ExtremeCloud IQ Self-Service Single Sign-On

Entra ID SAML Integration

Version 24.4.0

9039025-00 Rev AA

Published: May 2024

Extreme Networks, Inc.

www.extremenetworks.com

Contents

Integration Overview 3
Step 1 - Select Enterprise Applications in Azure Portal 3
Step 2 - Create a new Enterprise Application 4
Step 3 - Assign Users and Groups 5
Step 4 - Select SAML as the Single Sign-On Method 7
Step 5 – Import Entra ID Metadata Import to ExtremeCloud IQ 9
Step 6 – Map ExtremeCloud IQ User Profile Attributes to SAML Attibutes 13
Step 7 – Map ExtremeCloud IQ Group to Roles 14
Step 8 - Export SP Metadata and Import into Entra ID 15
Step 9 – Map Entra ID Security Groups to ExtremeCloud IQ Roles 17
Step 10 - Test - SP Initiated 19
Step 11 - Test - IdP Initiated 21
Notes and Caveats 23

Integration Overview

The following document outlines the procedure for integration between the Self-Service Single Sign-On framework that is supported in ExtremeCloud IQ and Microsoft Entra ID (formerly Azure Active Directory) through SAML for both IdP initiated and SP Initiated Single Sign-On.

Step 1 - Select Enterprise Applications in Azure Portal

From the Azure Portal, navigate to Azure services and select **Enterprise applications**.

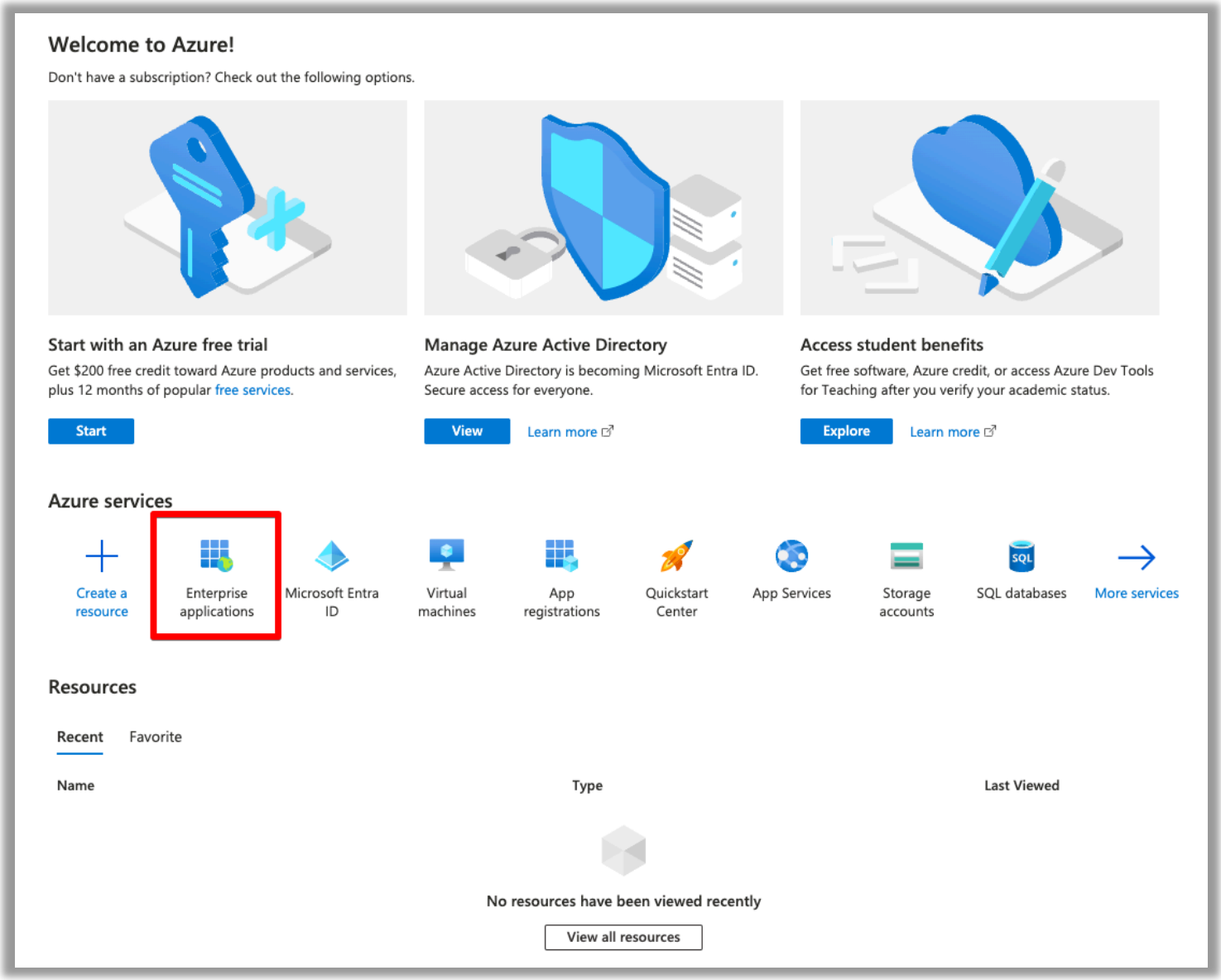


Figure 1 Azure Portal

Step 2 - Create a new Enterprise Application

From the Enterprise Applications, select **New application > Create your own application**.

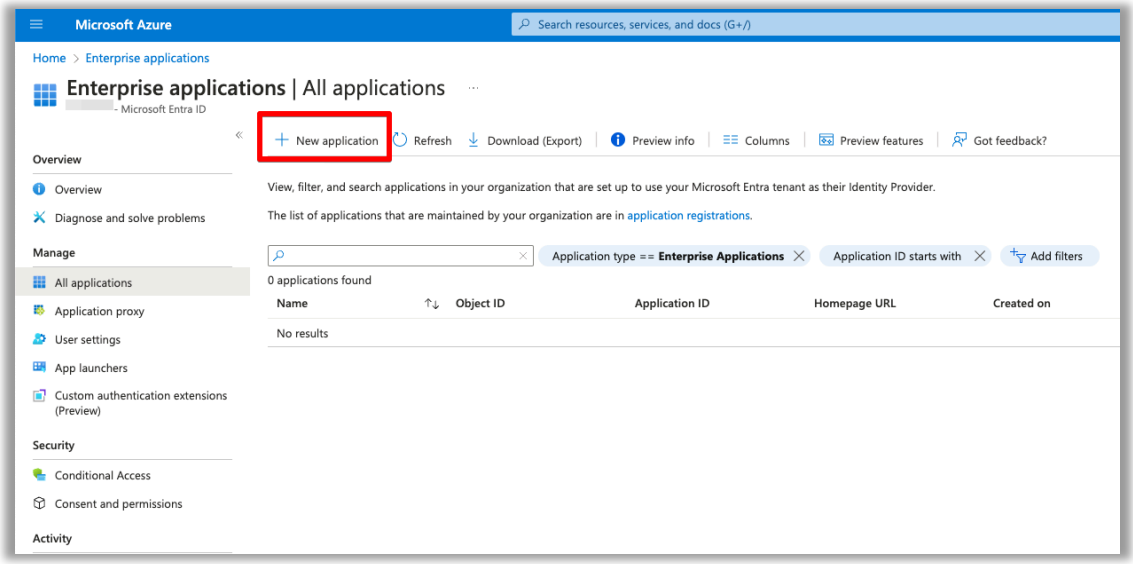


Figure 2 Azure - Enterprise Applications page

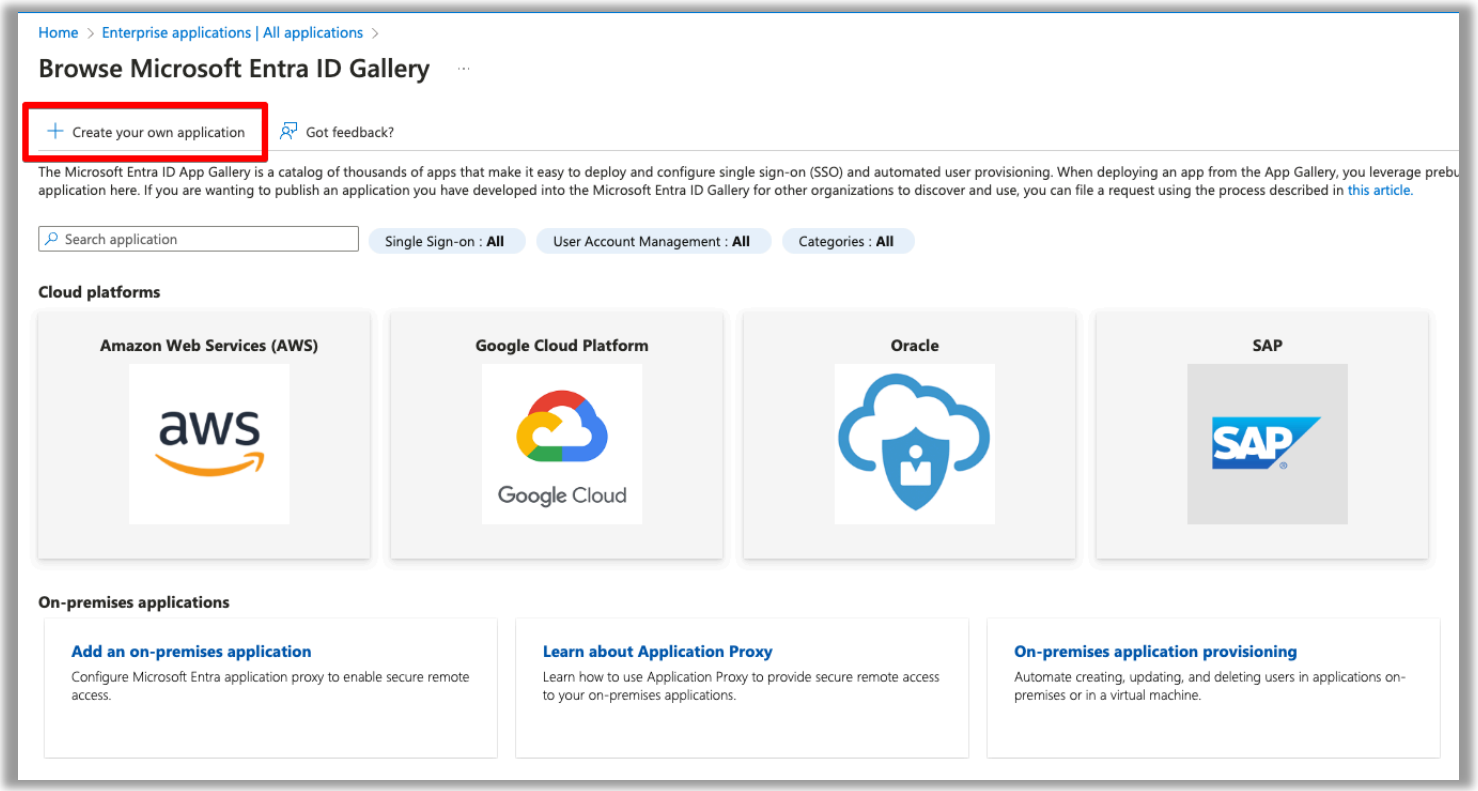


Figure 3 Azure – Create a new application.

