How to Integrate Jamf Pro with Google Secure LDAP as a Cloud Identity Provider

Contents

Integrating with Cloud Identity Providers, which is similar to integrating with an LDAP directory service, allows you to do the following:

- Look up and populate user information from the secure LDAP service for inventory purposes.
- Add Jamf Pro user accounts or groups from the secure LDAP service.
- Require users to log in to Self Service *or* the enrollment portal using their LDAP directory accounts.
- Require users to log in during mobile device setup using their LDAP directory accounts.
- Base the scope of remote management tasks on users or groups from the secure LDAP service.

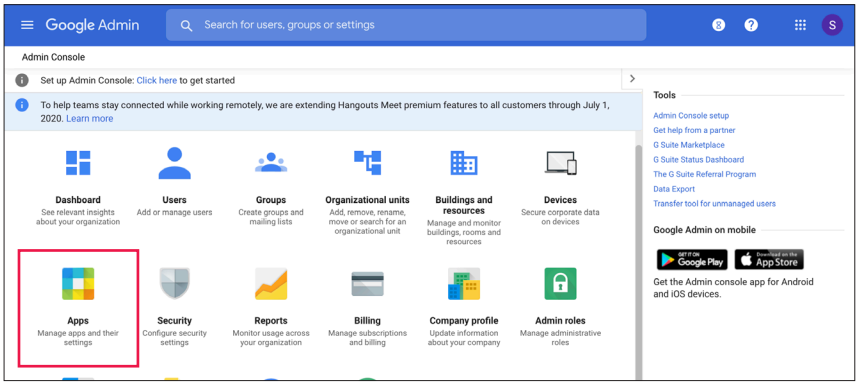
What you need

- Jamf Pro 10.19 or later (if your Jamf Pro server is on-premises, whenever this guide uses a jamfcloud.com based URL, replace it with your URL including the port number, which is 8443 by default)
- Google G Suite (Enterprise, Business, Basic, or Drive Enterprise) and Cloud Identity Premium" with “The Google Secure LDAP service is available with G Suite Enterprise, G Suite Enterprise for Education, G Suite for Education or Cloud Identity Premium
- To test using a Google account during the Setup Assistant, you'll need to have your Jamf Pro server integrated with Apple Business Manager or Apple School Manager, and an eligible Mac with macOS 10.15 or later at the Welcome screen, assigned by Apple Business Manager or Apple School Manager to your Jamf Pro server.

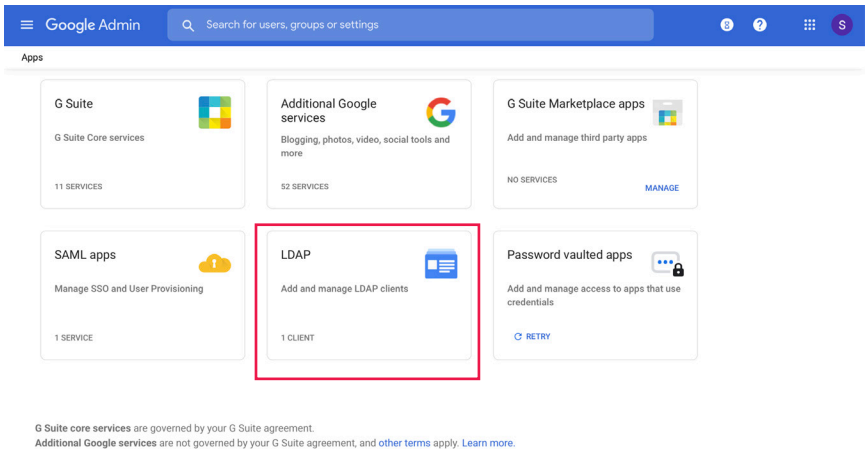
Configure Google and add LDAP clients to the service.

1. Sign in to your Google Admin console at admin.google.com. Be sure to sign in using your super administrator account, and not your personal Gmail account.

2. Select Apps.

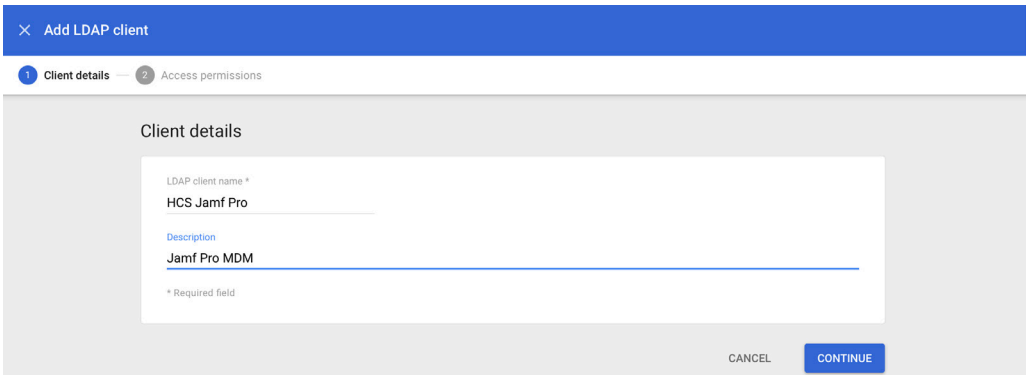


3. Select LDAP.

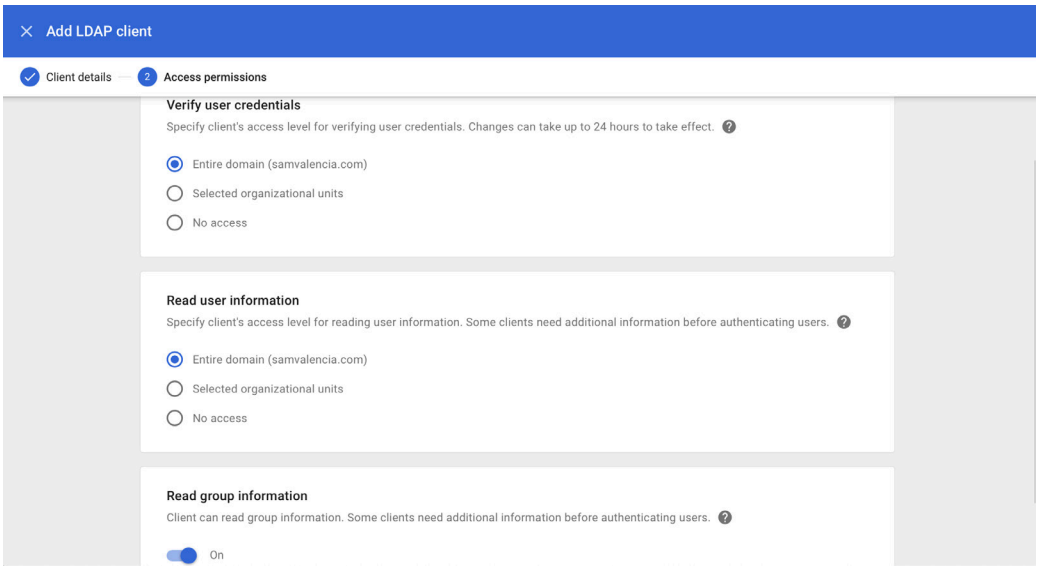


4. If you already have LDAP clients defined, click "Add Client." If you don't have LDAP clients defined yet, click "Add LDAP Client."

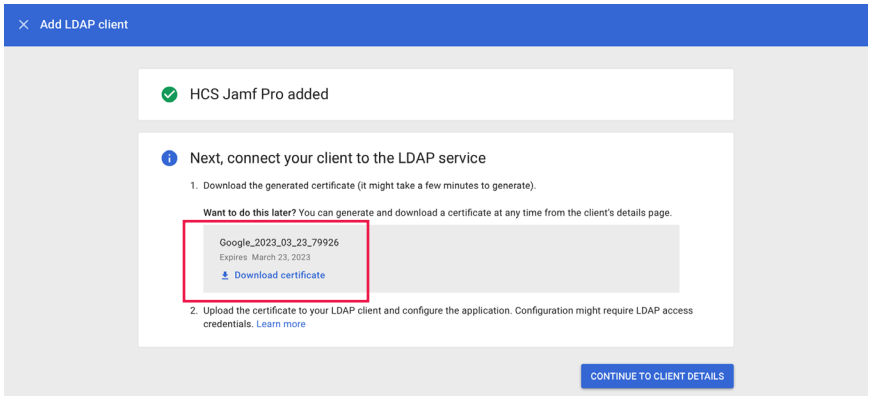
5. Enter a name in the LDAP client name field—for example, **HCS Jamf Pro**.
   Optional: Enter a description for the LDAP client—for example, **Jamf Pro MDM**.



