envi

Okta SCIM

Integration Guide

Contents

Introduction

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

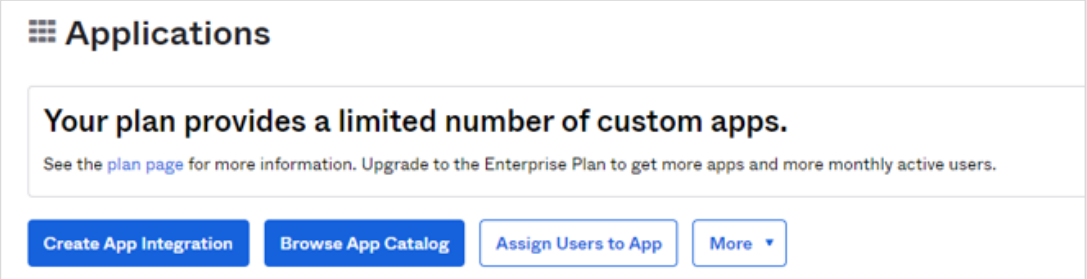
SCIM enables IT departments to automate provisioning and deprovisioning of accounts, which reduces manual redundant processes and increases security.

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

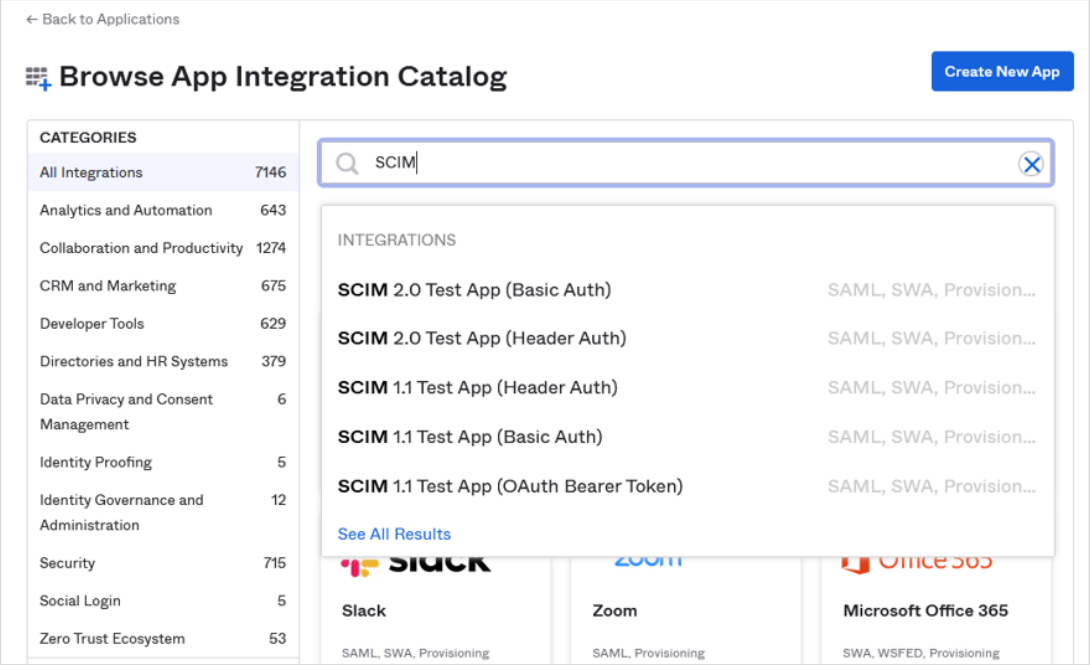
Okta Configuration

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

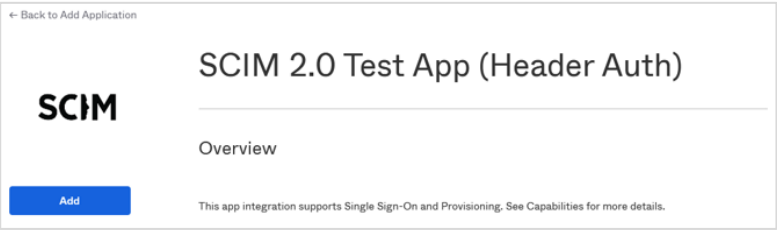
1. Sing in to the Okta site.
2. Select **Applications** > **Applications** from the site menu.
3. On the **Applications** page, select **Browse App Catalog**.



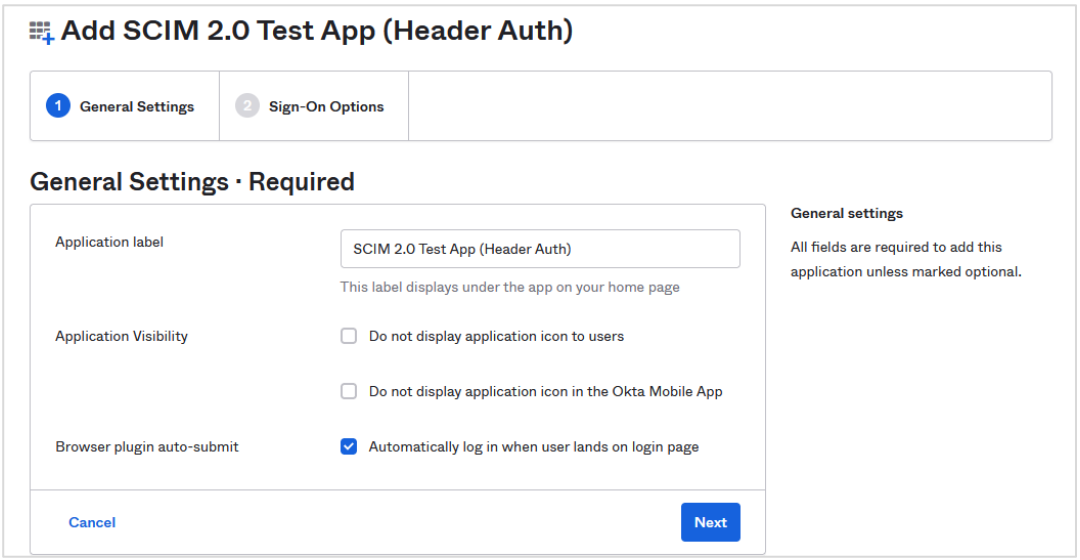
4. On the **Browse App Integration Catalog** page, type **SCIM** in the search box and select **SCIM 2.0 Test App** (**Header Auth**).



