



Okta SCIM

Integration Guide



Contents

Introduction.....	2
Okta Configuration	3
Provisioning.....	7
User Provisioning.....	7
Group Provisioning	10
Envi Configuration	12

Introduction

Envi supports **SCIM 2.0**, enabling user and group provisioning with different identity providers.

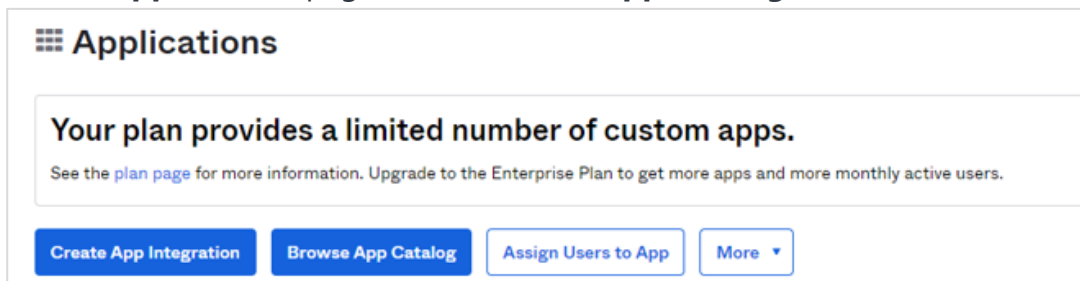
SCIM enables IT departments to automate provisioning and deprovisioning of accounts, which reduces manual redundant processes and increases security.

This step-by-step guide explains how to configure **Okta SCIM** connection with your **Envi** account.

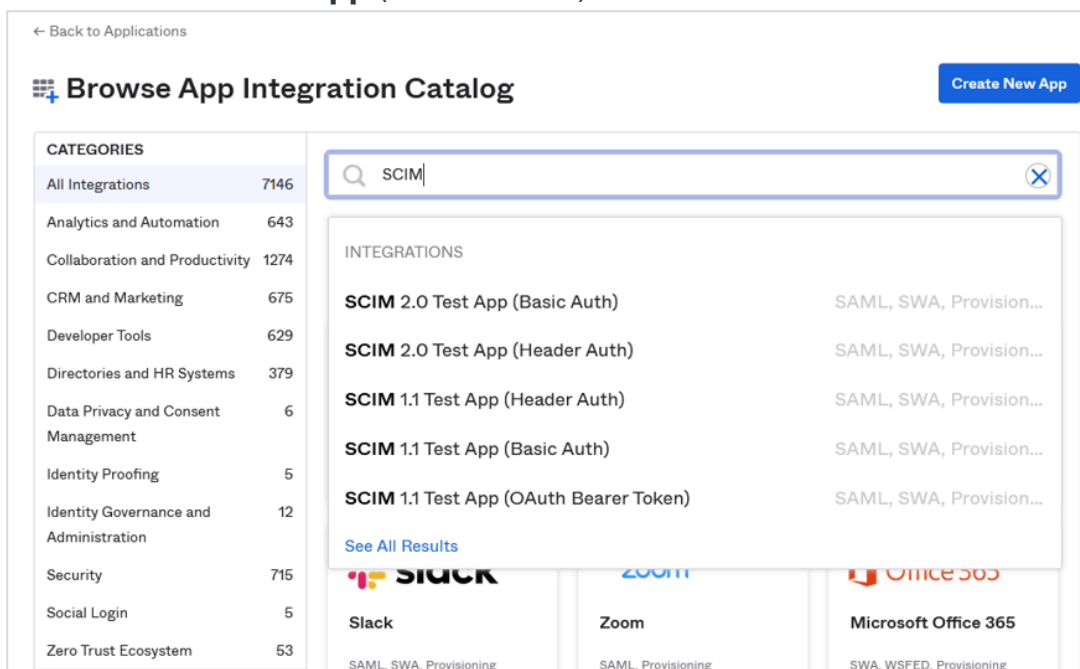
Okta Configuration

Perform the following steps to implement the **SCIM** provisioning with your **Envi** account.