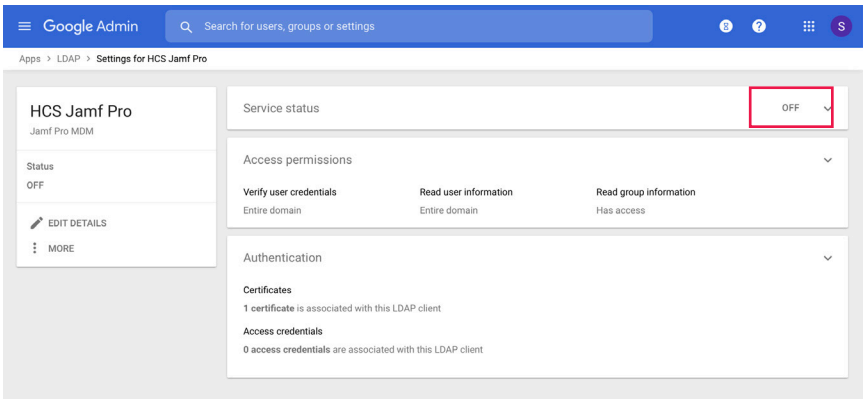
6. Click Continue.
7. Configure access permissions according to your environment. You can limit access to specific organizational units, but this guide illustrates enabling access for the entire domain, and enabling reading group access.



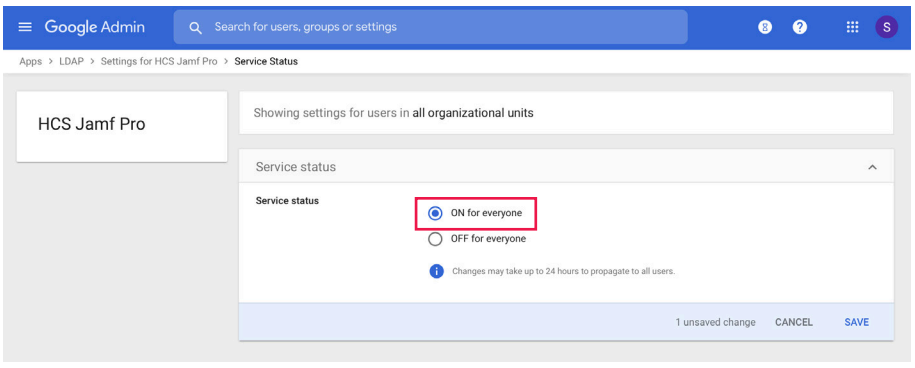
8. Click Add LDAP Client.
9. Click "Download certificate." You may need to wait a few minutes for Google to generate a certificate before the "Download certificate" link appears. Because there are only a few more steps before you require this certificate in order to continue with this guide, we recommend that you wait for the "Download certificate" link to be displayed before continuing with this guide.



10. If your browser displays a dialog that asks if you want to allow downloads from "admin.google.com," click Allow.
11. Click Continue To Client Details.
12. In the upper-right corner of the browser window, if the LDAP service status is listed as Off, click the Off button.

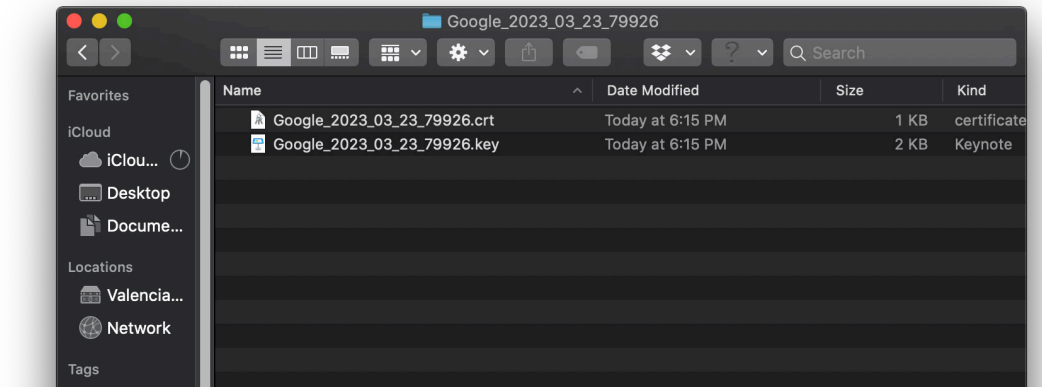


13. Select the “On for everyone” radio button and click Save.



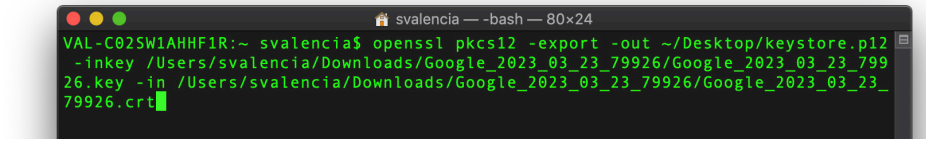
Convert the Google private key to a PKCS12 format file that you can upload to Jamf Pro

1. When you clicked "Download certificate," your browser downloaded an archived file in ZIP format. If your browser didn't automatically unzip the .zip file you downloaded, then in the Finder, double-click the .zip file to unarchive it.
2. Confirm that the unarchived folder contains the following files:
   - One certificate (.crt) file
   - One private key (.key) file.

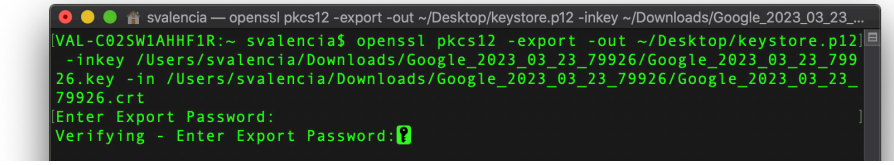


3. To generate the PKCS12 (.p12) keystore file, use the **openssl** command with a syntax similar to the following. The example in the following figure creates a new keystore file on the desktop of the currently-logged-in user. We recommend that to avoid typos, you drag each appropriate file from the Finder to Terminal. Enter the command without line breaks, or use the backslash character (\) to prevent the shell from running the command before you're finished entering the command:

```
openssl pkcs12 -export \
-out  ~/Desktop/keystore.p12 \
-inkey <path to the saved>/privatekey.key \
-in <path to the saved>/certificate.crt
```



4. The **openssl** command prompts you for a password to secure the keystore file. We recommend that you use a password management system to a) generate a secure password and b) document it for your team. Enter a secure password, then press Return.
5. Enter the password again to verify it, then press Return.

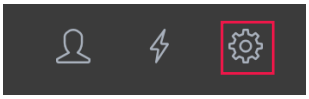


6. In the Finder, confirm that you see the generated PKCS12 (.p12) keystore file for your Google Cloud Identity Provider instance. You'll use it in the next section.

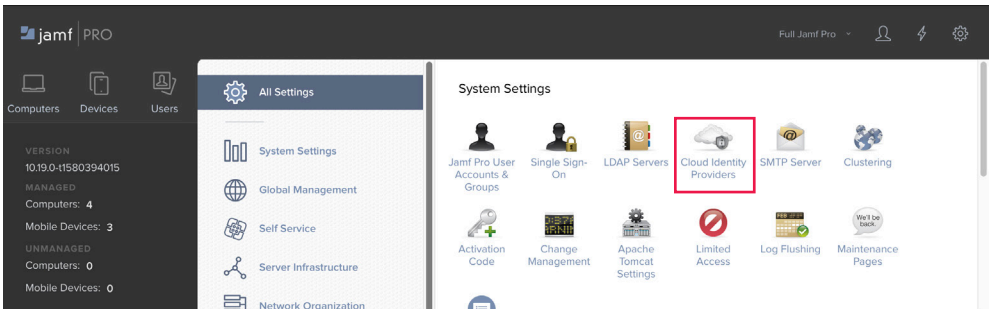
Connect your LDAP client (Jamf Pro) to the Secure LDAP service

The Secure LDAP service uses TLS client certificates as the primary authentication mechanism.

