Setting up Single Sign on with Google Workspace

Last Modified on 06.08.2025

Single Sign-On is a convenient, yet secure way of authenticating a user - without them having to set up a new password.

Requirements

- access to Google Admin center
- access to Userlane Portal

In order to configure the Single Sign-On for Userlane, follow these steps below:

1. Configuring Google Workspace

1. Open the Google Admin center (admin.google.com) and navigate to Apps / Web and mobile apps



- Security
- 2. Click on "Add app" and select "Add custom SAML app"

Apps (0)	Add app Settings	
+ Add a filte	Search for apps	
Name ↑	Add private Android app	User ac
	Add private Android web app	
	Add custom SAML app	

3. Enter "Userlane" as App name. Optionally add a description and App icon (these are non-essential parameters). Continue to the next screen.

× Add custom SAML app			
1 App details — 2 Google Identity Provider detail: — 3 Service provider details — 4 Attribute mapping			
	App details		
	Enter details for your custom SAML app. This information is shared with app users. Learn more		
	Appiname		
	Userlane		
	Description		

4. Copy the SSO URL from Google and paste it into the "IDP Entrypoint URL" field in the Userlane Portal's SSO configuration page (Account > Global settings > Single Sign-on).

Configure SSO
IDP ENTRYPOINT URL (FOR SAML)
https://accounts.google.com/o/saml2/idp?idpid=C033qktqm

5. Copy the Certificate from Google and paste it into the "IDP Certificate" field on the same page in the Userlane Portal.



6. Then remove the "---BEGIN CERTIFICATE---" and "---END CERTIFICATE---" lines from the beginning and ending of the textbox.



7. Confirm these edits by clicking "Save" on the Userlane Portal.

8. Copy the "Userlane Entity ID & Consumer URL" from the Userlane Portal. This typically looks like a URL starting with https://sso-saml.userlane.com/..

USERLANE ENTITY ID & CONSUMER URL	
https://sso-saml.userlane.com/c/12345/authenticate	

- 9. Back on the Google Admin page, continue to the next step.
- 10. We tried to make this as easy as possible for you at Userlane, so the copied URL same value goes into both the "ACS URL" and "Entity ID" on the Google Admin configuration screen. Tick the "Signed response" checkmark.

Service provider details

To configure Single Sign-On, add service provider details such as ACS URL and entity ID. Learn more

ACS URL

https://sso-saml.userlane.com/c/12345/authenticate

Entity ID

https://sso-saml.userlane.com/c/12345/authenticate

Start URL (optional)

\checkmark	Signed	response
--------------	--------	----------

11. For the Name ID confirmation, you can leave the default configuration unchanged.

Name ID

Defines the naming format supported by the identity provider. Learn more

Name ID	format
---------	--------

UNSPECIFIED

Name ID

Basic Information > Primary email

12. On the next step, you can optionally add attributes that should be handed over from Google Workspaces to Userlane for each user. This allows you to enhance the Userlane profile in Userlane, which can be used to segment users and show them targeted content. You can leave it blank or add a few relevant mappings:

Google directory attributes			App attributes	
Address > Country	Ŧ	\rightarrow	country	a ×
Employee Details > Employee ID	Ŧ	\rightarrow	id	×
Employee Details > Department	Ŧ	\rightarrow	department	×

- 13. Complete the configuration of Userlane as SAML App in Google Admin.
- 14. Make sure to enable access to the Userlane SAML App in Google Admin for your entire organization.

Service status:		^
Service status:	 ON for everyone OFF for everyone Most changes take effect within a few minutes. Learn more 	
	1 unsaved change CANCEL S	SAVE

2. Add information to Userlane Portal

Continue with step 4 from the article on setting up SSO for Userlane.