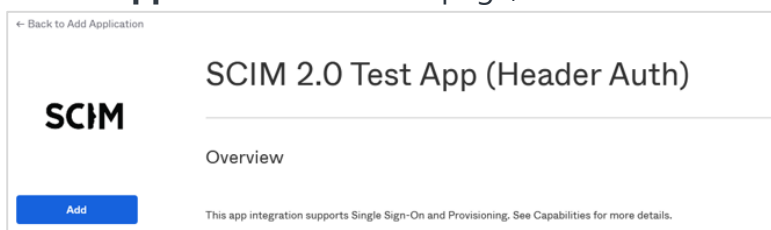
1. Sing in to the [Okta](#) site.
2. Select **Applications** > **Applications** from the site menu.
3. On the **Applications** page, select **Browse App Catalog**.



4. On the **Browse App Integration Catalog** page, type **SCIM** in the search box and select **SCIM 2.0 Test App (Header Auth)**.



5. On the **Application Overview** page, select **Add**.



6. On the **Add SCIM 2.0 Test App (Header Auth)** page, enter an **Application label** (name). Based on your needs, you can set other application configuration options. Then, select **Next**.

Note: To skip the **Sign-On options** page, select **Done** (leave all the default options unless you need to configure it according to your organization's rules).

7. Go to the **Provisioning** tab of the application details and select the **Configure API Integration** button.

8. To configure the **API** integration, perform the following steps:
 - a. Select the **Enable API integration** checkbox to make additional boxes appear.
 - b. In the **Base URL** box, enter the base URL of the **Envi SCIM** server + **/scim** (for example, <https://scim.envi.net/scim>).
 - c. In the **API Token** box, enter the **SCIM** token obtained from the **Envi** application (the [Envi Configuration](#) section, step 5) in the following format: **Bearer your token**.

- d. Select **Test API Credentials** which causes a test call from **Okta** to **Envi SCIM API** to make sure the entered information is correct.

← Back to Applications

SCIM 2.0 Test App (Header Auth)

Active

Once you have a working SCIM integration, submit it for Okta review to use in production and to publish in the OAN. [Submit your app for review](#)

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

Settings

Integration

☒ **Enable API integration**

Enter your SCIM 2.0 Test App (Header Auth) credentials to enable user import and provisioning features.

Base URL

API Token

[Test API Credentials](#)

[Save](#)

9. After a successful test connection, you will see the message:



10. Select **Save**.

11. After refreshing the page, you will see the new configuration options. In the **Settings** section, select **To App** and then **Edit**.

← Back to Applications

SCIM 2.0 Test App (Header Auth)

Active

Once you have a working SCIM integration, submit it for Okta review to use in production and to publish in the OAN. [Submit your app for review](#)

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

Settings

To App

To Okta

Integration

Provisioning to App

[Edit](#)

12. Select **Enable** in the following checkboxes: **Create Users**, **Update User Attributes**, and **Deactivate Users**. Leave **Sync Password** not selected. Then, select **Save**.

Settings
To App
To Okta
Integration

okta

→

SCIM

Provisioning to App

Cancel

Create Users

☒ Enable

Creates or links a user in SCIM 2.0 Test App (Header Auth) when assigning the app to a user in Okta.
The **default username** used to create accounts is set to **Okta username**.

Update User Attributes

☒ Enable

Okta updates a user's attributes in SCIM 2.0 Test App (Header Auth) when the app is assigned. Future attribute changes made to the Okta user profile will automatically overwrite the corresponding attribute value in SCIM 2.0 Test App (Header Auth).

Deactivate Users

☒ Enable

Deactivates a user's SCIM 2.0 Test App (Header Auth) 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

☐ Enable

Creates a SCIM 2.0 Test App (Header Auth) password for each assigned user and pushes it to SCIM 2.0 Test App (Header Auth).

Save

13. Move through the page to the **Attributes Mapping** section and remove all attributes, except for the following: **userName**, **givenName**, **familyName**, **email**, and **emailType**.