From the **Create your own application** dialog:

1. Provide the application name.
2. Select **Integrate any other application you don't find in the gallery (Non-Gallery)**.
3. Select **Create**.

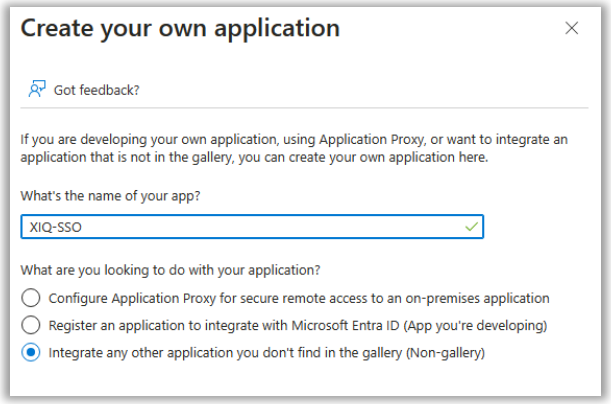


Figure 4 Azure - Creating an Azure application.

The application **Overview** page opens.

Step 3 - Assign Users and Groups

Note: User groups must be created in ExtremeCloud IQ before you can map the user roles.

Add the group objects that will be mapped to the Role Based Access Controls in ExtremeCloud IQ.

1. From the new application **Overview** page, select **Assign Users and Groups** > **Add user/group**.

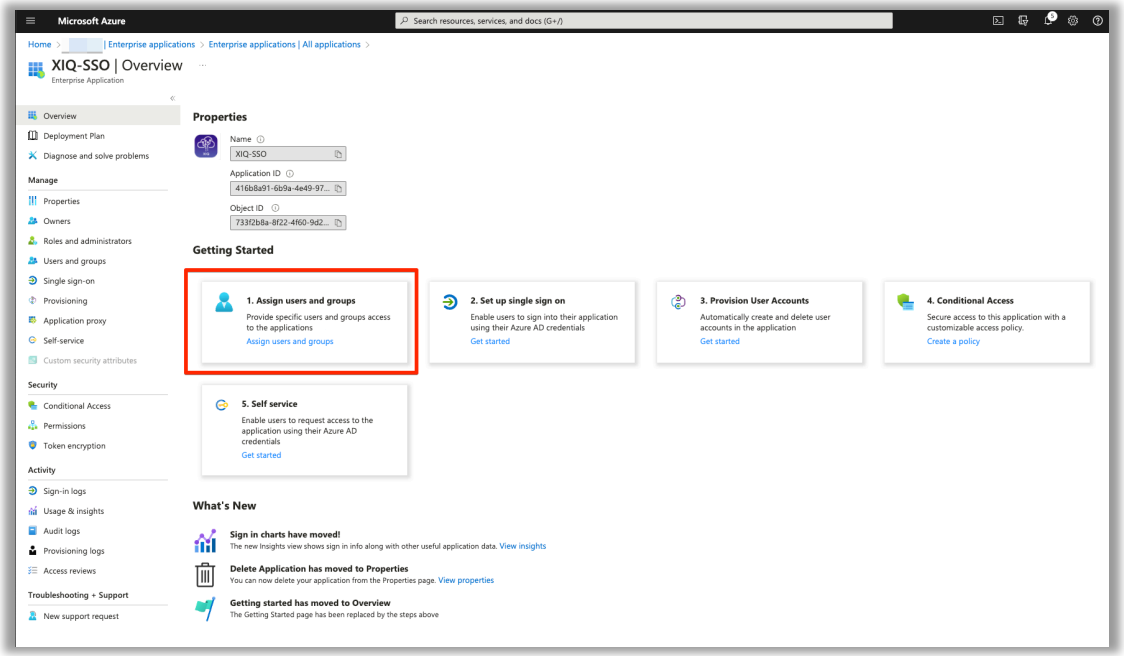


Figure 5 Azure - Assign users and groups to the application.

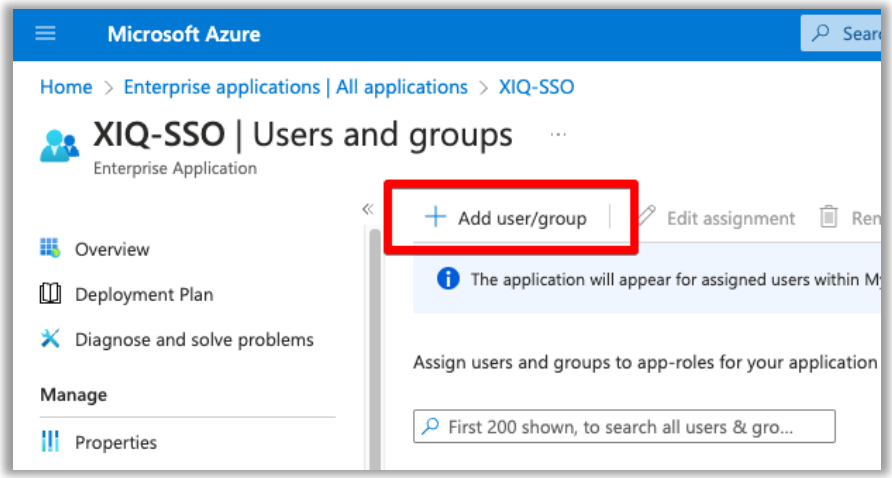


Figure 6 Azure - Adding a user group.

The **Add Assignment** page opens.

2. From the left pane, select the link under **Users and groups**.
   Azure displays ExtremeCloud IQ users and groups in the right pane.
3. Select the check box for each ExtremeCloud IQ required user group.
4. Click **Select**.

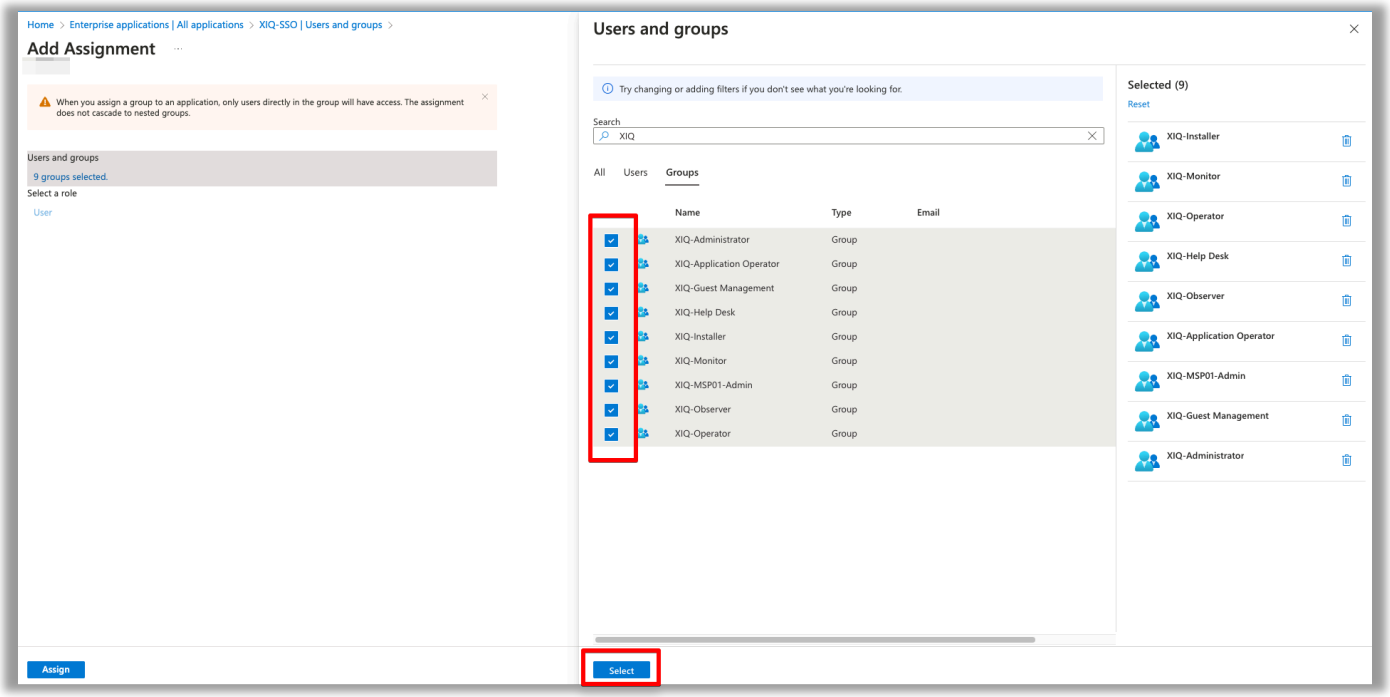


Figure 7 Azure - Assigning ExtremeCloud IQ user groups to an Azure user role.

5. Select **Assign**.

Figure 8 Azure - Assigning ExtremeCloud IQ user groups to an Azure user role.

The selected groups are mapped to the selected role.

Azure displays the selected groups on the **Users and Groups** page.

Note: Only users assigned to the defined groups have access to the defined roles in ExtremeCloud IQ.

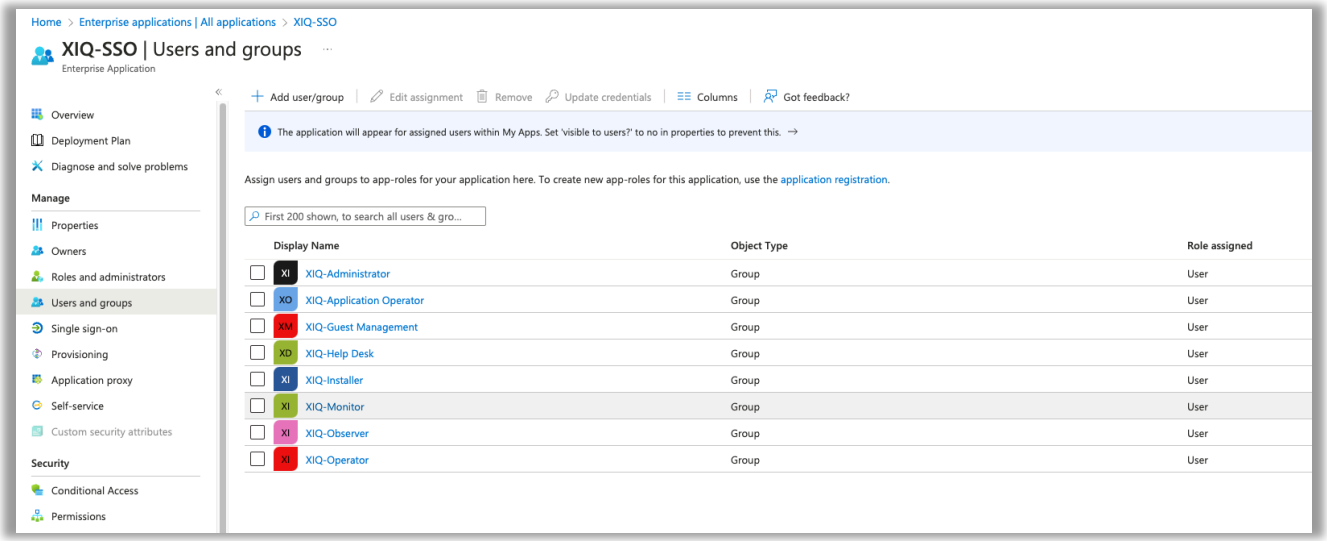


Figure 9 Azure - ExtremeCloud IQ user-defined user groups.