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

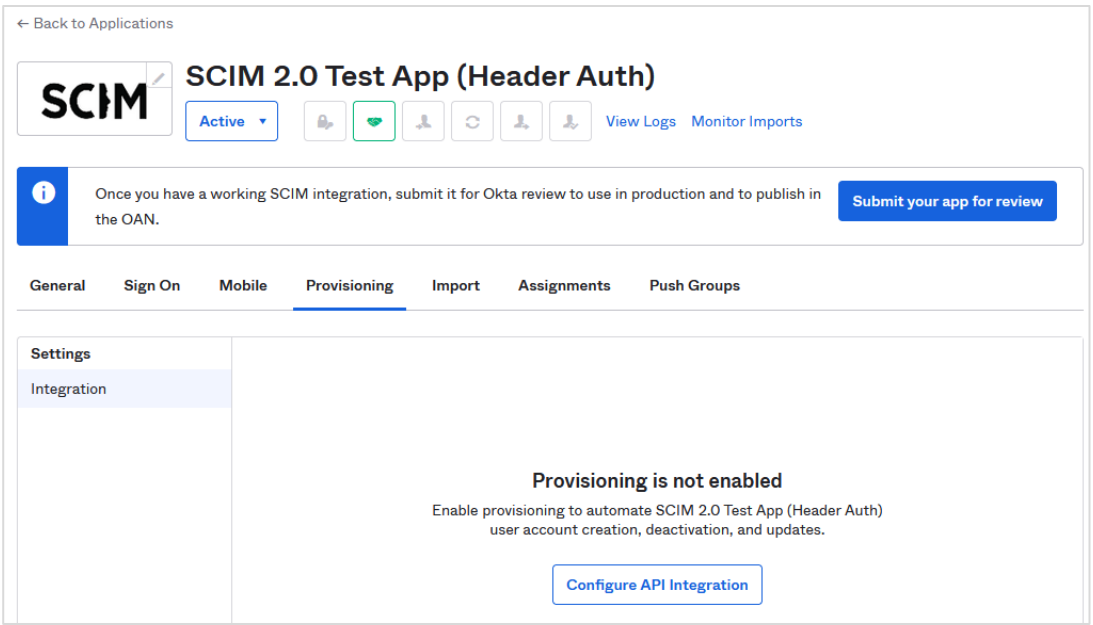


6. On the **Add SCIM 2.0 Test App (Header Auth)** page, enter an **Application label** (name). Based on your needs, you can set other application configuration options. Then, select **Next**.



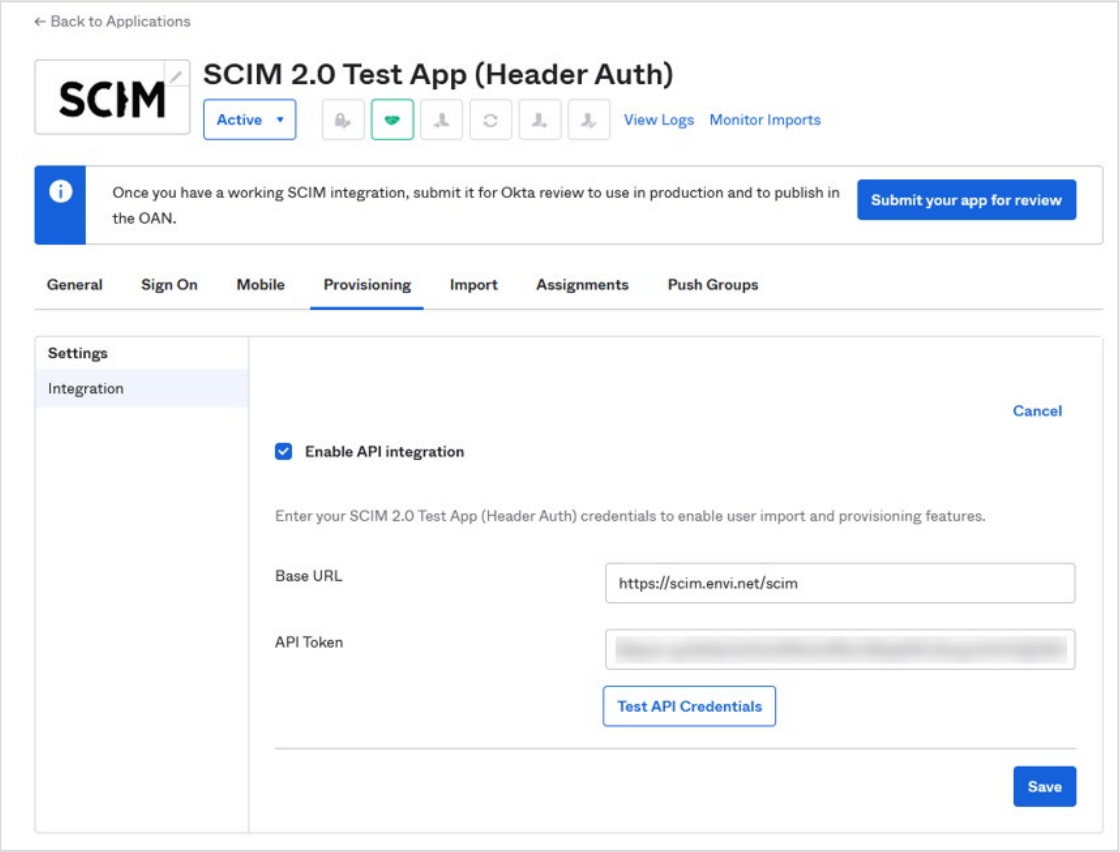
Note: To skip the **Sign-On options** page, select **Done** (leave all the default options unless you need to configure it according to your organization's rules).

