVault in the Setup Assistant.

7. Select the checkbox for "Create a local administrator account before the Setup Assistant."
8. In the Username, Password, and Verify Password fields, enter your in administrator credentials.
9. Under Local User Account Type, select Skip Account Creation. Click Save.



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: hcsadmin

Password: ••••••••

Verify Password: ••••••••

□ Hide managed administrator account in Users & Groups

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

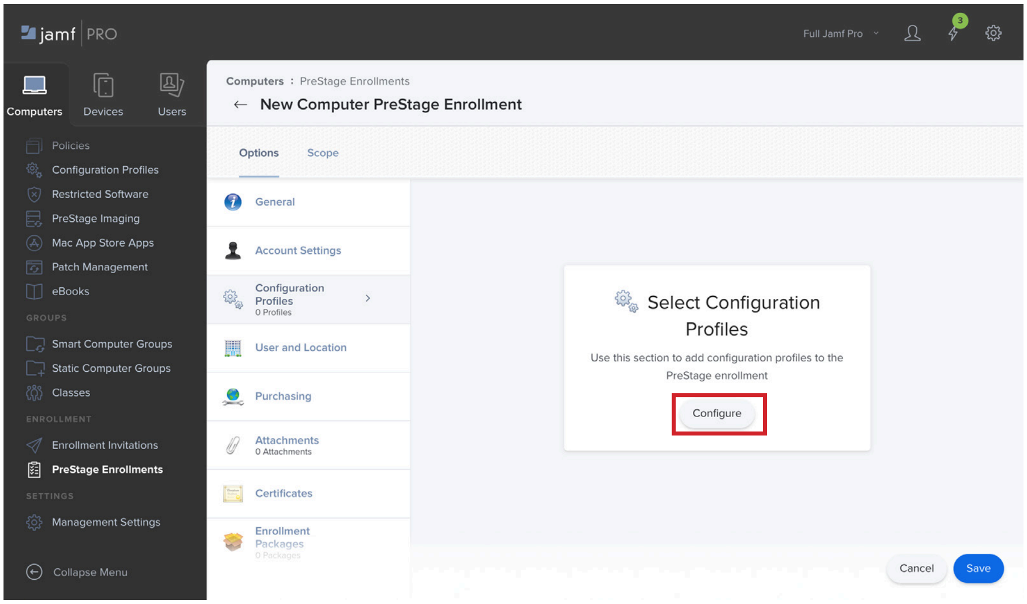
○ Administrator Account
Make the user an administrator for the computer

○ 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

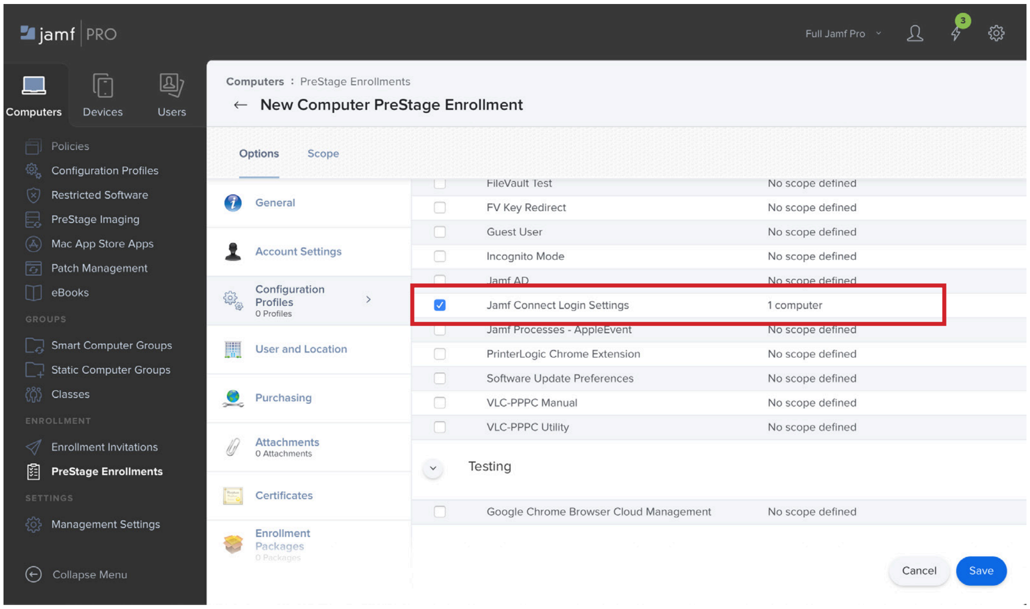
10. Click Configuration Profiles and click Configure.



