



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
- 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.

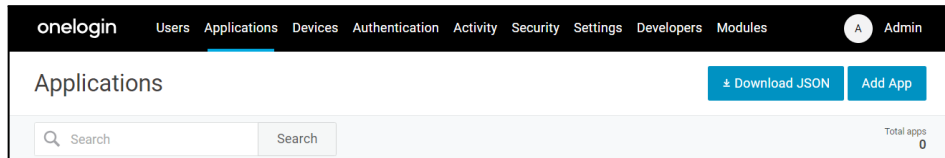
- To download the latest version, visit our [Updates](#) page, or update via the in-app updates feature
- Deactivate your current license by following **Help -> Manage License...**
- Let the Prime team know if your deactivation limit needs to be extended
- After deactivation, Prime should display the 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.

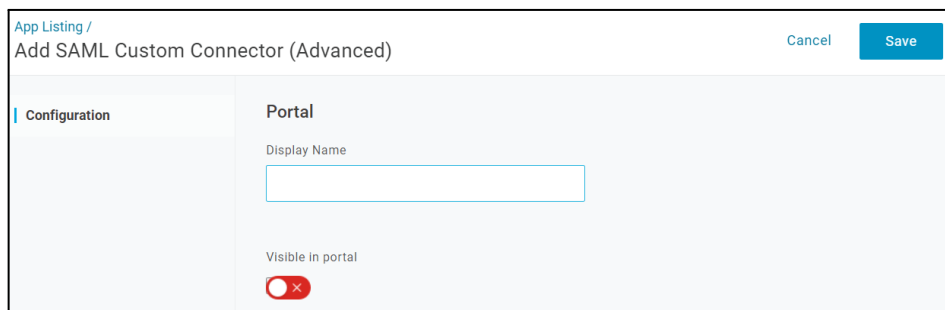
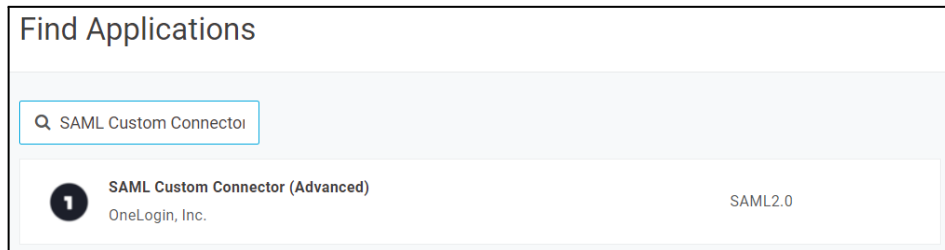
Creating an Application in OneLogin

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



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.