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



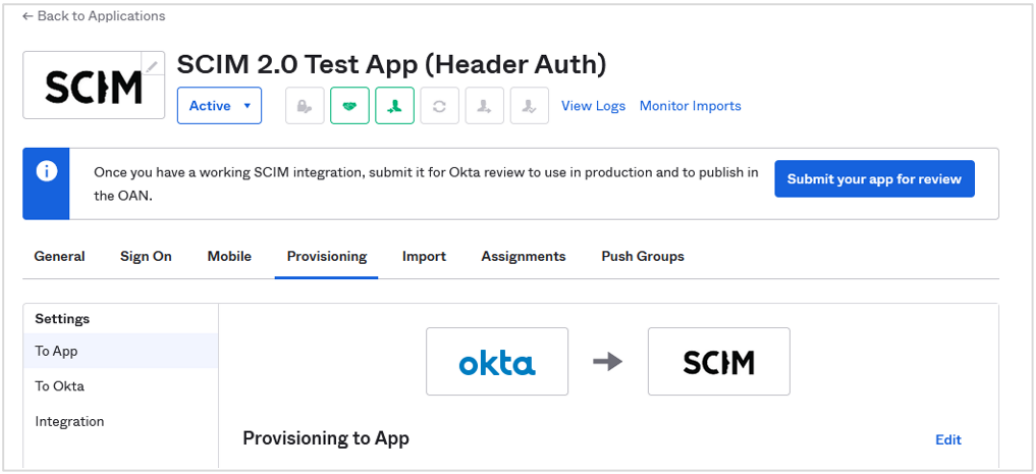
8. To configure the **API** integration, perform the following steps:
   a. Select the **Enable API integration** checkbox to make additional boxes appear.
   b. In the **Base URL** box, enter the base URL of the **Envi SCIM** server + **/scim** (for example, https://scim.envi.net/scim).
   c. In the **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.

