Dotmatics Geneious

Okta 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.

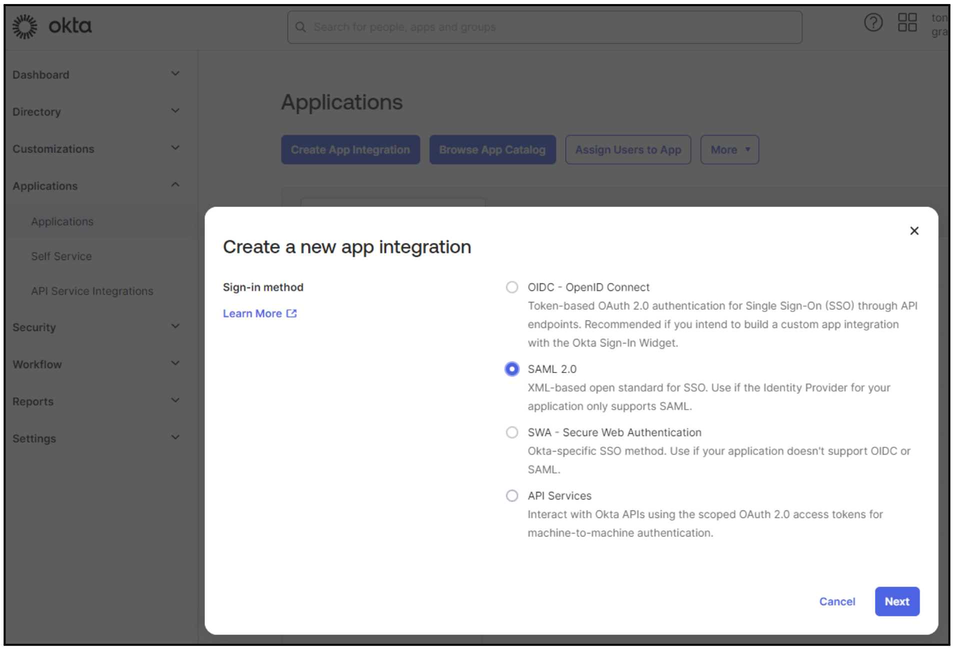
- To download the latest version, visit our Updates page, or update via the in-app updates feature
- Deactivate your current license by following **Help -> Manage License. . .**
- Let the Prime team know if your deactivation limit needs to be extended
- After deactivation, Prime should display the activation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

Okta Configuration

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

Creating an Application in Okta

1. From the Admin menu, select **Applications -> Applications** from the side menu. From here, select **Create App Integration** and select **SAML 2.0**. Click **Next**:



Create a new app integration

Sign-in method

Learn More

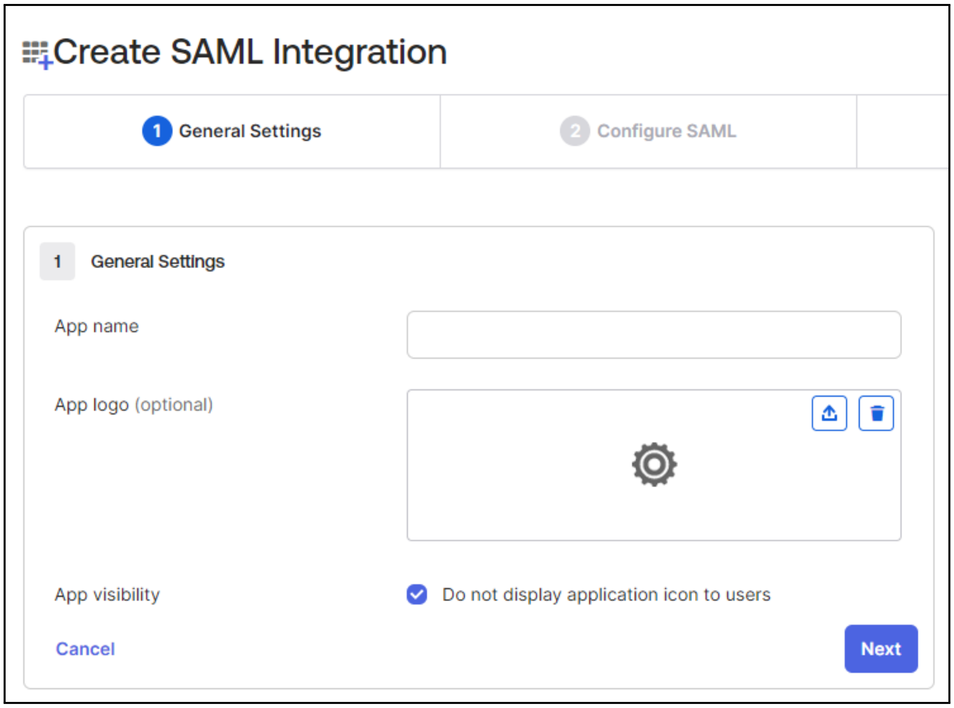
○ OIDC - OpenID Connect
Token-based OAuth 2.0 authentication for Single Sign-On (SSO) through API endpoints. Recommended if you intend to build a custom app integration with the Okta Sign-In Widget.

● SAML 2.0
XML-based open standard for SSO. Use if the Identity Provider for your application only supports SAML.

○ SWA - Secure Web Authentication
Okta-specific SSO method. Use if your application doesn't support OIDC or SAML.

○ API Services
Interact with Okta APIs using the scoped OAuth 2.0 access tokens for machine-to-machine authentication.

2. Add the application name e.g. Geneious Prime and any other display customisation you would like
3. Tick **Do not display application icon to users** for **App visibility**
4. Click **Next**:


Create SAML Integration

1 General Settings

App name

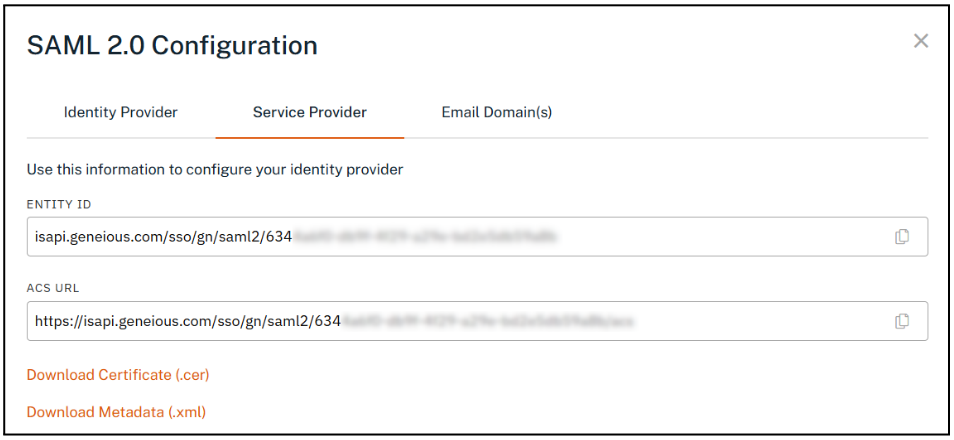
App logo (optional)

App visibility ☑ Do not display application icon to users

Single sign-on (SSO) Configuration

You'll next be presented with further configuration options in the **Configure SAML** step of Okta. Before continuing here, you will need to configure Geneious Prime's My Account, and use information from here to configure Okta.

