OneLogin SSO & SCIM Guide

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.

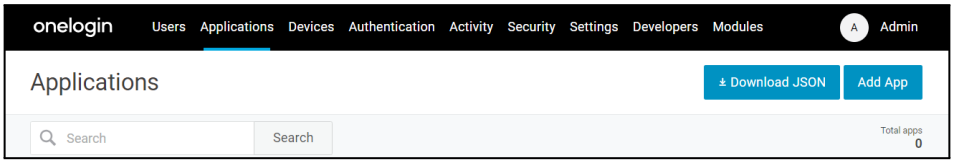
- To download the latest version, visit our Updates page, or update via the in-app updates feature
- Deactivate your current license by following **Help -> Manage License...**
- Let the Prime team know if your deactivation limit needs to be extended
- After deactivation, Prime should display the activation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

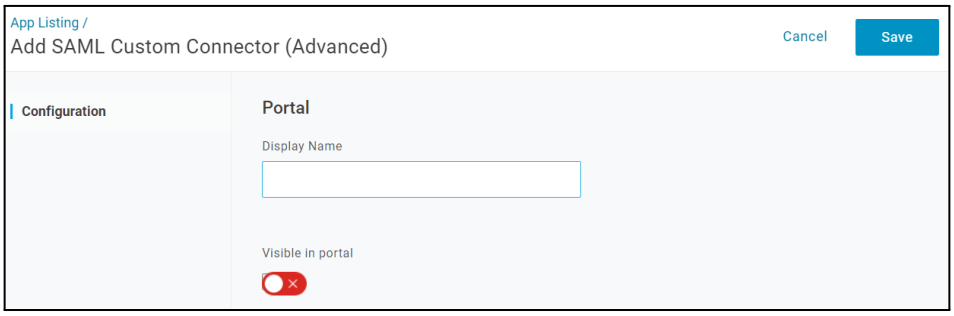
Creating an Application in OneLogin

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.

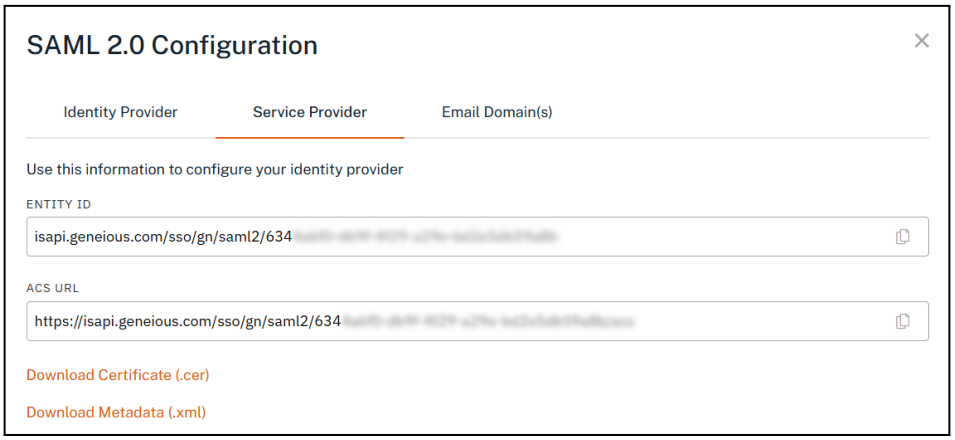


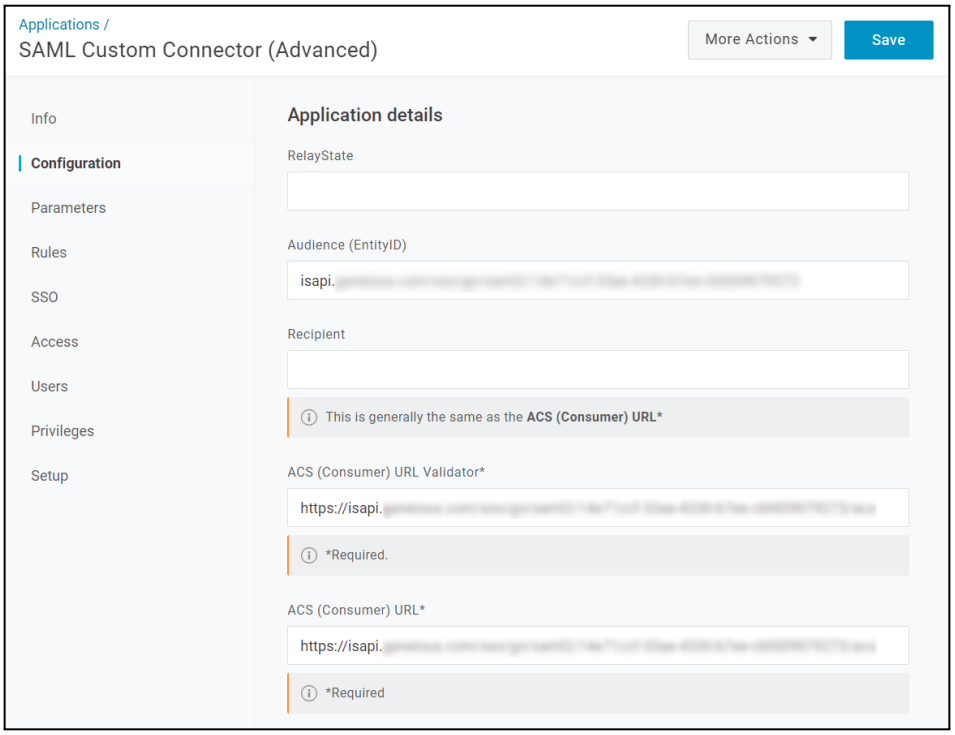
Single sign-on (SSO) Configuration

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.