Select Configuration Profiles

Use this section to add configuration profiles to the PreStage enrollment

11. Select the Jamf Connect Login profile created in Section 4.



Computers : PreStage Enrollments

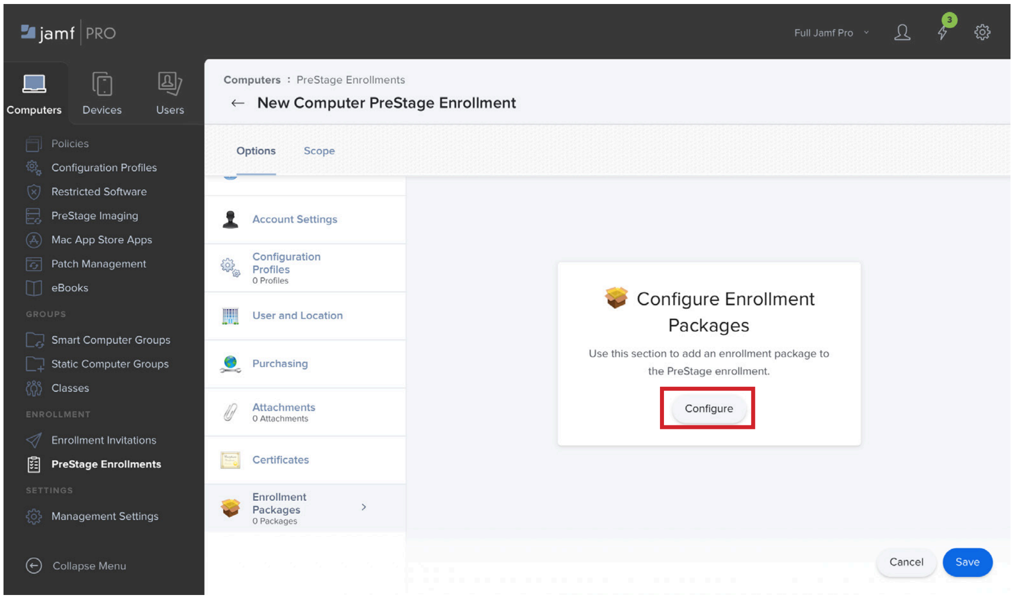
New Computer PreStage Enrollment

□	FileVault Test	No scope defined
□	FV Key Redirect	No scope defined
□	Guest User	No scope defined
□	Incognito Mode	No scope defined
□	Jamf AD	No scope defined
☑	Jamf Connect Login Settings	1 computer
□	Jamf Processes - AppleEvent	No scope defined
□	PrinterLogic Chrome Extension	No scope defined
□	Software Update Preferences	No scope defined
□	VLC-PPPC Manual	No scope defined
□	VLC-PPPC Utility	No scope defined

