

## Setting up SCIM with Okta

## Abstract

Informatica Intelligent Cloud Services<sup>SM</sup> user provisioning through SCIM 2.0 is available through Okta. This article provides instructions for setting up SCIM-based user and group sync for Okta.

## Supported Versions

- Informatica Intelligent Cloud Services April 2024

## Table of Contents

Overview. . . . .	2
Step 1. Create a provisioning app in Okta. . . . .	2
Step 2. Set up SAML and enable SCIM in Informatica Intelligent Cloud Services. . . . .	5
Step 3. Integrate the Okta provisioning app with Informatica Intelligent Cloud Services. . . . .	7
Step 4. Map SCIM attributes in the provisioning app. . . . .	9
Step 5. Provision Okta users in Informatica Intelligent Cloud Services. . . . .	16
Step 6. Map Okta groups to Informatica Intelligent Cloud Services roles. . . . .	21
Step 7. Push Okta groups to Informatica Intelligent Cloud Services. . . . .	22
Signing on to Informatica Intelligent Cloud Services as a provisioned user. . . . .	25
Guidelines for working with users. . . . .	26
Guidelines for working with groups. . . . .	27

## Overview

Informatica Intelligent Cloud Services<sup>SM</sup> user provisioning through SCIM 2.0 is available through Okta. If you are an Informatica Intelligent Cloud Services organization administrator, you can set up SCIM-based user and group sync for Okta. To do this, you must create an Okta provisioning application to sync your Okta users and groups with Informatica Intelligent Cloud Services.

**Note:** If you do not use SCIM, follow the setup instructions in this [Knowledge Base article](#) instead.

To set up SCIM with Okta, complete the following tasks:

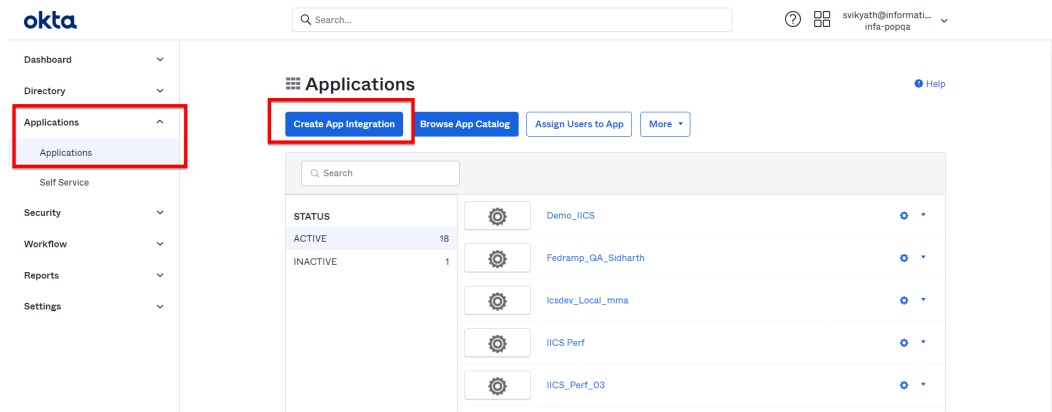
1. Create a provisioning app in Okta.
2. Set up SAML and enable SCIM in Informatica Intelligent Cloud Services.
3. Integrate the provisioning app with Informatica Intelligent Cloud Services.
4. Map SCIM attributes in the provisioning app.
5. Provision Okta users.
6. Map Okta groups to Informatica Intelligent Cloud Services roles.
7. Push Okta groups to Informatica Intelligent Cloud Services.

## Step 1. Create a provisioning app in Okta

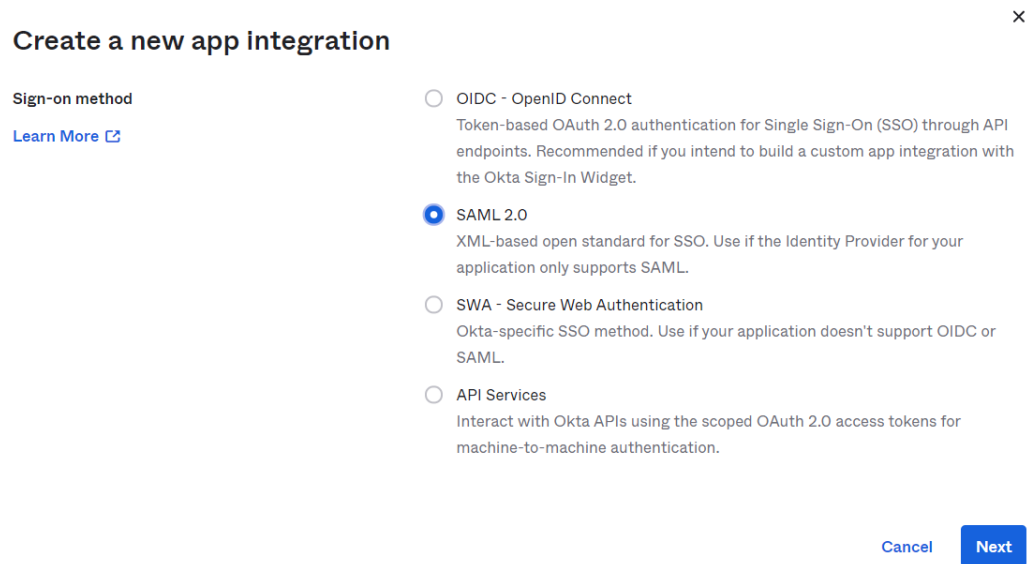
Create an app in Okta to provision users and groups in Informatica Intelligent Cloud Services.

1. Log in to Okta as an administrator.

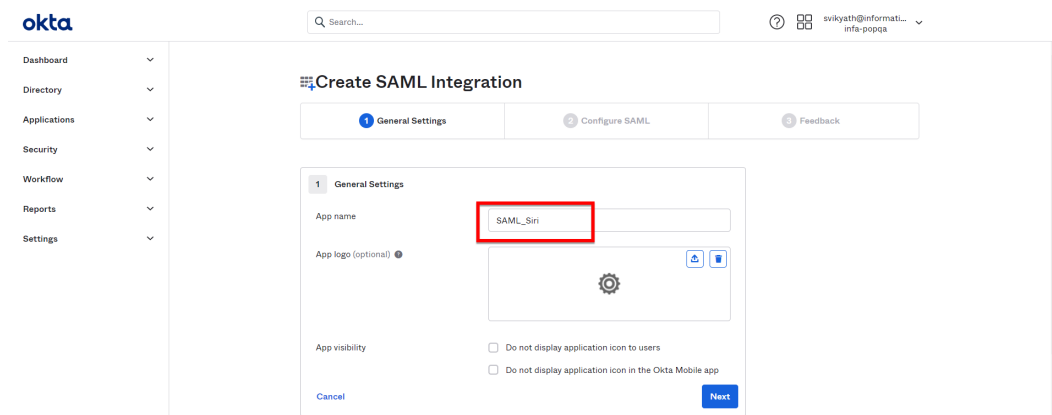
2. On the left panel, select **Applications > Applications**, and click **Create App Integration**.



