



Setting up SCIM with Okta

[©] Copyright Informatica LLC 2021, 2024. Informatica, the Informatica logo, and Informatica Cloud Data Integration are trademarks or registered trademarks of Informatica LLC in the United States and many jurisdictions throughout the world. A current list of Informatica trademarks is available on the web at https://www.informatica.com/trademarks.html

Abstract

Informatica Intelligent Cloud Services[™] 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 November 2024

Table of Contents

Overview

Informatica Intelligent Cloud Services[™] 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**.

okta	Q Search	Svikyath@informati vinfa-popqa
Dashboard ~		
Directory ~	III Applications	Help
Applications ^	Create App Integration Browse App Catalog Assign Users to App More	
Applications		
Self Service	Q. Search	
Security ~	STATUS Demo_IICS	o - •
Workflow ~	ACTIVE 18	
Reports ~		U .
Settings ~	Csdev_Local_mma	o - *
	IICS Perf	o - •
	IICS_Perf_03	o - *

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

Create a new app integration	×
Sign-on 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

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

okta		Q Search		Svikyath@informati infa-popqa
ashboard	~			
rectory	~	#4 Create SAML Integra	tion	
plications	~	1 General Settings	2 Configure SAML	6 Feedback
urity	~			
orkflow	~	1 General Settings		
eports	~	App name	SAML_Siri	
ettings	~	App logo (optional)		
			â	
			~~~	
		App visibility	Do not display application icon to users	
			Do not display application icon in the Okta Mobile a	app
		Cancel		Next

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

okta		Q Search			⑦ □□ svikyath@informati ~ infa-popqa	
Dashboard Directory	~ ~	<b>¤</b> Create SAML Integr	ation			<u>^</u>
Applications	~	1 General Settings	2 Configure SAML		3 Feedback	
Security	~					- 1
Workflow	~	A SAML Settings			What does this form do?	- 1
Reports	×	General			This form generates the XML needed	
Settings	~	Single sign on URL	https://dm-us.informaticacloud.com/ide	ntity-service/acs/	for the app's SAML request.	
			Use this for Recipient URL and Destination	ation URL	needs?	
			Allow this app to request other SSO U	JRLs	The app you're trying to integrate with should have its own documentation on	
		Audience URI (SP Entity ID)	https://12a3b4cdef5gh67ijklm8n.dm-us.	informaticacloud.	using SAML. You'll need to find that doc, and it should outline what	
		Default RelayState 🕘			information you need to specify in this form.	
			If no value is set, a blank RelayState is sent	it	Okta Certificate	
		Name ID format	Unspecified *		Import the Okta certificate to your	-

Setting	Value
Single sign on URL	<pre><iics base="" url="">/identity-service/acs/<organization id=""> For example, https://dm-us.informaticacloud.com/identity- service/acs/12a3b4cdef5gh67ijklm8n</organization></iics></pre>
Audience URI (SP Entity ID)	<pre>https://<organization id="">.<hostname> For example, https://l2a3b4cdef5gh67ijklm8n.dm-us.informaticacloud.com</hostname></organization></pre>

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

6. 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 🔹	.*
Add Another			

Configure the following statement:

- Name: groups
- Name format: Unspecified
- Value: Matches regex .*
- 7. Optionally, configure other attributes such as firstName and lastName.
- 8. Click Next.
- 9. 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.

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 3 rd party applicat Application username is determined by the user profile mapping. Configure profile mapping	ion.
SAML 2.0	
Default Relay State	
<ul> <li>SAML 2.0 is not configured until you complete the setup instructions.</li> <li>View Setup Instructions</li> <li>Identity Provider metadata is available if this application supports dynamic configured</li> </ul>	guration.

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.

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

🔶 Informatica: Ad	ministrator 🗸		Informatica ~ P & ?
Organization	₽ _® SAML Setup		Download Service Provider Metadata Save
