Okta SCIM

Integration Guide

Contents

Introduction

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

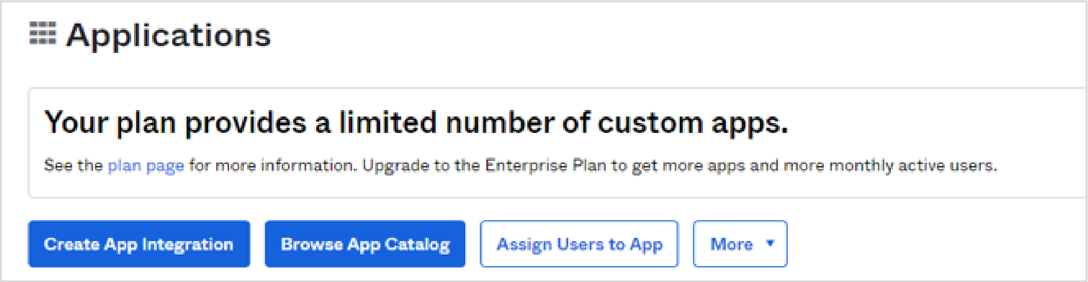
SCIM enables IT departments to automate provisioning and deprovisioning of accounts, which reduces manual redundant processes and increases security.

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**.

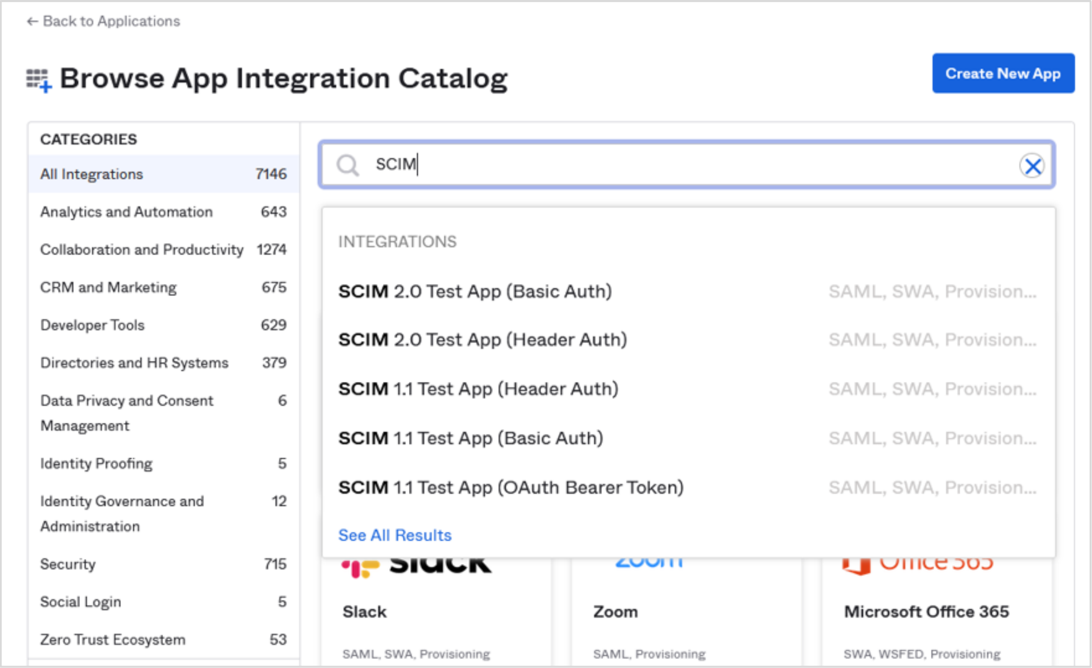


Applications

Your plan provides a limited number of custom apps.

See the plan page for more information. Upgrade to the Enterprise Plan to get more apps and more monthly active users.

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



← Back to Applications

Browse App Integration Catalog

CATEGORIES	
All Integrations	7146
Analytics and Automation	643
Collaboration and Productivity	1274
CRM and Marketing	675
Developer Tools	629
Directories and HR Systems	379
Data Privacy and Consent Management	6
Identity Proofing	5
Identity Governance and Administration	12
Security	715
Social Login	5
Zero Trust Ecosystem	53

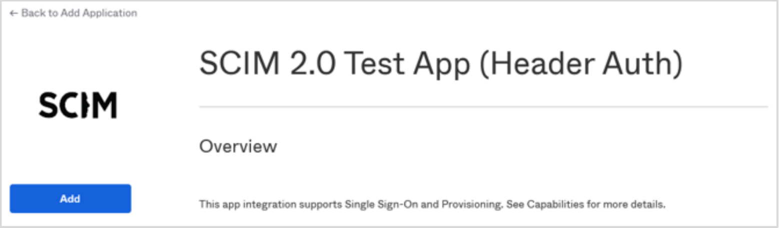
SCIM

INTEGRATIONS	
SCIM 2.0 Test App (Basic Auth)	SAML, SWA, Provision...
SCIM 2.0 Test App (Header Auth)	SAML, SWA, Provision...
SCIM 1.1 Test App (Header Auth)	SAML, SWA, Provision...
SCIM 1.1 Test App (Basic Auth)	SAML, SWA, Provision...
SCIM 1.1 Test App (OAuth Bearer Token)	SAML, SWA, Provision...