Step 4 - Select SAML as the Single Sign-On Method

Specify SAML protocol for Single Sign-On.

1. From the application **Overview** page, select **Get Started** in the Set up Single sign-on pane.
2. Select **SAML**.

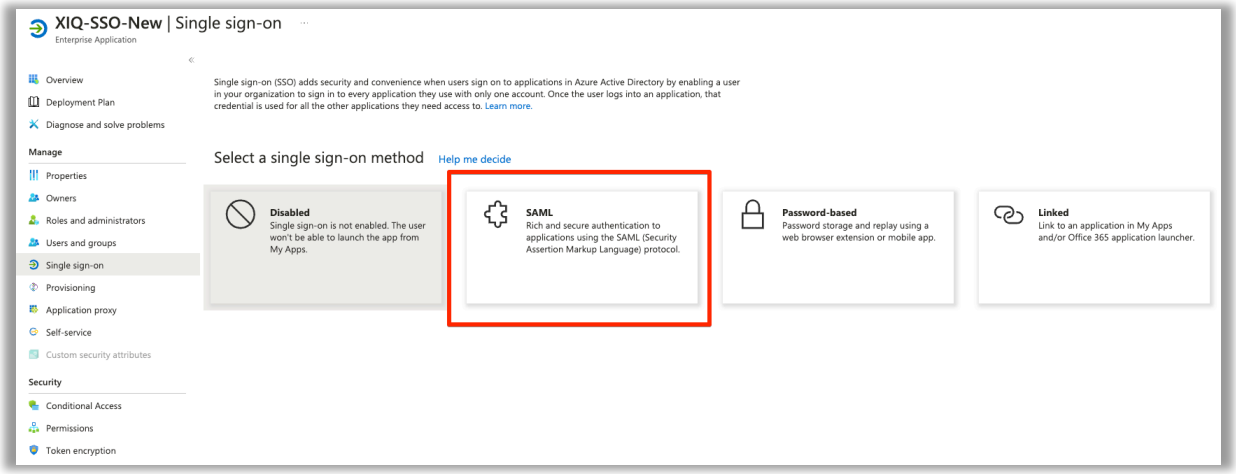


Figure 10 Azure - Specifying SAML protocol in Azure.

3. From the **Set Up Single Sign-On with SAML** page, select **Edit**.

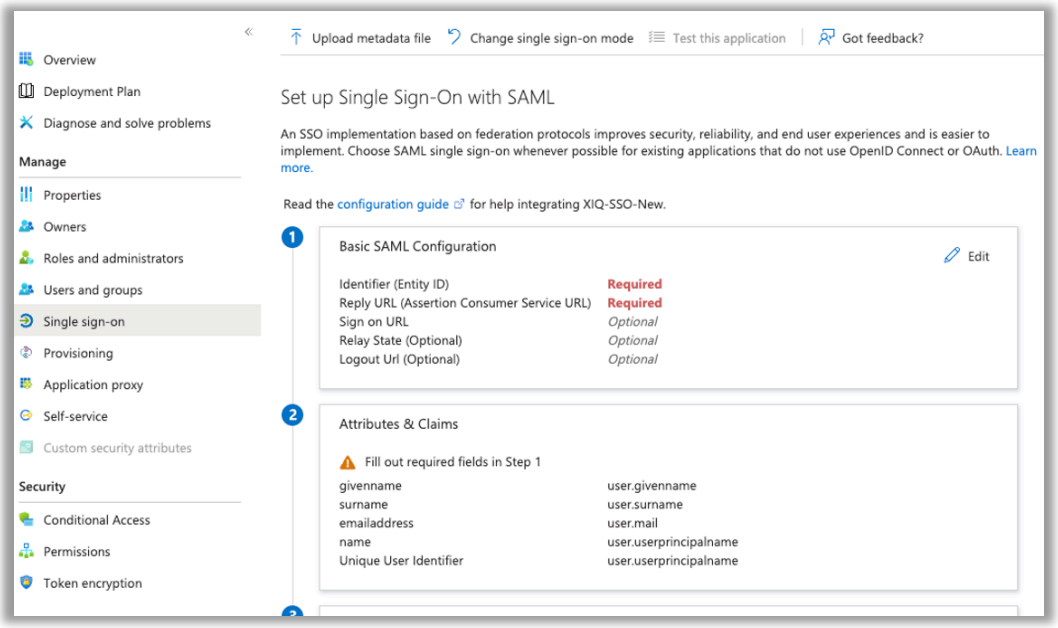


Figure 11 Azure - Basic SAML configuration indicating required fields.

4. Select **Add identifier** (Entity ID) and provide a temporary URL.

   For example, https://temp_ID

5. Select **Add reply URL** and add a temporary reply URL.

   For example, https://temp_reply

6. Select **Save**.

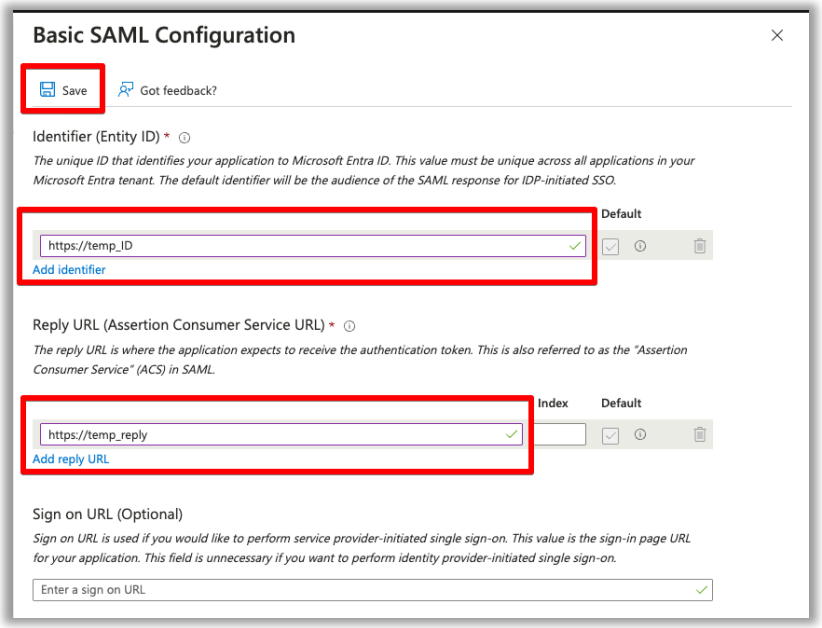
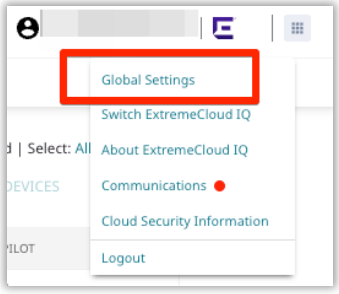


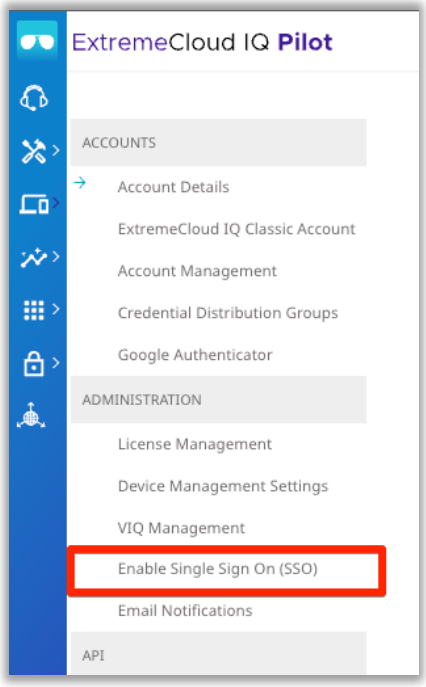
Figure 12 Azure - SAML configuration with place holder data.

Step 5 – Import Entra ID Metadata Import to ExtremeCloud IQ

To see the Enable SSO Global Settings option, log in to ExtremeCloud IQ using the Global Data Center (GDC) SSO URL. For example, *https://sso.xcloudiq.com/login*.

1. From ExtremeCloud IQ, select **Global Settings > Enable Single Sign On (SSO)**.





2. Select **Add Identity Provider**.

Figure 13 ExtremeCloud IQ - Enable SSO.

3. Select **Entra ID (Azure AD)**.

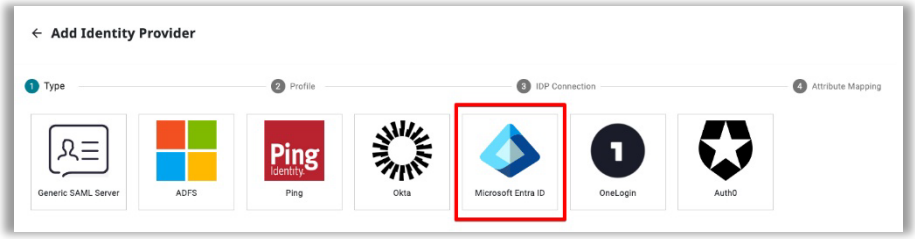


Figure 14 ExtremeCloud IQ - Select Identity Provider.

4. Enter the Fully Qualified Domain Name of the Azure Tenant and optional description.

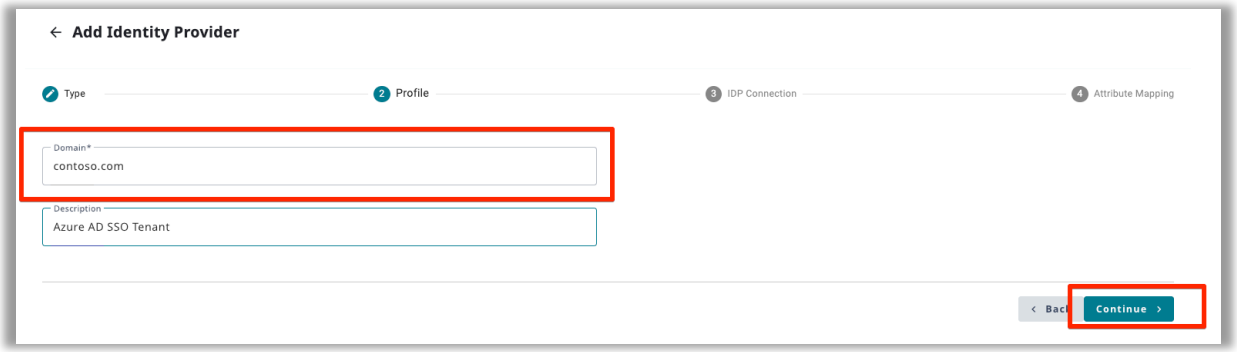


Figure 15 ExtremeCloud IQ - FQDN of the Azure Tenant and optional Description.

