

# 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

 $\odot$  2024 Extreme Networks, Inc. All rights reserved.

Extreme Networks and the Extreme Networks logo are trademarks or registered trademarks of Extreme Networks, Inc. in the United States and/or other countries. All other names are the property of their respective owners. All other registered trademarks, trademarks, and service marks are property of their respective owners. For additional information on Extreme Networks trademarks, see www.extremenetworks.com/company/legal/trademarks.

## 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**.

Microsoft Azure		₽ Sea	rch resources, services, and docs (G+/)		
Home > Enterprise applications					
• Microsoft Entra ID	ions   All applic	C Refresh ⊻ Download (Ex	port)   <b>1</b> Preview info   ≡≡ Columns	🐱 Preview features 🔗	Got feedback?
Overview					
<ol> <li>Overview</li> </ol>	View, filter, and search a	applications in your organization	that are set up to use your Microsoft Entra tenan	t as their Identity Provider.	
X Diagnose and solve problems	The list of applications t	hat are maintained by your organ	ization are in application registrations.		
Manage	<u>م</u>	×	Application type == Enterprise Applications	Application ID starts with	× + Add filters
All applications	0 applications found				
Application proxy	Name	↑↓ Object ID	Application ID	Homepage URL	Created on
User settings	No results				
🖽 App launchers					
<ul> <li>Custom authentication extensions (Preview)</li> </ul>					
Security					
👇 Conditional Access					
Consent and permissions					
Activity					

Figure 2 Azure - Enterprise Applications page

Create your own application				
Create your own application				
e Microsoft Entra ID App Gallery is a catalog of thousand plication here. If you are wanting to publish an applicatio	s of apps that make it easy to deploy and n you have developed into the Microsoft	configure single sign-on (SSO) and automated user Entra ID Gallery for other organizations to discover	provisioning. When deploying an app from and use, you can file a request using the p	m the App Gallery, you leverage process described in this article.
Search application	ala Cian, on i All	Cotogories : All		
Surer appreation	gie sign-on . All Oser Account in	Categories : All		
oud platforms				
Amazon Web Services (AWS)	Google Cloud Platform	Oracle		SAP
214/5				
avv5				SAP
	Google Cloud			
	0			
n-premises applications				
Add an on-premises application	Learn about A	plication Proxy	On-premises application pro	ovisioning
			On-premises application provisioning Automate creating, updating, and deleting users in applications on-	

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.

Create your own application	×
ℜ Got feedback?	
If you are developing your own application, using Application Proxy, or want to integrate application that is not in the gallery, you can create your own application here.	an
What's the name of your app?	
XIQ-SSO 🗸	
What are you looking to do with your application?	
O Configure Application Proxy for secure remote access to an on-premises application	
O Register an application to integrate with Microsoft Entra ID (App you're developing)	
<ul> <li>Integrate any other application you don't find in the gallery (Non-gallery)</li> </ul>	

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.

- 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**.

Home > Enterprise applications   All applications > XIQ-SSO   Users and groups >	Users and groups	×
When you assign a group to an application, only users directly in the group will have access. The assignment     ×     does not cascade to rested groups.	Try changing or adding filters if you don't see what you're looking for.     Selected (9)     Reset	
Users and groups	Sealon ho XIQ XIQ-Installer	Û
9 groups selected.	All Users Groups XIQ-Monitor	<b>i</b>
Jener La Jone	Name Type Email XIQ-Operator           XiQ-Administrator         Group           XiQ-Administrator         Group	1
	Image: Second and the second and t	1
	Image: Second	Ē
	Image: State	
	Z 24 XIQ-Operator Group	Û
	202. XIQ-Administrator	Û
Assign	Select	

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

#### 5. Select Assign.

Home > Enterprise applications   All applications > Browse Azure AD Gallery > XIQ-SSO   Users and Add Assignment	groups >
When you assign a group to an application, only users directly in the group will have access. The assignment does not cascade to nested groups.	×
Users and groups 8 groups selected.	
Select a role User	
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.