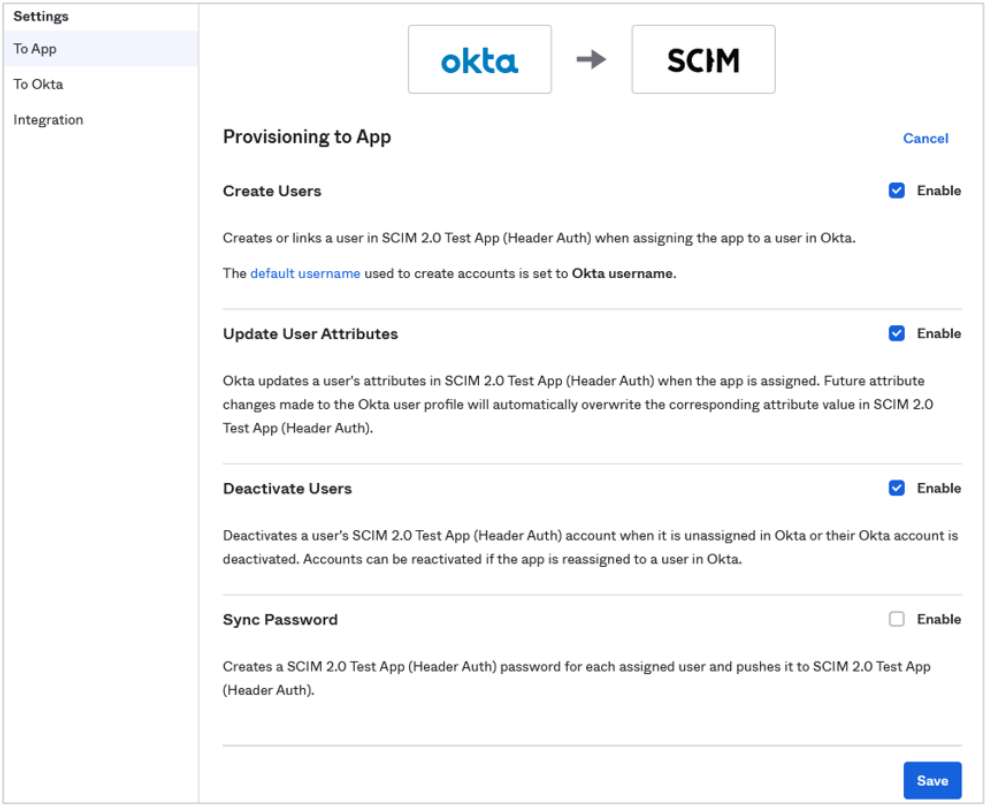


9. After a successful test connection, you will see the message:

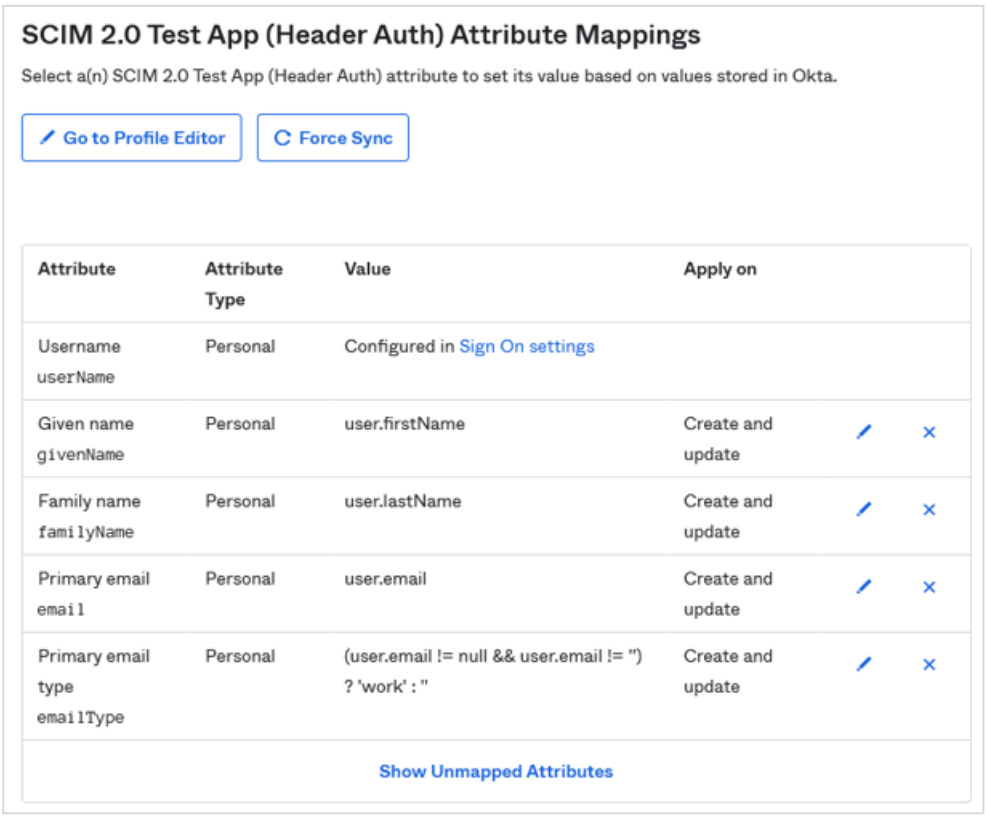
10. Select **Save**.
11. After refreshing the page, you will see the new configuration options. In the **Settings** section, select **To App** and then **Edit**.



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



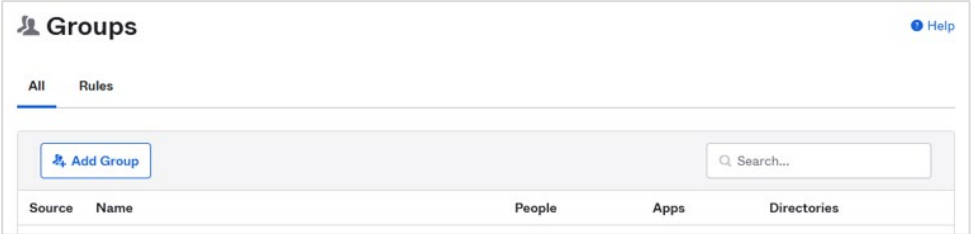
Your configuration will be saved automatically. At this point, it is ready for use.

Provisioning

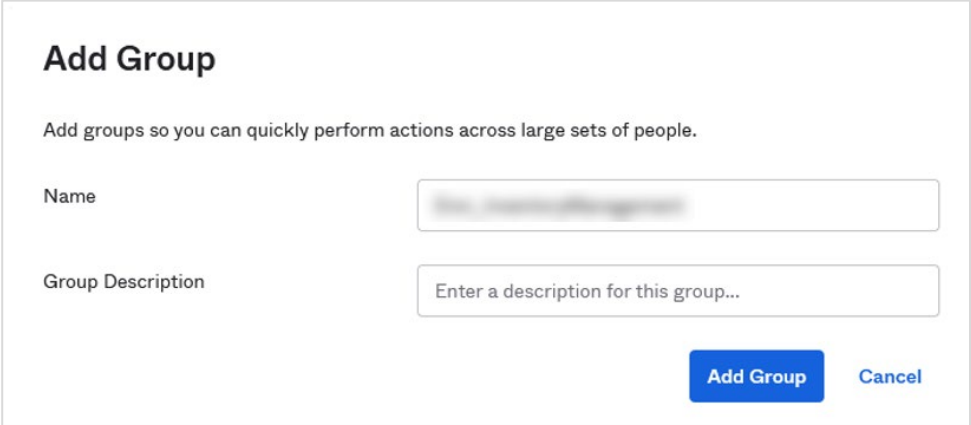
In this section, you will learn how to provision new users and groups.