5. Select **Continue**.
6. Select the preferred method of entering the IdP Metadata.

Note: In this example, we selected **Import From URL**. The data is imported from the App Federation Metadata URL.

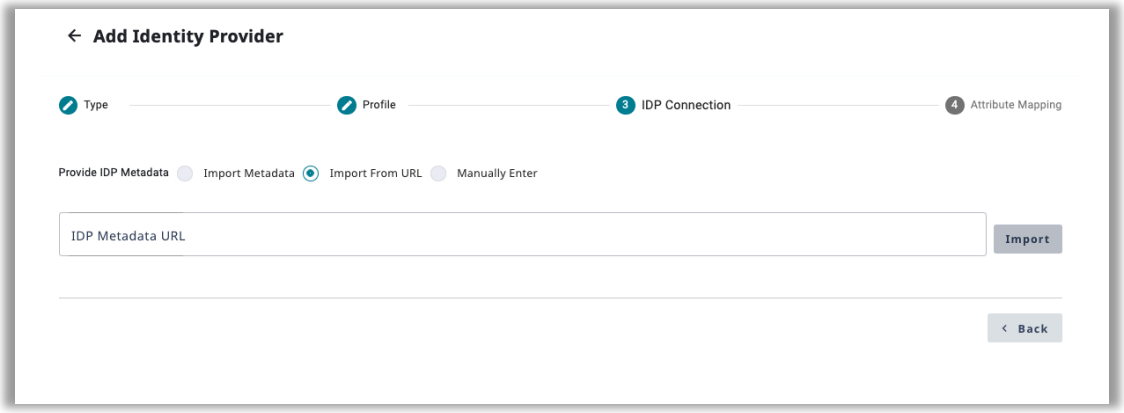


Figure 16 ExtremeCloud IQ - Import From URL option is selected.

7. From the Azure Enterprise Application, Section 3: SAML Certificates, select the App Federation Metadata URL Copy function.

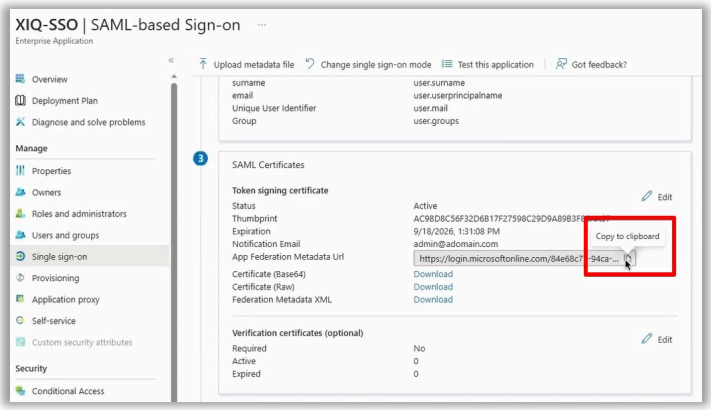


Figure 17. Azure - Copying the App Federation URL.

8. In ExtremeCloud IQ, paste the URL string into the IdP Metadata URL field and select **Import**.

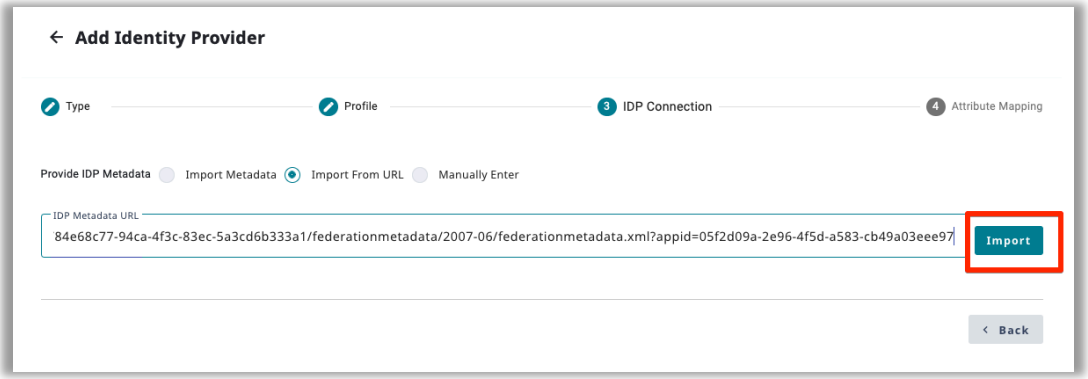


Figure 18 ExtremeCloud IQ - Pasting the App Federation URL for data import.

After importing, the fields in the **IdP Connection** tab populate, automatically including the Verification Certificate.

9. Select **Continue**.

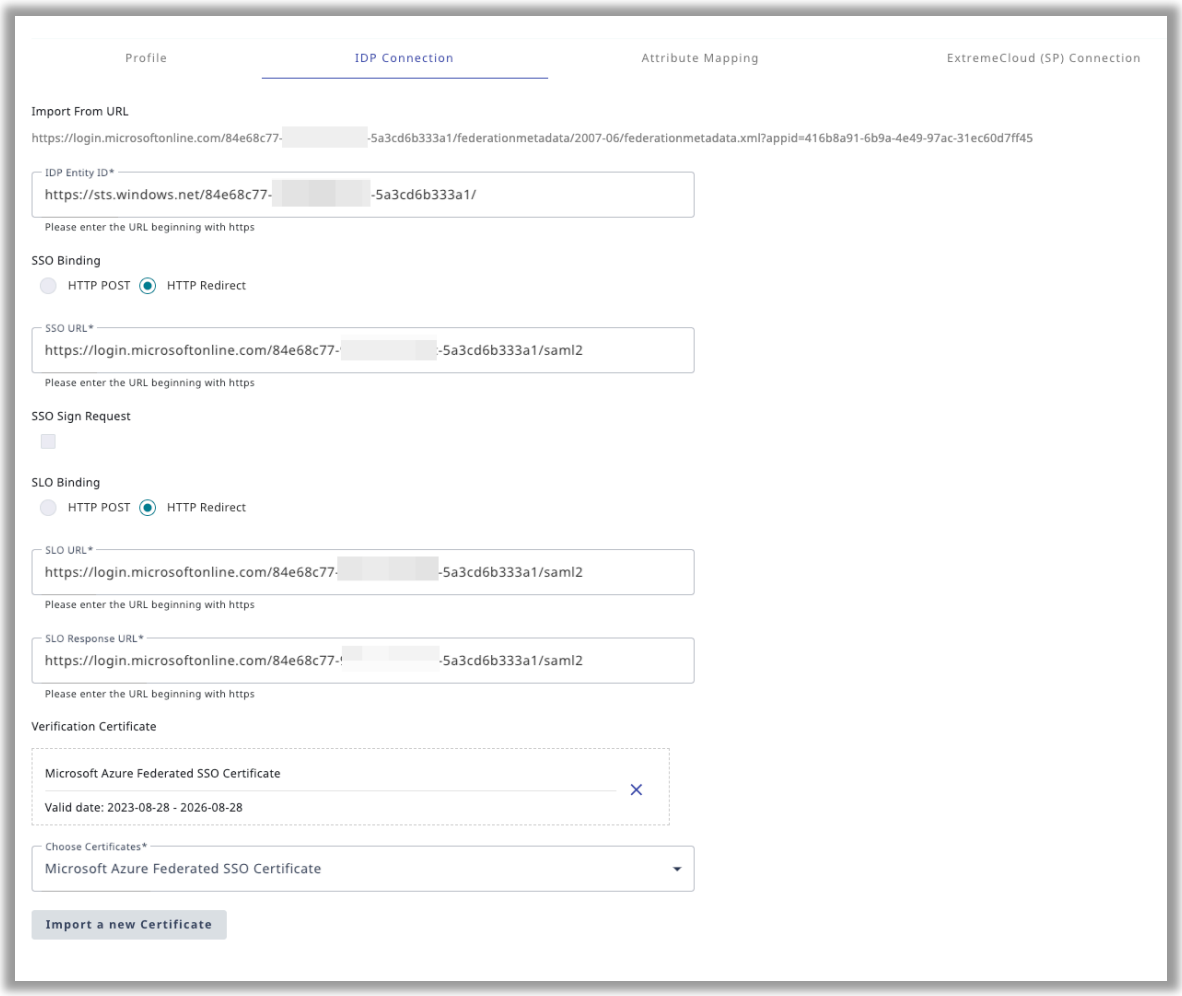


Figure 19 ExtremeCloud IQ - IdP Connection information is populated automatically.

Step 6 – Map ExtremeCloud IQ User Profile Attributes to SAML Attibutes

In ExtremeCloud IQ, you must map the appropriate User Profile Attributes to the SAML Attributes sent from the IdP. These strings must be created and in sync with both IdP and SP. The following SAML Attributes are required for **Entra ID** Single Sign-On:

- First Name
- Last Name
- Email
- Group

Note: To generate the SP Metadata required to complete the IdP SAML configuration, the SAML strings cannot be configured on the IdP until the ExtremeCloud IQ Workflow is completed. You must complete the ExtremeCloud IQ workflow first. If you do not know the SAML Attribute Strings, add place holder data to save and complete the configuration.