Home > Enterprise applications   All a	Home > Enterprise applications   All applications > XIQ-SSO							
KIQ-SSO   Users ar	XIQ-SSO   Users and groups            Enterprise Application							
Add user/group    2 Edit assignment								
Deployment Plan	1 The application will appear for assigned users within My Apps. Set 'visible to users?' to no in properties to prevent this. →							
X Diagnose and solve problems	X Diagnose and solve problems							
Manage	Assign users and groups to app-roles for your application here. To ch	eate new app-roles for this application, use the application registration.						
Properties	First 200 shown, to search all users & gro							
A Owners	Display Name	Object Type	Role assigned					
🛃 Roles and administrators	XI XIQ-Administrator	Group	User					
Users and groups	XIQ-Application Operator	Group	User					
Single sign-on	XM XIQ-Guest Management	Group	User					
Provisioning	XD XIQ-Help Desk	Group	User					
Application proxy	XI XIQ-Installer	Group	User					
Self-service	XI XIQ-Monitor	Group	User					
Custom security attributes	XI XIQ-Observer	Group	User					
Security	XIQ-Operator	Group	User					
🍨 Conditional Access								
Permissions								

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.

XIQ-SSO-New   Sin     Enterprise Application	ngle sign-on and and a second s
Overview     Deployment Plan     X Diagnose and solve problems	Single sign-on (ISO) adds security and convenience when users sign on to applications in Azure Active Directory by enabling a user in your organization to sign in to every application they use with only one account. Once the user logs into an application, that credential is used for all the other applications they need access to. Learn more.
Manage	Select a single sign-on method Help me decide
	Disabled Single sign on is not enabled. The user wort the able to launch the app from My Apps.       SAML Rich and secure authentication to applications using the SAML (Security Assertion Markup Language) protocol.       Passmort absrage and replay using a web browser extension or mobile app.       Linked Link to an application in My Apps and/or Office 365 application launcher.
Security Conditional Access Conditional Access Permissions Token encryption	

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.

Basic SAML Configuration	
🗟 Save 🕅 Got feedback?	
Identifier (Entity ID) * 💿	
The unique ID that identifies your application to Microsoft Entra ID. This value must be unique across all applications in your Microsoft Entra tenant. The default identifier will be the audience of the SAML response for IDP-initiated SSO.	
Default	
https://temp_ID	Î
Add identifier	
The reply URL (Assertion Consumer Service ORL) ~ ()	
The reply URL (ASSENTION Consumer Service VRL) * () The reply URL is where the application expects to receive the authentication token. This is also referred to as the "Assertion Consumer Service" (ACS) in SAML Index Default	
The reply URL (ASSENDITIONISHING SERVICE OKL) * ① The reply URL is where the application expects to receive the authentication token. This is also referred to as the "Assertion Consumer Service" (ACS) in SAML Index Default https://temp_reply	
https://temp_reply Add reply URL	Î
Index       Default         https://temp_reply       Index       Default         Add reply URL       Index       Index	Î
Index       Default         https://temp_reply       Index       Default         Add reply URL       Index       Index         Sign on URL (Optional)       Consumer default       Index       Index	
Reply URL (ACS) in SAML         Index       Default         https://temp_reply       Index       Default         Add reply URL       Index       Index         Sign on URL (Optional)       Sign on URL is used if you would like to perform service provider-initiated single sign-on. This value is the sign-in page URL for your application. This field is unnecessary if you want to perform identity provider-initiated single sign-on.	ii.
Kepy ORC (Assertion Consumer Service ORC) *          The reply URL is where the application expects to receive the authentication token. This is also referred to as the "Assertion Consumer Service" (ACS) in SAML         Index       Default         https://temp_reply          Add reply URL          Sign on URL (Optional)          Sign on URL (Optional)          For your application. This field is unnecessary if you want to perform identity provider-initiated single sign-on.       This value is the sign-in page URL for your application. This field is unnecessary if you want to perform identity provider-initiated single sign-on.	

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)**.

	•••	ExtremeCloud IQ Pilot
	Ø	
	*	ACCOUNTS
	LD>	→ Account Details
	****×	ExtremeCloud IQ Classic Account
	~	Account Management
	<b>₩</b> >	Credential Distribution Groups
	₽>	Google Authenticator
A F =		ADMINISTRATION
		License Management
Global Settings		Device Management Settings
I Select: All About ExtremeCloud IQ		VIQ Management
DEVICES Communications		Enable Single Sign On (SSO)
Cloud Security Information		Email Notifications
ILOT Logout		API

2. Select Add Identity Provider.

G					
*	ACCOUNTS	Single Sign On (SSO)			
	Account Details				
	ExtremeCloud IQ Classic Account				Add Identity Provider
<i>**</i> *>	Account Management				
	Credential Distribution Groups	DOMAIN	DESCRIPTION	STATUS	
د≙	Google Authenticator				
	ADMINISTRATION				
	License Management		No Data Fou	ind	
	Device Management Settings				
	VIQ Management				
	→ Enable Single Sign On (SSO)				
14	Email Notifications				

Figure 13 ExtremeCloud IQ - Enable SSO.

