



# OneLogin SCIM

## Integration Guide



# Table of Contents

<b>Introduction.....</b>	<b>2</b>
<b>OneLogin Configuration.....</b>	<b>3</b>
<b>Provisioning.....</b>	<b>7</b>
User Provisioning.....	7
Group Provisioning (Based on OneLogin Roles).....	9
Group Provisioning (Based on Existing Envi Roles).....	11
<b>Envi Configuration .....</b>	<b>14</b>

# Introduction

**Envi** supports **SCIM 2.0**, enabling user and group provisioning with various identity providers.

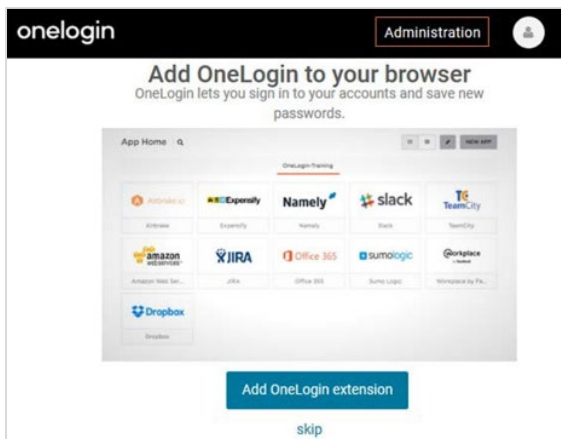
**SCIM** enables IT departments to automate provisioning and deprovisioning of accounts, which reduces manual redundant processes and increases security.

This step-by-step guide explains how to configure **OneLogin SCIM** connection with your **Envi** account.

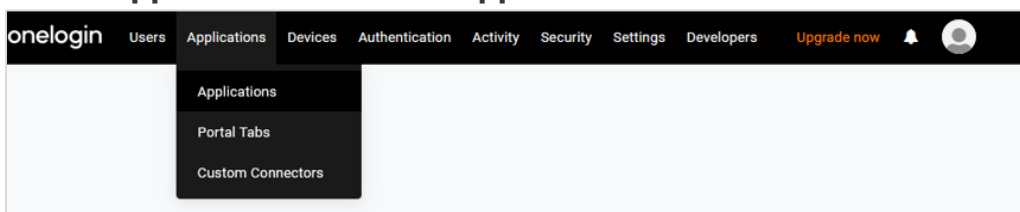
# OneLogin Configuration

Perform the following steps to implement the **SCIM** provisioning with your **Envi** account.

1. Sign in to the [OneLogin](#) site.
2. Select **Administration**.



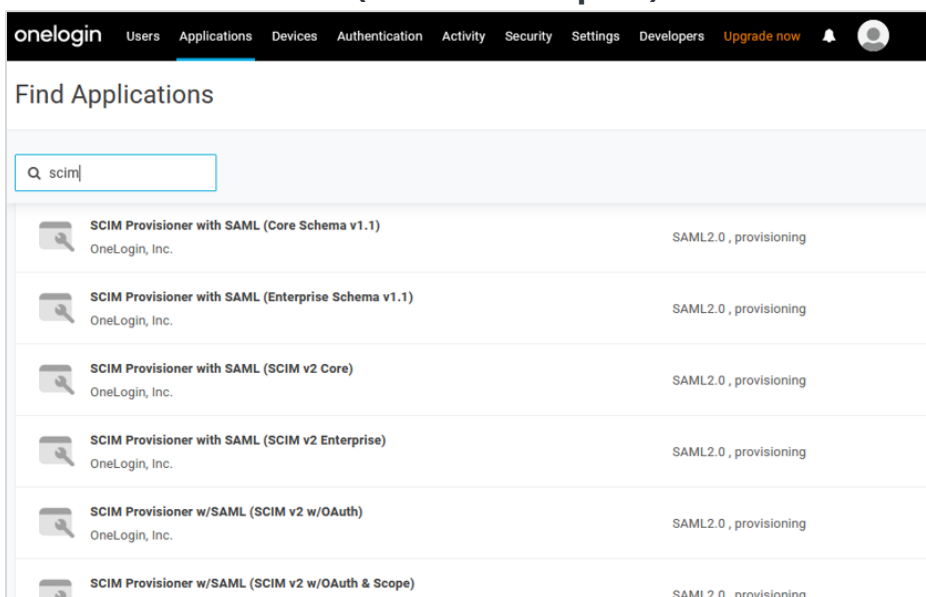
3. On the **Applications** tab, select **Applications**.



