

## Configure SCIM with Okta

### How to integrate Stack Overflow for Teams with the Okta identity provider.

Document generated 12/05/2024

[PDF VERSION](#)

Tags | [SCIM](#) | [Provisioning](#) | [Okta](#) |

#### ADMIN PRIVILEGES REQUIRED

Applies to: Free Basic Business Enterprise

Enterprise users can access their documentation [here](#). [Find your plan](#).

## Overview

SCIM is an open API for securely sharing user information between online systems. In Stack Overflow for Teams Basic and Business, SCIM 2.0 support allows an Identity Provider (IdP) to automatically update Stack Overflow with the user's activation status and/or role. This article details how to integrate Stack Overflow for Teams and the Okta IdP.

---

**THIS ARTICLE APPLIES TO STACK OVERFLOW FOR TEAMS BASIC AND BUSINESS ONLY.**

Stack Overflow for Teams Enterprise users should read [this article](#) instead. [Find your plan](#).

## Create a SCIM 2.0 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.

← Back to Applications

## Browse App Integration Catalog

Create New App

Search: SCIM 2.0

CATEGORIES	Count
All Integrations	7246
Analytics	666
Apps for Good	15
Collaboration and Productivity	1326
Developer Tools	640
Directories and HR Systems	386
Data Privacy and Consent Management	10
Identity Proofing	5
Identity Governance and Administration	18
CRM and Marketing	737

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

See All Results

## Okta General Settings tab

Set the **Application label** with a descriptive name (such as "Stack Overflow SCIM"). You can leave other settings at their defaults, or change them depending upon your requirements. Click **Next**.

1 General Settings    2 Sign-On Options

### General Settings · Required

Application label: Stack Overflow SCIM  
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

Cancel    Next

## Okta Sign-On Options tab

Make sure **Application username format** matches the **User Identifier Assertion** provided in /enterprise/auth-settings. This is how SOE properly identifies users. Click **Done**.

**Secure Web Authentication**

**Credentials Details**

Application username format: Okta username

Update application username on: Create and update

Password reveal:  Allow users to securely see their password (Recommended)

Password reveal is disabled, since this app is using SAML with no password.

**Sign on methods**

The sign-on method determines how a user signs into and manages their credentials for an

## Set up user deactivation and reactivation

To access the SCIM integration page, click **Admin Settings** in the Stack Overflow for Teams left-hand menu, then **SCIM integration** under the "ACCESS MANAGEMENT" heading. Click **Enable SCIM**, then click **Generate token**.

**SCIM integration**

System for Cross-domain Identity Management (SCIM) is a technology that connects your Identity Provider with Stack Overflow for Teams.  
Read our [implementation guide](#) for help with setup.

**Enable SCIM**

**Generate a SCIM authorization token**  
You'll need an authorization token to configure your Identity Provider.

**Generated**

**Save this token**  
You will not be able to retrieve this token again after reloading the page, so make sure you save it in a secure location. If your token is lost you can generate a new one, but your Identity Provider will need to be reconfigured with the new token.

72000eb66c66ba-----9310eb62a79

**Allow SCIM to manage user roles**  
Checking this box will allow you to promote and demote users from admin status using SCIM.

Note that this token will only be visible when you generate it. If you lose it, you'll need to generate a new token and reconfigure your Okta application.

If you plan to use SCIM 2.0 for administrator/moderator role promotion and demotion, check **Allow SCIM to manage user roles**.

Navigate to your SCIM 2.0 application in Okta. Click the Provisioning tab, then click **Configure API Integration**.

The screenshot shows the Okta management interface for a SCIM 2.0 Test App (OAuth Bearer Token). The app is currently in an 'Active' state. The 'Provisioning' tab is selected, and a message states: 'Provisioning is not enabled. Enable provisioning to automate SCIM 2.0 Test App (OAuth Bearer Token) user account creation, deactivation, and updates.' A 'Configure API Integration' button is prominently displayed. The left sidebar shows 'Settings' and 'Integration' options. The top navigation includes 'General', 'Sign On', 'Mobile', 'Provisioning', 'Import', 'Assignments', and 'Push Groups'.

Check (enable) **Enable API Integration** and set the following parameters:

- **SCIM 2.0 Base Url** `https://stackoverflowteams.com/c/[your_site]/auth/scim/v2`.
- **OAuth Bearer Token** The token that you generated previously in Stack Overflow for Teams.

Click **Test API Credentials**. You should get a positive (verified) result. Click **Save**.

**Settings**

Integration

[Cancel](#)

✔ SCIM 2.0 Test App (OAuth Bearer Token) was verified successfully!

**Enable API integration**

Enter your SCIM 2.0 Test App (OAuth Bearer Token) credentials to enable user import and provisioning features.

SCIM 2.0 Base Url

OAuth Bearer Token

[Test API Credentials](#)

---

[Save](#)

On the Provisioning tab, click the newly available **To App** setting panel. Then:

1. Click **Edit**.
2. Click the checkbox to enable both **Update User Attributes** and **Deactivate Users**.
3. Click **Save**.

