Stack Overflow Enterprise Documentation

Configure System for Cross-domain Identity Management (SCIM) with Microsoft Entra ID

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

Document generated 08/19/2025

PDF VERSION

Tags | **Provisioning** | **Azure** | **SCIM** | **Security** | **Entra ID** |

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.

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.*

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

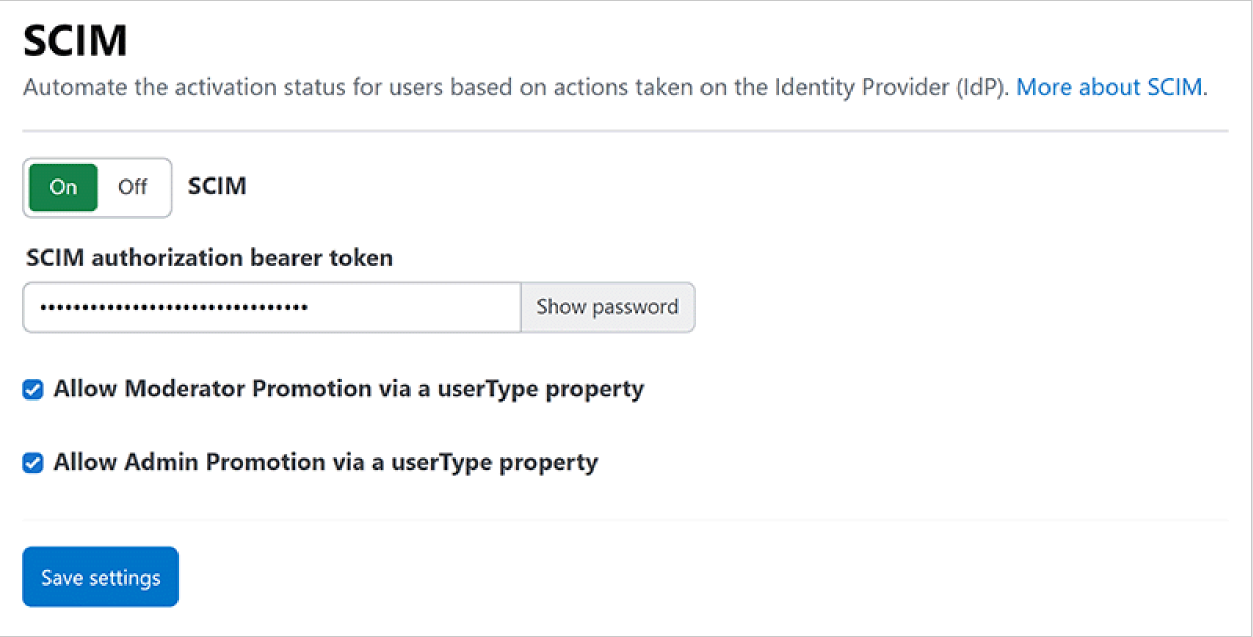
NOTE: *Before you can configure SCIM for Entra ID, you must have an Entra ID Enterprise application for your SOE site. If you haven't yet configured a SAML Entra ID Enterprise application, follow the instructions in the SSO with Microsoft Entra ID article.*

When setting up SCIM, you'll configure Entra ID and your SOE site 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.



