



# ExtremeCloud IQ v24.6.0 SSO Integration Guide

Configuring Self-Service SAML SSO with Microsoft  
Entra ID and Okta

9038990-00 Rev AB  
October 2024



Copyright © 2024 Extreme Networks, Inc. All rights reserved.

## Legal Notice

Extreme Networks, Inc. reserves the right to make changes in specifications and other information contained in this document and its website without prior notice. The reader should in all cases consult representatives of Extreme Networks to determine whether any such changes have been made.

The hardware, firmware, software or any specifications described or referred to in this document are subject to change without notice.

## Trademarks

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 (including any product names) mentioned in this document are the property of their respective owners and may be trademarks or registered trademarks of their respective companies/owners.

For additional information on Extreme Networks trademarks, see: <https://www.extremenetworks.com/about-extreme-networks/company/legal/trademarks>

## Open Source Declarations

Some software files have been licensed under certain open source or third-party licenses.

End-user license agreements and open source declarations can be found at: <https://www.extremenetworks.com/support/policies/open-source-declaration/>



# Table of Contents

---

Abstract.....	iv
<b>Preface.....</b>	<b>5</b>
Text Conventions.....	5
Documentation and Training.....	6
Open Source Declarations.....	7
Training.....	7
Help and Support.....	7
Subscribe to Product Announcements.....	8
Send Feedback.....	8
<b>Integration Overview.....</b>	<b>9</b>
<b>Integration with Microsoft Entra ID.....</b>	<b>10</b>
Step 1 — Create a New Enterprise Application in Entra ID .....	10
Step 2 — Assign Users and Groups in Entra ID.....	10
Step 3 — Select SAML as the Single Sign-On Method in Entra ID.....	11
Step 4 — Import Entra ID Metadata to ExtremeCloud IQ.....	12
Step 5 — Map ExtremeCloud IQ User Profile Attributes to SAML Attributes for Entra ID.....	13
Step 6 — Map ExtremeCloud IQ Group to Roles for Entra ID.....	13
Step 7 — Export SP Metadata and Import into Entra ID.....	14
Step 8 — Map Entra ID Security Groups to ExtremeCloud IQ Roles.....	15
Step 9 — Entra ID Test - SP Initiated.....	16
Step 10 — Entra ID Test - IdP Initiated.....	16
<b>Integration with Okta.....</b>	<b>17</b>
Step 1 — Navigate to the Okta Admin Portal.....	17
Step 2 — Create a New SAML Application and Define User Group Mappings in Okta.....	18
Step 3 — Assign Users and Groups in Okta.....	18
Step 4 — Create New Password Authentication Policy in Okta.....	19
Step 5 — Export Metadata for your Okta SAML Application.....	20
Step 6 — For Okta: Create IdP Profile, Import Metadata, and Edit Settings in ExtremeCloud IQ.....	20
Step 7 — Modify Okta SAML Application Metadata with ExtremeCloud IQ Settings.....	22
Step 8 — Okta Test - SP Initiated.....	24
Step 9 — Okta Test - IdP Initiated.....	25
<b>Notes and Caveats.....</b>	<b>26</b>



## Abstract

---

This Integration Guide for ExtremeCloud IQ version 24.6.0 provides in-depth technical instructions for configuring Self-Service SAML Single Sign-On (SSO) within the platform. Designed for system administrators, it covers integration with external Identity Providers (IdPs) such as Microsoft Entra ID (formerly Azure Active Directory) and Okta. Topics include the creation of enterprise applications, detailed user and group assignments, and advanced user attribute mapping for role-based access. Key steps involve exporting and importing Service Provider (SP) metadata, configuring SAML attributes, and conducting SP- and IdP-initiated login tests. Advanced sections focus on security group-to-role mapping and certificate management, along with future considerations for enhancing security through improved certificate handling. Technical details emphasize secure, scalable authentication workflows, complemented by troubleshooting guidance for seamless SSO integration with external IdP systems.



