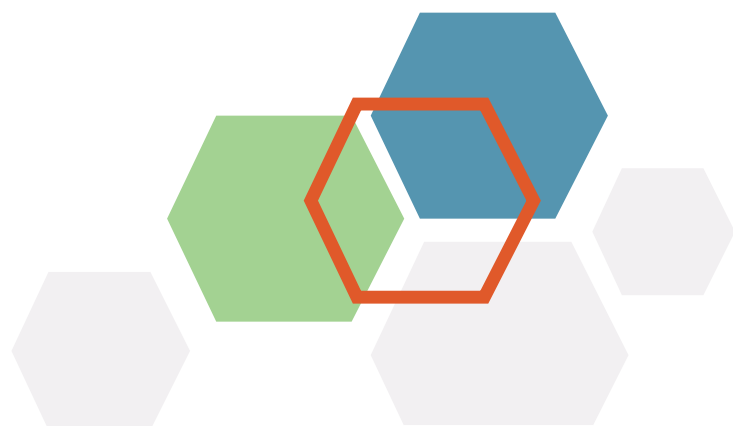


envi



# OneLogin SCIM

Integration Guide



# Table of Contents

<b>Introduction</b> .....	<b>2</b>
<b>OneLogin Configuration</b> .....	<b>3</b>
<b>Provisioning</b> .....	<b>8</b>
User Provisioning.....	8
Group Provisioning (Based on OneLogin Roles).....	10
Group Provisioning (Based on Existing Envi Roles).....	12
<b>Envi Configuration</b> .....	<b>15</b>

# Introduction

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

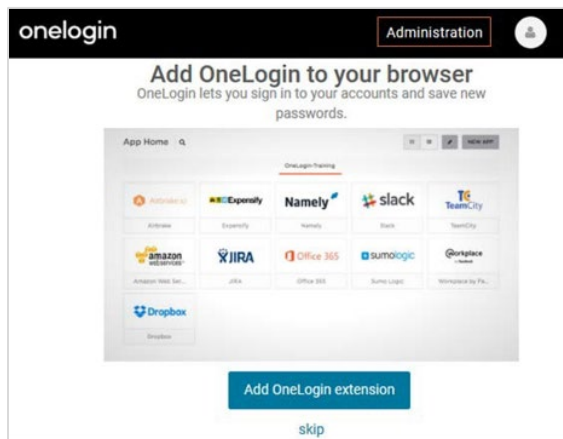
**SCIM** enables IT departments to automate provisioning and deprovisioning of accounts, which reduces manual redundant processes and increases security.