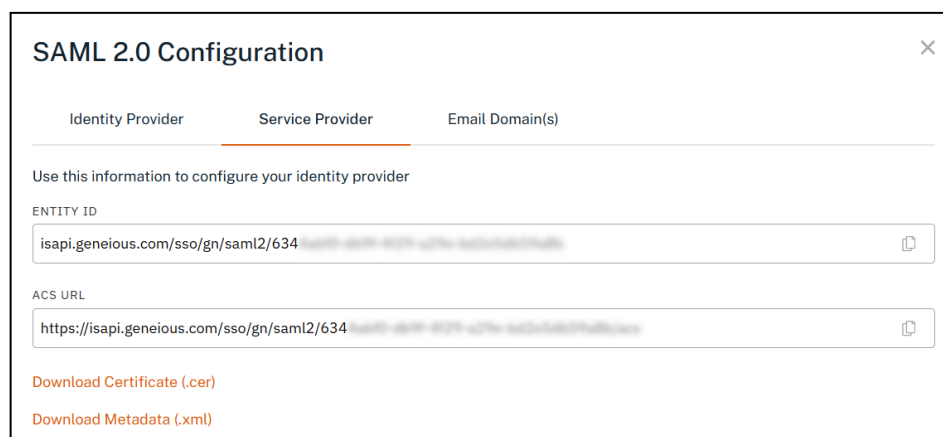


Single sign-on (SSO) Configuration

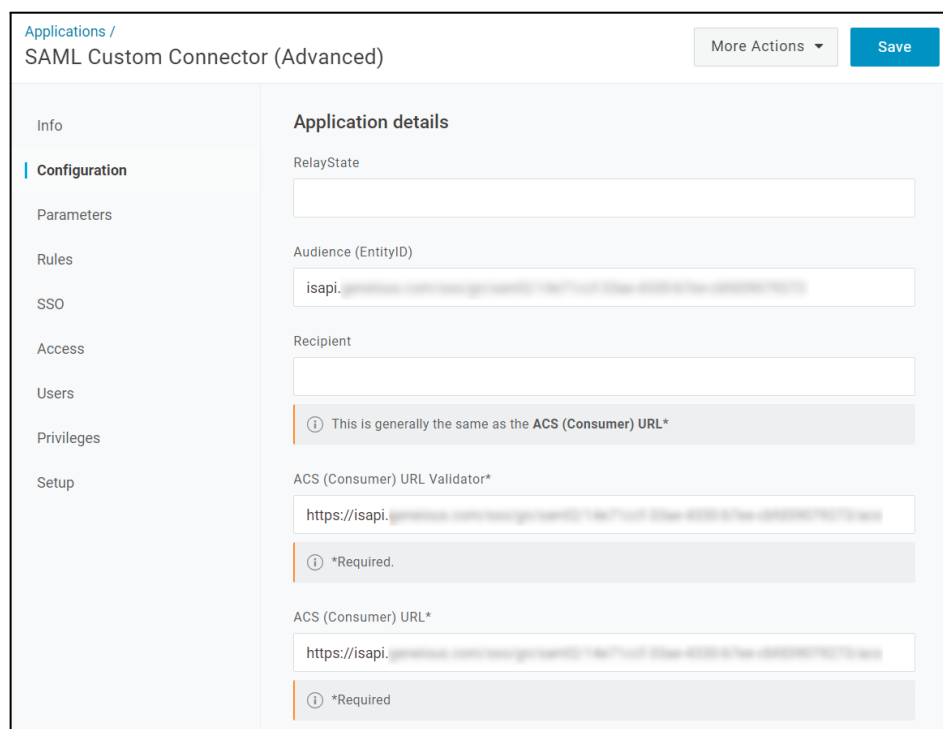
Once created, switch to the **Configuration** tab. Before continuing here, you will need to configure Geneious Prime's [My Account](#), and use information from here to configure OneLogin.

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:



The screenshot shows a 'SAML 2.0 Configuration' dialog box with a close button in the top right. It has three tabs: 'Identity Provider', 'Service Provider' (which is selected and underlined in red), and 'Email Domain(s)'. Below the tabs, it says 'Use this information to configure your identity provider'. There are two input fields: 'ENTITY ID' with the value 'isapi.geneious.com/sso/gn/saml2/634' and 'ACS URL' with the value 'https://isapi.geneious.com/sso/gn/saml2/634'. Both fields have a copy icon to their right. At the bottom, there are two links: 'Download Certificate (.cer)' and 'Download Metadata (.xml)'.



The screenshot shows the 'SAML Custom Connector (Advanced)' configuration page. On the left is a sidebar with a menu: 'Info', 'Configuration' (highlighted with a blue bar), 'Parameters', 'Rules', 'SSO', 'Access', 'Users', 'Privileges', and 'Setup'. The main area is titled 'Application details' and contains several fields: 'RelayState' (empty), 'Audience (EntityID)' with the value 'isapi.geneious.com/sso/gn/saml2/634', 'Recipient' (empty), 'ACS (Consumer) URL Validator*' with the value 'https://isapi.geneious.com/sso/gn/saml2/634', and 'ACS (Consumer) URL*' with the value 'https://isapi.geneious.com/sso/gn/saml2/634'. There are informational icons and text: 'This is generally the same as the ACS (Consumer) URL*' and '*Required.' for the ACS fields. At the top right of the main area are 'More Actions' and 'Save' buttons.

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**:

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)

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

NAME *

STATUS Enabled

☒ METADATA URL

☐ METADATA XML

☐ CONFIGURE MANUALLY

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**:

Dashboard Seats Settings

Domains

Verify your organization's domains

Add Domain

Add Domain

Enter the domain or sub-domain you want to verify.

DOMAIN NAME

Save

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)

EMAIL DOMAIN Add

EMAIL(S) / DOMAIN(S)	MODE	STATUS	
my.name@mycompany.com	Email	Enabled	Disable Delete

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**:

Users / My

More Actions Save User

User Info

Authentication

Applications

Activity

Admin-configured

Results per page

Edit login for My Name

☒ Allow the user to sign in

☒ Hide this app in Portal

NameID value

my.name@mycompany.com

ⓘ This value should match the format set for the SAML nameID format on the Configuration tab. The default is 'Email'

[Reset login \(What's this?\)](#)