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 **ACS URL**. Paste this into Okta as the **Single sign-on URL**
4. Also copy the **Entity ID** from My Account and paste this into Okta as the **Audience URI**
5. Set the **Name ID format** to **EmailAddress**
6. Set the **Application username** to **Email**
7. Expand the **Advanced Settings** and confirm the following details are correct:



SAML 2.0 Configuration

Use this information to configure your identity provider

ENTITY ID

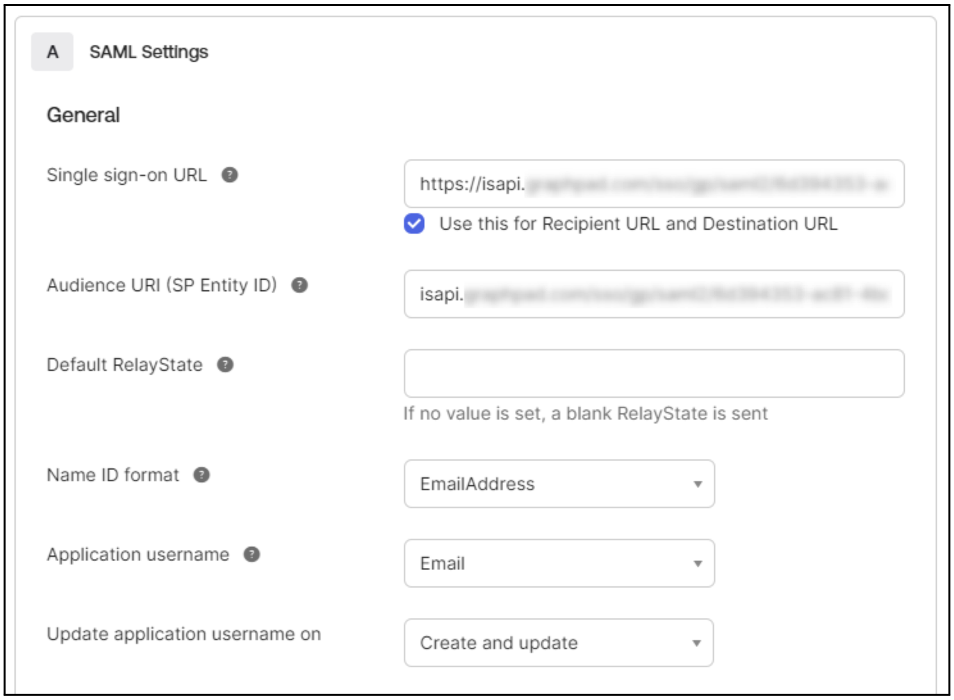
isapi.geneious.com/sso/gn/saml2/634[redacted]

ACS URL

https://isapi.geneious.com/sso/gn/saml2/634[redacted]

Download Certificate (.cer)

Download Metadata (.xml)



General

Single sign-on URL: https://isapi.[redacted]

☑ Use this for Recipient URL and Destination URL

Audience URI (SP Entity ID): isapi.[redacted]

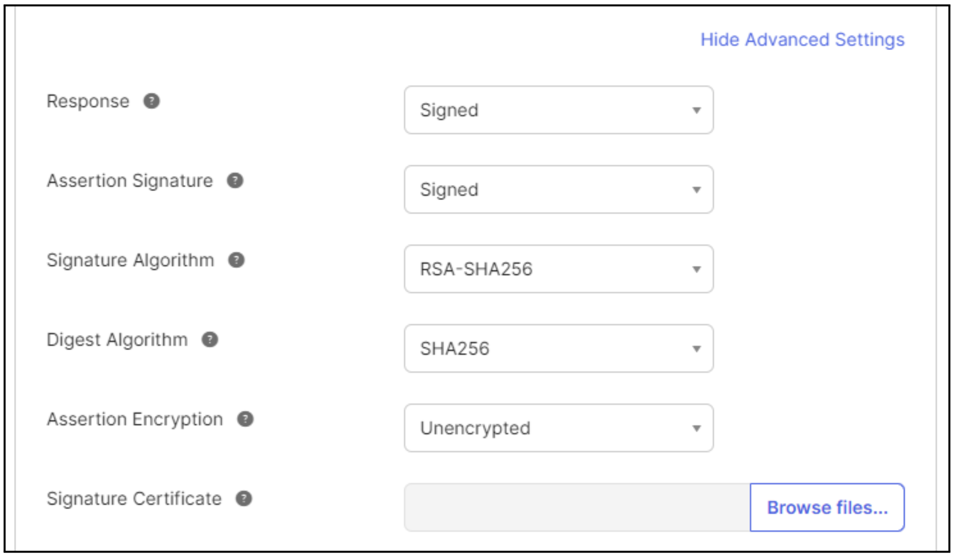
Default RelayState:

If no value is set, a blank RelayState is sent

Name ID format: EmailAddress

Application username: Email

Update application username on: Create and update



Response: Signed

Assertion Signature: Signed

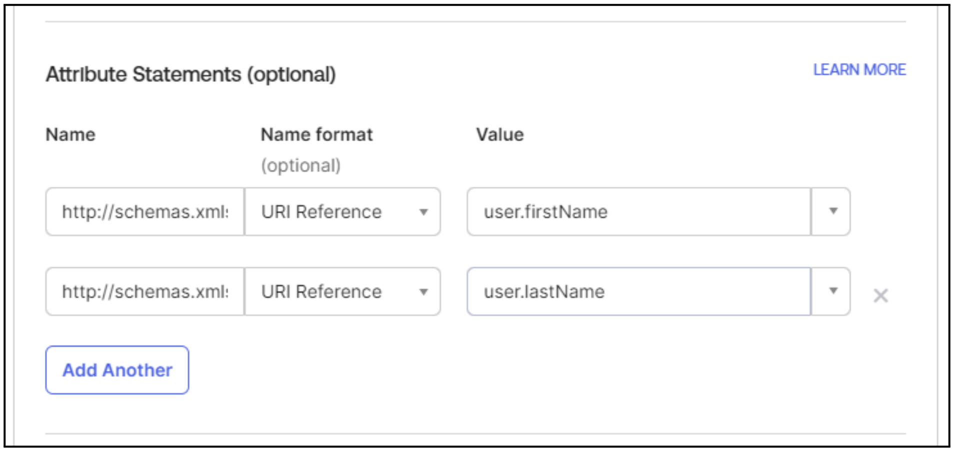
Signature Algorithm: RSA-SHA256

Digest Algorithm: SHA256

Assertion Encryption: Unencrypted

Signature Certificate:

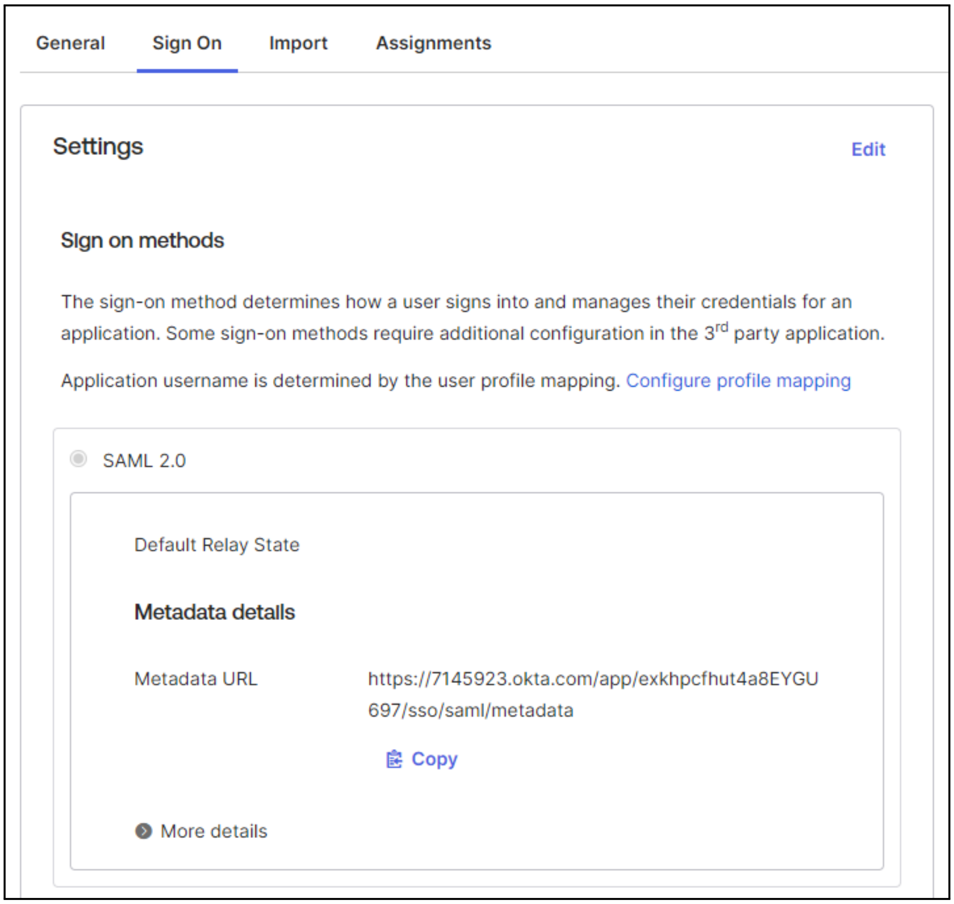
8. Add the following two **Attribute Statements**, using **URI Reference** as the **Name format**:
   - `http://schemas.xmlsoap.org/ws/2005/05/identity/claims/givenname` - user.firstName
   - `http://schemas.xmlsoap.org/ws/2005/05/identity/claims/surname` - user.lastName



Attribute Statements (optional)

Name	Name format (optional)	Value
http://schemas.xml:	URI Reference	user.firstName
http://schemas.xml:	URI Reference	user.lastName

9. Click **Next** and **Finish**
10. You will be presented with your Okta **Metadata URL** for this integration. Copy this.



Settings

Sign on methods

The sign-on method determines how a user signs into and manages their credentials for an application. Some sign-on methods require additional configuration in the 3rd party application.

Application username is determined by the user profile mapping. Configure profile mapping

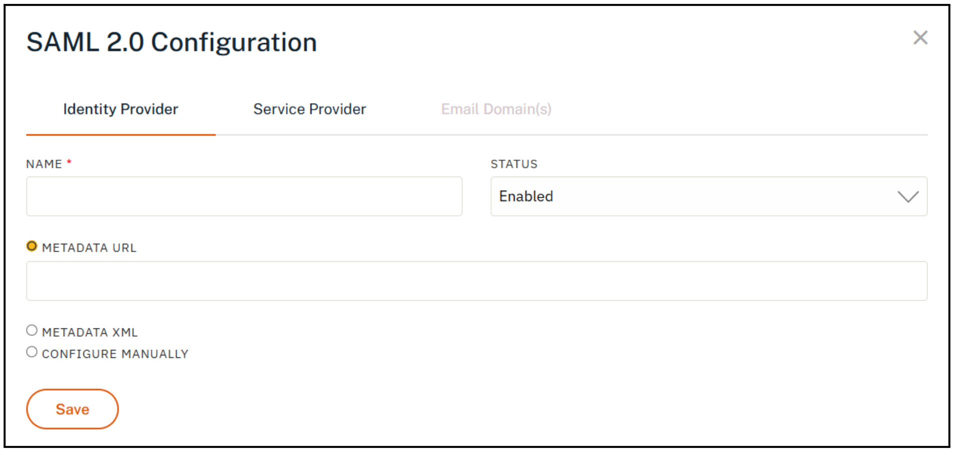
○ SAML 2.0

Default Relay State

Metadata details

Metadata URL https://7145923.okta.com/app/exkhpcfhut4a8EYGU697/sso/saml/metadata

11. Return to My Account and switch to the **Identity Provider** tab. Enter a name e.g. "Okta", and paste in the Metadata URL from Okta. Click **Save**:



SAML 2.0 Configuration

NAME *

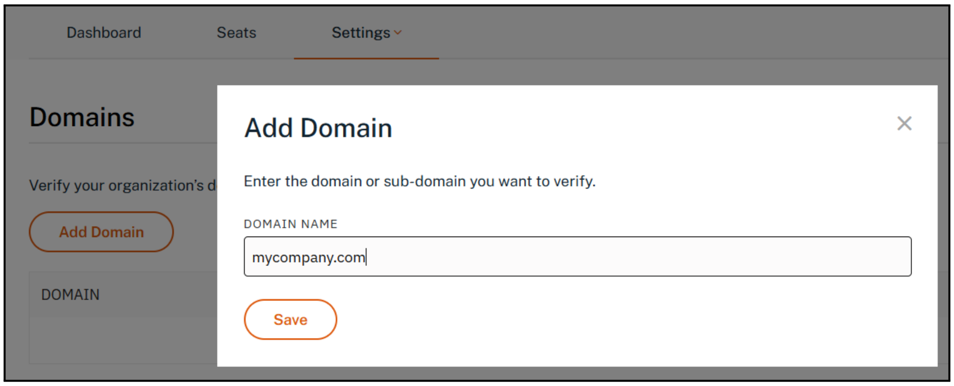
STATUS Enabled

● METADATA URL

○ METADATA XML

○ CONFIGURE MANUALLY

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



Domains

Verify your organization's d

DOMAIN

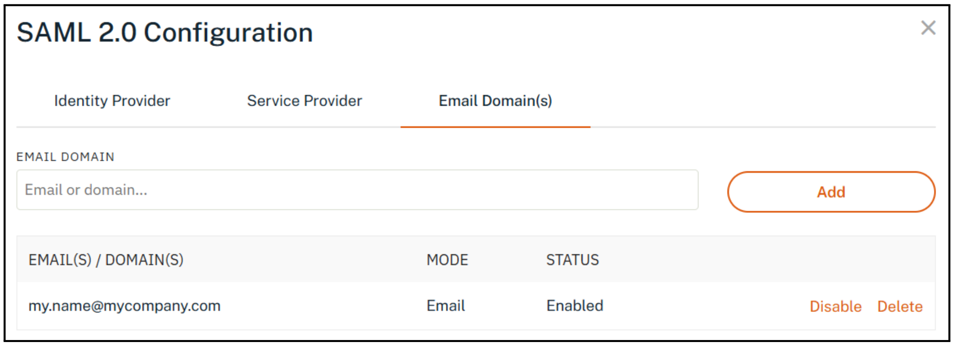
Add Domain

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

DOMAIN NAME

mycompany.com

13. 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.
14. 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:**



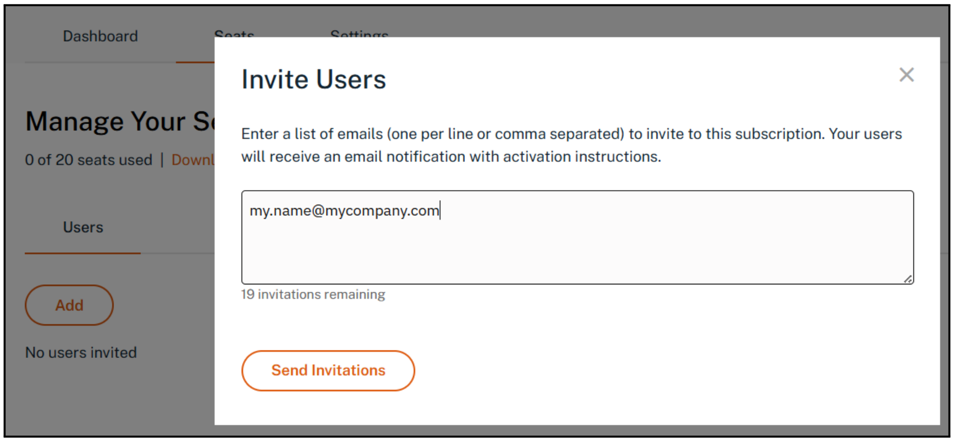
SAML 2.0 Configuration

EMAIL DOMAIN

Email or domain...

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

15. If you are using Okta 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 Okta in the SCIM configuration section later in this guide.



Manage Your S

0 of 20 seats used | Downl

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.

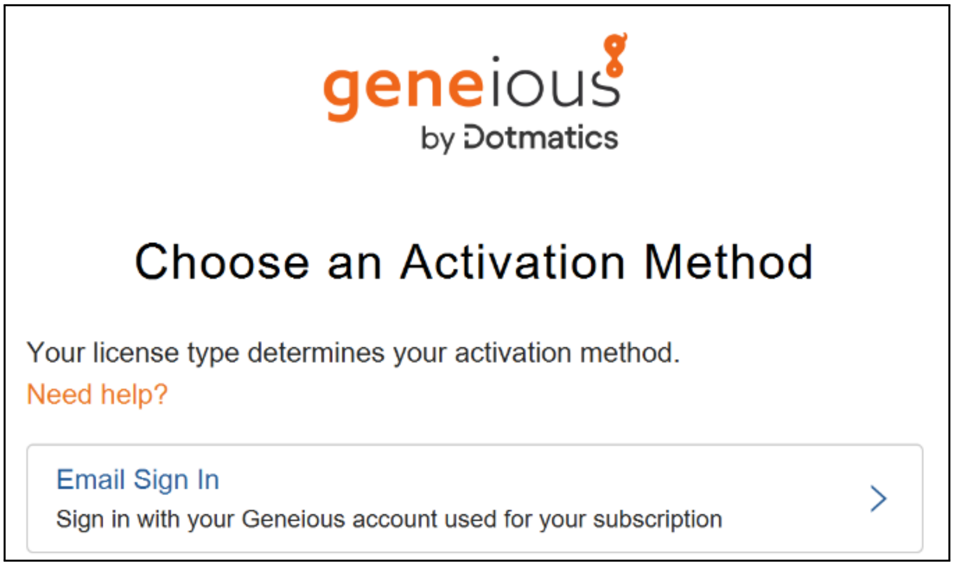
my.name@mycompany.com

19 invitations remaining

16. If this user does not yet exist in Okta, create them in Okta now.
From Okta, assign this user to your application from the Assignments tab.
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). Leave the