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

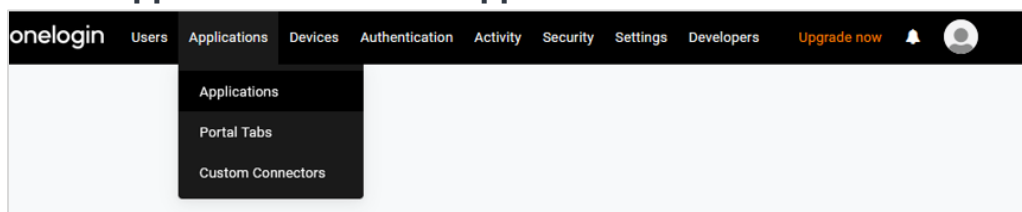
# OneLogin Configuration

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

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



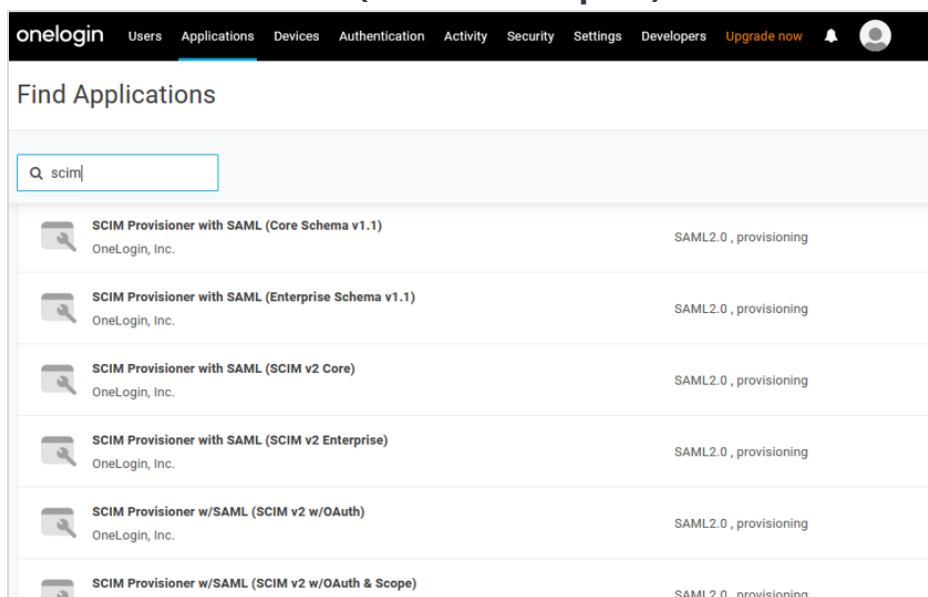
3. On the **Applications** tab, select **Applications**.



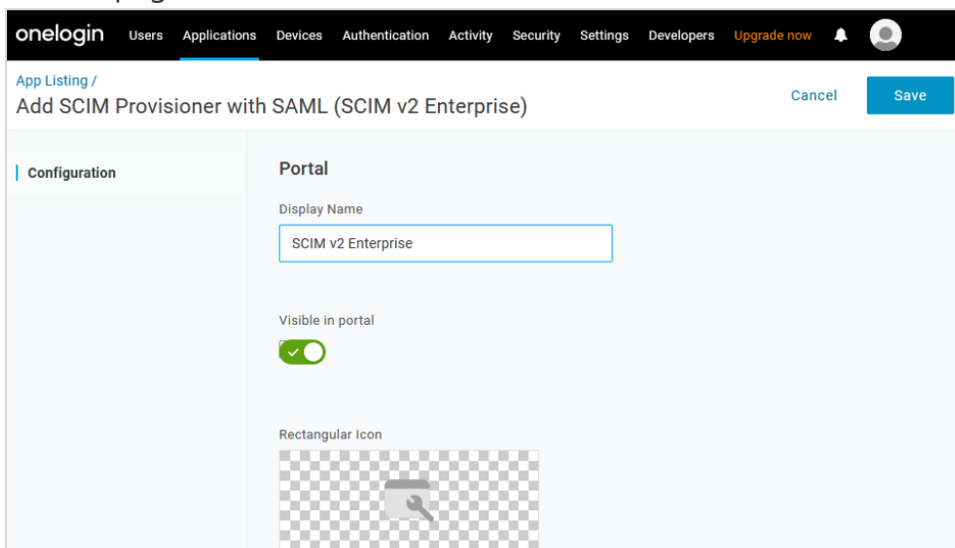
4. Select **Add App**.



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.

