RTH FacilityBot 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	Q Search for users, groups or settings					
Â	Home	Groups					
• °	Directory		i To easily identify and manage groups you apply policies to, such as access control, add the Security label to them.				
	Users						
	Groups	Groups Showing all groups Create group Inspect groups					
	Organizational units		$(\pm$	+ Add a filter			
	 Buildings and resources 			a b	Email address	Members	
	Directory settings			Group name 🔨	Email address	Members	Access type
	Directory sync BETA			Everyone	everyone@robusttechhouse.com	4	Custom
• [0	Devices			FacilityBot_ROLE_Admin	facilitybot_role_admin@robusttechhouse	1	Restricted
•	Apps			FacilityBot_ROLE_Manager	facilitybot_role_manager@robusttechhou	1	Restricted
→ 🔲	Billing			FacilityBot_ROLE_Requestor	facilitybot_role_requestor@robusttechho	1	Restricted
, @	Account			FacilityBot_ROLE_Responder	facilitybot_role_responder@robusttechho	1	Restricted
	Show more						

III. Setup custom SAML app

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

= 🔿 Admin	Q Search for users, groups or settings					
	Apps → Web and mobile apps					
Devices						
- III Apps	Apps (3) Add app 💌 Settings 💌					
Overview	L Add o filts Search for apps					
 Google Workspace 	+ Add a filte Search for apps					
Additional Google services	□ Name ↑ Add private Android app hentication User access Details					
Web and mobile apps	F Add private Android web app // ON for everyone Certificate expires on May 27, 2028					
Google Workspace Marketplace apps	Add custom SAML app IL ON for everyone Certificate expires on May 27, 2028					
> 😯 Security						
II Reporting	FacilityBot UAT Web SAML ON for everyone Certificate expires on May 27, 2028					
→ Billing						

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

1 App details — 2	Google Identity Provider detail: — 🗿 Service provider details — 🖪 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	e	
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	Ō	
Entity ID		
https://accounts.google.com/o/saml2?idpid=C0219o0bf		
Certificate		
Google_2028-5-27-2236_SAML2_0 Expires May 27, 2028	⊡ ₹	
Qpi6mGc2BCsh5LiLiilFezQ0ywhPFA2U3ufvGD8hA+tyX7tFy6rlVfTqEPlCmrcRj75w2b8wMBCQ uyDTQf3HBnQozY4Kki0/NoUQz7St7v2tQX9mirbQwtin7+nqahwRiyzog2fHFx5HdCHgvr2G6A68 iX/Rjx+k1rsxZnM1U+UMIZSbSkZBfWrJ1852gB0jkR6Ry4vc6zxbBCw3RYxXAzkmpC/Ah9zx8gWS xcSagyfWnxc7u4dlcw0h0eJ2fyF/+TdMC4vxrWSFBXceEND 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	ē	

Step 3. Add "ACS URL", "Entity ID", "Start URL", "Name ID format", "Name ID" with format below ACS URL: <u>https://portal.facilitybot.co/managers/auth/saml/callback</u> Entity URL: < your domain >

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

Name ID format: EMAIL

Name ID: Basic information > Primary Email

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

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	l information	above ->	FINISH
-------------	---------------	----------	--------

Attributes		
Add and select user fields in Google Director	ry, then map them to service provider attributes. Attributes marked	d with * are mandatory. Learn more
Google Directory attributes	App attributes	
Basic Information >		
Primary email	$\overline{} \rightarrow$ uid	×
	in the SAML response if the user belongs to any of the groups you	u add here.
Group membership information can be sent		u add here. ttribute
Group membership information can be sent	App a	ttribute
Group membership information can be sent Google groups Everyone S FacilityBot_ROLE_Admir	App a	ttribute
Google groups Everyone S FacilityBot_ROLE_Admir	App a n ⊗ FacilityBot_ROLE_Manager ⊗ → group	ttribute

IV. Setup SSO in the FacilityBot admin control panel.

⇒	Integrations	< SSO	Subscription Search Q Help
	🖸 Line	SSO Conf	
,M	O Viber	550 com	Create a SSO Config X
.tı	🍳 Webchat	Create SSO C	* Custom Domain 🕕 :
	G Google Chat	fcb gg (SA	facilitybot.co
	🖿 Email		* Kind:
	Sensors	Company Do	SAML
	BL BIM	IDP 550 Tar	* IDP SSO Target URL:
	API	BEGI MIIDdDCCA	https://accounts.google.com/o/saml2/idp?idpid=C0219o0bf
	Portfolio	bmMuMRYwf b2dsZSBGt MDkwMjM2V	* IDP Certificate:
	🖷 Stripe	TW91bnRha CzAJBgNVE	BEGIN CERTIFICATE MIIDdDCCAlygAwIBAgIGAYhmvsAiMA0GCSqGSIb3DQEBCwUAMHsxFDASBg
	🔆 Zapier	MIIBCgKC/ 9CnvEQ4V0	
	JTC Corporation	El+X+Wzni q9uLrljj(Cancel
*	C Procore		8AcTjK3xK2eiksAmaxg20LfmUQQpAFh6mB1DaycTPZBpp73gjHg/95E sh5LiLiiIFezQ0ywhPFA2U3ufvGD8hA+tyX7tFy6rlVfTgEPlCmrcRj
Ŷ	🔷 SSO	uyDTQf3HBn	QozY4Kki0/NoUQz7St7v2tQX9mirbQwtin7+nqahwRiyzog2fHFx5Hd sxZnM1U+UMlZSbSkZBfWrJ1852qB0jkR6Ry4vc6zxbBCw3RYxXAzkmp
¶→	● uHoo		c7u4dIcw0h0eJ2fyF/+TdMC4vxrWSFBXceEND CERTIFICATE

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.

./.