



# JumpCloud SSO & SCIM Guide

Getting Started . . . . .	1
Accessing your user-based license . . . . .	1
Preparing Prime . . . . .	1
JumpCloud Configuration . . . . .	1
Creating an Application in JumpCloud . . . . .	2
Single sign-on (SSO) Configuration . . . . .	4
SCIM Identity Management Configuration . . . . .	9
Revoke User . . . . .	11

## 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](https://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.

### JumpCloud Configuration

To use JumpCloud 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 JumpCloud, while the third configures SCIM for identity management.


## Creating an Application in JumpCloud

1. From the **SSO Applications** side menu in JumpCloud, select **Add New Application**. From here, select **Custom Application**, and follow the on-screen instructions:

The screenshot shows the 'Create New Application Integration' wizard with a four-step progress bar at the top: 1. Select Application, 2. Select Options, 3. Enter General Info, and 4. Review. The current step is 'Select Application', which asks 'Which application would you like to integrate?' and provides a search bar. Below the search bar is a 'Featured Applications' section with the subtitle 'Our most popular and powerful integrations.' It contains eight application cards, each with a logo, a brief description of integration capabilities, and a 'Select' button. The applications are: Google Workspace, AWS IAM Identity Center, Slack, Atlassian Cloud, Personio, Crowdstrike, Salesforce, and a 'Custom Application' option. The 'Custom Application' card is highlighted with a dashed border and includes the text: 'Can't find what you're looking for? Connect to any application with a custom integration.' A 'View More' link is located at the bottom right of the featured applications section.

Application	Integration Capabilities
Google Workspace	Enable SSO, sync users and groups from JumpCloud, import users into JumpCloud
aws IAM Identity Center	Enable SSO, sync users and groups from JumpCloud, import and update users in JumpCloud
slack	Enable SSO, sync users and groups from JumpCloud, import and update users in JumpCloud
Atlassian Cloud	Enable SSO, sync users and groups from JumpCloud, import and update users in JumpCloud
Personio	Enable SSO, import and update users into JumpCloud
CROWDSTRIKE	Enable SSO, import users into JumpCloud
salesforce	Enable SSO, sync users and groups from JumpCloud, import and update users in JumpCloud
Custom Application	Can't find what you're looking for? Connect to any application with a custom integration.

2. Select **Manage Single Sign-On (SSO)** and **Configure SSO with SAML**.  
To use JumpCloud as the identity authority for SCIM user provisioning, also select **Export users to this app (Identity Management)**, then click **Next**:



### Select the features you would like to enable

Select all features you would like to enable for your application.

Need help deciding? [Learn More](#)

☒

#### Manage Single Sign-On (SSO)

Allow users to securely authenticate into this application using JumpCloud.

Select One

☒ Configure SSO with SAML  
☐ Configure SSO with OIDC

☐

#### Import users from this app (Identity Management)

Import new users and user updates into JumpCloud from this application.

☒

#### Export users to this app (Identity Management)

Provision new users and user updates from JumpCloud to this application. JumpCloud will become the authority of the identity. Manage users in JumpCloud and have any changes to identities reflected to this application.


☐

#### Add a bookmark (no SSO)

Create a URL bookmark without SSO. If this application does not support SSO, the JumpCloud Password Manager can integrate with any application to secure and streamline the password authentication process.

Cancel
Back
Next

3. Add the application name and any other display customisation you would like
4. Untick **Show this application in User Portal**
5. Click **Save Application**, then **Configure Application**:







### Enter general info





These details will be displayed to end users unless the option to show in User Portal is unchecked.





Display Label \*


User Portal Image

☐ Logo  
☒ Color Indicator

☒ 
☐ 
☐ 
☐ 

☐ 
☐ 
☐ 
☐ 

☐ 
☐ 
☐ 
☐ 



Color Selected: Blue

**Show in User Portal**

Applications appear in the User Portal for any bound users by default. When deselected, the application will not appear in the User Portal for any users, and any users bound to the application will still be enabled for SSO access.