See All Results

Slack	Zoom	Microsoft Office 365
SAML, SWA, Provisioning	SAML, Provisioning	SWA, WSFED, Provisioning

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



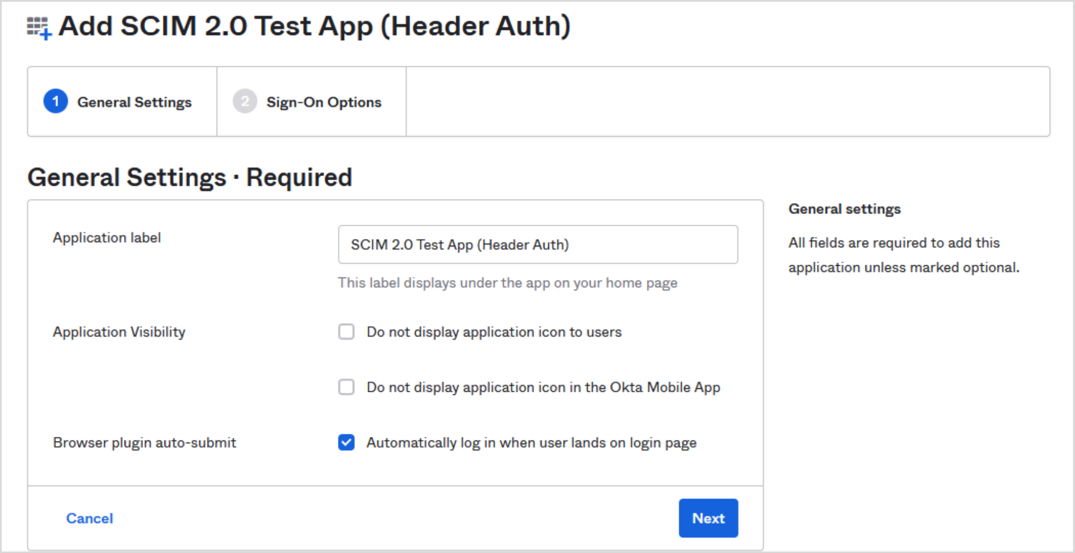
← Back to Add Application

SCIM 2.0 Test App (Header Auth)

Overview

This app integration supports Single Sign-On and Provisioning. See Capabilities for more details.

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**.



General Settings · Required

Application label: SCIM 2.0 Test App (Header Auth)

This label displays under the app on your home page

Application Visibility: ☐ Do not display application icon to users

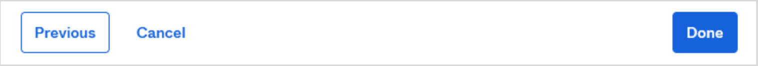
☐ Do not display application icon in the Okta Mobile App

Browser plugin auto-submit: ☑ Automatically log in when user lands on login page

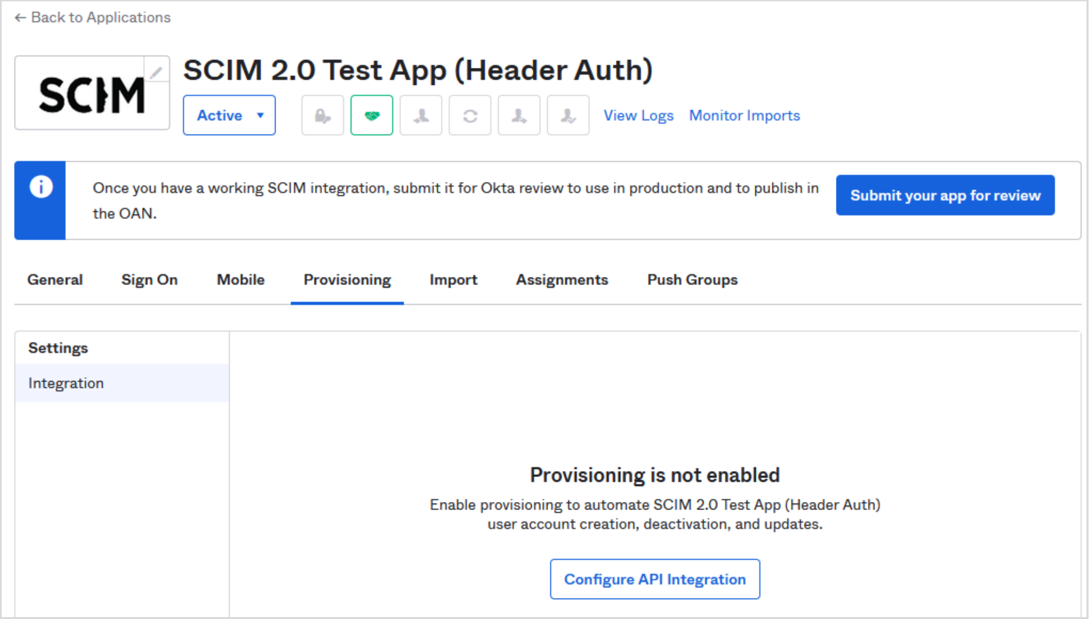
General settings

All fields are required to add this application unless marked optional.

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.



Once you have a working SCIM integration, submit it for Okta review to use in production and to publish in the OAN.

Provisioning is not enabled

Enable provisioning to automate SCIM 2.0 Test App (Header Auth) user account creation, deactivation, and updates.

