Configure System for Cross-domain Identity Management (SCIM) with Okta

How to set up Stack Overflow for Teams Enterprise for Okta SCIM 2.0 provisioning.

Document generated 02/05/2025

PDF VERSION

Tags | **Provisioning** | **Okta** | **SCIM** |

Applies to: Free Basic Business **Enterprise**

ADMIN PRIVILEGES REQUIRED

*This documentation is for **Stack Overflow for Teams Enterprise**. Free, Basic, and Business users can access their documentation here. Find your plan.*

Overview

System for Cross-domain Identity Management (SCIM) is an open API for securely sharing user information between online systems. In Stack Overflow for Teams Enterprise (SOE), SCIM 2.0 support allows an Identity Provider (IdP) to automatically update Stack Overflow with the user's activation status and/or role. Unlike SAML 2.0, which passes user information only at login, SCIM sends updates whenever they occur. This provides SOE near-real-time updates to user status and role as changes happen at the IdP.

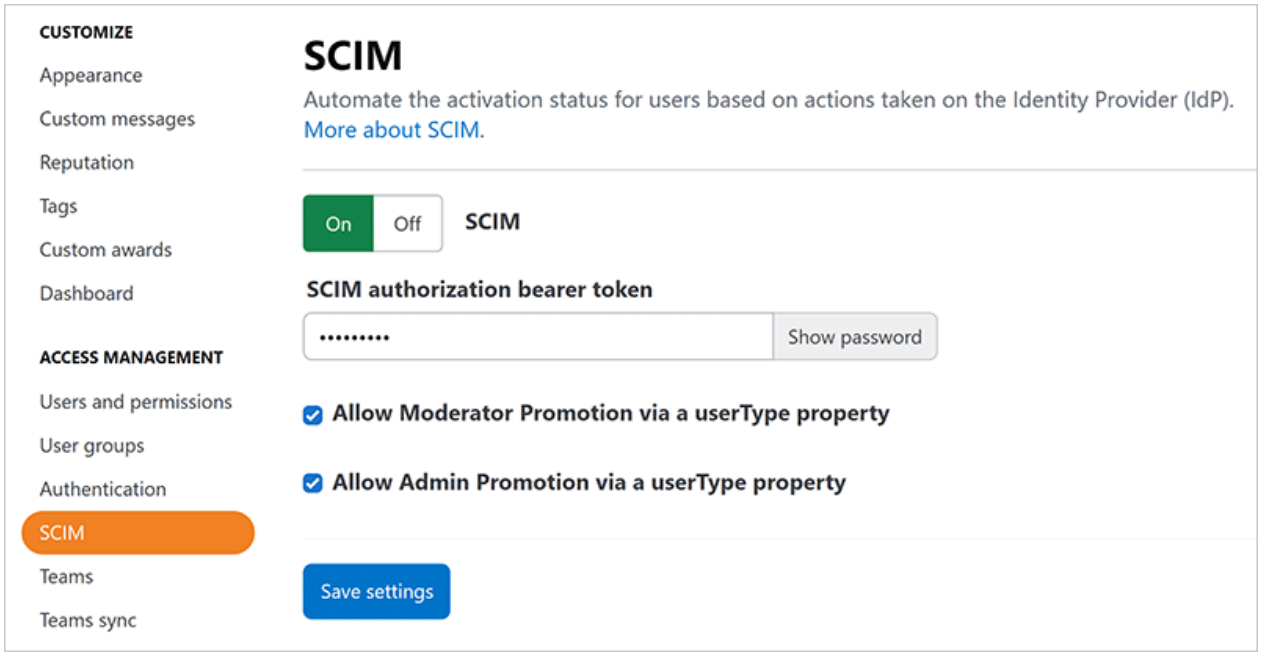
This article covers integrating Okta and your SOE site with SCIM. For a better understanding of using SCIM with SOE, read our SCIM 2.0 support article.

When setting up SCIM in Okta, you'll configure your SOE site and Okta in a back-and-forth process. We recommend having a browser tab open to each site.

THIS ARTICLE APPLIES TO STACK OVERFLOW FOR TEAMS ENTERPRISE ONLY.
Other Stack Overflow for Teams users should read this article instead. Find your plan.

Configure SCIM on SOE

1. As an SOE admin, click **Admin Settings** in the left-hand menu. Click **SCIM** under the "ACCESS MANAGEMENT" heading.



