



# OneLogin SSO & SCIM Guide

Getting Started . . . . .	1
Accessing your user-based license . . . . .	1
Preparing Prime . . . . .	1
OneLogin Configuration . . . . .	1
Creating an Application in OneLogin . . . . .	2
Single sign-on (SSO) Configuration . . . . .	3
SCIM Identity Management Configuration . . . . .	9
Revoke User . . . . .	12

## Getting Started

### Accessing your user-based license

You can find your new SSO/SCIM User Licensing subscription in My Account:

- Navigate to [www.geneious.com/account](http://www.geneious.com/account)
- Log in with your existing credentials
- From the header drop down, select your user based subscription

### Preparing Prime

In order to follow the below steps to enable your SSO/SCIM configuration, you will need to be using at least version 2024.0 of Prime, and have deactivated your existing Prime activation.

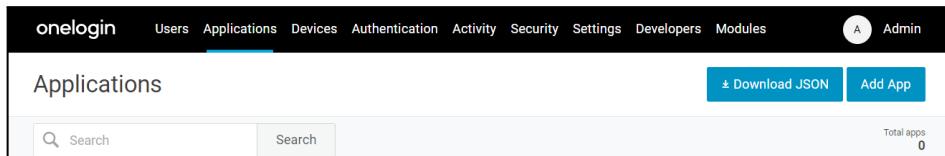
- To download the latest version, visit our [Updates](#) page, or update via the in-app updates feature
- Deactivate your current license by following **Help -> Manage License...**
- Let the Prime team know if your deactivation limit needs to be extended
- After deactivation, Prime should display the activation screen, or reopen in Restricted mode. You are now ready to apply your SSO and/or SCIM configuration following the steps below.

### OneLogin Configuration

To use OneLogin as your vendor, please follow the steps below to configure your application. The first two sections detail instructions for setting up Geneious Prime as an SSO application in OneLogin, while the third configures SCIM for identity management.

## Creating an Application in OneLogin

1. In the top menu of the Administration portal, navigate to **Applications** → **Applications**, and then select **Add App**:



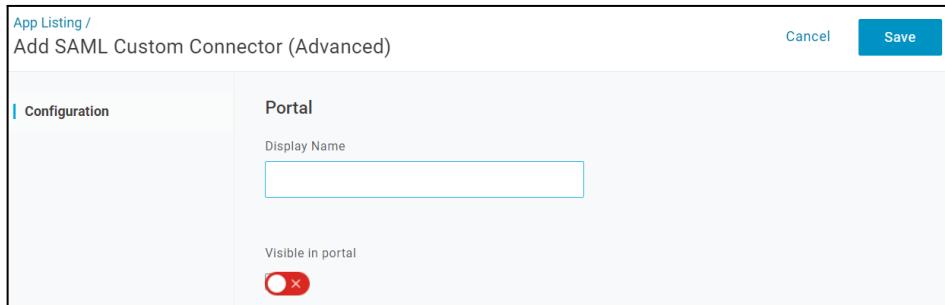
The screenshot shows the OneLogin Administration portal. The top navigation bar includes links for onelogin, Users, Applications (which is underlined in blue), Devices, Authentication, Activity, Security, Settings, Developers, and Modules. A user icon labeled 'Admin' is in the top right. The main content area is titled 'Applications' with a search bar below it. At the top right of the content area are buttons for 'Download JSON' and 'Add App'. Below the search bar, there are two input fields: 'Search' and 'Search'. At the bottom right of the content area, it says 'Total apps 0'.

2. If using OneLogin only for SSO, and not SCIM provisioning, search for **SAML Custom Connector (Advanced)**. Select this, enter a **Display Name** such as “Geneious Prime”, disable the **Visible in portal** option, and click **Save**.

Otherwise, if using OneLogin for both SSO and SCIM (or planning to in the future), then use the **SCIM Provisioner with SAML (SCIM v2 Enterprise, full SAML)** application instead. The following screenshots correspond to the SSO case, but also apply to the SCIM application type.



The screenshot shows a search results page titled 'Find Applications'. A search bar contains the text 'SAML Custom Connector'. Below the search bar, a list item is shown: '1 SAML Custom Connector (Advanced)' by 'OneLogin, Inc.'. To the right of the list item, the text 'SAML2.0' is displayed. The entire list item is enclosed in a light gray box.