SCIM

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

SCIM: On

SCIM authorization bearer token: ••••••••••••••••••••••••••••••••

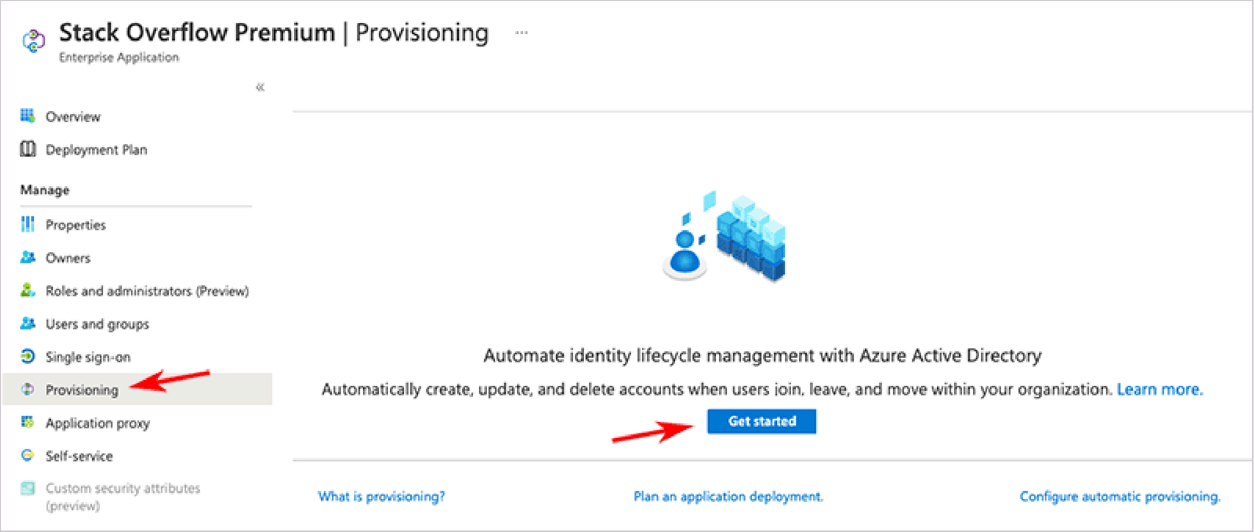
☑ Allow Moderator Promotion via a userType property

☑ 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 Entra ID

1. On Entra ID, open your Stack Overflow Enterprise application.
2. Click **Provisioning** in the left-hand menu, then **Get started**.



Stack Overflow Premium | Provisioning

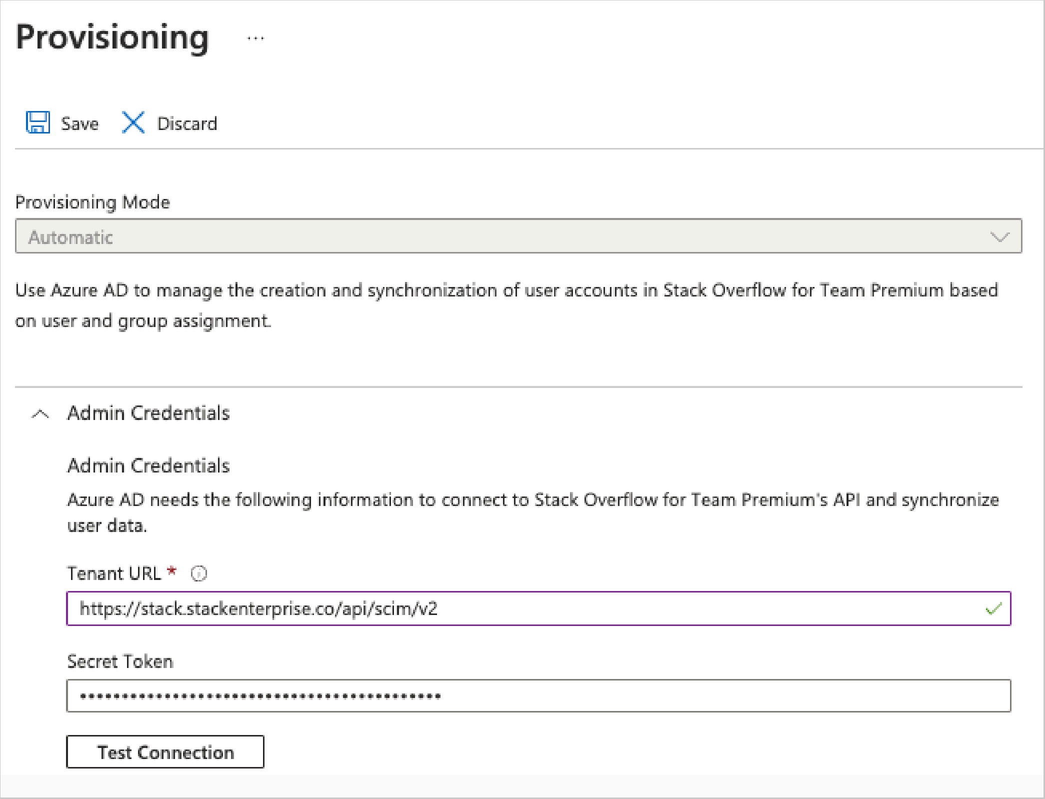
Enterprise Application

Automate identity lifecycle management with Azure Active Directory

Automatically create, update, and delete accounts when users join, leave, and move within your organization. Learn more.

Get started
What is provisioning?
Plan an application deployment.
Configure automatic provisioning.