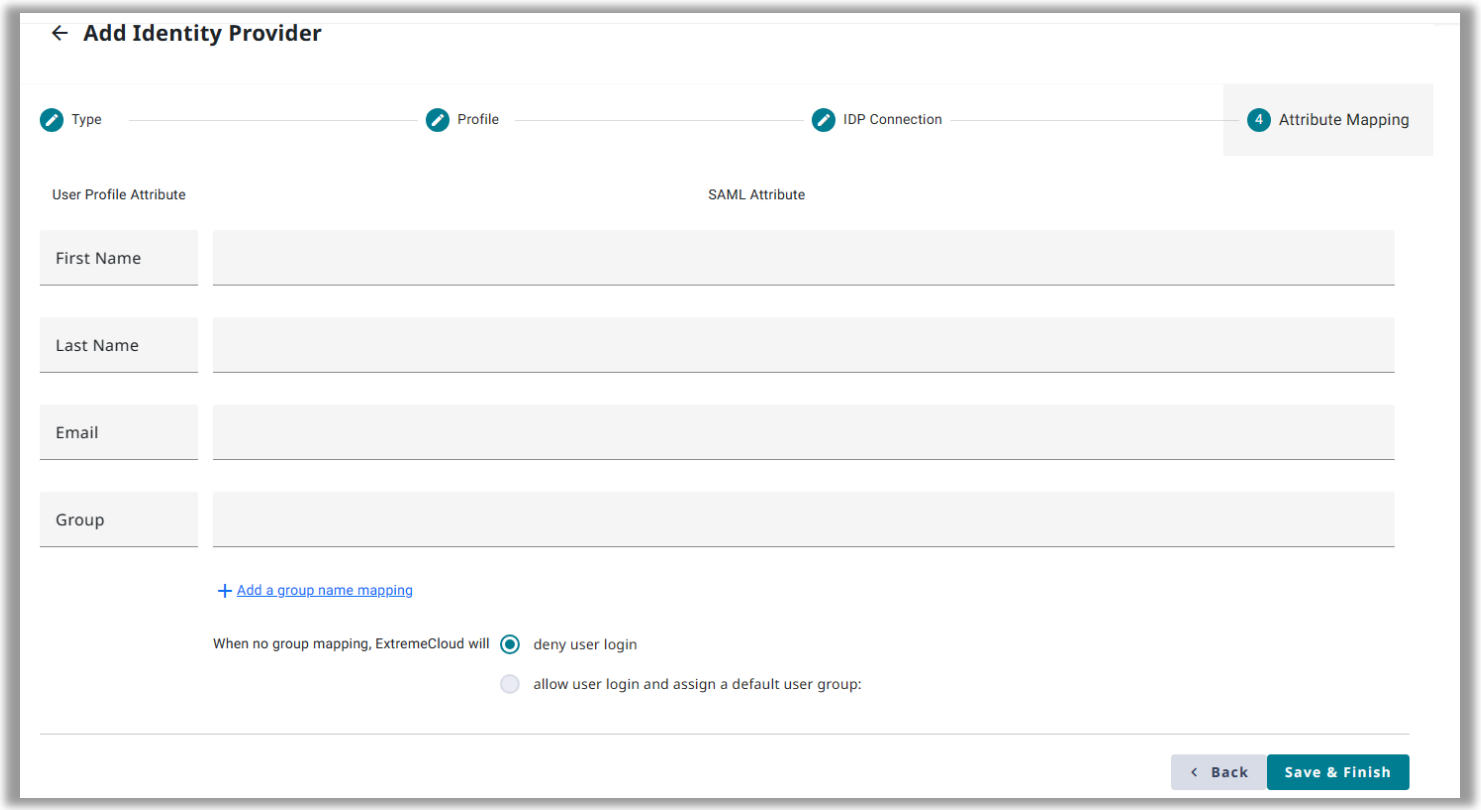


Figure 20 ExtremeCloud IQ - Providing user profile attributes.

The following table includes the required strings for integration with Entra ID.

Table 1. ExtremeCloud IQ - Required Strings for Microsoft Entra

User Profile Attribute	SAML Attribute
First Name	http://schemas.xmlsoap.org/ws/2005/05/identity/claims/givenname
Last Name	http://schemas.xmlsoap.org/ws/2005/05/identity/claims/surname
Email	http://schemas.xmlsoap.org/ws/2005/05/identity/claims/email
Group	http://schemas.microsoft.com/ws/2008/06/identity/claims/groups

Step 7 – Map ExtremeCloud IQ Group to Roles

The ExtremeCloud IQ roles must be mapped based on the user group membership that is created in Entra ID to enforce authorization.

Note: As an example, the following groups created in Entra ID map to ExtremeCloud IQ roles. Users added to these groups are assigned the corresponding role.

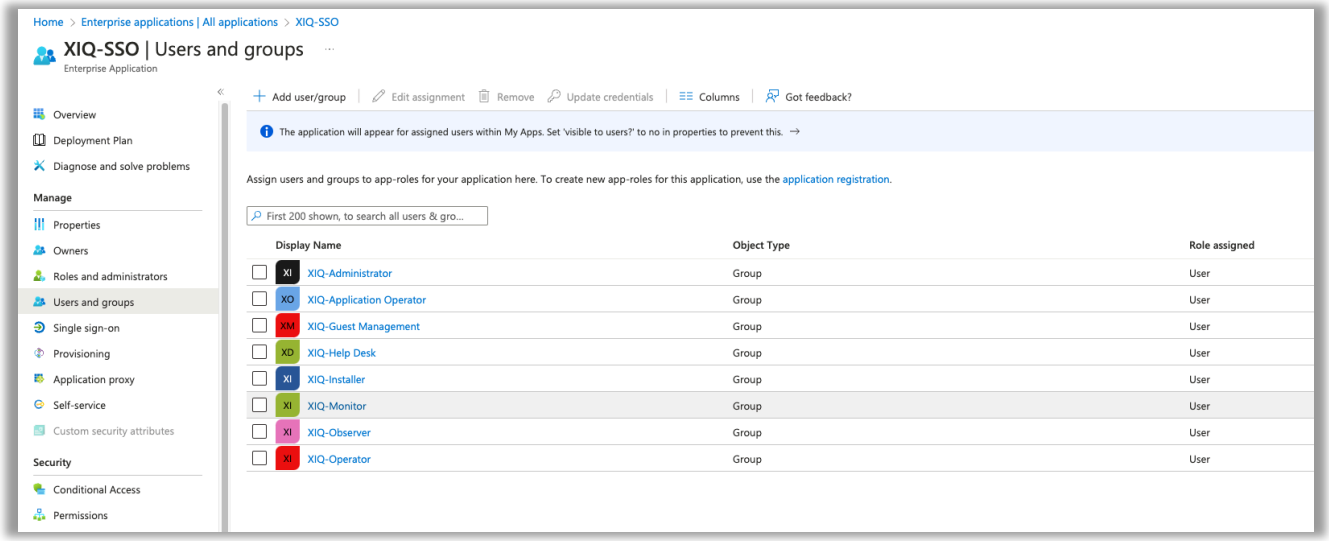


Figure 21 Azure - ExtremeCloud IQ user groups displayed in Azure.

1. In ExtremeCloud IQ, go to **Global Settings > Enable Single Sign On (SSO)**.
2. Select **Attribute Mapping**.
3. Select **+ Add a group name mapping**.
4. Enter the exact group name from Entra ID (for example, XIQ-Operator).
5. Then, select **Operator** from the ExtremeCloud IQ group.

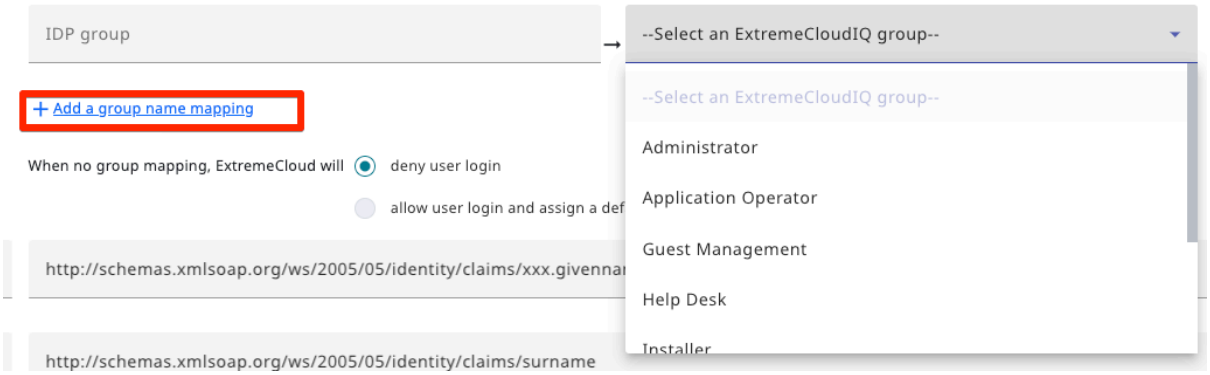


Figure 22 ExtremeCloud IQ - Group name mapping.

Build and order the rules based on First Match. To reorder the rules, select the icon. 

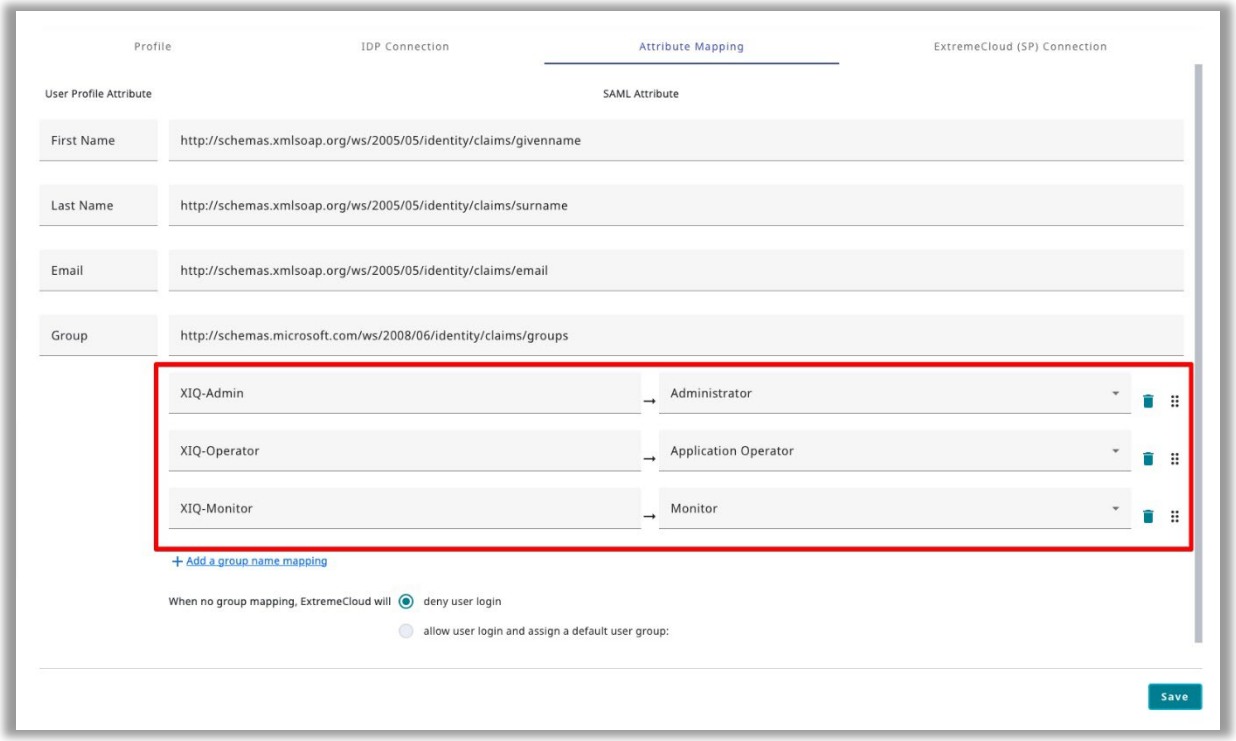


Figure 23 ExtremeCloud IQ - Attribute mapping.