Testing

□	Google Chrome Browser Cloud Management	No scope defined

12. Select Enrollment Package and click Configure.



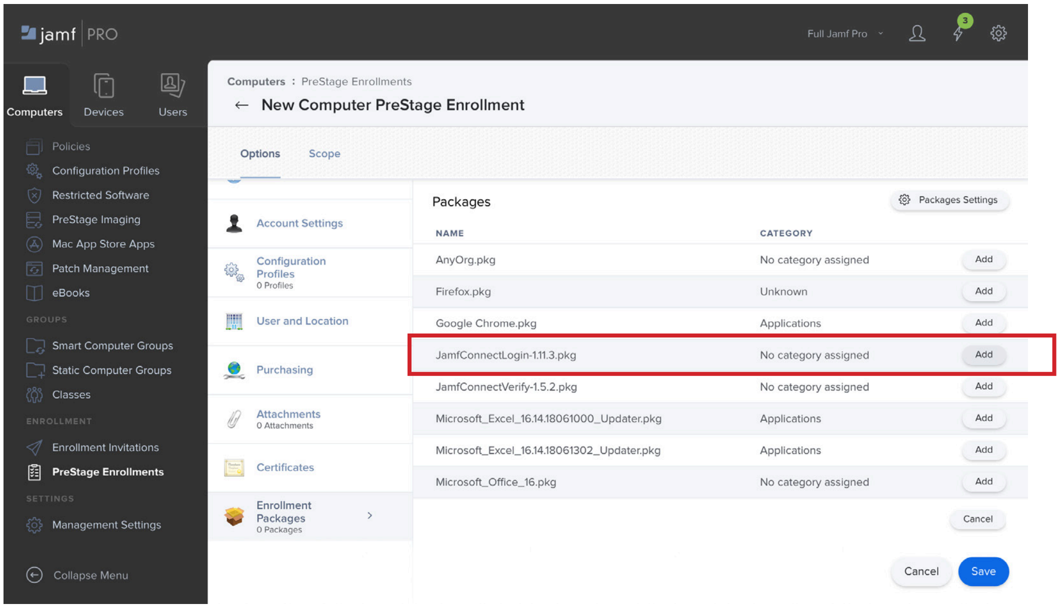
Computers : PreStage Enrollments

New Computer PreStage Enrollment

Configure Enrollment Packages

Use this section to add an enrollment package to the PreStage enrollment.

13. Next to your Jamf Connect Login package click Add.



NAME	CATEGORY	
AnyOrg.pkg	No category assigned	Add
Firefox.pkg	Unknown	Add
Google Chrome.pkg	Applications	Add
JamfConnectLogin-1.11.3.pkg	No category assigned	Add
JamfConnectVerify-1.5.2.pkg	No category assigned	Add
Microsoft_Excel_16.14.18061000_Updater.pkg	Applications	Add
Microsoft_Excel_16.14.18061302_Updater.pkg	Applications	Add
Microsoft_Office_16.pkg	No category assigned	Add

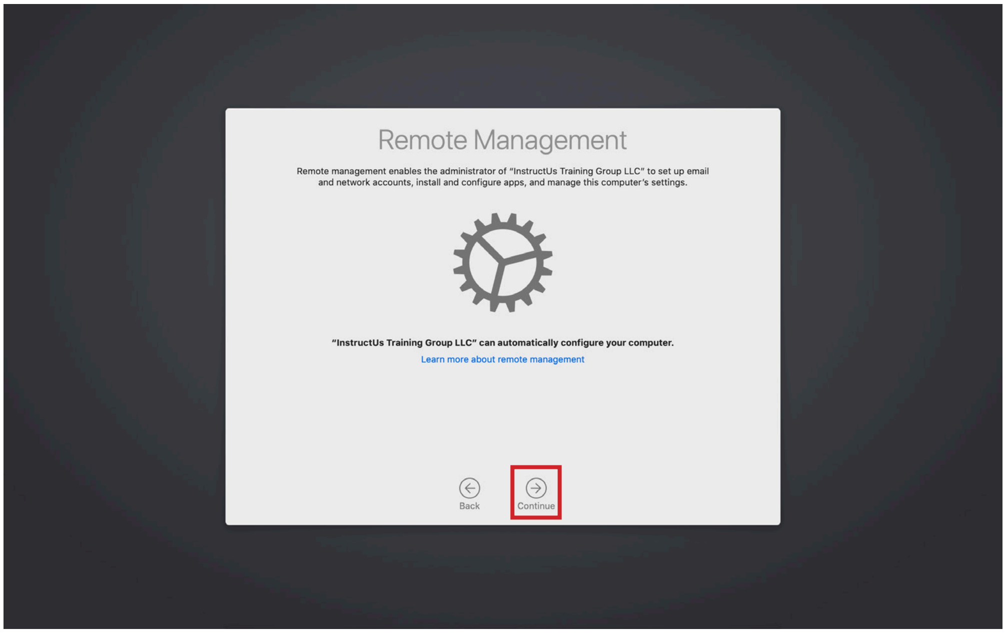
14. Click Scope to select your target computers.

15. Click Save.

You can now test authentication using a computer that has not yet been set up, and that is in the you scope of the PreStage just created.

1. Turn on the test Mac computer.

2. After connecting to a network in Setup Assistant, you should be presented with the Remote Management window. Click Continue.



