

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



Contents

Configure Google and add LDAP clients to the service.	3
Convert the Google private key to a PKCS12 format file that you can upload to your Jamf Pro server	6
Connect your LDAP client to the Secure LDAP service	7
Test the Google Cloud Identity Provider Attribute Mappings	9
Configure Single Sign-On (SSO) in Jamf Pro with Google as your SAML 2.0 Identity Provider	10
Configure and enable Single Sign-On (SSO) in Jamf Pro	15
Enable a Google account to administer your Jamf Pro service	17
Test the Single Sign-On configuration	18
Confirm Setup Google for SSO and LDAP	19
Add the Enrollment Customization configuration to a Computer PreStage Enrollment	21
Confirm that the Mac displays the Google account screen during enrollment	23



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.



G Suite core services are governed by your G Suite agreement. Additional Google services are not governed by your G Suite agreement, and other terms apply. Learn more



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

ADD 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**.

× Add LDAP client							
1 Client details	2 Access permissions						
	Client details						
LDAP client name * HCS Jamf Pro							
	Description Jamf Pro MDM						
	* Required field						
			CANCE	EL CONTINUE			

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.

	Add LDAP cli	ent		
0	Client details	2	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 (samvalencia.com) Selected organizational units No access 	
		Read user information Specify client's access level for reading user information. Some clients need additional information before authentical Image: Specify client's access Image: Specify client's access		
			Read group information Client can read group information. Some clients need additional information before authenticating users. Image: Client can read group information. Some clients need additional information before authenticating users. Image: Client can read group information. Some clients need additional information before authenticating users. Image: Client can read group information. Some clients need additional information before authenticating users. Image: Client can read group information. Some clients need additional information before authenticating users. Image: Client can read group information. Some clients need additional information before authenticating users. Image: Client can read group information. Some clients need additional information before authenticating users. Image: Client can read group information. Some clients need additional information before authenticating users. Image: Client can read group information. Some clients need additional information. Some clients need addition. Some clients need additional information. Some clients need additional information. Some clients need addition. Some clients need additinted addition. Some clients need additinterne	



- 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.

HCS Jamf Pro added Next, connect your client to the LDAP service Source of the service of the serv
HCS Jamf Pro added Next, connect your client to the LDAP service Download the generated certificate (t 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.2023.03.23,79926 Download certificate
Next, connect your client to the LDAP service 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.2023.03.23.79926 Expres March 23.2023 Download certificate Journal Configuration might require LDAP access certedential. Learn more
 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_2023_03_23_79926 Explore March 23_2023 Download certificate 2. Upload the certificate to your LDAP client and configure the application. Configuration might require LDAP access credentials. Learn more
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.2023.03.23.79926 Expires March 23, 2023 Download certificate 2. Upload the certificate to your LDAP client and configure the application. Configuration might require LDAP access credentials. Learn more
Want to do this later? You can generate and download a certificate at any time from the client's details page. Google_2023_03_23_79926 Express March 23, 2023 Download certificate 2. Upload the certificate to your LDAP client and configure the application. Configuration might require LDAP access credentials. Learn more
Google_2023_03_23_70926 Expires March 23, 2023 Download certificate 2. Upload the certificate to your LDAP client and configure the application. Configuration might require LDAP access credentials. Learn more
Expires March 23, 2023 Download certificate Upload the certificate to your LDAP client and configure the application. Configuration might require LDAP access credentials. Learn more
2. Upload the certificate to your LDAP client and configure the application. Configuration might require LDAP access credentials. Learn more
 Upload the certificate to your LDAP client and configure the application. Configuration might require LDAP access credentials. Learn more
CONTINUE TO CLIENT DETAILS

- 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.

