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

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

Document generated 08/08/2025

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.

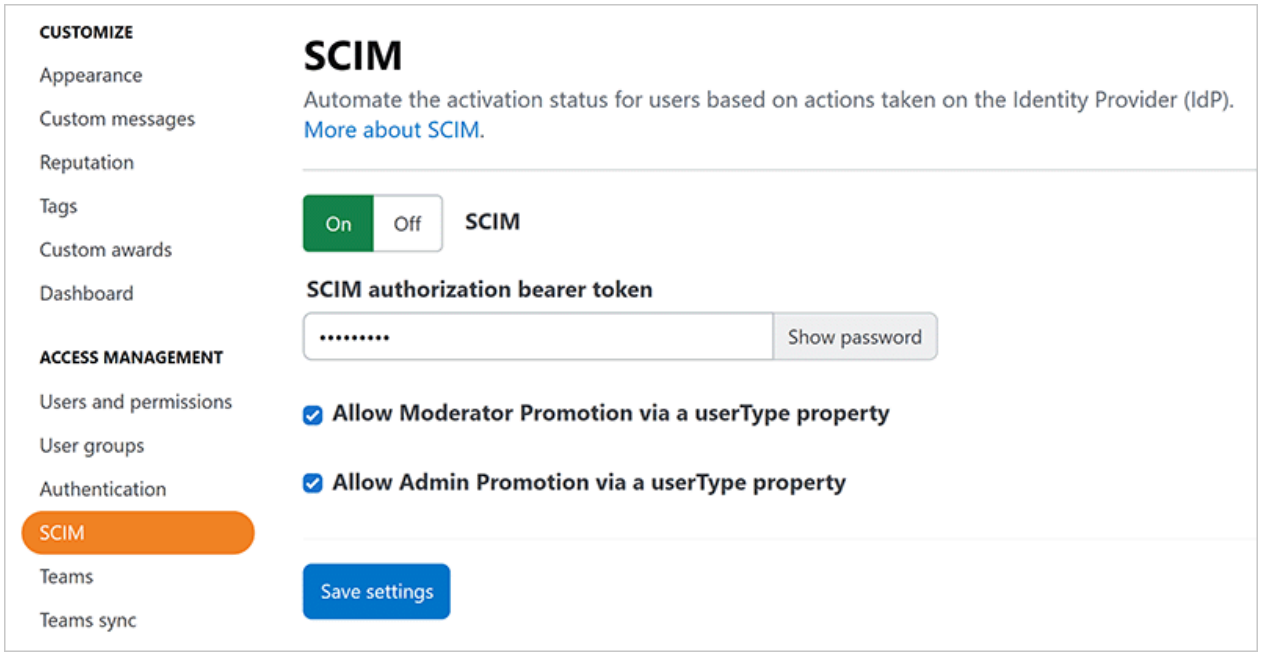
This article covers integrating Okta and your SOE site with SCIM. For a better understanding of using SCIM with SOE, read our SCIM 2.0 support article.

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.

***NOTE:** Setting up SCIM is a continuation of the Okta SAML SSO configuration process. If you haven't yet configured SSO in Okta, start with the Configure Single Sign-on (SSO) with Okta article.*

Configure SCIM in 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**.