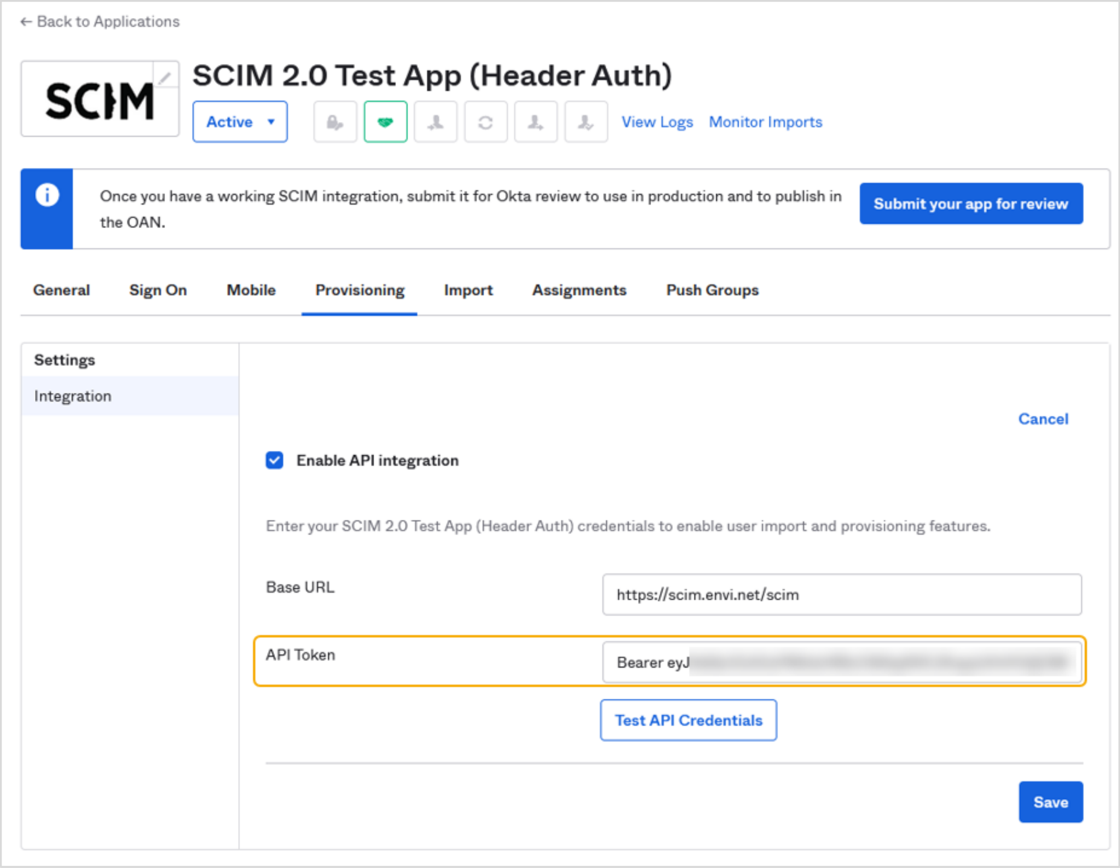
8. To configure the **API** integration, perform the following steps:

   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 **Bearer SCIM** token obtained from the **Envi** application (the Envi Configuration section, step 5).

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



Once you have a working SCIM integration, submit it for Okta review to use in production and to publish in the OAN.

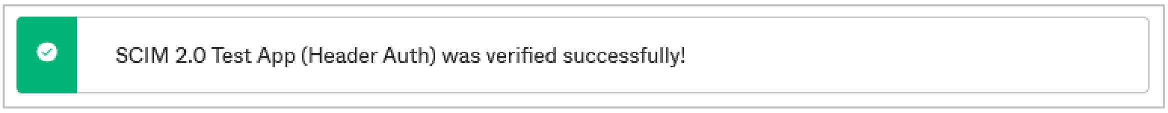
☑ Enable API integration

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

Base URL: https://scim.envi.net/scim

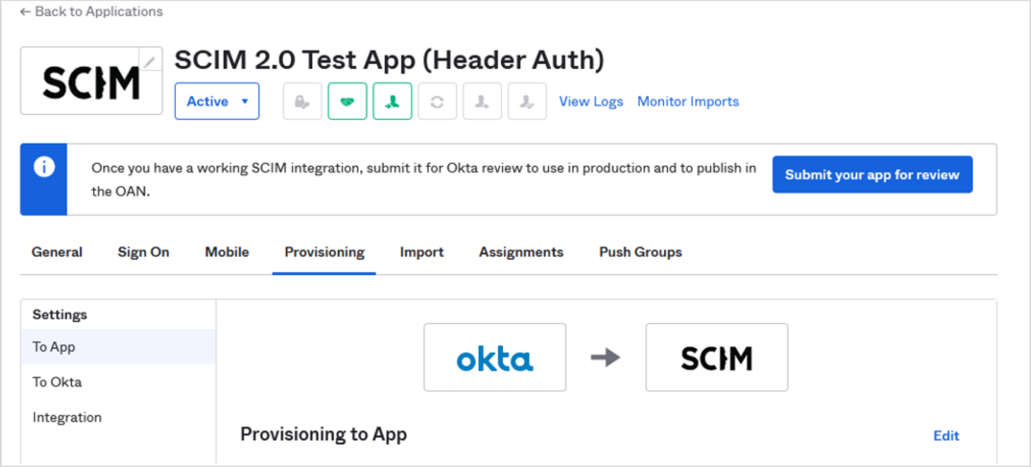
API Token: Bearer eyJ[redacted]

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



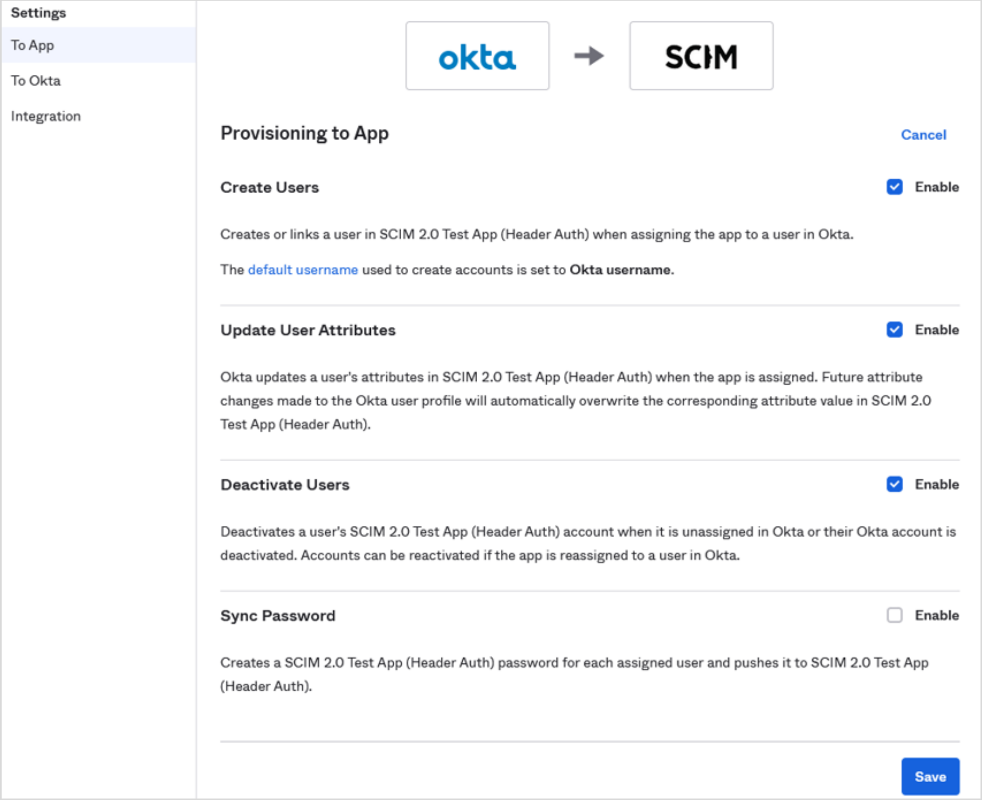
SCIM 2.0 Test App (Header Auth) was verified successfully!