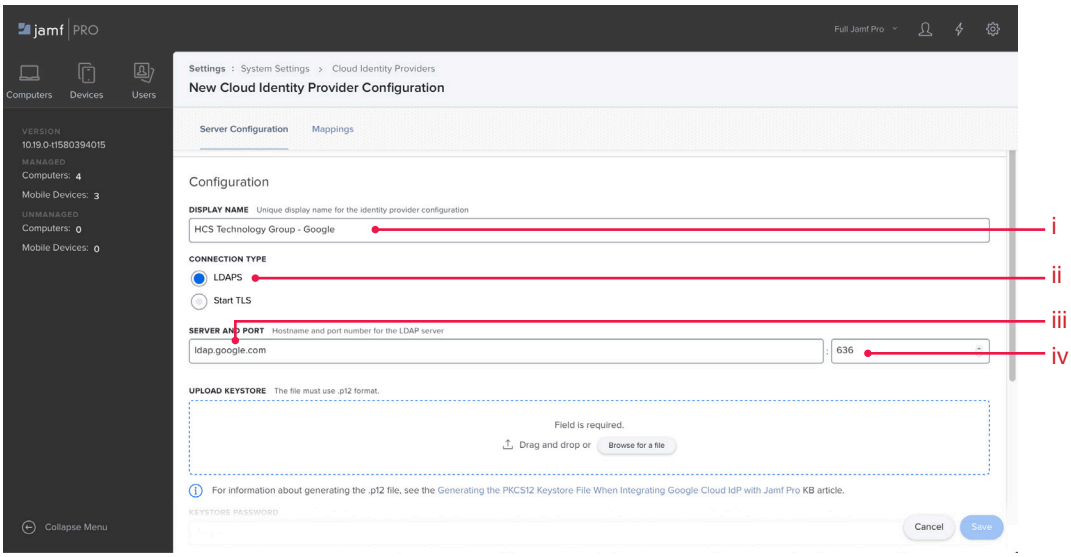
1. Log in to Jamf Pro.
2. In the upper-right corner of the page, click Settings (looks like a gear).



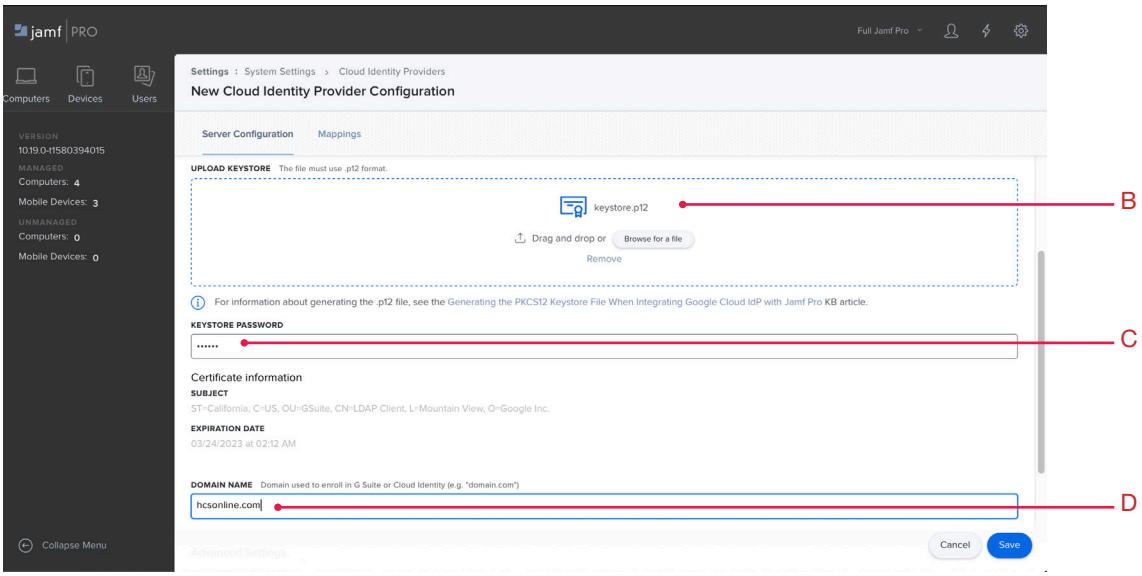
3. Click System Settings.
4. Click Cloud Identity Providers.



5. Click New.
6. Configure the settings in the Server Configuration pane.
   A. Consider the following:
      i. If you use multiple IdPs, the Display Name field for the configuration must be unique.
      ii. Leave the Connection Type as LDAPS.
      iii. Leave the Server at ldap.google.com.
      iv. Leave the Port at 636.



B. In the Upload Keystore field, add the keystore file you created in the previous section: either drag the keystore file from the Finder into the field, or click "Browse for a file."
C. In the Keystore Password field, enter the password you created for the keystore file. The keystore details will be shown after you enter the corrent password.
D. In the Domain Name field, enter your domain name.



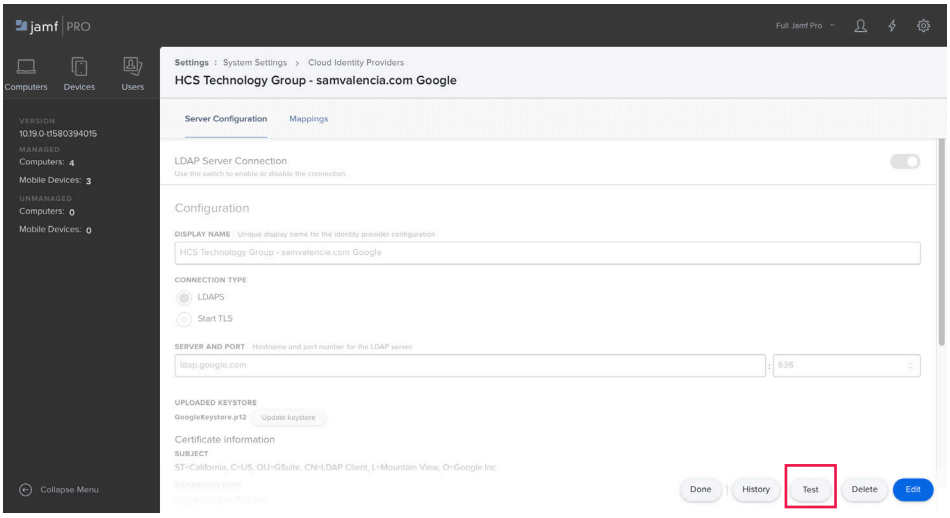
7. You can click the Mappings tab and modify settings.

   Note: When you configure Jamf Pro to integrate with an LDAP service, you need to configure the LDAP Search Base. However, when you configure Jamf Pro to integrate with a Cloud Identity Provider, the LDAP Search Base is automatically calculated. You can modify settings here to structure LDAP queries to reflect the hierarchical structure of your directory tree to ensure the search returns your desired results.

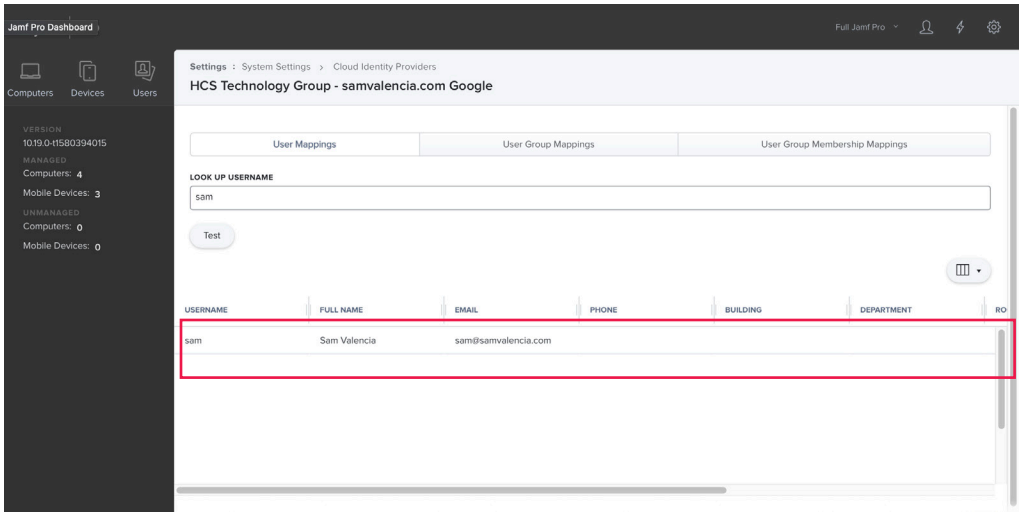
8.Click Save.

Test the Google Cloud Identity Provider Attribute Mappings

1. Click Test, or if you have Jamf Pro 10.20 or later, click Action (looks like a gear) and choose Test.



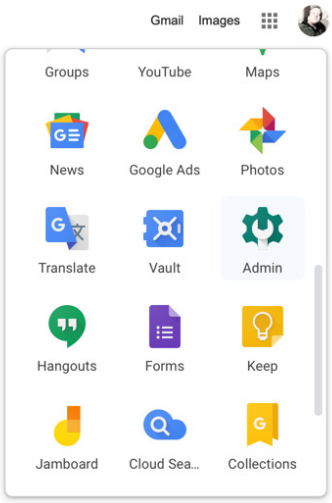
2. In the User Mappings tab, in the Look Up Username field, enter the account name of a user, then click Test.
3. Confirm that the username is displayed in the result.