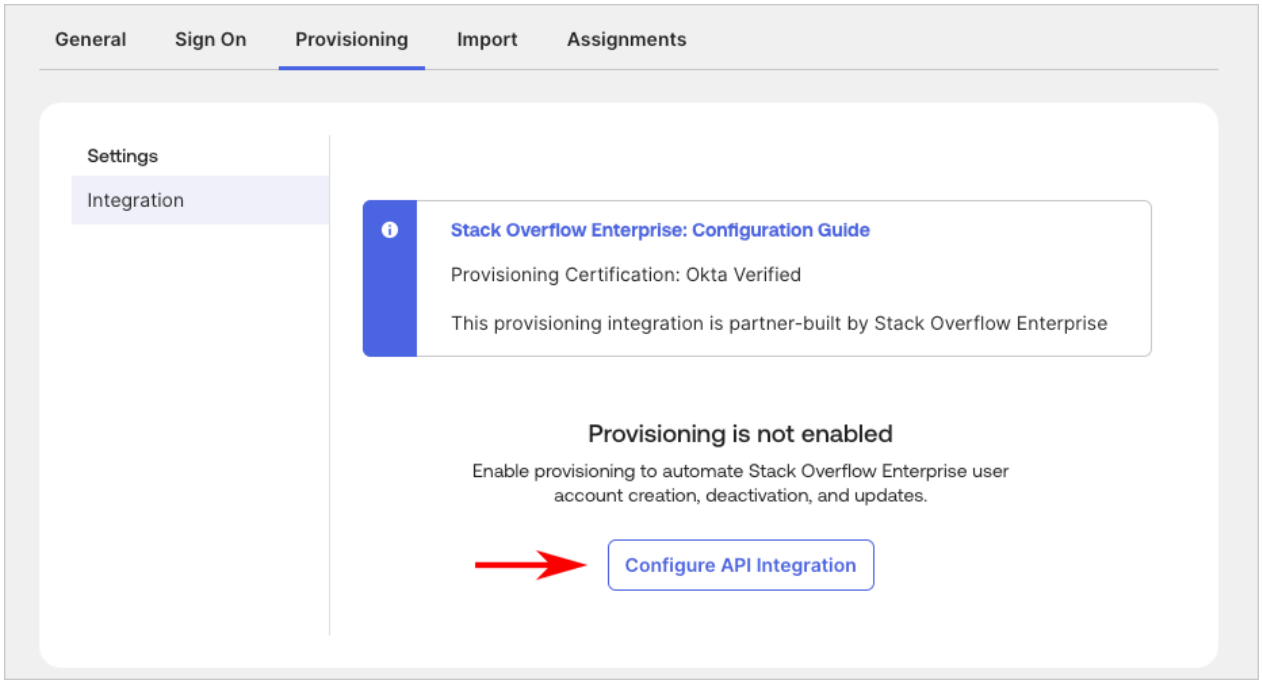
Configure SCIM in Okta

There are two ways to configure SCIM for your SOE site with Okta. We recommend the app integration method below unless you can't (or choose not to) access the Okta App Integration Catalog. If you aren't using the Okta app integration, skip down to the "ALTERNATE MANUAL CONFIGURATION METHOD" section.

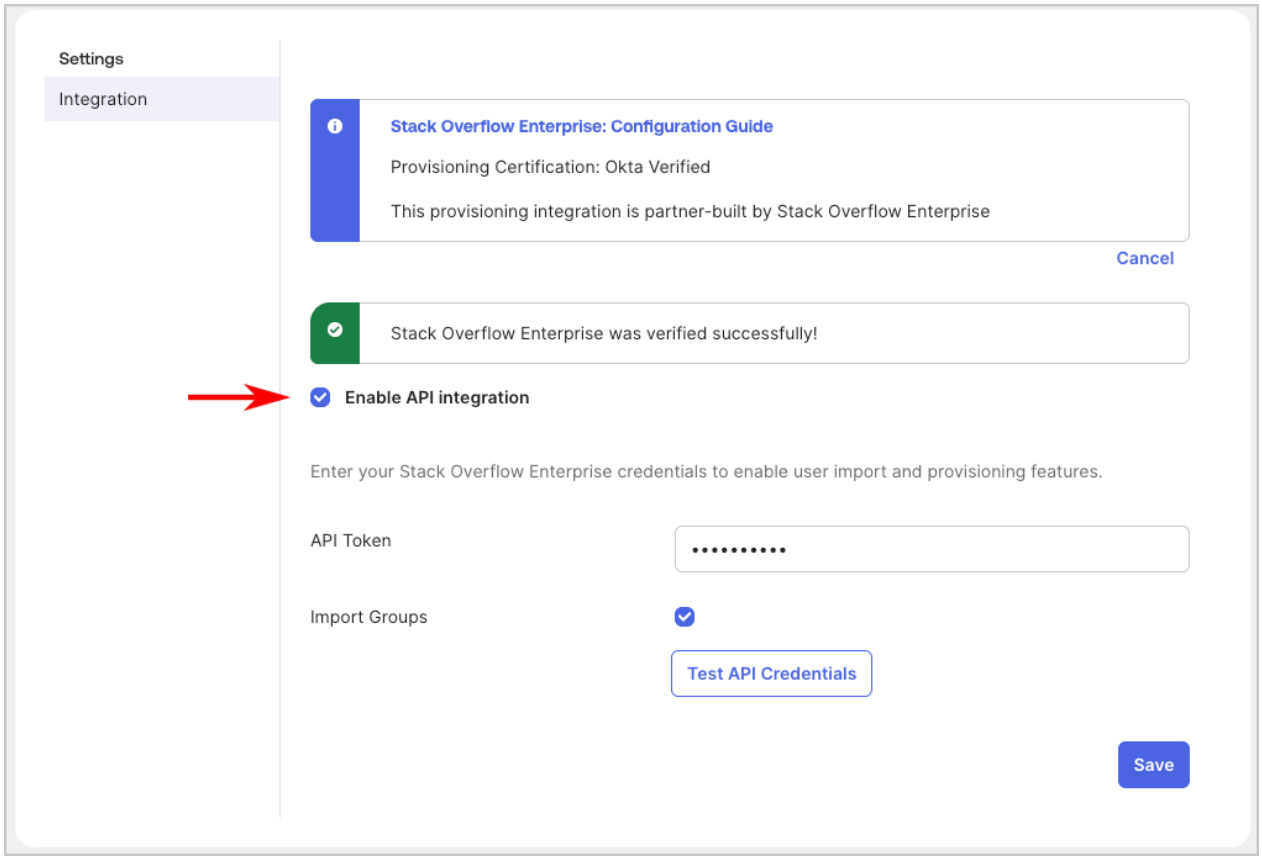
OKTA APP INTEGRATION METHOD

Return to the Stack Overflow Enterprise application you configured in the Configure Single Sign-on (SSO) with Okta article.