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**.



Once you have a working SCIM integration, submit it for Okta review to use in production and to publish in the OAN.

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



Provisioning to App

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).

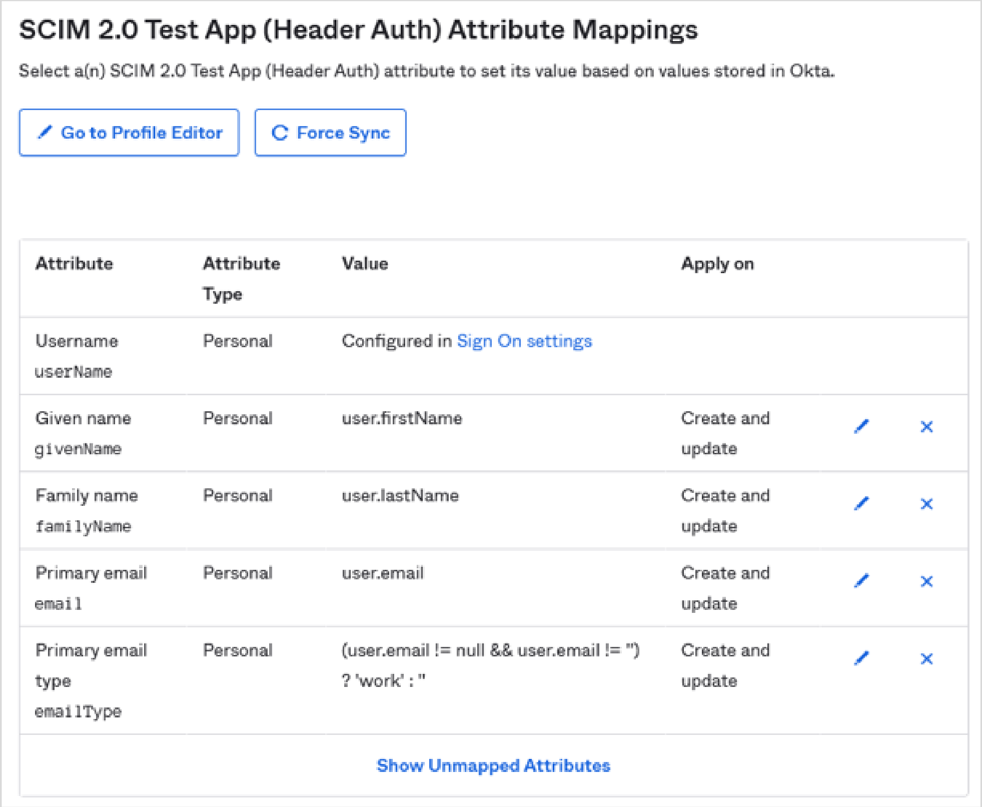
Deactivate Users ☑ Enable

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).

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.

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

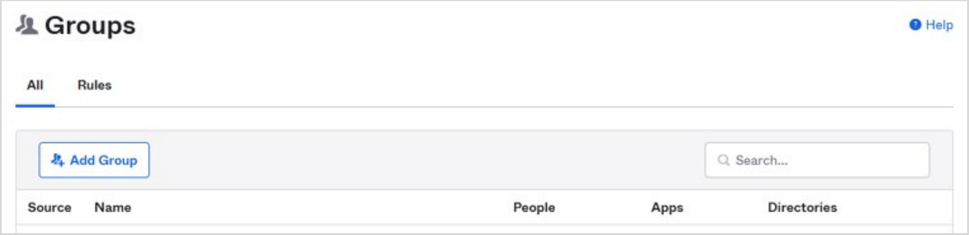
Your configuration will be saved automatically. At this point, it is ready for use.

Provisioning

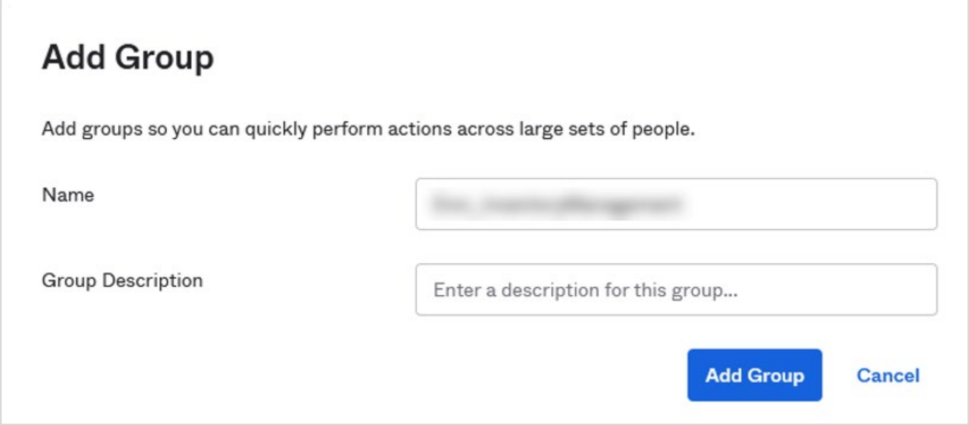
In this section, you will learn how to provision new users and groups.