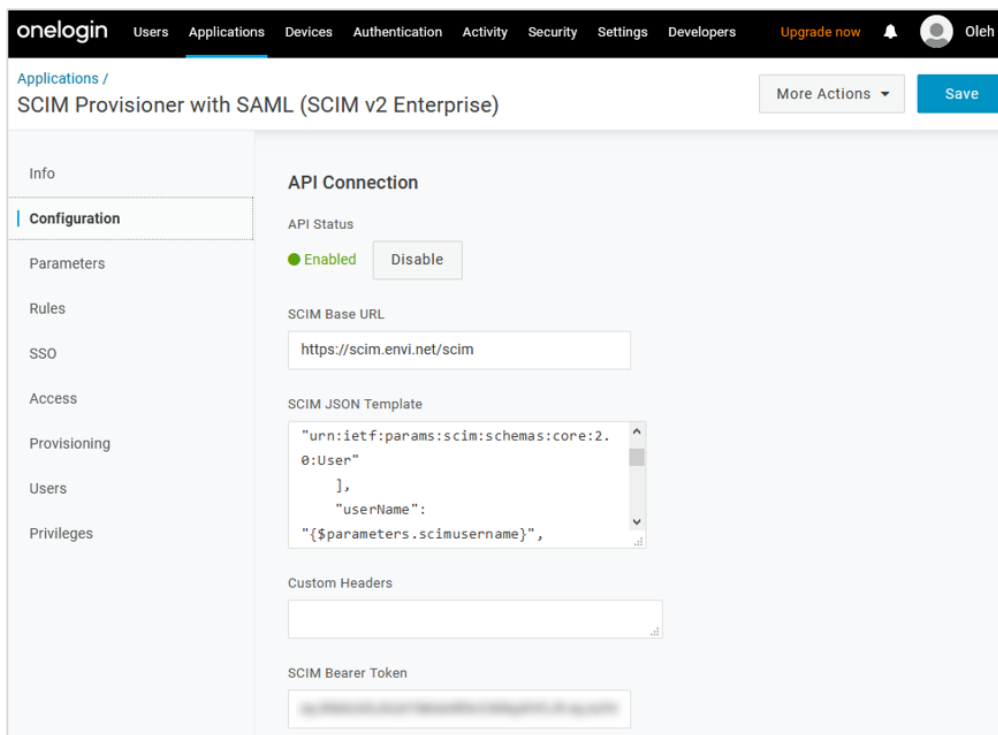


7. On the **Application Details** page, perform the following steps:
  - a. Go to the **Configuration** menu item.
  - b. In the **SCIM Base URL** box, enter the base URL of the **Envi SCIM** server + **/scim** (for example, <https://scim.envi.net/scim>).
  - c. In the **SCIM JSON Template** box, enter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