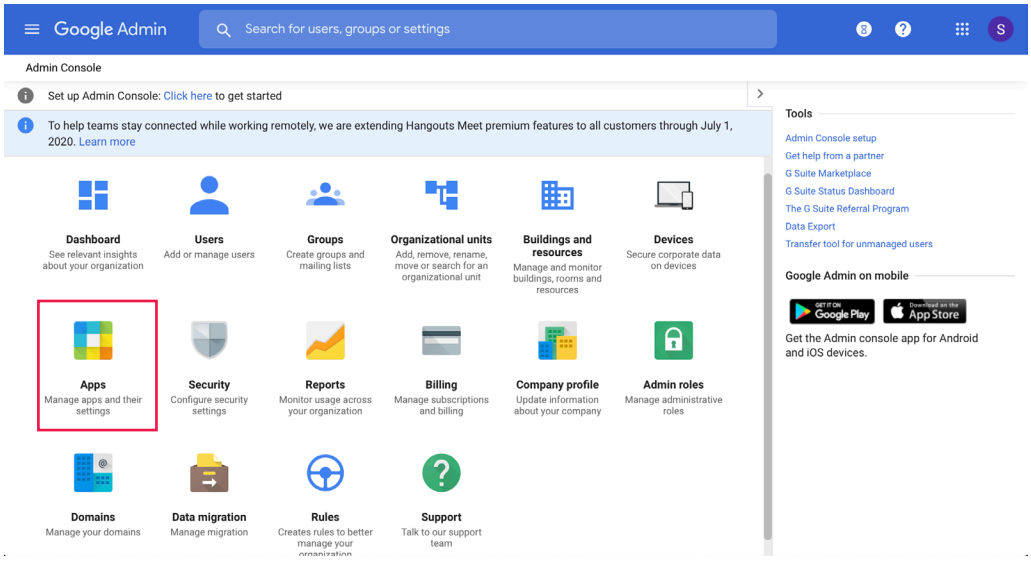
4. Click the User Group Mappings tab.
5. In the Look Up User Group field, enter a group name, then click Test.
6. Confirm that the result contains the user group name.
7. Click the User Group Membership Mappings tab.
8. In the Check If Username field, enter a user name.
9. In the Is A Member Of User Group field, enter a group that the user is a member of.
10. Click Test.
11. Confirm that the "Is Member" column is displayed as "true."
12. Click Done.

Configure Single Sign-On (SSO) in Jamf Pro with Google as your SAML 2.0 Identity Provider
Enabling Single Sign-On with Google authentication requires configuring both your Google domain and Jamf Pro.

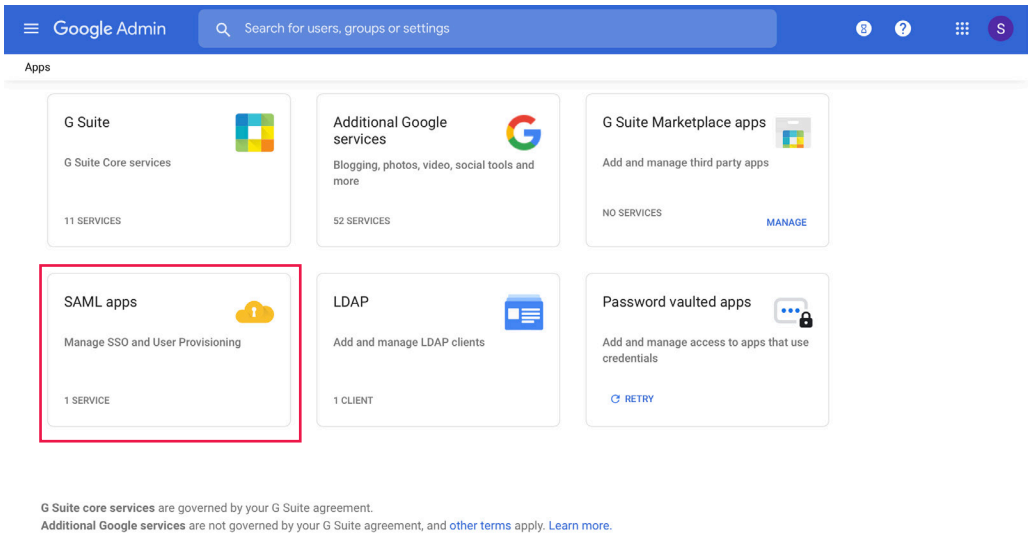
1. If you're not already logged in to you Google Admin console at admin.google.com, do so now. Be sure to sign in using your super administrator account, and not your personal Gmail account.