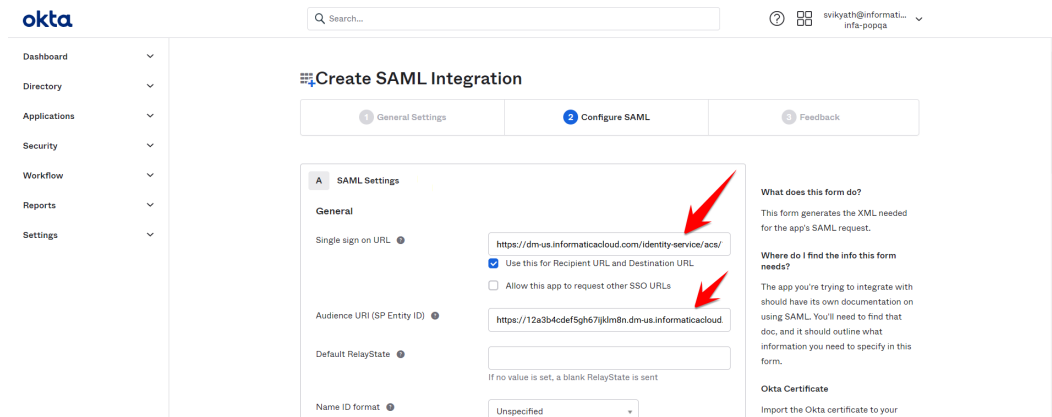
3. In the **Create a new app integration** window, select **SAML 2.0** and click **Next**.



4. On the **General Settings** tab, enter an app name and click **Next**.



- On the **Configure SAML Settings** tab, configure the **Single sign on URL** and **Audience URI**.



Setting	Value
Single sign on URL	<IICS base URL>/identity-service/acs/<organization ID> For example, https://dm-us.informaticacloud.com/identity-service/acs/12a3b4cdef5gh67ijklm8n
Audience URI (SP Entity ID)	https://<organization ID>.<hostname> For example, https://12a3b4cdef5gh67ijklm8n.dm-us.informaticacloud.com

Accept the default values for **Name ID format**, **Application username**, and **Update application username**.

- In the **Group Attribute Statements** section, enter the SAML attributes to send all groups that are associated with the user in the SAML token during sign on.

#### Group Attribute Statements (optional)

Name	Name format (optional)	Filter
groups	Unspecified	Matches regex <code>.*</code>

[Add Another](#)

Configure the following statement:

- Name:** groups
- Name format:** Unspecified
- Value:** Matches regex `.*`

- Optionally, configure other attributes such as `firstName` and `lastName`.
- Click **Next**.
- On the **Feedback** tab, click **Finish**.

10. When the app is created, open the **Settings** tab, click the **Identity Provider metadata** link, and save the identity provider metadata to an XML file.

The screenshot shows a 'Settings' page with an 'Edit' link in the top right. Under the 'Sign on methods' section, there is explanatory text about sign-on methods and a link to 'Configure profile mapping'. A radio button is selected for 'SAML 2.0', and there is a text input field for 'Default Relay State'. A yellow warning banner at the bottom states that SAML 2.0 is not configured until setup instructions are completed, with a 'View Setup Instructions' button and a note that 'Identity Provider metadata' is available if the application supports dynamic configuration.

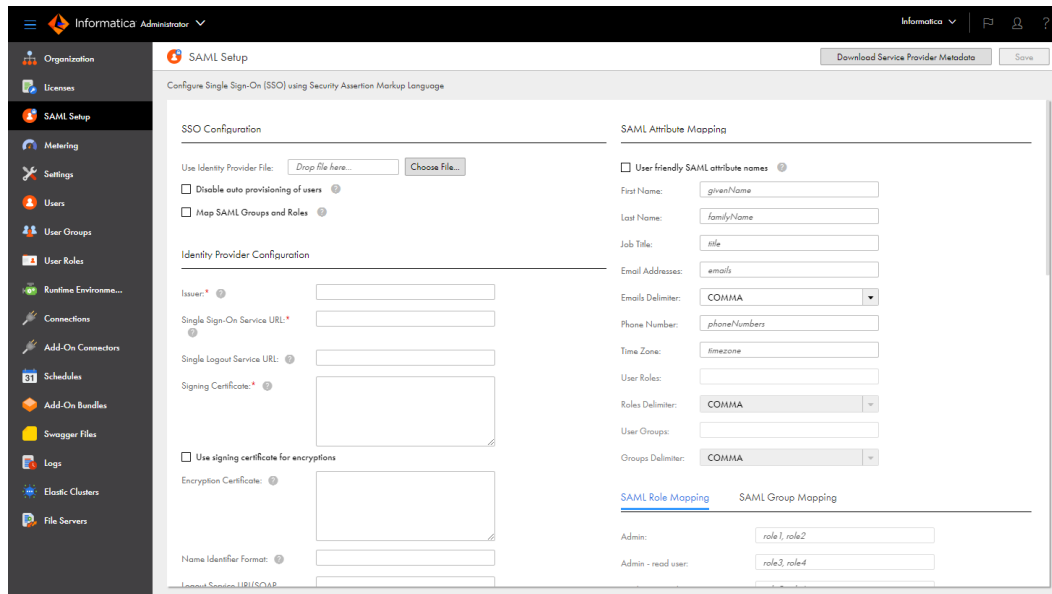
You will use this file to set up SAML in Informatica Intelligent Cloud Services.

## Step 2. Set up SAML and enable SCIM in Informatica Intelligent Cloud Services

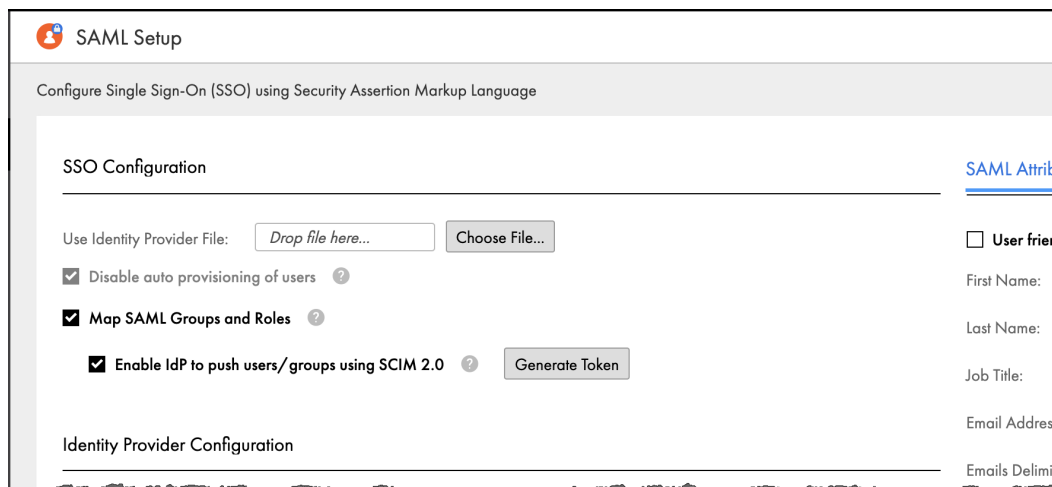
Set up SAML by uploading the metadata XML file that you generated in Okta. Then enable SCIM 2.0 and generate the token for the SCIM provisioning app.

1. Log in to Informatica Intelligent Cloud Services as a user with the Admin role.  
**Note:** If you are setting up SAML for a sub-organization, log in to the sub-organization as a native user with the Admin role. Do not log in to the parent organization and switch to the sub-organization from the parent organization.

- In Administrator, open the **SAML Setup** page.

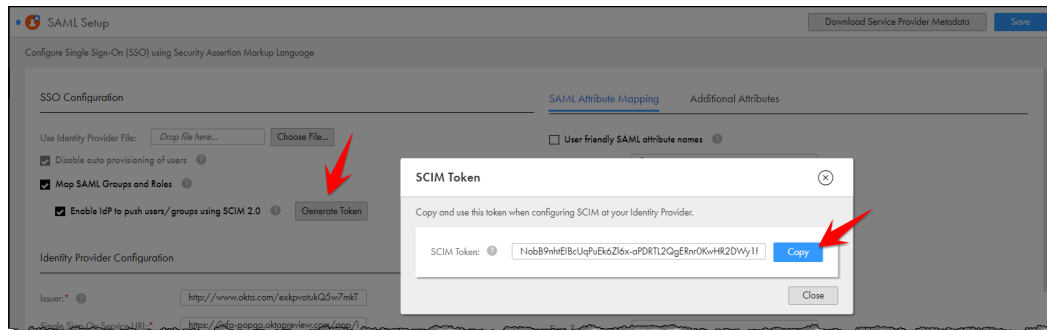


- In the SSO Configuration area, click **Choose File** and upload the metadata XML file to define the identity provider properties.
- In the SSO Configuration area, enable the **Map SAML Groups and Roles** option, and then enable the **Enable IdP to push users/groups using SCIM 2.0** option.



