Stack Overflow Enterprise Documentation

System for Cross-domain Identity Management (SCIM) 2.0 Support

An overview of the SCIM 2.0 implementation in Stack Overflow for Teams Enterprise.

Document generated 12/06/2024

PDF VERSION

Tags | **Security** | **Authentication** | **SCIM** |

Applies to: Free Basic Business Enterprise

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

Supported activites

The SCIM integration supports the following activities for users that have already been created in SOE:

- Deactivate a user.
- Reactivate a deactivated user.
- Promote/demote a user between administrator, moderator, and regular user roles.

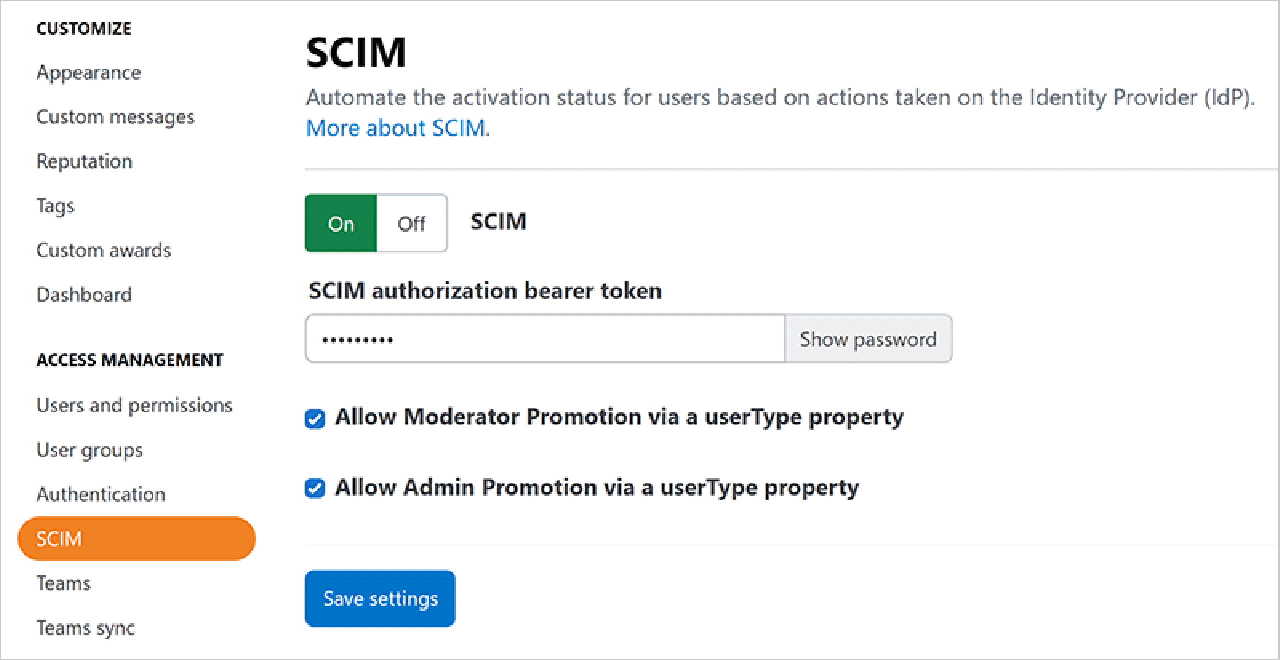
SOE's SCIM integration *will not* create users. Users must still log in with a valid assertion from their IdP to create an account. That is, Stack Overflow uses "just in time" provisioning when a user presents a valid identity assertion. It does not support user creation over SCIM.

Enabling SCIM support does not disable user management options within SOE. This means a user may have an active status in the IdP, yet be deactivated in SOE through the admin user management settings. We recommend standardizing on a single provisioning workflow within your organization to avoid confusion.

Configure SCIM support on SOE

The SCIM configuration on SOE is the same regardless of IdP.

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



SCIM

Automate the activation status for users based on actions taken on the Identity Provider (IdP). More about SCIM.

On | Off SCIM

SCIM authorization bearer token

•••••••••

☑ Allow Moderator Promotion via a userType property

☑ Allow Admin Promotion via a userType property

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 Entra ID. 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 the Identity Provider

The following instructions are general instructions for SCIM compliant systems. If you're using one of the following IdPs, follow the links for detailed configuration information.

- Okta
- OneLogin
- Microsoft Entra ID

The IdP must send SCIM requests to https://[your_site]/api/scim/v2. In addition, the IdP must send the following values part of the user resource to correctly map the user and set their status:

- `userName` The user ID (must match the **User Identifier Assertion** at https://[your_site]/enterprise/auth-settings).

- `active` (**true**/**false**) Determines whether or not the user should be deactivated or reactivated in SOE.
- Required fields for SCIM (these are commonly mapped for you by your IdP, requiring no action on your part):
  - `name.givenName`
  - `name.familyName`
  - `emails`
- `userType` (optional) Requires enabling **Allow Moderator Promotion via a userType property** and/or **Allow Admin Promotion via a userType property** on the SCIM Integration settings page on SOE. SOE will change a user's role based on the following `userType` values: **Registered**, **Moderator**, or **Admin**.

NOTE: *Microsoft Entra ID SCIM doesn't support user role promotion or demotion.*

If your IdP does not support SCIM, an alternative is to have a separate application issuing the SCIM API calls to https://[your_site]/api/scim/v2 as outlined above.

If you need further support or have questions, contact your site administrator.