The screenshot shows a configuration page for 'Add SAML Custom Connector (Advanced)'. The top bar includes 'App Listing /' and the page title 'Add SAML Custom Connector (Advanced)'. On the right are 'Cancel' and 'Save' buttons. The main area has two tabs: 'Configuration' (selected) and 'Portal'. Under 'Configuration', there is a 'Display Name' field with an empty input box. Under 'Portal', there is a 'Visible in portal' checkbox, which is currently unchecked (indicated by a red 'X').

## Single sign-on (SSO) Configuration

Once created, switch to the **Configuration** tab. Before continuing here, you will need to configure Geneious Prime's [My Account](#), and use information from here to configure OneLogin.

1. From My Account, select **Manage Seats**, then **Authentication**
2. Add a **SAML2 ID Provider**
3. Switch to the **Service Provider** tab and copy the **Entity ID** and **ACS URL**. Paste these into the **Configuration** tab in your OneLogin application.

The **Entity ID** corresponds to the **Audience (Entity ID)** (this is called **SAML Audience URL** in SCIM), and the **ACS URL** corresponds to both the **ACS (Consumer) URL Validator** and **ACS (Consumer) URL** fields:

**SAML 2.0 Configuration**

Identity Provider      Service Provider      Email Domain(s)

Use this information to configure your identity provider

ENTITY ID  
isapi.geneious.com/sso/gn/saml2/634

ACS URL  
https://isapi.geneious.com/sso/gn/saml2/634

[Download Certificate \(.cer\)](#)  
[Download Metadata \(.xml\)](#)

Applications /  
SAML Custom Connector (Advanced)

More Actions **Save**

<b>Info</b>	<b>Application details</b>
<b>Configuration</b>	<input type="text" value="RelayState"/>
Parameters	<input type="text" value="Audience (EntityID)"/>
Rules	<input type="text" value="isapi. ...."/>
SSO	<input type="text" value="Recipient"/>
Access	<p><small> ⓘ This is generally the same as the <b>ACS (Consumer) URL</b>*</small></p> <input type="text" value="ACS (Consumer) URL Validator*"/>
Users	<p><small> ⓘ *Required.</small></p> <input type="text" value="ACS (Consumer) URL*"/>
Privileges	<p><small> ⓘ *Required</small></p>
Setup	

4. Set the **SAML Initiator** to **Service Provider** and the **SAML signature element** to **Both**. Check that the other fields match the below screenshot. Click **Save**:

The screenshot shows the 'Configuration' tab selected in the left sidebar. The right panel contains several dropdown menus and input fields for SAML configuration. The fields include:

- SAML initiator: Service Provider
- SAML nameID format: Email
- SAML issuer type: Specific
- SAML signature element: Both
- Encrypt assertion: (checkbox)
- SAML encryption method: TRIPLEDES-CBC

5. In the **Parameters** menu, add the following two fields:

- **Field name:** `http://schemas.xmlsoap.org/ws/2005/05/identity/claims/givenname`  
**Value:** First Name
- **Field name:** `http://schemas.xmlsoap.org/ws/2005/05/identity/claims/surname`  
**Value:** Last Name

Select the **Include in SAML assertion** flag (and **Include in User Provisioning** for SCIM)

The screenshot shows the 'Parameters' tab selected in the left sidebar. The right panel displays a table for SCIM Provisioner with SAML (SCIM v2 Enterprise, full SAML) configuration. The table has columns for 'Field' and 'Value'.

Field	Value	
Groups	-No transform- (Single value output)	
Manager ID	- User Manager -	
SAML NameID (Subject)	Email	
department	Department	
<code>http://schemas.xmlsoap.org/ws/2005/05/identity/claims/givenname</code>	First Name	custom parameter
<code>http://schemas.xmlsoap.org/ws/2005/05/identity/claims/surname</code>	Last Name	custom parameter
scimusername	Username	
title	Title	

6. In the SSO menu, set the **SAML Signature Algorithm** to **SHA-256**:

7. From the **More Actions** menu in the top right, download the **SAML Metadata** file
8. Return to My Account and switch to the **Identity Provider** tab. Enter a name e.g. "OneLogin", and copy the content of the downloaded file from OneLogin into the **Metadata XML** field. Click **Save**:

**SAML 2.0 Configuration**

Identity Provider	Service Provider	Email Domain(s)
<b>NAME *</b> <input type="text"/>	<b>STATUS</b> <input type="text" value="Enabled"/>	
<input checked="" type="radio"/> <b>METADATA URL</b> <input type="text"/>		
<input type="radio"/> <b>METADATA XML</b> <input type="radio"/> <b>CONFIGURE MANUALLY</b>		
<input type="button" value="Save"/>		