**Note:** When you enable the **Enable IdP to push users/groups using SCIM 2.0** option, auto-provisioning of users is disabled automatically because users are provisioned through the SCIM client.

5. Click **Generate Token** and copy the token to the clipboard.



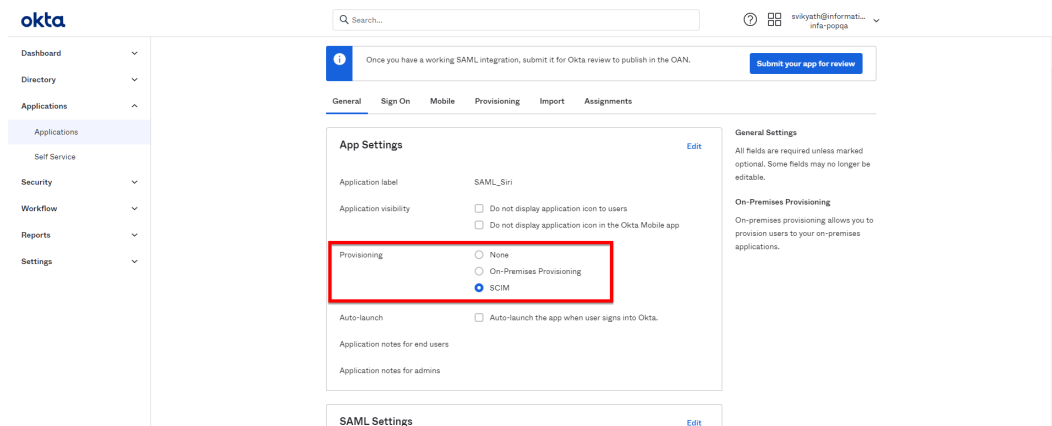
You will need the SCIM token when you enable SCIM in the provisioning app. The SCIM token is valid for six months from the time of generation.

6. Click **Save** to save the configuration.

## Step 3. Integrate the Okta provisioning app with Informatica Intelligent Cloud Services

To integrate the provisioning app with Informatica Intelligent Cloud Services, configure the provisioning mode, the integration settings, and the provisioning to app settings.

1. In Okta, open the app you created.
2. On the **General** tab, in the **App Settings** area, set the provisioning to **SCIM**.



3. On the **Provisioning** tab, select **Settings > Integration**, and configure the SCIM connection settings.

The screenshot shows the 'SCIM Connection' configuration page. The 'Provisioning' tab is selected, indicated by a red arrow. The page contains the following settings:

- SCIM version:** 2.0
- SCIM connector base URL:** https://dm-us.infa.com/scim-service
- Unique identifier field for users:** email
- Supported provisioning actions:**
  - Import New Users and Profile Updates
  - Push New Users
  - Push Profile Updates
  - Push Groups
- Authentication Mode:** HTTP Header
- HTTP Header:**
  - Authorization:** Bearer [redacted]

Buttons for 'Test Connector Configuration', 'Save', and 'Cancel' are visible at the bottom of the form.

Setting	Value
SCIM connector base URL	Enter the tenant URL. For example: https://dm-us.informaticacloud.com/scim-service
Unique identifier field for users	Enter email.
Supported provisioning actions	Enable <b>Push New Users</b> , <b>Push Profile Updates</b> , and <b>Push Groups</b> .
Authentication Mode	Select <b>HTTP Header</b> .
Bearer Token	Copy the token you generated when you enabled SCIM in Informatica Intelligent Cloud Services.

4. Click **Test Connector Configuration** to test the configuration, and then click **Close**.
5. Click **Save**.
6. On the **Provisioning** tab, select **Settings > To App**.



7. In the **Provisioning to App** settings, enable provisioning for **Create Users**, **Update User Attributes**, and **Deactivate Users**.

The screenshot shows the 'Provisioning to App' settings page in Okta. The sidebar on the left has 'Settings' selected, with sub-items 'To App', 'To Okta', and 'Integration'. The main content area is titled 'Provisioning to App' and includes a 'Cancel' button. Below this, there are four sections:

- Create Users** (checked): Creates or links a user in SAML\_Siri when assigning the app to a user in Okta. The default username used to create accounts is set to Okta username.
- Update User Attributes** (checked): Okta updates a user's attributes in SAML\_Siri when the app is assigned. Future attribute changes made to the Okta user profile will automatically overwrite the corresponding attribute value in SAML\_Siri.
- Deactivate Users** (checked): Deactivates a user's SAML\_Siri account when it is unassigned in Okta or their Okta account is deactivated. Accounts can be reactivated if the app is reassigned to a user in Okta.
- Sync Password** (unchecked): Creates a SAML\_Siri password for each assigned user and pushes it to SAML\_Siri.

8. Click **Save**.

## Step 4. Map SCIM attributes in the provisioning app

When you create the provisioning app in Okta, most attribute mappings are already correct. However, some attributes might need to be added or changed. Map attributes in the Profile Editor.

1. In Okta, go to **Directory > Profile Editor**.
2. Select the app that you created.

3. In the **Attributes** area, click **Mappings**.

The screenshot shows the configuration page for a SAML\_Siri User. The top section displays the user's details: Display name (SAML\_Siri User), Description, and Variable name (infapopqa\_samlisiri\_1). Below this is the 'Attributes' section, which contains two tabs: '+ Add Attribute' and 'Mappings'. A red arrow points to the 'Mappings' tab. The 'Mappings' tab displays a table of attributes with columns for Display Name, Variable Name, Data type, and Attribute Type. The table lists several attributes, including Username, Given name, Family name, Middle name, Honoric prefix, and Honoric suffix.

FILTERS	Display Name	Variable Name	Data type	Attribute Type
All	Username	userName	string	Base
Base	Given name	givenName	string	Custom
Custom	Family name	familyName	string	Custom
	Middle name	middleName	string	Custom
	Honorific prefix	honorificPrefix	string	Custom
	Honorific suffix	honorificSuffix	string	Custom

4. Verify that the following attributes are mapped for each user:

- id
- externalId
- username
- displayName
- title
- preferredLanguage
- locale
- timezone
- active
- addresses[type eq "work"].streetAddress
- addresses[type eq "work"].locality
- addresses[type eq "work"].region
- addresses[type eq "work"].postalCode
- addresses[type eq "work"].country
- roles
- employeeNumber
- organization
- department

- emails[type eq "work"]
- givenName
- familyName
- phoneNumbers[type eq "work"]

The attribute mapping should look like the following images. You need to map the attributes on the **SAML to Okta User** and **Okta User to SAML** tabs.