Username unchanged as their email address. Click **Save**:

17. 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

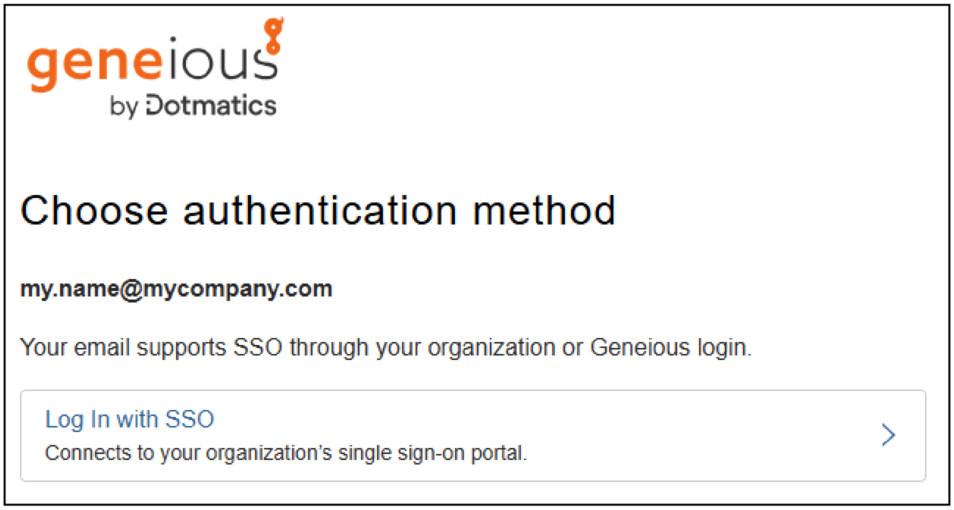
Choose an Activation Method

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

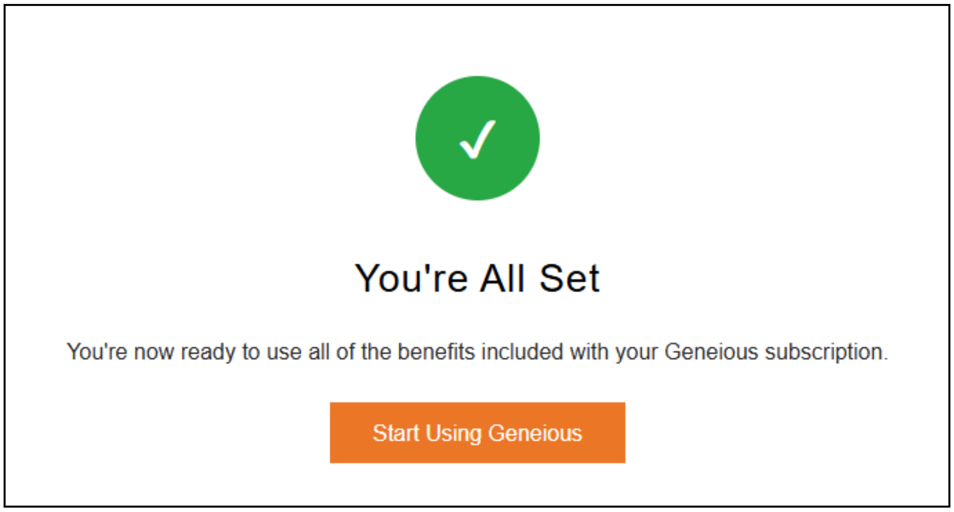
Choose authentication method

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.

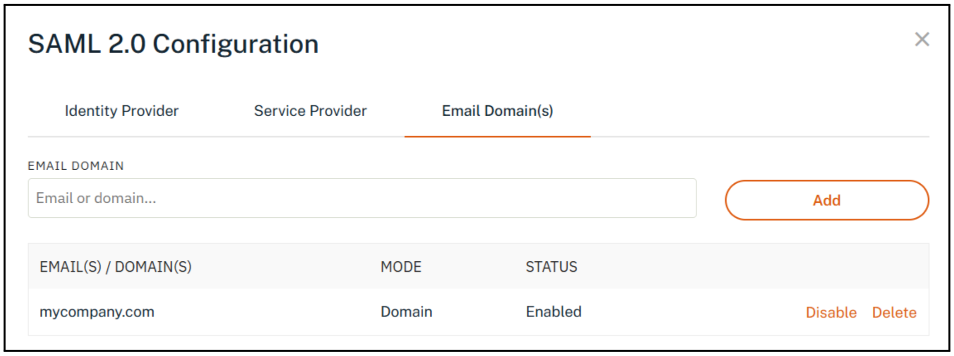


You're All Set

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

Start Using Geneious

18. 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 Okta as you have above:



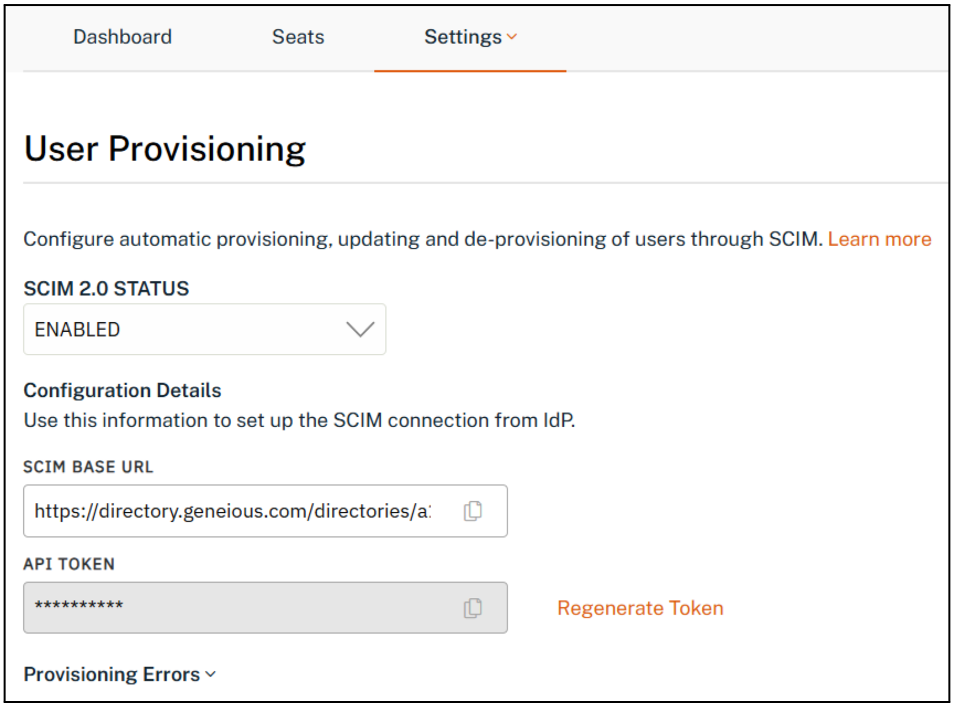
EMAIL DOMAIN

Email or domain...