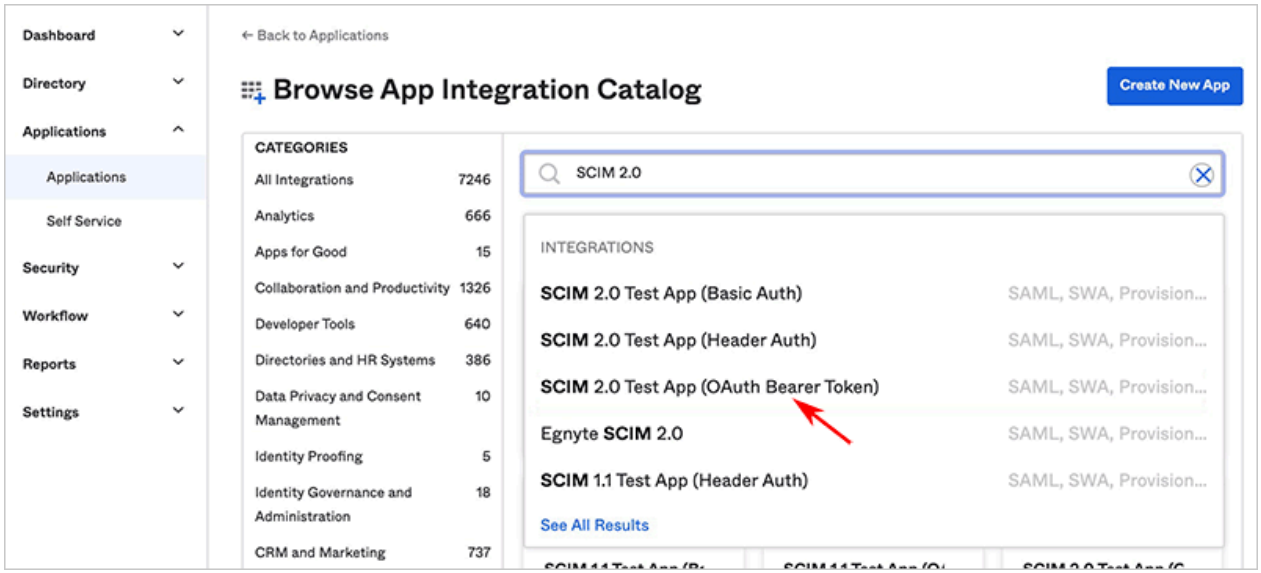
2. Configure the following settings:
    - **SCIM** Set to **On** to enable SCIM.
    - **SCIM authorization bearer token** Create a token (password) you'll later enter into the SCIM configuration on Okta. You can enter any string of characters, but be sure to follow best practices for creating a strong password. SOE hides the value by default. Click **Show password** to view and copy the value.
    - **Allow Moderator Promotion via a userType property** Check this box to enable SCIM promotion/demotion between regular user and moderator roles.
    - **Allow Admin Promotion via a userType property** Check this box to enable SCIM promotion/demotion between regular user and admin roles.
3. Click **Save settings**.

Configure SCIM in Okta

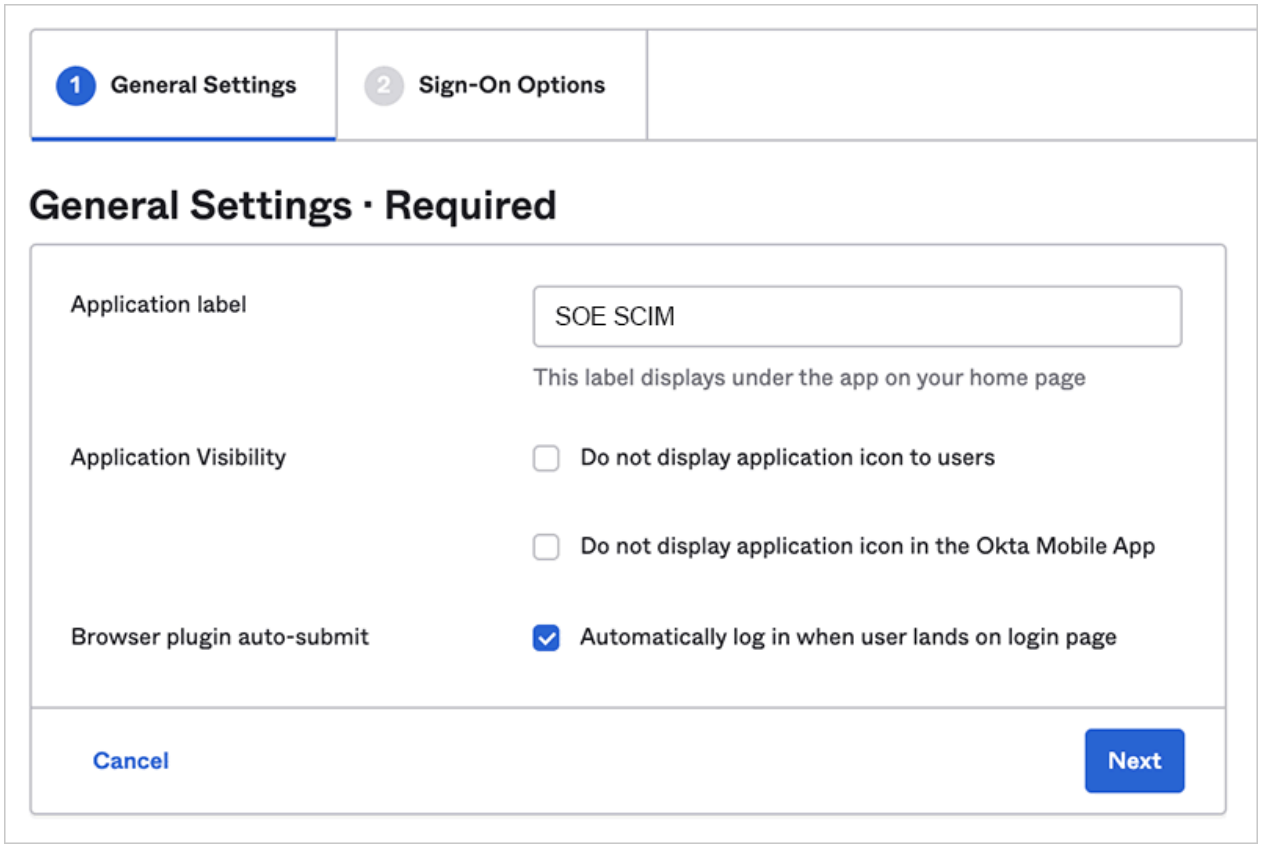
There are two ways to integrate SOE with Okta SCIM: 1) create a new SCIM application in Okta, or 2) create a SCIM connection using an existing SSO connector. Choose the first method only if you want (or need) separation between your SSO and SCIM integrations. If you already have an Okta SSO application configured, we recommend the second method.