User Provisioning

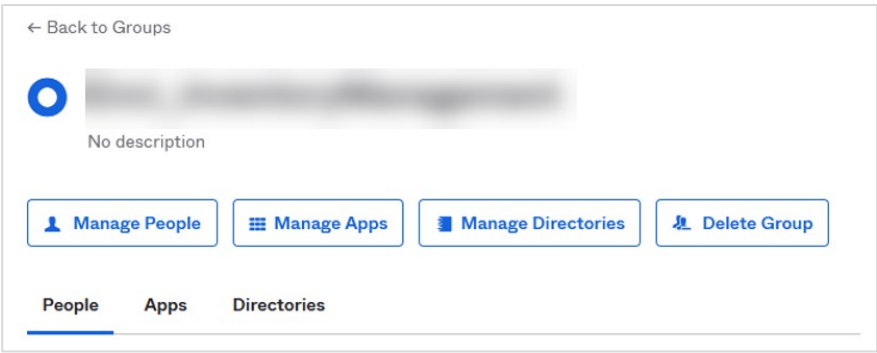
1. To add a new member, go to **Directory** > **Groups** in the site menu.
2. On the **Groups** page, select **+Add Group**.



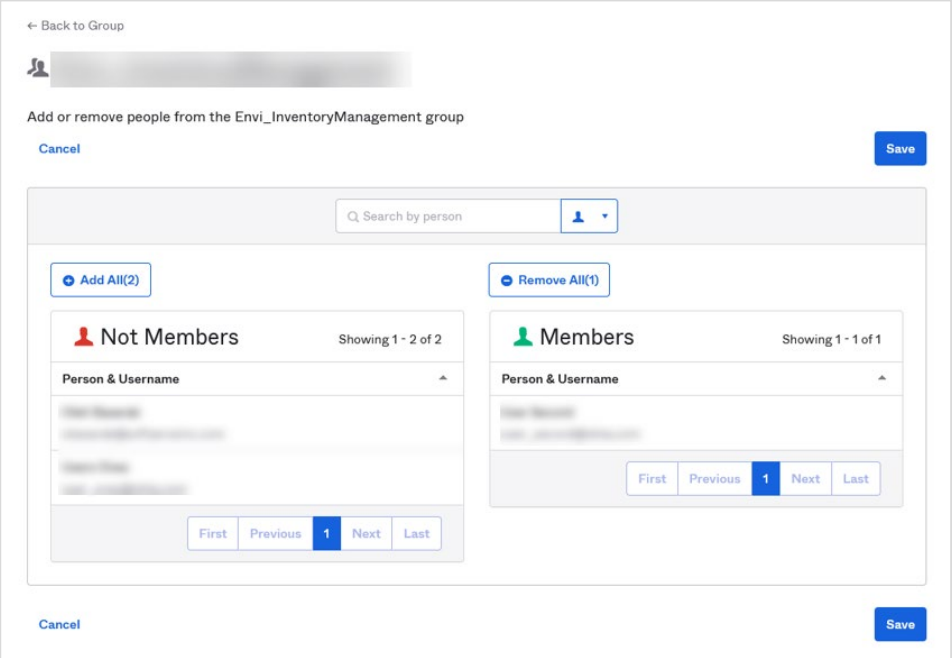
3. Enter the **Name** and **Description** of your group, then select **Add Group**.



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**.

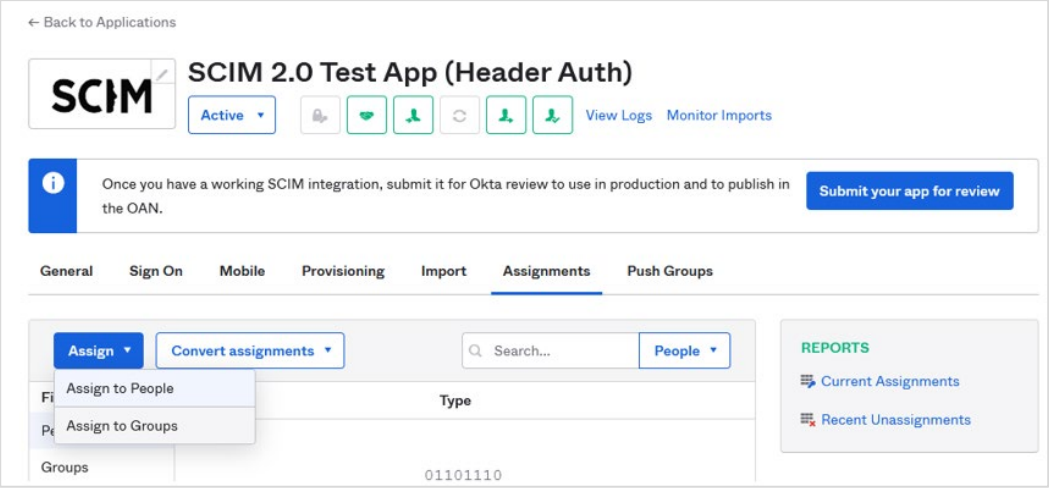


Note: Repeat the process of group creation and user assigning for all other users and groups that you want to provision.

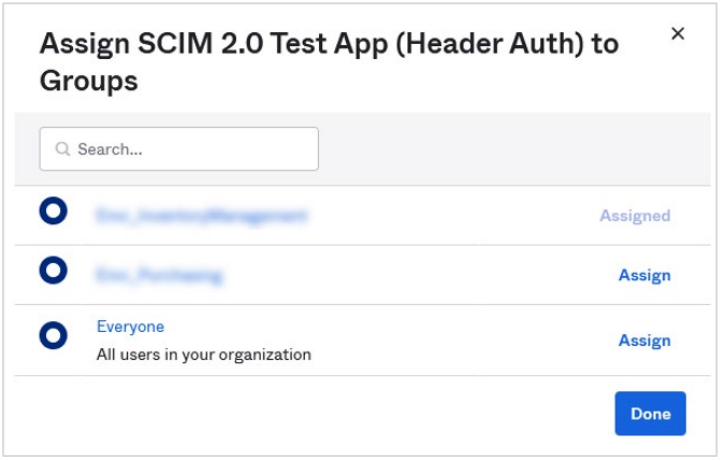
Note: If you are going to use group provisioning from **Okta** to **Envi**, you need to create a separate group for each **Envi** role. According to the configurations, your group name should have the same prefix as **User Role Prefix** (Envi_) on the **SCIM Configuration** page (the Envi Configuration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

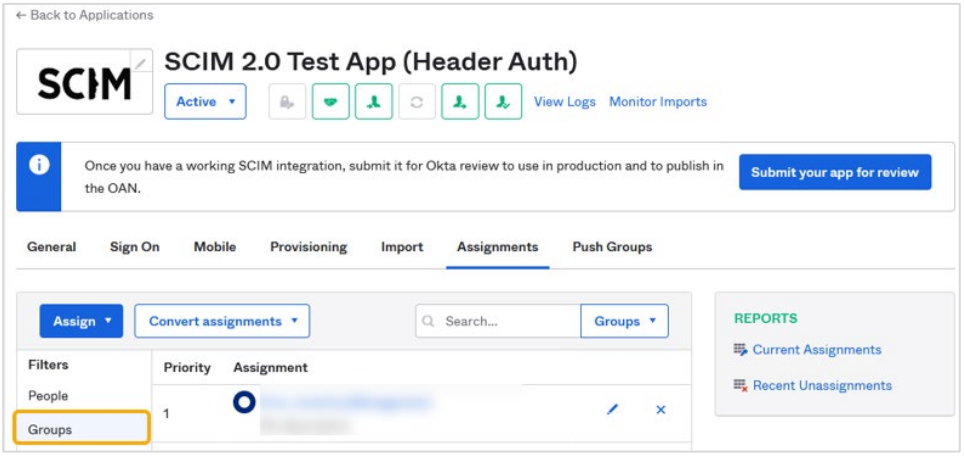
6. Go to the details of your application (select **Applications** > **Applications** in the menu and select your application from the list), and to the **Assignments** tab. Then select **Assign** and **Assign to Groups**.



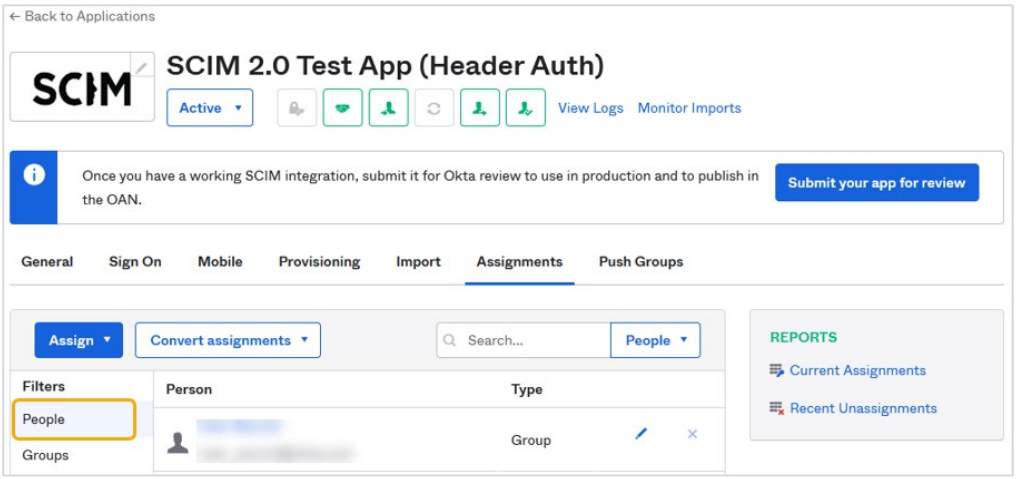
7. To add a group, select **Assign**, then select **Save** and **Go Back** to enable member provisioning for this group. When all needed groups are added, select **Done**.



