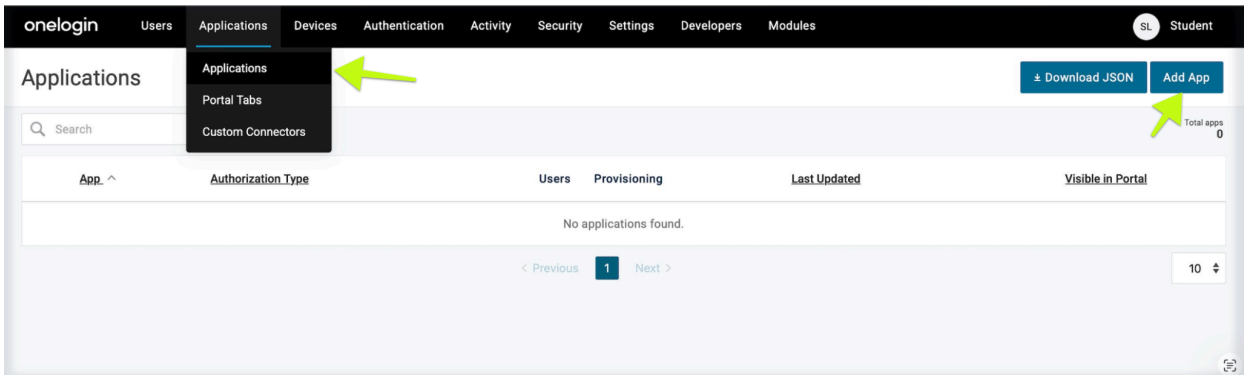
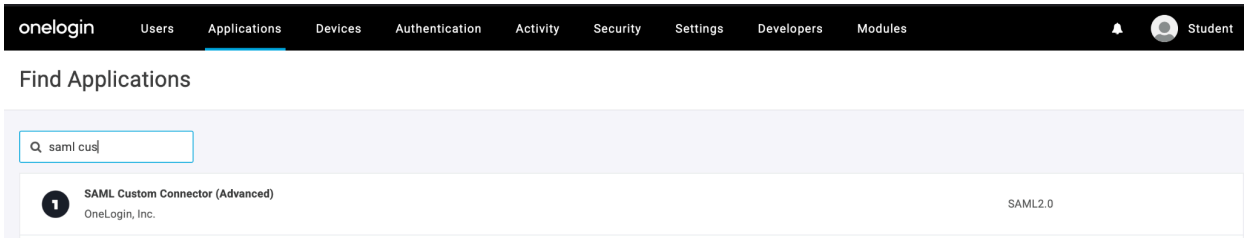
OneLogin SSO Setup: Admin Steps

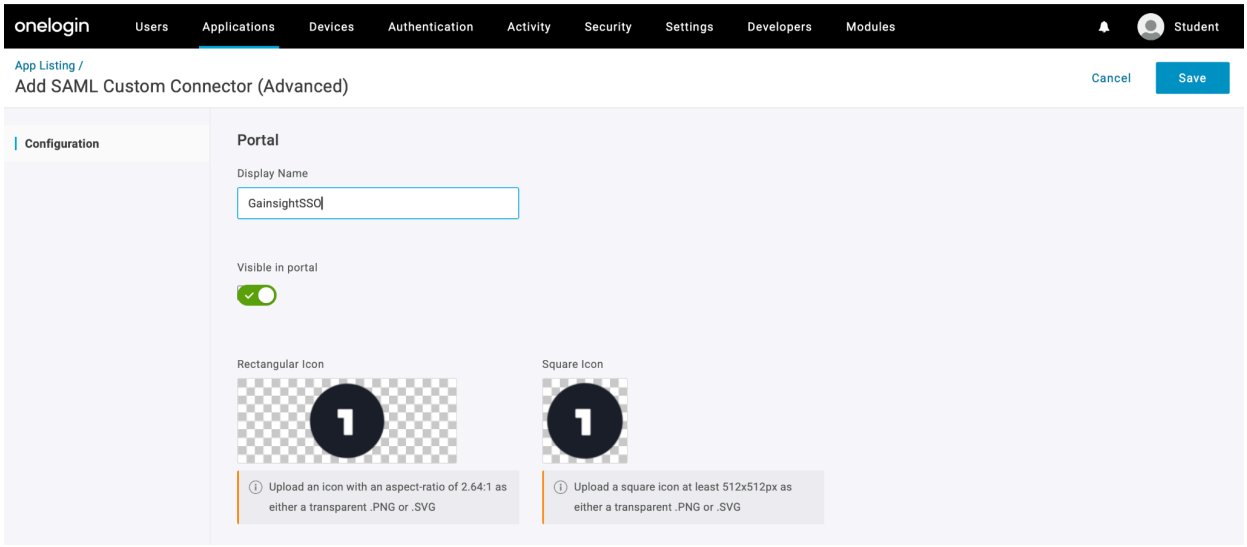
1. Log in to OneLogin as an Administrator.
2. Navigate to **Applications** and select **Add App**.



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.

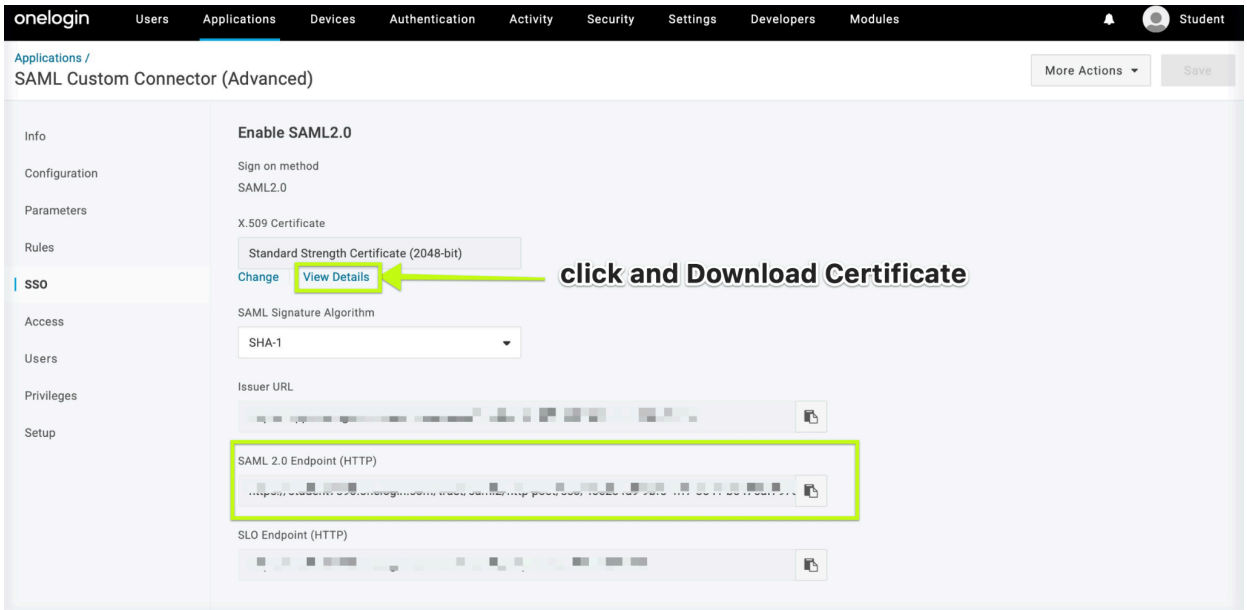


Once you have provided the app name and saved the preceding step, you will be directed to the App setup page.

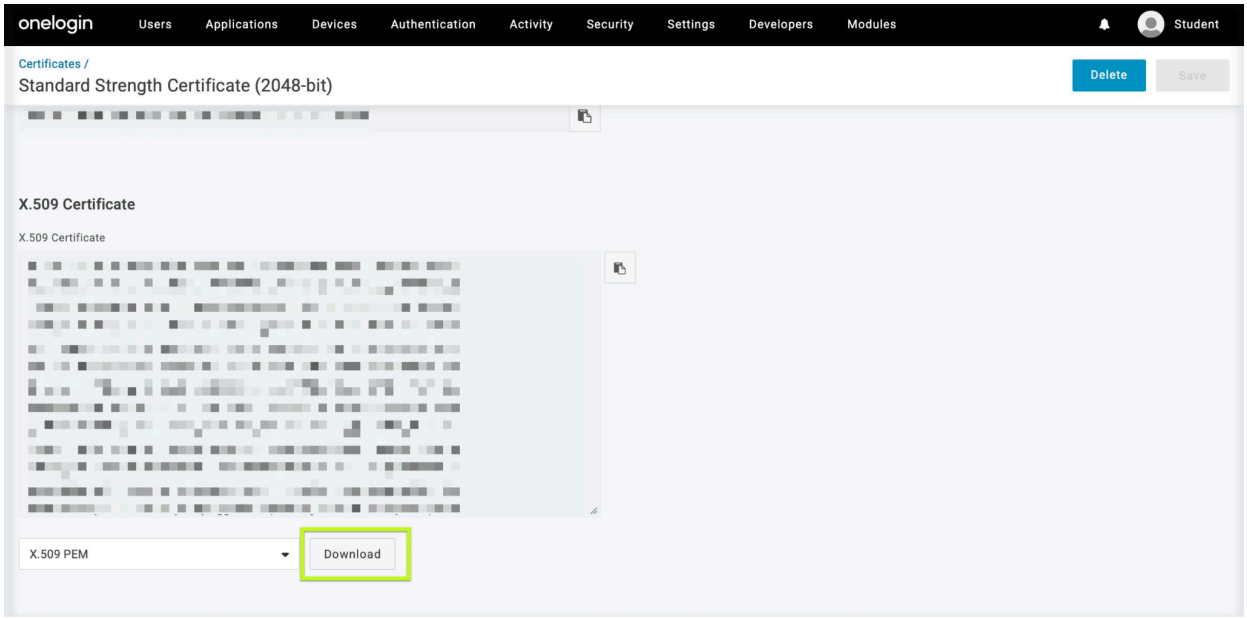
Next, Proceed to the SSO Section

You will need to:

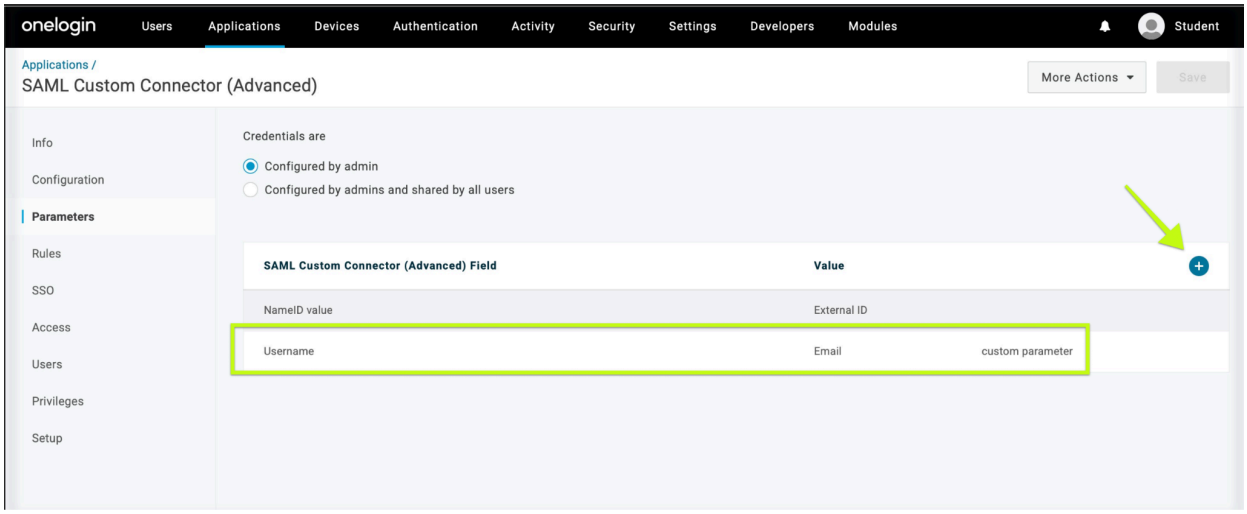
- Copy the SAML 2.0 Endpoint (HTTP).
- Download the x.509 certificate.

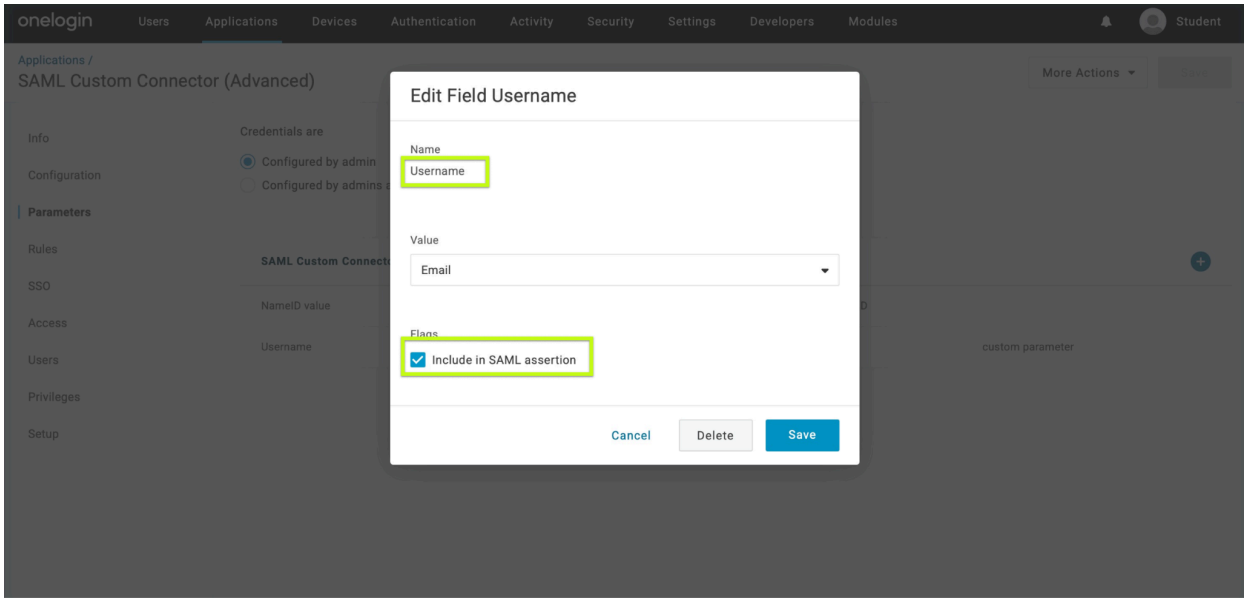


x.509 cert download



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*.





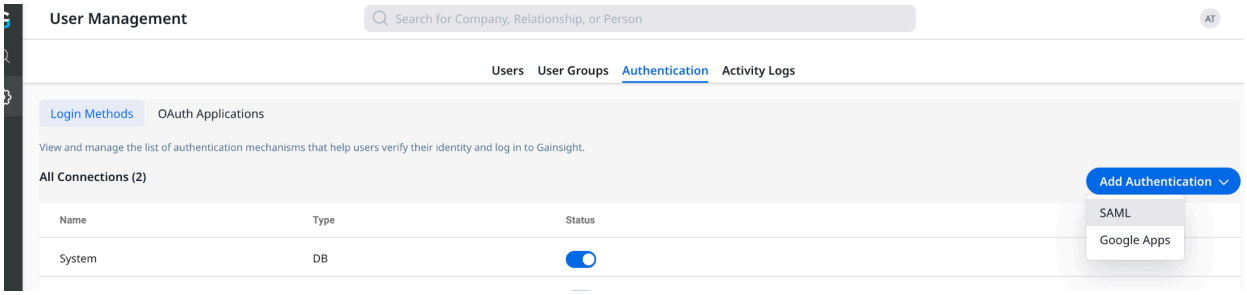
Now, Login to Gainsight:

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 *

[redacted]ent#

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	Target Field
Username	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 *

Enter the domain name for SAML authentication

Sign In URL *

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	Target Field
Username	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.

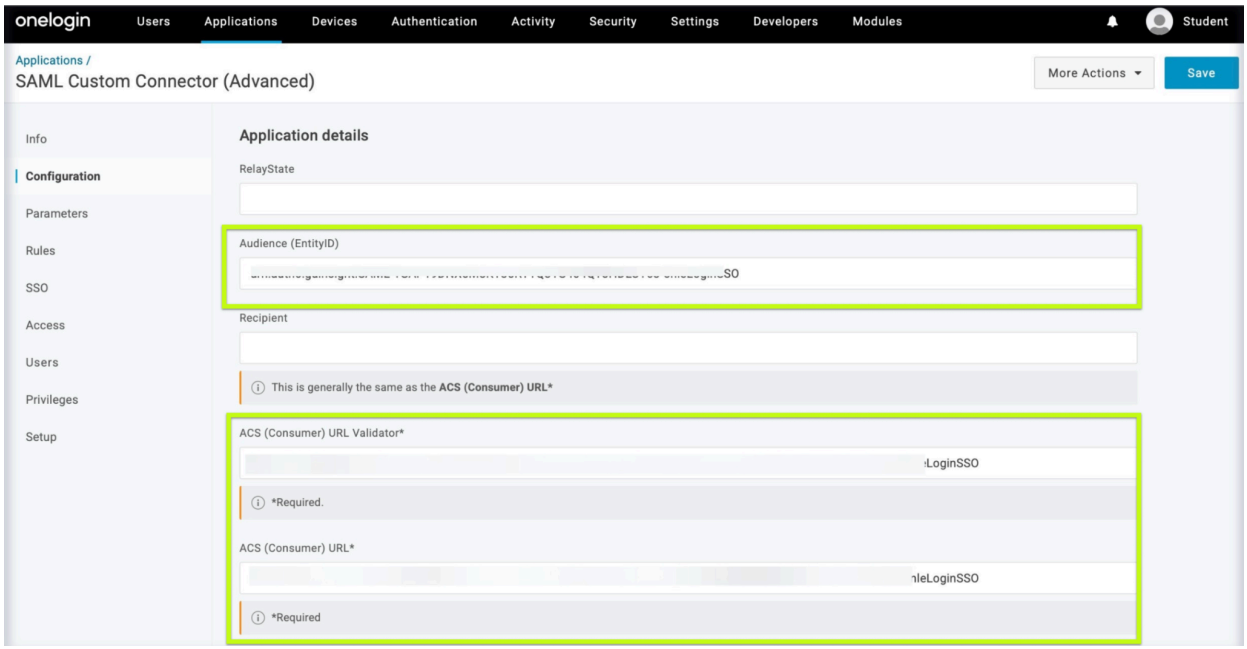
b. Entity ID. Towards the top of the file**..** It would be the blurred out section from below image. This would need to be copied.

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