Method 1: Create a new SCIM application in Okta

1. From the Applications page in Okta, click **Browse App Catalog**. This takes you to the application directory.
2. Search for **SCIM 2.0 Test App (OAuth Bearer Token)**.
3. Click **Add** to begin the setup.

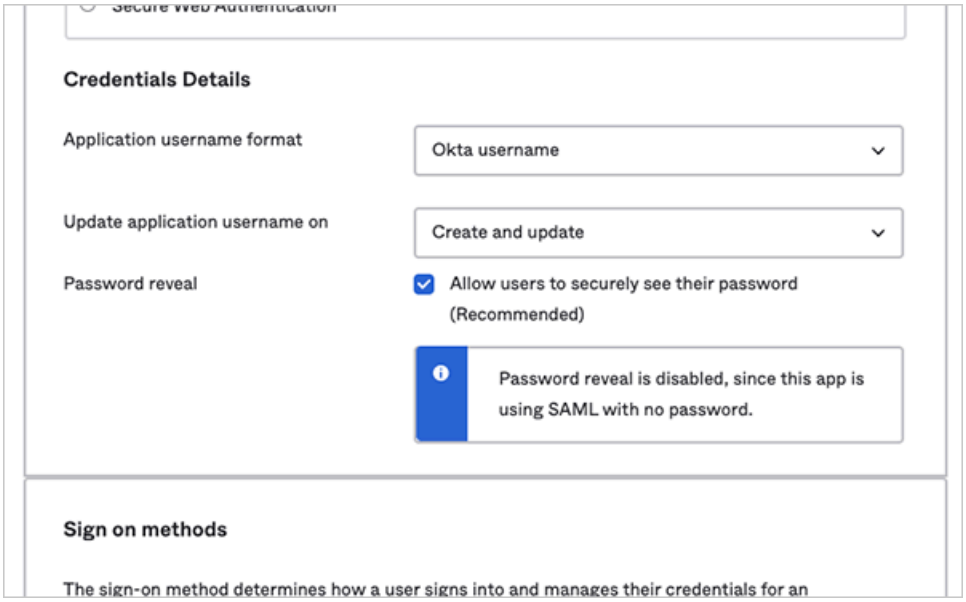


4. Select the General Settings tab.
5. Enter a descriptive name (such as "SOE SCIM") in the **Application label** field. You can leave other settings at their defaults, or change them depending upon your requirements.
6. Click **Next**.