3. Set **Provisioning Mode** to **Automatic**.
4. Enter the following for Admin Credentials:
    - **Tenant URL** Set to https://[your_site].stackenterprise.co/api/scim/v2.
    - **Secret Token** Paste the authorization bearer token you created on the SOE SCIM page.
5. Click **Test Connection**. A green checkmark will appear in **Tenant URL** if the connection is successful.
6. Click **Save**.



Provisioning

Provisioning Mode: Automatic

Use Azure AD to manage the creation and synchronization of user accounts in Stack Overflow for Team Premium based on user and group assignment.

Admin Credentials

Admin Credentials

Azure AD needs the following information to connect to Stack Overflow for Team Premium's API and synchronize user data.

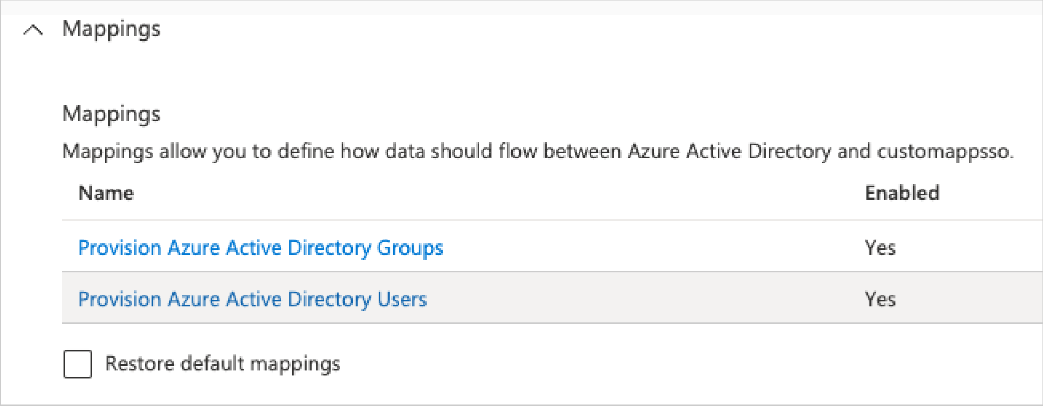
Tenant URL *: https://stack.stackenterprise.co/api/scim/v2 ✓

Secret Token: ••

Configure Entra ID SCIM user mapping

User mapping lets you define which SOE users SCIM will affect.

1. Go to the Entra ID application's "Mappings" page. Set mapping at the user level by clicking **Provision Azure Active Directory Users**. Entra ID SCIM does not support user group management.