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

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:



User Provisioning

Configure automatic provisioning, updating and de-provisioning of users through SCIM. Learn more

SCIM 2.0 STATUS

ENABLED

Configuration Details

Use this information to set up the SCIM connection from IdP.

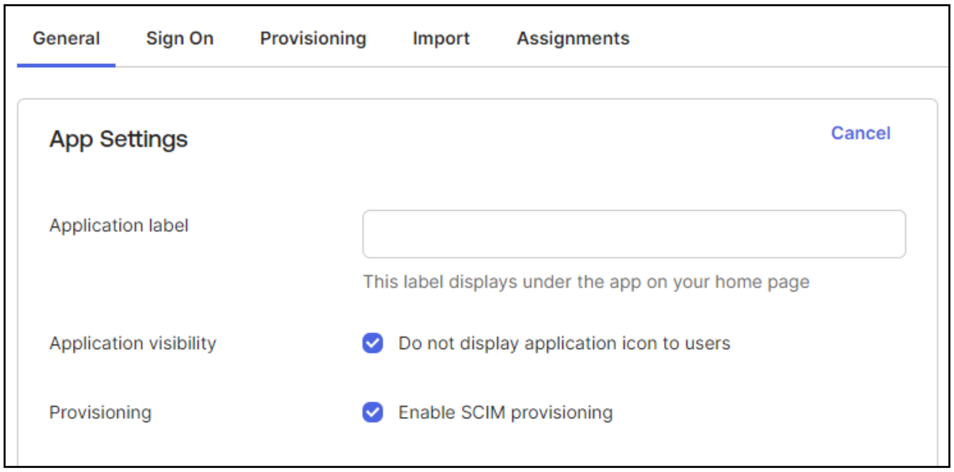
SCIM BASE URL

https://directory.geneious.com/directories/a:

API TOKEN

****

2. Then in the **General** tab of your Okta application, **Edit** the **App Settings**, select **SCIM**, and click **Save**:



App Settings

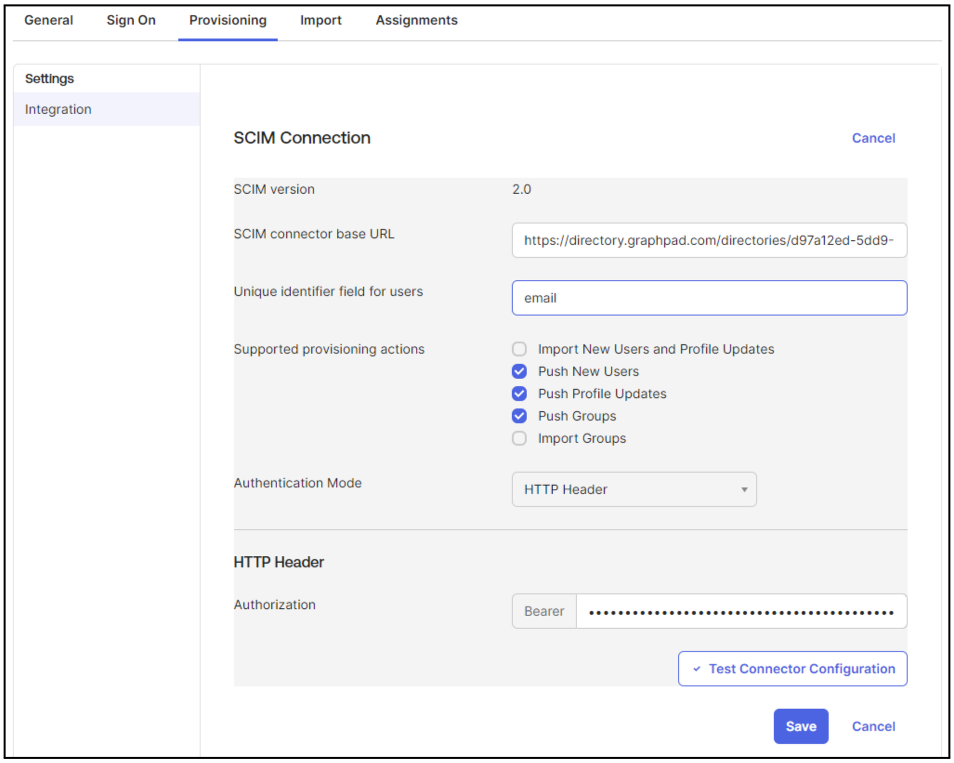
Application label

This label displays under the app on your home page

Application visibility ☑ Do not display application icon to users

Provisioning ☑ Enable SCIM provisioning

3. Navigate to the **Provisioning** tab and **Edit** the **SCIM Connection**
4. Copy the **SCIM Base URL** from My Account as the **SCIM connector base URL**
5. Enter “email” as the **Unique identifier field for users**
6. Select all the “**Push**” (from Okta to Prism) **Supported provisioning actions**
7. Select **HTTP Header** as the **Authentication Mode**
8. Copy the **API Token** from My Account as the **Authorization Bearer Token**
9. **Test** and **Save** the configuration:



General Sign On Provisioning Import Assignments

Settings
Integration

SCIM Connection — Cancel

SCIM version: 2.0

SCIM connector base URL: https://directory.graphpad.com/directories/d97a12ed-5dd9-

Unique identifier field for users: email

Supported provisioning actions:
- ☐ Import New Users and Profile Updates
- ☑ Push New Users
- ☑ Push Profile Updates
- ☑ Push Groups
- ☐ Import Groups