Note: If a user is successfully authenticated but is not a member of a defined group, you have the option to deny the user login or you can specify a default catchall Role in which to place the user. For example, **Monitor Only**.

6. Select **Save and Finish** to complete the ExtremeCloud IQ workflow.

Step 8 - Export SP Metadata and Import into Entra ID

After saving the completed Add IdP Workflow in ExtremeCloud IQ, export the SP metadata and import the data into the IdP to complete the configuration.

1. Go to the main **Single Sign On** page in ExtremeCloud IQ and edit the saved IdP configuration.

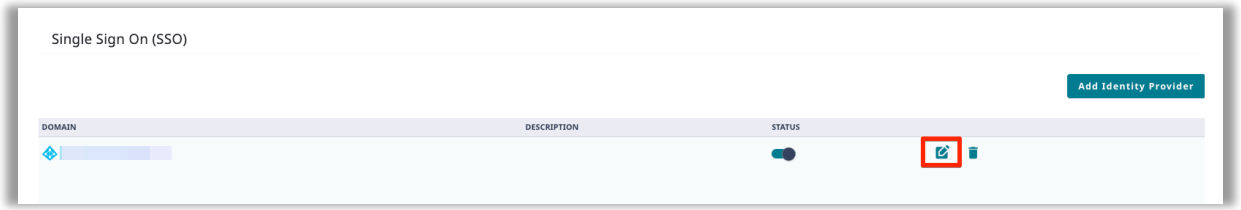


Figure 24 ExtremeCloud IQ - From the main SSO page edit the Domain's saved IdP configuration.

2. Select the **ExtremeCloud (SP) Connection** tab and select **Download SP Metadata**.

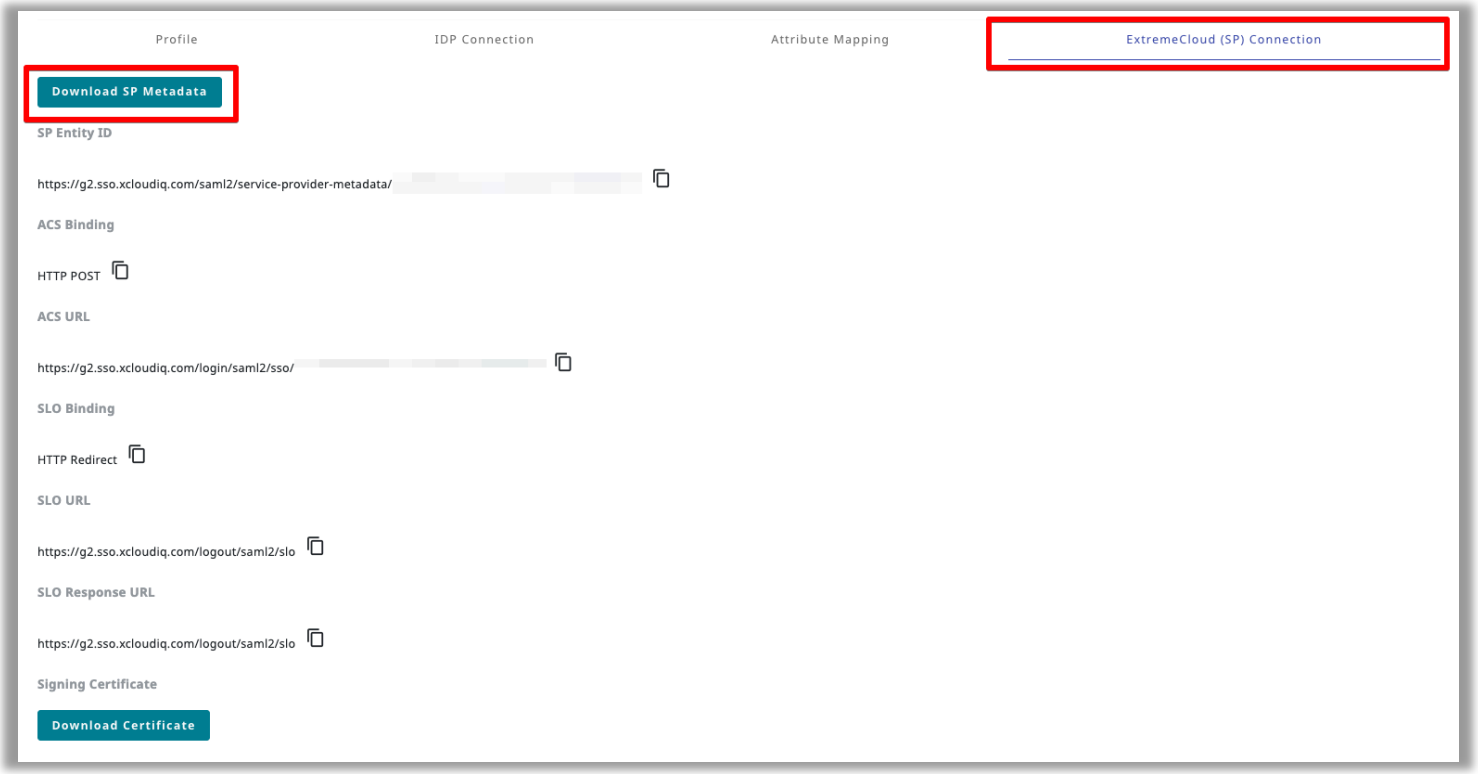


Figure 25 ExtremeCloud IQ - Download SP Metadata from ExtremeCloud (SP) Connection tab.

3. Download and keep the .XML file.

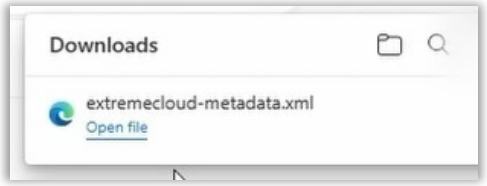


Figure 26 Azure - Download and open XML file.

4. In the Entra ID (XIQ-SSO) Enterprise Application **SAML-based Sign-on** page, select **Upload metadata file** and navigate to the saved exported file from ExtremeCloud IQ.

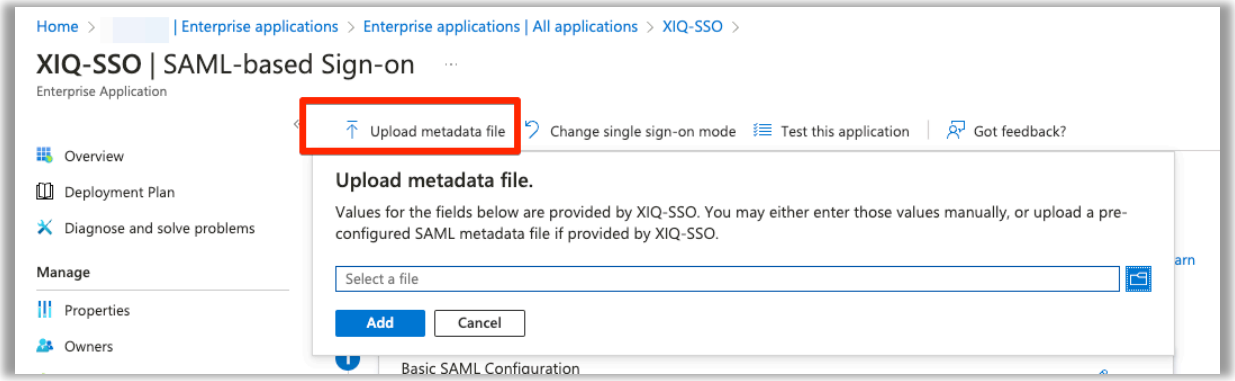


Figure 27 Azure - Upload Metadata XML file.

5. Confirm that the imported data is correct; then save the configuration.

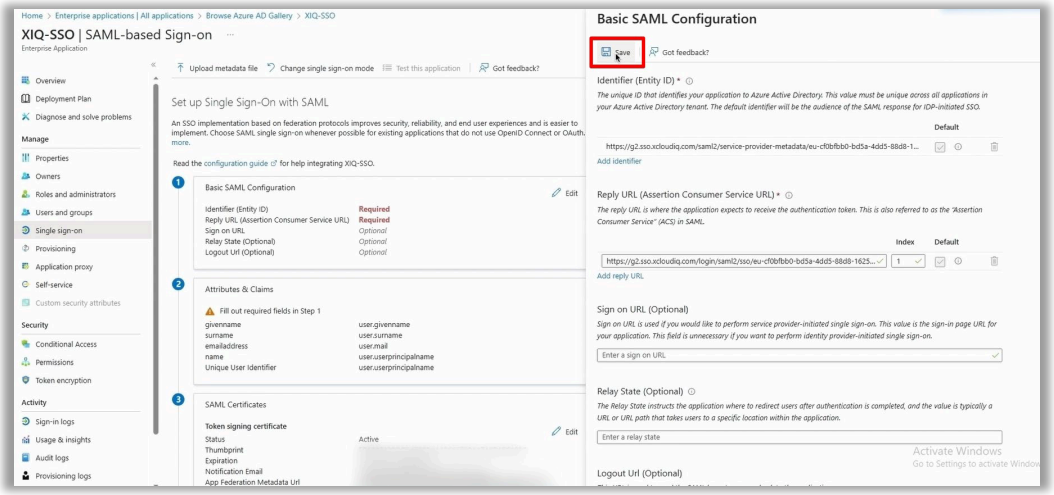


Figure 28 Azure - Save the SAML Configuration.

The configuration updates. Now you can edit Section 2: Attributes and Claims.

Note: When prompted to test the application, select **No I'll test later**.

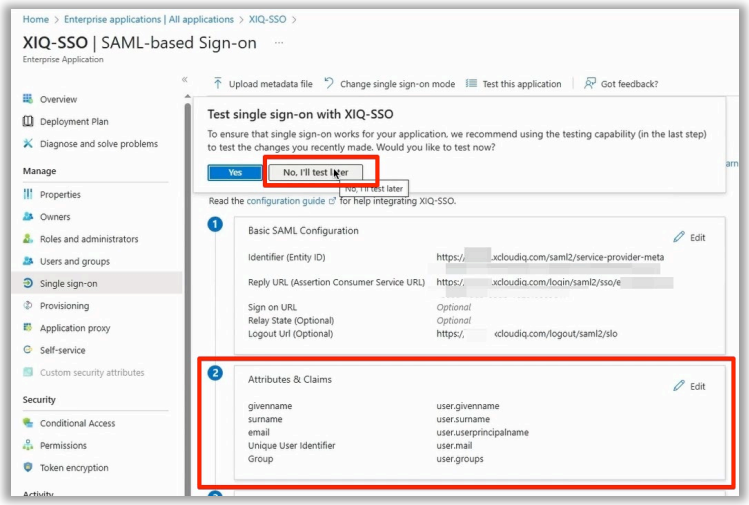


Figure 29 Azure - Attributes and Claims display. Test Later.

