

SSO against OKTA Identity Provider

This article describes how to configure Okta to enable Imagicl users to login to web portal, gadgets and Attendant Console with Single Sign-on based on SAML protocol.

Prerequisites

In order to successfully configure your Okta, you should have the following data:

- **User Pool ID**
- **Redirect URI**

More details available [here](#).

Moreover, you must have a valid administrative account on your Okta production instance to perform the following configurations.

Procedure

1. Sign in to Okta portal, using your domain account with administrative rights.
2. In the navigation menu, expand **Applications**, and then choose **Applications**.
3. Choose **Create App Integration**.
4. In the **Create a new app integration** menu, choose **SAML 2.0** as the **Sign-in method**.
5. Hit **Next**.

Edit SAML Integration

1 General Settings


2 Configure SAML



1 General Settings

App name

Imagicl UC Suite

App logo (optional)



App visibility

☒ Do not display application icon to users

Cancel

Next

6. Please enter an App name, like above "Imagicl UC Suite" and hit **Next**.

A SAML Settings

General

Single sign-on URL ⓘ

☒ Use this for Recipient URL and Destination URL

Audience URI (SP Entity ID) ⓘ

Default RelayState ⓘ

If no value is set, a blank RelayState is sent

Name ID format ⓘ

Application username ⓘ

Attribute Statements (optional)

[LEARN MORE](#)

Name	Name format (optional)	Value
<input type="text" value="http://schemas.xmlsoap."/>	<input type="text" value="Basic"/>	<input type="text" value="user.email"/>
Add Another		<ul style="list-style-type: none"> user.firstName user.lastName user.email user.login device.trusted

Group Attribute Statements (optional)

Name	Name format (optional)
------	---------------------------

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

7. Compile above form with following data, leaving other fields with default values:

- **Single sign-on URL:** Enter here the *Redirect URI* provided by Imagicle
- **Audience URI (SP Entity ID):** Enter here the *User Pool ID* provided by Imagicle
- Under **Attribute Statements (optional)**, please enter:
 - ◆ **Name:** `http://schemas.xmlsoap.org/ws/2005/05/identity/claims/emailaddress`
 - ◆ **Name Format:** Basic
 - ◆ **Value:** user.email

8. At the bottom of this web page, you can click on "*Preview the SAML Assertion*" to trigger the pop-up of a new web panel including the SAML Assertion. Please verify that all data is consistent.

9. Hit **Next**.

10. Choose a feedback response for Okta Support.

11. Choose **Finish**.

Imagicle_Test

Active

View Logs

Monitor Imports

i

Once you have a working SAML integration, submit it for Okta review to publish in the OAN.

Submit your app for review

SAML Signing Certificates

Generate new certificate

Type	Created	Expires	Status	Actions
SHA-2	Today	Jan 2033	Active	<div>Actions</div> <div> <div>View IdP metadata</div> <div>Download certificate</div> </div>

View SAML Setup

Single Sign On (SSO) will work until you trust Okta as a provider.

View S

12. The configuration is accomplished.

13. In "SAML Signing Certificates", please select **View IdP metadata**, available for the Active SHA-2 certificate.
14. A new web window is displayed, including XML SAML certificate. Please save XML code as text file and send it to Imagicle Support team.
15. Assign the new created App Integration to the relevant company users/groups that need to leverage the SSO (*Applications* > select the Imagicle app integration > *Assignments*).