Authentication Mode: HTTP Header

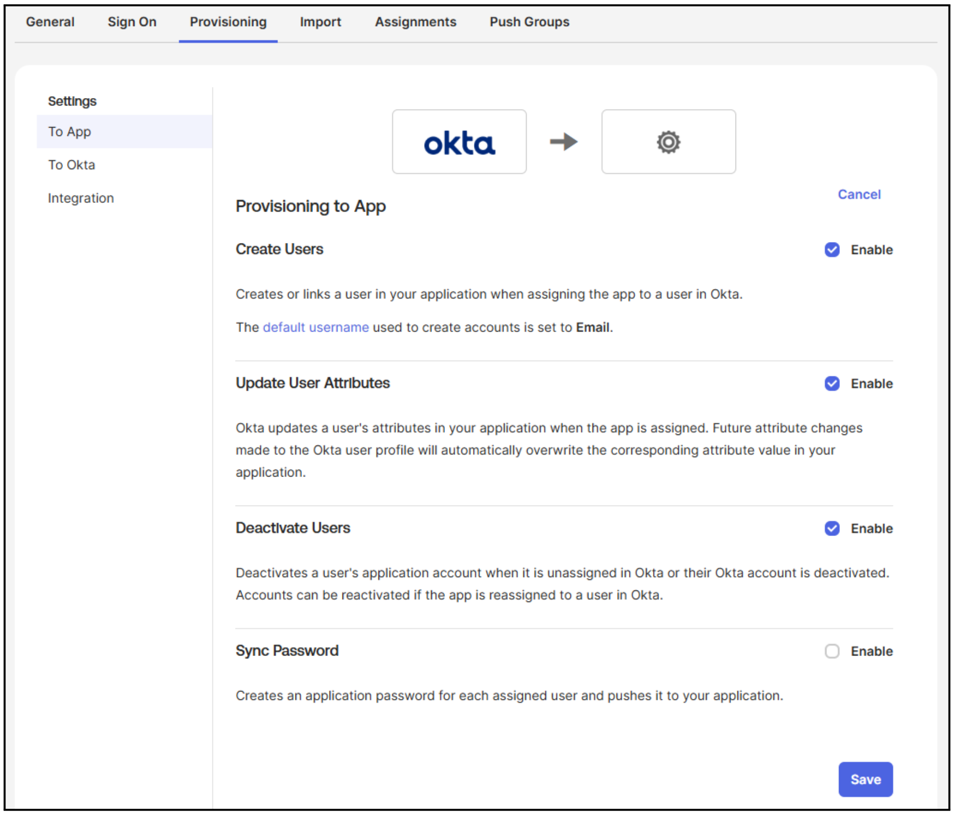
HTTP Header

Authorization: Bearer ••

✓ Test Connector Configuration

Save Cancel

10. In the **To App** menu, click **Edit**, and enable **Create Users**, **Update User Attributes**, and **Deactivate Users**. Click **Save**:



General Sign On Provisioning Import Assignments Push Groups

Settings
To App
To Okta
Integration

Provisioning to App — Cancel

Create Users — ☑ Enable

Creates or links a user in your application when assigning the app to a user in Okta.

The default username used to create accounts is set to **Email**.

Update User Attributes — ☑ Enable

Okta updates a user's attributes in your application when the app is assigned. Future attribute changes made to the Okta user profile will automatically overwrite the corresponding attribute value in your application.

Deactivate Users — ☑ Enable

Deactivates a user's application account when it is unassigned in Okta or their Okta account is deactivated. Accounts can be reactivated if the app is reassigned to a user in Okta.

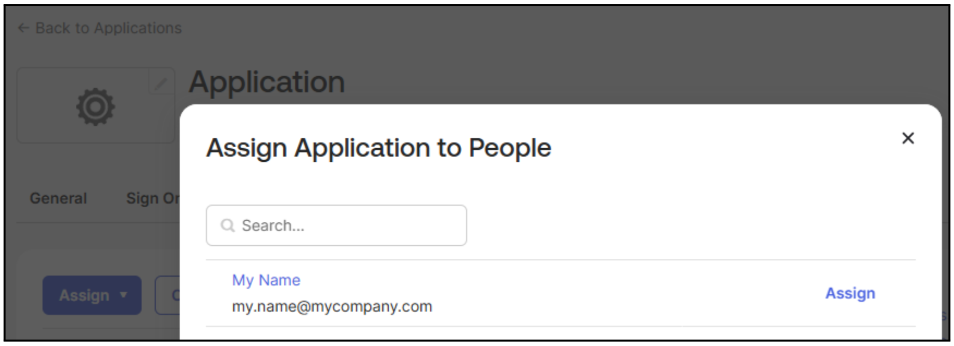
Sync Password — ☐ Enable

Creates an application password for each assigned user and pushes it to your application.

Save

11. You have now successfully configured your user provisioning connection between Okta and Geneious Prime. You can now provision users from Okta into Prime by using the **Assignments**

tab in Okta to assign users or groups to Prime:

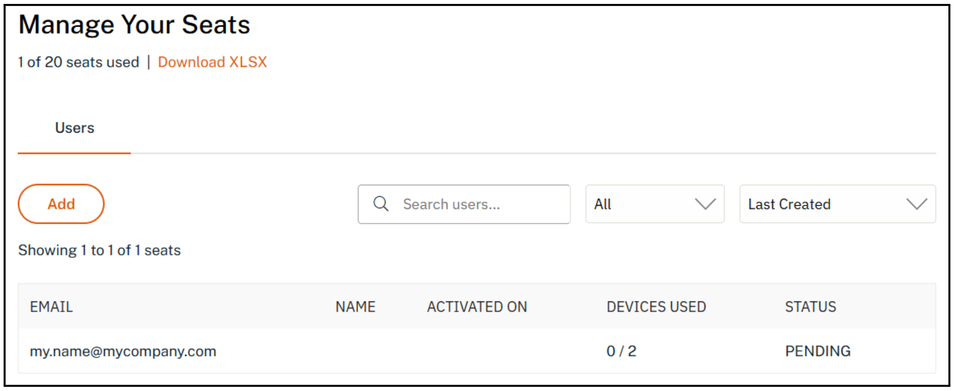


Application

Assign Application to People

My Name
my.name@mycompany.com

12. 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:



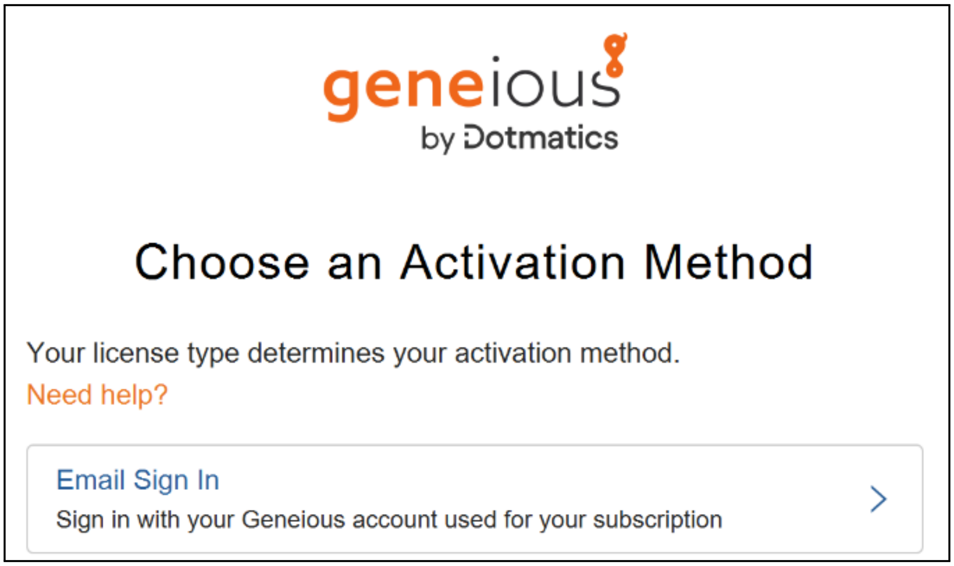
Manage Your Seats

1 of 20 seats used

Showing 1 to 1 of 1 seats

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

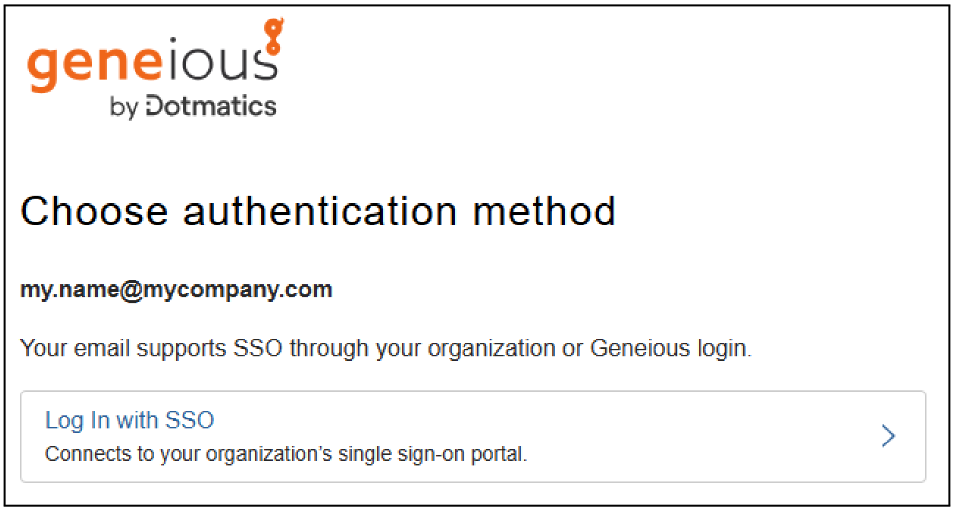
13. In the Prime application, activate your software, selecting the **Email Sign In** option. Continue through the screens, selecting **Log In with SSO** as your authentication method:



Choose an Activation Method

Your license type determines your activation method.

Sign in with your Geneious account used for your subscription



geneious by Dotmatics

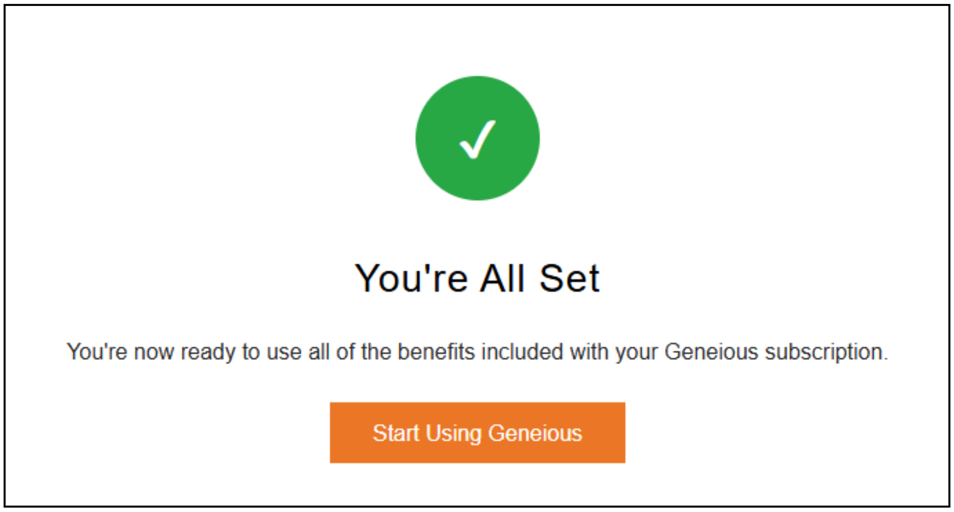
Choose authentication method

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.



You're All Set

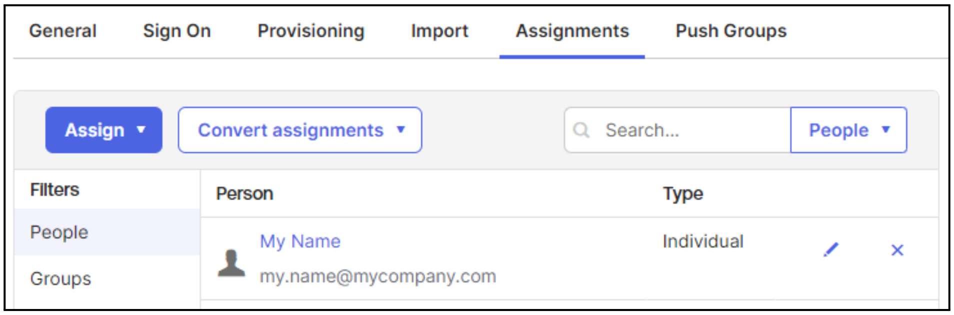
You're now ready to use all of the benefits included with your Geneious subscription.

Start Using Geneious

Revoke User

To revoke a user via Okta:

1. In the **Assignments** tab within your Okta application, click the **x** to remove that user:



Person	Type
My Name my.name@mycompany.com	Individual

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.