☐ Show this application in User Portal

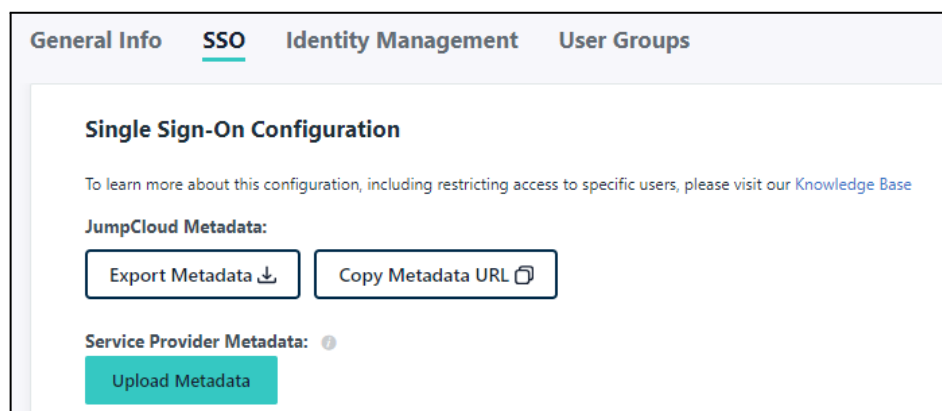
[Advanced Settings](#)

Cancel
Back
Save Application

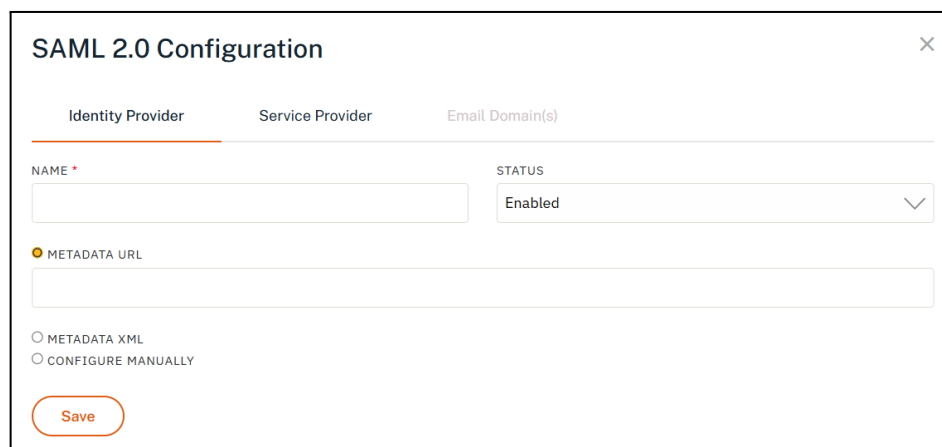
## Single sign-on (SSO) Configuration

You'll next be presented with further configuration options in JumpCloud. Before continuing here, you will need to configure Geneious Prime's [My Account](#), and use information from here to configure JumpCloud.

1. From My Account, select **Manage Seats**, then **Authentication**
2. Add a SAML2 **ID Provider**
3. Copy the **Metadata URL** from the **SSO** tab in JumpCloud
4. Enter a name e.g. "JumpCloud", and paste in the Metadata URL from JumpCloud. Click **Save**:



The screenshot shows the 'Single Sign-On Configuration' page in JumpCloud. The page has four tabs: 'General Info', 'SSO' (which is selected and underlined), 'Identity Management', and 'User Groups'. Below the tabs, the title 'Single Sign-On Configuration' is displayed. A link to the 'Knowledge Base' is provided for more information. Under 'JumpCloud Metadata:', there are two buttons: 'Export Metadata' with a download icon and 'Copy Metadata URL' with a copy icon. Under 'Service Provider Metadata:', there is a teal 'Upload Metadata' button.



The screenshot shows the 'SAML 2.0 Configuration' modal window. It has three tabs: 'Identity Provider' (selected), 'Service Provider', and 'Email Domain(s)'. The 'Identity Provider' tab contains a 'NAME' field with an asterisk, a 'STATUS' dropdown menu set to 'Enabled', a 'METADATA URL' field with a yellow dot icon, and two radio buttons: 'METADATA XML' and 'CONFIGURE MANUALLY'. A red 'Save' button is at the bottom.