### SAML\_Siri User Profile Mappings ×

SAML\_Siri to Okta User
Okta User to SAML\_Siri

SAML_Siri User Profile appuser		Okta User User Profile user
Username is set by SAML_Siri		
<input type="text" value="appuser.givenName"/>	➔	login string
<input type="text" value="appuser.familyName"/>	➔	firstName string
<input type="text" value="Choose an attribute or enter an expression..."/>	➔	lastName string
<input type="text" value="Choose an attribute or enter an expression..."/>	➔	middleName string
<input type="text" value="Choose an attribute or enter an expression..."/>	➔	honorificPrefix string
<input type="text" value="Choose an attribute or enter an expression..."/>	➔	honorificSuffix string
<input type="text" value="appuser.email"/>	➔	email email
<input type="text" value="appuser.title"/>	➔	title string
<input type="text" value="appuser.displayName"/>	➔	displayName string
<input type="text" value="Choose an attribute or enter an expression..."/>	➔	nickName string
<input type="text" value="Choose an attribute or enter an expression..."/>	➔	profileUrl uri
<input type="text" value="Choose an attribute or enter an expression..."/>	➔	secondEmail email
<input type="text" value="Choose an attribute or enter an expression..."/>	➔	mobilePhone string
<input type="text" value="appuser.primaryPhone"/>	➔	primaryPhone string
<input type="text" value="appuser.streetAddress"/>	➔	streetAddress string
<input type="text" value="appuser.locality"/>	➔	city string
<input type="text" value="appuser.region"/>	➔	state string

appuser.region	→	state	string
appuser.postalCode	→	zipCode	string
appuser.country	→	countryCode	country code
Choose an attribute or enter an expression...	↔	postalAddress	string
appuser.preferredLanguage	→	preferredLanguage	language code
appuser.locale	→	locale	locale
appuser.timezone	→	timezone	timezone
Choose an attribute or enter an expression...	↔	userType	string
appuser.employeeNumber	→	employeeNumber	string
Choose an attribute or enter an expression...	↔	costCenter	string
appuser.organization	→	organization	string
Choose an attribute or enter an expression...	↔	division	string
appuser.department	→	department	string
Choose an attribute or enter an expression...	↔	managerId	string
Choose an attribute or enter an expression...	↔	manager	string

Preview

Save Mappings



Cancel

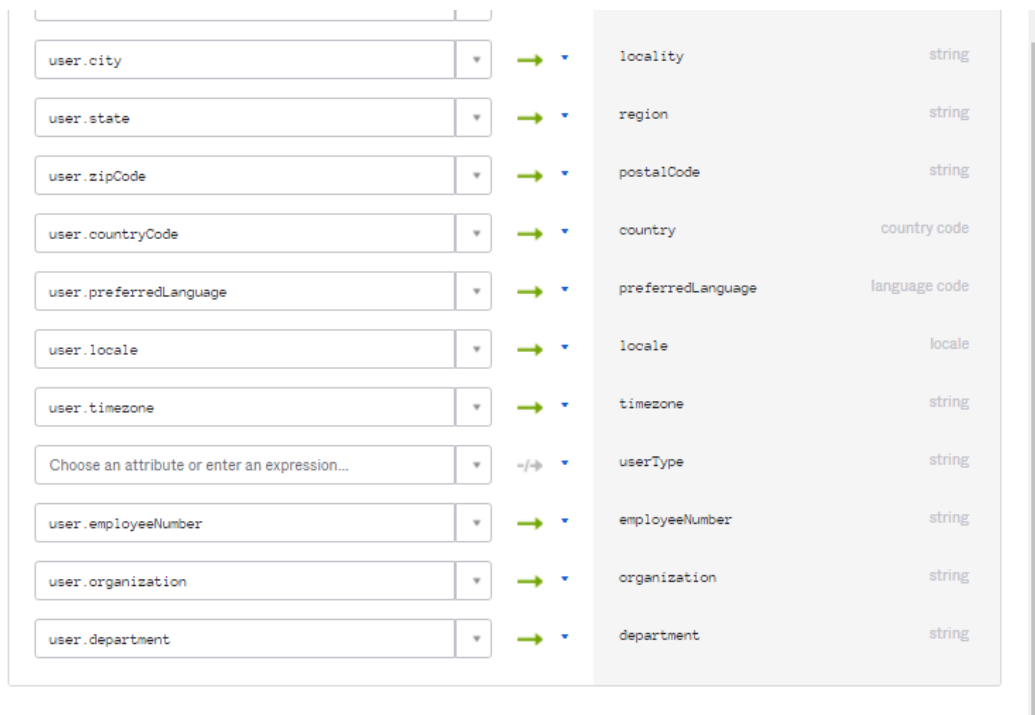
## SAML\_Siri User Profile Mappings



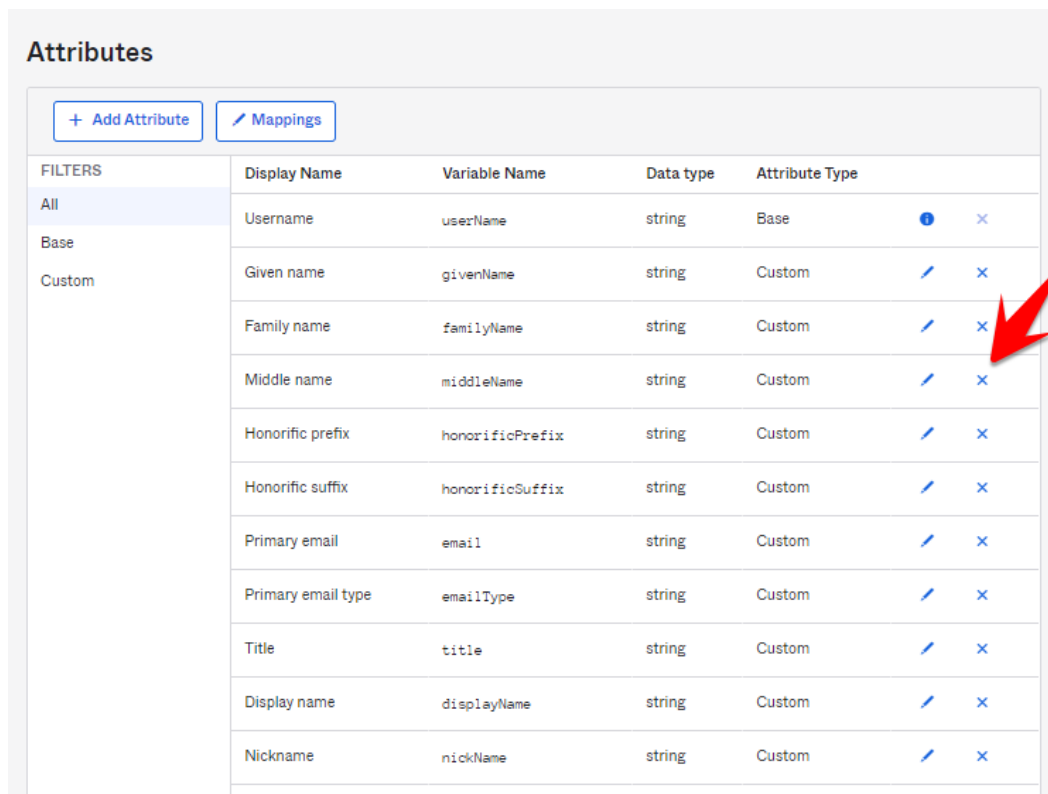
SAML\_Siri to Okta User

Okta User to SAML\_Siri

 Okta User User Profile user	 SAML_Siri User Profile appuser
Username is set by SAML_Siri	
<input type="text" value="user.firstName"/>	userName string
<input type="text" value="user.lastName"/>	givenName string
<input type="text" value="Choose an attribute or enter an expression..."/>	familyName string
<input type="text" value="Choose an attribute or enter an expression..."/>	middleName string
<input type="text" value="Choose an attribute or enter an expression..."/>	honorificPrefix string
<input type="text" value="Choose an attribute or enter an expression..."/>	honorificSuffix string
<input type="text" value="user.email"/>	email email
<input type="text" value="Choose an attribute or enter an expression..."/>	emailType email
<input type="text" value="user.title"/>	title string
<input type="text" value="user.displayName"/>	displayName string
<input type="text" value="Choose an attribute or enter an expression..."/>	nickName string
<input type="text" value="Choose an attribute or enter an expression..."/>	profileUrl uri
<input type="text" value="user.primaryPhone"/>	primaryPhone string
<input type="text" value="Choose an attribute or enter an expression..."/>	primaryPhoneType string
<input type="text" value="Choose an attribute or enter an expression..."/>	addressType string
<input type="text" value="user.streetAddress"/>	streetAddress string
<input type="text" value="user.city"/>	locality string



- To delete an attribute, close the editing pane and click the "X" icon.



The final list of attributes should look like the following image:

FILTERS		Display Name	Variable Name	Data type	Attribute Type		
All		Username	userName	string	Base	●	×
Base		Given name	givenName	string	Custom	/	×
Custom		Family name	familyName	string	Custom	/	×
		Primary email	email	string	Custom	/	×
		Title	title	string	Custom	/	×
		Display name	displayName	string	Custom	/	×
		Primary phone	primaryPhone	string	Custom	/	×
		Street address	streetAddress	string	Custom	/	×
		Locality	locality	string	Custom	/	×
		Region	region	string	Custom	/	×
		Postal Code	postalCode	string	Custom	/	×
		Country code	country	string	Custom	/	×
		Preferred language	preferredLanguage	string	Custom	/	×
		Locale	locale	string	Custom	/	×
		Time zone	timeZone	string	Custom	/	×
		Employee number	employeeNumber	string	Custom	/	×
		Organization	organization	string	Custom	/	×
		Department	department	string	Custom	/	×

## Step 5. Provision Okta users in Informatica Intelligent Cloud Services

To provision Okta users in Informatica Intelligent Cloud Services, create users in Okta, assign the users to a group, and then assign the provisioning app to the group.

Before you provision users, ensure that SCIM is enabled in both Informatica Intelligent Cloud Services and the provisioning app and that the test connection from the app is successful.



**Note:** Every user that you want to provision must be part of a group because Informatica Intelligent Cloud Services roles are mapped to Okta groups. If the user is not part of an Okta group, the user will have no Informatica Intelligent Cloud Services role and cannot sign on to Informatica Intelligent Cloud Services.

1. Create users in Okta:

- a. In Okta, on the left panel, select **Directory > People**, and click **Add person**.

The screenshot shows the Okta People management interface. The left sidebar contains a navigation menu with the following items: Dashboard, Directory, People (selected), Groups, Profile Editor, Directory Integrations, Profile Sources, Applications, Security, Workflow, Reports, and Settings. The main content area is titled 'People' and includes a search bar, a '+ Add person' button, and buttons for 'Reset passwords' and 'Reset multifactor'. Below this is a table of users with the following data:

	Person & username	Primary email	Status
Everyone	67		
	RajUser_01 raj@gmail.com	raj@gmail.com	Password expired
Onboarding			
Staged	5		
	minion1 minion1@gmail.com	minion1@gmail.com	Active
Pending user action	1		
	minion10 minion10@gmail.com	minion10@gmail.com	Active
Active			
	minion11 minion11@gmail.com	minion11@gmail.com	Active
Active	55		
	minion12 minion12@gmail.com	minion12@gmail.com	Active
Password reset	0		
	minion13 minion13@gmail.com	minion13@gmail.com	Active
Locked out	0		
	minion14 minion14@gmail.com	minion14@gmail.com	Active
Inactive			
Suspended	3		
	minion15 minion15@gmail.com	minion15@gmail.com	Active
Deactivated	2		
	minion16 minion16@gmail.com	minion16@gmail.com	Active

- b. In the **Add Person** dialog box, enter the user details.

**Add Person**

User type ⓘ User

First name

Last name

Username

Primary email

Secondary email (optional)

Groups (optional) Admin x

Password ⓘ Set by user

Send user activation email now ⓘ

**Save** **Save and Add Another** Cancel

- c. Click **Save** or click **Save and Add Another** to add another user.

2. Assign the users to groups:

- a. Select **Directory > Groups**, select a group, and click **Manage people**.

okta Search... svkyt@informati... ife-ppop

← Back to Groups

**Admin**  
Admin Group

[Manage People](#) [Manage Apps](#) [Manage Directories](#) [Delete Group](#)

People Apps Directories

Search Show 60

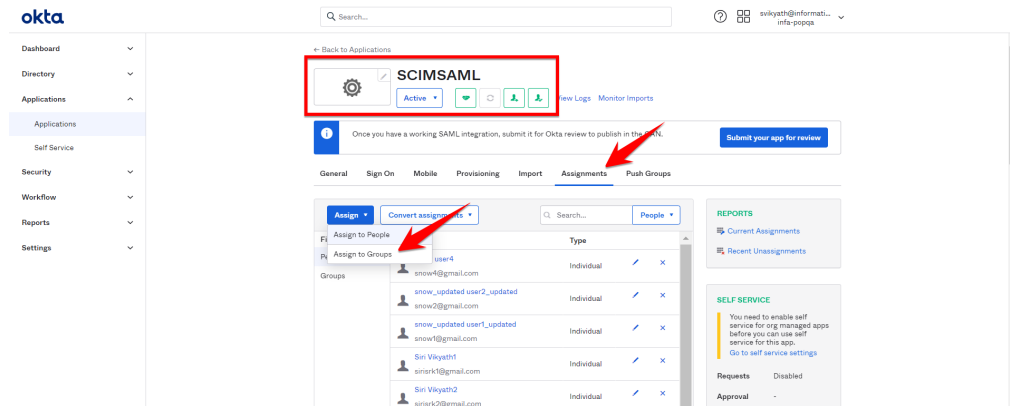
Person & Username	Status
admin user adminuser@informatica.com	Staged

Showing 1 - 1 of 1 [First](#) [Previous](#) [1](#) [Next](#) [Last](#)

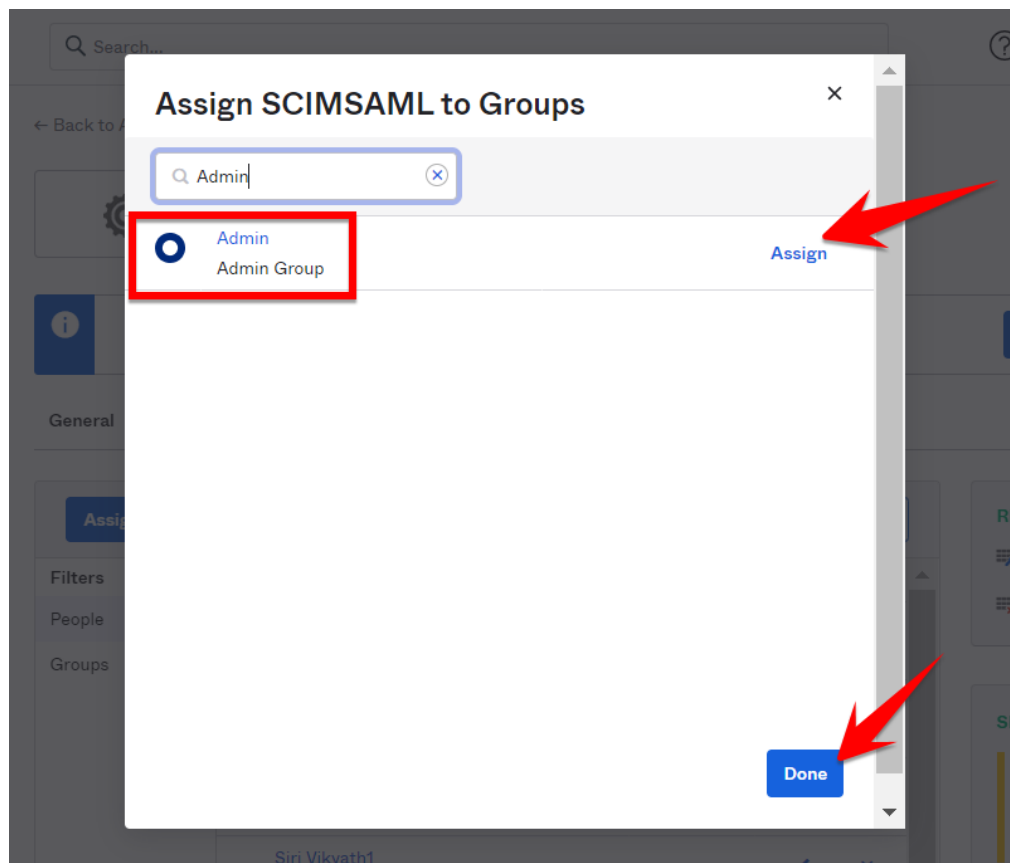
**Group Members**  
People and apps can be members of a group. People are automatically assigned any apps that are members of a group.  
Use [Manage People](#) to add and remove people from this group. Use [Add Apps](#) and [Remove Apps](#) to do the equivalent for apps.  
How do I edit the group name and description?  
Hover your mouse over the group name or description to edit them inline.