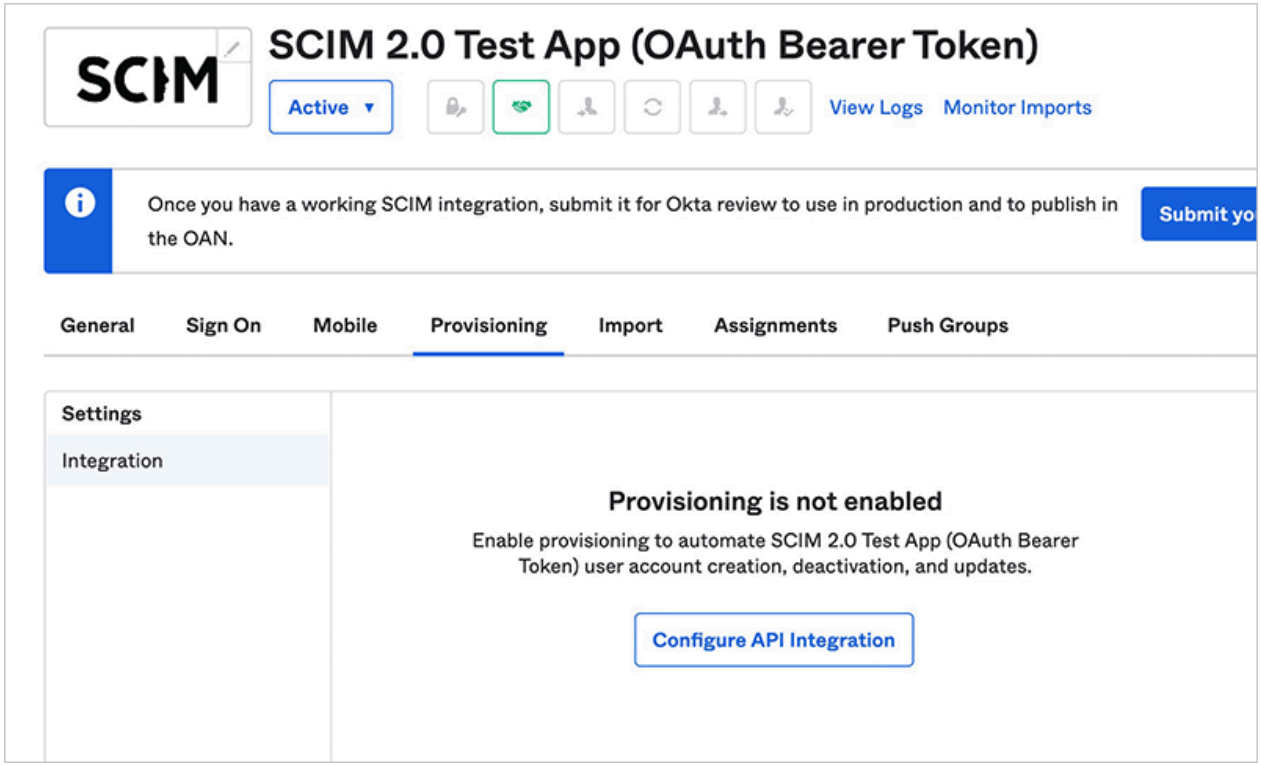


7. Select the Sign-On Options tab.
8. Make sure **Application username format** matches the **User Identifier Assertion** at https://[your_site]/enterprise/auth-settings. This is how SOE properly identifies users.