Licenses	Configure Single Sign-On (SSO) using Security Assertion Markup Language		
A SAML Setup			
A Metering	SSO Configuration	SAML Attribute N	Apping
Settings			
🗂 Users	Use Identity Provider File: Drop file here Choose File	U Oser mendiy SAMIL a	aking the second s
💍 User Groups	Disable auto provisioning of users	First Name:	givenreame
E User Roles	Map SAME Groups and Koles	Last Name:	familyName
G Runtime Environ			
Serverless Enviro	Identity Provider Configuration	Job Title:	title
Or Connections	Issuer: • 🖗	Email Addresses:	emails
🖉 Add-On Connecto	Single Sign-On Service URL: •	Emails Delimiter:	сомма
Schedules			
Data Services Re	Single Logout Service URL:* @	Phone Number:	phoneNumbers
Add-On Bundles	Signing Certificate: * 🖗	Time Zone:	timezone
Swagger Files			
E Logs		User Roles:	
Advanced Clusters		Polas Delimitar	COMMA
File Servers	Use signing certificate for encryptions		
	Encryption Certificate:	User Groups:	
		Groups Delimiter:	сомма

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

nfigure Single Sign-On (SSO) using Security Assertion Markup Language	
ingle onge orge of (oco) boing occorry noor ion manap zangoogo	
SSO Configuration	SAML Attribute Mapp
Use Identity Provider File: Drop file here Choose File	User friendly SAM
Map SAML Groups and Roles	First Name:
Enable IdP to push users/groups using SCIM 2.0     Manage Token	Last Name:

**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 Manage Token.

• 🎗 SAML Setup				Download Service Provider Mete
Configure Single Sign-On (SSO) using Security Assertion Markup Language				
SSO Configuration		SAML Attribute Mappir	g Additional Attributes	
Use identity Provider File: Drop file here Choose File				
Disable auto provisioning of users		User friendly SAML a	attribute names 🛛 😡	
Map SAML Groups and Roles	SCIM Tokens			× }
Enable IdP to push users/groups using SCIM 2.0 Manage Token	agust Talan	Dural and Data	General	te Token
Identity Provider Configuration			status	
Issuer: * 🖗		<ul> <li>Nothing to dis</li> </ul>	play.	
Single Sign-On Service URL: *				Close
Single Logout Service URL:* •		Time Zone:	timezone	
Signing Certificate: * 0	monterman	······································	man man	

The **SCIM Tokens** dialog box displays the SCIM tokens that have been created for your organization along with the expiration date and status of each token. If two tokens are listed, you'll need to delete one before you can generate a new token.

6. 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 180 days from the time of generation. When the token expires, you'll need to generate a new one, even for an existing connection.

**Tip:** You can create two tokens on different days so that one token is always available. For example, you might want to generate a token on one day and a second token 90 days later. Informatica Intelligent Cloud Services notifies you when a token is about to expire.

7. 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.

okta		Q Search		Svikyath@informati infa-popqa
Dashboard	~	Once you have a working	g SAML integration, submit it for Okta review to publish in the OAN	Submit your app for review
Directory	~			
Applications	^	General Sign On Mobil	le Provisioning Import Assignments	
Applications				General Settings
Self Service		App Settings		Edit All fields are required unless marked optional. Some fields may no longer b
Security	~	Application label	SAML_Siri	editable.
Workflow	~	Application visibility	Do not display application icon to users	On-Premises Provisioning
Reports	~		<ul> <li>Do not display application icon in the Okta Mobile app</li> </ul>	On-premises provisioning allows you provision users to your on-premises
Settings	~	Provisioning	O None	applications.
			On-Premises Provisioning     SCIM	
		Auto-launch	Auto-launch the app when user signs into Okta.	
		Application notes for end users		
		Application notes for admin		
		Application notes for adminis		
		CAMI Continue		
		SAML Settings		Edit

ettings		
tegration		
	SCIM Connection	Cancel
	SCIM version	2.0
	SCIM connector base URL	https://dm-us.infa.com/scim-service