- b. Assign people to the group and click **Done** when finished.

- c. Repeat steps a and b for all groups that you need to provision users for.
3. When the users are created and are part of a group, assign the app to the groups:
  - a. Open the provisioning app that you created.
  - b. On the **Assignments** tab, select **Assign > Assign to Groups**.



- c. Select the group you want to assign, click **Assign**, and then click **Done**.



- d. Optionally, enter group attributes such as **Preferred language**, **Locale**, and **Time zone**.

## Assign SCIMSAML to Groups ×

**i** Extra info is needed to assign this app to a group.  
The attributes below will apply to all people assigned to this group.

Preferred language

Locale

Time zone

User type

Cost center

Organization

Division

Department

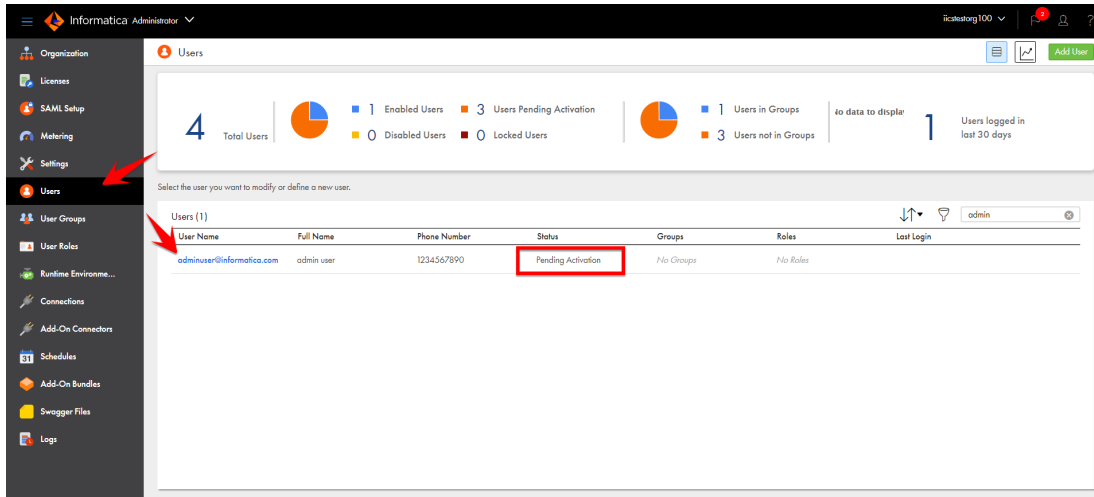
**Save and Go Back** **Cancel and Go Back**

These attributes will be assigned to all users in the group.

**Note:** The attributes that appear on this page vary based on the attribute mappings configured in the profile editor.

- e. Click **Save and Go Back**.
- f. Repeat steps c through e for all groups that you want to provision users for.
- g. Click **Done**.

After a group is assigned to the provisioning app, all users in the group are immediately provisioned in Informatica Intelligent Cloud Services. You can view users on the **Users** page in Administrator.



Users will be in the Pending Activation state until they first sign on to Informatica Intelligent Cloud Services. Users are editable while in the Pending Activation state, but once they sign on and the status changes to Enabled, the user details become read-only. Any changes you make to the user details will be overwritten the first time the user signs on to Informatica Intelligent Cloud Services.

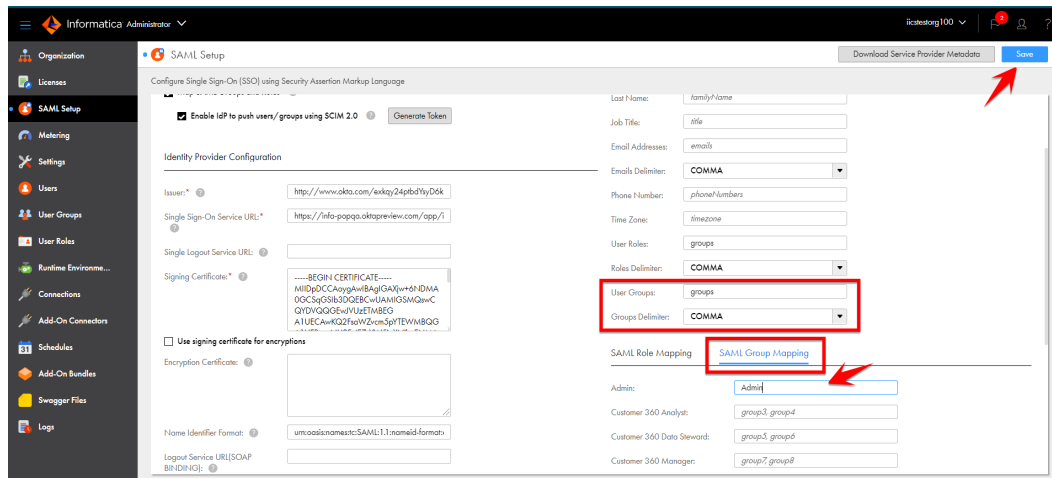
**Note:** At this point, the users have no groups assigned. If a user has no groups or roles assigned in Informatica Intelligent Cloud Services, the user cannot sign on. You must map the Okta groups to Informatica Intelligent Cloud Services roles and push the Okta groups to Informatica Intelligent Cloud Services so that the users get their group and role assignments.

## Step 6. Map Okta groups to Informatica Intelligent Cloud Services roles

Map Okta groups to Informatica Intelligent Cloud Services roles to ensure that SAML users have the appropriate levels of access to Informatica Intelligent Cloud Services assets. Users will be assigned the Informatica Intelligent Cloud Services roles that correspond to the mapped Okta groups.