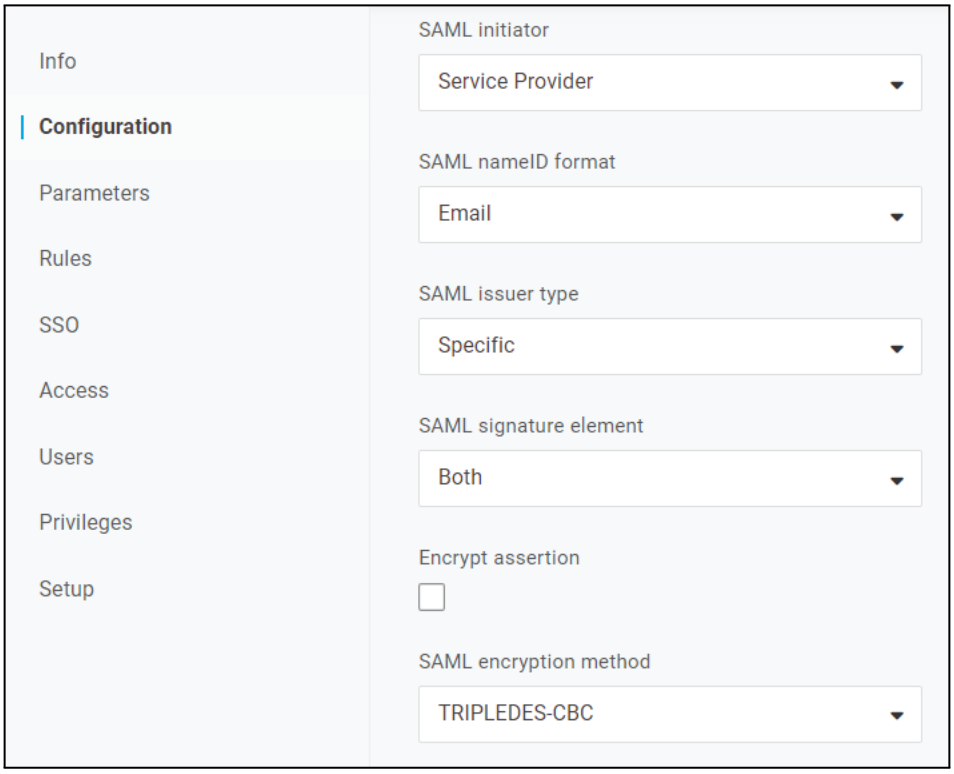
1. From My Account, select **Manage Seats**, then **Authentication**
2. Add a SAML2 **ID Provider**
3. Switch to the **Service Provider** tab and copy the **Entity ID** and **ACS URL**. Paste these into the **Configuration** tab in your OneLogin application.

   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:



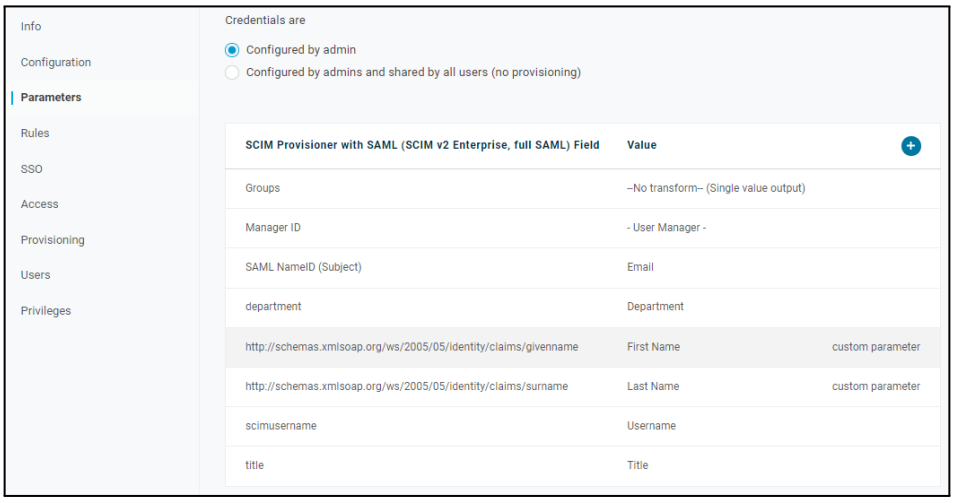


4. Set the **SAML Initiator** to **Service Provider** and the **SAML signature element** to **Both**. Check that the other fields match the below screenshot. Click **Save**:

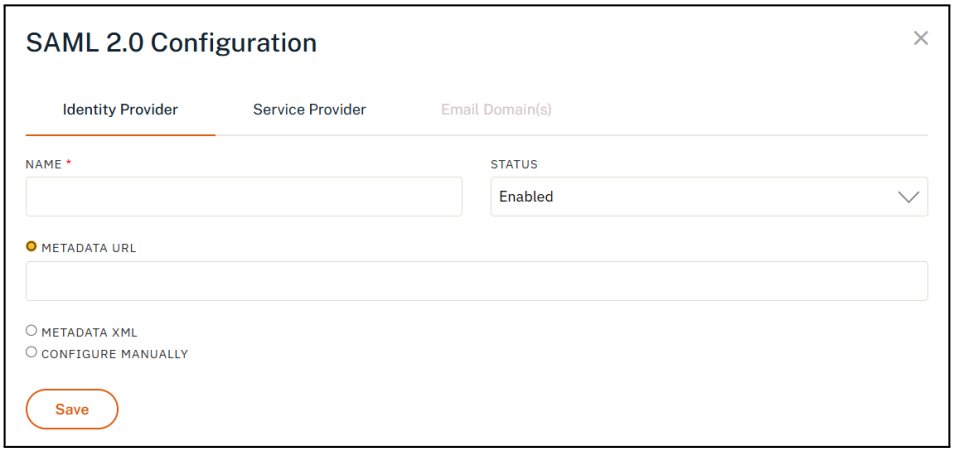


5. In the **Parameters** menu, add the following two fields:
   - **Field name**: `http://schemas.xmlsoap.org/ws/2005/05/identity/claims/givenname` **Value**: First Name
   - **Field name**: `http://schemas.xmlsoap.org/ws/2005/05/identity/claims/surname` **Value**: Last Name

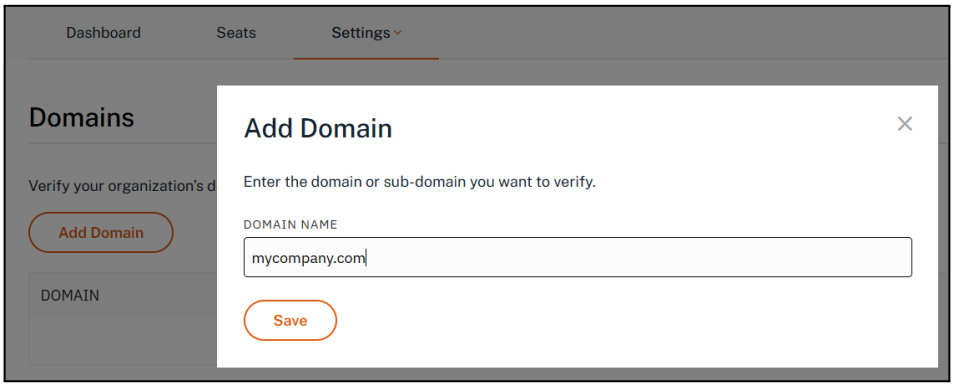
   Select the **Include in SAML assertion** flag (and **Include in User Provisioning** for SCIM)



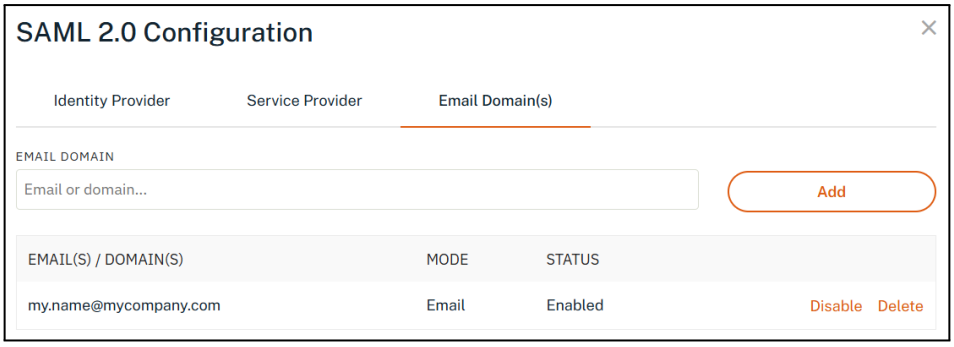
6. In the SSO menu, set the **SAML Signature Algorithm** to **SHA-256**:
7. From the **More Actions** menu in the top right, download the **SAML Metadata** file
8. Return to My Account and switch to the **Identity Provider** tab. Enter a name e.g. “OneLogin”, and copy the content of the downloaded file from OneLogin into the **Metadata XML** field. Click **Save**:



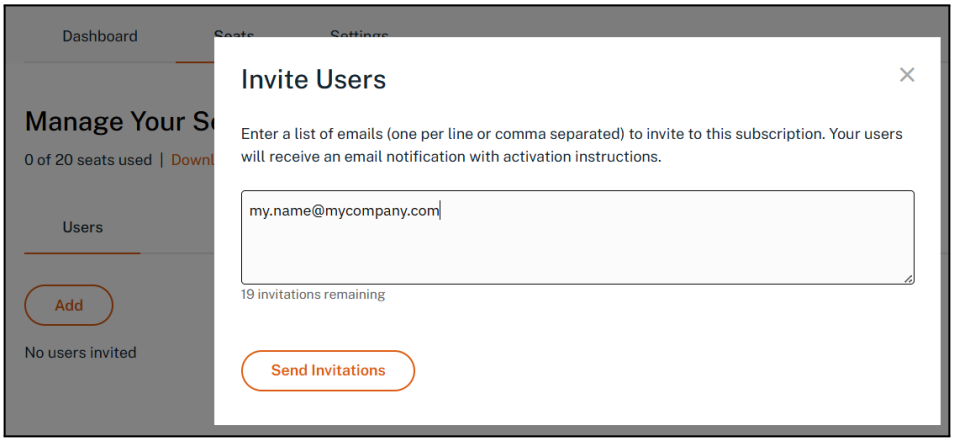
9. Navigate to the **Domains** tab and add the email domain(s) that you wish to be able to use with SSO. Click **Save**:



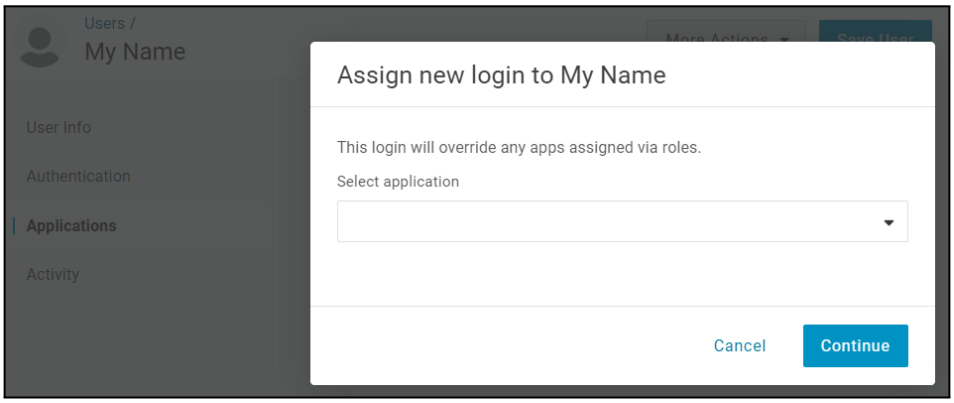
10. You will need to verify ownership of this domain. Click **View** and follow the on-screen instructions to verify this, either by HTML file or DNS TXT record.
11. Once verified, return to the **Authentication** tab, and use the **Email Domain(s)** SAML tab to provide email addresses and/or email domains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

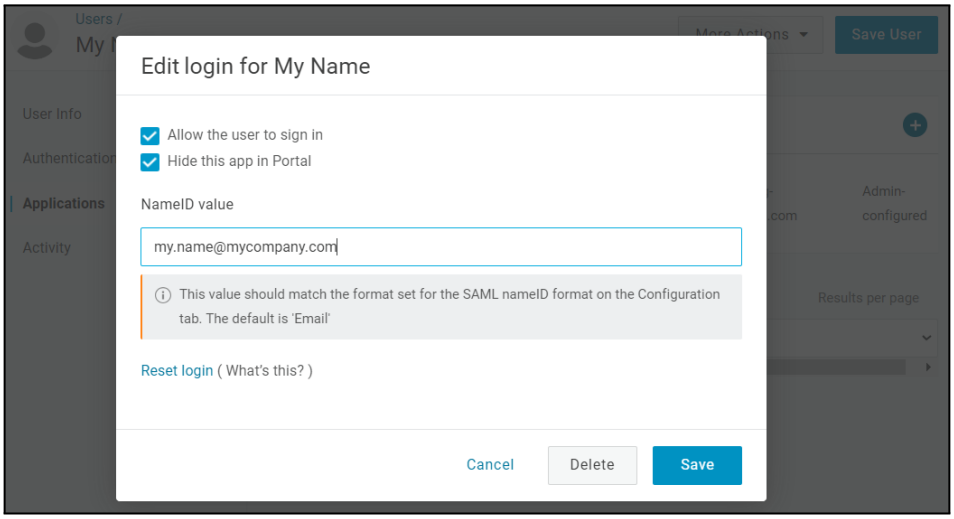


12. If you are using OneLogin only for SSO, and not SCIM, you will need to invite these user(s) under the **Users** tab in My Account. Otherwise, SCIM users will be provisioned from OneLogin in the SCIM configuration section later in this guide.