1. Select the "Provisioning" tab, and click **Configure API Integration**.



2. Check **Enable API Integration**.

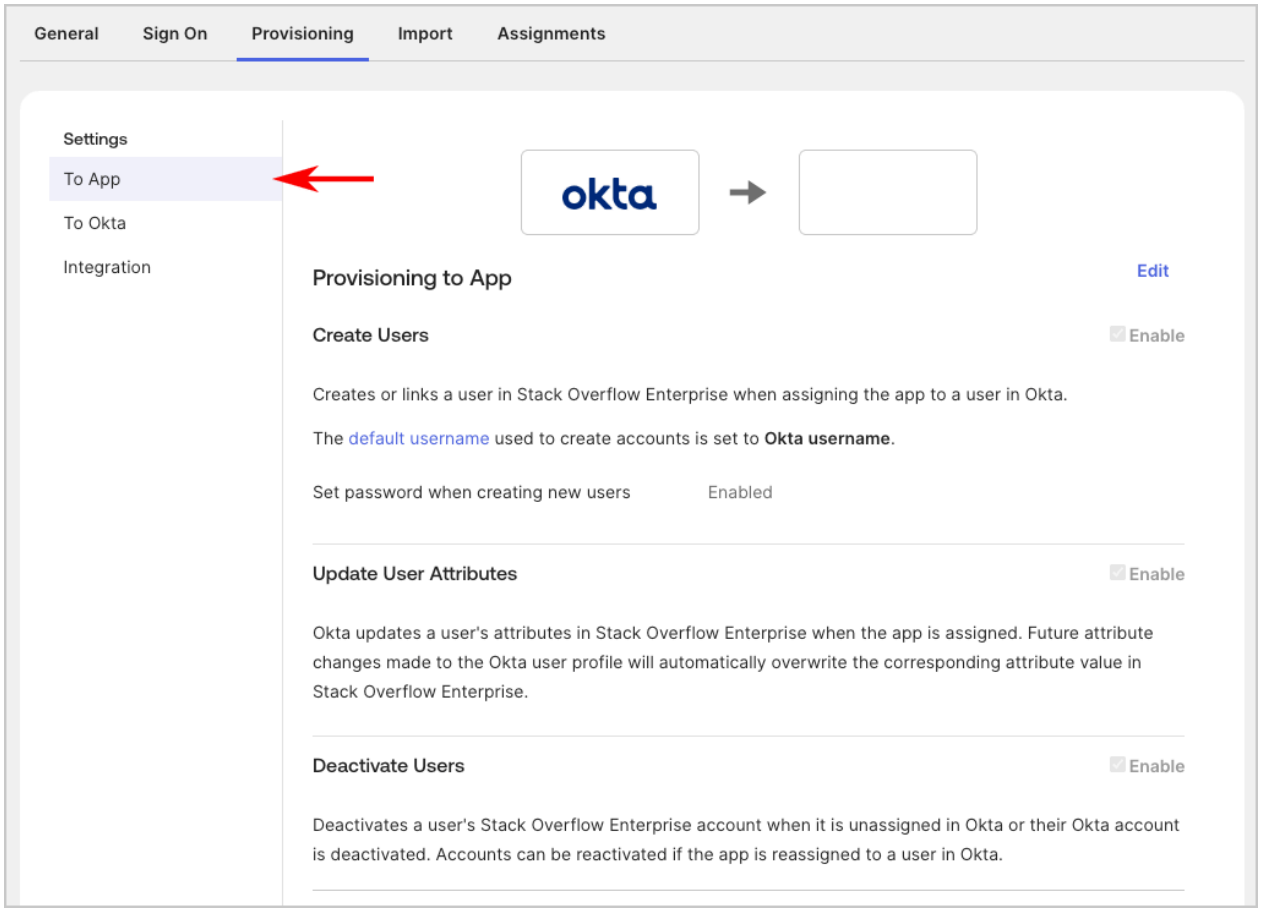


3. Set the following parameters.

- **SCIM 2.0 Base Url** Set to https://[your_site].stackenterprise.co/api/scim/v2.