1. In Administrator, open the **SAML Setup** page.

2. In the SAML Attribute area, configure the **User Groups** and **Groups Delimiter** fields.



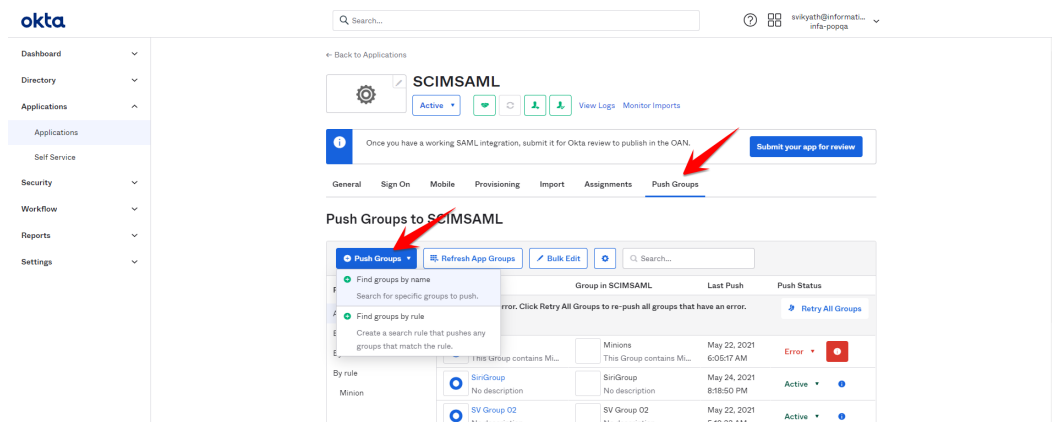
Property	Description
User Groups	SAML attribute used to pass the assigned user groups.
Groups Delimiter	Delimiter to separate the groups if multiple groups are passed.

3. On the **SAML Group Mapping** tab, map the Okta groups to Informatica Intelligent Cloud Services roles.
4. Click **Save**.

## Step 7. Push Okta groups to Informatica Intelligent Cloud Services

For successful authorization, each user must have at least one Informatica Intelligent Cloud Services role. Push Okta groups to Informatica Intelligent Cloud Services so that users get their role assignments. Users will be assigned the roles that correspond to the SAML groups on the **SAML Setup** page in Administrator.

1. In Okta, open the provisioning app that you created.
2. On the **Push Groups** tab, click **Push Groups**, and choose to push groups by name or by rule.



Pushing groups by name pushes the groups one at a time. Pushing groups by rule pushes multiple groups at once according to a rule.

To push groups by name, select **Find groups by name**, find and select the group, and click **Save**.

General Sign On Mobile Provisioning Import Assignments **Push Groups**

### Push Groups to SCIMSAML

Close

Pushed Groups

All

Errors

**By name**

By rule

Minion

Push groups by name

To sync group memberships from Okta to SCIMSAML, choose a group in Okta and a group in the app.

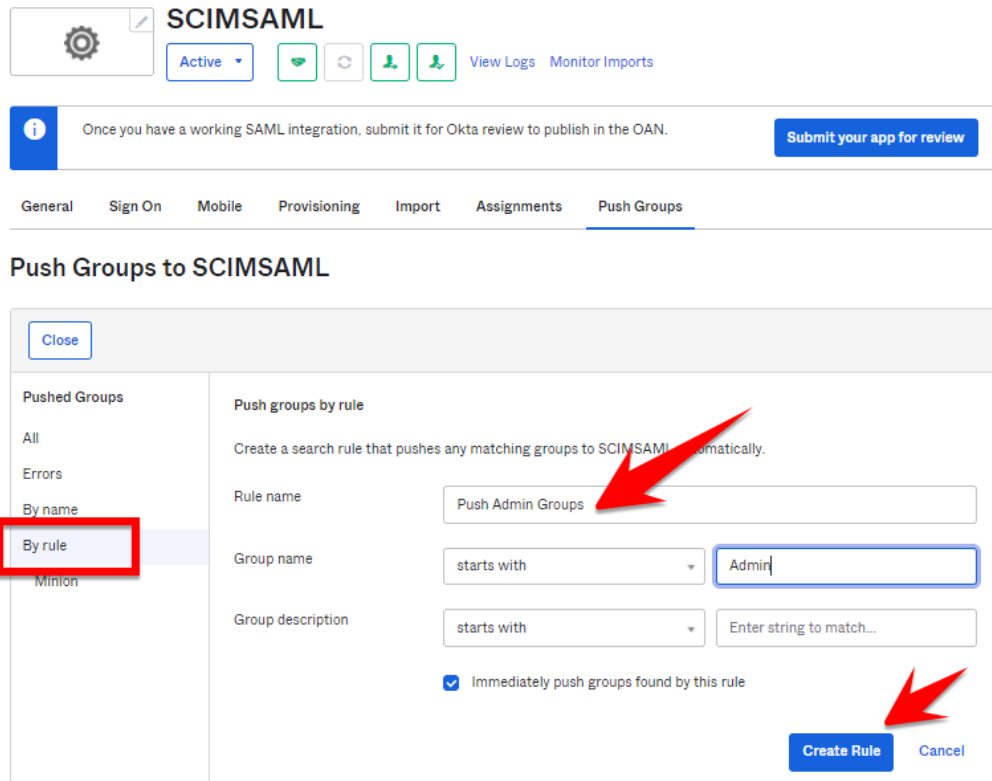
Admin

Push group memberships immediately

Group	Match result & push action
<input checked="" type="radio"/> Admin	No Match found <a href="#">Create Group</a>
	Admin

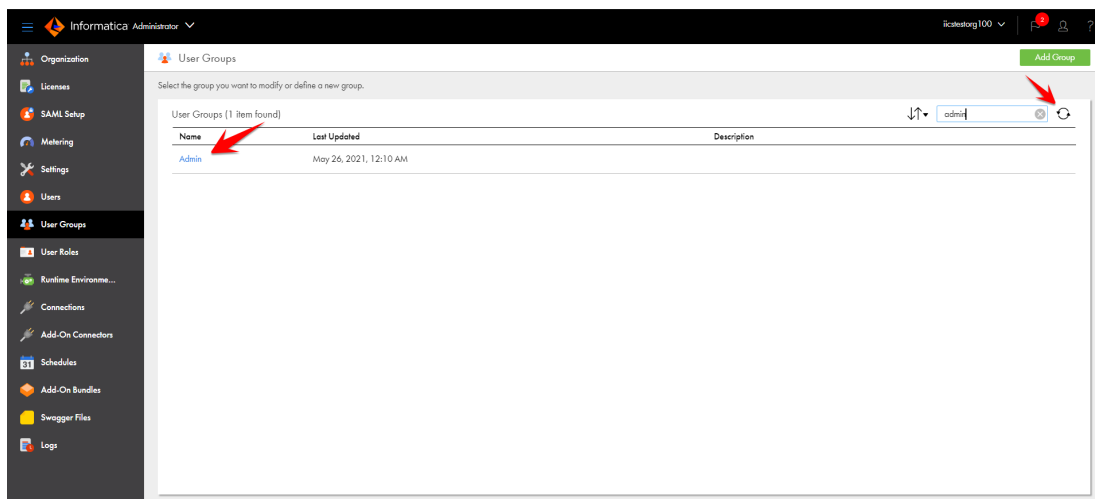
Save Save & Add Another

To push groups by rule, select **Find groups by rule**, create the rule, select **Immediately push groups found by this rule**, and click **Create Rule**.



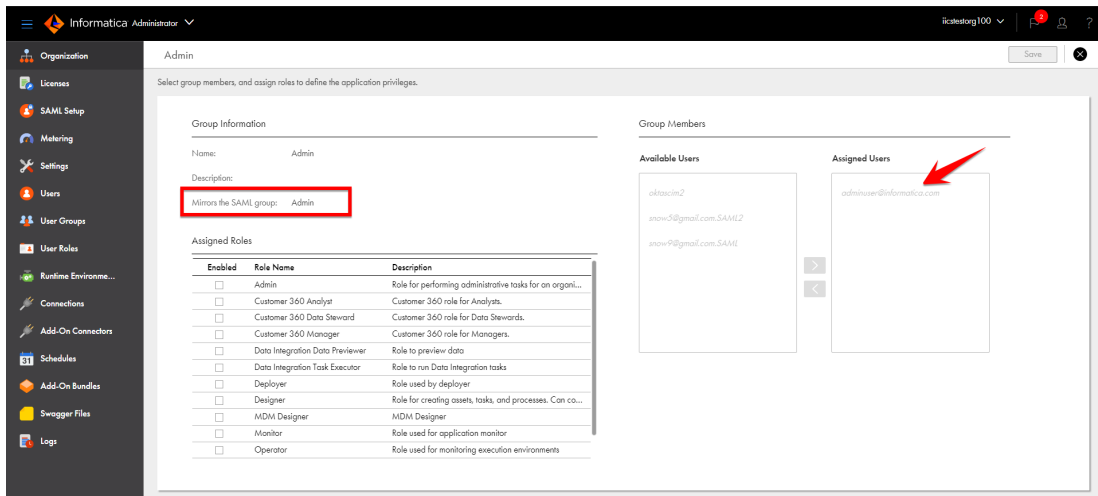
3. Verify that the push status for the groups you pushed is **Active**.