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

← Add Identity Provider						
1 Туре	2 Profile		IDP Cont	nection		Attribute Mapping
RE	Ping		$\wedge$	G		
Generic SAML Server ADFS	Identity.5	Okta	Microsoft Entra ID	OneLogin	Auth0	

Figure 14 ExtremeCloud IQ - Select Identity Provider.

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

← Add Identity Provider			
💋 Туре	2 Profile	3 IDP Connection	4 Attribute Mapping
Domain* contoso.com			
Azure AD SSO Tenant			
			< Bacl Continue >

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.

🖉 Туре	🖉 Profile	3 IDP Connection	4 Attribute Mappi
Provide IDP Metadata 🔵 Impor	rt Metadata 💿 Import From URL 🔵 Manua	lly Enter	
			Import
IDP Metadata URL			Import

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.

0	↑ Upload metadata file  ♦ Change	je single sign-on mode 🛛 🗮 Test this application 👘 🖗 Got feedbar	ck?
Overview     Deployment Plan     Diagnose and solve problems	surname email Unique User Identifier Group	user.sumame user.userprincipalname user.groups	
Manage			
Properties	SAML Certificates		
A Owners	Token signing certificate		/ Edit
8 Roles and administrators	Status	Active	5 CON
A Liters and groups	Expiration	9/18/2026, 1:31:08 PM	to state and
	Notification Email	admin@adomain.com	to cipodard
Single sign-on	App Federation Metadata Un	https://login.microsoftonline.com/84e68c7 -94ca	
Provisioning	Certificate (Baseo4) Certificate (Raw)	Download	
Application proxy	Federation Metadata XML	Download	
G Self-service			
Custom security attributes	Verification certificates (opt Required	onal) No	0 Edit
	Active	0	

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.

← Add Identity P	rovider		
🖉 Туре	Profile	3 IDP Connection	4 Attribute Mapping
Provide IDP Metadata Imp IDP Metadata URL 84e68c77-94ca-4f3c-83e	ort Metadata      Import From URL Manually c-5a3cd6b333a1/federationmetadata/2007-06	Enter 5/federationmetadata.xml?appid=05f2d09a-2e96-4f5	d-a583-cb49a03eee97
			< Back

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.

Profile	IDP Connection	Attribute Mapping	ExtremeCloud (SP) Connection
Import From URL			
https://login.microsoftonline.com/84e68c77-	-5a3cd6b333a1/federationmetadata	a/2007-06/federationmetadata.xml?appid=416b8	a91-6b9a-4e49-97ac-31ec60d7ff45
IDP Entity ID*			
https://sts.windows.net/84e68c77-	-5a3cd6b333a1/		
Please enter the URL beginning with https			
SSO Binding			
HTTP POST  HTTP Redirect			
C SSO URL*			
https://login.microsoftonline.com/84e68	-5a3cd6b333a1/san	112	
Please enter the URL beginning with https			
SSO Sign Request			
SLO Binding			
HTTP POST  HTTP Redirect			
C SLO URL*			
https://login.microsoftonline.com/84e68	-5a3cd6b333a1/san	n12	
Please enter the URL beginning with https			
SLO Response URL*			
https://login.microsoftonline.com/84e68	-5a3cd6b333a1/san	nl2	
Please enter the URL beginning with https			
Verification Certificate			
Microsoft Azura Endersted SSO Cartificate			
		— ×	
vano date: 2023-08-28 - 2026-08-28			
Choose Certificates*			
wicrosoft Azure rederated SSO Certificat	e	•	
Import a new Certificate			

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.

← Add Identi	ty Provider		
🕗 Туре	Profile	IDP Connection	4 Attribute Mapping
User Profile Attribute		SAML Attribute	
First Name			
Last Name			
Email			
Group			
	+ Add a group name mapping		
	When no group mapping, ExtremeCloud will      deny user     allow user	r login r login and assign a default user group:	
			< Back Save & Finish

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

© 2024 Extreme Networks, Inc. All rights reserved.