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

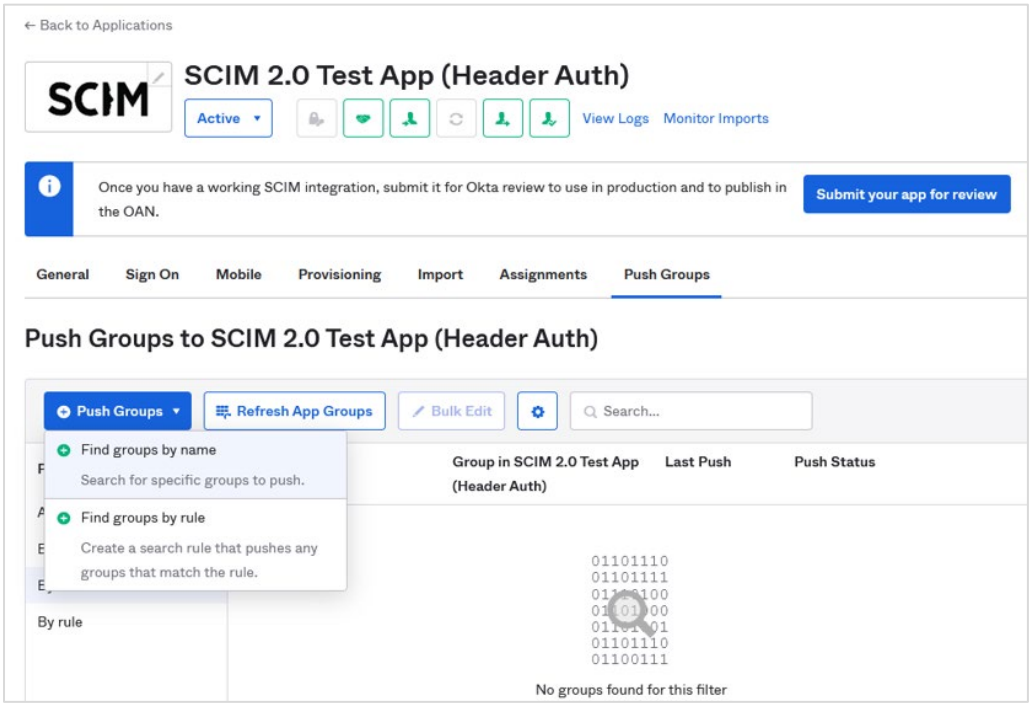


9. To see users that are assigned due to the user group assignment, go to the **People** section.



Group Provisioning

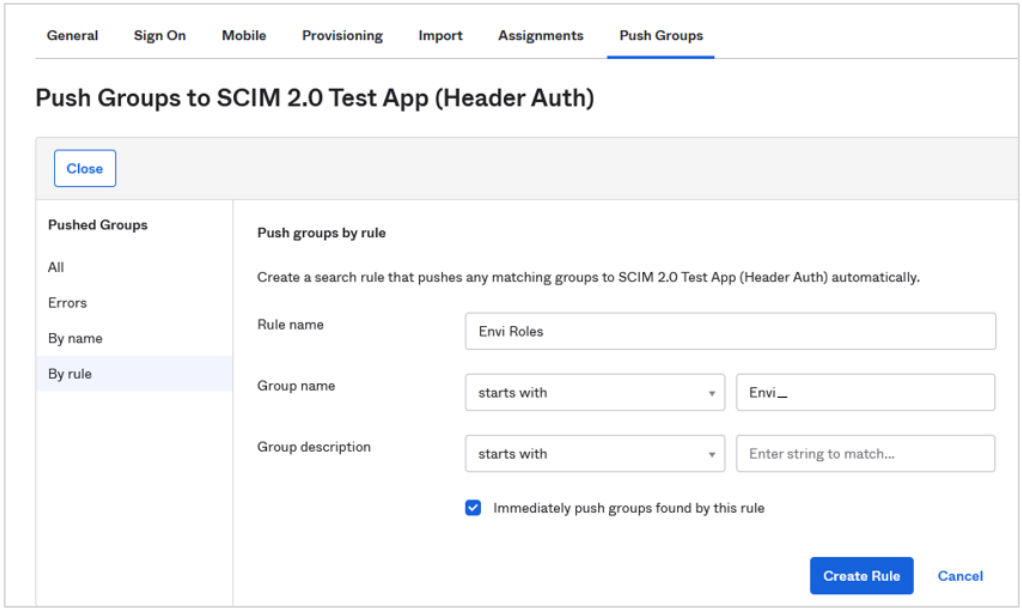
1. To add a new group, go to the application details page, to the **Push Groups** tab, then select **Push Groups** and select **Find groups by rule option**.



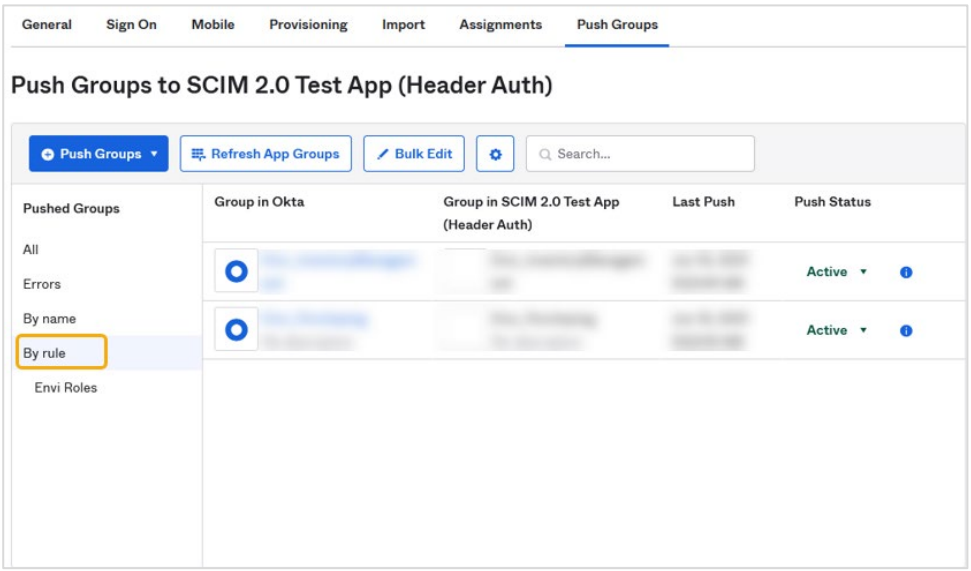
2. On the **Push groups by rule** page, perform the following steps:

   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_).



