Shibboleth 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.

Shibboleth Configuration

Please use the following as a reference to support the configuring of your Shibboleth platform.

Shibboleth does not include a graphical user interface (UI) for management; instead, its configuration is handled through XML files. These files govern various aspects of its operation, including metadata exchange, relying party trust relationships, credential management, attribute filtering, and security settings. The following sections provide general direction on how to configure these files. Here we refer to Geneious Prime as the Service Provider (SP).

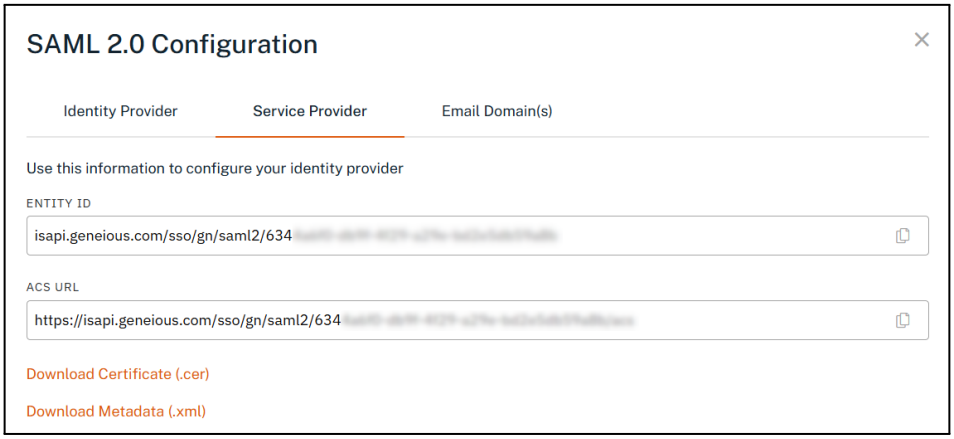
For those experienced with Shibboleth configuration, please still refer to sections 1, 5, 6 and 7 for specific requirements of integrating with Geneious Prime.

	Step	Configuration Resource
1	**Obtain Service Provider Data** Collect the SP's XML metadata file, SP Entity ID, SP ACS URL and metadata URL	*N/A*
2	**Upload Service Provider Metadata** Place the metadata file on the Shibboleth host	*./metadata - SP metadata*
3	**Add a New Metadata Provider** Register the source of the metadata of the SP	*conf/metadata-providers.xml*
4	**Add a New Relying Party** Define the SP settings	*conf/relying-party.xml*
5	**Configure Attribute Mapping** Map and release necessary attributes	*conf/attribute-resolver.xml* *conf/attribute-filter.xml*
6	**Configure NameID Format** Specify the format for user identifiers	*conf/nameid.xml*
7	**Turn Off Signing Key Rotation** Specify single key to sign the SAML Responses for the Service provider	*conf/credentials.xml* *conf/relying-party.xml*

1. Obtain Service Provider Metadata

To configure the service provider in Shibboleth, the following information is required: - Entity ID - ACS URL - Metadata URL - Metadata XML file - SP signing key certificate

This information is available at: My Account → Manage Seats → Authentication → ID Provider → Service Provider:



2. Upload Service Provider Data to Shibboleth

Upload the following file:

- XML metadata file to the `/opt/shibboleth-idp/metadata` folder

Ensure that the Shibboleth service process has access to the file: `sudo chown <user>:<group> <path-to-metadata>`

Where `<user>:<group>` depends on the Shibboleth deployment type and could be the following:

- *shibd:shibd*
- *shibboleth:shibboleth*
- *tomcat:tomcat*
- *tomcat8:tomcat8*
- *apache:apache*
- *httpd:httpd*

```
sudo chmod 644 <path-to-metadata>
```

3. Add a new Metadata Provider

Add the following XML-snippet to the `/opt/shibboleth-idp/conf/metadata-providers.xml` file:

```
<MetadataProvider xsi:type="FileBackedHTTPMetadataProvider"
    id="<any-short-sp-id>"
    metadataURL="<sp-metadata-url>"
    backingFile="<path-to-metadata>"
    maxRefreshDelay="PT2H"/>
```

Where:

- `<any-short-sp-id>` - a short ID for the service provider, respecting Shibboleth's XML Schema
- `<sp-metadata-url>` - the metadata URL obtained from My Account
- `<path-to-metadata>` - the path to the metadata file uploaded to Shibboleth

4. Add a new Relying Party

Add the following XML-snippet to the `/opt/shibboleth-idp/conf/relying-party.xml` file in the `<util:list id="shibboleth.RelyingPartyOverrides">` section:

```
<bean parent="RelyingPartyByName" c:relyingPartyIds="<sp-entity-id>">
    <property name="profileConfigurations">
        <list>
            <bean parent="SAML2.SSO" p:signAssertions="true"
                p:signRequests="true" p:encryptAssertions="false"
                p:encryptNameIDs="false" />
            <bean parent="SAML2.Logout" p:signResponses="true" />
        </list>
    </property>
</bean>
```

Where:

- `<sp-entity-id>` - the Service Provider Entity ID obtained from My Account

5. Configure Attribute Mapping

1. Ensure that **Email**, **Given Name** and **Surname** are exported from your Data Provider.

   If using LDAP here, check that `givenName sn email` is included in:
   `DataConnector[@xsi:type="LDAPDirectory"]/@exportAttributes`.
   Depending on your configuration, this may require updating:
   `idp.attribute.resolver.LDAP.exportAttributes`

2. Ensure that attributes are registered. Add the following XML-snippet to the `/opt/shibboleth-idp/conf/attribute-resolver.xml` file, or ensure the equivalent attributes are defined:

```
<AttributeDefinition id="<givenNameAttrName>" xsi:type="Simple">
    <InputDataConnector ref="<data-provider>" attributeNames="givenName"/>
    <AttributeEncoder xsi:type="SAML2String"
    name="http://schemas.xmlsoap.org/ws/2005/05/identity/claims/givenname"
    friendlyName="givenName"/>
</AttributeDefinition>

<AttributeDefinition id="<surnameAttrName>" xsi:type="Simple">
    <InputDataConnector ref="<data-provider>" attributeNames="sn"/>
    <AttributeEncoder xsi:type="SAML2String"
    name="http://schemas.xmlsoap.org/ws/2005/05/identity/claims/surname"
    friendlyName="surname"/>
</AttributeDefinition>
```

Where:

- `<data-provider>` - the ID of the data provider that exports the corresponding data
- `<givenNameAttrName>` and `<surnameAttrName>` - valid attribute definition IDs referring to the attributes in the `./attribute-filter.xml` file

3. Release the Attributes to the Relying Party. Add to the `/opt/shibboleth-idp/conf/attribute-filter.xml` file the following XML-snippet:

```
<AttributeFilterPolicy id="SPFilterPolicy">
   <PolicyRequirementRule xsi:type="Requester" value="<sp-entity-id>"/>
   <AttributeRule attributeID="mail" permitAny="true" />
   <AttributeRule attributeID="<givenNameAttrName>" permitAny="true" />
   <AttributeRule attributeID="<surnameAttrName>" permitAny="true"/>
</AttributeFilterPolicy>
```

Where:

- `<sp-entity-id>` - the Service Provider Entity ID obtained from My Account
- `<givenNameAttrName>` - a valid attribute definition ID specified for the Given Name specified in the `./attribute-resolver.xml` file
- `<surnameAttrName>` - a valid attribute definition ID specified for the Surname specified in the `./attribute-resolver.xml` file

6. Configure NameID Format

Email address is required as the NameID format.
Uncomment or add to the `/opt/shibboleth-idp/conf/saml-nameid.xml` the following XML-snippet in the `<util:list id="shibboleth.SAML2NameIDGenerators">` section:

```
<bean parent="shibboleth.SAML2AttributeSourcedGenerator"
    p:omitQualifiers="true"
    p:format="urn:oasis:names:tc:SAML:1.1:nameid-format:emailAddress"
    p:attributeSourceIds="#{ {'mail'} }" />
```

7. Turn Off Signing Key Rotation

Geneious Prime does not currently support multiple keys to be used for signing SAML Responses, so the service provider in Shibboleth must be configured with security configuration referring to a single key.

If your Shibboleth identity provider uses a single singing key, you can omit this section, otherwise follow the instructions below.