	Unique identifier field for users	email
	Supported provisioning actions	<ul> <li>Import New Users and Profile Updates</li> <li>Push New Users</li> <li>Push Profile Updates</li> <li>Push Groups</li> </ul>
	Authentication Mode	HTTP Header *
	HTTP Header	
	Authorization	Bearer ·····
		✓ Test Connector Configuration
		Save Cancel

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

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 Push New Users, Push Profile Updates, and Push Groups.
Authentication Mode	Select HTTP Header.
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**.

Settings									
То Арр		okta	->	Ö					
To Okta				*					
Integration	Provisioning to App				Cancel				
	Create Users				Enable				
	Creates or links a user in SAM	ML_Siri when assigning	g the app to a u	ser in Okta.					
	The default username used to	o create accounts is se	t to <b>Okta usern</b>	name.					
	Update User Attributes								
	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								
	Deactivates a user's SAML_S can be reactivated if the app	Siri account when it is u is reassigned to a user	inassigned in O in Okta.	kta or their Okta acc	ount is deactivated. Accounts				
	Sync Password				Enable				
	Creates a SAML_Siri passwo	ord for each assigned us	ser 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.

SAML_Siri User			🖍 Edit	Ó	F	
Display name	SAML_Si	ri User		SAML_	Siri	
Description						
Variable name 🛛 🔞	infapopq	a_samlsiri_1				
ttributes + Add Attribute	/ Mappings	Veriekte News	Data form	Adduibuda Tura		
	Display Name	Variable Name	Data type	Attribute Type		
Paga	Username	userName	string	Base	0	×
Custom	Given name	givenName	string	Custom	1	×
	Family name	familyName	string	Custom	1	×
	Middle name	middleName	string	Custom	1	×
	Honorific prefix	honorificPrefix	string	Custom	1	×
	Honorific suffix	honorificSuffix	string	Custom	1	×

- 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
  - 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 to Okta User Okta	User to SAML_Siri		
SAML_Siri User Profile appuser		okta User User F user	Profile
ername is set by SAML_Siri		login	string
appuser.givenName	* 0 <del>)</del> *	firstName	string
appuser.familyName	* <b>0</b> + *	lastName	string
Choose an attribute or enter an expression	• -/-}>	middleName	string
Choose an attribute or enter an expression	• -/-)>	honorificPrefix	string
Choose an attribute or enter an expression	• -/-)>	honorificSuffix	string
appuser.email	v 0+ •	email	email
appuser.title	• O> •	title	string
appuser.displayName	* O+ *	displayName	string
Choose an attribute or enter an expression	• -/->	nickName	string
Choose an attribute or enter an expression	• -/->	profileUrl	uri
Choose an attribute or enter an expression	• -/-)> •	secondEmail	email
Choose an attribute or enter an expression	• -/-)>	mobilePhone	string
appuser.primaryPhone	• O> •	primaryPhone	string
appuser.streetAddress	• 0+ •	streetAddress	string
appuser.locality	v 0+ •	city	string

appuser.region	٣	0→ *	state	string
appuser.postalCode	¥	• •	zipCode	string
appuser.country	٣	• •	countryCode	country code
Choose an attribute or enter an expression	٠	-/->	postalAddress	string
appuser.preferredLanguage	٠	• •	preferredLanguage	language code
appuser.locale	٠	• •	locale	locale
appuser.timezone	¥	0+ T	timezone	timezone
Choose an attribute or enter an expression	¥	-/-> •	userType	string
appuser.employeeNumber	¥	• •	employeeNumber	string
Choose an attribute or enter an expression	٠	-/->	costCenter	string
appuser.organization	¥	• •	organization	string
Choose an attribute or enter an expression	٠	-/->	division	string
appuser.department	*	• •	department	string
Choose an attribute or enter an expression	٠	-/->	managerId	string
Choose an attribute or enter an expression	٠	-/->	manager	string

Preview Enter an Okta user to preview their mappi

Save Mappings

Cancel

SAML_Siri to Okta User Okta Us	er to SAML_Siri		
okta User User Profile user		SAML_Siri User	r Profile
ername is set by SAML_Siri		userName	string
user.firstName	• • •	givenName	string
user.lastName	· - ·	familyName	string
