

SSO Setup Guide (SAML - Okta)

Apr 2024

I. Objective

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

- A. Create Groups on an Okta account.
- B. Setup SSO on an Okta account.
- C. Setup SSO in FacilityBot admin portal.

II. Create Groups on an Okta account.

1. Go to <https://developer.okta.com/> -> Sign In -> Admin portal

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

- Our system supports 4 group names (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
- Within Okta, you can create and assign email addresses to the respective Role
- Note however, that if an account has already been created within FacilityBot admin portal for that email address, the role specified within the FacilityBot admin portal will override the role specified in Okta
- 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 Okta when the user signs in

Okta Admin Portal - Groups Page

Search for people, apps and groups

Groups

FacilityBot_ROLE_Requestor
No description
1 People, 1 Application

FacilityBot_ROLE_Manager
No description
3 People, 1 Application

FacilityBot_ROLE_Admin
No description
3 People, 1 Application

Everyone
All users in your organization
3 People, 0 Applications

FacilityBot_ROLE_Responder
No description
1 People, 1 Application

Okta Administrators
Okta manages this group, which contains all administrators in your organization.

III. Setup SSO on an Okta account.

1. In Admin portal find “Applications” -> Click button “Create App Integration”

Okta Admin Portal - Applications Page

Search for people, apps and groups

Applications

Create App Integration | Browse App Catalog | Assign Users to App | More

Facility Bot Local Saml

Facilitybot Local
Client ID: 0oa79nwjhipW94Zba697

2. In “Create a new app integration” select option “SAML 2.0” -> Next

Create a new app integration

Sign-in method

[Learn More](#)

☐ OIDC - OpenID Connect

Token-based OAuth 2.0 authentication for Single Sign-On (SSO) through API endpoints. Recommended if you intend to build a custom app integration with the Okta Sign-In Widget.

☒ SAML 2.0

XML-based open standard for SSO. Use if the Identity Provider for your application only supports SAML.

☐ SWA - Secure Web Authentication

Okta-specific SSO method. Use if your application doesn't support OIDC or SAML.

☐ API Services

Interact with Okta APIs using the scoped OAuth 2.0 access tokens for machine-to-machine authentication.

Cancel

Next

3. In General Settings enter your App name -> Next

Create SAML Integration


1 General Settings	2 Configure SAML	
---------------------------	-------------------------	--



1 General Settings

App name

Your App Name

App logo (optional)





App visibility

☐ Do not display application icon to users

☐ Do not display application icon in the Okta Mobile app

Cancel

Next

4. Add Single sign-on URL: <https://portal.facilitybot.co/managers/auth/saml>

5. Add Audience URI (SP Entity ID): Users will enter the Identifier (SP Entity ID) in the FacilityBot Sign In page to identify your company.

1 General Settings	2 Configure SAML	
--------------------	------------------	--

A SAML Settings

General

Single sign-on URL ?

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

☒ Use this for Recipient URL and Destination URL

Audience URI (SP Entity ID) ?

CompanyName

Default RelayState ?

If no value is set, a blank RelayState is sent

Name ID format ?

Unspecified

Application username ?

Okta username

Update application username on

Create and update

[Show Advanced Settings](#)

6. Click “Show Advanced Settings” -> add Other Requestable SSO URLs :
<https://portal.facilitybot.co/managers/auth/saml/callback>

Hide Advanced Settings

Response ?

Signed

Assertion Signature ?

Signed

Signature Algorithm ?

RSA-SHA256

Digest Algorithm ?

SHA256

Assertion Encryption ?

Unencrypted

Signature Certificate ?

Browse files...

Enable Single Logout ?

☐ Allow application to initiate Single Logout

Signed Requests ?