5. Next, we need to provide JumpCloud with Prime's details. Switch to the **Service Provider** tab and copy the **Entity ID** and **ACS URL**, and paste these into JumpCloud's **SP Entity ID** and **ACS URL**, respectively. Alternatively, you can upload the XML Metadata file available from My Account
6. Select **emailAddress** as the **SAMLSubject NameID Format**
7. Select **Assertion and Response** as the **Sign**
8. Add two **User Attributes**, and **save**:
  - <http://schemas.xmlsoap.org/ws/2005/05/identity/claims/givenname> - firstname
  - <http://schemas.xmlsoap.org/ws/2005/05/identity/claims/surname> - lastname

## SAML 2.0 Configuration ✕

Identity Provider
Service Provider
Email Domain(s)

Use this information to configure your identity provider

ENTITY ID

ACS URL

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

SP Entity ID: ⓘ

ACS URLs ⓘ

Enter at least one ACS URL. IdP initiated logins will use the first, or lowest index. ACS URL listed. The ACS URL used for SP initiated logins will depend on the authentication request received.

Index	Default URL *	
0	https://isapi/	

SAMLSubject NameID Format: ⓘ

Signature Algorithm: ⓘ

Sign \* ⓘ

☐ Response  
☐ Assertion  
☒ Assertion and Response

### Attributes

If attributes are required by this Service Provider for SSO authentication, they are not editable. Additional attributes may be included in assertions, although support for each attribute will vary for each Service Provider. [Learn more.](#)

User Attributes: ⓘ

Service Provider Attribute Name	JumpCloud Attribute Name	
http://schemas.xmlsoap.org/ws/2005/05/identity/claims/givenname	firstname	
http://schemas.xmlsoap.org/ws/2005/05/identity/claims/surname	lastname	

- 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 domain

**Add Domain**

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

DOMAIN NAME

mycompany.com

**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

Email or domain... **Add**

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

**Disable Delete**

12. If you are using JumpCloud 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 JumpCloud in the SCIM configuration section later in this guide.

Dashboard Seats **Settings**

**Manage Your Subscription**

0 of 20 seats used | Download

**Users**

**Add**

No users invited

**Invite Users**

Enter a list of emails (one per line or comma separated) to invite to this subscription. Your users will receive an email notification with activation instructions.