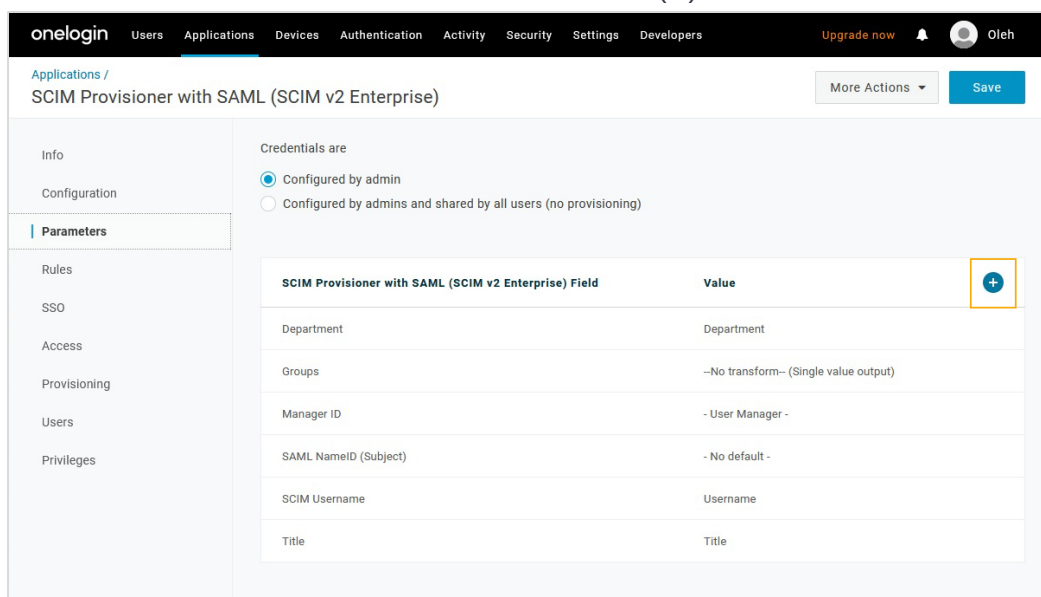
```
{
  "schemas": [
    "urn:ietf:params:scim:schemas:core:2.0:User"
  ],
  "userName": "${parameters.scimusername}",
  "name": {
    "givenName": "${user.firstname}",
    "familyName": "${user.lastname}"
  },
  "externalId": "${user.id}",
  "emails": [
    {
      "value": "${user.email}",
      "type":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

- 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**.

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



- 8. Go to the **Parameters** tab and select the **Add (+)** button.



9. In the **New Field** dialog, perform the following steps:

a. In the **Field name** box, enter **Title**.

**Note:** By default, the **Title** parameter is not added to the **SCIM Parameters**.

b. Select the **Include in User Provisioning** checkbox.

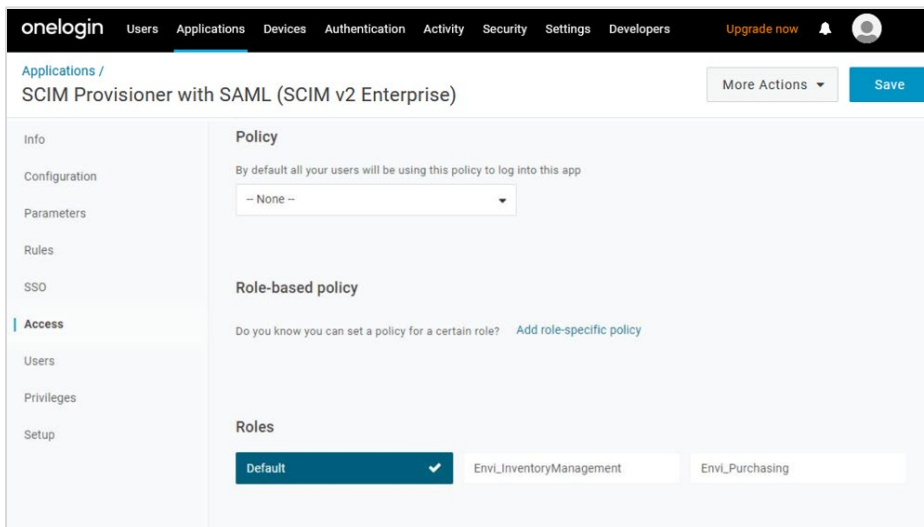
c. Select **Save**.

10. In the **Edit Field** dialog, perform the following steps:

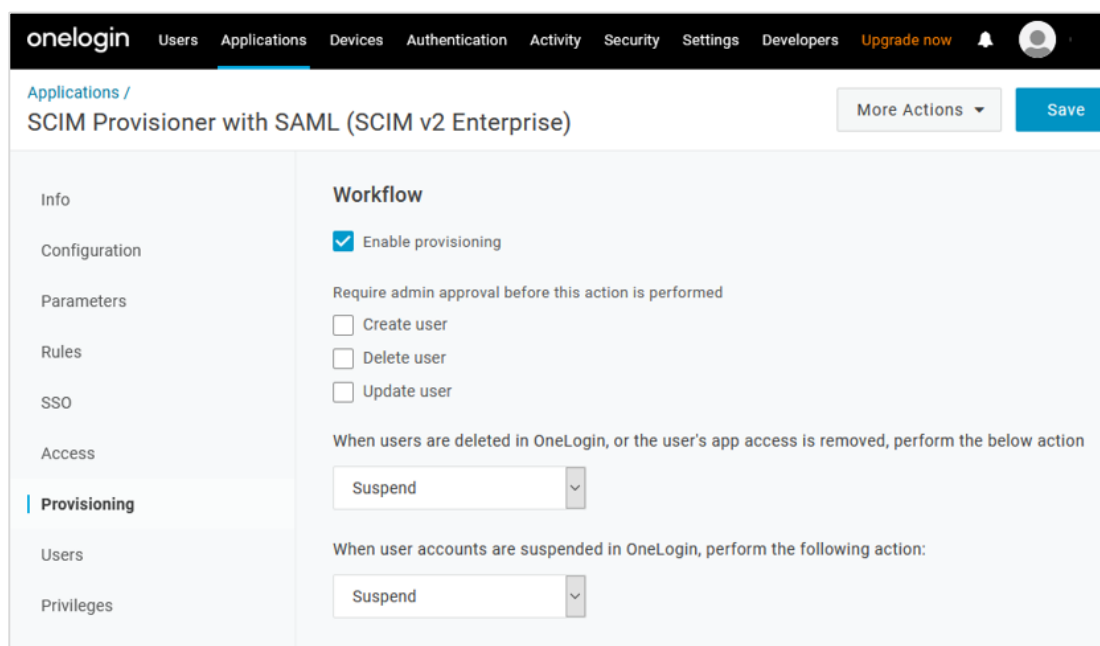
a. In the **Value** dropdown, select **Title**.

b. Select **Save**.

11. 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).



12. 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**.



Now, your configuration is ready for use.

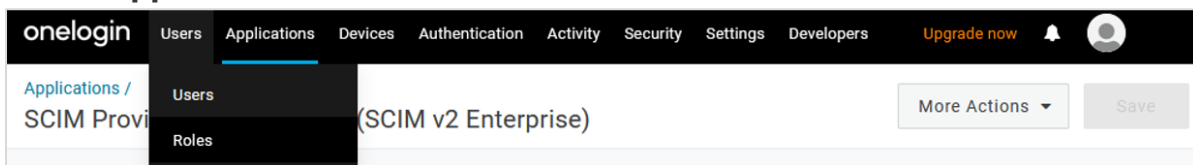


# Provisioning

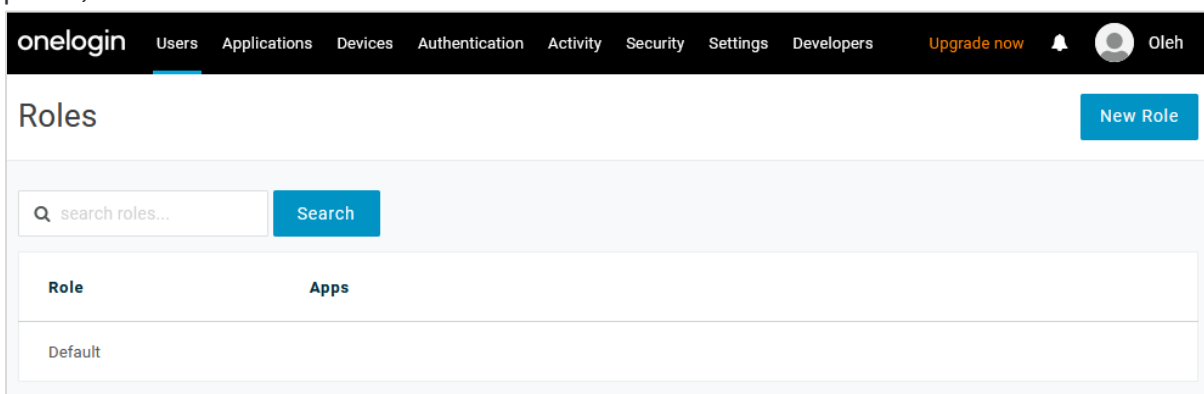
This section describes how to provision new users and groups.