SCIM 2.0 Test App (Header Auth) Attribute Mappings

Select a(n) SCIM 2.0 Test App (Header Auth) attribute to set its value based on values stored in Okta.

Go to Profile Editor
Force Sync

Attribute	Attribute Type	Value	Apply on
Username userName	Personal	Configured in Sign On settings	
Given name givenName	Personal	user.firstName	Create and update <div>✎ ✕</div>
Family name familyName	Personal	user.lastName	Create and update <div>✎ ✕</div>
Primary email email	Personal	user.email	Create and update <div>✎ ✕</div>
Primary email type emailType	Personal	(user.email != null && user.email != "") ? 'work' : "	Create and update <div>✎ ✕</div>

Show Unmapped Attributes

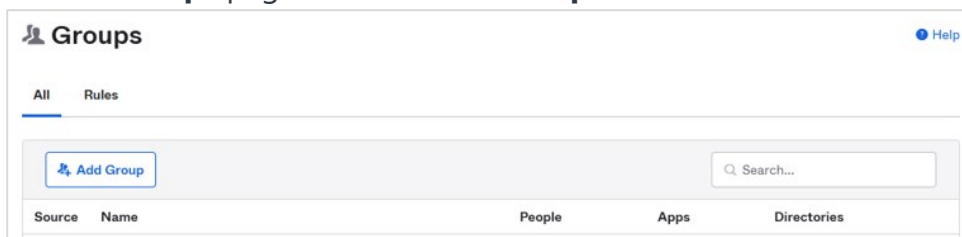
Your configuration will be saved automatically. At this point, it is ready for use.

Provisioning

In this section, you will learn how to provision new users and groups.

User Provisioning

1. To add a new member, go to **Directory > Groups** in the site menu.
2. On the **Groups** page, select **+Add Group**.



3. Enter the **Name** and **Description** of your group, then select **Add Group**.

Add Group

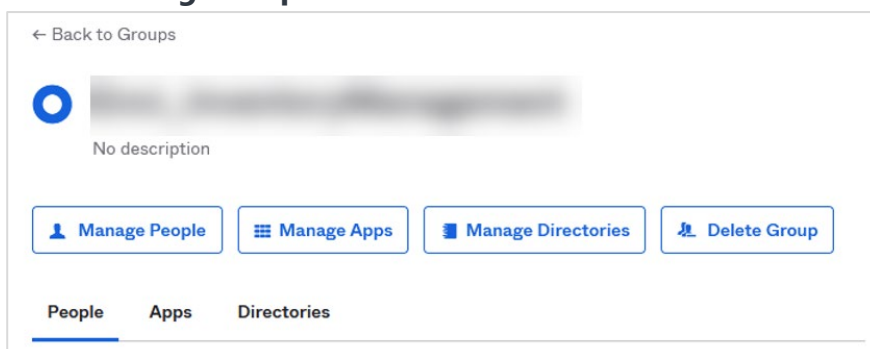
Add groups so you can quickly perform actions across large sets of people.

Name

Group Description

Add Group
Cancel

4. To assign the needed users to the group, go to the newly created group details and select **Manage People**.



5. Add needed users from the **Not Members** and **Members** lists, then select **Save**.

Note: Repeat the process of group creation and user assigning for all other users and groups that you want to provision.

Note: If you are going to use group provisioning from **Okta** to **Envi**, you need to create a separate group for each **Envi** role. According to the configurations, your group name should have the same prefix as **User Role Prefix** (Envi_) on the **SCIM Configuration** page (the [Envi Configuration](#) section).

If you are not going to use automatic user provisioning for groups, it is enough to have only one group, and you are free to set any name for it.

6. Go to the details of your application (select **Applications** > **Applications** in the menu and select your application from the list), and to the **Assignments** tab. Then select **Assign** and **Assign to Groups**.

- To add a group, select **Assign**, then select **Save** and **Go Back** to enable member provisioning for this group. When all needed groups are added, select **Done**.

Assign SCIM 2.0 Test App (Header Auth) to Groups

Search...