User Provisioning

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

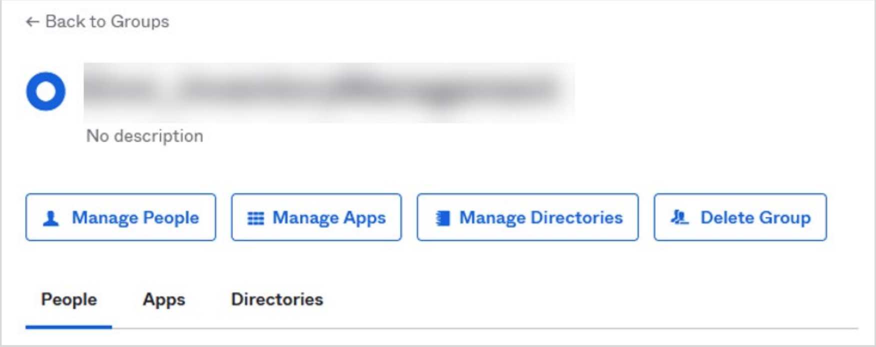


3. Enter the **Name** and **Description** of your group, then select **Add Group**.

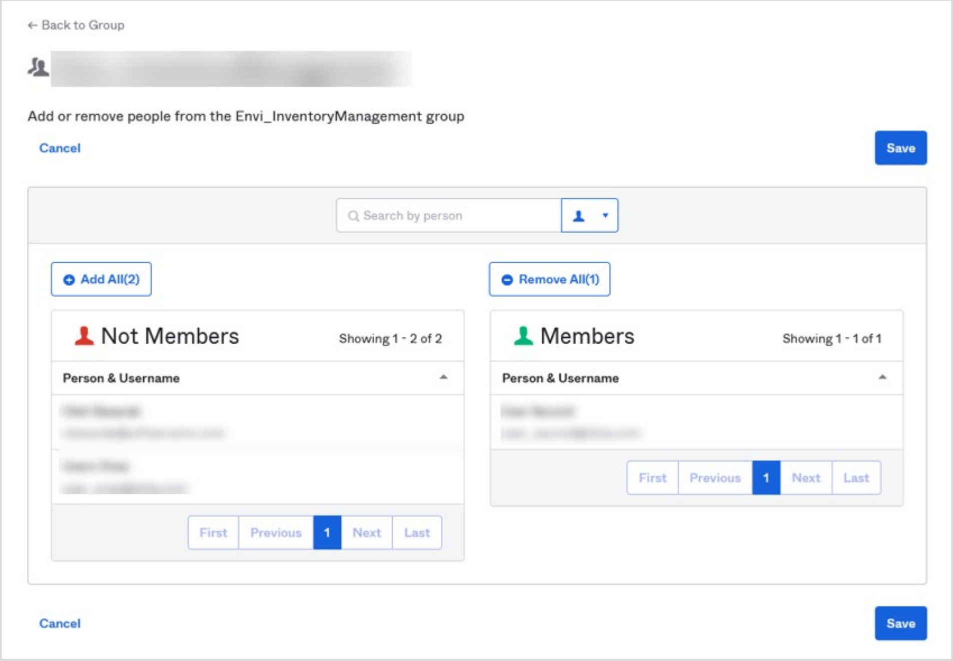

Add Group

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

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**.



← Back to Group

[redacted]

Add or remove people from the Envi_InventoryManagement group

[redacted]

[redacted]

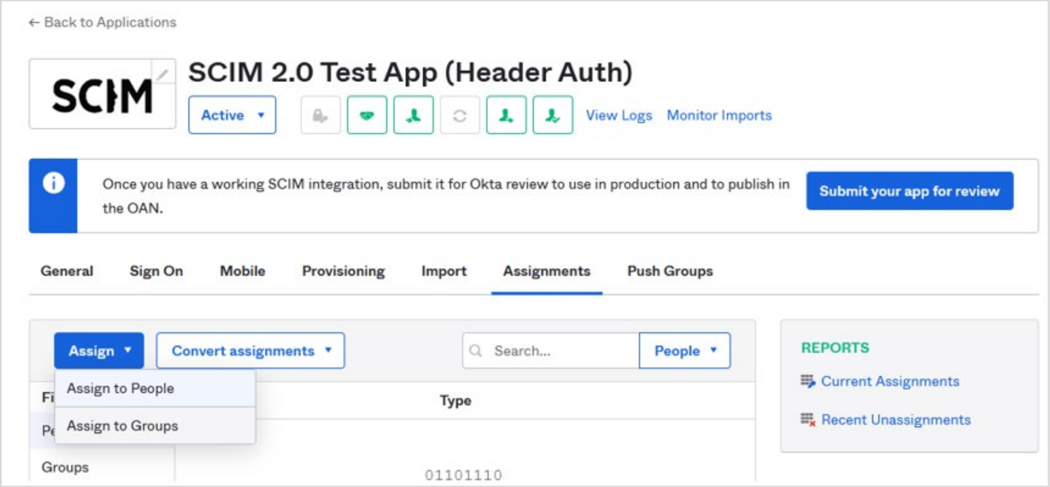
[redacted]

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**.