## 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.

Home > Enterprise applications   All applications > XIQ-SSO				
XIQ-SSO   Users and groups				
3 Overview	+ Add user/group   2/ Edit assignment 1 Remove 2/ Update credentials   III Columns   2/ Got feedback?			
<ul> <li>Deployment Plan</li> <li>Diagnose and solve problems</li> </ul>	Assign users and groups to ano-roles for your annihilation here. To c	visue to users: to no in properties to prevent units.		
Manage	First 200 shown, to search all users & gro	reate new apprivation registration.		
Properties Owners	Display Name	Object Type	Role assigned	
and administrators	XI XIQ-Administrator	Group	User	
Users and groups	XIQ-Application Operator	Group	User	
Single sign-on	XM XIQ-Guest Management	Group	User	
Provisioning	XIQ-Help Desk	Group	User	
Application proxy	XI XIQ-Installer	Group	User	
Self-service	XI XIQ-Monitor	Group	User	
Custom security attributes	XI XIQ-Observer	Group	User	
Security	XI XIQ-Operator	Group	User	
Conditional Access				
Permissions				

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.

IDP group →	Select an ExtremeCloudIQ group
+ Add a group name mapping	Select an ExtremeCloudIQ group
When no group mapping, ExtremeCloud will 💿 deny user login	Administrator
allow user login and assign a def	Application Operator
http://schemas.xmlsoap.org/ws/2005/05/identity/claims/xxx.givennar	Guest Management
	Help Desk
http://schemas.xmlsoap.org/ws/2005/05/identity/claims/surname	Installer

Figure 22 ExtremeCloud IQ - Group name mapping.

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

**i** ::

		Accordate mapping	extremectoda (SF) connection
lser Profile Attribute		SAML Attribute	
First Name	http://schemas.xmlsoap.org/ws/2005/05/identity/claim	s/givenname	
Last Name	http://schemas.xmlsoap.org/ws/2005/05/identity/claim	s/surname	
Email	http://schemas.xmlsoap.org/ws/2005/05/identity/claim	s/email	
Group	http://schemas.microsoft.com/ws/2008/06/identity/cla	ms/groups	
	XIQ-Admin	→ Administrator	* 1
	XIQ-Operator	Application Operator	* = =
	XIQ-Monitor	→ Monitor	* • •
	+ Add a group name mapping		
	When no group mapping, ExtremeCloud will 💿 deny user login		
	allow user login	and assign a default user group:	

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.

Single Sign On (SSO)				
				Add Identity Provider
DOMAIN	DESCRIPTION	STATUS		
Image: A start of the start		-	<b>e</b>	

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.

Profile	IDP Connection	Attribute Mapping	ExtremeCloud (SP) Connection
Download SP Metadata SP Entity ID			
https://g2.sso.xcloudiq.com/saml2/service-provider-metadata/	0		
ACS Binding			
ACS URL			
https://g2.sso.xcloudiq.com/login/saml2/sso/	Ō		
SLO Binding			
HTTP Redirect			
SLO URL			
https://g2.sso.xcloudiq.com/logout/saml2/slo			
SLO Response URL			
https://g2.sso.xcloudiq.com/logout/saml2/slo			
Signing Certificate			
Download Certificate			

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

3. Download and keep the .XML file.

Down	loads	0	Q
ex ex	tremecloud-metadata.xml		
OF	en 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.

Home >   Enterprise applica	ations > Enterprise applications   All applications > XIQ-SSO >
XIQ-SSO   SAML-base	d Sign-on
Enterprise Application	
<pre></pre>	ក Upload metadata file 🏷 Change single sign-on mode 📁 Test this application 🛛 🖗 Got feedback?
III Overview	
Deployment Plan	Upload metadata file.
🗙 Diagnose and solve problems	Values for the fields below are provided by XIQ-SSO. You may either enter those values manually, or upload a pre- configured SAML metadata file if provided by XIQ-SSO.
Manage	Select a file
Properties	Add Cancel
🚨 Owners	
	Basic SAME Confiduration

Figure 27 Azure - Upload Metadata XML file.