In Informatica Intelligent Cloud Services Administrator, you can see the groups on the **User Groups** page. You might have to refresh the page to see the groups.

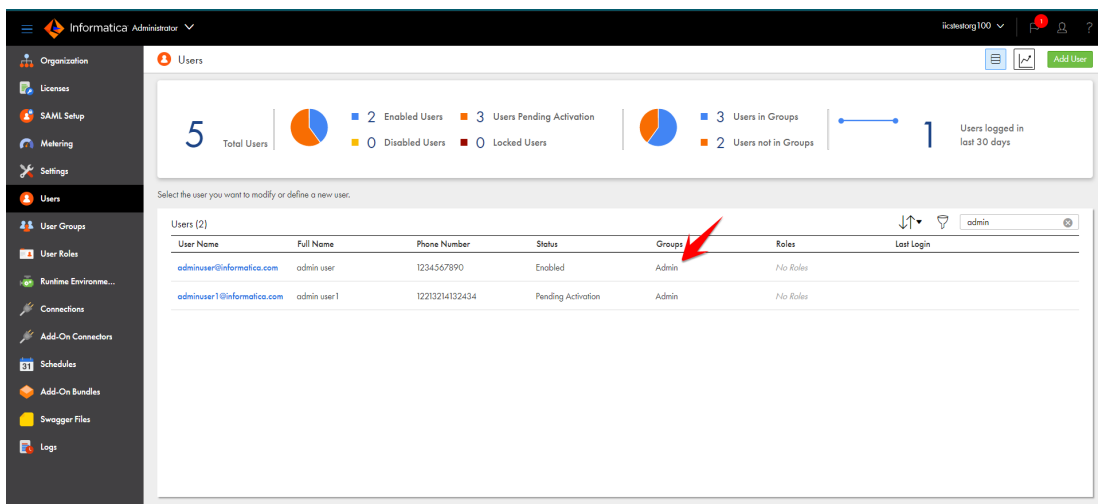




The SAML groups are all read-only. If you open the group, the **Mirrors the SAML group** field lists the mapped SAML group.



If you open the **Users** page, you can see that the Okta SAML users are now mapped to the new SAML groups.



If the group has no roles assigned at this point, go back and map the SAML groups to Informatica Intelligent Cloud Services roles on the **SAML Setup** page, or the users in the group will not be able to sign on to Informatica Intelligent Cloud Services.

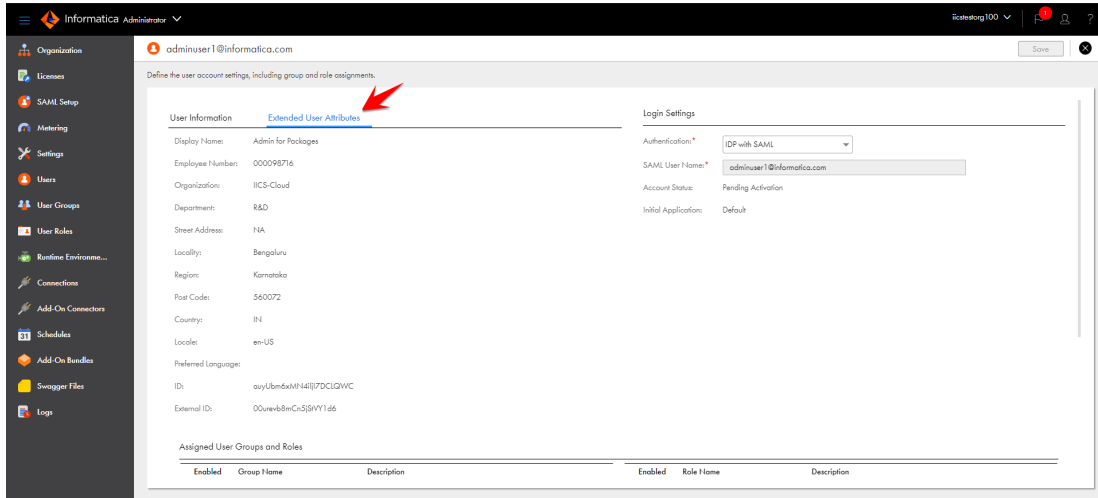
If the group has roles assigned, group members can sign on to Informatica Intelligent Cloud Services.

## Signing on to Informatica Intelligent Cloud Services as a provisioned user

After users and groups are pushed to Informatica Intelligent Cloud Services and the Okta groups have been mapped to Informatica Intelligent Cloud Services roles, provisioned users can sign on to Informatica Intelligent Cloud Services.

1. In Administrator, open the **Users** page and select the user.
2. In the Login Settings area of the user details page, copy the SAML username.
3. Sign in to Okta using this username and enter the password.
4. If this is the first time you are signing on, enter the recovery question and answer and click **Create My Account**.

After the user signs on to Informatica Intelligent Cloud Services, the user details page for that user shows the groups that the user is a member of and that at least one role is configured for the user. The extended user attributes are also visible.



## Guidelines for working with users

Consider the following guidelines when you work with users:

- The user attributes "username" and "email" are required. If these attributes are not provided, provisioning of the user will fail.
- User email addresses must be in the format: <local part>@<domain>, for example, jsmith@mycompany.com.
- In Informatica Intelligent Cloud Services, user names are unique to each user. Therefore, if you edit a user name in Okta after provisioning, Informatica Intelligent Cloud Services creates two users: one with the old user name and one with the new user name.

If you need to edit a user name after provisioning, delete the user in Okta, and then re-create the user with the new name.

- During provisioning, the user attribute "title" is truncated at 100 characters.
- User phone numbers must contain 10-25 characters. They can contain only numbers, spaces, parentheses, hyphens, periods, and a plus sign as the first character.
- If you suspend a user in Okta, the user's status will still be displayed as Pending Activation or Enabled in Informatica Intelligent Cloud Services, but the user will not be able to sign on to Informatica Intelligent Cloud Services.
- If you delete a user in Okta, the user will be disabled but not deleted in Informatica Intelligent Cloud Services. Disabled users cannot sign on to Informatica Intelligent Cloud Services.
- If you remove a user from the provisioning app after users have been pushed and then add the user back to the app, the user's state in Informatica Intelligent Cloud Services will be Enabled instead of Pending Activation.

## Guidelines for working with groups

Consider the following guidelines when you work with groups:

- If you rename an Okta group that has been pushed to Informatica Intelligent Cloud Services, ensure that you update the group name in the group mapping on the **SAML Setup** page. If you do not update the group mapping, users might not be able to sign on to Informatica Intelligent Cloud Services or might lose access to assets.
- If you unlink and delete an Okta group that is mapped on the **SAML Setup** page and has been pushed to Informatica Intelligent Cloud Services, the next group push fails.
- Pushing a group from Okta fails when you switch from using SAML for authentication and authorization to using SAML for authentication only, delete an Okta group that was pushed to Informatica Intelligent Cloud Services, and then switch back to using SAML for authentication and authorization.

## Author

**Siri Vikyath**  
**Senior QA Engineer**