9. Click **Done**.

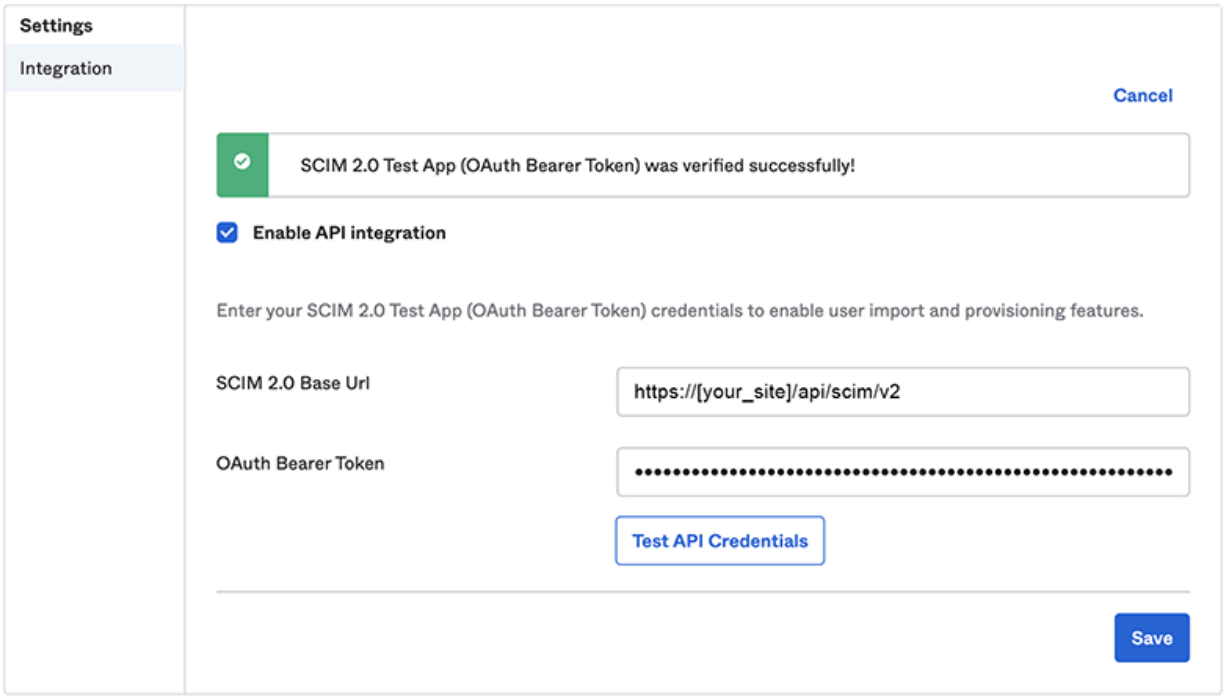


10. Select the Provisioning tab.
11. Click **Configure API Integration**.

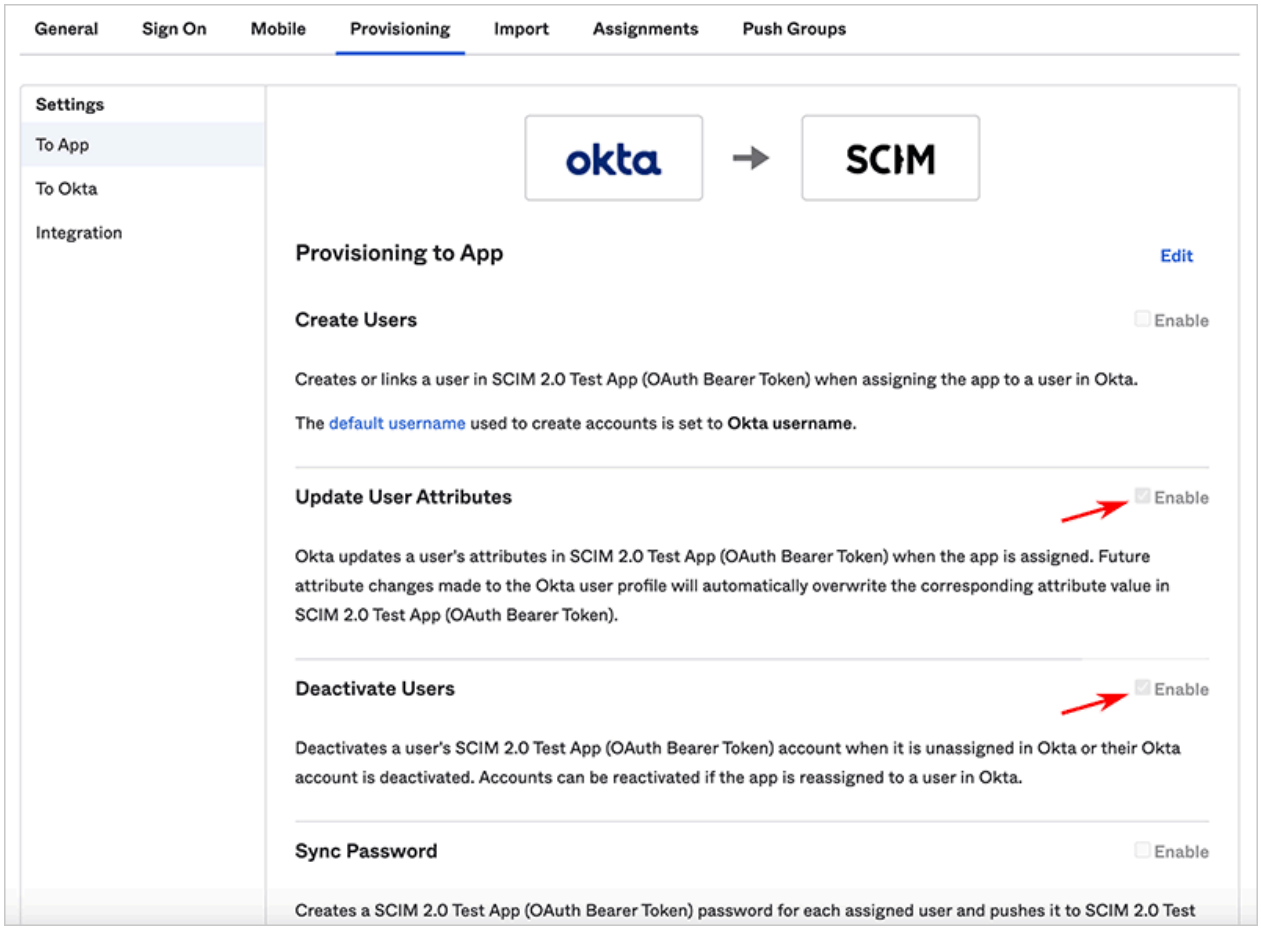


12. Check **Enable API Integration** and set the following parameters:
    - **SCIM 2.0 Base Url** Set to https://[your_site]/api/scim/v2.
    - **OAuth Bearer Token** Enter the **SCIM authorization bearer token** you created on your SOE SCIM settings screen.

13. Click **Test API Credentials**. You should get a "verified" message.
14. Click **Save**.



15. On the Provisioning tab, click the newly available **To App** setting panel.
16. Click **Edit**.
17. Click the checkbox to enable both **Update User Attributes** and **Deactivate Users**.
18. Click **Save**.