# Preface

---

Read the following topics to learn about:

- The meanings of text formats used in this document.
- Where you can find additional information and help.
- How to reach us with questions and comments.






## Text Conventions

---

Unless otherwise noted, information in this document applies to all supported environments for the products in question. Exceptions, like command keywords associated with a specific software version, are identified in the text.

When a feature, function, or operation pertains to a specific hardware product, the product name is used. When features, functions, and operations are the same across an entire product family, such as Extreme Networks switches or SLX routers, the product is referred to as *the switch* or *the router*.

**Table 1: Notes and warnings**

Icon	Notice type	Alerts you to...
	Tip	Helpful tips and notices for using the product
	Note	Useful information or instructions
	Important	Important features or instructions
	Caution	Risk of personal injury, system damage, or loss of data
	Warning	Risk of severe personal injury

**Table 2: Text**

Convention	Description
screen displays	This typeface indicates command syntax, or represents information as it is displayed on the screen.
The words <i>enter</i> and <i>type</i>	When you see the word <i>enter</i> in this guide, you must type something, and then press the Return or Enter key. Do not press the Return or Enter key when an instruction simply says <i>type</i> .
Key names	Key names are written in boldface, for example <b>Ctrl</b> or <b>Esc</b> . If you must press two or more keys simultaneously, the key names are linked with a plus sign (+). Example: Press <b>Ctrl+Alt+Del</b>
Words in italicized type	Italics emphasize a point or denote new terms at the place where they are defined in the text. Italics are also used when referring to publication titles.
<b>NEW!</b>	New information. In a PDF, this is searchable text.

**Table 3: Command syntax**

Convention	Description
<b>bold text</b>	Bold text indicates command names, keywords, and command options.
<i>italic text</i>	Italic text indicates variable content.
[ ]	Syntax components displayed within square brackets are optional. Default responses to system prompts are enclosed in square brackets.
{ <b>x</b>   <b>y</b>   <b>z</b> }	A choice of required parameters is enclosed in curly brackets separated by vertical bars. You must select one of the options.
<b>x</b>   <b>y</b>	A vertical bar separates mutually exclusive elements.
< >	Nonprinting characters, such as passwords, are enclosed in angle brackets.
...	Repeat the previous element, for example, <i>member [member...]</i> .
\	In command examples, the backslash indicates a “soft” line break. When a backslash separates two lines of a command input, enter the entire command at the prompt without the backslash.

## Documentation and Training

Find Extreme Networks product information at the following locations:

[Current Product Documentation](#)

[Release Notes](#)

[Hardware and Software Compatibility](#) for Extreme Networks products

[Extreme Optics Compatibility](#)

[Other Resources](#) such as articles, white papers, and case studies

## Open Source Declarations

Some software files have been licensed under certain open source licenses. Information is available on the [Open Source Declaration](#) page.

## Training

Extreme Networks offers product training courses, both online and in person, as well as specialized certifications. For details, visit the [Extreme Networks Training](#) page.

## Help and Support

---

If you require assistance, contact Extreme Networks using one of the following methods:

### Extreme Portal

Search the GTAC (Global Technical Assistance Center) knowledge base; manage support cases and service contracts; download software; and obtain product licensing, training, and certifications.

### The Hub

A forum for Extreme Networks customers to connect with one another, answer questions, and share ideas and feedback. This community is monitored by Extreme Networks employees, but is not intended to replace specific guidance from GTAC.

### Call GTAC

For immediate support: (800) 998 2408 (toll-free in U.S. and Canada) or 1 (408) 579 2800. For the support phone number in your country, visit [www.extremenetworks.com/support/contact](http://www.extremenetworks.com/support/contact).

