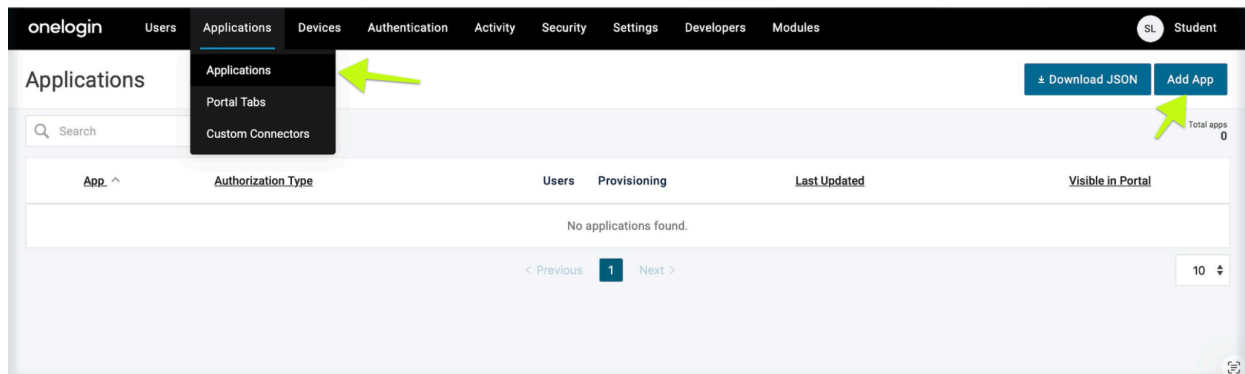
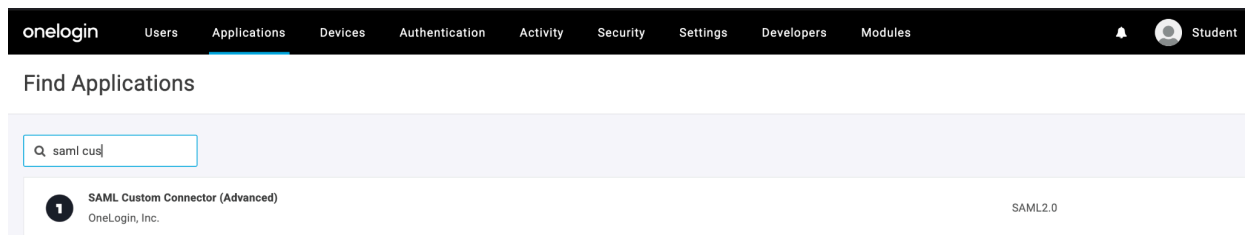


OneLogin SSO Setup: Admin Steps

1. Log in to OneLogin as an Administrator.
2. Navigate to **Applications** and select **Add App**.



This will direct you to the "Find Applications" page. Search for "SAML Custom Connector (Advanced)" and select it.



Save the configuration after updating the display name to "Gainsight SSO" or your preferred name.

onelogin Users Applications Devices Authentication Activity Security Settings Developers Modules Student

App Listing / Add SAML Custom Connector (Advanced) Cancel Save

Configuration

Portal

Display Name

GainsightSSO

Visible in portal

Visible in portal

Rectangular Icon

Square Icon

1

1

Upload an icon with an aspect-ratio of 2.64:1 as either a transparent .PNG or .SVG

Upload a square icon at least 512x512px as either a transparent .PNG or .SVG

Once you have provided the app name and saved the preceding step, you will be directed to the App setup page.

Next, Proceed to the SSO Section

You will need to:

- Copy the SAML 2.0 Endpoint (HTTP).
- Download the x.509 certificate.

onelogin Users Applications Devices Authentication Activity Security Settings Developers Modules Student

Applications / SAML Custom Connector (Advanced) More Actions Save

Info Configuration Parameters Rules SSO Access Users Privileges Setup

Enable SAML2.0

Sign on method

SAML2.0

X.509 Certificate

Standard Strength Certificate (2048-bit)

Change View Details

click and Download Certificate

SAML Signature Algorithm

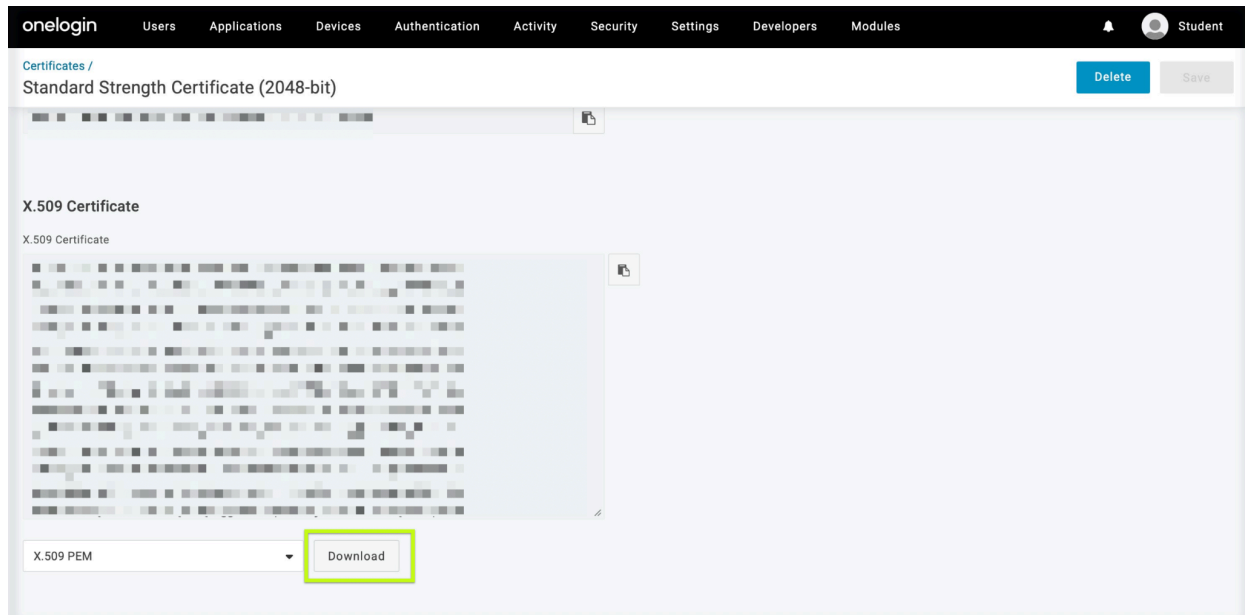
SHA-1

Issuer URL

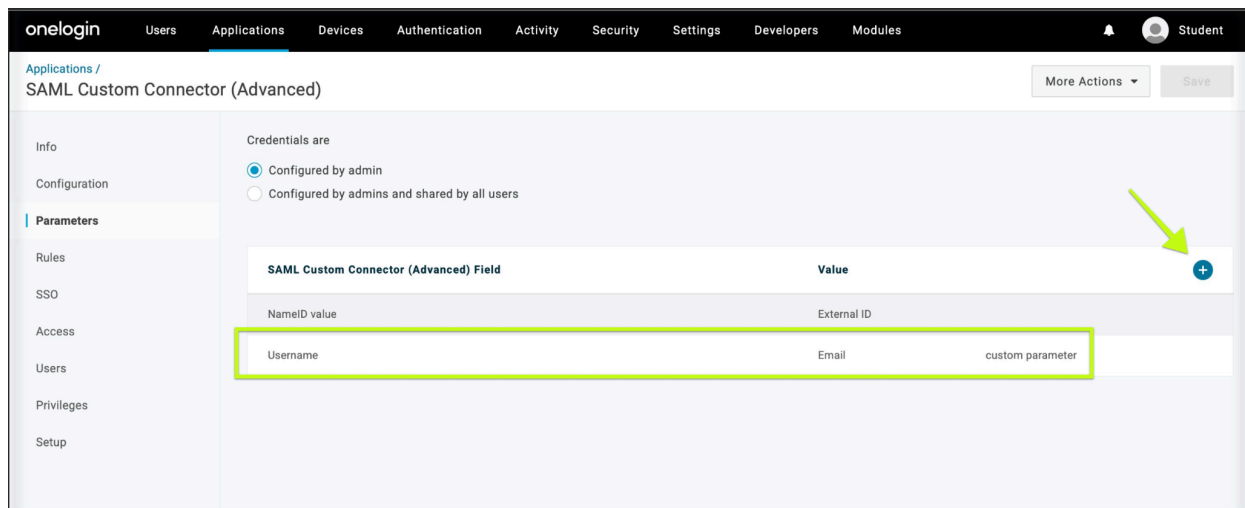
SAML 2.0 Endpoint (HTTP)

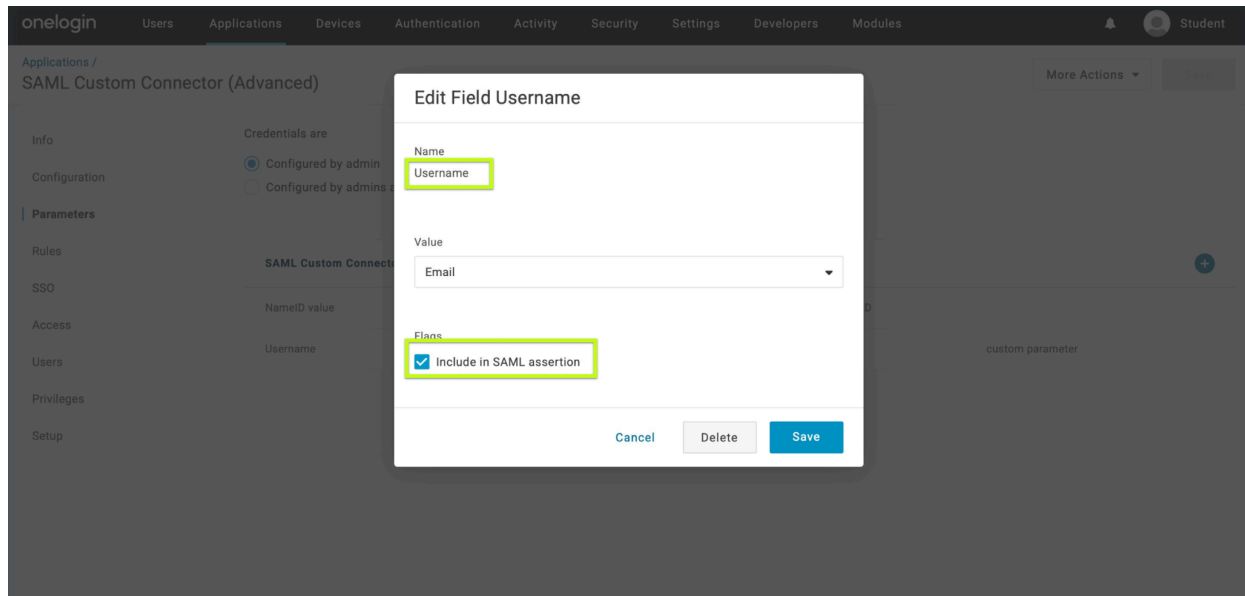
SLO Endpoint (HTTP)

x.509 cert download



Next, navigate to the Parameters section. Create a Custom parameter named **Username** and map it to **Email**, making sure to select *Include in SAML assertion*.





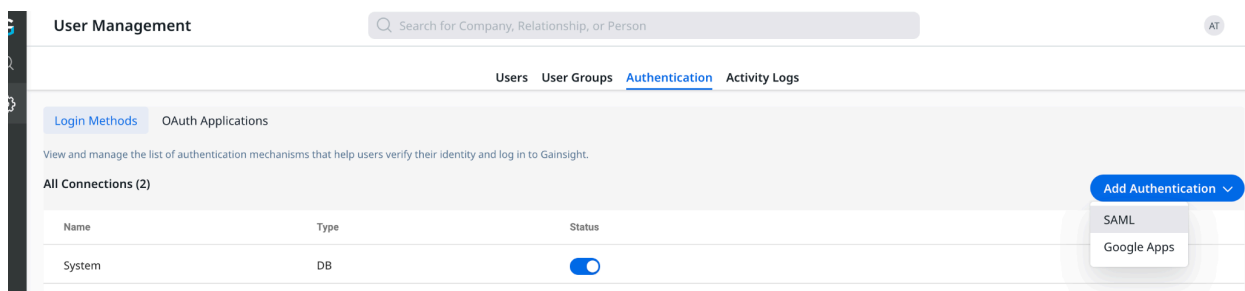
Now, Login to Gainsight:

1. Navigate to Gainsight Administration

Go to **Administration > User Management > Authentication**.

2. Add SAML Authentication

Click **Add Authentication** and select **SAML**.



Now enter the below details:

Name : Give Name of the APP, Ex: OneloginSSO

Email Domain : Your organisation domain

Sign In URL : Copy paste SAML 2.0 Endpoint(HTTP) URL copied from Onlogin SSO section

Certificate : Upload the certificate downloaded from onelogin

Now save the connection

SAML Mechanism



Name *

OnrloginSSO

Enter a unique connection name for authentication

Email Domain *

domain.com

Enter the domain name for SAML authentication

Sign In URL *

https://demo-identity-gateway.com/#!/usermanagement#

Enter SAML login URL for authentication

Sign Out URL

Enter Sign Out URL

Enter SAML logout URL to exit from authentication

Certificate *



onelogin.pem

Field Mapping

Source Field

Username

Target Field

Username

Enter the name of the claim containing User attributes from the source to be mapped to the Username.

Cancel

Save

Now, when you edit the connection, you will see a "Download" option, allowing you to download an XML file.

SAML Mechanism



Name *

onleLoginSSO

Enter a unique connection name for authentication

Email Domain *

[Redacted]

Enter the domain name for SAML authentication

Sign In URL *

[Redacted]2c4:

Enter SAML login URL for authentication

Sign Out URL

Enter Sign Out URL

Enter SAML logout URL to exit from authentication

Certificate *



Drag and drop file
here or [Browse](#)

Field Mapping

Source Field

Username

Target Field

Username

Enter the name of the claim containing User attributes from the source to be mapped to the Username.



Download

Cancel

Save

Extract the AssertionConsumerService->Location and Entity ID from downloaded XML file

- Open the XML file and locate the following:
 - a. **AssertionConsumerService->Location.** Towards the bottom of the file. It would be the blurred out section from below image. This would need to be copied.

```
23 <NameIDFormat>urn:oasis:names:tc:SAML:1.1:nameid-format:unspecified</NameIDFormat>
24 <NameIDFormat>urn:oasis:names:tc:SAML:1.1:nameid-format:emailAddress</NameIDFormat>
25 <NameIDFormat>urn:oasis:names:tc:SAML:2.0:nameid-format:persistent</NameIDFormat>
26 <NameIDFormat>urn:oasis:names:tc:SAML:2.0:nameid-format:transient</NameIDFormat>
27 <AssertionConsumerService Binding="urn:oasis:names:tc:SAML:2.0:bindings:HTTP-POST" Location=" "
28 </SPSSODescriptor>
29 </EntityDescriptor>
30
```

- b. **Entity ID.** Towards the top of the file.. It would be the blurred out section from below image. This would need to be copied.

Configuring the OneLogin Application

Navigate to the OneLogin Application setup and configuration section. Use the information extracted from the Gainsight XML file to populate the following fields:

- **Audience (EntityID):** Use the **Entity ID** value.
- **ACS (Consumer) URL Validator:** Use the **AssertionConsumerService -> Location URL** value.
- **ACS (Consumer) URL:** This should be the same as the **ACS (Consumer) URL Validator** (the **AssertionConsumerService -> Location URL**).

After entering the required information, save the connection.

The screenshot shows the OneLogin application configuration interface. The 'Configuration' tab is active. The 'Audience (EntityID)' field is highlighted with a green box. Below it, the 'Recipients' section is visible. The 'ACS (Consumer) URL Validator*' and 'ACS (Consumer) URL*' fields are also highlighted with a green box. The 'Save' button is in the top right corner.

The setup is now complete. Proceed to assign the user to the newly created application.