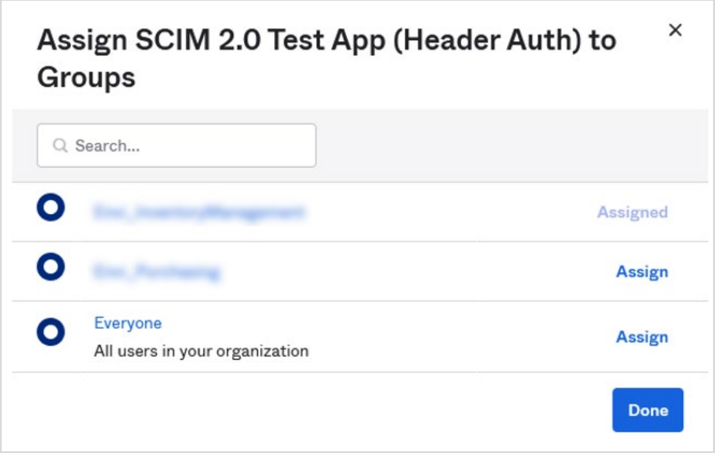


← Back to Applications

SCIM 2.0 Test App (Header Auth)

Once you have a working SCIM integration, submit it for Okta review to use in production and to publish in the OAN.

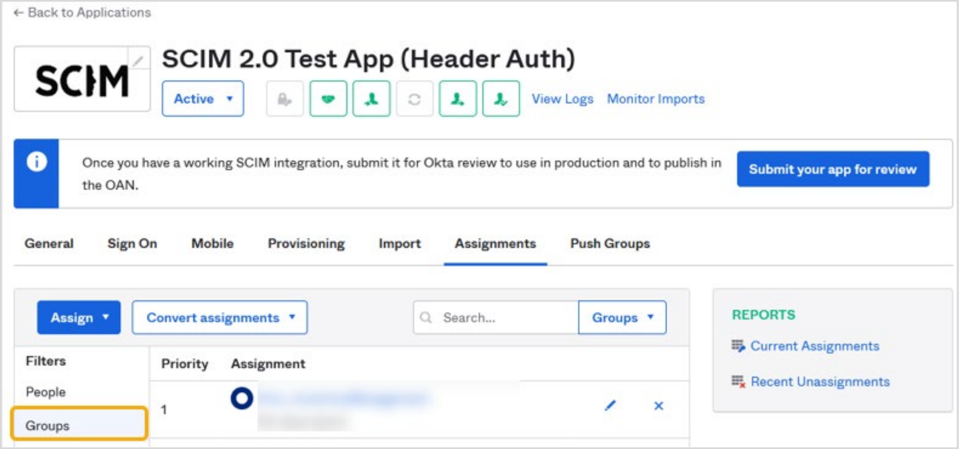
7. To add a group, select **Assign**, then select **Save** and **Go Back** to enable member provisioning for this group. When all needed groups are added, select **Done**.



Assign SCIM 2.0 Test App (Header Auth) to Groups

[redacted]	Assigned
[redacted]	Assign
Everyone All users in your organization	Assign

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

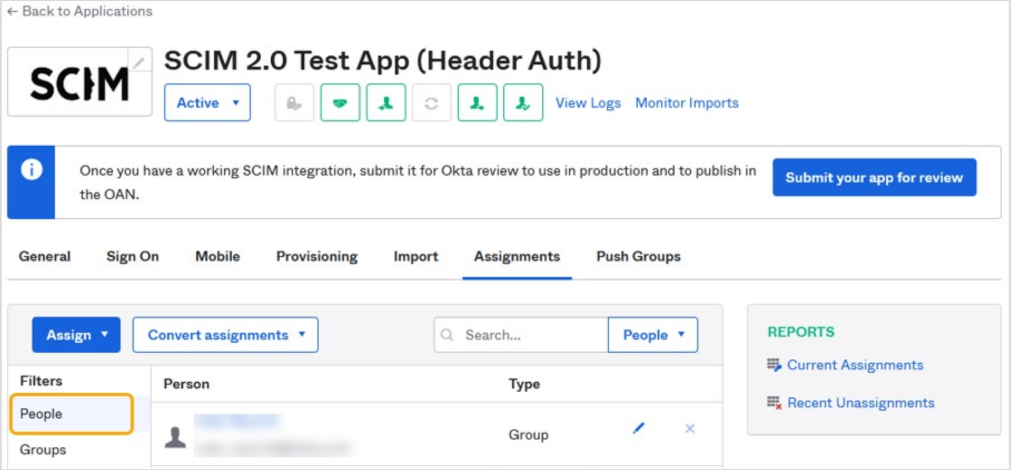


SCIM 2.0 Test App (Header Auth)

Once you have a working SCIM integration, submit it for Okta review to use in production and to publish in the OAN.

Priority	Assignment
1	[redacted]

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



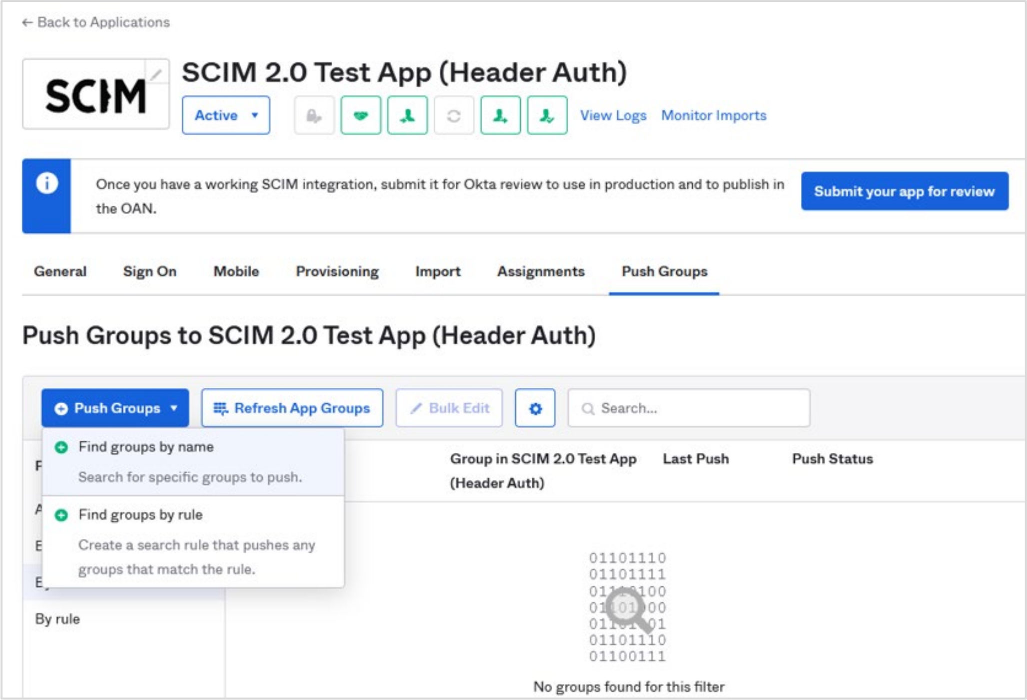
SCIM 2.0 Test App (Header Auth)