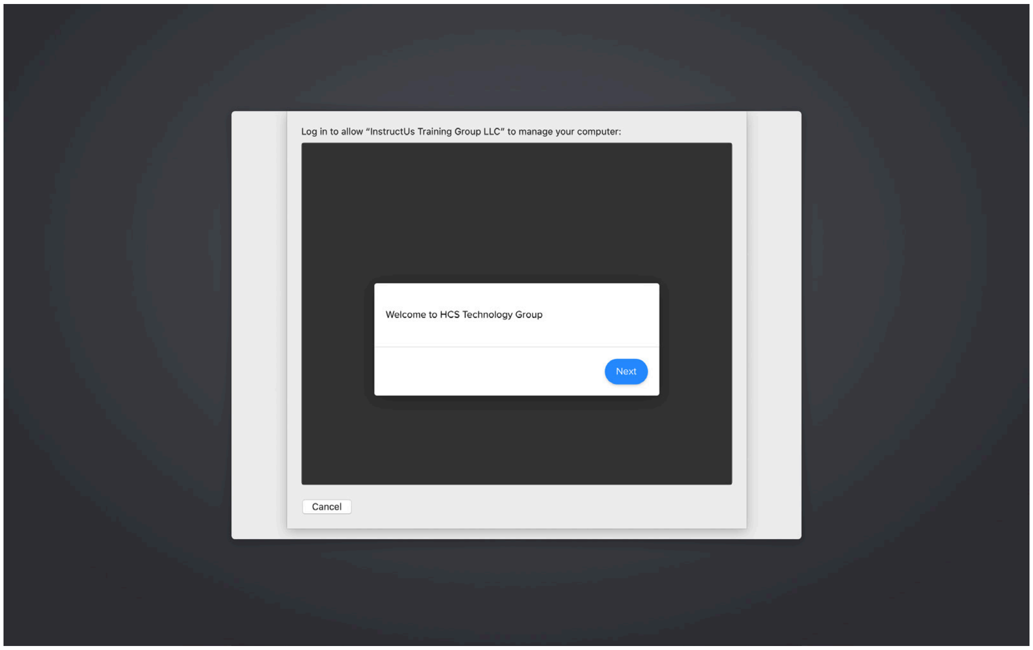
Remote Management

Remote management enables the administrator of "InstructUs Training Group LLC" to set up email and network accounts, install and configure apps, and manage this computer's settings.

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

Learn more about remote management

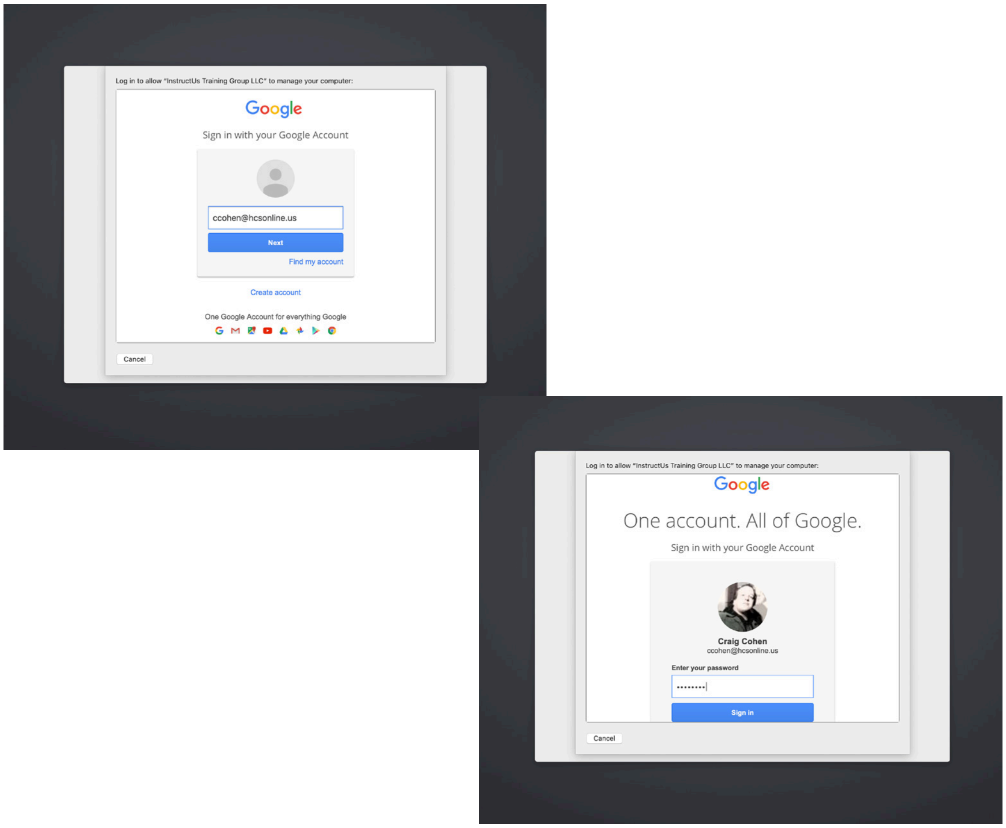
3. If you have configured verbiage for your Enrollment Customization in Jamf Pro, you would see something similar to the figure below.