≡ Google Admin				8		# S
Apps > LDAP > Settings for HCS J	amf Pro					
						_
HCS Jamf Pro Jamf Pro MDM	Service status				OFF	v
Status OFF	Access permissions	Read user information	Read group information			~
P EDIT DETAILS	Entire domain	Entire domain	Has access			
MORE	Authentication					~
	Certificates					
	1 certificate is associated with this	s LDAP client				
	Access credentials					
	0 access credentials are associate	ed with this LDAP client				

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

≡ Google Admin	Q Search for users, groups or settings		• •	₩ S			
Apps > LDAP > Settings for HCS	Apps > LDAP > Settings for HCS Jamf Pro > Service Status						
HCS Jamf Pro	Showing settings for users in all organizational units						
	Service status			^			
	Service status OFF for everyone OFF for everyone Changes may take up to 24 hours to propagate to all users.						
		1 unsaved change	CANCEL	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.

	🖿 Google_20	023_03_23_79926	
$\langle \rangle$		▲	Q Search
Favorites	Name	^ Date Modified	Size Kind
Cloud	🕅 Google_2023_03_23_79926.crt	Today at 6:15 PM	1 KB certificate
	😤 Google_2023_03_23_79926.key	Today at 6:15 PM	2 KB Keynote
Desktop			
Docume			
Locations			
🚮 Valencia			
🚳 Network			
Tags			

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.pl2 \
-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.

🗖 jamf PRO		
Computers Devices Users	All Settings	System Settings
VERSION 10.19.0-11580394015 MANAGED	Giobal Management	Jamt Pro User Single Sign- Could Identity Groups SMTP Server Clustering
Computers: 4 Mobile Devices: 3 UNMANAGED Computers: 0	Self Service	Activation Code Change Apache Code Management Settinos
Mobile Devices: 0	Network Organization	

- 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 Idap.google.com.
 - iv. Leave the Port at 636.

🏜 jamf 🛛 PRO	Full Janf Poo 🕤 <u>೧</u> 🗳 🤯
Computers Devices	Settings : System Settings > Cloud Identity Providers New Cloud Identity Provider Configuration
VERSION 10.19.0-t1580394015	Server Configuration Mappings
MANAGED Computers: 4 Mobile Devices: 3	Configuration
	DISPLAY NAME Unique display name for the identity provider configuration
	HCS Technology Group - Google
Mobile Devices: 0	CONNECTION TYPE
	DLAPS
	Start TLS
	SERVER AND PORT Hostname and port number for the LDAP server
	kdap.google.com
	UFLOAD KEYSTORE The file must use p12 format.
	Field is required.
	1. Drag and drop or Browse for a file
	For information about generating the .pt2 file, see the Generating the PKCS12 Keystore File When Integrating Google Cloud kIP with Jamf Pro KB article.
	KEYSTORE PASSWORD
	Cancel Save



- 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.

┛ jamf PRO	Full Jamf Pro 🗸 <u>()</u> 🞸 🀯	
Computers Devices Users	Settings : System Settings → Cloud Identity Providers New Cloud Identity Provider Configuration	
VERSION 10.19.0-11580394015	Server Configuration Mappings	
Computers: 4 Mobile Devices: 3	keystore.pl2	—— В
Computers: 0 Mobile Devices: 0	Drag and drop or Browse for a file Remove	
	For information about generating the .pt2 file, see the Generating the PKCS12 Keystore File When Integrating Google Cloud IdP with Jamf Pro KB article. KEYSTORE PASSWORD	C
	Certificate information	0
	ST-California, C-US, OU-GSuite, CN-LDAP Client, L-Mountain View, O-Google Inc. EXPIRATION DATE 03/24/2023 at 02:12 AM	
	DOMAIN NAME Domain used to erroll in G Suite or Cloud Identity (e.g. "domain.com") Accontine.com	D
	Advanced Settings.	

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.