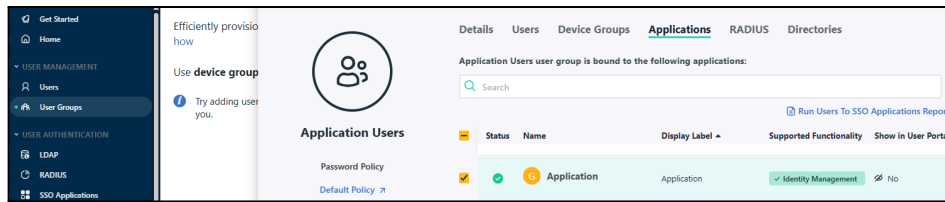
my.name@mycompany.com

19 invitations remaining

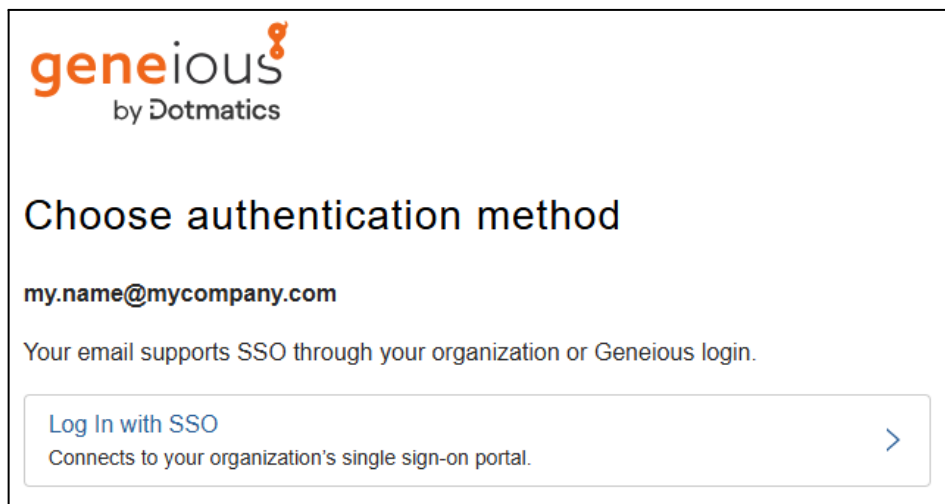
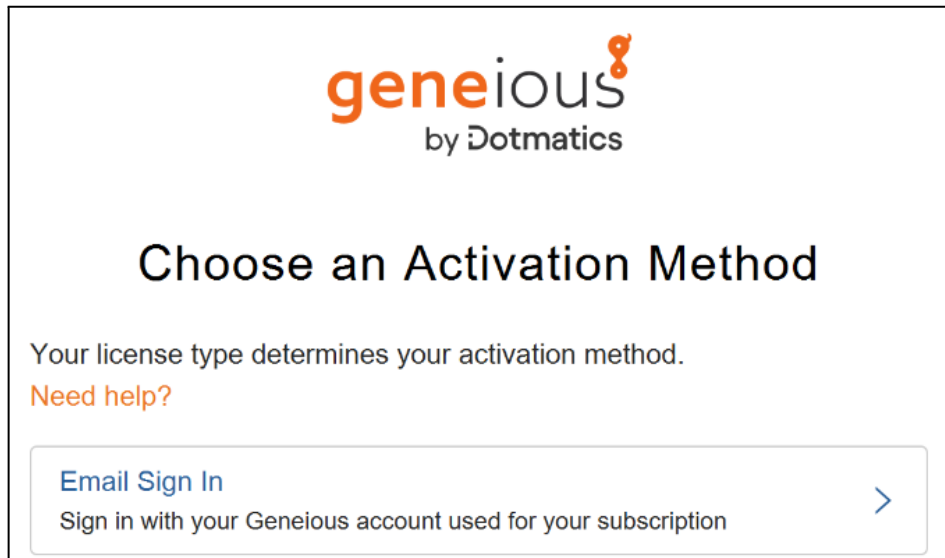
**Send Invitations**

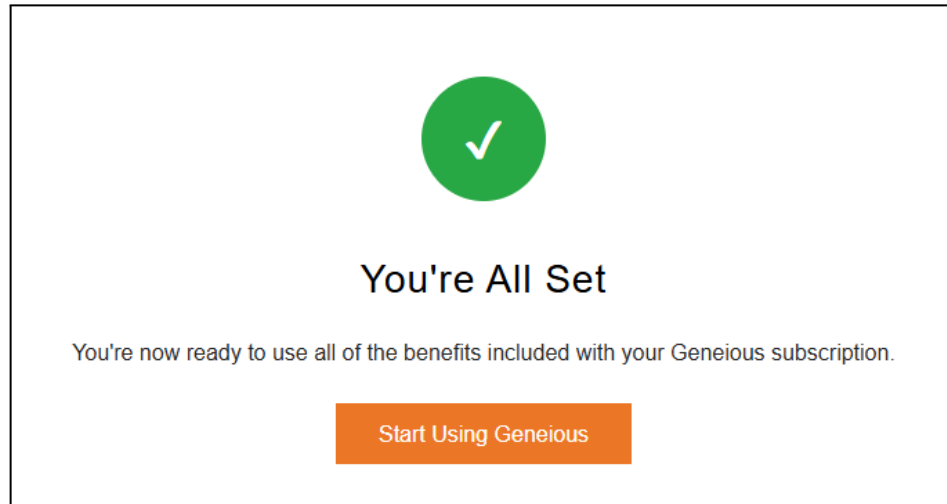
13. If this user does not yet exist in JumpCloud, create them in JumpCloud now. From JumpCloud, assign this user to your application from the Applications tab of the user's User Group. If you are also configuring SCIM, then this process will instead be done later after provisioning

has been configured (see the SCIM section of this guide for provisioning users).



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 JumpCloud 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

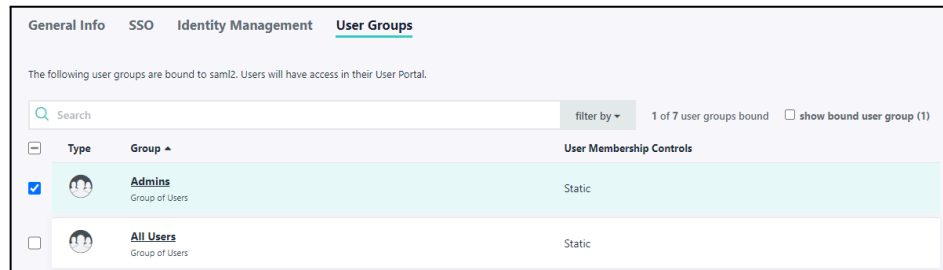
1. To configure SCIM, you will first need to retrieve your Prime connection details from [My Account](#)
  1. From My Account, select **Manage Seats**, then **User Provisioning**
  2. Enable SCIM 2.0 and keep your **SCIM Base URL** and **API Token** handy for the next step:

The screenshot shows the 'User Provisioning' settings page. At the top, there are tabs for 'Dashboard', 'Seats', and 'Settings'. The 'Settings' tab is active. Below the tabs, the page title is 'User Provisioning'. A description states: 'Configure automatic provisioning, updating and de-provisioning of users through SCIM. [Learn more](#)'. Under 'SCIM 2.0 STATUS', there is a dropdown menu set to 'ENABLED'. Below this, 'Configuration Details' are shown, including the 'SCIM BASE URL' (https://directory.geneious.com/directories/a) and the 'API TOKEN' (masked with asterisks). A 'Regenerate Token' button is next to the API token field. At the bottom, there is a 'Provisioning Errors' section with a dropdown arrow.

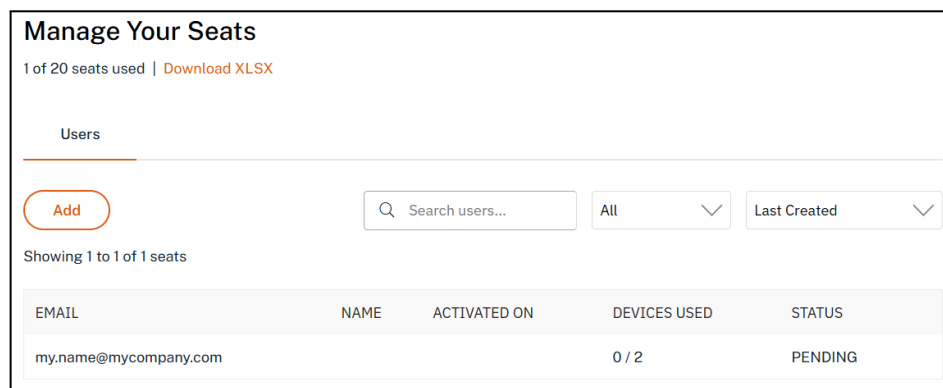
2. Then in the **Identity Management** tab of your JumpCloud application:
  1. Select **SCIM API** as the **API Type**
  2. Select **SCIM 2.0** as the **SCIM Version**
  3. Add your **SCIM Base URL** and **API Token Key**, copied from My Account
  4. Enter an email address that you own as the Test User Email
  5. Click **Test Connection**
  6. Click **Activate** and **Save**

The screenshot shows the 'Identity Management' configuration page. At the top, there are tabs for 'General Info', 'SSO', 'Identity Management', and 'User Groups'. The 'Identity Management' tab is active. Below the tabs, the page title is 'Configuration Settings'. Under 'Service Provider (SP) Configuration', there is a section for 'API Type' with two buttons: 'SCIM API' (selected) and 'Custom API Import'. Below this, a note states: 'SCIM API lets you configure a real-time provisioning/ deprovisioning or an import integration. [Learn More](#)'. Under 'Mutual TLS (mTLS)', there is a checkbox for 'Use mTLS' which is unchecked. Below this, there is a section for 'SCIM Version' with two buttons: 'SCIM 1.1' and 'SCIM 2.0' (selected). At the bottom, there are fields for 'Base URL\*' (https://directory. /scim/v2) and 'Token Key' (masked with asterisks). Below these fields is a 'Test User Email\*' field with the value email@domain.com.