2. Navigate to the Admin console Home page and click Apps.

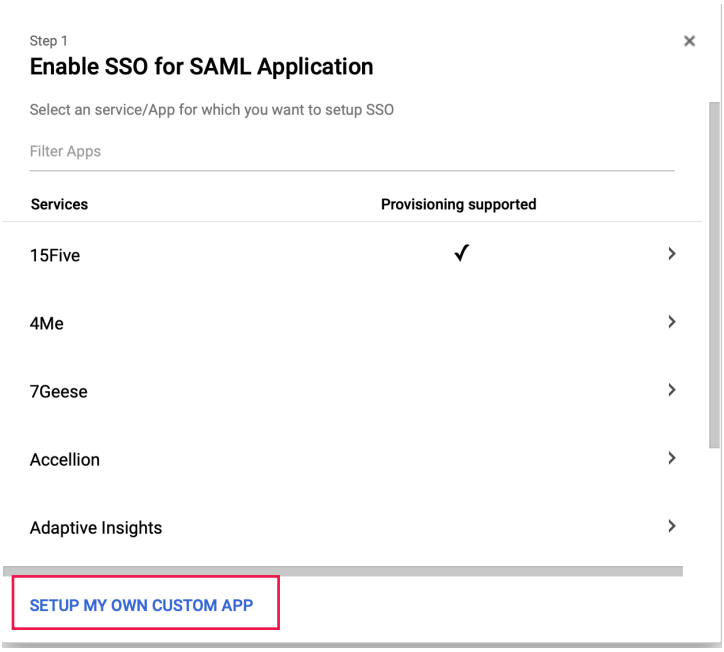


3. Click "SAML apps."

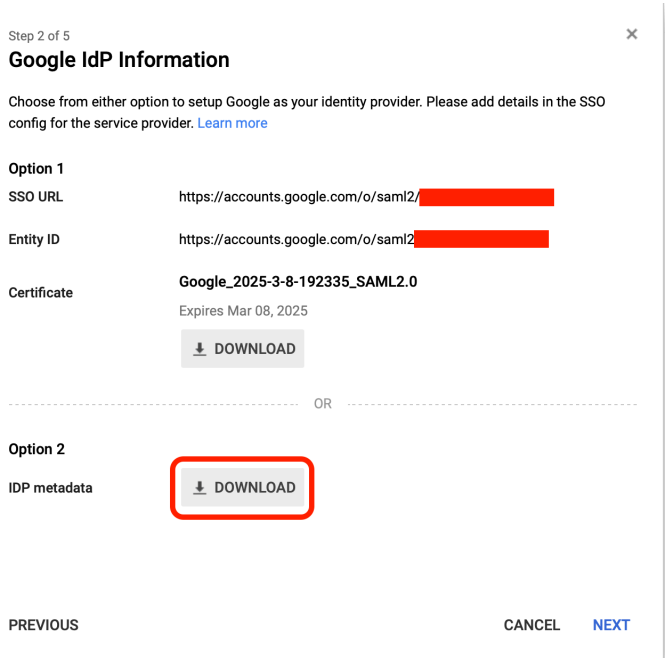


4. Click the yellow Add (+) button in the lower-right corner.

5. Click Set Up My Own Custom App.

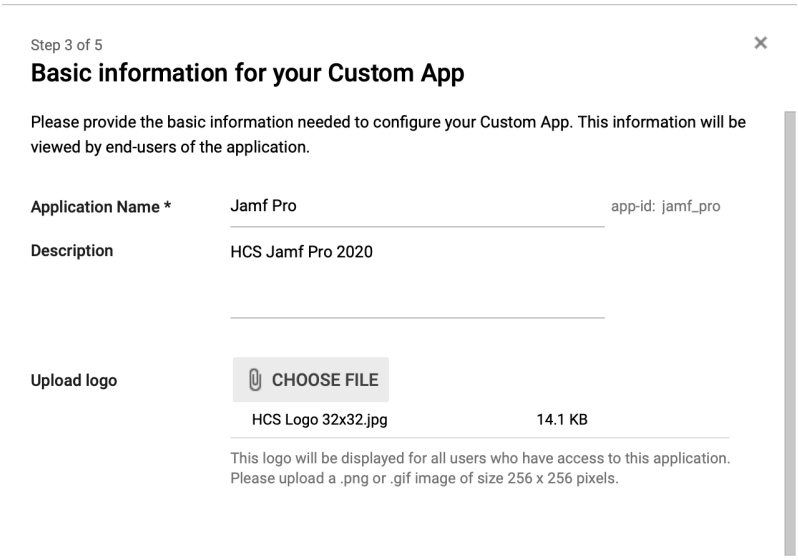


6. In the Google IdP Information pane, in the Option 2 section, click Download.

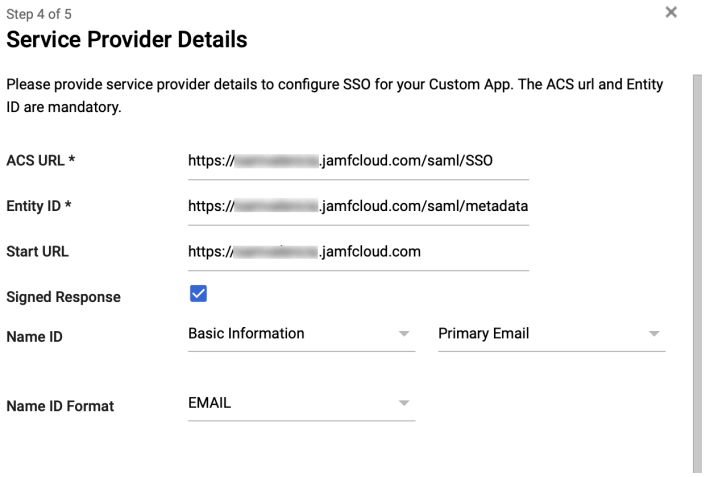


7. Click Next.

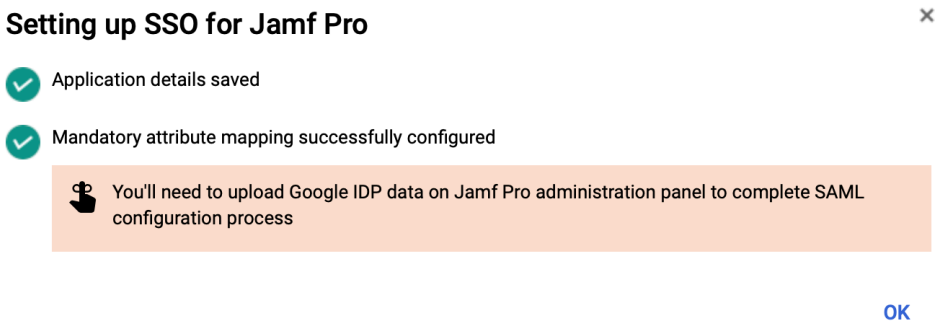
8. In the "Basic information for your Custom App" pane, in the Application Name field, enter **Jamf Pro**.
   a. (Optional) In the Description field, enter an application description.
   b. (Optional) In the "Upload logo" section, click Choose File, then navigate to a .png or .gif file that contains your organization's logo, with an image of size 256 x 256 pixels.



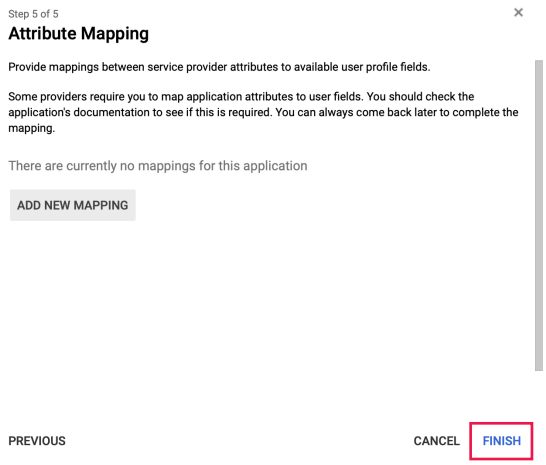
9. Click Next.
10. Configure the Service Provider Details window like the following (if your Jamf Pro server is on-premises, use the appropriate URL including the default port 8443).:
    - ACS URL: https://YOURDOMAINHERE.jamfcloud.com/saml/SSO
    - Entity ID: https://YOURDOMAINHERE.jamfcloud.com/saml/metadata
    - Start URL: https://YOURDOMAINHERE.jamfcloud.com
11. Select the checkbox for "Signed Response."
12. Leave the Name ID fields at their defaults: “Basic Information” and “Primary Email.”
13. Click the Name ID Format menu, then choose Email.



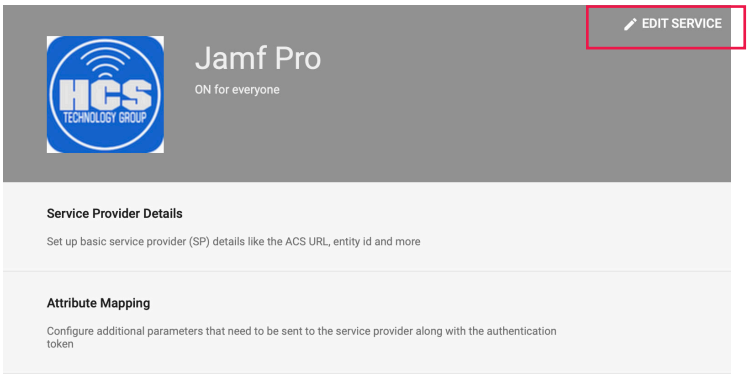
14. Click Next.
15. Confirm that "Setting up SSO for Jamf Pro" window displays "Application details saved" and "Mandatory attribute mapping successfully configured", then click OK.



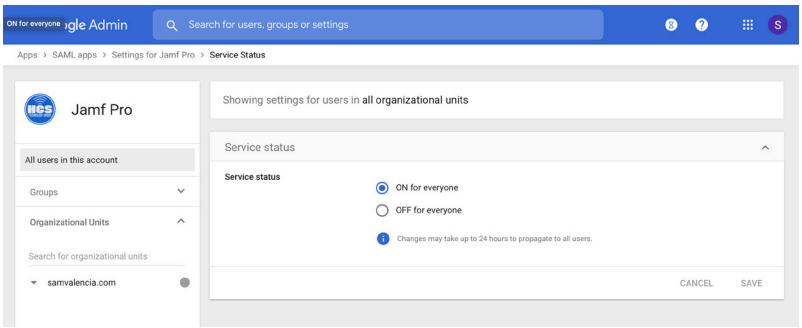
16. Click Finish.



17. At the top right of the SAML app, click More or Edit Service.



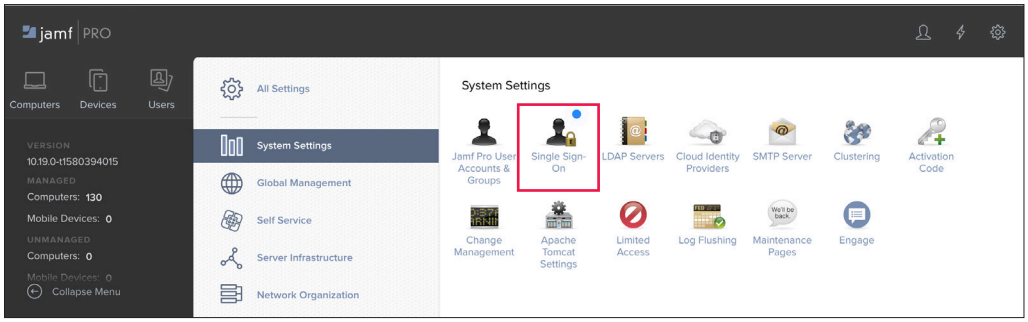
18. In the "Service status" field, we recommend that in the sidebar, you select your root organizational unit (OU), then select "On," then complete this guide to validate that you've successfully integrated Jamf Pro and Google IdP. Afterwards you return to this step to limit service to one or more child OUs with the following procedure: select your root OU, set the "Service status" to Off, click Save, select a child OU, select On for the "Service status", then click Override.



