

SSO Setup Guide (SAML - Google)

Jun 2024

I. Objective

This guide helps administrators of FacilityBot setup SSO login. The process includes 3 parts:

- A. Create groups on Google Admin.
- B. Setup a custom SAML app.
- C. Setup SSO in FacilityBot admin portal.

II. Create Groups on an Okta account.

1. Go to <https://admin.google.com/>

2. To create groups go to Directory -> Groups - > Create group

- Our system supports 4 groups name (FacilityBot_ROLE_Admin, FacilityBot_ROLE_Manager, FacilityBot_ROLE_Responder, FacilityBot_Role_Requestor), which map to the Admin, Manager, Responder and Requestor roles in FacilityBot respectively
- Note however, that if an account has already been created within the FacilityBot admin portal for that email address, the role specified within the FacilityBot admin portal will override the role specified in Google.
- If there is no account created within the FacilityBot admin portal for that email address, then a new account will be created in the FacilityBot admin portal with the role specified in Google group when the user signs in

Admin

Search for users, groups or settings

Groups

To easily identify and manage groups you apply policies to, such as access control, add the Security label to them.

Groups Showing all groups [Create group](#) [Inspect groups](#)

+ Add a filter

<input type="checkbox"/>	Group name ↑	Email address	Members	Access type
<input type="checkbox"/>	Everyone	everyone@robusttechhouse.com	4	Custom
<input type="checkbox"/>	FacilityBot_ROLE_Admin	facilitybot_role_admin@robusttechhouse....	1	Restricted
<input type="checkbox"/>	FacilityBot_ROLE_Manager	facilitybot_role_manager@robusttechhou...	1	Restricted
<input type="checkbox"/>	FacilityBot_ROLE_Requestor	facilitybot_role_requestor@robusttechho...	1	Restricted
<input type="checkbox"/>	FacilityBot_ROLE_Responder	facilitybot_role_responder@robusttechho...	1	Restricted

III. Setup custom SAML app

In Admin portal find “Apps” -> “Web and mobile app” -> “Add custom SAML app”

Admin

Search for users, groups or settings

Apps > Web and mobile apps

Apps (3) [Add app](#) [Settings](#)

+ Add a filter

Search for apps

<input type="checkbox"/>	Name ↑	Authentication	User access	Details
<input type="checkbox"/>	Add private Android app			
<input type="checkbox"/>	Add private Android web app	SAML	ON for everyone	Certificate expires on May 27, 2028
<input type="checkbox"/>	Add custom SAML app	SAML	ON for everyone	Certificate expires on May 27, 2028
<input type="checkbox"/>	FacilityBot UAT	Web SAML	ON for everyone	Certificate expires on May 27, 2028

Step 1. Add app name, description, logo -> Continue

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](#)

App name


FacilityBot

Description

Description

App icon

Attach an app icon. Maximum upload file size: 4 MB



Step 2. Copy “SSO URL” and “Certificate”

To configure single sign-on (SSO) for SAML apps, follow your service provider's instructions. [Learn more](#)

Option 1: Download IdP metadata

[DOWNLOAD METADATA](#)

OR

Option 2: Copy the SSO URL, entity ID, and certificate

SSO URL

`https://accounts.google.com/o/saml2/idp?idpid=C0219o0bf`



Entity ID

`https://accounts.google.com/o/saml2?idpid=C0219o0bf`



Certificate

Google_2028-5-27-2236_SAML2_0

Expires May 27, 2028



```
Qpi6mGc2BCsh5LiilFezQ0ywhPFA2U3ufvGD8hA+tyX7tFy6rIVtTqEPICmrcRj75w2b8wMBCQ
uyDTQf3HBnQozY4Kki0/NoUQz7St7v2tQX9mirbQwtin7+nqahwRiyzog2fHfX5HdCHgvr2G6A68
iX/Rjx+k1rsxZnM1U+UMIZSbSkZBfWrJ1852gB0jR6Ry4vc6zxbBCw3RYxXAzkmpC/Ah9zx8gWS
xcSagyfWnxc7u4dlcw0h0eJ2fyF/+TdMC4vvrWSFBXce -----END CERTIFICATE-----
```

SHA-256 fingerprint

`3E:99:3B:59:4C:61:21:DC:64:8A:EF:8F:15:8B:2D:3D:F1:E7:16:69:9E:4D:B6:03:EF:BB:BF:61:27:6B:7E:20`



Step 3. Add “ACS URL”, “Entity ID”, “Start URL”, “Name ID format”, “Name ID” with format below

ACS URL: <https://portal.facilitybot.co/managers/auth/saml/callback>

Entity URL: < your domain >

Start URL: <https://portal.facilitybot.co/managers/auth/saml>

Name ID format: EMAIL

Name ID: Basic information > Primary Email

✓ Google Identity Provider detail: — 3 Service provider details — 4 Attribute mapping

Service provider details

To configure single sign on, add service provider details such as ACS URL and entity ID. [Learn more](#)

ACS URL

<https://portal.facilitybot.co/managers/auth/saml/callback>

Entity ID

facilitybot.co

Start URL (optional)

<https://portal.facilitybot.co/managers/auth/saml>

☐ Signed response

Name ID

Defines the naming format supported by the identity provider. [Learn more](#)

Name ID format

EMAIL

Name ID

Basic Information > Primary email

Step 4. Attribute mapping

In Attributes section mapping **Primary Email -> uid**

In Group membership mapping 5 groups (**Everyone, FacilityBot_ROLE_Admin, FacilityBot_ROLE_Manager, FacilityBot_ROLE_Responder, FacilityBot_Role_Requestor**) -> groups (**downcase**)

After added information above -> **FINISH**

Provider detail: — ☒ Service provider details — **4** Attribute mapping

Attributes

Add and select user fields in Google Directory, then map them to service provider attributes. Attributes marked with * are mandatory. [Learn more](#)

Google Directory attributes		App attributes
Basic Information >		
Primary email	→	uid

[ADD MAPPING](#)

Group membership (optional)

Group membership information can be sent in the SAML response if the user belongs to any of the groups you add here.