Before contacting Extreme Networks for technical support, have the following information ready:

- Your Extreme Networks service contract number, or serial numbers for all involved Extreme Networks products
- A description of the failure
- A description of any actions already taken to resolve the problem
- A description of your network environment (such as layout, cable type, other relevant environmental information)
- Network load at the time of trouble (if known)
- The device history (for example, if you have returned the device before, or if this is a recurring problem)
- Any related RMA (Return Material Authorization) numbers

## Subscribe to Product Announcements

You can subscribe to email notifications for product and software release announcements, Field Notices, and Vulnerability Notices.

1. Go to [The Hub](#).
2. In the list of categories, expand the **Product Announcements** list.
3. Select a product for which you would like to receive notifications.
4. Select **Subscribe**.
5. To select additional products, return to the **Product Announcements** list and repeat steps 3 and 4.

You can modify your product selections or unsubscribe at any time.

## Send Feedback

---

The User Enablement team at Extreme Networks has made every effort to ensure that this document is accurate, complete, and easy to use. We strive to improve our documentation to help you in your work, so we want to hear from you. We welcome all feedback, but we especially want to know about:

- Content errors, or confusing or conflicting information.
- Improvements that would help you find relevant information.
- Broken links or usability issues.

To send feedback, email us at [documentation@extremenetworks.com](mailto:documentation@extremenetworks.com).

Provide as much detail as possible including the publication title, topic heading, and page number (if applicable), along with your comments and suggestions for improvement.





# Integration Overview

---

This guide details the process for integrating Self-Service Single Sign-On (SSO) within ExtremeCloud IQ, allowing administrators to log in using credentials from select Identify Providers, such as Microsoft Entra ID (formerly Azure Active Directory) and Okta.

This guide provides comprehensive steps including: creating enterprise applications in the IdP, assigning users and groups, importing IdP metadata, mapping groups to roles in ExtremeCloud IQ, exporting and importing Service Provider (SP) metadata, and conducting both SP- and IdP-initiated tests. The guide also includes notes on administrative roles, account creation, location assignments, and planned future features for managing SSO configurations and certificates. This integration framework supports a seamless authentication process, enhancing security and user management in ExtremeCloud IQ.

## Related Topics

[Integration with Microsoft Entra ID](#) on page 10

[Integration with Okta](#) on page 17



# Integration with Microsoft Entra ID

---

- [Step 1 — Create a New Enterprise Application in Entra ID](#) on page 10
- [Step 2 — Assign Users and Groups in Entra ID](#) on page 10
- [Step 3 — Select SAML as the Single Sign-On Method in Entra ID](#) on page 11
- [Step 4 — Import Entra ID Metadata to ExtremeCloud IQ](#) on page 12
- [Step 5 — Map ExtremeCloud IQ User Profile Attributes to SAML Attributes for Entra ID](#) on page 13
- [Step 6 — Map ExtremeCloud IQ Group to Roles for Entra ID](#) on page 13
- [Step 7 — Export SP Metadata and Import into Entra ID](#) on page 14
- [Step 8 — Map Entra ID Security Groups to ExtremeCloud IQ Roles](#) on page 15
- [Step 9 — Entra ID Test - SP Initiated](#) on page 16
- [Step 10 — Entra ID Test - IdP Initiated](#) on page 16

## Step 1 — Create a New Enterprise Application in Entra ID

---

1. From the Azure Portal, under **Azure services**, select **Enterprise applications**.
2. From the Enterprise Applications, select **New application** > **Create your own application**.  
The **Create your own application** dialog displays.
3. Provide the application name, select **Integrate any other application you don't find in the gallery (Non-Gallery)**, and then select **Create**.  
The application **Overview** page opens.