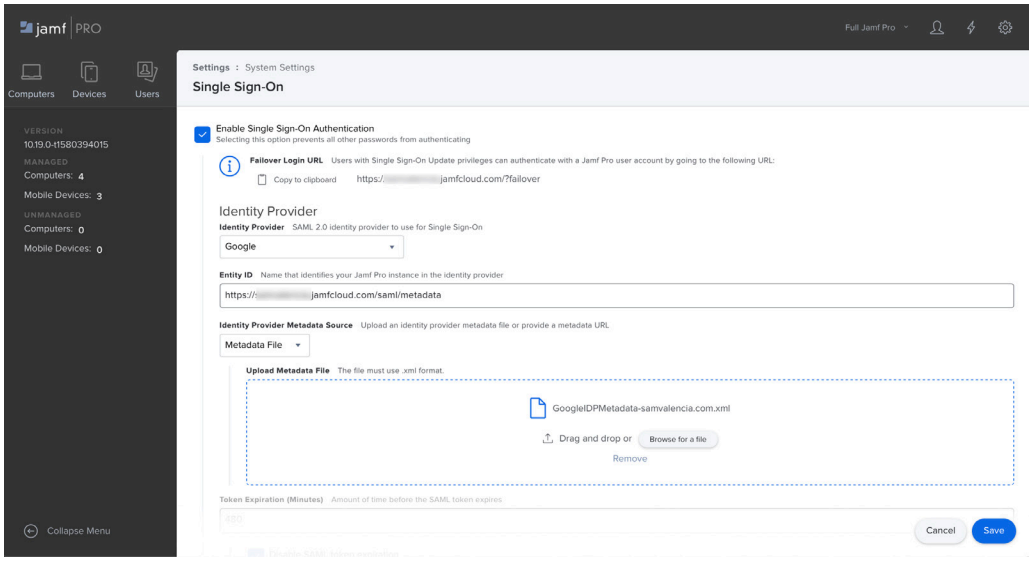
19. Click Save.

Configure and enable Single Sign-On (SSO) in Jamf Pro.

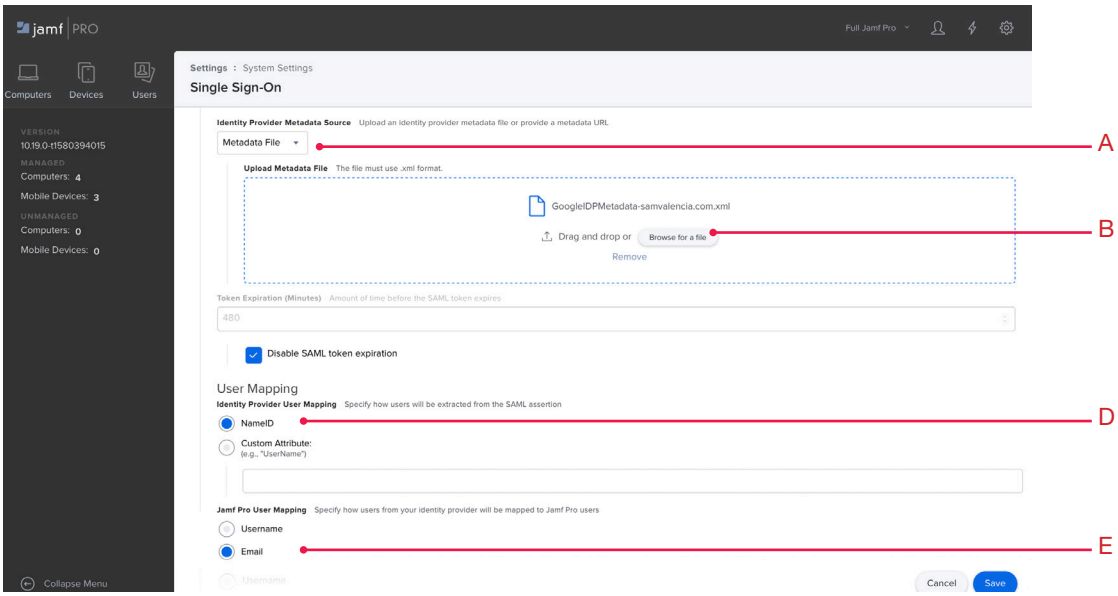
1. In Jamf Pro, navigate to Settings > System Settings > Single Sign-On.



2. Click Edit.
   A. Select the checkbox for "Enable Single Sign-On Authentication".
   B. Click the Identity Provider menu then choose Google.
   C. Ensure that the Entity ID field matches the following format:
   https://YOURDOMAINHERE.jamfcloud.com/saml/metadata



3. Configure the Identity Provider Metadata Source.
   A. Click the Identity Provider Metadata Source menu and choose Metadata File.
   B. In the Upload Metadata File field, click "Browse for a file."
   C. In your browser's file browser pane, select the Google metadata file you downloaded in Step 6 of the previous section, then click Choose.
   D. For Identity Provider User Mapping, select "NameID."
   E. In the User Mapping section, for Jamf Pro User Mapping, select "Email."
      Note: Only use "Username" if the username matches email, firstname or lastname.
   F. (Optional) Add the RDN Key for your LDAP group.

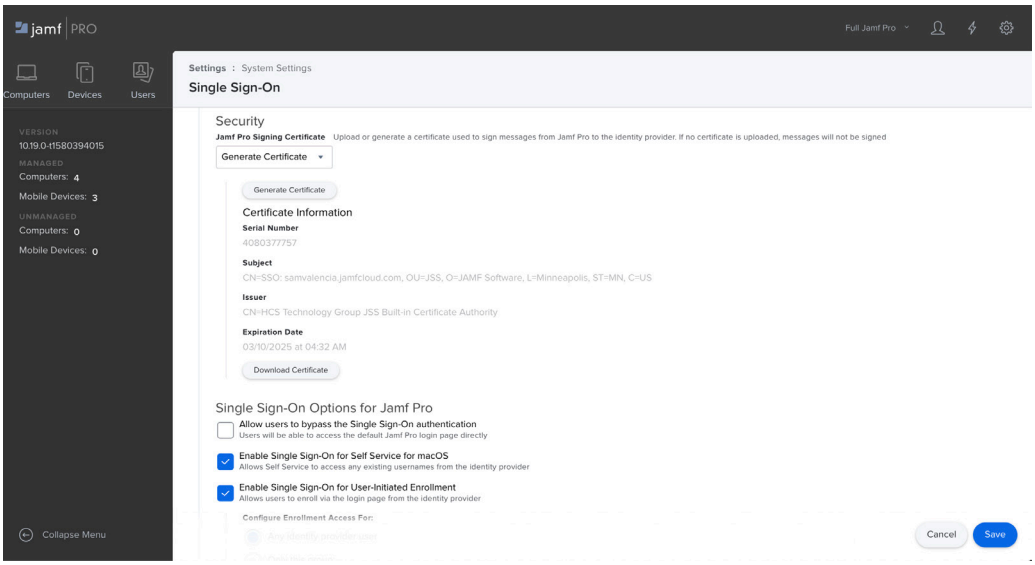


4. In the Security section, for Jamf Pro Signing Certificate, click the menu and choose Generate Certificate.

5. Optional: Select the checkbox for “Enable Single Sign-On for Self Service for macOS.”

6. Select the checkbox for “Enable Single Sign-On for User-Initiated Enrollment.” NOTE: leave the default “Configure Enrollment Access For:Any identity provider user” selected

7. Click Save.

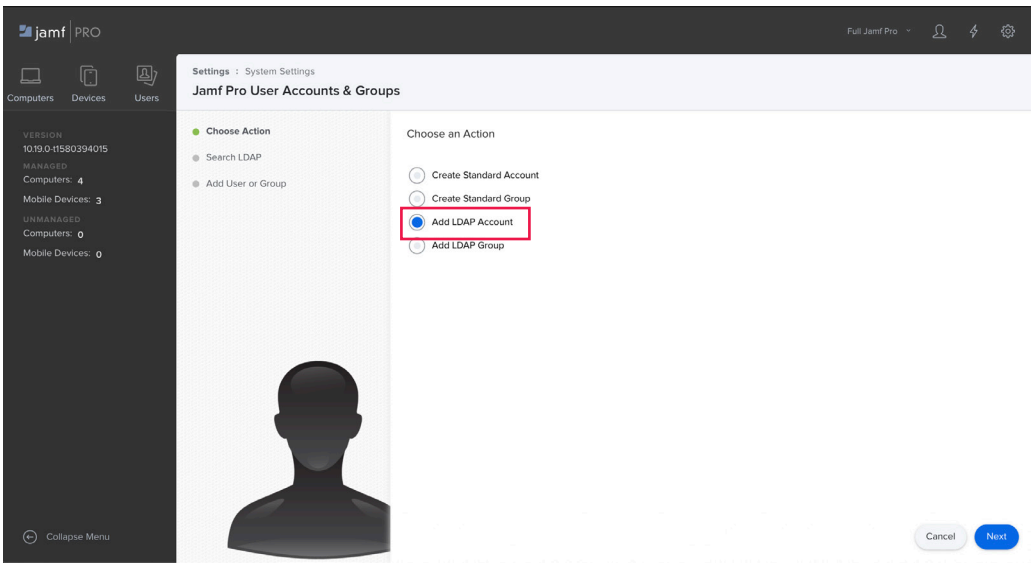


Enable a Google account to administer Jamf Pro

Use this procedure to use a specific Google account to administer Jamf Pro. After you validate the procedure and access the Jamf Pro with the Google account, you can modify and repeat the procedure for a Google group of accounts.