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

Home > Enterprise applications   All	applications > Browse Azure AD Gallery > XIQ-SSO	Basic SAML Configuration
XIQ-SSO   SAML-base	ad Sign-on	E sun Ø der fandhards
Overview     Deployment Plan     Clagnose and solve problems     Manage     Properties     Owners	<sup>4</sup> Tupload metadata lie <sup>1</sup> Charge single sign-on mode IIII that this application   <i>R</i> Got Reaback Set up Single Sign-On with SAML A SSD implementation based on federation protocols improves security, reliability, and end user experiences an implement. Choose SAML single sign-on whenever possible for existing applications that do not use OpenID Common. Read the configuration guide of for help integrating XQ SSD.	
Roles and administrators     Users and groups     Single sign-on     Provisioning     Application provy	Basic SAML Configuration     Identifier (Entity 0)     Regularied     Sign on URI,     Sign on URI,     Sign on URI,     Copional     Deployable     Copional     Logosit UM (Optional)     Optional	Ø       Edit       Reply URL (Assertion Consumer Service URL) * ○         The reply URL is where the application opects to receive the authentication toteler. This is also referred to as the "Assertion Consumer Service" (ACD in SAML       Index       Default         Interprivation Consumer Service" (ACD in SAML       Index       Default       Index       Default
Self-service     Custom security attributes     Security     Conditional Access     Permissions     Token encyption	Attributes & Claims     Attributes & Claims     Affit out required fields in Step 1     giverrame     summe     user givername     emailed/dets     user mail     name     user suprincipalmame     Unique User Identifier     user useprincipalmame	Add reply URL Sign on URL (Optional) Sign on URL (Optional) Sign on URL is used if you would like to perform service provider-indicated single sign-on. This value is the sign-in page URL for your application. This field is unnecessor (fyour work to perform identity provider-indicated single sign-on. Enter as sign on URL
Activity کانوب المحمد المحم المحمد المحمد المحم المحمد المحمد المحم المحمد المحمد	SANL Certificates     Status signing certificate     Status     Tumutorint     Explandin     Active     Constraint of the status     Active     Active     Constraint of the status	Relay State (Optional)     Relay State (optional)     The Relay State (optional)     The Relay State (optional)     The Relay State (optional)

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.

* 1	Upload metadata file 🏷 Change single sign-on	mode 🗐	Test this application R <sup>J</sup> Got feedback?	
Te	st single sign-on with XIO-SSO			
Deployment Plan	ensure that single sign-on works for your applica	tion we reco	mmend using the testing canability (in the	last sten)
K Diagnose and solve problems to	test the changes you recently made. Would you li	ike to test no	w?	last step)
Manage	Nee Ill text litter			
	Tes No, Th test liker			
Properties Re	ad the configuration guide c? for help integrating XI	Q-SSO.		
Mowners 1				
Roles and administrators	Basic SAML Configuration			🖉 Edit
Users and groups	Identifier (Entity ID)	https://	.xcloudiq.com/saml2/service-provider-meta	
Single sign-on	Reply URL (Assertion Consumer Service URL)	https:/.	.xcloudiq.com/login/saml2/sso/e	
Provisioning	Sign on URL	Optional		
Application provy	Relay State (Optional)	Optional		
<ul> <li>Application ploxy</li> </ul>	Logout Url (Optional)	https:/,	ccloudiq.com/logout/saml2/slo	
Self-service				
Custom security attributes	Attributes & Claims			A
Security				6 Edit
	givenname	user.givenn	ame	
Conditional Accord	email	user.userpri	incipalname	
Conditional Access				
Conditional Access	surname email	user.suman user.userpri	ne incipalname	

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.

Attributes & Claims		🖉 Edit
surname	user.surname	
givenname	user.givenname	
email	user.userprincipalname	
Unique User Identifier	user.mail	
Group	user.groups	

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.

1

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

	Sign In With SSO	
Er	nter your company Email address	10
	Continue	
	I don't have SSO account	

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.

-	Extren	neClou	d IQ Pilo	:										a 📫 🛃	0	IE.	
Ø	C CONNECTION STATUS 5 Online / 9 Offline			C CONNECTION STATUS C TOTAL APPS 0					CLIENTS 19					USERS 0			
*	T.	Defa	ult View											Showing 0 o	f 0   <b>0</b> Selected   Selec	t: All Pages, Nor	e
<b>L0</b> >		+	± / #						Enter Host Na	me, MAC Addr, Se	rial #, or MGT IP A:	ddr Q				<b>m</b> C	
**		<b></b> 5	TATUS	HOST NAME	NETWORK     POLICY	MANAGED BY	UPTIME	MGT IP AD	DRESS DEFAULT GATEWAY	CLIENTS	MAC	LOCATION	SERIAL #	FEATURE LICENSE	DEVICE LICENSE	MODEL	
														No records found.			
٥												_					
, <b>å</b> ,																	
2																	
>		_															
		_										_		_			

Figure 35 ExtremeCloud IQ Default View.