Step 9 – Map Entra ID Security Groups to ExtremeCloud IQ Roles

Configure the SAML attribute strings required to map the Entra ID security groups to the ExtremeCloud IQ Role-Based Access Control (RBAC) roles for authorization.

This step includes manually adding the additional Attributes/Claims required in the Entra ID Enterprise Application to map user accounts to ExtremeCloud IQ RBAC roles.

Figure 30 Azure - Edit Attributes and Claims.

Note: You must manually add the items in red to the Default Attributes and Claims created by Entra ID.

Under Additional Claims, select a row from the table. The claim properties open.

User Profile Attribute	SAML Attribute	AAD Value
Email	http://schemas.xmlsoap.org/ws/2005/05/identity/claims/email	user.userprincipalname
Group	http://schemas.microsoft.com/ws/2008/06/identity/claims/groups	user.groups[ApplicationGroup]
First Name	http://schemas.xmlsoap.org/ws/2005/05/identity/claims/givenname	user.givenname
Last Name	http://schemas.xmlsoap.org/ws/2005/05/identity/claims/surname	user.surname

The following Attributes and Claims edits are required:

- Unique User ID – Change the value to `'user.mail'`
- Default name claim – Change from `'name'` to `'email'`
- Remove emailaddress claim with value `user.mail`

To add a group claim, from the Attributes and Claims page, select **Add a group claim**.

- Select **Groups assigned to the application** and **Cloud-only group display names**.

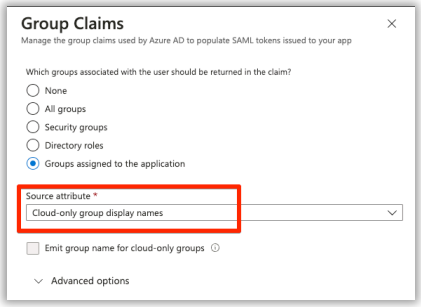


Figure 31 Azure - Group Claims edits.

Step 10 - Test - SP Initiated

To log in to ExtremeCloud IQ through SP initiated:

1. Browse to the GDC Login Page https://sso.extremecloudiq.com/login and select the SSO icon.

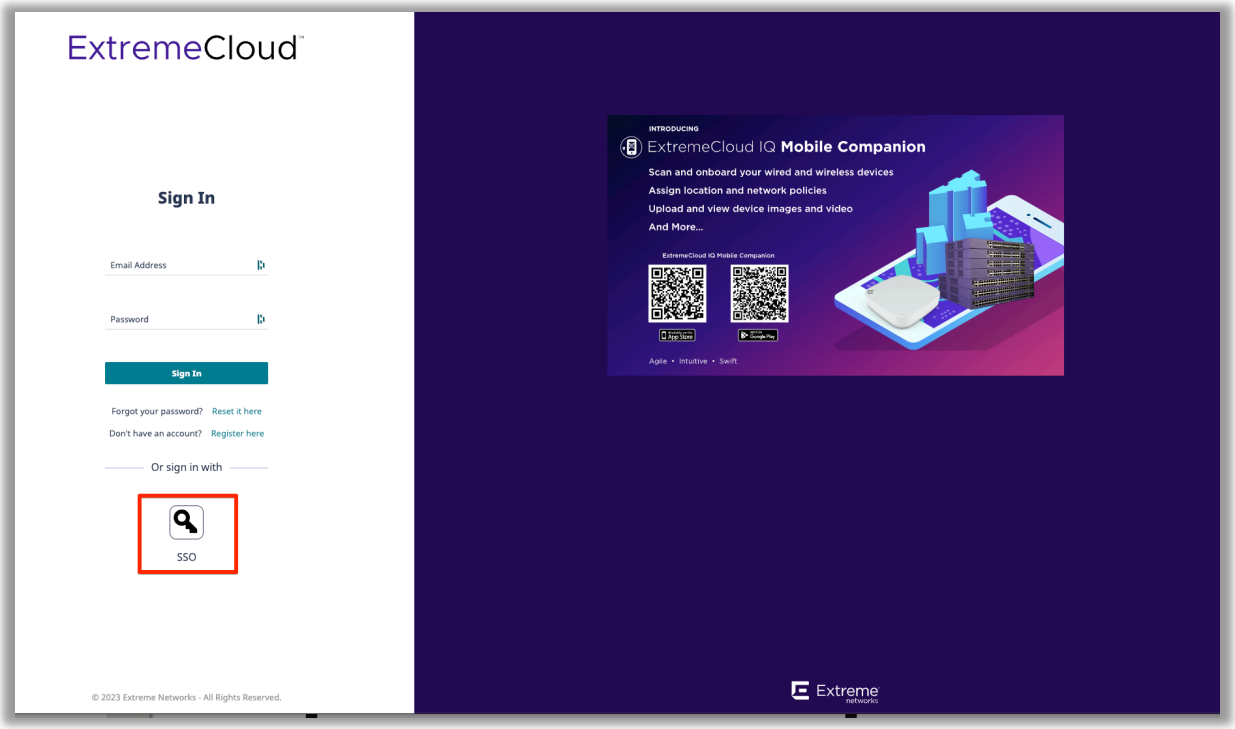


Figure 32 ExtremeCloud IQ Login.

2. Enter the email address of the IdP account and complete the IdP login process.

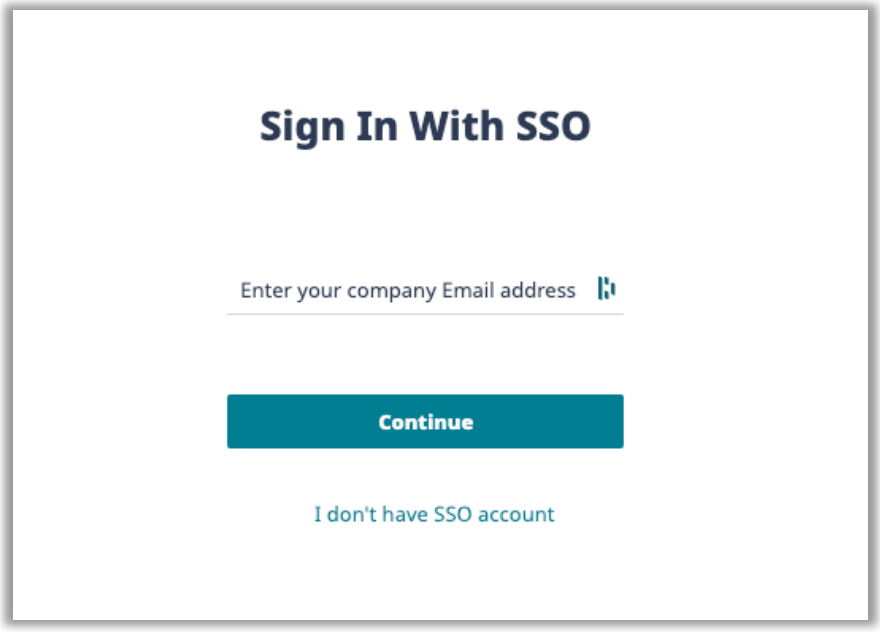


Figure 33 ExtremeCloud IQ SSO Login.

The browser is redirected to the Microsoft Login Portal. After a successful sign in, the browser redirects to the ExtremeCloud IQ default view.

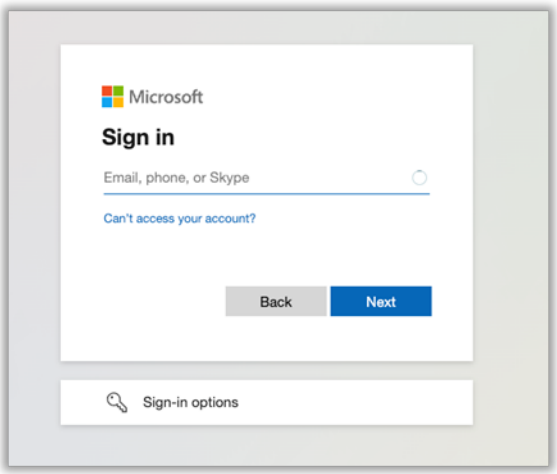


Figure 34 Microsoft Login Portal for ExtremeCloud IQ.

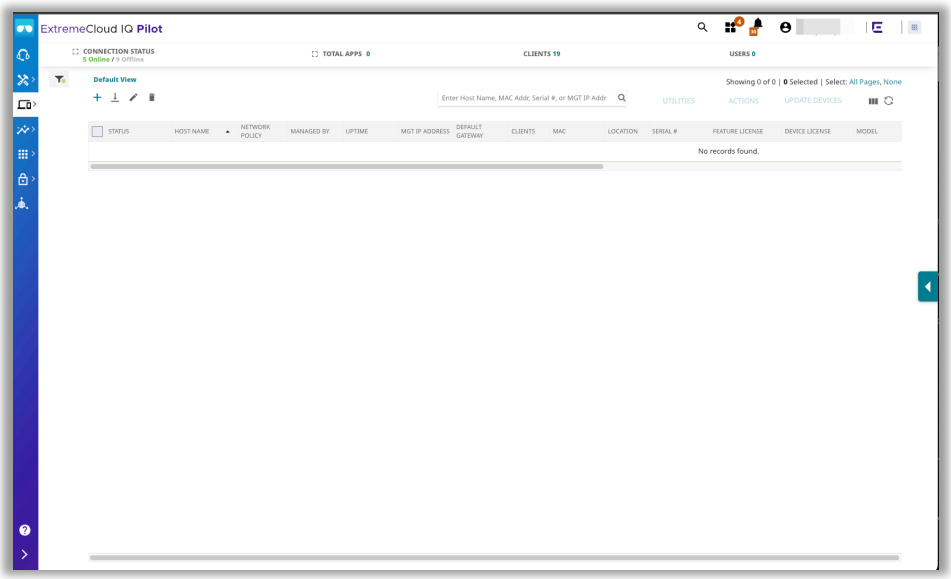


Figure 35 ExtremeCloud IQ Default View.

The ExtremeCloud IQ Audit Logs include the login action.

Figure 36 ExtremeCloud IQ Audit Logs.

Step 11 - Test - IdP Initiated

After the integration is complete, test the application.

To start an IdP initiated test:

1. Go to the Azure main Single Sign On page for the XIQ-SSO application.
2. Select **Test**.

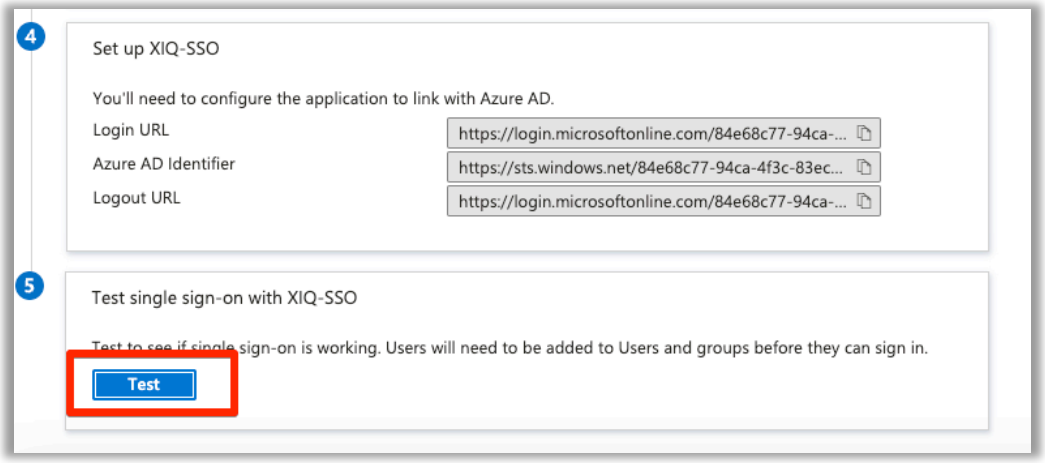


Figure 37 Azure - Test XIQ-SSO application.

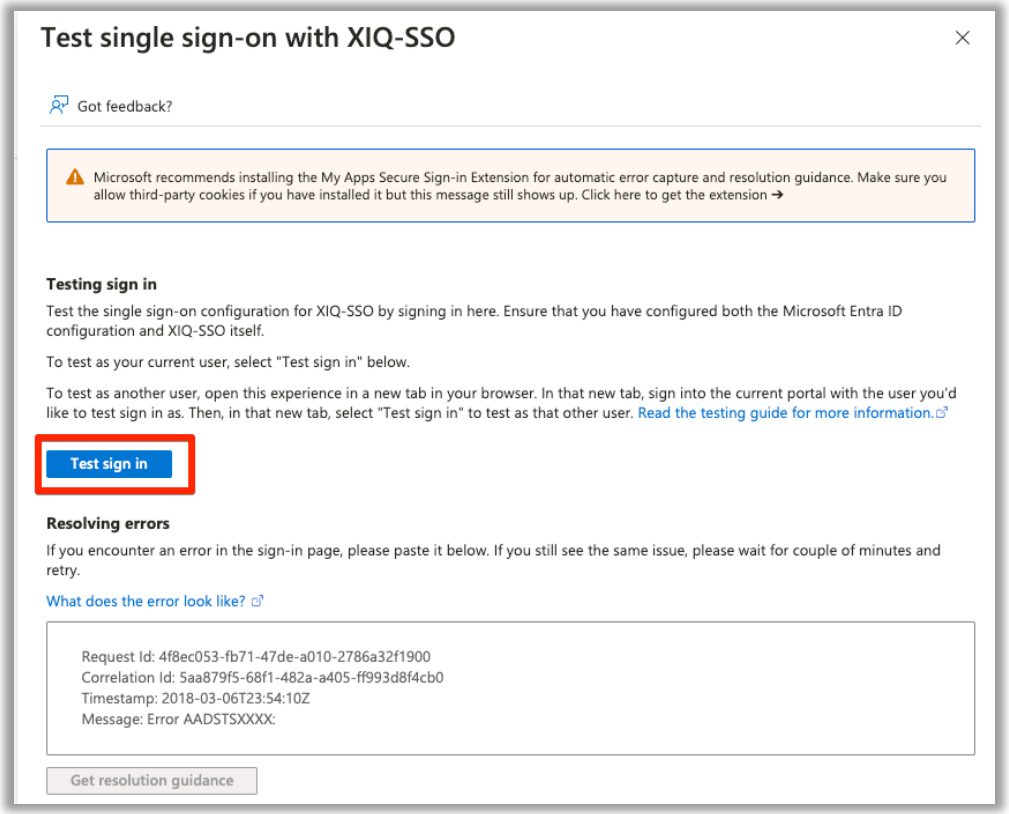


Figure 38 Azure - Test Sign in for XIQ-SSO application.

The browser redirects to the Microsoft Login Portal. After a successful login, you are redirected to the ExtremeCloud IQ default view.

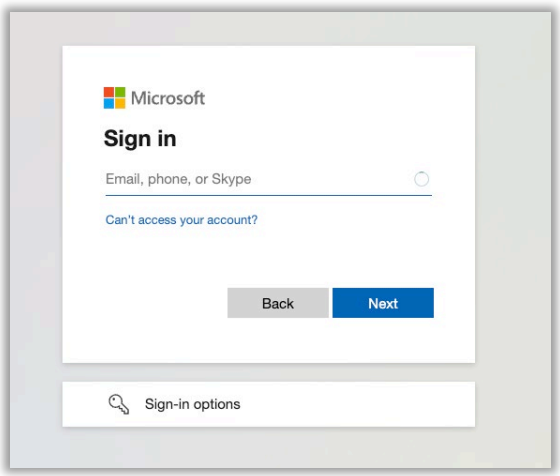


Figure 39 Microsoft Login Portal for ExtremeCloud IQ.

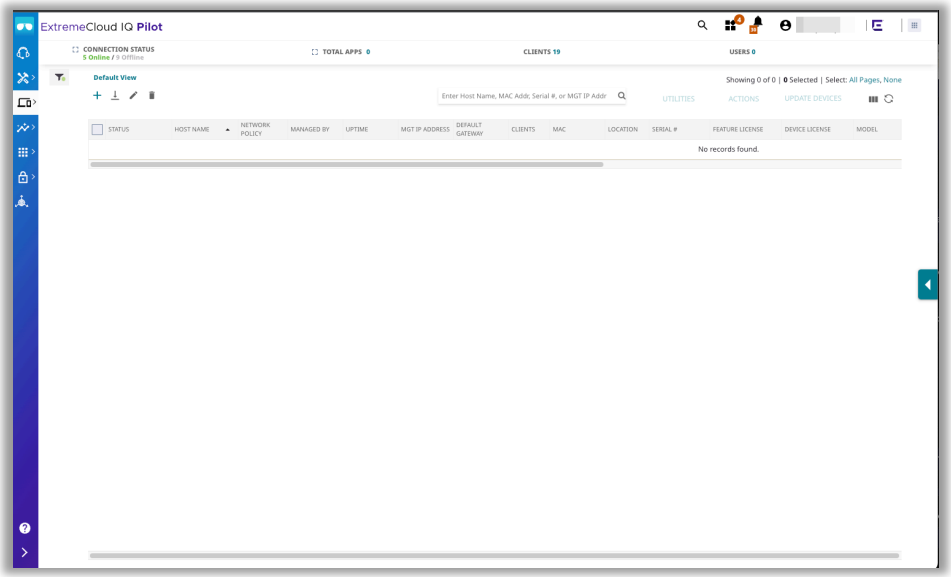


Figure 40 ExtremeCloud IQ Default View.

The ExtremeCloud IQ Audit Logs include the login action.

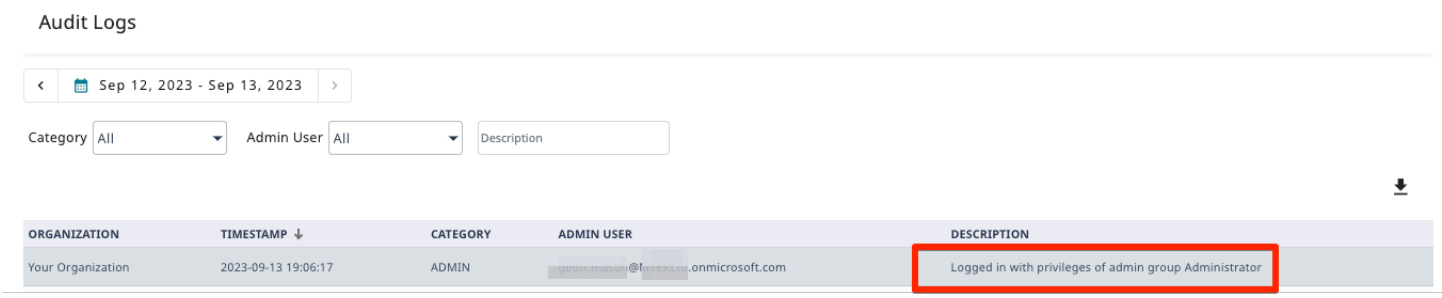


Figure 41 ExtremeCloud IQ Audit Logs.

Notes and Caveats

- The first time an admin user logs in, ExtremeCloud IQ creates a corresponding entry in the ExtremeCloud IQ Accounts database for that VIQ (account) mapped to the appropriate role based on the mapping rules. An SSO-created account includes a blue flag that indicates the account is automatically created.

  For example,'test.user@company.onmicrosoft.com' is a member of the group mapped to the Operator Role, and ExtremeCloud IQ creates the following entry:

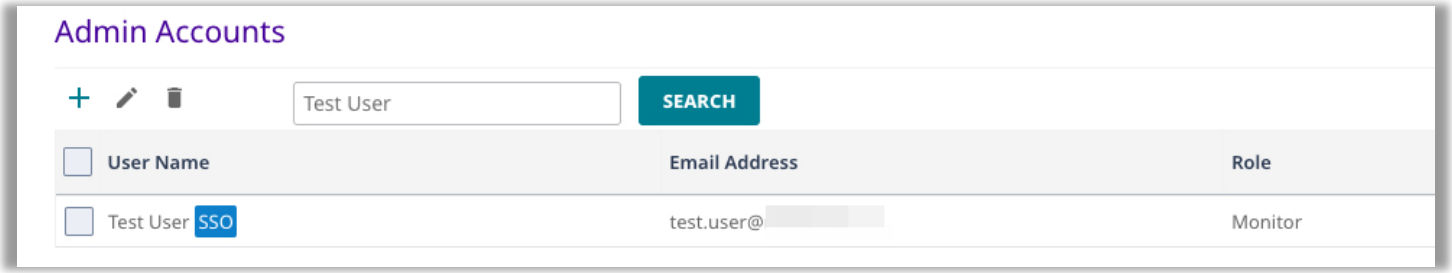


Figure 42 Admin Accounts list shows user and assigned role.

- The Username field is created only if the Entra ID User object is provisioned with the First Name / Last Name field and the Attributes are added in ExtremeCloud IQ.
- SSO-created accounts must be assigned to a location manually in ExtremeCloud IQ.
- Planned in a future release, SSO-created accounts will not be assigned as external Admins to other VIQs (accounts).
- A single IdP SSO domain may be linked to multiple VIQs (accounts), however at this time switching between each requires manually logging in to each VIQ (account).
- If individual IdP groups to RBAC roles are not defined, you must configure a Catchall group, and add all users who require access, along with the Catchall rule. Without this configuration, the user authentication will fail.
- At this time, deleting an SSO configuration in ExtremeCloud IQ does not purge all certificates. This feature is planned for a future release.