1. Define new credentials. Add to the file `/opt/shibboleth-idp/conf/credentials.xml` the following XML-fragment:

```
<bean id="<single-key-cred-id>"
    parent="shibboleth.BasicX509CredentialFactoryBean"
    p:privateKeyResource="%{idp.signing.key}"
    p:certificateResource="%{idp.signing.cert}"
    p:entityId-ref="entityID" />
```

Where:

- `<single-key-cred-id>` - a valid credential ID referring to the `relying-party.xml` file

2. Specify the dedicated credential for the Relying Party. Add the following snippet to the `/opt/shibboleth-idp/relying-party.xml` file (to the root node):

```
<bean id="<security-conf-id>"
    parent="shibboleth.DefaultSecurityConfiguration">
    <property name="signatureSigningConfiguration">
        <bean
            parent="shibboleth.SigningConfiguration.SHA256"
            p:signingCredentials-ref="<single-key-cred-id>"
        />
    </property>
</bean>
```

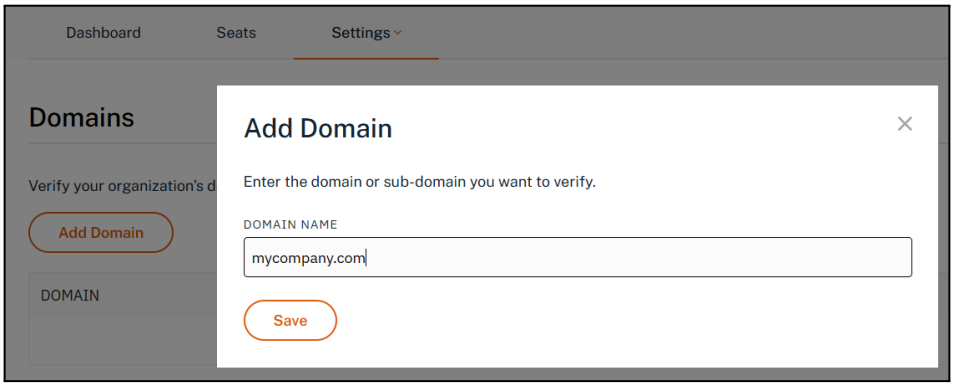
Where:

- `<security-conf-id>` - a valid ID for the security configuration
- `<single-key-cred-id>` - the ID of the single key credential registered in the `credentials.xml` file

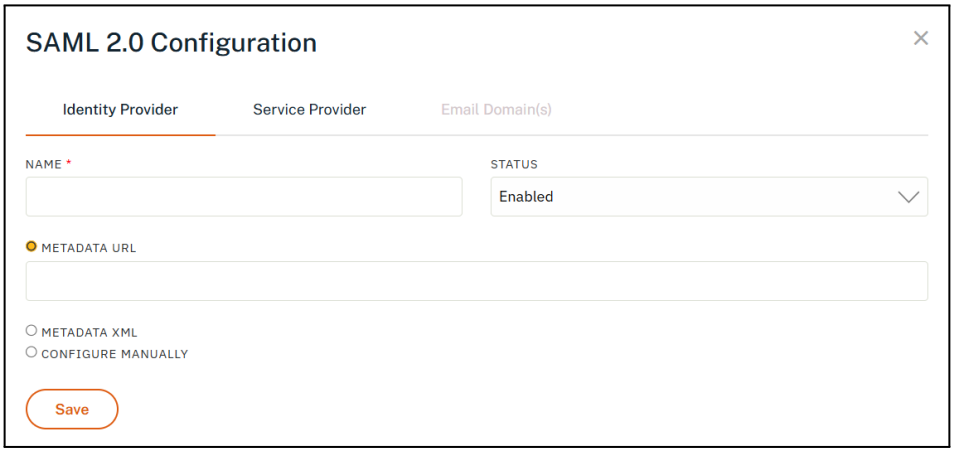
Prime My Account Configuration

In addition to configuring Shibboleth, you will also need to enable the connection from My Account.