Choose an attribute or enter an expression	• -/-> •	middleName	string
Choose an attribute or enter an expression	• -/-)> •	honorificPrefix	string
Choose an attribute or enter an expression	• -/-> •	honorificSuffix	string
user.email	• - •	email	email
Choose an attribute or enter an expression	• -/	emailType	email
user.title	· → ·	title	string
user.displayName	· → ·	displayName	string
Choose an attribute or enter an expression	• -/-> •	nickName	string
Choose an attribute or enter an expression	• -/-)> •	profileUrl	uri
user.primaryPhone	• •	primaryPhone	string
Choose an attribute or enter an expression	• -/-} •	primaryPhoneType	string
Choose an attribute or enter an expression	• -/-)> •	addressType	string
user.streetAddress	· → ·	streetAddress	string

		locality	string
· → ·		region	string
· → ·		postalCode	string
· → ·		country	country code
· → ·		preferredLanguage	language code
· → ·		locale	locale
· → ·		timezone	string
• -/->	•	userType	string
· → ·		employeeNumber	string
· → ·		organization	string
· → ·		department	string
		$\begin{array}{cccccccccccccccccccccccccccccccccccc$	Image: state

-- - --

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

+ Add Attribute	Mappings					
ILTERS	Display Name	Variable Name	Data type	Attribute Type		
I	Username	userName	string	Base	0	×
istom	Given name	givenName	string	Custom	1	×
	Family name	familyName	string	Custom	1	×
	Middle name	middleName	string	Custom	1	×
	Honorific prefix	honorificPrefix	string	Custom	1	×
	Honorific suffix	honorificSuffix	string	Custom	1	×
	Primary email	email	string	Custom	1	×
	Primary email type	emailType	string	Custom	1	×
	Title	title	string	Custom	1	×
	Display name	displayName	string	Custom	1	×
	Nickname	nickName	string	Custom	1	×

Attributes							
+ Add Attribute	✓ Mappings						
FILTERS	Display Name	Variable Name	Data type	Attribute Type			
AI	Username	userName	string	Base	• ×		
Base Custom	Given name	givenName	string	Custom	× ×		
	Family name	familyName	string	Custom	× ×		
	Primary email	ema i l	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	1 ×		
	Postal Code	postalCode	string	Custom	/ ×		
	Country code	country	string	Custom	× ×		
	Preferred language	preferredLanguage	string	Custom	1 ×		
	Locale	locale	string	Custom	× ×		
	Time zone	Limezone	string	Custom	× ×		
	Employee number	employeeNumber	string	Custom	× ×		
	Organization	organization	string	Custom	× ×		
	Department	department.	string	Custom	× ×		

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

### **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**.

okta		Q Search				0 == *	ikyath@informati , infa-popqa
Dashboard	×		/				
Directory	^	1 People					Help
People		Add person	Rese	t passwords	More actions *		
Groups		Q. Search					
Profile Editor		-		Person & username	Primary email	Status	
Profile Sources		Onboarding	67	RajUser 01 raj@gmail.com	raj@gmail.com	Password	expired
Applications	Ŷ	Staged	6	minion 1 minionf@gmail.com	minion1@gmail.com	Active	
Security	~	Pending user action	1	minion 10 minion10@gmail.com	minion10@gmail.com	Active	
Workflow	~	Active	55	minion 11 minion11@gmail.com	minion11@gmail.com	Active	
Reports	Ý	Password reset	0	minion 12 minion12@gmail.com	minion12@gmail.com	Active	
Settings	Ý	Inactive	2	minion 13 minion13@gmail.com	minion13@gmail.com	Active	
		Suspended	3	minion 14 minion14@gmail.com	minion14@gmail.com	Active	
		Deactrated	2	minion 15	minion15@gmail.com	Active	

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

Add Person	
User type 🔞	User 🔹
First name	admin
Last name	user
Username	adminuser@informatica.com
Primary email	adminuser@informatica.com
Secondary email (optional)	
Groups (optional)	O Admin ×
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			Q Search			O svikyath@informati infa-popqa
Dashboard	~	*	Back to Groups			
Directory	^		O Admin			
People			Admin Group			
Groups		۲ آ	1 Manage People   III Manage A	pps Manage Directories	A. Delete Group	
Profile Editor		L. L				
Directory Integrations			People Apps Directories			
Profile Sources					Show 50 ×	Group Members
Applications	ř		Descen & Hannama			People and apps can be members of a group. People are automatically