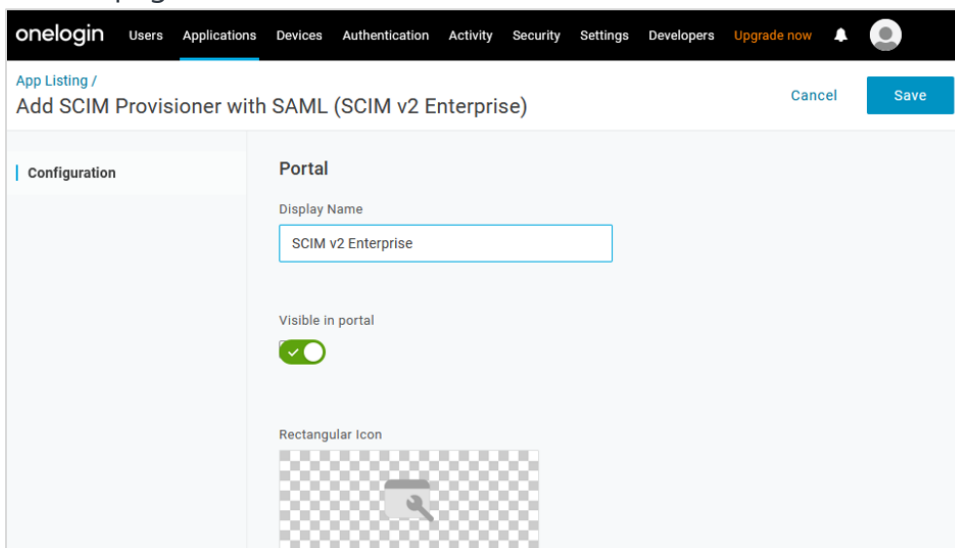
4. Select **Add App**.



5. On the **Find Applications** page, enter **SCIM** in the search box and select the **SCIM Provisioner with SAML (SCIM v2 Enterprise)**.



6. On the **Add SCIM Provisioner with SAML (SCIM v2 Enterprise)** page, change the name of the application and upload other icons if needed. Then, select **Save**. Once you have added the application, you will be redirected to the **Application Details** page.

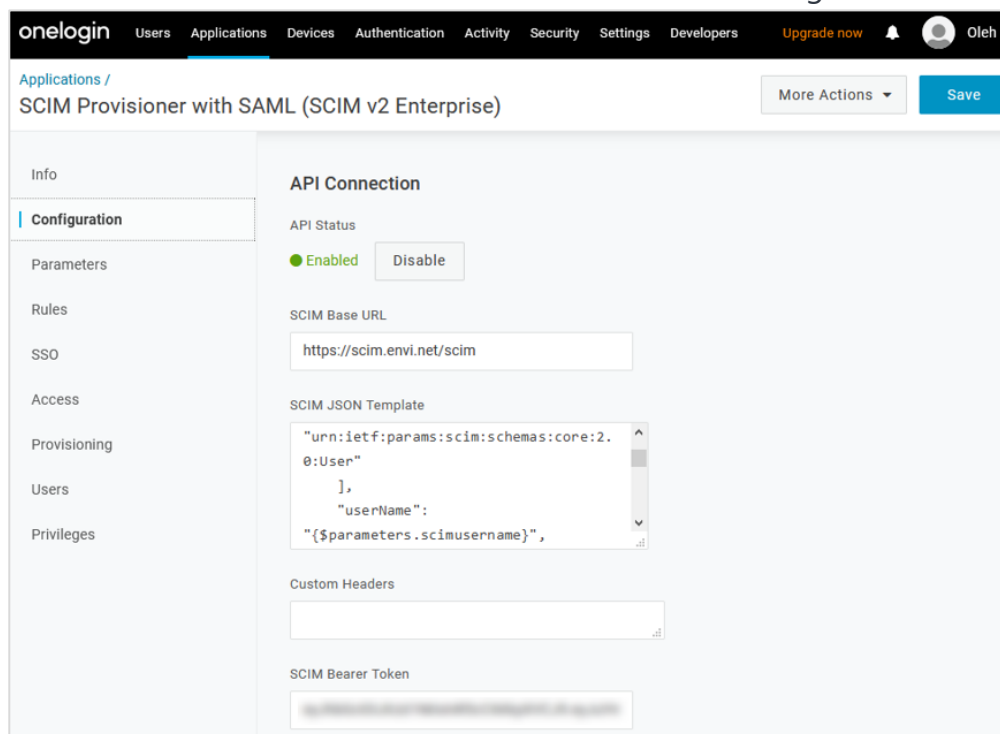


7. On the **Application Details** page, perform the following steps:
  - a. Go to the **Configuration** menu item.
  - b. In the **SCIM Base URL** box, enter the base URL of the **Envi SCIM** server + **/scim** (for example, <https://scim.envi.net/scim>).
  - c. In the **SCIM JSON Template** box, enter the following script template:

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

- d. In the **SCIM Bearer Token** box, enter the **SCIM** token you obtained from the **Envi** application (the [Envi Configuration](#) section, step 5).
  - e. Under **API Status**, select **Enable**, which causes a test call from **OneLogin** to **Envi SCIM API** to make sure the entered information is correct.

- f. After a successful test connection, the status will be changed to **Enabled**.



The screenshot shows the OneLogin SCIM Provisioner configuration page for 'SCIM Provisioner with SAML (SCIM v2 Enterprise)'. The left sidebar contains a menu with items: Info, Configuration (selected), Parameters, Rules, SSO, Access, Provisioning, Users, and Privileges. The main content area is titled 'API Connection' and includes the following fields:

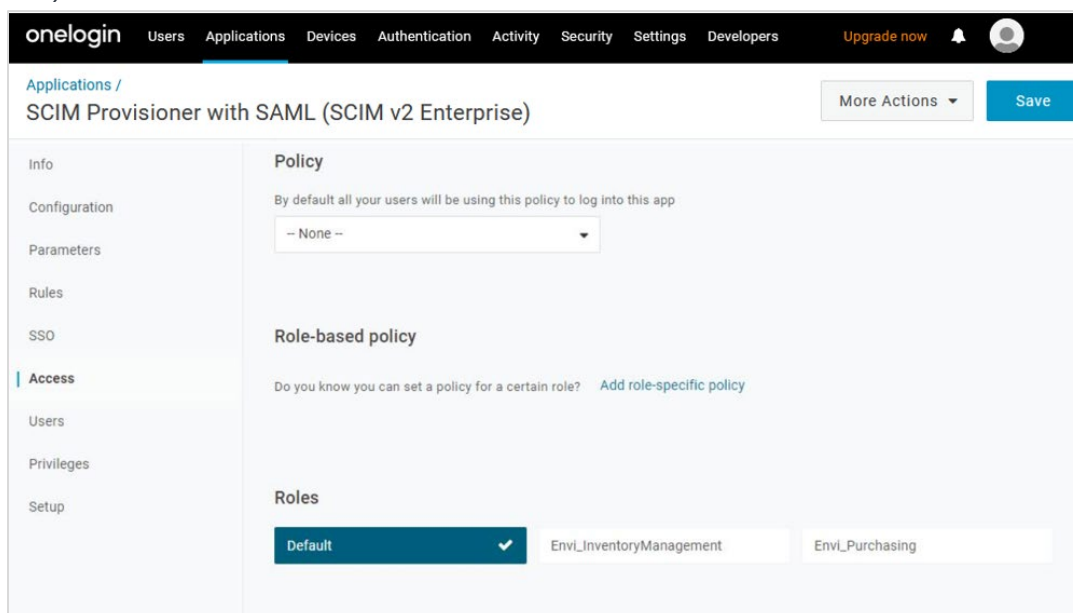
- API Status:** A toggle switch set to 'Enabled' (green dot).
- SCIM Base URL:** A text input field containing 'https://scim.envi.net/scim'.
- SCIM JSON Template:** A text area containing a JSON snippet:
 

```
"urn:ietf:params:scim:schemas:core:2.0:User":
  {
    "userName":
      "${parameters.scimusername}"
  },
```
- Custom Headers:** An empty text input field.
- SCIM Bearer Token:** A text input field containing a blurred token.

Buttons for 'More Actions' and 'Save' are located at the top right of the configuration area.

**Note:** To avoid automatic provisioning during the configuration, do **NOT** save changes at this point.

8. Go to the **Access** menu item and unselect all the roles because some of the existing ones can be assigned automatically. All roles in the list must be unselected (grayed out).