9. Navigate to the **Domains** tab and add the email domain(s) that you wish to be able to use with SSO. Click **Save**:

**Domains**

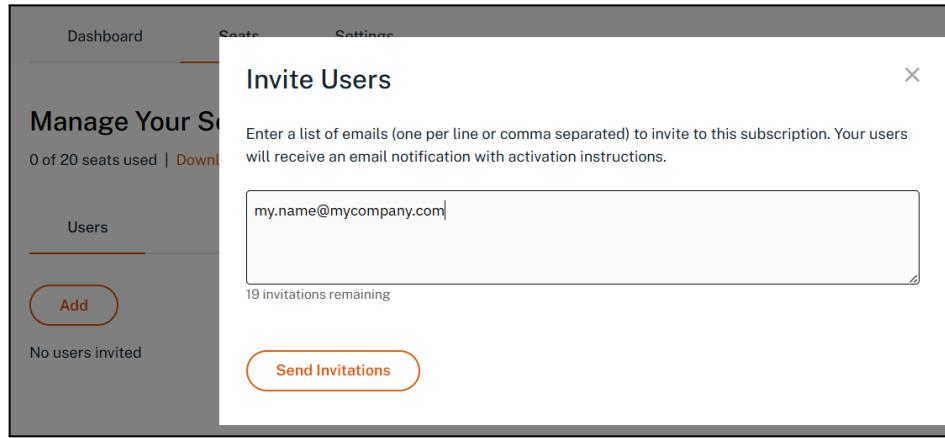
Dashboard	Seats	Settings
<b>Add Domain</b> Enter the domain or sub-domain you want to verify. <b>DOMAIN NAME</b> <input type="text" value="mycompany.com"/> <input type="button" value="Save"/>		
<b>DOMAIN</b>		

10. You will need to verify ownership of this domain. Click **View** and follow the on-screen instructions to verify this, either by HTML file or DNS TXT record.
11. Once verified, return to the **Authentication** tab, and use the **Email Domain(s)** SAML tab to provide email addresses and/or email domains SSO access to Prime. **First, test SSO access with a single email address by adding that email address in full:**

**SAML 2.0 Configuration**

Identity Provider	Service Provider	Email Domain(s)
<b>EMAIL DOMAIN</b> <input type="text" value="Email or domain..."/>		
<input type="button" value="Add"/>		
<b>EMAIL(S) / DOMAIN(S)</b> <b>MODE</b> <b>STATUS</b> my.name@mycompany.com      Email      Enabled <b>Disable</b> <b>Delete</b>		

12. If you are using OneLogin only for SSO, and not SCIM, you will need to invite these user(s) under the **Users** tab in My Account. Otherwise, SCIM users will be provisioned from OneLogin in the SCIM configuration section later in this guide.