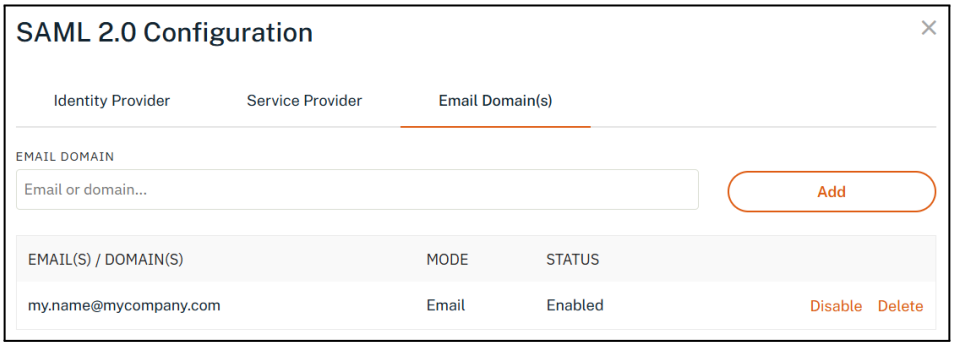
1. First navigate to My Account → Manage Seats → **Domains**. You must register and verify ownership of the email domain(s) that you wish to use with SSO. Add the email domain(s) that your users belong to and follow the onscreen instructions from **View** to verify ownership either by HTML file or DNS TXT record:



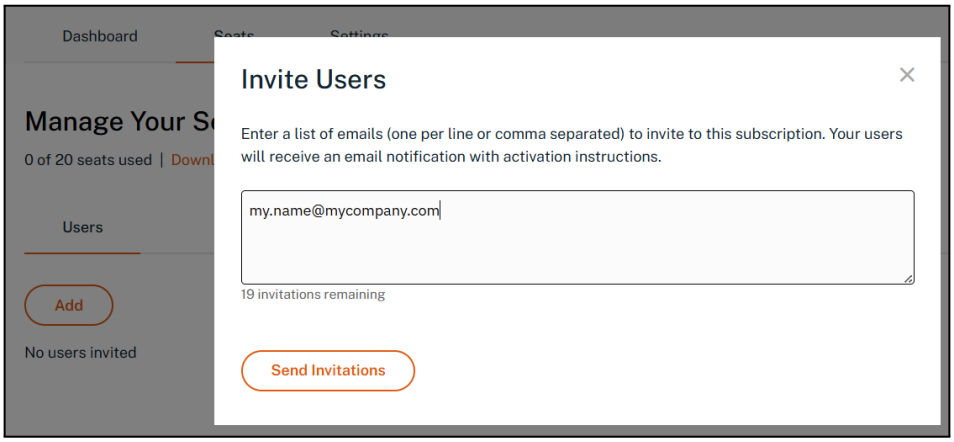
2. Once verified, create an Identity Provider entry from the **Authentication** tab
3. Enter a name e.g. “Shibboleth”:



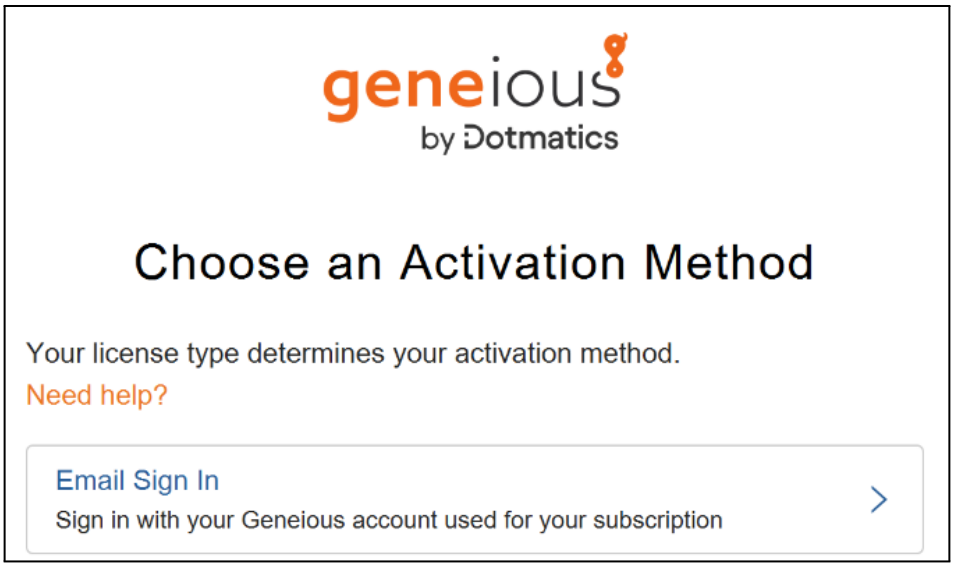
4. Use the **Email Domain(s)** SAML tab to provide email addresses and/or email domains SSO access to Prime. **First, test SSO access with a single email address by adding that email address in full**:

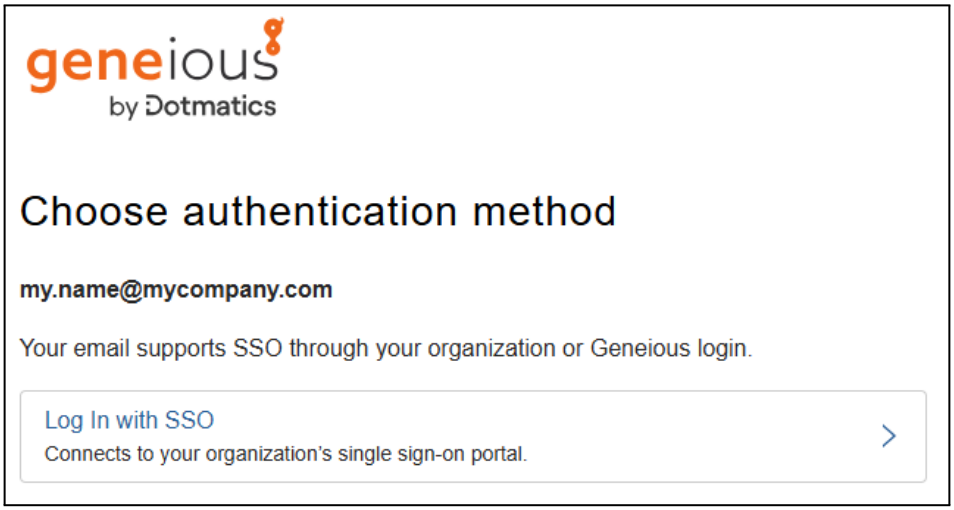


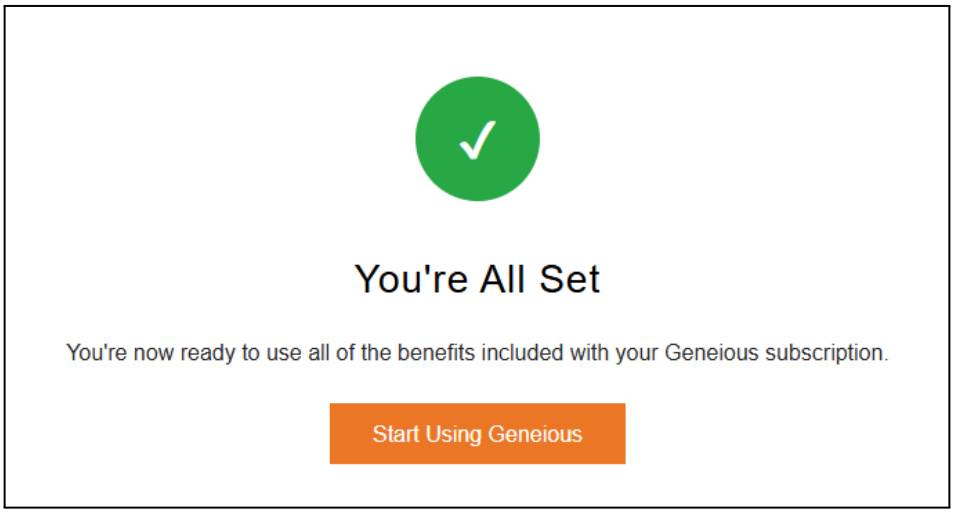
5. If you are using only SSO, and not SCIM, you will need to invite these user(s) under the **Users** tab in My Account. Otherwise, SCIM users can be provisioned from your identity provider by establishing a connection using the **User Provisioning** tab in My Account.



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:







7. 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 Shibboleth as you have above: