

Automatically Fetch User Accounts without Manually Importing for OneLogin (via SCIM)

OneLogin (via SCIM)

Introduction:

OneLogin gives users the ability to access the applications and other resources they need to do their job by logging in once to a single interface. Platforms like OneLogin are known as **Identity and Access Management (IAM)** solutions that are primarily used to provide their users with a **Single Sign-on (SSO)** experience. OneLogin allows you to automatically send user account data (name, email, role, etc.) into external apps like **Slack, Zoom, Salesforce, or your custom platform** using SCIM without any CSV uploads or manual entry.

SCIM

SCIM (System for Cross-domain Identity Management) is a standard protocol that automates how users are created, updated, or removed across applications. With SCIM, OneLogin can sync user details, like name, email, role to apps like Zoom, or custom platforms that support SCIM.

SCIM helps by:

- Automatically creating users when they're added to OneLogin
- Updating user info when their OneLogin profile changes
- Disabling or deleting users from apps when removed in OneLogin

SCIM is ideal for improving security, reducing IT overhead, and ensuring consistent identity data across platforms.

SAML

SAML (Security Assertion Markup Language) is a standard used for **Single Sign-On (SSO)**. It allows users to log in once to OneLogin and gain access to multiple connected apps (like G Suite, Zoom, or Salesforce) without logging in again.

How it works:

- The user logs in to OneLogin.
- OneLogin sends a **secure login token** (assertion) to the app (service provider).
- The app trusts OneLogin and grants access, no separate password needed.

SAML is useful for improving security and user convenience. It’s often used alongside **SCIM**, where SAML handles authentication and SCIM handles user creation, updates, and removals.

What is Automatic User Provisioning via OneLogin?

Automatic provisioning means **OneLogin pushes user details to your app** when a user is added, updated, or deleted using the SCIM protocol. This reduces errors, saves IT time, and ensures data stays in sync.

What You Need to Integrate App with OneLogin (SCIM)

Requirement	Description
SCIM API Endpoint	A web link where OneLogin can send create/update/delete user requests
Bearer Token	A secret token (like a password) so OneLogin can authenticate securely
SCIM 2.0 Support	Your app must support SCIM 2.0 (understand user creation/update requests)

Set Up SCIM Integration from OneLogin to Your App

Description:

Use OneLogin’s SCIM connector to automatically create, update, or deactivate user accounts in your SCIM-compatible application.

What It Does:

- Auto-creates users in your app.
- Syncs updates to user info (like title, phone, etc.).
- Deactivates/suspends users when removed in OneLogin.

Setup Steps:

Prepare Your App for SCIM Integration

- Create a **SCIM 2.0-compatible API endpoint** in your app.
- Generate a **Bearer Token** your app will recognize.
- Support basic SCIM actions:
 - POST /Users (create)
 - PATCH /Users/{id} (update)
 - DELETE /Users/{id} or deactivate (active: false)

Add Your App in OneLogin

- Go to **Admin Portal → Apps → Add App**.
- Search and select your app (e.g., Zoom, Slack, or Custom SCIM).
- Save and go to the app configuration.

Enable SCIM Provisioning

- Navigate to the **Provisioning** tab in the app.
- Enable "**Enable Provisioning**".
- Enter:
 - **SCIM Base URL** (from your app)
 - **Bearer Token** (from your app)
- Save your settings.

Configure Provisioning Behavior

- Choose what OneLogin does when:
 - A user is added → Create in your app
 - A user is updated → Sync changes
 - A user is removed → Suspend/Delete in your app
- Toggle actions to "**Automatically**" if you don't want manual approval.

Set Up User Mappings

- Go to **Users → Mappings**.
- Create or edit a mapping rule:
 - Assign users to the app based on role, department, etc.
 - Define how OneLogin sends attributes like name, email, title.

Assign the App to Users or Roles

- Go to the **Users** tab:
 - Assign the app directly to users
 - Or assign it to a Role, then assign users to that role

If provisioning is active, users matching the rules will be auto-synced to your app.

What Happens Next?

Once integrated:

- When a user is added to OneLogin → They are automatically created in your app.
- If their profile changes in OneLogin → Your app is updated.
- If they're removed → OneLogin disables or deletes them in your app.

Requirement	Purpose
SCIM API URL	Endpoint where OneLogin sends user actions
Bearer Token	Authenticates OneLogin to your app
SCIM 2.0 Support	Lets your app understand and apply user changes
OneLogin Step	Description
Add App	Add your SCIM-compatible app to OneLogin
Enable Provisioning	Enter SCIM URL + Token
Set Provisioning Rules	Choose when to create/update/delete users
Create Mappings	Map OneLogin attributes to your app fields
Assign Users/Roles	Control which users get sent to your app

Revision #7

Created 18 June 2025 05:51:35 by Kent Lauron

Updated 19 June 2025 06:57:48 by Kent Lauron