Before you perform these steps, confirm that the local Jamf Pro user account you are using to administer Jamf Pro has the full "Administrator" privilege set, or has "Update" privileges for "Single Sign-On", so you can continue using this local Jamf Pro user account to administer Jamf Pro if you have trouble logging in with a Google account that uses Single Sign-On.

1. In Jamf Pro, navigate to Settings > System Settings > Jamf Pro Users Accounts & Groups.
2. Click New.
3. Select Add LDAP Account.



4. In the Search Users field, enter the Google account and click Next. It may take several moments for the result to appear.
5. Once your user is listed, click Add.
6. Configure the desired privileges in Jamf Pro (for example, to use a Google account to administer Jamf Pro click the Privilege Set menu and choose Administrator) and Save.

Test the Single Sign-On configuration

1. In your browser window for admin.google.com, in the upper-right corner, click your user icon, then click "Sign Out" or "Sign out of all accounts", (depending on what options are available).
2. In your browser window for Jamf Pro, in the upper-right corner, click the user sihlouette then select Logout *accountname*.
3. Close the browser window that displays "You have successfully logged out."
3. In a web browser, navigate to your Jamf Pro URL, which now requires Single Sign-On (SSO):
    - https://YOURDOMAINHERE.jamfcloud.com/
4. You should be redirected to the Google sign in page.
5. If necessary, enter your Google account email address then click Next, or select a displayed account.
6. Enter your Google account password, then click Sign in.
7. If your Google account requires 2-Step Verification, enter the 6-digit code, then click Done.
8. Confirm that you are logged in to Jamf Pro.

If your browser displays a "Single Sign-On Error" message (or other message), try again from step 3 with a private or incognito window. For example, if you're using Safari, choose File > New Private Window; If you're using Google Chrome, choose File > New Incognito Window.

If your browser displays an "Access Denied" message, close the browser window, then navigate to the failover URL, which has the form of https://YOURDOMAINHERE.jamfcloud.com/?failover to log in with your local Jamf Pro administrator user account and double-check your settings.

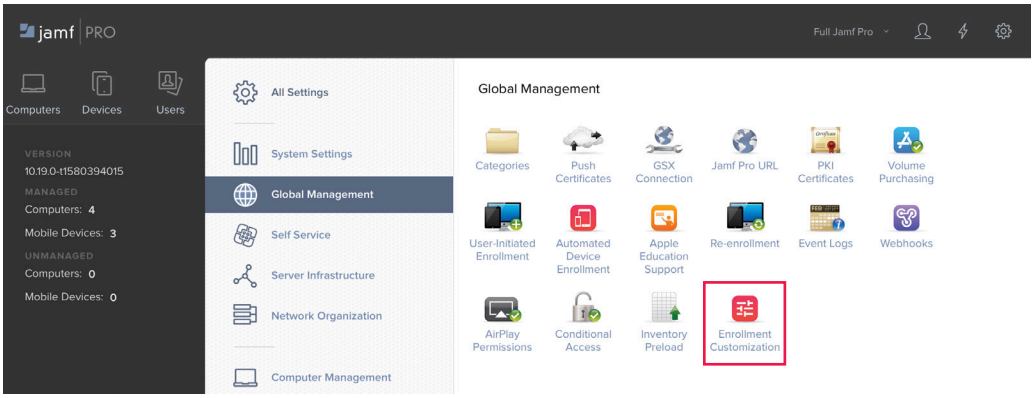
If your browser displays an"app_not_configured_for_user" message, confirm that you are using a Google account from a domain that you integrated with Jamf Pro.

Configure a Computer PreStage Enrollment to use Single Sign-On

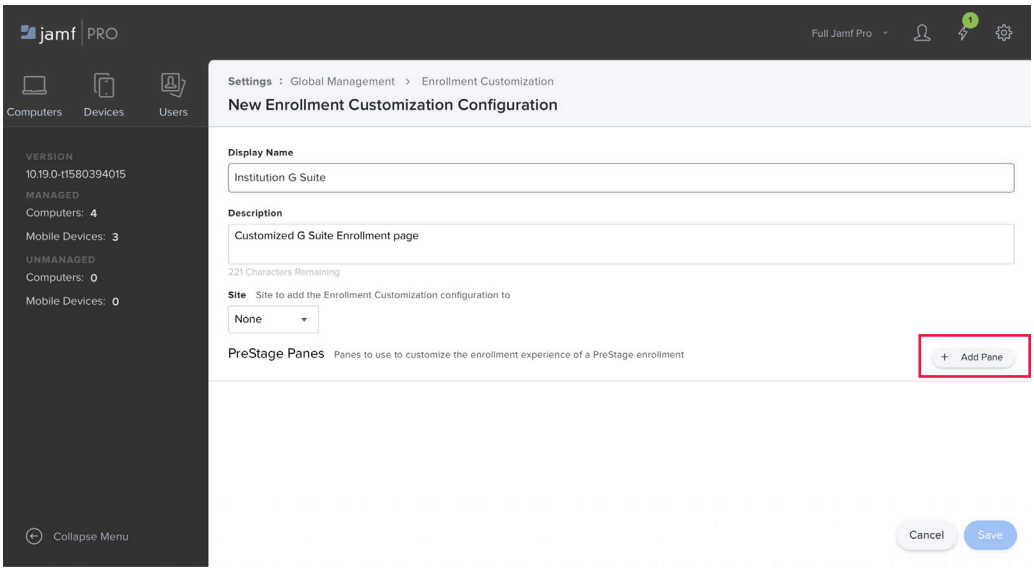
In the next few sections you'll configure an Enrollment Customization and assign it to a PreStage. You'll start up an out-of-the-box Mac, provide Google account credentials, and your Mac will be enrolled and assigned to the LDAP user that gets created in Jamf Pro (if it didn't already exist).

First, setup an Enrollment Customization.

1. In Jamf Pro, navigate to Settings > Global Management > Enrollment Customization.

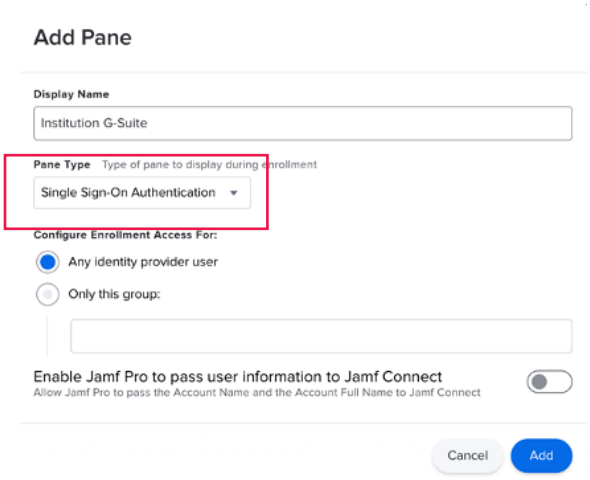


2. In the upper-right corner of your browser window, click New.
3. In the Display Name field, enter descriptive text. This guide uses **Institution G Suite** as an example. The text that you enter in this field appears as a choice later on, when you edit Computers > PreStage Enrollments > General, in the Enrollment Customization Configuration menu.
4. In the Description field, enter a description. Jamf Pro displays this field in this pane only, as an aid for administrators.
5. In the PreStage Panes section, click the Add Pane button.