#### The ExtremeCloud IQ Audit Logs include the login action.

Audit Logs					
< 🛗 Sep 12, 2023 -	Sep 13, 2023 >				
Category All	✓ Admin User All	▼ Description	n		
					<u>+</u>
ORGANIZATION	TIMESTAMP ↓	CATEGORY	ADMIN USER	DESCRIPTION	
Your Organization	2023-09-13 19:06:17	ADMIN	geon mason@lan execta.onmicrosoft.com	Logged in with privileges of admin group Administrator	

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.

Set up XIQ-SSO										
You'll need to configure the application	ation to link with Azure AD.									
Login URL https://login.microsoftonline.com/84e68c77-94ca										
Azure AD Identifier	https://sts.windows.net/84e68c77-94ca-4f3c-83ec									
Logout URL	https://login.microsoftonline.com/84e68c77-94ca									
Test single sign-on with XIQ-SSC Test to see if single sign-on is work	) ing. Users will need to be added to Users and groups before they can sign in.									

Figure 37 Azure - Test XIQ-SSO application.

Test single sign-on with XIQ-SSO	×
₽ Got feedback?	
▲ Microsoft recommends installing the My Apps Secure Sign-in Extension for automatic error capture and resolution guidance. Make sure you allow third-party cookies if you have installed it but this message still shows up. Click here to get the extension →	
Testing sign in	
Test the single sign-on configuration for XIQ-SSO by signing in here. Ensure that you have configured both the Microsoft Entra ID configuration and XIQ-SSO itself.	
To test as your current user, select "Test sign in" below.	
To test as another user, open this experience in a new tab in your browser. In that new tab, sign into the current portal with the user you' like to test sign in as. Then, in that new tab, select "Test sign in" to test as that other user. Read the testing guide for more information.	d
Test sign in	
Resolving errors	
If you encounter an error in the sign-in page, please paste it below. If you still see the same issue, please wait for couple of minutes and retry.	
What does the error look like? 🖻	
Request Id: 4f8ec053-fb71-47de-a010-2786a32f1900 Correlation Id: 5aa879f5-68f1-482a-a405-ff993d8f4cb0 Timestamp: 2018-03-06T23:54:10Z Message: Error AADSTSXXXX:	
Get resolution guidance	

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.

	Extrem	eCl	oud IG	Pilot											م 📌 🛃	θ.	E	Ш
O.	CONNECTION STATUS 5 Online / 9 Offline			NECTION STATUS C TOTAL APPS 0						CLIENTS 19					USERS 0			
*	Τ.	Þ	efault Vie	w											Showing 0	of 0   <b>0</b> Selected   Sele	ct: All Pages, Nor	1e
ED>		- 1	± ,	/ 1						Enter Host Nam	ie, MAC Addr, Ser	ial #, or MGT IP Ad	dr Q					
2422			STATUS		HOST NAME	NETWORK     POLICY	MANAGED BY	UPTIME	MGT IP AL	DEFAULT GATEWAY	CLIENTS	MAC	LOCATION	SERIAL #	FEATURE LICENSE	DEVICE LICENSE	MODEL	
															No records found.			
∂>																		
0																		
>																		0

Figure 40 ExtremeCloud IQ Default View.

## The ExtremeCloud IQ Audit Logs include the login action.

Audit Logs					
< i Sep 12, 2023	- Sep 13, 2023 >				
Category All	← Admin User All	✓ Description	1		
					<u>*</u>
ORGANIZATION	TIMESTAMP 🦆	CATEGORY	ADMIN USER	DESCRIPTION	
Your Organization	2023-09-13 19:06:17	ADMIN	geon.mason@lanex.co.onmicrosoft.com	Logged in with privileges of admin group Administrator	

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:

Admin Accounts					
+ 🖍 🔋 Test User SEARCH					
User Name	Email Address	Role			
Test User SSO	test.user@	Monitor			

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.