☐ Validate SAML requests with signature certificates.
SAML request payload will be validated. SSO URLs will be read dynamically from the request. [Read more](#)

Other Requestable SSO URLs

URL	Index	
t.co/managers/auth/saml/callback	0	×

+ Add Another

7. In Group Attribute Statements (optional) add some information below -> Next

Name: **groups**

Name format: **Unspecified**

Starts with: **.***

Add Another

Group Attribute Statements (optional)

Name

Name format
(optional)

Filter

groups

Unspecified ▼

Starts with ▼

.*

Add Another

B Preview the SAML assertion generated from the information above

<> Preview the SAML Assertion

This shows you the XML that will be used in the assertion - use it to verify the info you entered above

Previous

Cancel

Next

8. On the Feedback step, select app type as an internal app -> Finish


Create SAML Integration

1 General Settings	2 Configure SAML	3 Feedback
--------------------	------------------	------------

3 Help Okta Support understand how you configured this application

1

The optional questions below assist Okta Support in understanding your app integration.

App type 

☒ This is an internal app that we have created


[Previous](#)

[Finish](#)


Why are you asking me this?

This form provides Okta Support with useful background information about your app. Thank you for your help—we appreciate it.

9. On the Assignments tab, assign the groups created above to the groups with the same image below.



SAML Test

Active ▾ View Logs Monitor Imports

GeneralSign OnMobileImportAssignments

Assign ▾
















Convert assignments ▾

Search...

Groups ▾

Assign to People

Assign to Groups

	Assignment		
1	 FacilityBot_ROLE_Admin No description		
2	 Everyone All users in your organization		
3	 FacilityBot_ROLE_Manager No description		
4	 FacilityBot_ROLE_Requestor No description		
5	 FacilityBot_ROLE_Responder No description		

10. On the Sign On tab, click “More details” in SAML 2.0 section then copy “Sign on URL” and “Signing Certificate” to Facility SSO config.

Settings

[Edit](#)

Sign on methods

The sign-on method determines how a user signs into and manages their credentials for an application. Some sign-on methods require additional configuration in the 3rd party application.

Application username is determined by the user profile mapping. [Configure profile mapping](#)

☒ SAML 2.0

Default Relay State

Metadata details

Metadata URL `https://dev-40542892.okta.com/app/exkgnd5stsHW6zVLW5d7/sso/saml/metadata`

 [Copy](#)

☒ Hide details

Sign on URL `https://dev-40542892.okta.com/app/dev-40542892_samltest_1/exkgnd5stsHW6zVLW5d7/sso/saml`

 [Copy](#)

Sign out URL `https://dev-40542892.okta.com`

 [Copy](#)

Issuer `http://www.okta.com/exkgnd5stsHW6zVLW5d7`

 [Copy](#)

Signing Certificate

 [Download](#)

 [Copy](#)

IV. Setup SSO in the FacilityBot admin control panel.

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

The screenshot shows the FacilityBot admin control panel. On the left is a sidebar with various integration options: Viber, Webchat, Google Chat, Email, Sensors, BIM, API, Portfolio, Stripe, Zapier, JTC Corporation, Procore, SSO (highlighted), and uHoo. The main content area is titled 'SSO' and contains a 'Create SSO Config' button. A modal window titled 'Create a SSO Config' is open, showing the following fields:

- Custom Domain:** facilitybot
- Kind:** SAML
- IDP SSO Target URL:** https://dev-40542892.okta.com/app/dev-40542892_samltest_1/
- IDP Certificate:** MIIDqDCCApCgAwIBAgIGAY8PT1QuMA0GCSqGSIb3DQEBCwUAMIGUMQswCQYDVQQGEwJVUzETMBEGA1UECAwKQ2FsaWZvcn5pYTEWMBBQA1UEB...

At the bottom of the modal are 'Cancel' and 'Create' buttons.

2. In **Custom Domain** should be the same Audience URI (SP Entity ID) value(section 3 of III)

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

4. In **IDP SSO Target URL** is Sign On URL that you copied above(section 10 of III)

5. In **IDP Certificate** is Signing Certificate that you copied above(section 10 of III)

Now the SSO should work fine.

./.