- **OAuth Bearer Token** Enter the SCIM authorization bearer token you created on your SOE SCIM settings page.

4. Click **Test API Credentials**. You should get a "verified" message.
5. Click **Save**.
6. Click the "Provisioning" tab, then **To App** in the left-hand menu.



7. Click the "Provisioning to App" **Edit** link.
8. Click the checkboxes to enable **Create Users**, **Update User Attributes**, and **Deactivate Users**.
9. Click **Save**.

When you deactivate or reactivate users assigned to this Okta SCIM app, the SCIM process will change their status on your SOE site as well.

ALTERNATE MANUAL CONFIGURATION METHOD

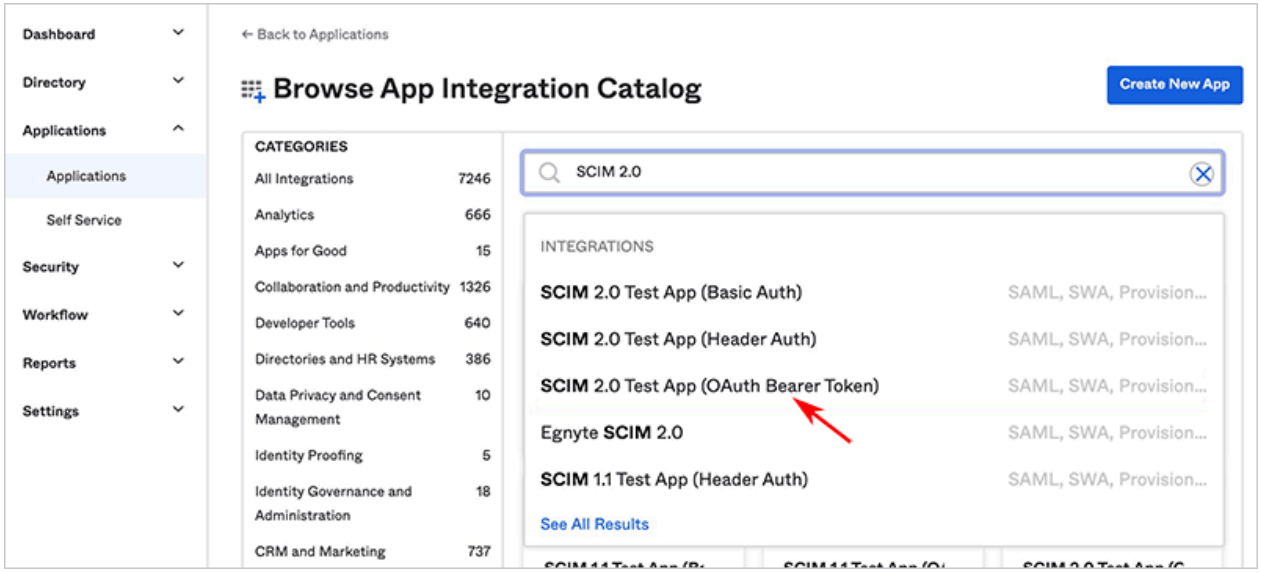
NOTE: *The following steps allow for manual configuration of an Okta SCIM integration that remains separate from your Okta SSO integration. Use this process if you can't (or choose not to) access the Okta App Integration Catalog.*

In Okta, you'll create a new SCIM application to integrate with SOE. This allows you to maintain separation between your SSO and SCIM integrations.