Once you have a working SCIM integration, submit it for Okta review to use in production and to publish in the OAN.

Person	Type
[redacted]	Group

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**.



Once you have a working SCIM integration, submit it for Okta review to use in production and to publish in the OAN.

Push Groups to SCIM 2.0 Test App (Header Auth)

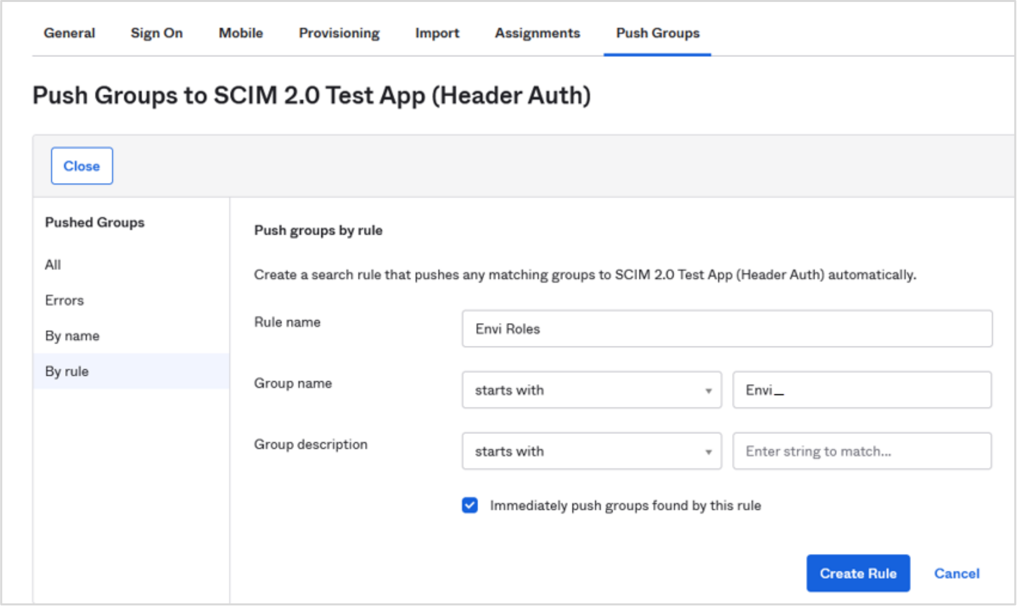
Search for specific groups to push.

Create a search rule that pushes any groups that match the rule.

No groups found for this filter

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_).



Push Groups to SCIM 2.0 Test App (Header Auth)

Push groups by rule

Create a search rule that pushes any matching groups to SCIM 2.0 Test App (Header Auth) automatically.

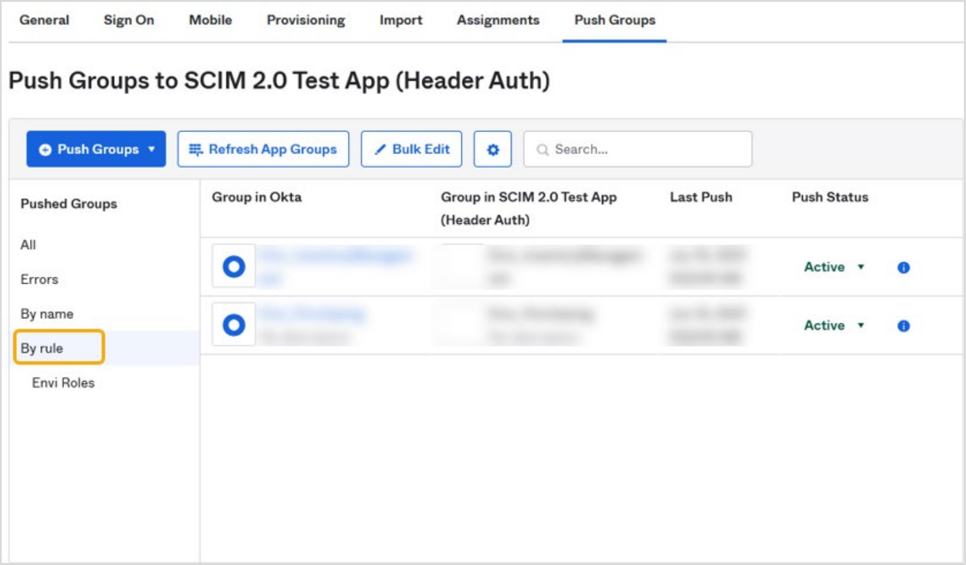
Rule name: Envi Roles

Group name: starts with ▾ Envi_

Group description: starts with ▾ Enter string to match...