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



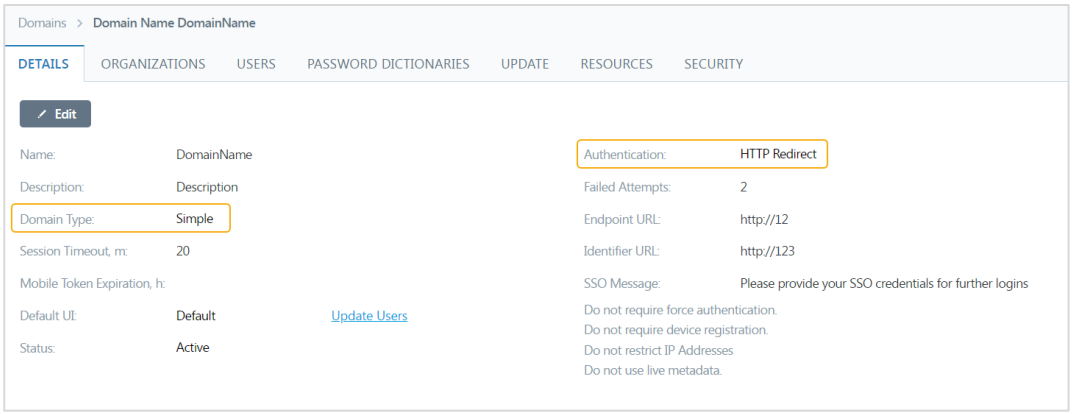
Now, the needed members and groups are added.

Envi Configuration

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

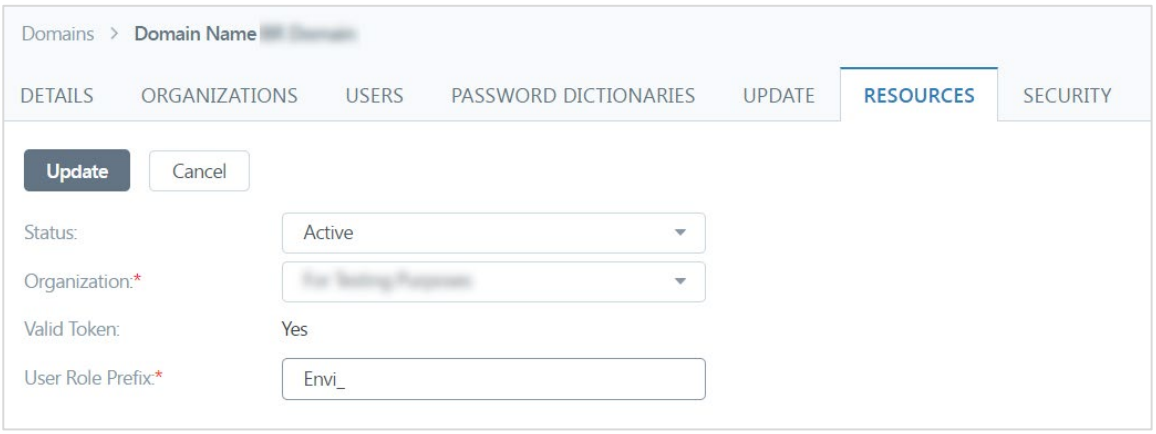
1. Sign in to the **Envi** application.
2. Go to **My Profile** > **My Domain** > **Recourses** tab.
3. On the **Recourses** tab, select the **SCIM Configuration** link.

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



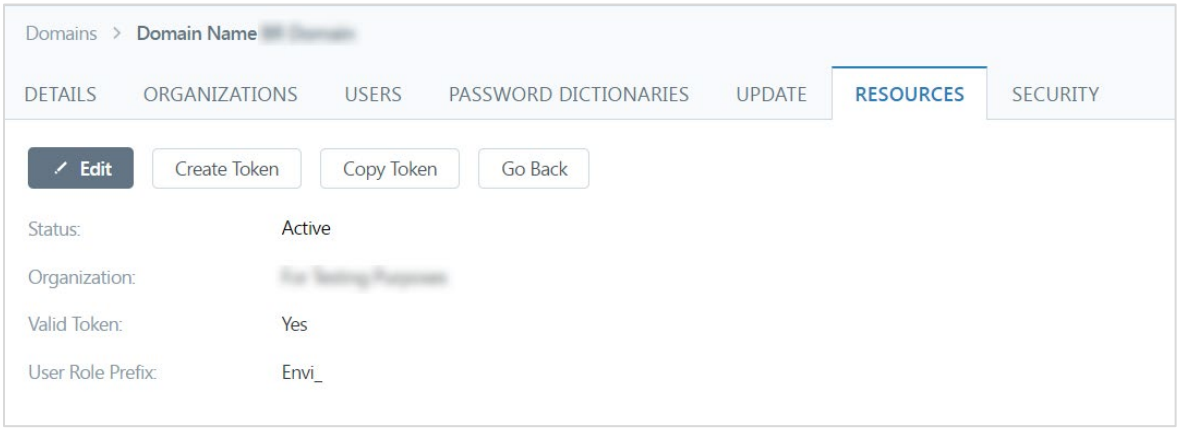
4. On the **SCIM Configuration** page, you will find the domain details of your configuration. By default, a new configuration will be **Inactive** and will contain no organizations. To proceed with further **SCIM** configuration, perform the following steps:

   a. Select **Edit**.
   b. In the **Status** dropdown, select **Active**.
   c. In the **Organization** dropdown, select a needed organization.
   d. Select **Update**.



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).



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