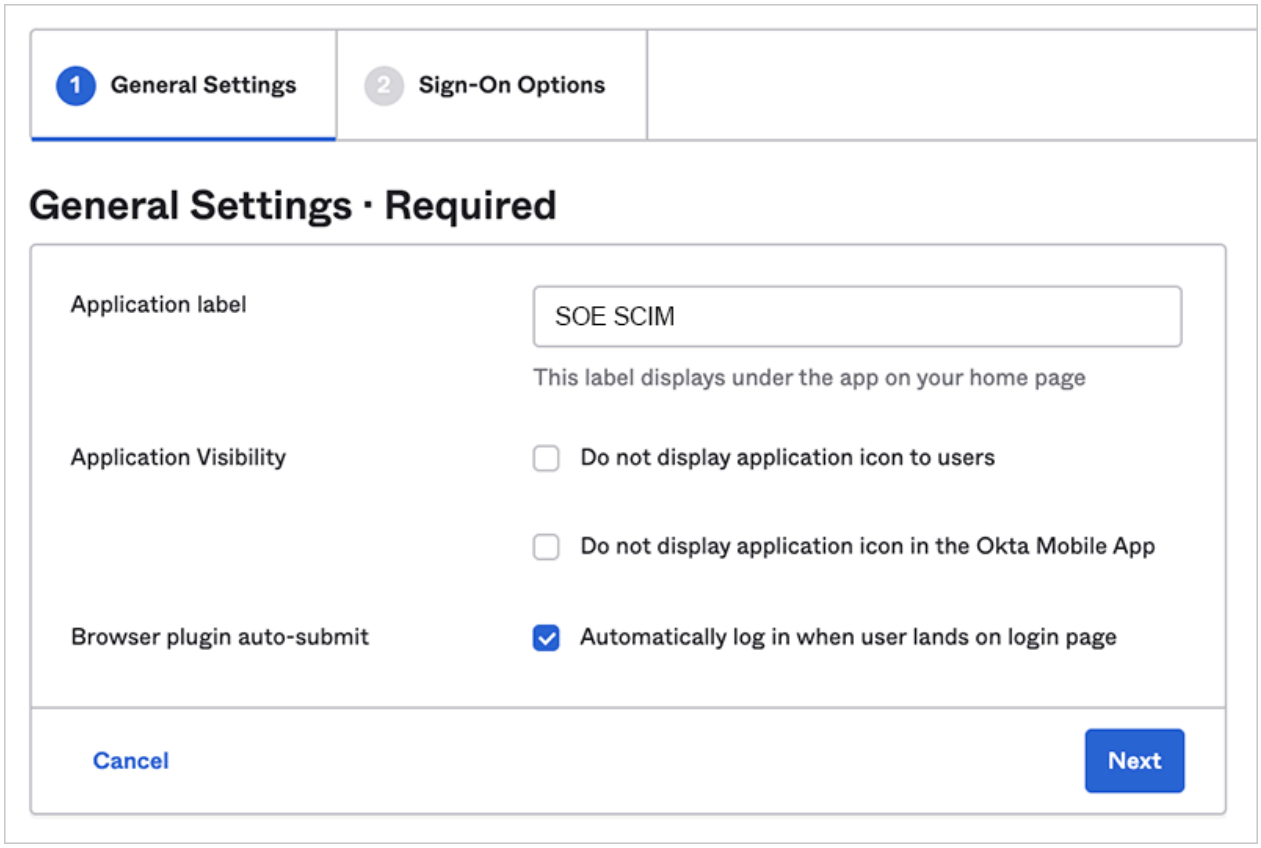
NOTE: *Even if you have an existing Okta SSO application configured, you'll need to create a new SCIM application for this integration.*

Create a new SCIM application in Okta

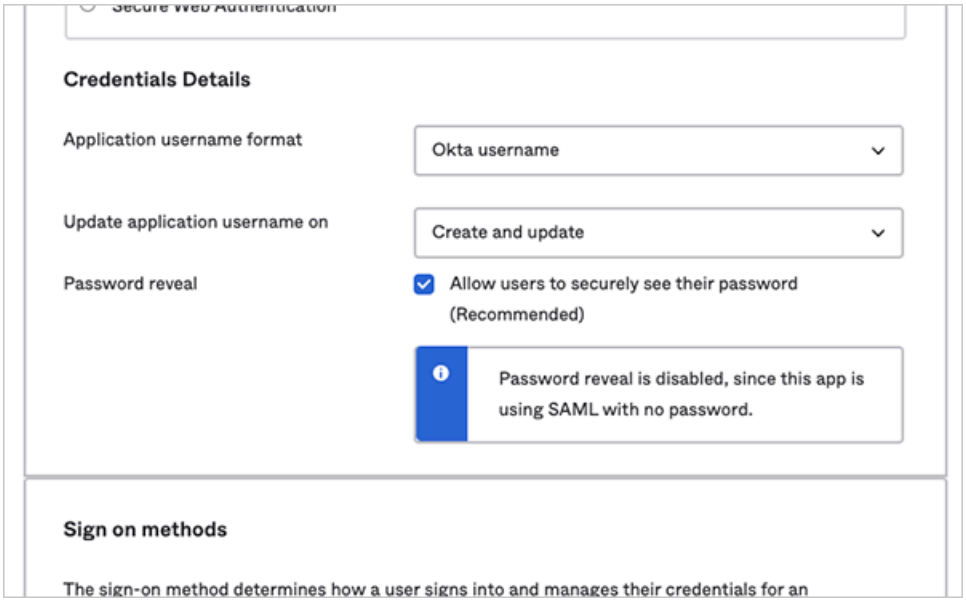
1. From the Applications page in Okta, click **Browse App Catalog**. This takes you to the application directory.
2. Search for **SCIM 2.0 Test App (OAuth Bearer Token)**.
3. Click **Add** to begin the setup.