Log in to allow "InstructUs Training Group LLC" to manage your computer:

Welcome to HCS Technology Group

4. At the Google authentication window, enter your G Suite credentials.



Log in to allow "InstructUs Training Group LLC" to manage your computer:

Google

Sign in with your Google Account

ccohen@hcsonline.us

Log in to allow "InstructUs Training Group LLC" to manage your computer:

Google

One account. All of Google.

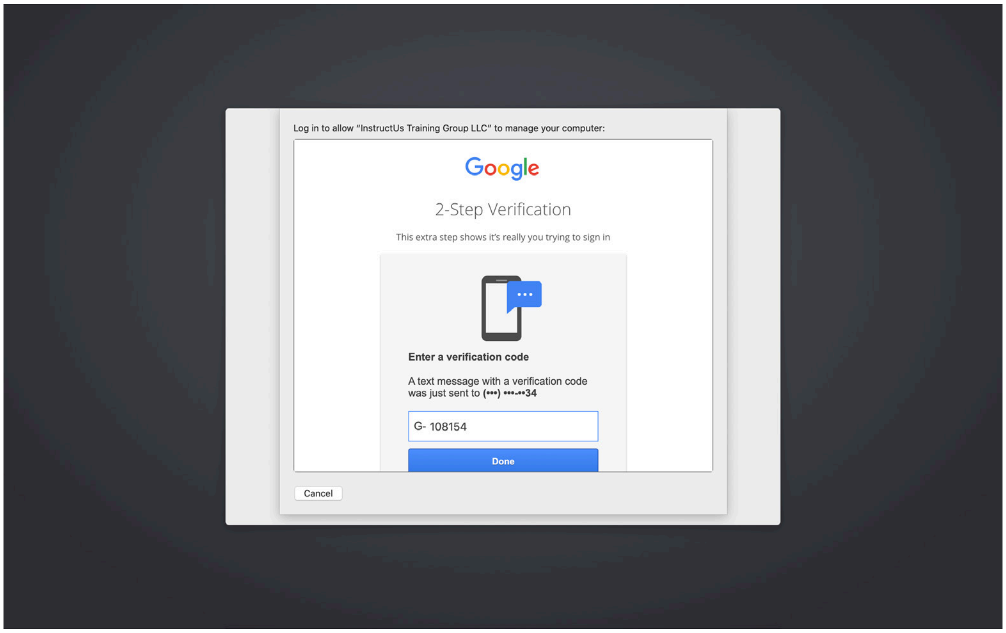
Sign in with your Google Account

Craig Cohen
ccohen@hcsonline.us

Enter your password

••••••••

5. If you have 2-step verification enabled, enter your verification code then click Done.



Log in to allow "InstructUs Training Group LLC" to manage your computer:

2-Step Verification

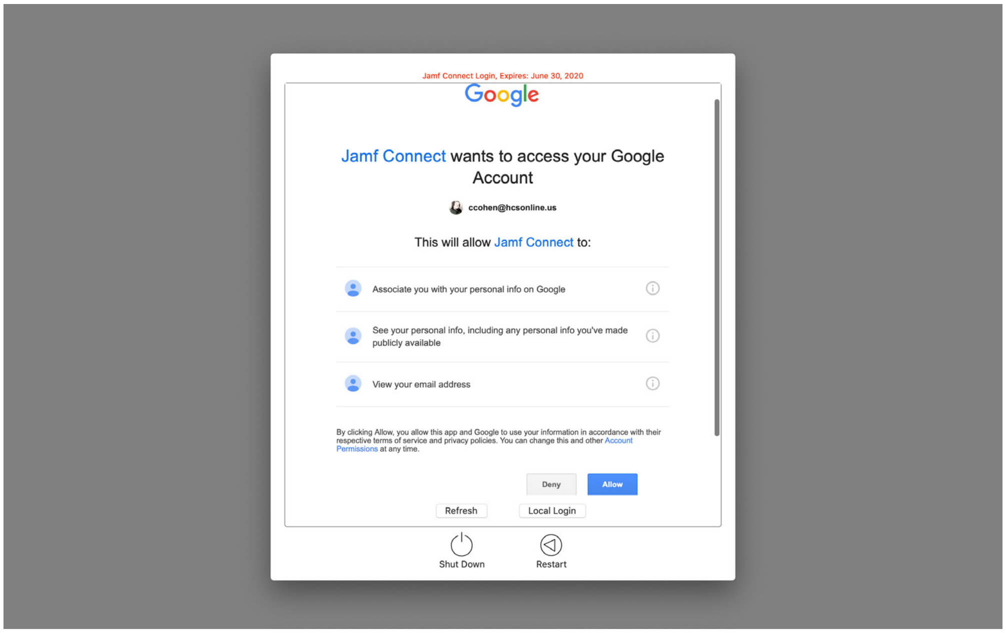
This extra step shows it's really you trying to sign in

Enter a verification code

A text message with a verification code was just sent to **(•••) •••-••34**

G- 108154

6. In the message that indicates what you will be allowing Jamf Connect to have access to, click Allow.



Jamf Connect Login, Expires: June 30, 2020

Jamf Connect wants to access your Google Account

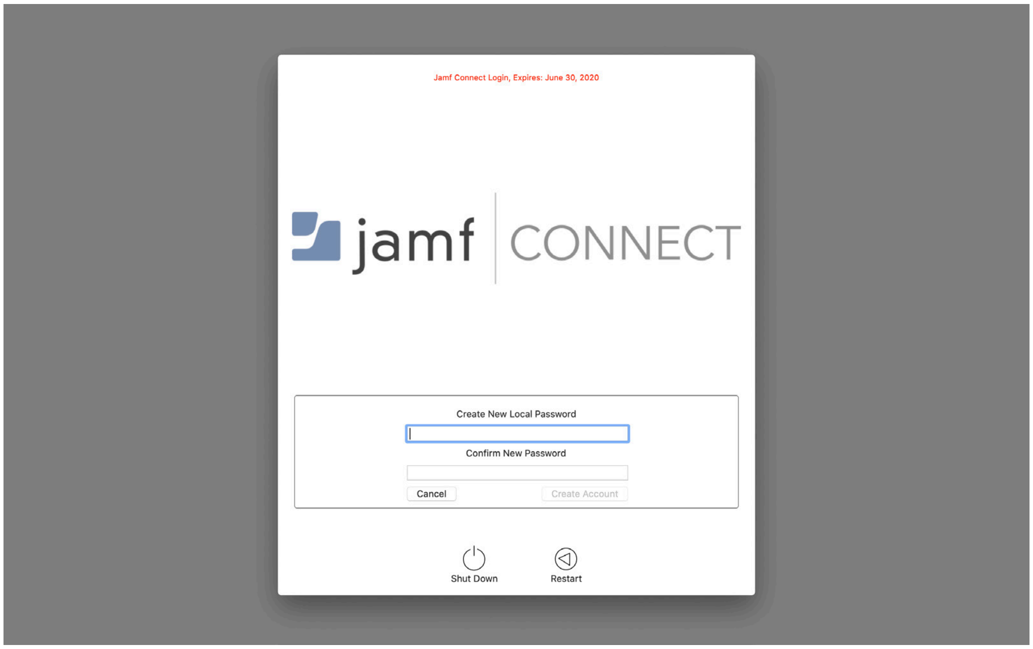
ccohen@hcsonline.us

This will allow Jamf Connect to:

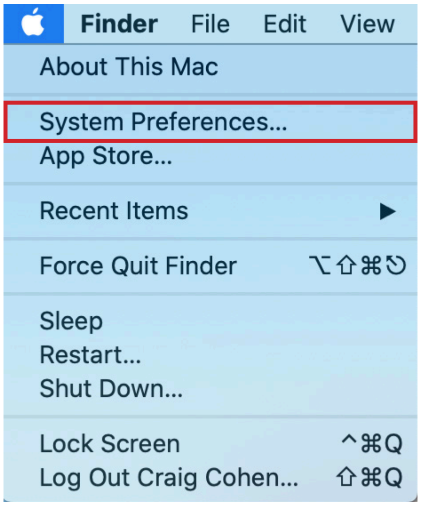
- Associate you with your personal info on Google
- See your personal info, including any personal info you've made publicly available
- View your email address

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.