6. In the Display Name field, enter a name. This appears only to an administrator in the list of Pre-Stage Panes.

7. For Pane Type, select Single Sign-On Authentication.

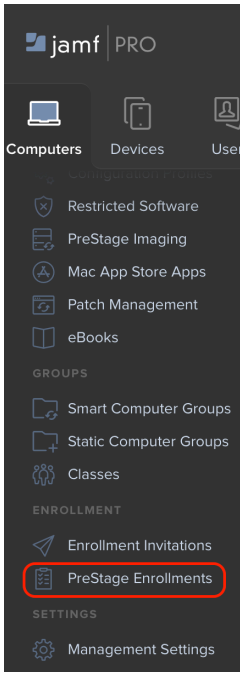


8. Click Add.
9. Click Save.

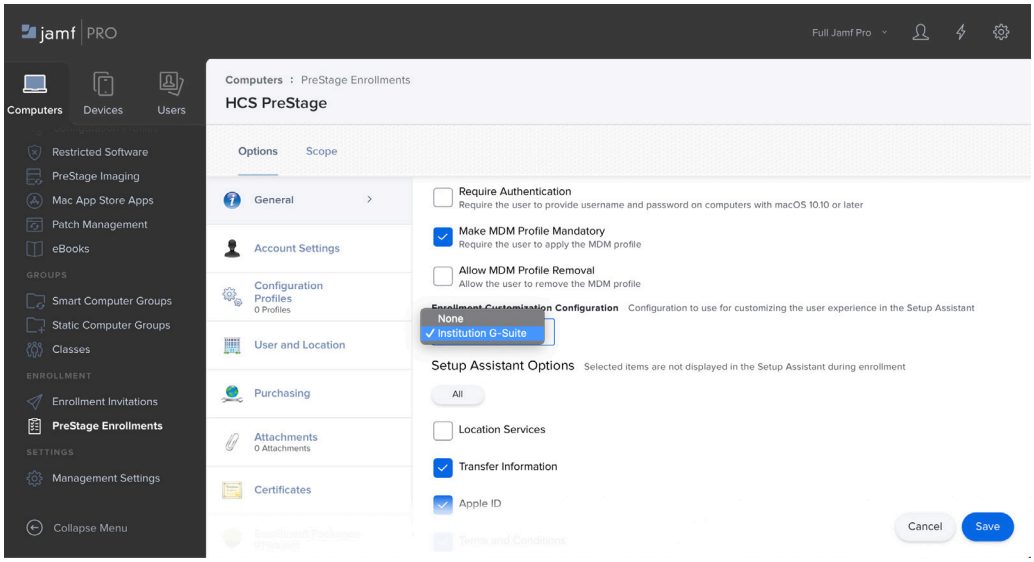
Add the Enrollment Customization configuration to a Computer PreStage Enrollment

To force a user to authenticate using a G Suite account during enrollment that uses a PreStage Enrollment, use the following procedure to add the Enrollment Customization configuration to a Computer PreStage Enrollment.

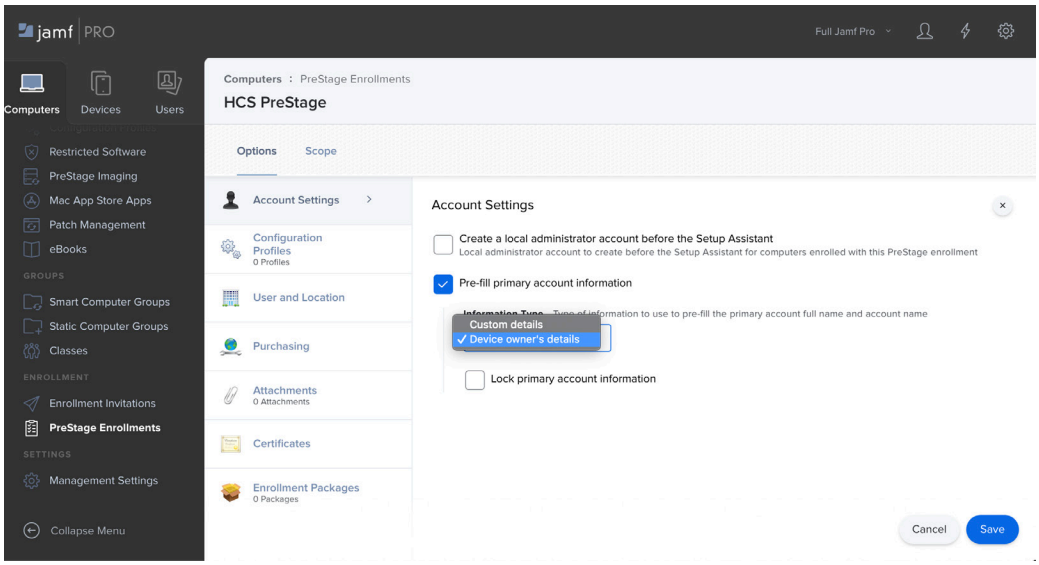
1. In Jamf Pro, navigate to Computers > PreStage Enrollments



2. Optionally, click New to create a PreStage Enrollment to test with. Otherwise, select an existing PreStage Enrollment, then click Edit.
3. In the General pane, be sure that the "Make MDM Profile Manadatory" option is selected.
4. Click the Enrollment Customization Configuration menu then choose the configuration youcreated in the previous section.



5. In the sidebar, click Account Settings.
6. Click Configure and select the checkbox, "Pre-fill primary account information."
7. Click the Information Type menu then choose "Device owner's details."
8. Optionally, if you want to force the user to create a local account on their Mac with the "Full name" and "Account name" fields pre-populated (and not editable) with information from their Google account, select the checkbox for "Lock primary account information."



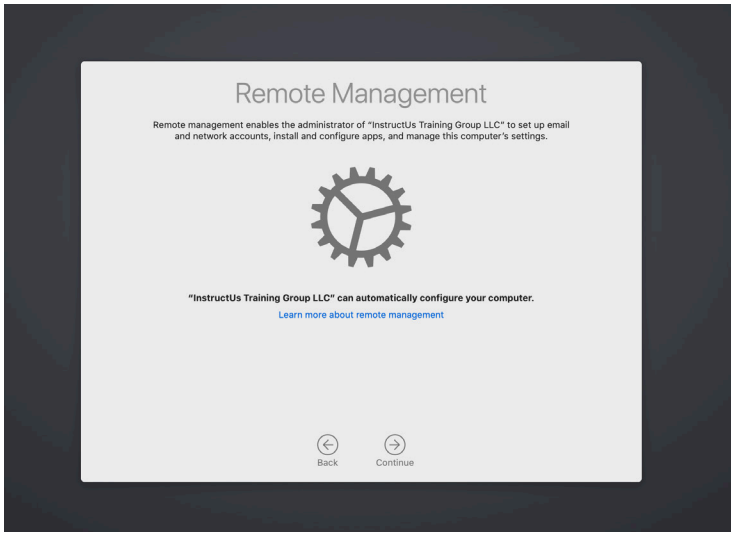
9. Click the Scope tab.
10. Select the checkbox for the Mac you will test.
11. Click Save.

Confirm that the Mac displays the Google account screen during enrollment

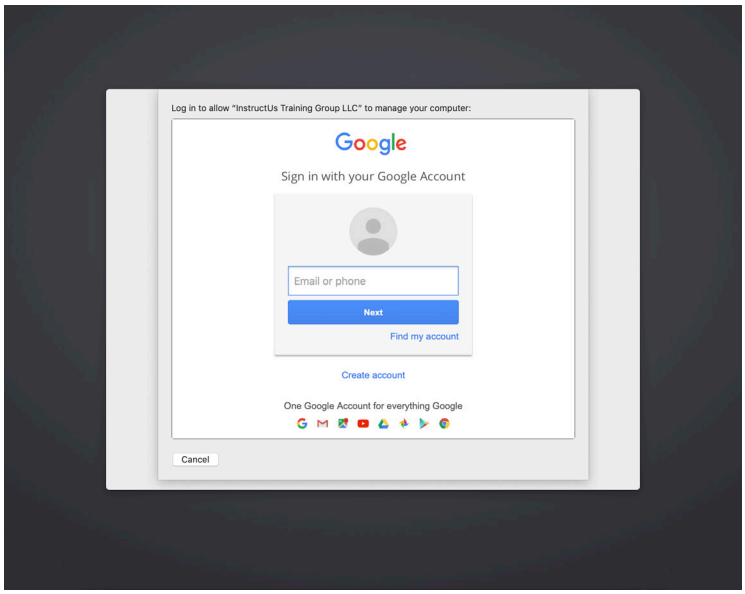
1. Power on the Mac with an unconfigured installation of macOS 10.15 or later, which you have scoped to your PreStage Enrollment that you created in the previous section.

2. When prompted, ensure you are connecting to a network with an internet connection.

3. Confirm that your Mac displays the screen for Remote Management, then click Continue. If your Mac does not display the Remote Management screen, it may have downloaded information from Jamf Pro before you modified your PreStage Enrollment, in which case you'll need to erase your Mac and reinstall macOS (or use an unsupported workaround to reload the PreStage Enrollment, which is outside the scope of this guide). ; see https://grahamrpugh.com/2020/02/21/resetting-dep-without-reinstalling.html for more information)



4. Enter your Google account credentials when prompted to "Sign in with your Google Account."



Once you have completed that Single Sign-On (SSO) Authentication, Jamf Pro has assigned that device to the matched LDAP user.

5. The “Create a Computer Account” screen will be displayed with the "Full name" and "Account name" fields populated with values from the assigned LDAP user's information (which is the Google account that the person used to authenticate at the Enrollment Customization Screen.)

NOTE: The local computer account password and your Google account password are NOT synced. Changes to credentials made on the local computer will not reflect back to G-Suite and vice versa.

NOTE: If your PreStage Enrollment displays the Apple ID screen during Setup Assistant and you enter an Apple ID at the "Sign In with Your Apple ID" screen, the "Create a Computer Account" screen will contain fields that are populated with information from the Apple ID and NOT the G Suite username.

This completes the Google Single Sign-On Guide. 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.