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

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

Document generated 12/06/2024

PDF VERSION

Tags | **Provisioning** | **OneLogin** | **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

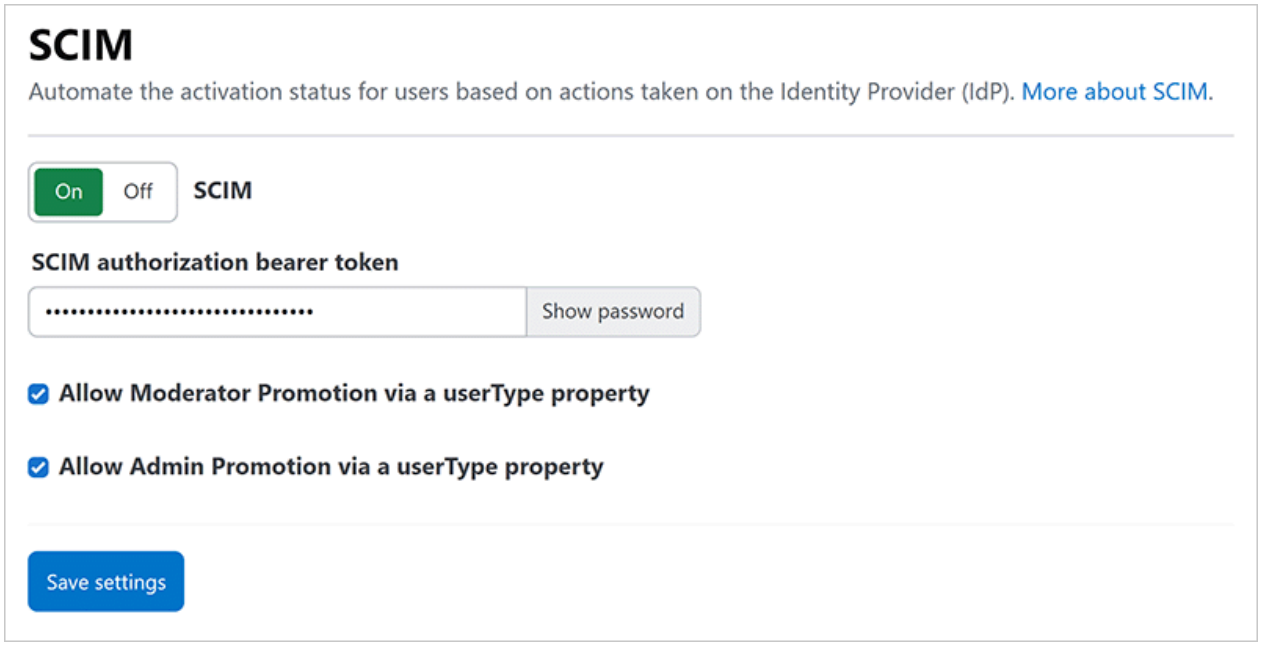
System for Cross-domain Identity Management (SCIM) is an open API for securely sharing user information between online systems. In Stack Overflow for Teams Enterprise (SOE), SCIM 2.0 support allows an Identity Provider (IdP) to automatically update Stack Overflow with the user's activation status and/or 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 OneLogin and your SOE site with SCIM. For a better understanding of using SCIM with SOE, read our SCIM 2.0 support article.

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 OneLogin. 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**.

Create a SCIM application in OneLogin

OneLogin has an article on creating a SCIM 2.0 application which we recommend reviewing before proceeding.

1. Using the OneLogin Administration panel, navigate to **Apps**, then **Add Apps**.
2. Search for SCIM apps that support SCIM 2.0 and OAuth bearer tokens (such as **SCIM Provisioner with SAML (SCIM v2)**) and add that application. This will take you to an application creation wizard.
3. On the configuration page, set the **Display Name** with a descriptive name (such as **SCIM SOE**). Leave other settings at their defaults, or change them as needed for your application.
4. Click **Save**.

Set up user deactivation and reactivation

1. Click on your new SCIM application and click the **Configuration** tab.
2. Check **Enable API Integration** and set the following parameters

- **SCIM Base Url** Set to https://[your_site]/api/scim/v2.
- **SCIM Bearer Token** Enter the **SCIM authorization bearer token** you created on your SOE SCIM settings screen.
- **SCIM JSON Template** SCIM requires a JSON template to pass the correct data to SOE. Specifics will vary by organization, but you can modify the following example template as required.

Example JSON template (no userType field)

```
{
    "userName": "{$parameters.scimusername}",
    "name": {
        "familyName": "{$user.lastname}",
        "givenName": "{$user.firstname}",
        "formatted": "{$user.display_name}"
    },
    "emails": [
        {
            "value": "{$user.email}",
            "type": "work",
            "primary": true
        }
    ],
    "schemas": [
        "urn:ietf:params:scim:schemas:core:2.0:User"
    ]
}
```

3. Click **Enable**. You should see an "Enabled" confirmation message.
4. Click **Save**.
5. On the Provisioning tab, check **Enable provisioning**.
    - Make changes to the fields on this page as required. To have OneLogin events deactivate SOE users, choose **Suspend** from the action drop-down. SOE does not support deletion of users via SCIM.
    - Click **Save**.

When users are deactivated or reactivated in OneLogin, and are assigned to the appropriate SCIM app, the SCIM update should change their status in SOE as well.

Assign users to the SCIM application

You can add users either directly or by role, both under the Users menu. Select a target user or role, then click through to the Applications tab. Add applications with the **[+]** icon.

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.*

To set up user promotion and demotion in OneLogin:

1. Add a custom user field by selecting **Users** then **Custom User Fields** from the top navigation menu.
2. Click **CREATE NEW USER FIELD**. The `Shortname` must be **userType**. We recommend setting the field's `Name` to **userType** as well for consistency. The case of the characters must match that of the SCIM JSON template (for example: $user.custom_fields.**userType**).
3. Modify the SCIM JSON template by clicking the **Configuration** tab. Add the `userType` field to the payload. Click **Save**.

Below is an example template with the optional `userType` field.

Example JSON template with optional userType field

```
{
    "userName": "{$parameters.scimusername}",
    "name": {
        "familyName": "{$user.lastname}",
        "givenName": "{$user.firstname}",
        "formatted": "{$user.display_name}"
    },
    "emails": [
        {
            "value": "{$user.email}",
            "type": "work",
            "primary": true
        }
    ],
    "schemas": [
        "urn:ietf:params:scim:schemas:core:2.0:User"
    ],
    "userType": "{$user.custom_fields.userType}"
}
```

3. Add the `userType` parameter in the OneLogin application by clicking the **Parameters** tab, then **Add parameter**. Create a parameter with **Name userType** and **Value userType (Custom)**. Enable both **Include in SAML assertion** and **Include in User Provisioning**. Click **Save** to update the application.
4. Use one of the following methods to configure `userType` mapping in OneLogin.
    - By custom field on the individual user profile at Users -> All Users. You can edit a user and set the `userType` field under the "Custom Fields" section of the User Info tab. You may need to click **Show Custom Fields** to expand the options. You'll have to do this for every user you want to promote to moderator or administrator.
    - By Application mapping under Users -> Mappings. You can configure field mappings for each application based on certain conditions. For example: you could define a mapping for admin or moderator permissions based on role membership. See OneLogin documentation for more information.

NOTE: *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.