🏜 jamf 🛛 PRO			. 4 🏟
	Settings : System Settings · > Cloud Identity Providers HCS Technology Group - samvalencia.com Google		
VERSION 10.19.0-11580394015	Server Configuration Mappings		
	LDAP Server Connection Use the and/or detailed the connection.		
UNMANAGED Computers: 0	Configuration		
	DISPLAY NAME Unique display name for the identity provider configuration		
	HCS Technology Group - samvalencia.com Google		
	CONNECTION TYPE		
	LDAPS		
	Start TLS		
	SERVER AND PORT Hostname and port number for the LDAP server		
	idap.google.com	: 636	
	UPLOADED KEYSTORE		
	GoogleKeystore.p12 Update keystore		
	Certificate information		
	SUBJECT		
	ST=California, C=US, OU=GSuite, CN=LDAP Client, L=Mountain View, O=Google Inc.		
	Done	History Test Dele	ete Edit

- 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.

Jamf Pro Dashboard	Settings : System HCS Technolo	Settings >: Cloud Identity Provid gy Group - samvalencia.c	ers com Google		Fu	ill Jamf Pro 👻 🧕	4 ©
VERSION 1019.0-11580394015 MANAGED Computers: 4 Mobile Devices: 3 UMMANAGED Computers: 0 Mobile Devices: 0	LOOK UP USERNAME Sam Test	Jser Mappings	User Group Map	pings	User Group Member	rship Mappings	
	USERNAME	FULL NAME	EMAIL	PHONE	BUILDING	DEPARTMENT	RO
	sam	Sam Valencia	sam@samvalencia.com				
					_		

- 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."

≡ Google Admin	Q Search for u			8	?	S
Apps						
G Suite G Suite Core services		Additional Google services G Blogging, photos, video, social tools and more	G Suite Marketplace apps			
11 SERVICES		52 SERVICES	NO SERVICES MANAGE			
SAML apps			Password vaulted apps			
Manage SSO and User Pro	ovisioning	Add and manage LDAP clients	Add and manage access to apps that use credentials			
1 SERVICE		1 CLIENT	C RETRY			
L						

G Suite core services are governed by your G Suite agreement. Additional Google services are not governed by your G Suite agreement, and other terms apply. Learn more.

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.

Step 2 of 5 × Google IdP Information				
Choose from either option to setup Google as your identity provider. Please add details in the SSO config for the service provider. Learn more				
Option 1				
SSO URL	https://accounts.google.com/o/saml2/			
Entity ID	https://accounts.google.com/o/saml2			
Certificate	Google_2025-3-8-192335_SAML2.0			
Gertineate	Expires Mar 08, 2025			
	± DOWNLOAD			
	OR			
Option 2				
IDP metadata	± DOWNLOAD			
PREVIOUS	CANCEL NEXT			

- 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.

Please provide the basi viewed by end-users of	c information needed to configure yo the application.	our Custom App. This information will be
Application Name *	Jamf Pro	app-id: jamf_pro
Description	HCS Jamf Pro 2020	
Upload logo	CHOOSE FILE	



9. Click Next.

- 10. Configure the Service Provider Details window like the following (if your Jamf Pro server is onpremises, 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.

Step 4 of 5 Service Provide	Details	
Please provide service p ID are mandatory.	ovider details to configure SSO for your Custom App. The ACS url and Entity	
ACS URL *	https:// .jamfcloud.com/saml/SSO	
Entity ID *	https:// .jamfcloud.com/saml/metadata	
Start URL	https:// .jamfcloud.com	
Signed Response		
Name ID	Basic Information - Primary Email -	
Name ID Format	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.

Set	Setting up SSO for Jamf Pro		
\checkmark	Application details saved		
\checkmark	Mandatory attribute mapping successfully configured		
	You'll need to upload Google IDP data on Jamf Pro administration panel to complete SAML configuration process		



16. Click Finish.

Step 5 of 5 Attribute Mapping	×
Provide mappings between service provider attributes to available user profile fields.	- E
Some providers require you to map application attributes to user fields. You should check the application's documentation to see if this is required. You can always come back later to compl mapping.	ete the
There are currently no mappings for this application	
ADD NEW MAPPING	
PREVIOUS CANCEL	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.

for everyone)gle Admin				8 ?	
Apps > SAML apps > Settings fo	r Jamf Pro	Service Status			
Jamf Pro		Showing settings	for users in all organizational units		
All users in this account		Service status			^
Groups	~	Service status	ON for everyone		
Organizational Units	^		OFF for everyone		
Search for organizational units			Changes may take up to 24 hours to propagate to all users.		
 samvalencia.com 				CANCEL	SAVE

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.