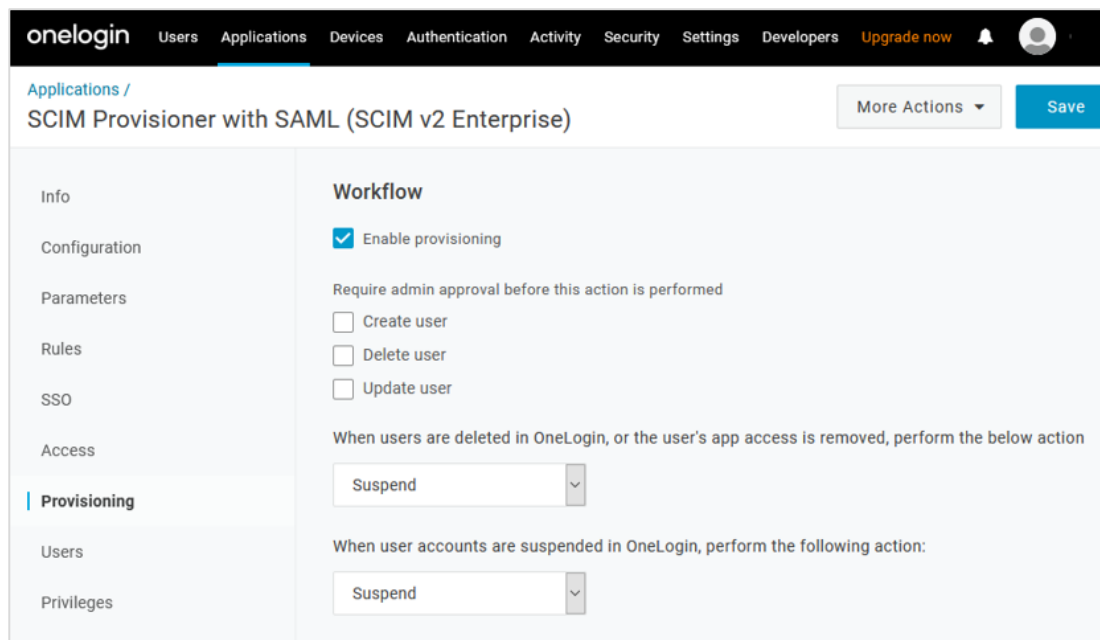


The screenshot shows the OneLogin SCIM Provisioner configuration page for 'SCIM Provisioner with SAML (SCIM v2 Enterprise)', now on the 'Access' tab. The left sidebar menu is the same, but 'Access' is selected. The main content area is titled 'Policy' and includes the following sections:

- Policy:** A dropdown menu set to 'None'.
- Role-based policy:** A section with the text 'Do you know you can set a policy for a certain role?' and a link 'Add role-specific policy'.
- Roles:** A list of roles with checkboxes:
  - Default:** Checked (blue button with a white checkmark).
  - Envi\_InventoryManagement:** Unchecked (grayed out button).
  - Envi\_Purchasing:** Unchecked (grayed out button).

Buttons for 'More Actions' and 'Save' are located at the top right of the configuration area.

9. Go to the **Provisioning** menu item and perform the following steps:
  - a. Select the **Enable provisioning** checkbox.
  - b. Select specific actions that require admin approval.
  - c. Set **Suspend** for both the **Deleting** and **Suspending** actions.
  - d. Select **Save**.



onelogin Users Applications Devices Authentication Activity Security Settings Developers Upgrade now

Applications / SCIM Provisioner with SAML (SCIM v2 Enterprise) More Actions Save

Info Configuration Parameters Rules SSO Access **Provisioning** Users Privileges

**Workflow**

☒ Enable provisioning

Require admin approval before this action is performed

☐ Create user

☐ Delete user

☐ Update user

When users are deleted in OneLogin, or the user's app access is removed, perform the below action

Suspend

When user accounts are suspended in OneLogin, perform the following action:

Suspend

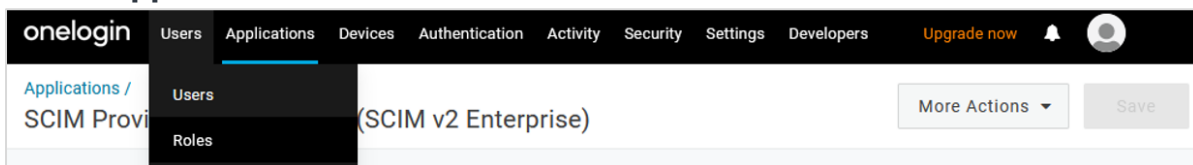
Now, your configuration is ready for use.