## User Provisioning

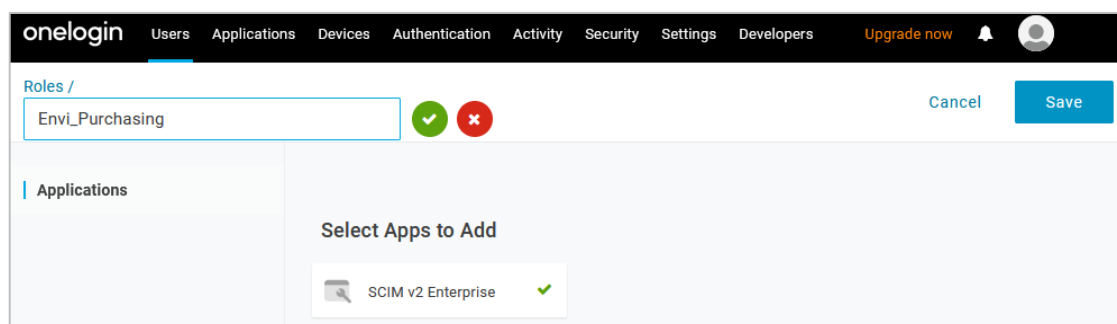
1. On the **Applications** tab, select **Roles**.



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**.



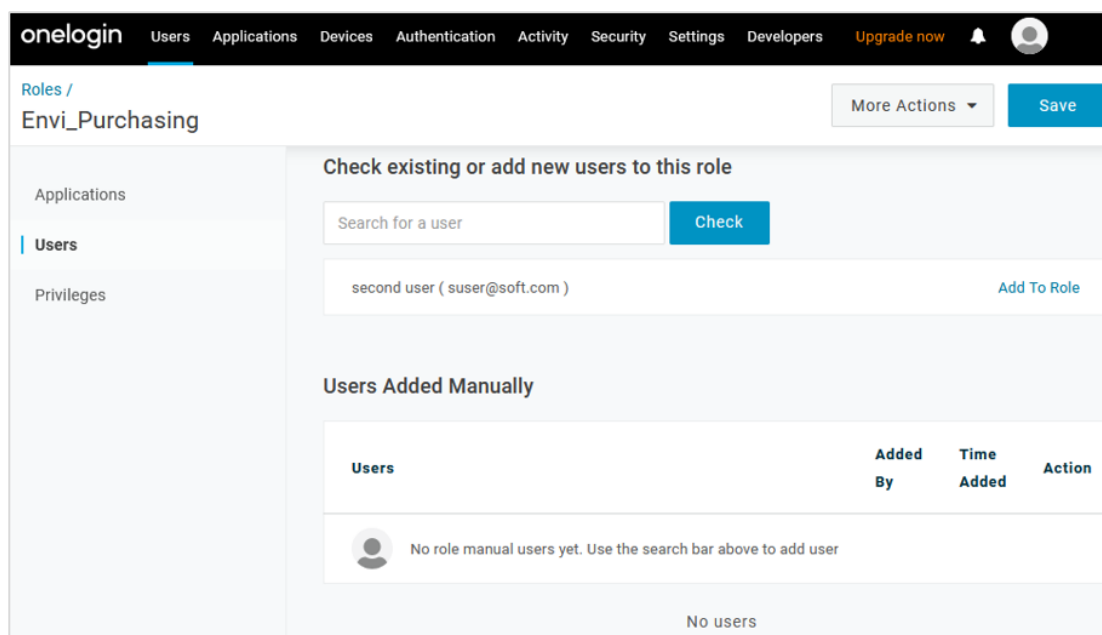
4. In the roles list, select the newly created role to view its details. Then, perform the following steps:
  - a. Go to the **Users** menu item.
  - b. In the search box, enter names of users you would like to be provisioned to **Envi** with this current role.
  - c. Select **Check**.

**Note:** The list under the search box will show all matched users.

- d. Select **Add To Role** to give a particular user a role.

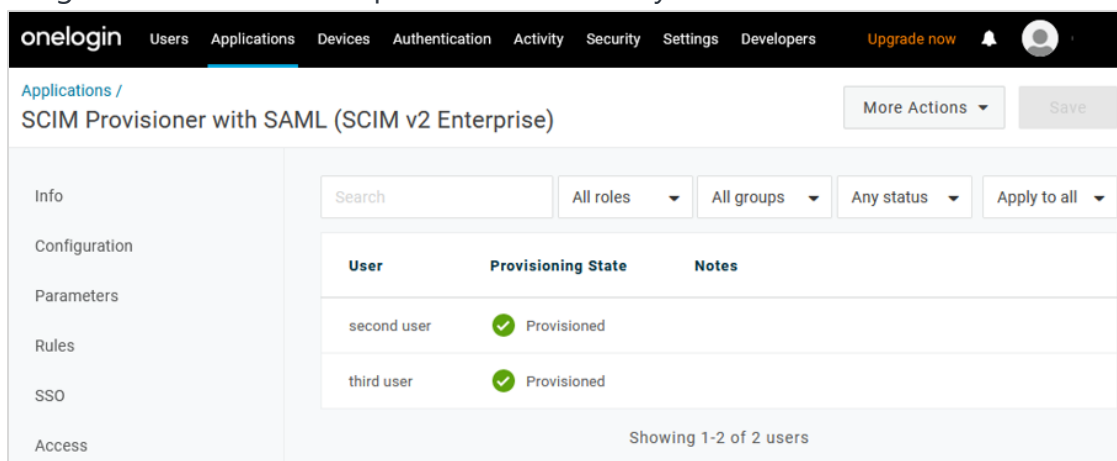
**Note:** The list under **Users Added Manually** will show added users.

- e. Select **Save**.



**Note:** Repeat these same steps for all users that should be added to this role and 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.



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**.

The screenshot shows the OneLogin interface for configuring a SCIM Provisioner with SAML (SCIM v2 Enterprise). The left sidebar contains a navigation menu with items: Info, Configuration, Parameters (selected), Rules, SSO, Access, Provisioning, Users, and Privileges. The main content area is titled 'SCIM Provisioner with SAML (SCIM v2 Enterprise)' and includes a 'More Actions' dropdown and a 'Save' button. Under 'Credentials are', the 'Configured by admin' radio button is selected. Below this is a table of parameters:

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
Title	Title

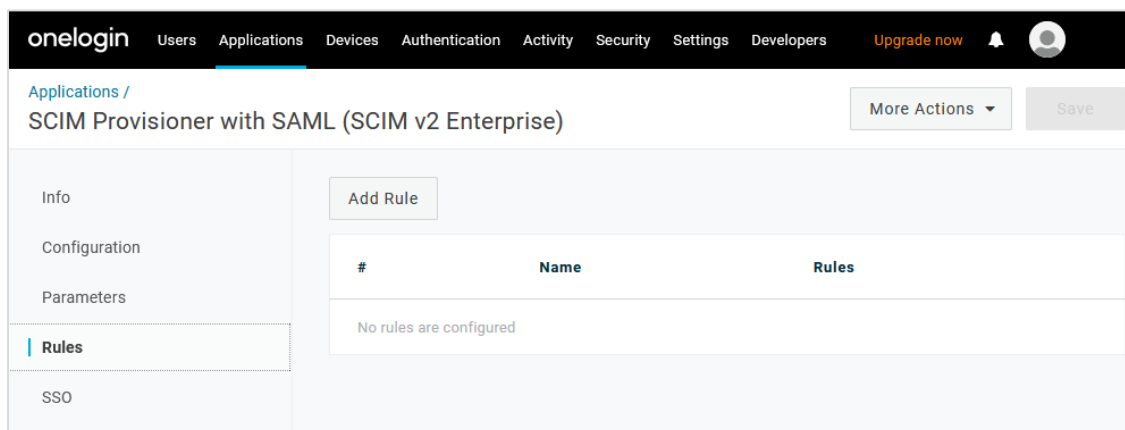
2. In the **Edit Field Groups** dialog, select the **Include in User Provisioning** checkbox and select **Save**. Then, select **Save** once more in the application.

The 'Edit Field Groups' dialog box shows the following configuration:

- Name:** Groups
- Value:** A dropdown menu set to 'Select Groups' with an 'Add' button next to it.
- Added Items:** An empty box for listing added items.
- Flags:**
  - Include in SAML assertion
  - Include in User Provisioning

At the bottom right, there are 'Cancel' and 'Save' buttons.

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

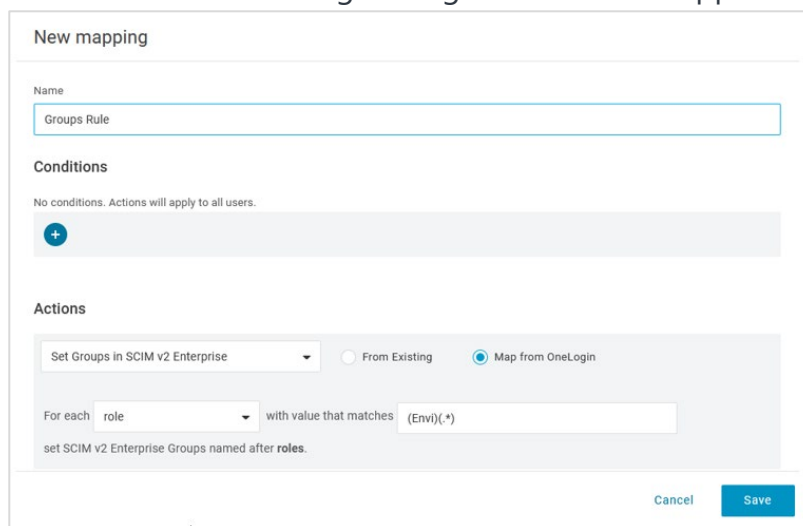


4. In the **New mapping** dialog, perform the following steps:

- a. Enter **Name**.
- b. Leave **Conditions** empty.
- c. In **Actions**:
  - I. Select **Set Groups in YourAppName**.
  - II. Select the **Map from OneLogin** option.
  - III. 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.

d. 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).

The screenshot shows the OneLogin interface for configuring a SCIM Provisioner with SAML (SCIM v2 Enterprise). The left sidebar has 'Provisioning' selected. The main content area is titled 'Entitlements' and includes a 'Refresh' button. An information tooltip is displayed, stating: '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**.

The screenshot shows the 'Parameters' section of the SCIM Provisioner configuration. The 'Groups' parameter is selected. The interface shows a table of parameters with their corresponding values:

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

- 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

**Added Items**

Flags  
 Include in SAML assertion  
 Include in User Provisioning

- 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

Search All roles All groups Any status Apply to all

User	Provisioning State	Notes
[blurred]	✓ Provisioned	
[blurred]	✓ Provisioned	

Showing 1-2 of 2 users

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

- 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

suser

(i) Shared identifier between SCIM and OneLogin

Groups ⚠

Select Groups Add

Envi\_InventoryManagement

Envi\_Purchasing

manager id

N/A

SAML NameID (Subject)

Title

Department

⚠ 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.

The screenshot shows the 'DETAILS' tab of a domain configuration page. The domain name is 'DomainName'. The 'Domain Type' is set to 'Simple' and the 'Authentication' is set to 'HTTP Redirect'. Other details include 'Failed Attempts: 2', 'Endpoint URL: http://12', 'Identifier URL: http://123', and 'SSO Message: Please provide your SSO credentials for further logins'. There are also checkboxes for 'Do not require force authentication', 'Do not require device registration', 'Do not restrict IP Addresses', and 'Do not use live metadata'. An 'Update Users' link is visible.