🗖 jamf PRO			
Computers Devices Users	දිරිදි All Settings	System Settings	¢
VERSION	System Settings	Jamf Pro User Single Sign- LDAP Servers Cloud Identity SMTP Server Clustering	Activation
MANAGED Computers: 130	Global Management	Accounts & On Providers Groups	Code
Mobile Devices: 0	Self Service		
Computers: 0	Server Infrastructure	Change Apache Limited Log Hushing Maintenance Engage Management Tomcat Access Pages Settings	
Collapse Menu	Network Organization		

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

🖆 jamf 🛛 PRO		Full Jamf Pro 🛛 👻	ম	\$	٩
Computers Devices Users	Settings : System Settings Single Sign-On				
VEBSION 1019.0-1580394015 KAAAGGD Computers: 4 Mobile Devices: 3 UNIMAAGED Computers: 0 Mobile Devices: 0	Exbets Single Sign-On Authentication Subtraction prevents all other passwords from authenticating Allower Login URL: Users with Single Sign-On Update privileges can authenticate with a Jam/ Pro user account by going to the following URL: Copy to clocked https:// Introduct Com/Single Sign-On Update privileges can authenticate with a Jam/ Pro user account by going to the following URL: Copy to clocked https:// Introduct Com/Single Sign-On Update privileges can authenticate with a Jam/ Pro user account by going to the following URL: Copy to clocked https:// Introduct Com/Single Sign-On Update privileges can authenticate with a Jam/ Pro user account by going to the following URL: Coogle				
	Token Expiration (Minutes) Amount of time before the SAML token expires				
	488		Cancel) (s	ave



- 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.

┛ jamf PRO	Fuil Jant Pro × <u>Ω</u> & ®	
mputers Devices	Settings : System Settings Users Single Sign-On	
VERSION 10.19.0-t1580394015	Identity Provider Metadata Source Upload an identity provider metadata file or provide a metadata URL. Metadata File *	A
MANAGED Computers: 4	Upload Metadata File The file multicas and format.	
Mobile Devices: 3	GoogleIDPMetadata-samvalencia.com.xml	_
Computers: 0	1. Drag and drop or Browse for a file	— E
Mobile Devices. 0	Remove	
	Token Expiration (Minutes) - Amount of time before the SAML token expires	
	480	
	Disable SAML token expiration User Mapping Identify Provider User Mapping Sectify The start User Mapping NameD	_ [
	Custom Attribute: (e.g., 'UserName')	
	Janf fro User Mapping Specify how users from your identity provider will be mapped to Janf Pro users	
	Username	_
	Email	— E
	Usernanie Coppel Saw	

- 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.

🛂 jamf PRO	Full Jamf Pro - <u>D</u> 🗳 🎯
Computers Devices Users	Settings : System Settings Single Sign-On
VERSION	Security Jamf Pro Signing Certificate Upload or generate a certificate used to sign messages from Jamf Pro to the identity provider. If no certificate is uploaded, messages will not be signed
MANAGED	Generate Certificate *
Mobile Devices: 3	Generate Certificate
UNMANAGED Computers: 0 Mobile Devices: 0	Certificate Information Serial Number 4080377757 Subject CN-NSCS issmellencia Jamfcloud.com, OU=JSS, O=JAMF Software, L=Minneapolis, ST=MN, C=US Issuer CN-NSCS Technology Group JSS Built-In Certificate Authonity Expirates Date 0310/2025 at 0432 AM
	Diversibility Single Sign-On Options for Jamf Pro Diversibility Allow users to bypass the Single Sign-On authentication Duces will be able to access the default Jamf Pro login space directly. Zinable Single Sign-On for Self Service for macOS Allows Self Service to access any existing usersames from the identity provider Zinable Single Sign-On tor Self Service for Content. Allows users to event via the login page from the identity provider.
Collapse Menu	Configure Evolution Access For:



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.