# Provisioning

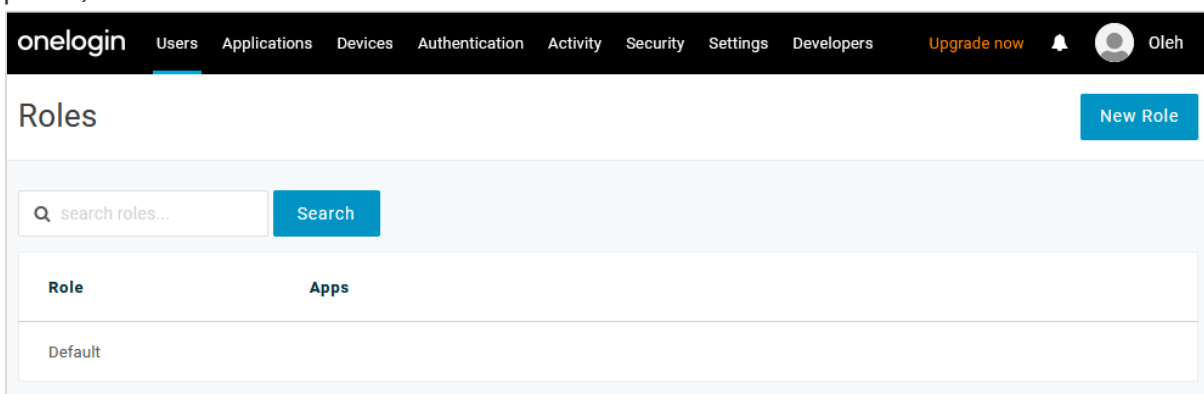
This section describes how to provision new users and groups.

## User Provisioning

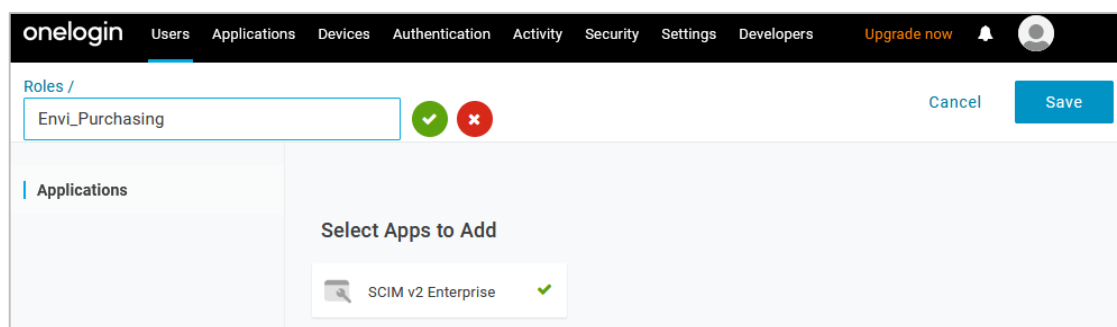
1. On the **Applications** tab, select **Roles**.



2. Select **New Role**, to add roles that should be provisioned to **Envi** (with the **Envi** prefix).



3. On the **Add Role** page, perform the following steps:
  - a. Enter a role name.
  - b. In **Select Apps to Add**, select your **SCIM** application.
  - c. Select **Save**.





4. In the roles list, select the newly created role to view its details. Then, perform the following steps:
  - a. Go to the **Users** menu item.
  - b. In the search box, enter names of users you would like to be provisioned to **Envi** with this current role.
  - c. Select **Check**. The list under the search box, will show all matched users.
  - d. Select **Add To Role**, to give a particular user a role. The list under **Users Added Manually** will show added users.
  - e. Select **Save**.

The screenshot shows the OneLogin interface for the 'Envi\_Purchasing' role. The left sidebar has a menu with 'Roles /', 'Users', 'Applications', 'Privileges', and 'Users' (selected). The main content area is titled 'Check existing or add new users to this role'. It contains a search box with the text 'second user ( suser@soft.com )' and a 'Check' button. Below the search box is a table titled 'Users Added Manually' with columns 'Users', 'Added By', 'Time Added', and 'Action'. The table is currently empty, with a message 'No role manual users yet. Use the search bar above to add user'. At the bottom, it says 'No users'.

**Note:** Repeat these same steps for all users that should be added to this role. Perform the same action for all the roles you need to provision.