Mappings

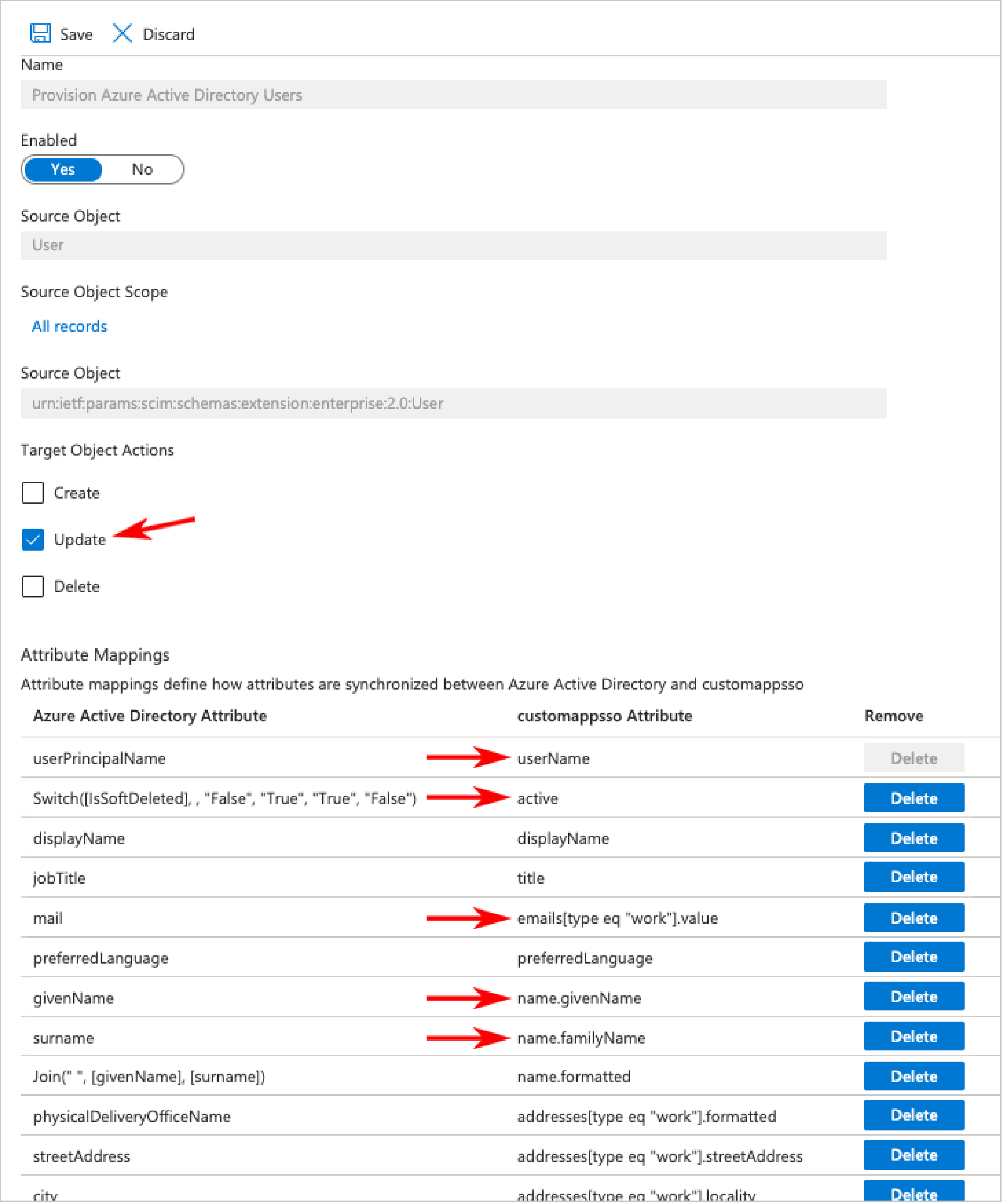
Mappings

Mappings allow you to define how data should flow between Azure Active Directory and customappsso.

Name	Enabled
Provision Azure Active Directory Groups	Yes
Provision Azure Active Directory Users	Yes

□ Restore default mappings

2. On the provisioning configuration page, under the "Target Object Actions", check **Update**. You can optionally check **Create** to provision SOE users automatically.



Name

Provision Azure Active Directory Users

Enabled

[✓ Yes] No

Source Object

User

Source Object Scope

All records

Source Object

urn:ietf:params:scim:schemas:extension:enterprise:2.0:User

Target Object Actions

□ Create

☑ Update

□ Delete

Attribute Mappings

Attribute mappings define how attributes are synchronized between Azure Active Directory and customappsso

Azure Active Directory Attribute	customappsso Attribute	Remove
userPrincipalName	userName	Delete
Switch([IsSoftDeleted], , "False", "True", "True", "False")	active	Delete
displayName	displayName	Delete
jobTitle	title	Delete
mail	emails[type eq "work"].value	Delete
preferredLanguage	preferredLanguage	Delete
givenName	name.givenName	Delete
surname	name.familyName	Delete
Join(" ", [givenName], [surname])	name.formatted	Delete
physicalDeliveryOfficeName	addresses[type eq "work"].formatted	Delete
streetAddress	addresses[type eq "work"].streetAddress	Delete
city	addresses[type eq "work"].locality	Delete

3. Configure the following attributes:

- `userName` Set this to the **Display Name Assertion** from your SOE SAML 2.0 authentication settings (check this value by clicking **Admin Settings**, then **Authentication**, then **Configure SAML 2.0** in SOE).
- `active` (**true**/**false**) Determines whether the user should be deactivated or reactivated in SOE.
- Other required fields for SCIM (Entra ID usually maps these automatically):
  - `name.givenName`
  - `name.familyName`

        - `emails`
    - `stackUserType` (optional) Allows you to change a user's role on your SOE site. Values are **Registered**, **Moderator**, or **Admin**.
    - `department` (optional) Allows you to update the user's department on your SOE site.
    - `title` (optional) Allows you to update the user’s title on your SOE site.
4. Click **Save**.

NOTE: *Adding the optional user department and job title fields allows you to use SOE's connectivity reporting feature. Learn more in the Connectivity article.*