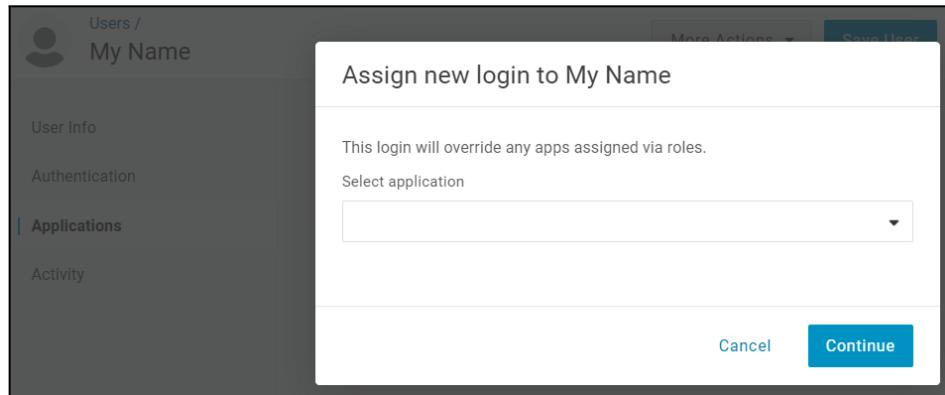


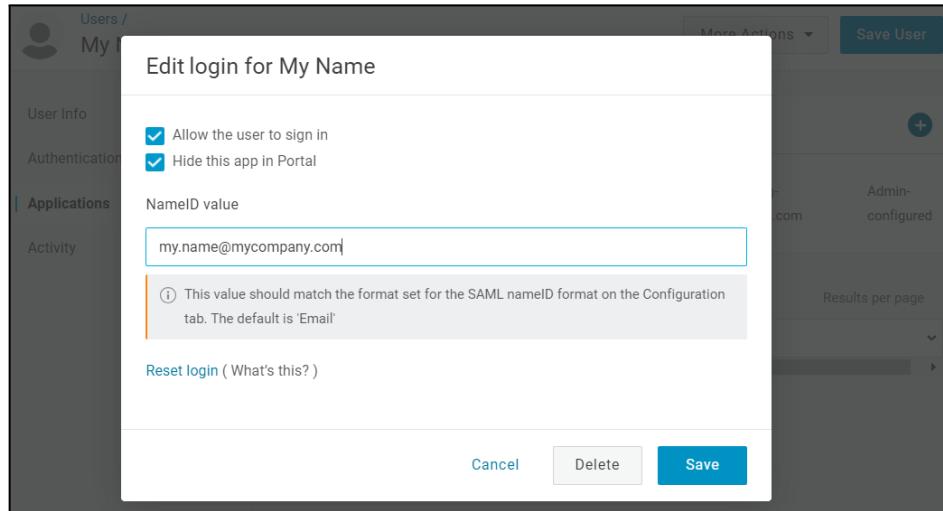
13. If this user does not yet exist in OneLogin, create them in OneLogin now.

From OneLogin, assign this user to your application from the Applications menu.

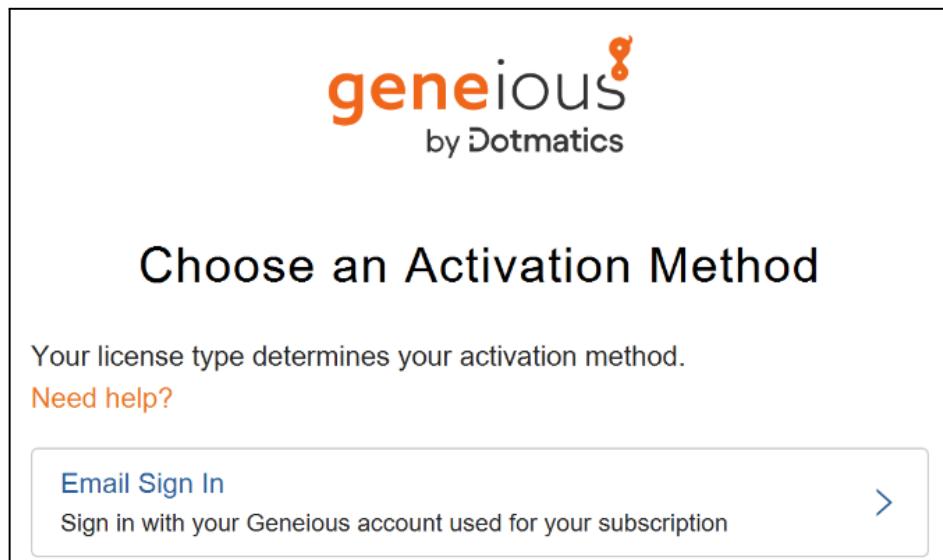
If you are also configuring SCIM, then this process will instead be done later after provisioning has been configured (see the SCIM section of this guide for provisioning users).

Tick **Allow the user to sign in** and **Hide this app in Portal**:





14. In the Prime application, activate your software, selecting the **Email Sign In** option. Continue through the screens, selecting **Log In with SSO** as your authentication method:





## You're All Set

You're now ready to use all of the benefits included with your Geneious subscription.

[Start Using Geneious](#)

15. Once you have verified that Prime activates with this method, and are ready to enable SSO for your entire domain, add the email domain(s) that you wish to use with SSO. Also add the other users in both the **Users** tab of My Account, and in OneLogin as you have above:

EMAIL(S) / DOMAIN(S)	MODE	STATUS	
mycompany.com	Domain	Enabled	<a href="#">Disable</a> <a href="#">Delete</a>

## SCIM Identity Management Configuration

1. To configure SCIM, you will first need to retrieve your Prime connection details from [My Account](#)
  1. From My Account, select **Manage Seats**, then **User Provisioning**
  2. Enable SCIM 2.0 and keep your **SCIM Base URL** and **API Token** handy for the next step:

The screenshot shows the 'User Provisioning' configuration page. At the top, there are three tabs: 'Dashboard', 'Seats', and 'Settings' (which is currently selected). Below the tabs, the title 'User Provisioning' is displayed. A sub-instruction reads: 'Configure automatic provisioning, updating and de-provisioning of users through SCIM. [Learn more](#)'. The 'SCIM 2.0 STATUS' section shows 'ENABLED' in a dropdown menu. The 'Configuration Details' section contains the 'SCIM BASE URL' (set to 'https://directory.geneious.com/directories/a...') and the 'API TOKEN' (set to '\*\*\*\*\*'). A 'Regenerate Token' link is located next to the API token input field. At the bottom, there is a 'Provisioning Errors' section with a dropdown menu.