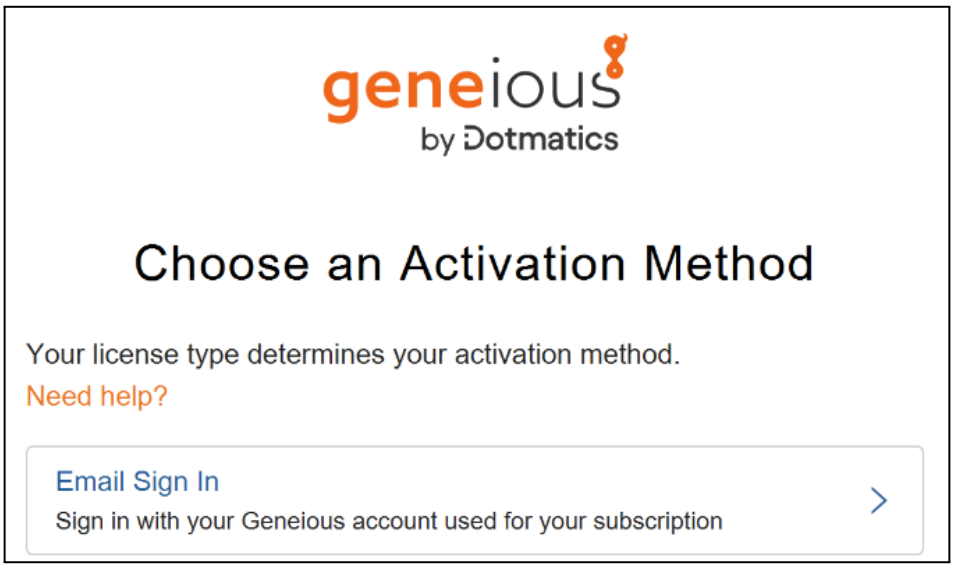


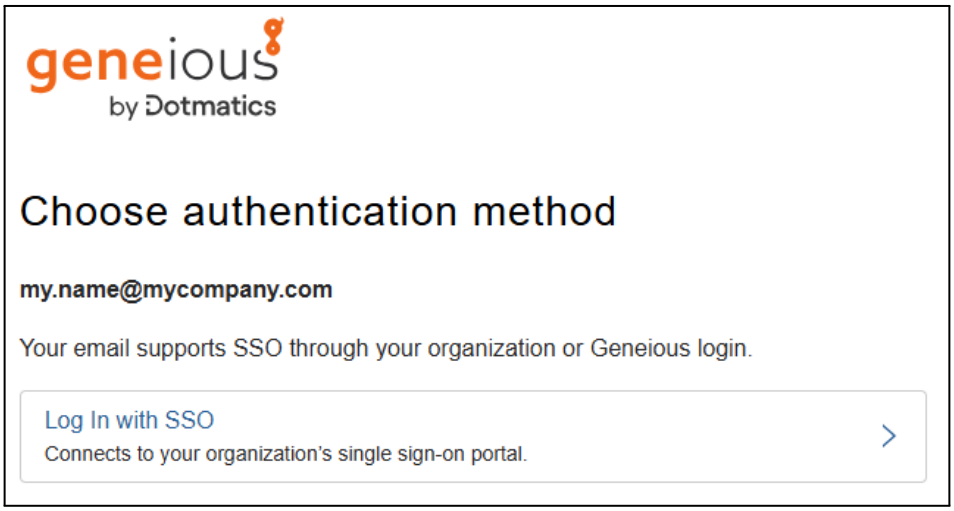
13. If this user does not yet exist in OneLogin, create them in OneLogin now.
    From OneLogin, assign this user to your application from the Applications menu.
    If you are also configuring SCIM, then this process will instead be done later after provisioning has been configured (see the SCIM section of this guide for provisioning users).
    Tick **Allow the user to sign in** and **Hide this app in Portal**:

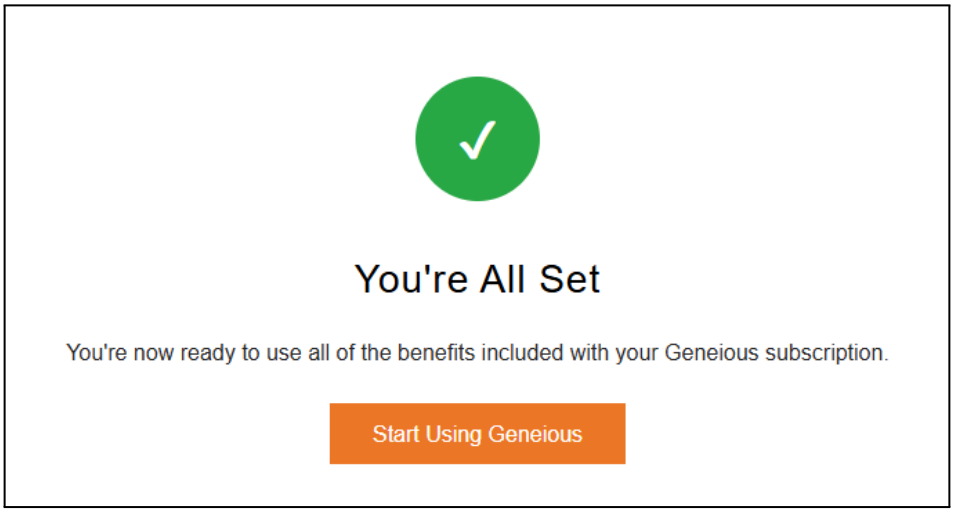




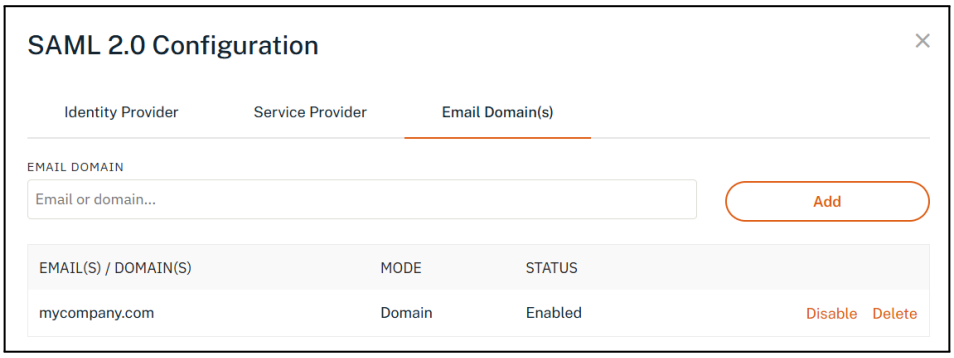
14. In the Prime application, activate your software, selecting the **Email Sign In** option. Continue through the screens, selecting **Log In with SSO** as your authentication method:





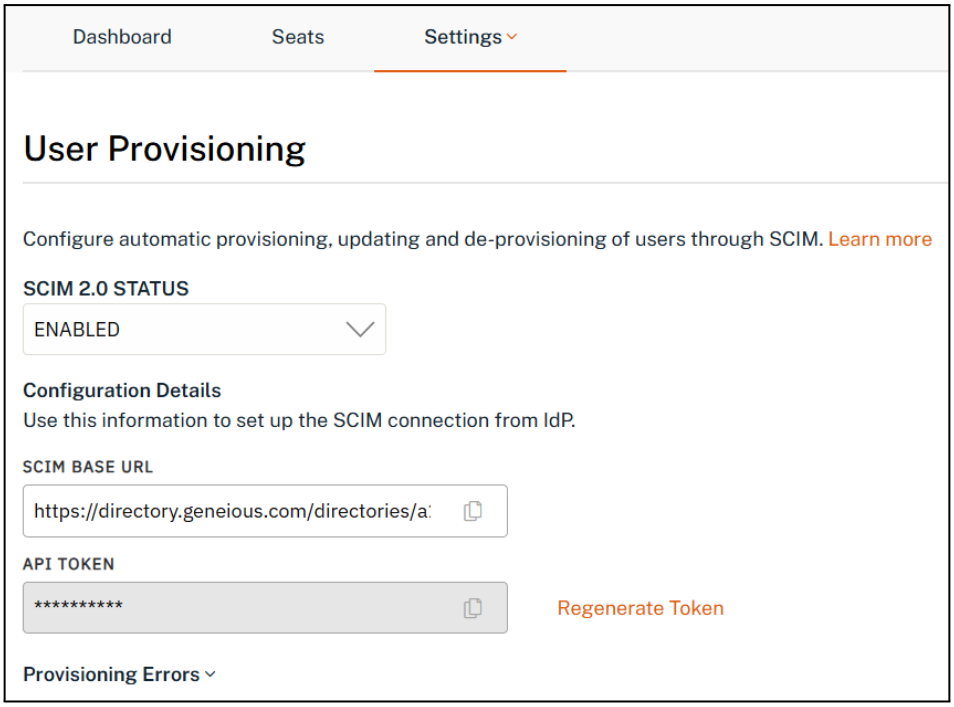


15. Once you have verified that Prime activates with this method, and are ready to enable SSO for your entire domain, add the email domain(s) that you wish to use with SSO. Also add the other users in both the **Users** tab of My Account, and in OneLogin as you have above:

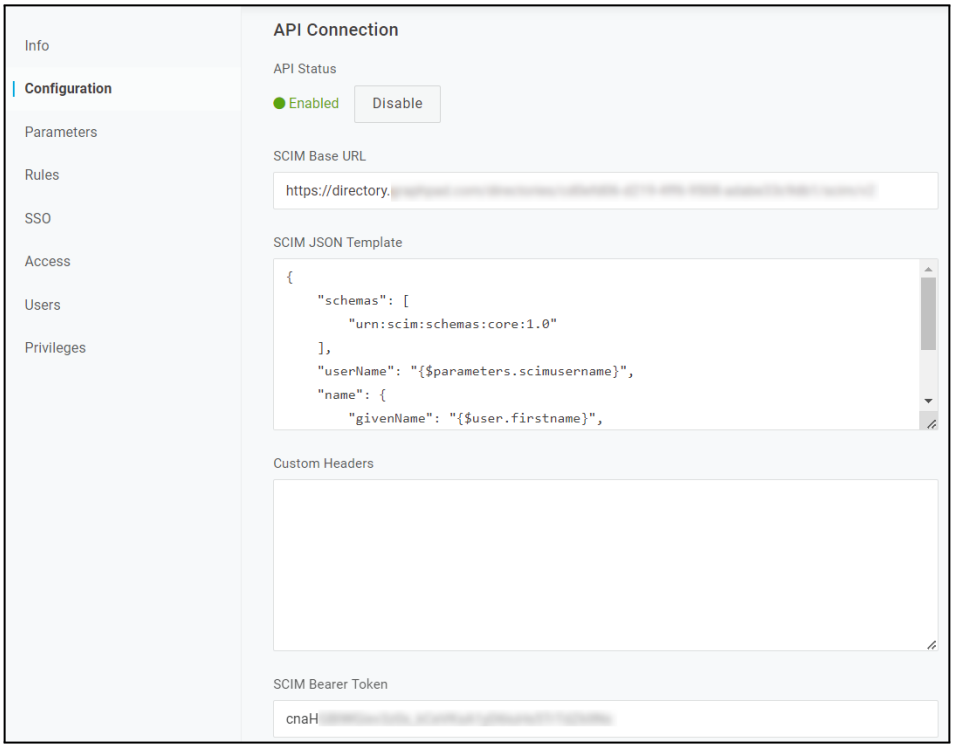


SCIM Identity Management Configuration

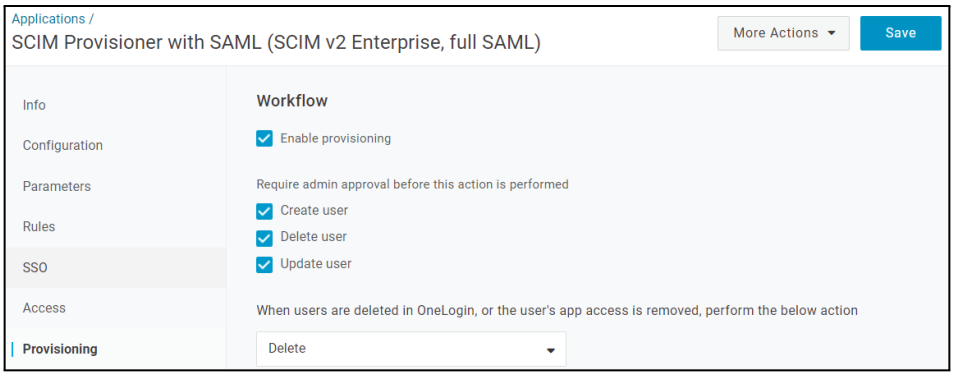
1. To configure SCIM, you will first need to retrieve your Prime connection details from My Account
    1. From My Account, select **Manage Seats**, then **User Provisioning**
    2. Enable SCIM 2.0 and keep your **SCIM Base URL** and **API Token** handy for the next step:



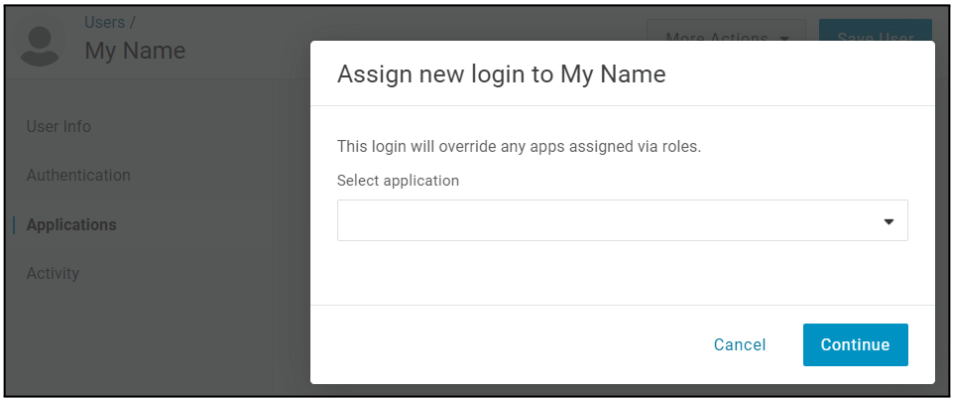
2. Then in the **Configuration** menu of your OneLogin application:
    1. Add your **SCIM Base URL** and **API Token Key**, copied from My Account, as the **SCIM Base URL** and **SCIM Bearer Token**, respectively
    2. **Enable** the **API Connection**
    3. Click **Save**



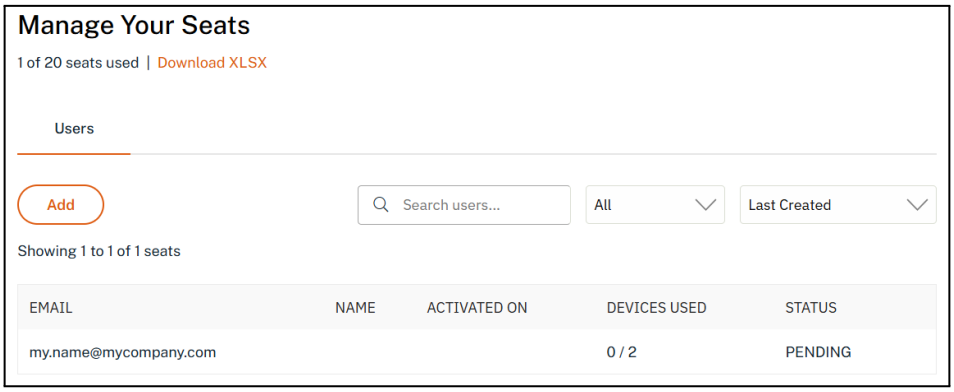
3. From the **Provisioning** tab, enable provisioning:



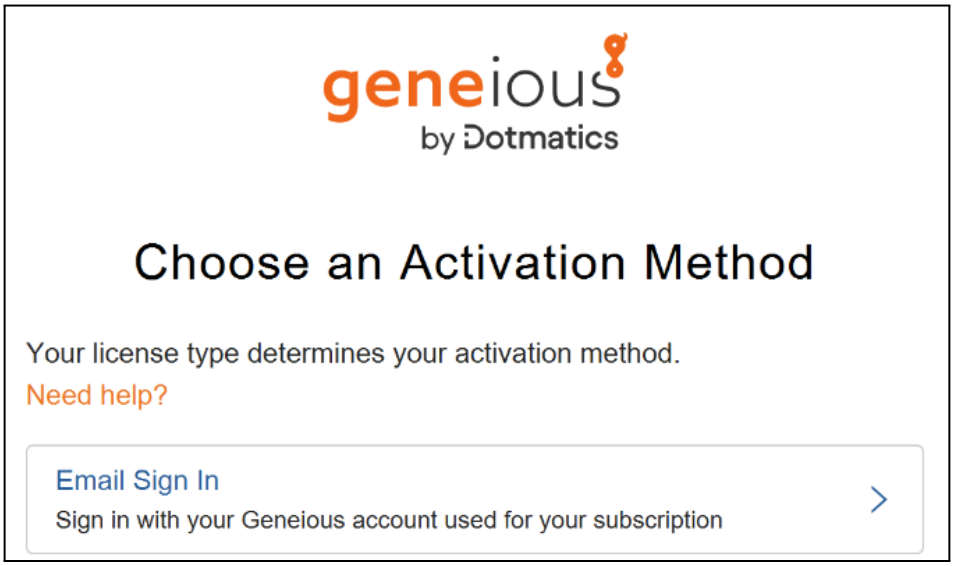
4. You have now successfully configured your user provisioning connection between OneLogin and Geneious Prime. You can now provision users from OneLogin into Prime by
    1. Navigate to that user from the top level **Users** menu
    2. Using the **Applications** side menu of that user, add your application
    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

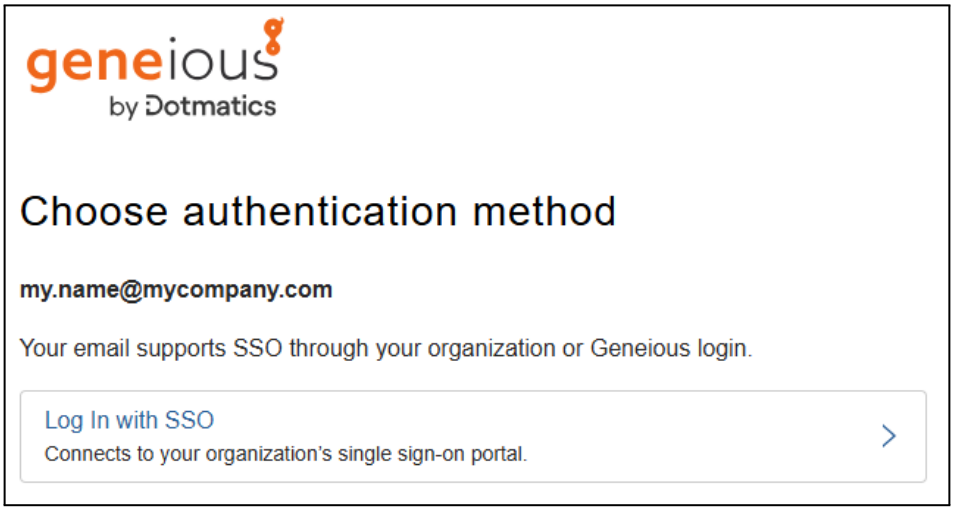


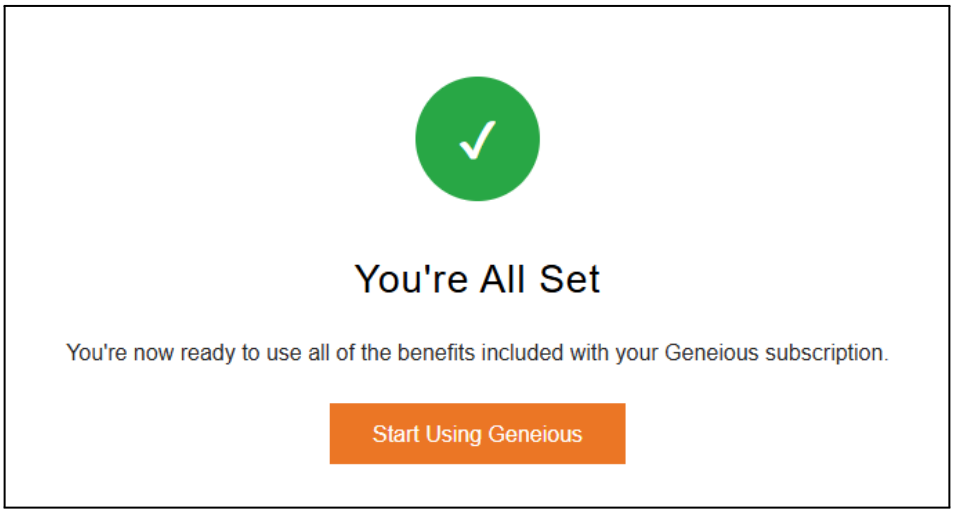
5. Returning to My Account after provisioning is complete will show the end user(s) ready to activate Geneious Prime in the **Seats** tab - please reload the page:



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:







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.