iecurity	~		admin user		Staged	assigned any apps that are members of a group.
orkflow	~		adminuser@informatica.com			Use Manage People to add and remove
leports	Ý		Showing 1 - 1 of 1	First	revious 1 Next Last	and Remove Apps to do the equivalent
attings	~					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.

okta	
ashboard	~
Directory	~
Applications	^
Applications	
Self Service	
curity	Ý
N	Ý
	Ý
ţs.	Ý

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

Q Sear	rch	_	?
← Back to /	Assign SCIMSAML to Groups	×	
	Q Admin 🛞		
t	Admin Admin Group	Assign	
0			
General			
Assis			
Filters			-
People			
Groups			
		Done	
	Siri Vikyath1		

Extra info is need	ed to assign this app to a group.
The attributes bel	ow will apply to all people assigned to this group.
Preferred language	1
Locale	
Time zone	
Jser type	
Cost center	
Organization	
Division	
Department	

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

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.

= 🔶 Informatica 🖂	ninistrator 🗸	iicateolog 100 🗸   🔔 g. ?
Crganization	• 🚯 SAML Setup	Download Service Provider Metadata
🛃 Licenses	Configure Single Sign-On (SSO) using Security Assertion Markup Language	1
SAML Setup	Enable IdP to push users/groups using SCIM 2.0  Generate Taken	Last Name: ItamilyName
n Metering		Job life: new
Y Settings	Identity Provider Configuration	Email Addresses: emails
<b>0</b> 11		Emails Delimiter: COMMA 🔻
Users	Issuer:*	Phone Number: phoneNumbers
4 User Groups	Single Sign-On Service URL:* https://infa-popqa.oktapreview.com/app/i	Time Zone: timezone
🔼 User Roles	Single Lagout Service URL: 🔘	User Roles: groups
👼 Runtime Environme	Signing Certificate: *	Roles Delimiter: COMMA 🔻
🖋 Connections	MIIDpDCCAoygAwlBAgIGAXjw+6NDMA 0GCSqGSib3DQEBCwUAMIGSMQswC	User Groups: groups
📁 Add-On Connectors	QYDVQQGEwJVUzETMBEG A I UECAwKQZFxxVVZxm5pYTEV/MBQG	Groups Delimiter: COMMA 🔹
Schedules	Use signing certificate for encryptions	SAMI Role Manning SAMI Group Manning
🔶 Add-On Bundles	Encryption Certificate: 🔘	
C. Summer Elec		Admin: Admin
- Swogger hies		Customer 360 Analyst: group3, group4
🛃 logs	Name Identifier Format:	Customer 360 Data Steward: group <i>5</i> , group <i>6</i>
	Logout Service URL(SOAP BINDING): 🚳	Customer 360 Manoger: group? group?

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.

okta		Q Search	Svikyath@informati
Dashboard	~	e- Back to Applications	
Directory	~		
Applications	^	Active  Control Active  Contro	
Applications		Once you have a working SAML integration, submit it for Okta review to publish in the OA	N. Bubmit your and far mainer
Self Service			Sability your approvinew
ecurity	~	General Sign On Mobile Provisioning Import Assignments Push Gr	ups
rkflow	~	Push Groups to SEMSAML	
orts	~		
	~	O Push Groups ▼ III, Refresh App Groups ✓ Bulk Edit O Q Search	
		Find groups by name     Group in SCIMSAML      Search for specific groups to push.	Last Push Push Status
		Find groups by rule	hat have an error. 👂 Retry All Groups
		E Create a search rule that pushes any groups that match the rule.	May 22, 2021
		E This Group contains Mi This Group contains Mi	i 6:05:17 AM
		By rule SiriGroup SiriGroup No description No description	May 24, 2021 Active 🔹 🕚 8:18:50 PM
		SV Group 02 No description No description	May 22, 2021 Active • 0

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 Okto p SecureAn Admin Version Push group memberships immediately	/L, choose a group in Okta and a group in the app.
	Group	Match result & push action
	Admin	No Match found Create Group Admin
		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**.

¢,	) )	Active •	AML	r r	View Logs Moni	tor Imports		
•	Once you have a working SAML integration, submit it for Okta review to publish in the OAN.     Submit your app for review							
General	Sign On	Mobile	Provisioning	Import	Assignments	Push Groups		

#### Push Groups to SCIMSAML

Close		
Pushed Groups	Push groups by rule	
All	Create a search rule that p	ushes any matching groups to SCINSAML comatically.
Errors	Rule name	Push Admin Groups
By rule		
Minion	Group name	starts with • Admin