☑ Immediately push groups found by this rule

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



Push Groups to SCIM 2.0 Test App (Header Auth)

Group in Okta	Group in SCIM 2.0 Test App (Header Auth)	Last Push	Push Status
[redacted]	[redacted]	[redacted]	Active ▾
[redacted]	[redacted]	[redacted]	Active ▾

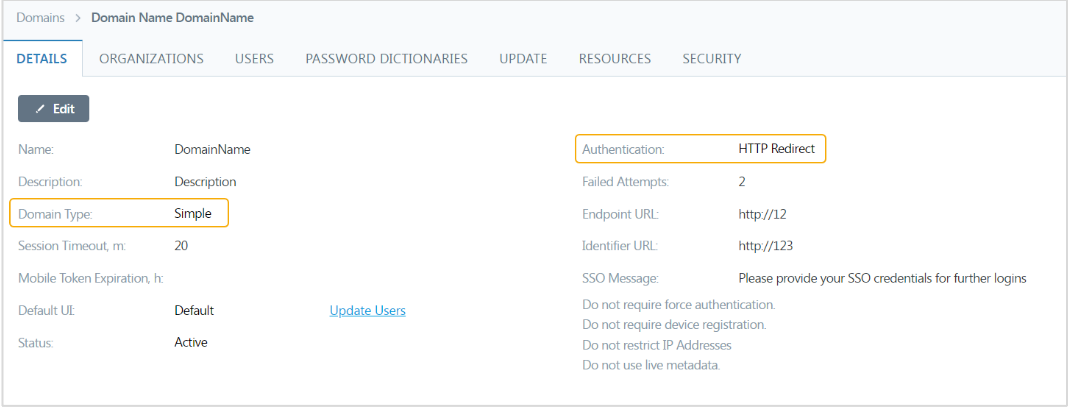
Now, the needed members and groups are added.

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.



Domains > Domain Name DomainName

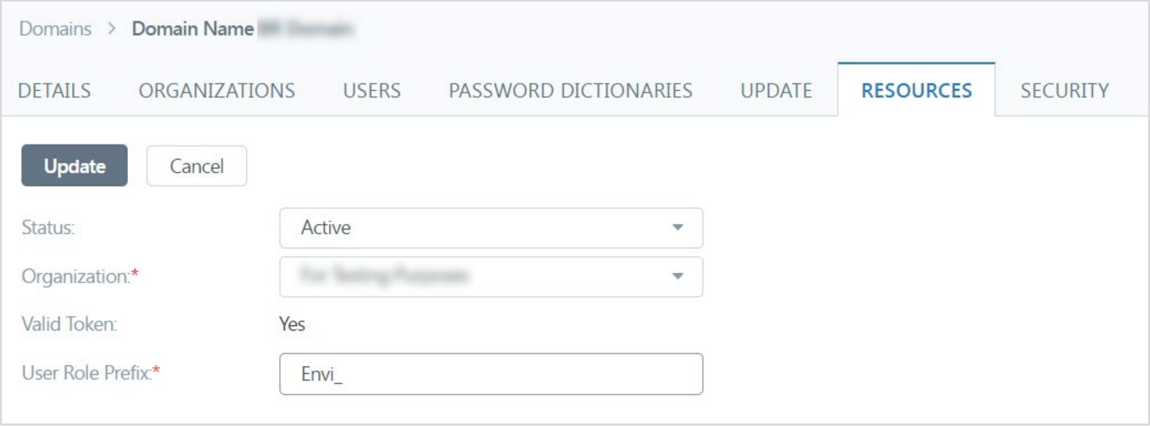
DETAILS ORGANIZATIONS USERS PASSWORD DICTIONARIES UPDATE RESOURCES SECURITY

Edit

Name:	DomainName		Authentication:	HTTP Redirect
Description:	Description		Failed Attempts:	2
Domain Type:	Simple		Endpoint URL:	http//12
Session Timeout, m:	20		Identifier URL:	http//123
Mobile Token Expiration, h:			SSO Message:	Please provide your SSO credentials for further logins
Default UI:	Default	Update Users	Do not require force authentication. Do not require device registration. Do not restrict IP Addresses Do not use live metadata.	
Status:	Active			

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**.



Domains > Domain Name [redacted]

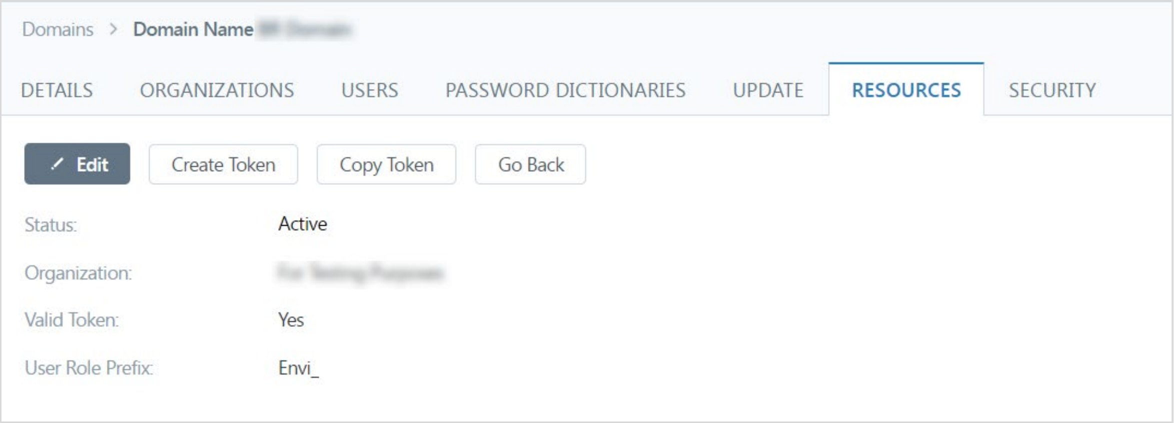
DETAILS ORGANIZATIONS USERS PASSWORD DICTIONARIES UPDATE RESOURCES SECURITY

Update Cancel

Status:	Active
Organization:*	[redacted]
Valid Token:	Yes
User Role Prefix:*	Envi_

5. 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).



Status: Active

Organization: [redacted]

Valid Token: Yes

User Role Prefix: Envi_

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