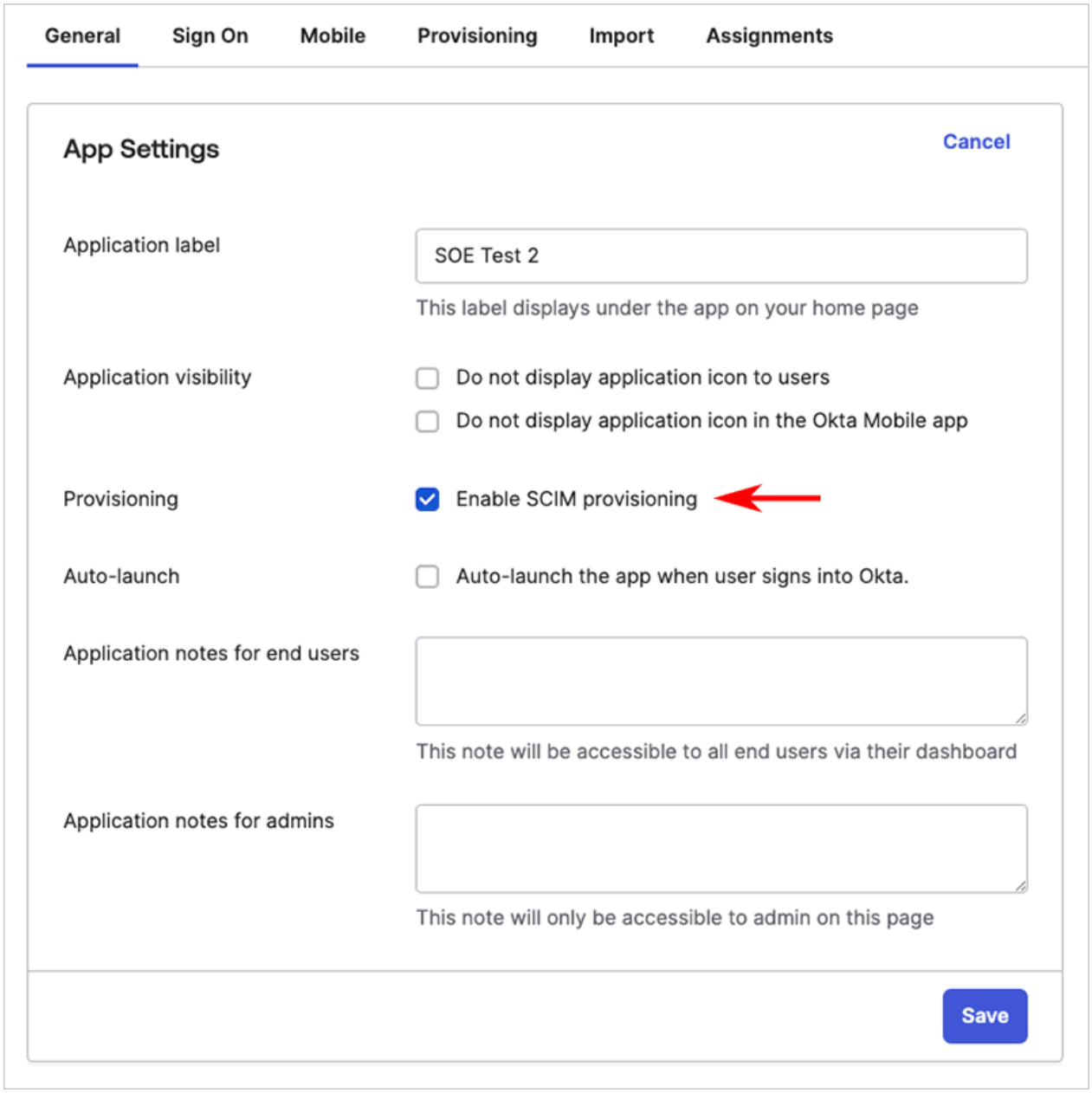


When users are deactivated or reactivated in Okta and are assigned to the appropriate SCIM app, their status should be changed in SOE as well.

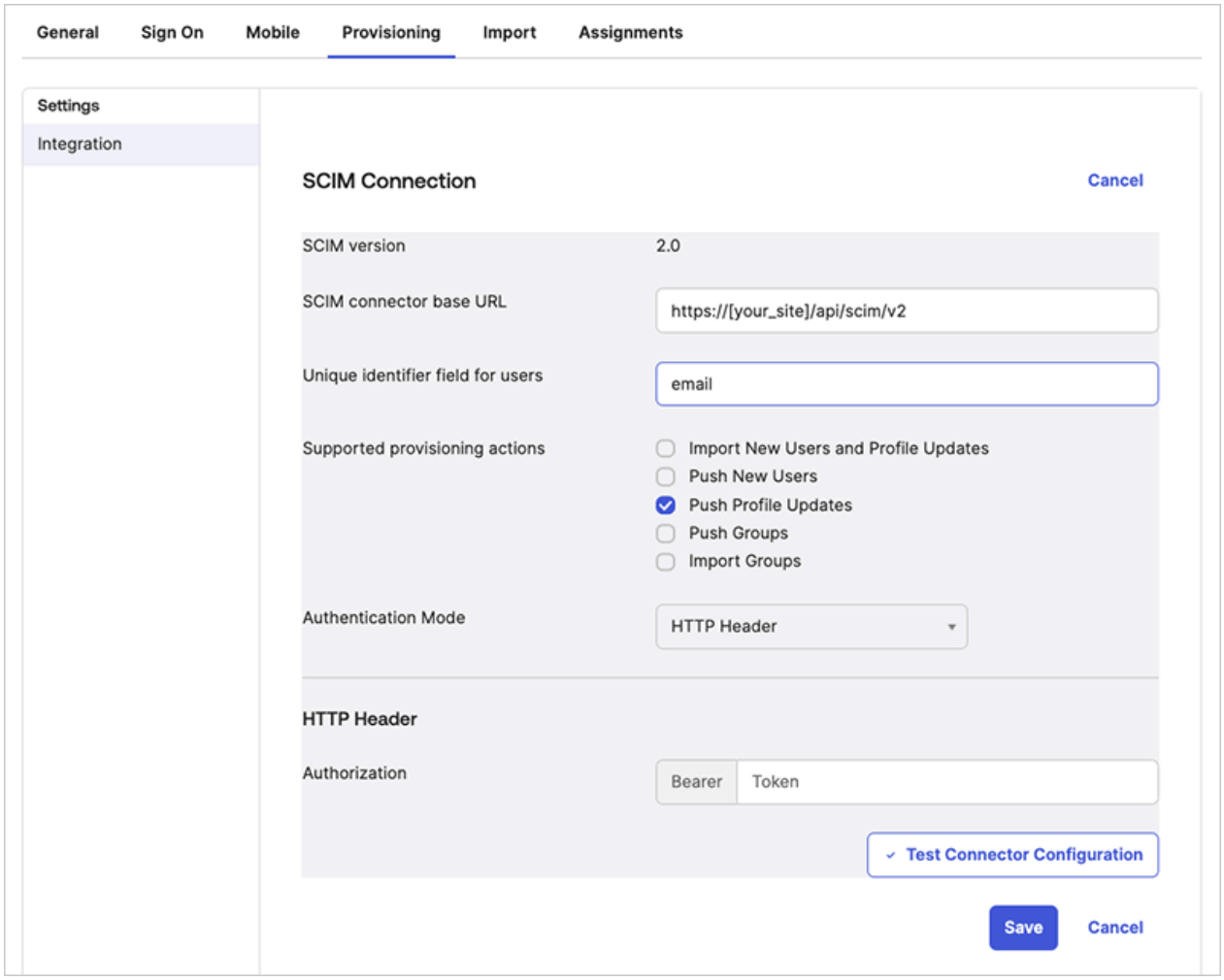
Method 2: Create a SCIM connection using an existing SSO connector