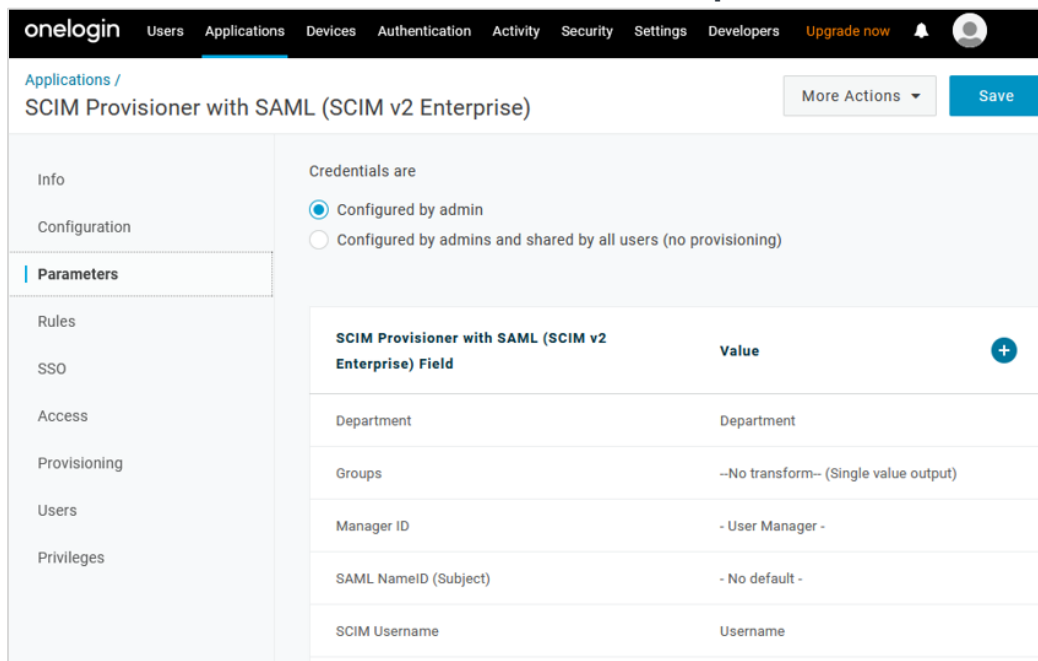
5. Go to the **Application Details** page, to the **Users** menu item and check whether all assigned users have been provisioned correctly.

The screenshot shows the OneLogin interface for the 'SCIM Provisioner with SAML (SCIM v2 Enterprise)' application. The left sidebar has a menu with 'Applications /', 'Info', 'Configuration', 'Parameters', 'Rules', 'SSO', and 'Access'. The main content area is titled 'SCIM Provisioner with SAML (SCIM v2 Enterprise)'. It contains a search box and several filters: 'All roles', 'All groups', 'Any status', and 'Apply to all'. Below the filters is a table with columns 'User', 'Provisioning State', and 'Notes'. The table shows two users: 'second user' and 'third user', both with a green checkmark and the state 'Provisioned'. At the bottom, it says 'Showing 1-2 of 2 users'.

Now, you have added the needed members and roles.

# Group Provisioning (Based on OneLogin Roles)

1. Go to the **Parameters** menu item and select **Groups**.



onelogin Users Applications Devices Authentication Activity Security Settings Developers Upgrade now

Applications / SCIM Provisioner with SAML (SCIM v2 Enterprise) More Actions Save

Info Configuration **Parameters** Rules SSO Access Provisioning Users Privileges

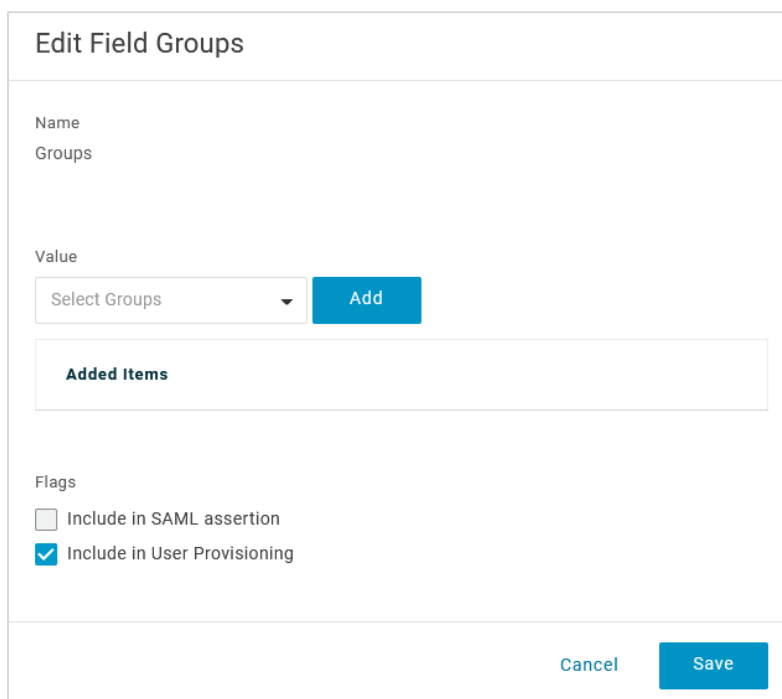
Credentials are

☒ Configured by admin

☐ Configured by admins and shared by all users (no provisioning)