🛂 jamf 🛛 PRO		Full Jamf Pro × 🗘 🗳 🧔
Computers Devices Users	र्रेट्रेरे All Settings	Global Management
VERSION 10.19.0-11580394015	System Settings	Categories Push GSX Jamf Pro URL PKI Volume Categories Contraction Casedition
MANAGED Computers: 4	Global Management	
Mobile Devices: 3	Self Service	User-Initiated Automated Apple Re-enrollment Event Logs Webhooks Errollment Device Education
Computers: 0	Server Infrastructure	Enrollment Support
Mobile Devices: 0	Network Organization	AirPlay Conditional Inventory Preload
	Computer Management	

- 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.

┛ jamf 🛛 PRO		Full Jamf Pro 🗸	<u>ይ</u>	به
Computers Devices Users	Settings : Global Management > Enrollment Customization New Enrollment Customization Configuration			
VERSION 1019.0-11580394015 MANAGED Computers: 4	Display Name Institution G Suite Description Contemport			
Mobile Devices: 3 UNMANAGED Computers: 0 Mobile Devices: 0	221 Characters Remaining Site Site to add the Enrollment Customization configuration to None PreStage Panes Panes to use to customize the enrollment experience of a PreStage enrollment		+ .	Add Pane
Collapse Menu			Cancel	Save

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.

Add Pane

	1 G-Sulte					
Pane Type Single Si	Type of pane to dis gn-On Authenticati	play during	enrollment			
Configure I	nrollment Access F	or:				
Any	identity provider u	ser				
Only	this group:					
Enable J	amf Pro to pass Pro to pass the Acco	user ini unt Name a	ormation t	o Jamf Co It Full Name to	nnect Jamf Connect	

- 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.

🗖 jamf 🛛 PRO		Full Jamf Pro 🗸 🖇 🐯
Computers Devices Users	Computers : PreStage Enrollmer HCS PreStage	ts
Restricted Software PreStage Imaging	Options Scope	
Mac App Store Apps	👔 General >	Require Authentication Require the user to provide username and password on computers with macOS 10.10 or later
eBooks	Account Settings	Make MDM Profile Mandatory Require the user to apply the MDM profile
GROUPS	Configuration Profiles 0 Profiles	Allow the user to remove the MDM profile South and Contiguration Configuration to use for customizing the user experience in the Setup Assistant None
L_∔ Static Computer Groups ௹௺ Classes	User and Location	Vinsthuldor G-Suite Satur Assistant Ontions Salested lange are not direbund in the Solue Arcistant durine excellencet
ENROLLMENT	eurchasing	
PreStage Enrollments	Attachments O Attachments	Location Services
🔅 Management Settings	Certificates	Transfer Information Apple ID
Collapse Menu	Enclinent Packages	Cancel Save



- 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."

🞜 jamf PRO		Full Jamf Pro 🗸 👌	ŝ	
Computers Devices Users	omputers : PreStage Enrollments			
Configuration of online Restricted Software PreStage Imaging	Options Scope			
Mac App Store Apps	Account Settings >	Account Settings	×	
Patch Management eBooks	Configuration Profiles 0 Profiles	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		
GROUPS	User and Location	Pre-fill primary account information Information Tune Tune Tune and account name		
Classes	Purchasing	Custom details V Device owner's details		
ENROLLMENT	Attachments 0 Attachments	Lock primary account information		
PreStage Enrollments	Certificates			
🔅 Management Settings	Enrollment Packages 0 Packages			
🔶 Collapse Menu		Cancel	ave	

- 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)

Remote Management	
Render 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.	1
"InstructUs Training Group LLC" can automatically configure your computer. Learn more about remote management	
	2
Ereck Operations	1
beux. Commue	

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.)

Create a Computer Account	
Full name: Sam Valencia Account name: sam This will be the name of your home folder. Password:	
Eack Continue	

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.