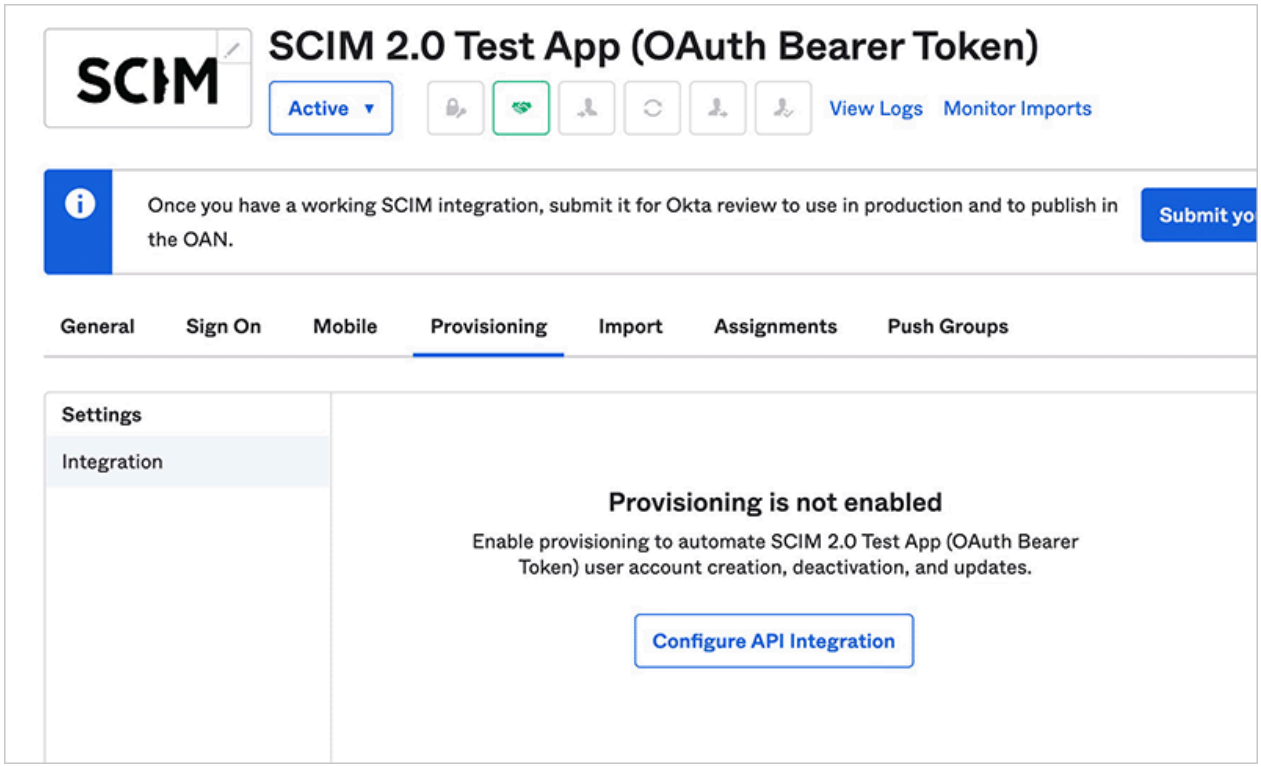
4. Select the "General Settings" tab.
5. Enter a descriptive name (such as "SOE SCIM") in the **Application label** field. You can leave other settings at their defaults, or change them depending upon your requirements.
6. Click **Next**.



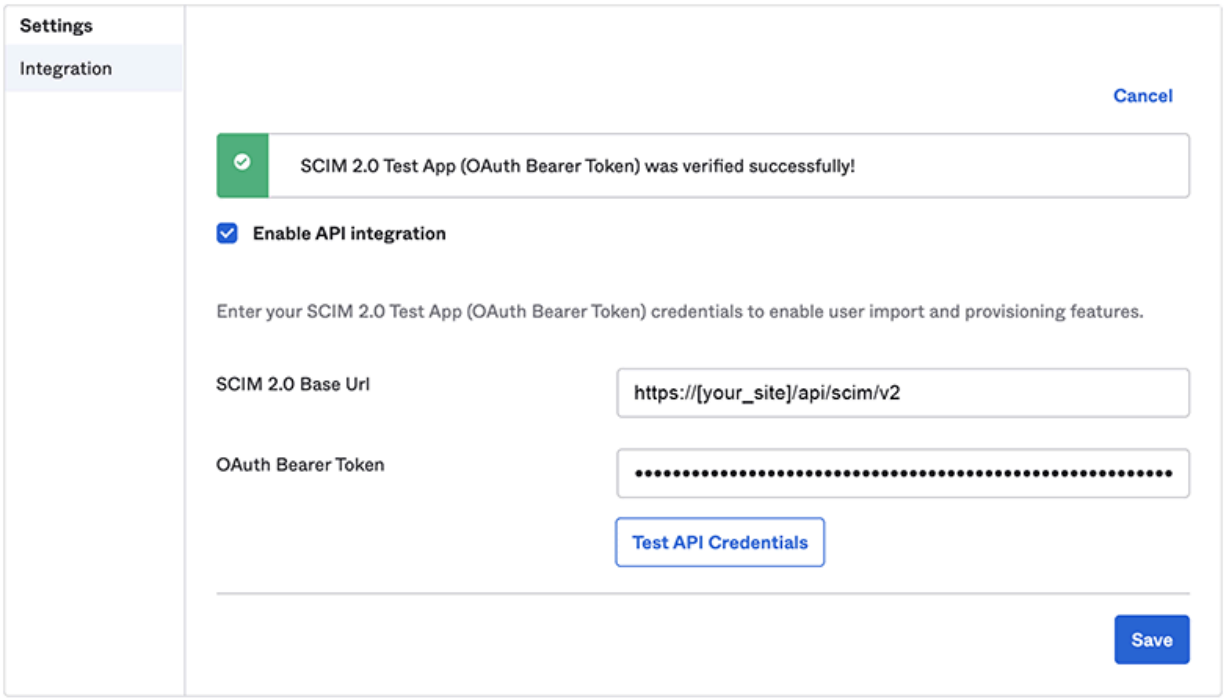
7. Select the "Sign-On Options" tab.
8. Make sure **Application username format** matches the **User Identifier Assertion** at https://[your_site].stackenterprise.co/enterprise/auth-settings. This is how SOE properly identifies users.
9. Click **Done**.