SCIM Provisioner with SAML (SCIM v2 Enterprise) Field	Value
Department	Department
Groups	--No transform-- (Single value output)
Manager ID	- User Manager -
SAML NameID (Subject)	- No default -
SCIM Username	Username

2. In the **Edit Field Groups** dialog, select the **Include in User Provisioning** checkbox and select **Save**. Then, select **Save** once more in the application.



Edit Field Groups

Name  
Groups

Value  
Select Groups Add

Added Items

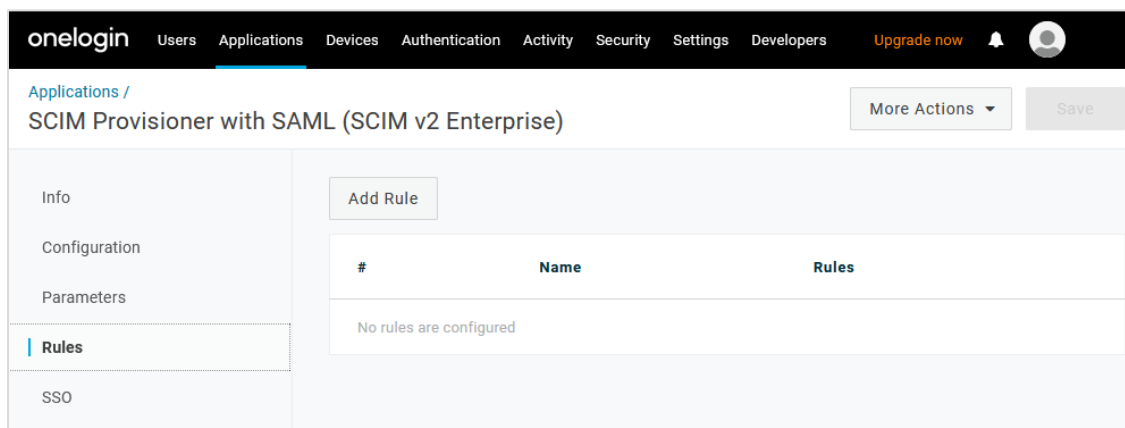
Flags

☐ Include in SAML assertion

☒ Include in User Provisioning

Cancel Save

- Go to the **Rules** menu item and select **Add Rule**.



- In the **New mapping** dialog, perform the following steps:

- Enter **Name**.
- Leave **Conditions** empty.
- In **Actions**:
  - Select **Set Groups in YourAppName**.
  - Select the **Map from OneLogin** option.
  - In the **For each** dropdown, select the **role** value.

**Note:** The value that matches should start with the following regex: `(Envi)(.*)`.  
This is based on the convention that roles that are eligible for provisioning should start with the **Envi** prefix.

- Select **Save** in the dialog and again **Save** in the application

Now, you have created group provisioning based on **OneLogin** roles.

## Group Provisioning (Based on Existing Envi Roles)

1. Go to **Application Details > Provisioning**. In the **Entitlements** section, select **Refresh** to import your organization's app entitlements values (such as a group name).

onelogin Users Applications Devices Authentication Activity Security Settings Developers Upgrade now

Applications / SCIM Provisioner with SAML (SCIM v2 Enterprise) More Actions Save

Info Configuration Parameters Rules SSO Access **Provisioning** Users Privileges

When users are deleted in OneLogin, or the user's app access is removed, perform the below action

Suspend

When user accounts are suspended in OneLogin, perform the following action:

Suspend

### Entitlements

[Refresh](#)

Entitlements are user attributes that are usually associated with fine-grained app access, like app group, department, organization, or license level. When you click [Refresh](#), OneLogin imports your organization's app entitlement values (such as group names or license types) so you can map them to OneLogin attribute values. Entitlement refresh can take several minutes. Check Activity > Events for completion status.

2. Go to the **Parameters** menu item and select **Groups**.

onelogin Users Applications Devices Authentication Activity Security Settings Developers Upgrade now

Applications / SCIM Provisioner with SAML (SCIM v2 Enterprise) More Actions Save

Info Configuration **Parameters** Rules SSO Access Provisioning Users Privileges

Credentials are

☒ Configured by admin

☐ Configured by admins and shared by all users (no provisioning)

SCIM Provisioner with SAML (SCIM v2 Enterprise) Field	Value
Department	Department
Groups	--No transform-- (Single value output)
Manager ID	- User Manager -
SAML NameID (Subject)	- No default -
SCIM Username	Username

3. In the **Edit Field Groups** dialog, select the **Include in User Provisioning** checkbox and select **Save**. Then, select **Save** in the application.

Edit Field Groups

Name

Groups

Value

Select Groups

Add

Added Items

Flags

☐ Include in SAML assertion

☒ Include in User Provisioning

Cancel

Save

4. Go to **Application Details > Users** menu item and select a user you want to assign to the **Envi** role.

onelogin

Users Applications Devices Authentication Activity Security Settings Developers

Upgrade now

Applications /

SCIM Provisioner with SAML (SCIM v2 Enterprise)

More Actions

Save

Info

Configuration

Parameters

Rules

SSO

Access

Provisioning

Users

Privileges

Search

All roles

All groups

Any status

Apply to all

User	Provisioning State	Notes
	✓ Provisioned	
	✓ Provisioned	

Showing 1-2 of 2 users

5. In the **SCIM** dialog, select the needed role from the **Groups** dropdown and select **Add**. Perform the same action for all the **Envi** roles that should be assigned to the user.

Edit SCIM v2 Enterprise login for second user

☒ Allow the user to sign in  
☐ Hide this app in Portal

SCIM Username

*i* Shared identifier between SCIM and OneLogin

Groups *w*  

Select Groups
Add

Envi\_InventoryManagement  
Envi\_Purchasing

manager id  
N/A

SAML NameID (Subject)

Title

Department  
*w* Manually editing a field overrides any mapping. To restore all mappings, reset the user.

Cancel Save

At this point, you have configured group provisioning based on existing **Envi** roles.

# Envi Configuration

To synchronize **OneLogin** with **Envi** via **SCIM**, perform the following actions:

1. Sign in to the **Envi** application.
2. Go to **My Profile > My Domain > Recourses** tab.
3. On the **Recourses** tab, select the **SCIM Configuration** link.

**Note:** The link is only available for domains with the **Simple** domain type and with the **HTTP Redirect** or **WS Trust** authentication.

Domains > Domain Name DomainName

**DETAILS** ORGANIZATIONS USERS PASSWORD DICTIONARIES UPDATE RESOURCES SECURITY

[Edit](#)

Name: DomainName

Description: Description

Domain Type: Simple

Session Timeout, m: 20

Mobile Token Expiration, h:

Default UI: Default [Update Users](#)

Status: Active

Authentication: HTTP Redirect

Failed Attempts: 2

Endpoint URL: http://12

Identifier URL: http://123

SSO Message: Please provide your SSO credentials for further logins

Do not require force authentication.

Do not require device registration.

Do not restrict IP Addresses

Do not use live metadata.

4. On the **SCIM Configuration** page, you will find the domain details of your configuration. By default, a new configuration will be **Inactive** and will contain no organizations. To proceed with further **SCIM** configuration, perform the following steps:
  - a. Select **Edit**.
  - b. In the **Status** dropdown, select **Active**.
  - c. In the **Organization** dropdown, select a needed organization.
  - d. Select **Update**.

Domains > Domain Name **For Testing Purpose**

**DETAILS** ORGANIZATIONS USERS PASSWORD DICTIONARIES UPDATE **RESOURCES** SECURITY

[Update](#) [Cancel](#)

Status: Active

Organization\*: For Testing Purpose

Valid Token: Yes

User Role Prefix\*: Envi\_

- Once you have updated **SCIM** configurations, select the **Create Token**, then **Copy Token** button.

**Note:** Enter the obtained **SCIM** token in the **SCIM Bearer Token** box (the [OneLogin Configuration](#) section, step 7).

Domains > Domain Name **Test Domain**

[DETAILS](#)
[ORGANIZATIONS](#)
[USERS](#)
[PASSWORD DICTIONARIES](#)
[UPDATE](#)
[RESOURCES](#)
[SECURITY](#)

[Edit](#)
[Create Token](#)
[Copy Token](#)
[Go Back](#)

Status: Active

Organization: **For Testing Purpose**

Valid Token: Yes

User Role Prefix: Envi\_

Now, **OneLogin SCIM** is configured and synchronized.