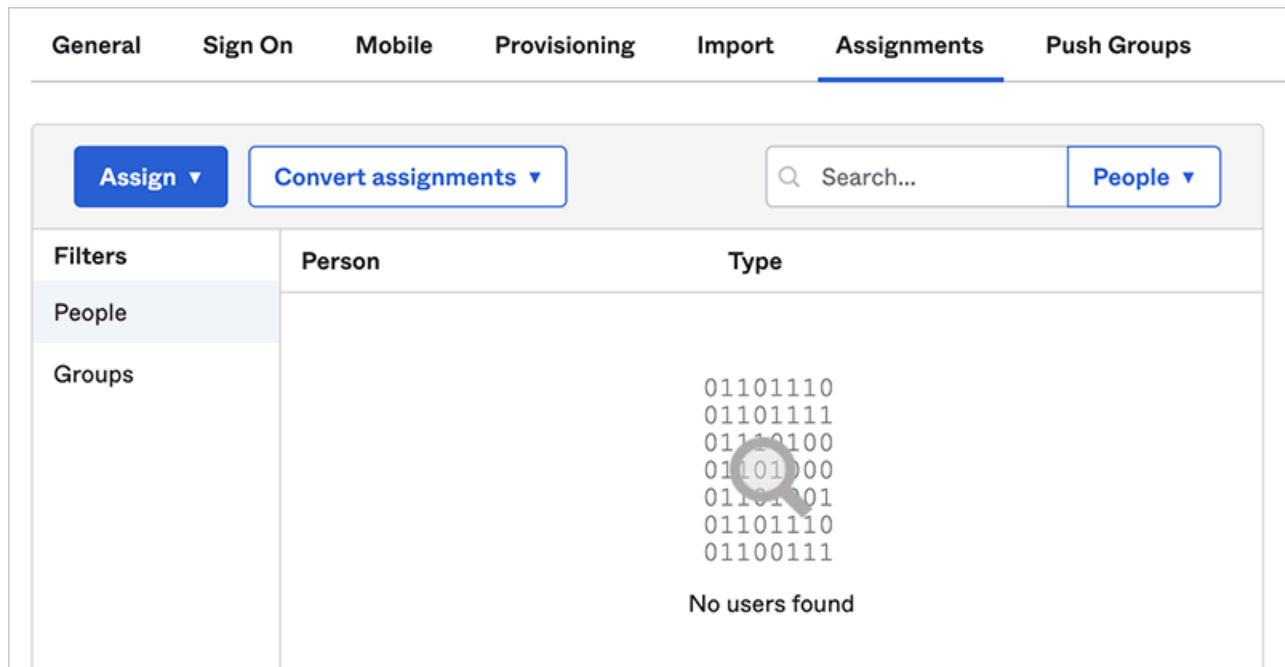
The screenshot shows the Okta Provisioning settings for a SCIM 2.0 Test App. The navigation tabs at the top are General, Sign On, Mobile, Provisioning (selected), Import, Assignments, and Push Groups. On the left, the Settings menu includes To App (selected), To Okta, and Integration. The main content area is titled 'Provisioning to App' and features a diagram showing 'Okta' pointing to 'SCIM'. Below this, there are four settings:

- Create Users**:  Enable. Description: Creates or links a user in SCIM 2.0 Test App (OAuth Bearer Token) 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. Description: Okta updates a user's attributes in SCIM 2.0 Test App (OAuth Bearer Token) 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 (OAuth Bearer Token). A red arrow points to the 'Enable' checkbox.
- Deactivate Users**:  Enable. Description: Deactivates a user's SCIM 2.0 Test App (OAuth Bearer Token) 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. A red arrow points to the 'Enable' checkbox.
- Sync Password**:  Enable. Description: Creates a SCIM 2.0 Test App (OAuth Bearer Token) password for each assigned user and pushes it to SCIM 2.0 Test

When users are deactivated or reactivated in Okta and are assigned to the appropriate SCIM 2.0 app, their status should be changed in Stack Overflow Business as well.

## Assign users to the SCIM 2.0 application

The SCIM 2.0 application should be open in Okta. Click the Assignments tab, and add users as appropriate for your organization. This may be by individual, by groups, or a combination of the two approaches. Continue on to the next section to finish the integration and enable deactivation/reactivation.



## Set up administrator/moderator promotion and demotion (optional)

You can use SCIM 2.0 to promote/demote users between administrator, moderator, and regular user roles. This requires enabling **Allow SCIM to manage user roles** on the SCIM Integration settings page on Stack Overflow for Teams.

User role is determined by the `userType` field in the SCIM 2.0 payload. This field can have the value of "Registered", "Moderator", or "Admin".

You can set `userType` value in Okta in several ways, including:

- On the individual user profile under **Directory** -> **Users**, edit the user and set the `userType` field under the Profile tab. You'll have to do this for every user you want to promote to moderator or administrator.
- At **Directory** -> **Profile Editor**, you can control field mappings at the application (Stack Overflow for Teams) level. Click **Attribute Mappings** for the SCIM 2.0 application, then select the **Okta to SCIM 2.0** application label tab. You can now assign the `userType` field to any value or valid [Okta expression](#). For example, you could assign the administrator role to all users in the group "Stack Overflow for Business Admins" with this Okta ternary expression:

```
isMemberOfGroupName("Stack Overflow for Business Admins") ? "Admin" : "Registered"
```

## Notes

- Okta doesn't always initiate a SCIM 2.0 user update based on group membership changes. If you add a user to a group, for example, Okta may not automatically push that change to Stack Overflow for Teams. After changing group memberships, have the SCIM 2.0 application in Okta perform a force sync. This is a known limitation of Okta.
- Enabling SCIM 2.0 support does not disable user management options within Stack Overflow for Teams. This means a user may have an active status in the IdP, yet be deactivated in Stack Overflow for Teams through the admin user

management settings. We recommend standardizing on a single provisioning workflow within your organization to avoid confusion.

---

Need help? Submit an issue or question through our [support portal](#).