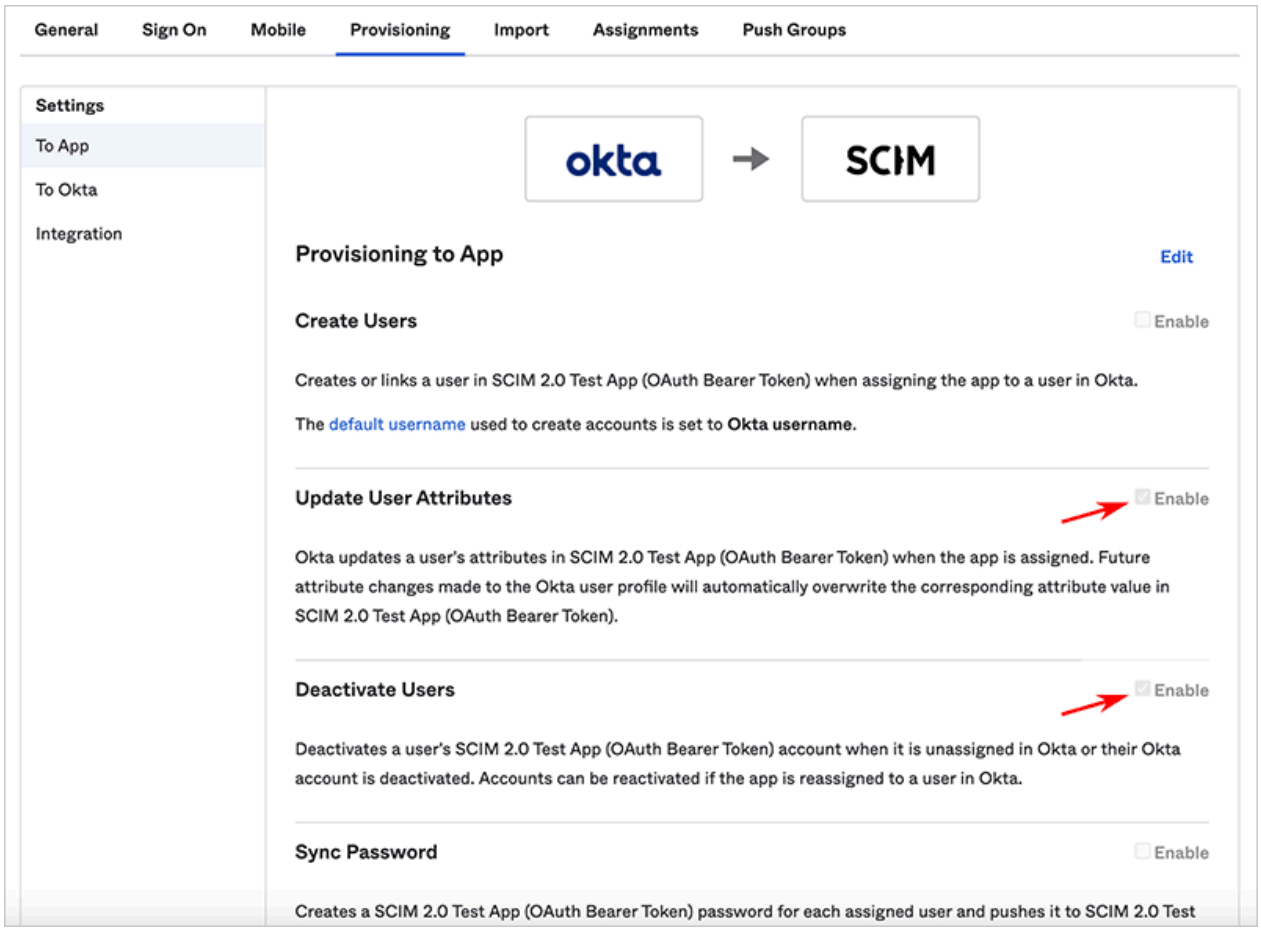
10. Select the "Provisioning" tab.
11. Click **Configure API Integration**.