2. Then in the **Configuration** menu of your OneLogin application:
  1. Add your **SCIM Base URL** and **API Token Key**, copied from My Account, as the **SCIM Base URL** and **SCIM Bearer Token**, respectively
  2. **Enable the API Connection**
  3. Click **Save**

Info

Configuration

Parameters

Rules

SSO

Access

Users

Privileges

**API Connection**

API Status

Enabled  Disable

SCIM Base URL

SCIM JSON Template

```
{
  "schemas": [
    "urn:scim:schemas:core:1.0"
  ],
  "userName": "{$parameters.scimusername}",
  "name": {
    "givenName": "{$user.firstname}"
  }
}
```

Custom Headers

SCIM Bearer Token

3. From the **Provisioning** tab, enable provisioning:

Applications /

SCIM Provisioner with SAML (SCIM v2 Enterprise, full SAML)

More Actions  Save

Info

Configuration

Parameters

Rules

SSO

Access

Provisioning

**Workflow**

Enable provisioning

Require admin approval before this action is performed

Create user

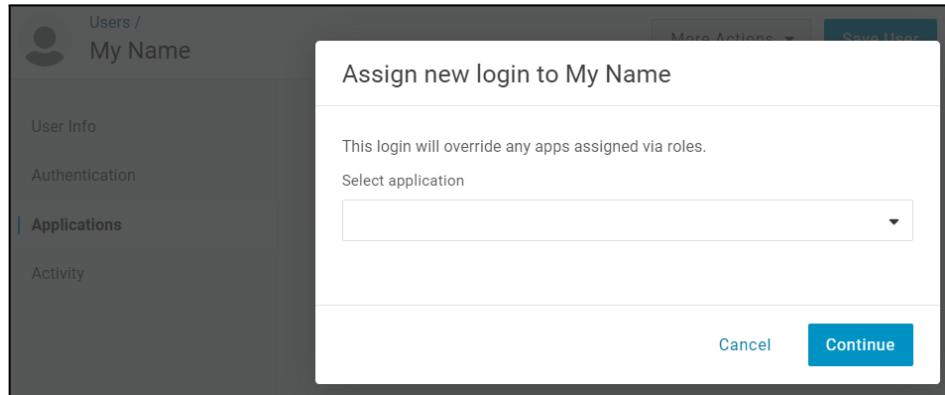
Delete user

Update user

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

4. You have now successfully configured your user provisioning connection between OneLogin and Geneious Prime. You can now provision users from OneLogin into Prime by

1. Navigate to that user from the top level **Users** menu
2. Using the **Applications** side menu of that user, add your application
3. No changes should need to be made in the following screen. Scroll down to confirm that the first name and last name have been mapped correctly from their user account, and click **Save**
4. If the status of the provisioning is showing as **Pending**, then click that status to complete the provisioning



5. Returning to My Account after provisioning is complete will show the end user(s) ready to activate Geneious Prime in the **Seats** tab - please reload the page:

EMAIL	NAME	ACTIVATED ON	DEVICES USED	STATUS
my.name@mycompany.com		0 / 2		PENDING

6. In the Prime application, activate your software, selecting the **Email Sign In** option. Continue through the screens, selecting **Log In with SSO** as your authentication method:

Choose an Activation Method

Your license type determines your activation method.

Need help?

Email Sign In

Sign in with your Geneious account used for your subscription >



## Choose authentication method

my.name@mycompany.com

Your email supports SSO through your organization or Geneious login.

[Log In with SSO](#)

Connects to your organization's single sign-on portal.



## You're All Set

You're now ready to use all of the benefits included with your Geneious subscription.

[Start Using Geneious](#)

## Revoke User

To revoke a user via OneLogin:

1. Either from the **Applications** tab in the **User**, or the **User** tab in the **Application**, delete the association between the two. This may need to be approved in a second step if a status of **Pending** is shown - click the status to do so. Alternatively, remove the group, or the user from the group, if you have assigned a group to the application instead.
2. Return to My Account and refresh the page. That user will now be removed from the **Users** list
3. Finally, in Prime, follow the **Help -> About Prime** menu. Here you will be notified that the activation has been revoked.