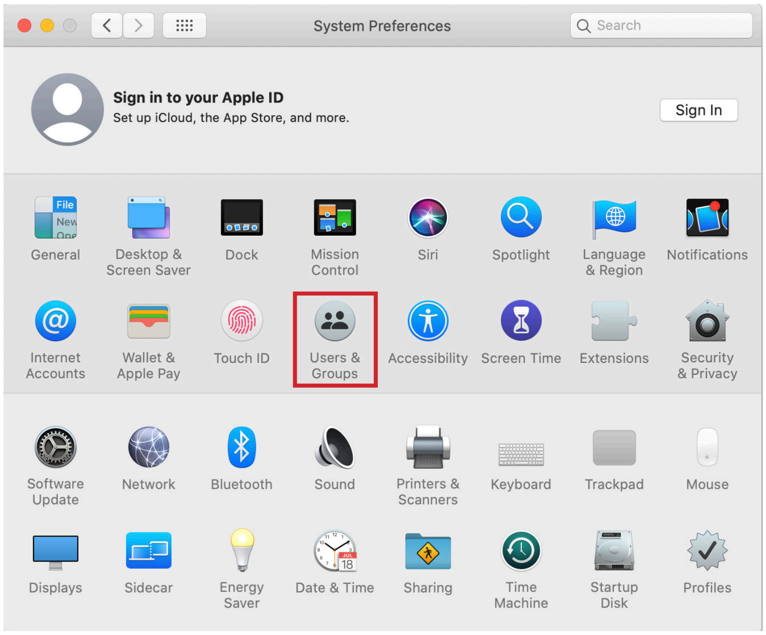
7. Enter and re-enter your G Suite password.
8. Click Create Account.
   NOTE: Jamf Connect Login does NOT synchronize your Google password with the local account password after creation.



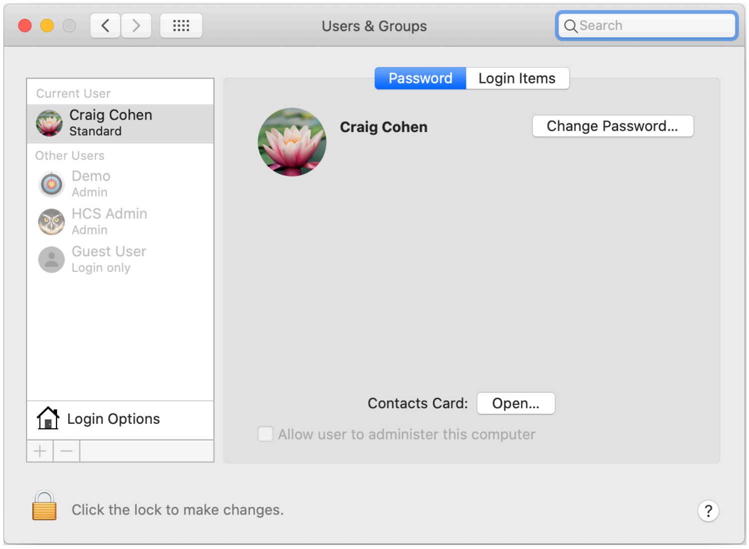
9. Once logged in, click the Apple menu and choose System Preferences.



10. Click Users & Groups.



10. Select the newly created account.
    Note the following details:
    - The account created by this process is a Standard account. As of this writing, Admin Roles is a feature not currently supported with Google ID: https://docs.jamf.com/jamf-connect/1.19.0/administrator-guide/
    - Standard accounts cannot enable FileVault
    - Standard accounts can be promoted to admin



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

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

For more white papers, visit https://hcsonline.com/support/white-papers.

For more information about HCS, visit https://hcsonline.com.