12. Check **Enable API Integration** and set the following parameters:
    - **SCIM 2.0 Base Url** Set to https://[your_site].stackenterprise.co/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. Click the "Provisioning" tab, then **To App** in the left-hand menu.

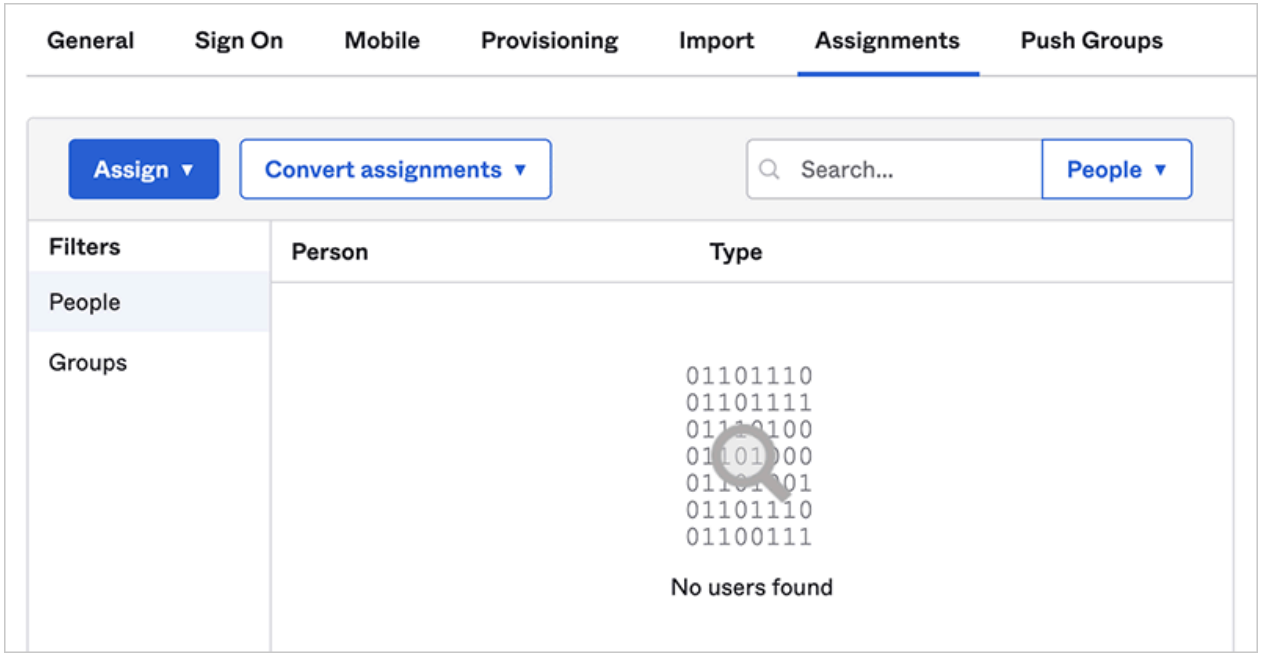


16. Click the "Provisioning to App" **Edit** link.
17. Click the checkboxes to enable **Create Users**, **Update User Attributes**, and **Deactivate Users**.
18. Click **Save**.

When you deactivate or reactivate users assigned to this Okta SCIM app, the SCIM process will change their status on your SOE site as well.

Assign users to the SCIM application

1. In the SCIM 2.0 application in Okta, click the "Assignments" tab.
2. Assign your users (and/or groups) with the **Assign** button.



BOTH METHODS: 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 user groups, Okta does not consider group membership changes to be a user event. If you add or remove a user in an Okta group, Okta will not send a SCIM request to SOE. To update your SOE site after changing a group roster in Okta, click **Force Sync**. This is a known limitation of Okta.
- **Manual method only:** enabling automatic user management by SCIM does not disable manual user management in SOE. An admin can disable a user in SOE, for example, without changing their status in Okta. Okta and SOE will then be out-of-sync. We recommend standardizing on a single user management workflow (Okta only or SOE in-app only– not both) to avoid confusion.