<input checked="" type="radio"/>	envi_managed	Assigned
<input type="radio"/>	envi_testing	Assign
<input type="radio"/>	Everyone All users in your organization	Assign

Done

- Assigned user groups will appear in the **Groups** section.

← Back to Applications

SCIM SCIM 2.0 Test App (Header Auth)

Active [Icons] View Logs Monitor Imports

Once you have a working SCIM integration, submit it for Okta review to use in production and to publish in the OAN. [Submit your app for review](#)

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

Assign Convert assignments Search... Groups

Filters: People, **Groups**

Priority	Assignment
1	[Group Name]

REPORTS: Current Assignments, Recent Unassignments

- To see users that are assigned due to the user group assignment, go to the **People** section.

← Back to Applications

SCIM SCIM 2.0 Test App (Header Auth)

Active [Icons] View Logs Monitor Imports

Once you have a working SCIM integration, submit it for Okta review to use in production and to publish in the OAN. [Submit your app for review](#)

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

Assign Convert assignments Search... People

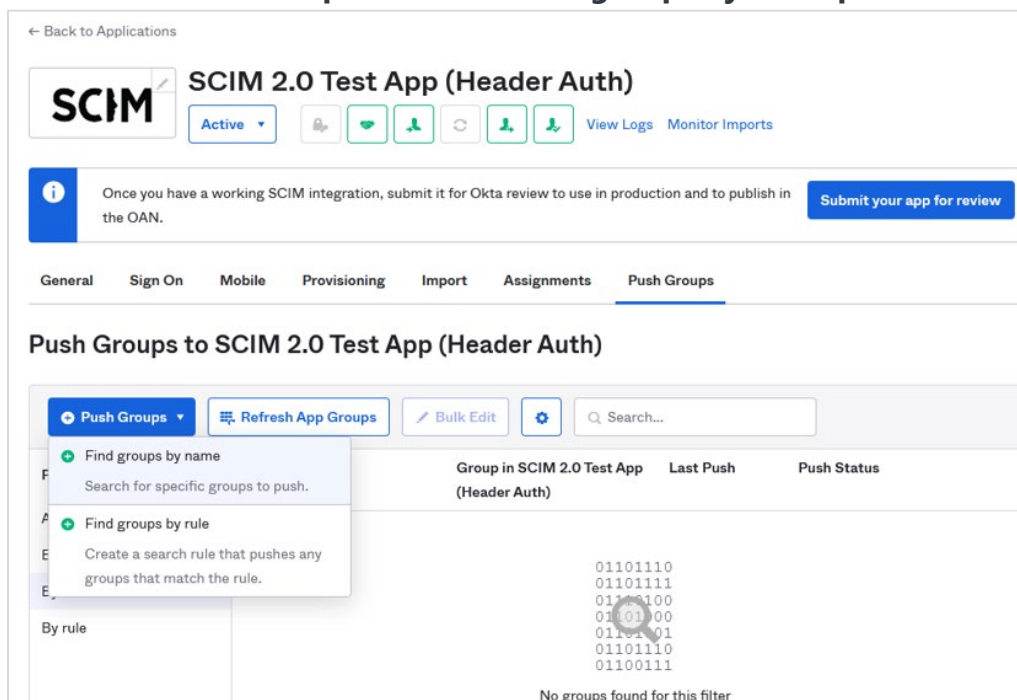
Filters: **People**, Groups

Person	Type
[Person Name]	Group

REPORTS: Current Assignments, Recent Unassignments

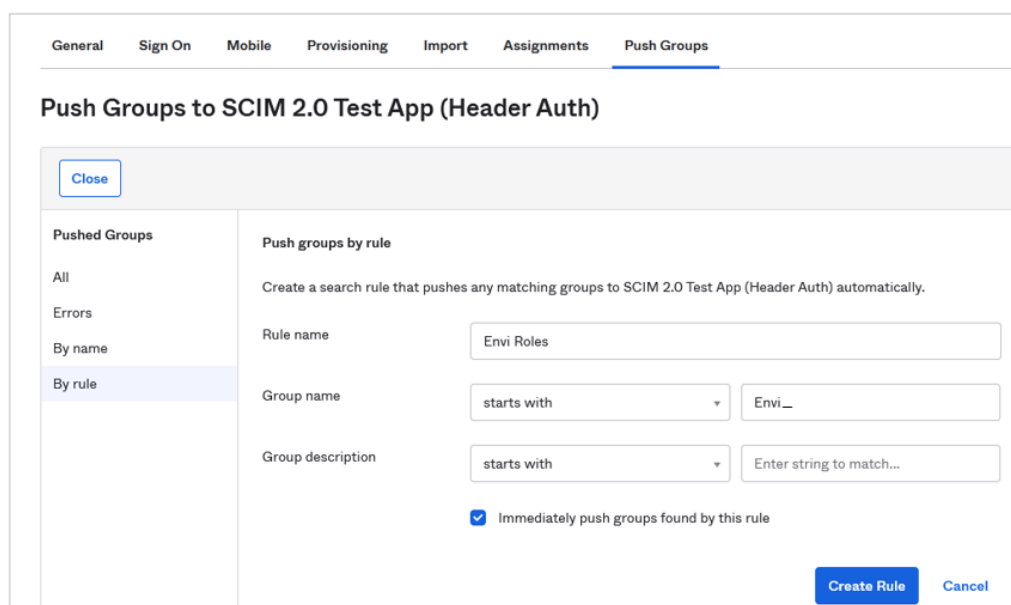
Group Provisioning

1. To add a new group, go to the application details page, to the **Push Groups** tab, then select **Push Groups** and select **Find groups by rule option**.



2. On the **Push groups by rule** page, perform the following steps:
 - a. Enter **Rule name**.
 - b. In the **Group name** box, set **starts with**.
 - c. In the next box, enter **Envi_** to match with the **Envi** value, and select **Create Rule**.

Note: To have **Okta** group provisioning work correctly, all names of groups that participate in the provisioning should start with the **Envi** prefix (Envi_).



- To verify the list of groups pushed to **Envi**, select **By rule**.

General Sign On Mobile Provisioning Import Assignments <u>Push Groups</u>				
Push Groups to SCIM 2.0 Test App (Header Auth)				
<div> <div>Push Groups</div> <div>Refresh App Groups</div> <div>Bulk Edit</div> <div></div> <div>Search...</div> </div>				
Pushed Groups	Group in Okta	Group in SCIM 2.0 Test App (Header Auth)	Last Push	Push Status
All				
Errors				
By name				
By rule				
Envi Roles				

Now, the needed members and groups are added.

Envi Configuration

To synchronize **Okta** with **Envi** via **SCIM**, perform the following actions:

1. Sign in to the **Envi** application.
2. Go to **My Profile > My Domain > Recourses** tab.
3. On the **Recourses** tab, select the **SCIM Configuration** link.

Note: The link is only available for domains with the **Simple** domain type and with the **HTTP Redirect** or **WS Trust** authentication.

4. On the **SCIM Configuration** page, you will find the domain details of your configuration. By default, a new configuration will be **Inactive** and will contain no organizations. To proceed with further **SCIM** configuration, perform the following steps:
 - a. Select **Edit**.
 - b. In the **Status** dropdown, select **Active**.
 - c. In the **Organization** dropdown, select a needed organization.
 - d. Select **Update**.

- Once you have updated **SCIM** configurations, select the **Create Token**, then **Copy Token** button.

Note: Enter the obtained **SCIM** token in the **Secret Token** box (the [Okta Configuration](#) section, step 8).

Domains > Domain Name **envi.com**

DETAILS ORGANIZATIONS USERS PASSWORD DICTIONARIES UPDATE **RESOURCES** SECURITY

Edit Create Token Copy Token Go Back

Status: Active
 Organization: **For Testing Purpose**
 Valid Token: Yes
 User Role Prefix: Envi_

Now, **Okta SCIM** is configured and synchronized.