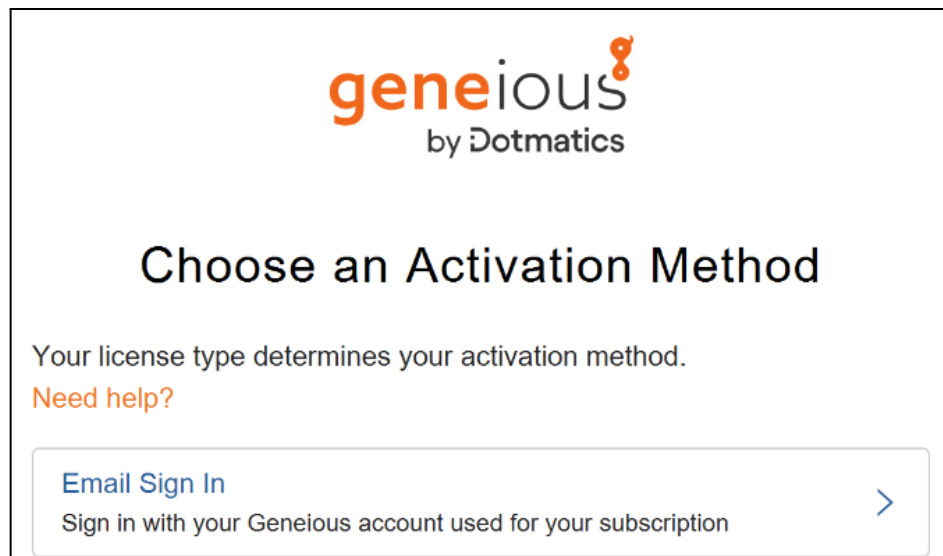
3. You have now successfully configured your user provisioning connection between JumpCloud and Geneious Prime. You can now provision users from JumpCloud into Prime by selecting a given User Group in the JumpCloud application's **User Groups** tab, and clicking **Save**:



4. 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:



5. 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:



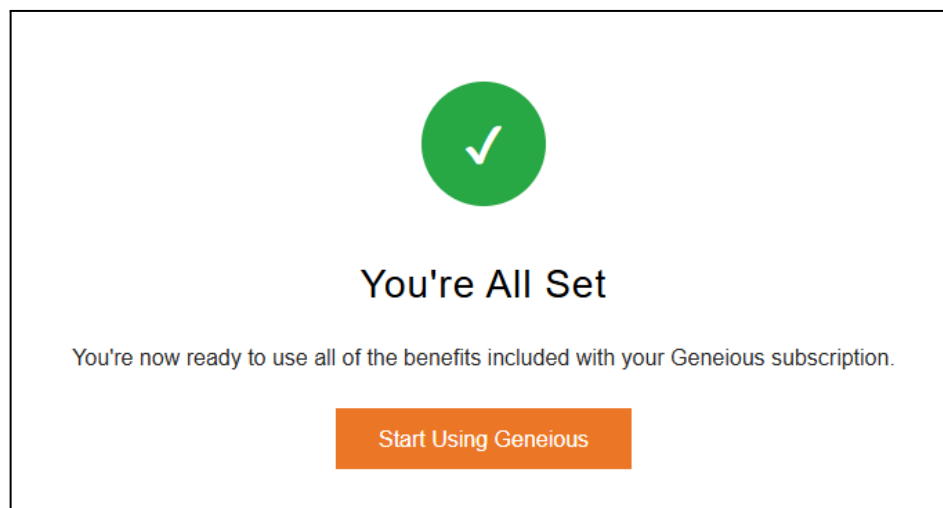
geneious<sup>g</sup>  
by Dotmatics

## Choose authentication method

my.name@mycompany.com

Your email supports SSO through your organization or Geneious login.

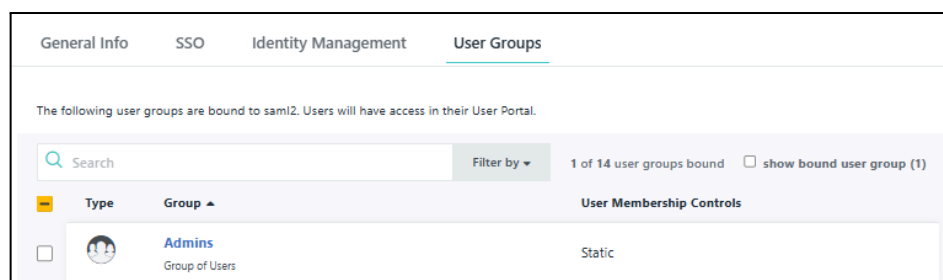
[Log In with SSO](#) >  
Connects to your organization's single sign-on portal.



### Revoke User

To revoke a user via JumpCloud:

1. In the **User Groups** menu within your **Configured Application**, unselect the group and click **Save**:



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.