	Group description	starts with * Enter string to match
		Immediately push groups found by this rule
		- 
		Create Rule Cancel

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.

= 🔶 Informatica 🗛	dministrator 🗸			iicatestorg100 ∨   ⊨ <mark>2</mark> ቧ ?			
🔒 Organization	😵 User Groups	👔 User Groups					
🛃 Licenses	Select the group you want to m	odify or define a new group.					
🚺 SAML Setup	User Groups (1 item fo	und)		J∱• odmin ⊙			
👩 Metering	Name	Last Updated	Description				
🄀 Settings	Admin	May 26, 2021, 12:10 AM					
Users							
4 User Groups							
User Roles							
👼 Runtime Environme							
🖋 Connections							
🖋 Add-On Connectors							
31 Schedules							
🔶 Add-On Bundles							
Swagger Files							
🛃 Logs							

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

😑 🔶 Informatica 🗚	ministrator V						iicstest	org100 🗸 🚽	<mark>ے</mark> م	?
Crganization	Admin						S	ave	⊗	
🌄 Licenses	Select group members, a	nd assign roles to define the applicatio	n privileges.							
🚺 SAML Setup										
Metering	Group Inform	nation		_	Group Members					
NG A	Name:	Admin			Available Users		Assigned Users			
Joseffings	Description:									
Users	Mirrors the SA/	ML group: Admin			oktascim2		adminuser@informatica.com			
4 User Groups										
Liser Roles	Assigned Rol	es								
	Enabled	Role Name	Description	Ī		$\geq$				
Kuntime Environme		Admin	Role for performing administrative tasks for an organi							
🖋 Connections		Customer 360 Analyst	Customer 360 role for Analysts.							
4		Customer 360 Data Steward	Customer 360 role for Data Stewards.							
Add-On Connectors		Customer 360 Manager	Customer 360 role for Managers.							
Schedules		Data Integration Data Previewer	Role to preview data							
		Data Integration Task Executor	Role to run Data Integration tasks							
🔶 Add-On Bundles		Deployer	Role used by deployer							
		Designer	Role for creating assets, tasks, and processes. Can co							
Swagger Files		MDM Designer	MDM Designer							
🚮 Logs		Monitor	Role used for application monitor							
		Operator	Role used for monitoring execution environments							
										_

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

😑 🚸 Informatica Administrator 🗸 iistentorg)00 v   🗳 🖉 ?									
🛱 Organization	O Users								Add User
🌄 Licenses									
🚺 SAML Setup	_	•	2 Enabled Users 📕 3 Users	Pending Activation	• 3	Users in Groups		User langed in	
n Metering	5 Total Users	<b>·</b>	O Disabled Users 🔳 🔘 Locked	d Users	2	Users not in Groups		last 30 days	
🄀 Settings									
Users	Select the user you want to modify or	define a new user.							
4 User Groups	Users (2)						jt• 🖓	admin	۲
User Roles	User Name	Full Name	Phone Number	Status	Groups	Roles	Last Login		
	adminuser@informatica.com	admin user	1234567890	Enabled	Admin	No Roles			
Kunhime Environme	adminuser 1 @informatica.com	admin user 1	12213214132434	Pending Activation	Admin	No Roles			
🖋 Connections									_
🖋 Add-On Connectors									
Schedules									
🧼 Add-On Bundles									
Swagger Files									
🛃 Logs									

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.

😑 🚸 Informatica Administrator 🗸 🕅 Ticateology 100 v   🖓 g. ?										
Graganization	edminuser1@information	Save								
🌄 Licenses	Define the user account setting	Define the user account retirings, including group and role assignments.								
👩 SAML Setup			1							
👩 Metering	User Information	Extended User Attributes	Login Settings							
🄀 Settings	Display Name:	Admin for Packages	Authentication: IDP with SAML							
🙆 Users	Organization:	IICS-Cloud	SAMLUser Name: adminuser I @informatica.com							
4 User Groups	Department:	R&D	Initial Application: Default							
User Roles	Street Address:	NA								
👼 Runtime Environme	Locality:	Bengoluru								
🗯 Connections	Region:	Kamataka								
🗯 Add-On Connectors	Post Code:	560072								
31 Schedules	Country:	VI								
🔶 Add-On Bundles	Relevant Longonge									
🦲 Swagger Files	ID:	auyUbm6xMN4ilj(7DCLQWC								
🛃 logs	External ID:	00urevb8mCn5jStVY1d6								
	Assigned User Gr									

#### **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