NOTE: *This method assumes you've already followed the instructions in the Configure Single Sign-on (SSO) with Okta article to create an SSO connector.*

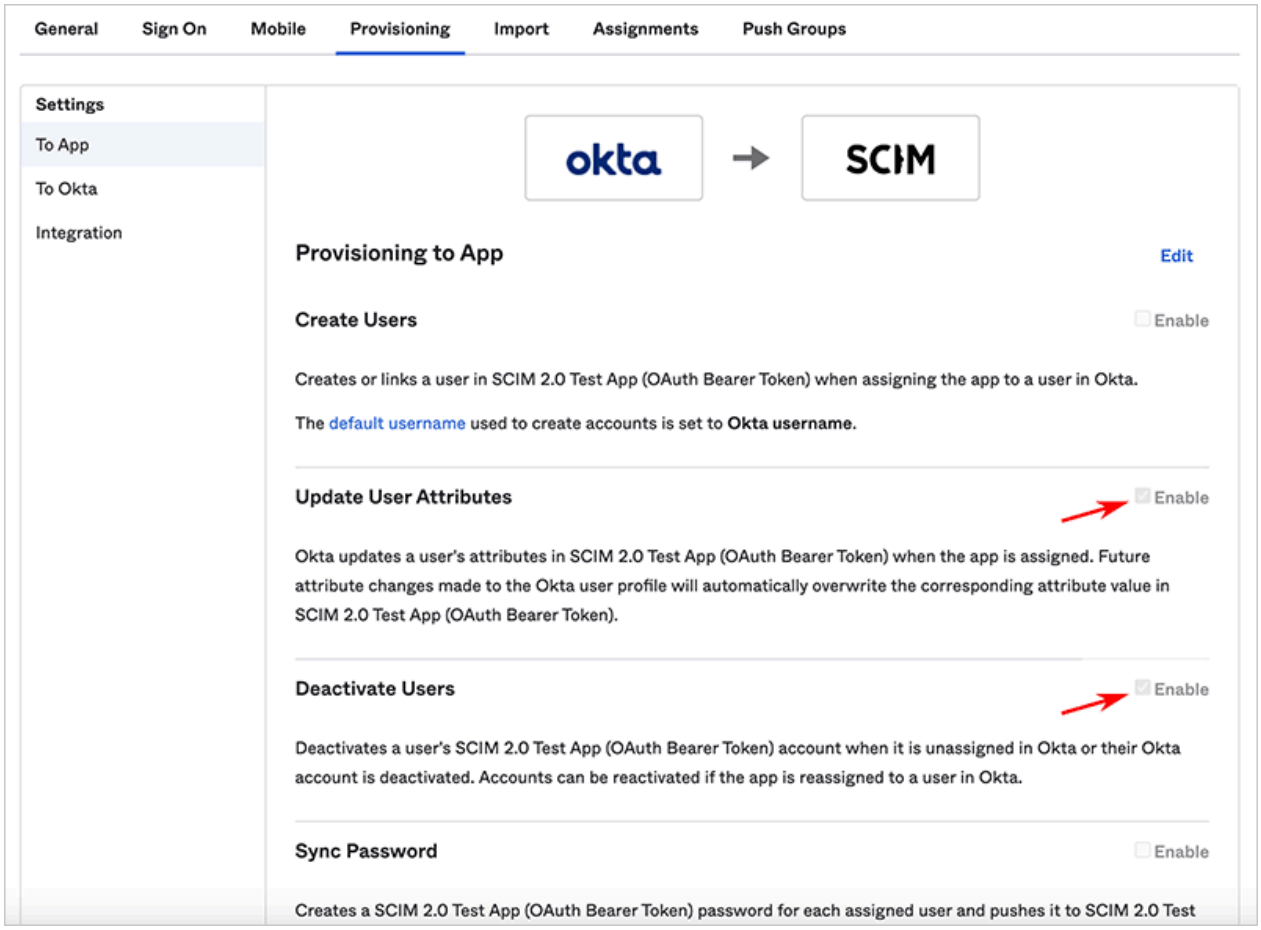
1. In Okta, navigate to your SSO application and select the General tab.
2. Under "App Settings", check **Provisioning** to **Enable SCIM provisioning**.



3. Select the Provisioning tab.
4. Click **Edit** and set the following parameters:
    - **SCIM connector** base URL Set to https://[your_site]/api/scim/v2.
    - **Unique identifier field for users** Set to **email** (this is the default value for Okta).
    - **Supported provisioning actions** Set to **Push Profile Updates** (SOE supports only this option).
    - **Authentication Mode** Set to **HTTP Header**.
    - **Authorization** Set to the SCIM authorization bearer token you created earlier on Stack Overflow.