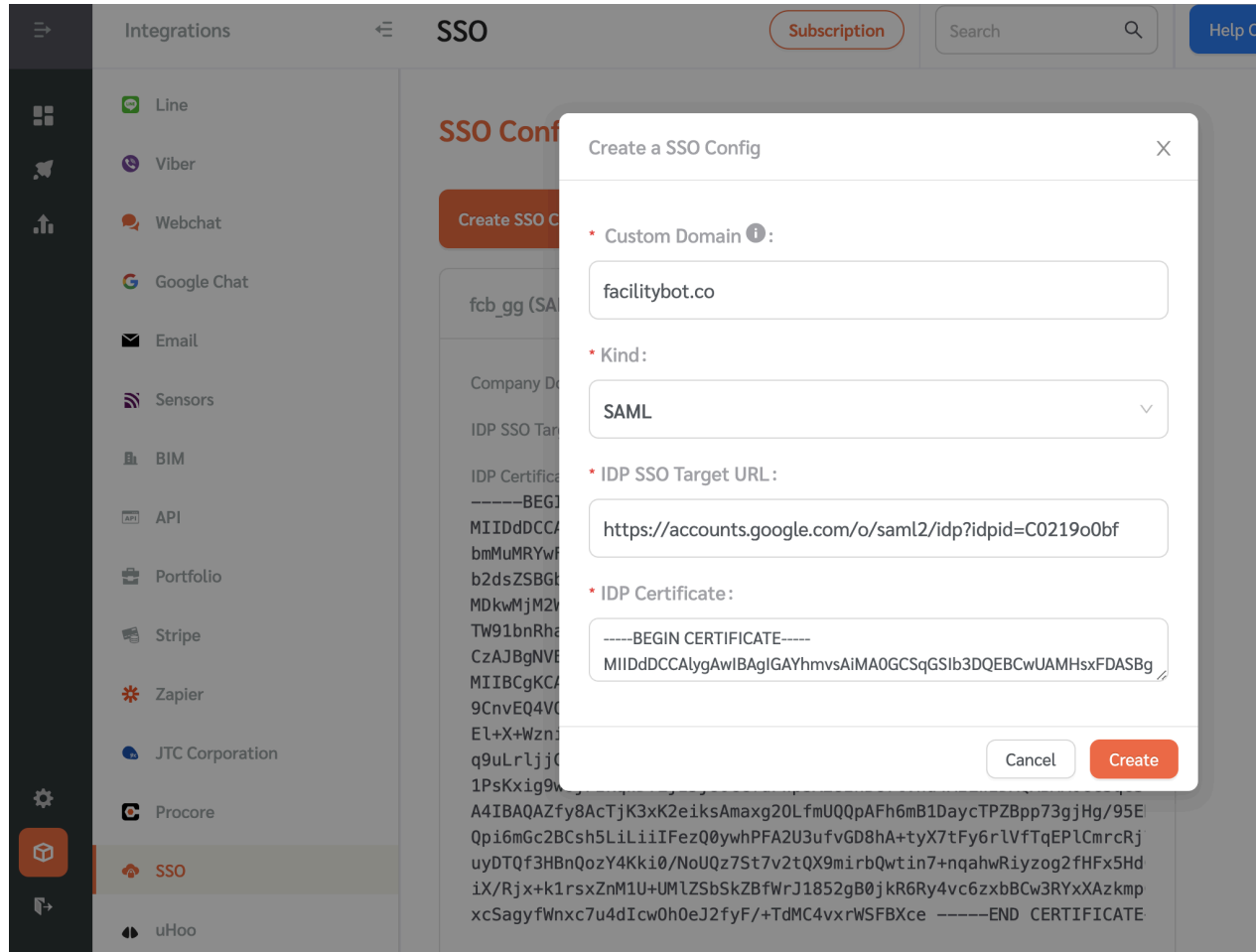
Google groups		App attribute
Everyone ✕		
FacilityBot_ROLE_Admin ✕		
FacilityBot_ROLE_Manager ✕		
FacilityBot_ROLE_Requestor ✕		
FacilityBot_ROLE_Responder ✕		
	→	groups

Search for a group

[BACK](#)[CANCEL](#)[FINISH](#)

IV. Setup SSO in the FacilityBot admin control panel.

1. Login to Admin portal -> Integrations -> SSO -> Click button Create SSO Config



2. In **Custom Domain** should be the same Entity URL value(step 3 of III)

3. In **Kind** field, select SAML

4. In **IDP SSO Target URL** is SSO URL that you copied above(step 2 of III)

5. In **IDP Certificate** is Certificate that you copied above(step 2 of III)

Now the SSO should work fine.

./.