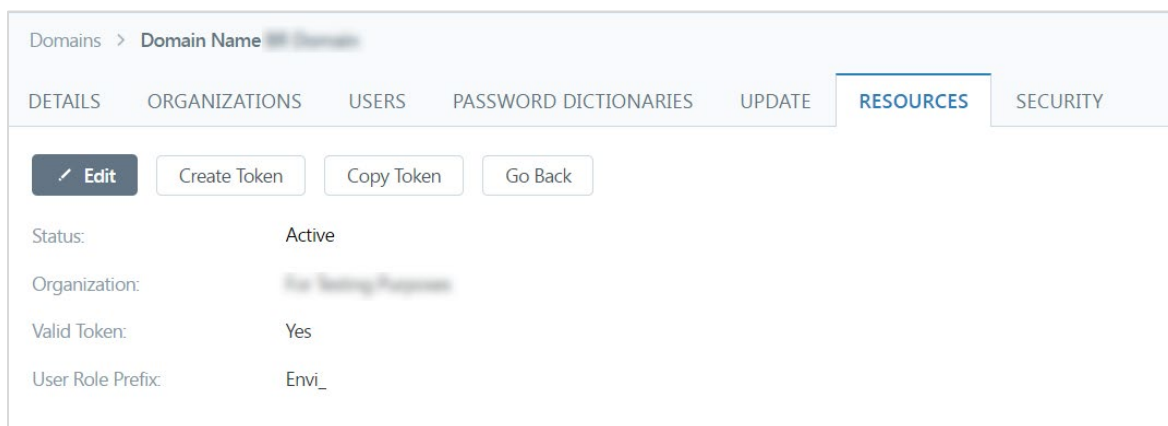
4. On the **SCIM Configuration** page, you will find the domain details of your configuration. By default, a new configuration will be **Inactive** and will contain no organizations. To proceed with further **SCIM** configuration, perform the following steps:
  - a. Select **Edit**.
  - b. In the **Status**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

The screenshot shows the 'RESOURCES' tab of the domain configuration page. It features an 'Update' button and a 'Cancel' button. The 'Status' dropdown is set to 'Active'. The 'Organization' dropdown is set to 'For Testing Purpose'. The 'Valid Token' checkbox is checked, and the 'User Role Prefix' is set to '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).



The screenshot shows the OneLogin configuration interface for a domain. The breadcrumb is 'Domains > Domain Name'. The navigation tabs are 'DETAILS', 'ORGANIZATIONS', 'USERS', 'PASSWORD DICTIONARIES', 'UPDATE', 'RESOURCES' (selected), and 'SECURITY'. Below the tabs are four buttons: 'Edit', 'Create Token', 'Copy Token', and 'Go Back'. The configuration details are as follows:

Status:	Active
Organization:	For Testing Purposes
Valid Token:	Yes
User Role Prefix:	Envi_

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