Cancel Delete Save

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:

geneious
by Dotmatics

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

geneious
by Dotmatics

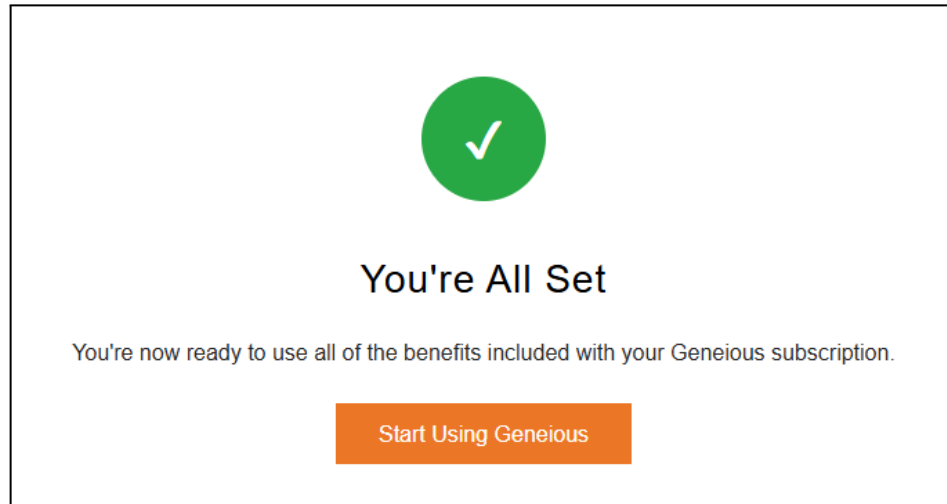
Choose authentication method

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.



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:

SAML 2.0 Configuration

Identity ProviderService ProviderEmail Domain(s)

EMAIL DOMAIN

Email or domain...Add

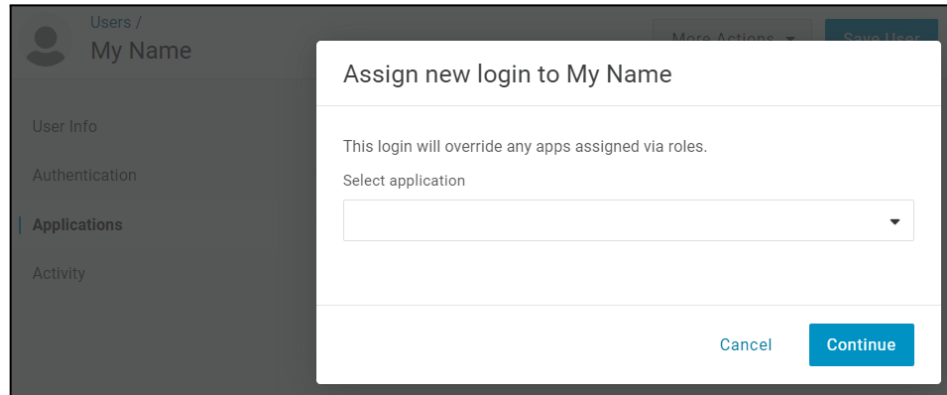
EMAIL(S) / DOMAIN(S)	MODE	STATUS	
mycompany.com	Domain	Enabled	DisableDelete

SCIM Identity Management Configuration

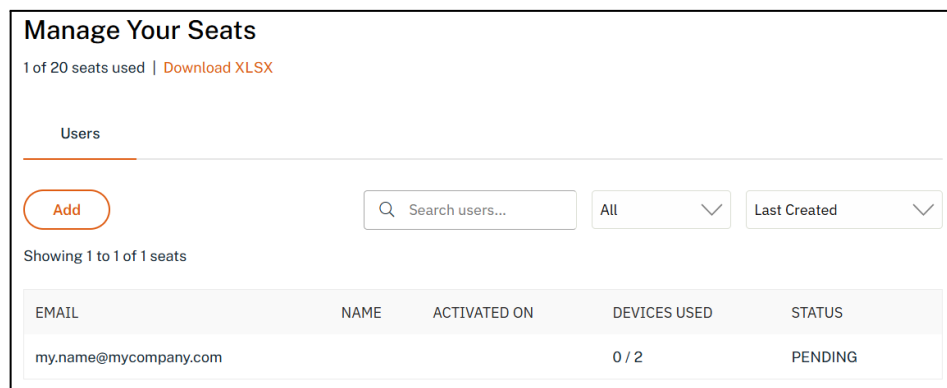
1. To configure SCIM, you will first need to retrieve your Prime connection details from [My Account](#)
 1. From My Account, select **Manage Seats**, then **User Provisioning**
 2. Enable SCIM 2.0 and keep your **SCIM Base URL** and **API Token** handy for the next step:

The screenshot shows the 'User Provisioning' settings page. At the top, there is a navigation bar with 'Dashboard', 'Seats', and 'Settings' (selected). Below the navigation bar, the page title 'User Provisioning' is displayed. A descriptive text states: 'Configure automatic provisioning, updating and de-provisioning of users through SCIM. [Learn more](#)'. The 'SCIM 2.0 STATUS' is set to 'ENABLED' in a dropdown menu. Under 'Configuration Details', it says 'Use this information to set up the SCIM connection from IdP.'. The 'SCIM BASE URL' field contains 'https://directory.geneious.com/directories/a.' with a copy icon. The 'API TOKEN' field is masked with '*****' and has a copy icon and a 'Regenerate Token' link. At the bottom, there is a 'Provisioning Errors' section with a dropdown arrow.

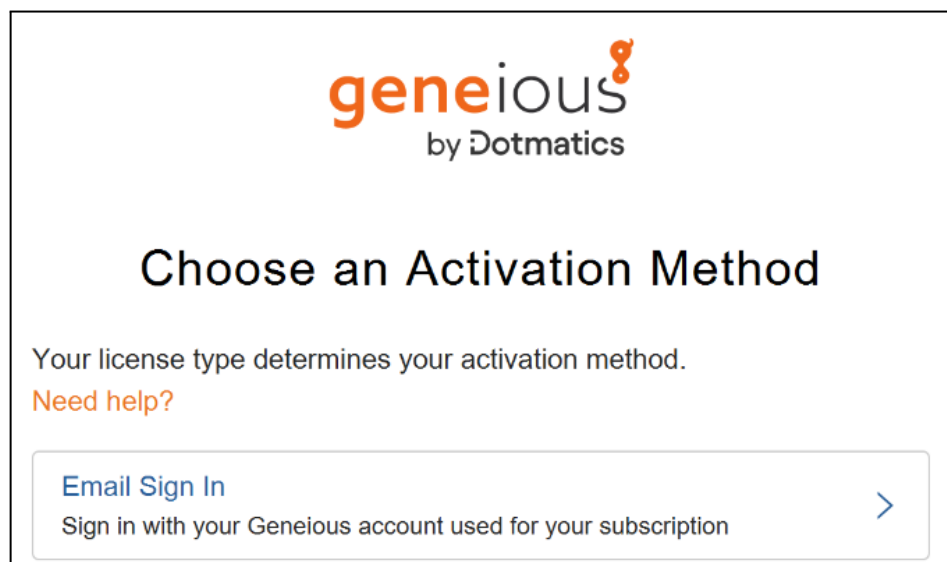
2. Then in the **Configuration** menu of your OneLogin application:
 1. Add your **SCIM Base URL** and **API Token Key**, copied from My Account, as the **SCIM Base URL** and **SCIM Bearer Token**, respectively
 2. **Enable** the **API Connection**
 3. Click **Save**




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:



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:



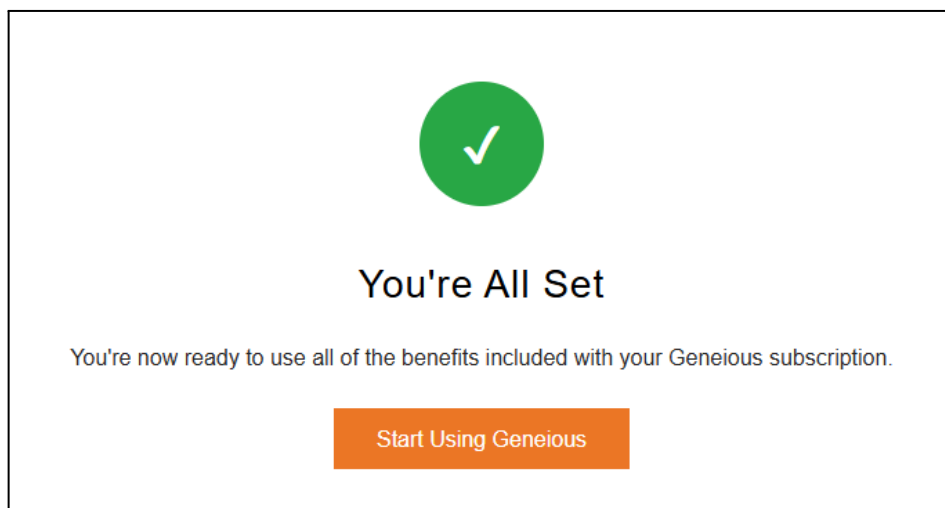


Choose authentication method

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.



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.