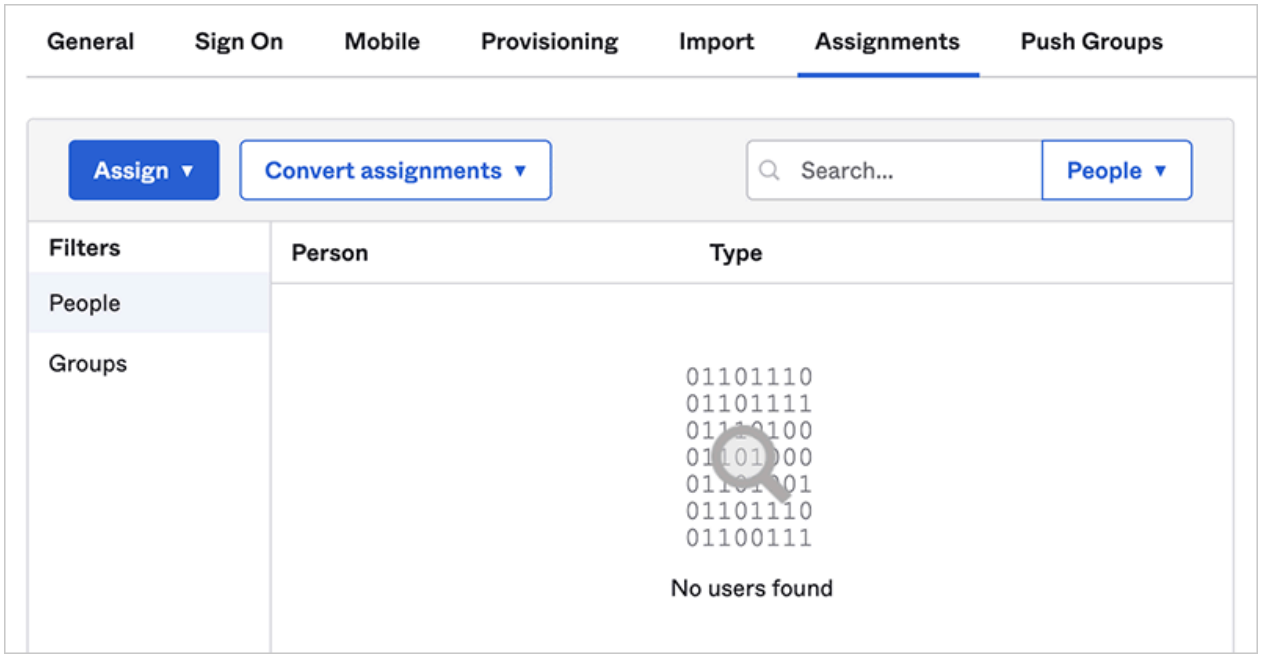
5. Click **Test Connector Configuration**. You should see a "verified" message.
6. Click **Save**.
7. On the Provisioning tab, click the newly available **To App** setting panel.
8. Click **Edit**.
9. Click the checkbox to enable both **Update User Attributes** and **Deactivate Users**.
10. Click **Save**.



Assign users to the SCIM application

Whether you created a new SCIM application (method 1) or added SCIM to an existing SSO application (method 2), the next step is to assign users to the SCIM application.

1. In the SCIM 2.0 application in Okta, click the **Assigments** tab.
2. Add users as appropriate for your organization. This may be by individual, by groups, or a combination of the two.



Configure administrator/moderator promotion and demotion (optional)

You can use SCIM to promote/demote users between administrator, moderator, and regular user roles. This requires enabling **Allow Moderator Promotion via a userType property** and/or **Allow Admin Promotion via a userType property** on the SCIM integration settings page in SOE.

User promotion is determined by the `userType` field in the SCIM payload. SOE will change a user's role based on the following `userType` values: **Registered**, **Moderator**, or **Admin**.

NOTE: *Site administrators users have moderator privileges, but moderators do not have admin privileges.*

You can configure `userType` mapping in Okta in multiple ways, including:

- **On the user profile** Under Directory -> Users, you can edit a user and set the `userType` field under the Profile tab. This must be done for each admin or moderator individually.
- **By application mapping** Under Directory -> Profile Editor, field mappings may be controlled for each application. Click `Mappings` for the SCIM application, then select the `Okta to SCIM 2.0 application label` tab. the `userType` field may be modified to any value or valid Okta expression. For example, you could grant moderator privileges to all users in the group "Stack Overflow Enterprise Moderators" with this Okta expression:

```
isMemberOfGroupName("Stack Overflow Enterprise Moderators") ? "Moderator" : "Registered"
```

NOTE: *Group membership changes are not considered user events and do not trigger SCIM requests in Okta (see "Notes" section, below).*

Notes

- When using groups, please note that group membership changes are not considered a user event. That is if a user is added to or removed from a group in Okta, the user is not considered changed and no SCIM request is sent. After

changing group permissions, have the SCIM application in Okta `Force Sync`. This is a limitation of Okta.

- Enabling SCIM user management in SOE does not disable user management within SOE. A user may be active in Okta and assigned to the SOE SCIM app, and they may still be manually disabled within SOE. We recommend standardizing on a single workflow within your organization so that expectations are shared.