### Related Topics

- [Step 2 — Assign Users and Groups in Entra ID](#) on page 10

## Step 2 — Assign Users and Groups in Entra ID

---



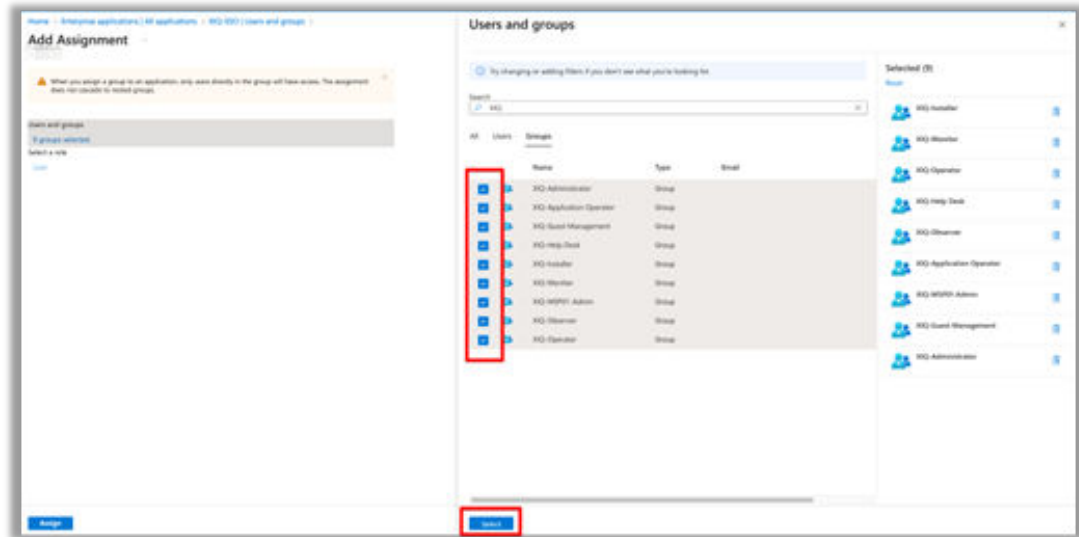
### Important

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

Add the group objects to map to the Role Based Access Controls in ExtremeCloud IQ.

1. From the application **Overview** page, select **Assign Users and Groups**, and then select **Add user/group**.  
The **Add Assignment** page opens.

2. From the left pane, select the link under **Users and groups**. Azure displays ExtremeCloud IQ required user group.
3. Select the check box for each ExtremeCloud IQ required user group, and then click **Select**.



**Figure 1: Azure - Assigning ExtremeCloud IQ User Groups to an Azure User Role**

4. Select **Assign**. 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.

#### Related Topics

[Step 3 — Select SAML as the Single Sign-On Method in Entra ID](#) on page 11

## Step 3 — Select SAML as the Single Sign-On Method in Entra ID

Use this task to select the SAML protocol method for Single Sign-On.

1. From the application **Overview** page, navigate to **Manage > Single sign-on**, and then select **Get Started**.
2. Select the **SAML** single sign-on method.
3. On the **Set Up Single Sign-On with SAML** page, from the **Basic SAML Configuration** section, select **Edit**.
4. For **Identifier (Entity ID)**, select **Add identifier** and provide a temporary URL.  
For example: `https://temp_ID`
5. For **Reply URL (Assertion Consumer Service URL)**, select **Add reply URL** and add a temporary reply URL.  
For example: `https://temp_reply`

6. Select **Save**.

#### Related Topics

[Step 4 — Import Entra ID Metadata to ExtremeCloud IQ](#) on page 12

## Step 4 — Import Entra ID Metadata 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.extremecloudiq.com/login?sso=true>.



### Note

Single Sign-on integration can only be configured by ExtremeCloud IQ users with Administrator permissions in their home account (VIQ). External administrators cannot access the SSO configuration page when administering other customer accounts.

1. From ExtremeCloud IQ, go to **Global Settings > Enable Single Sign On (SSO)**.
2. Select **Add Identity Provider**.
3. Select **Microsoft Entra ID (Azure AD)**.
4. Enter the Fully Qualified **Domain** name of the Azure Tenant and optional **Description**.



### Note

You can only define a single domain name per IdP Profile. If your IdP supports multiple domains, you must create a separate IdP Profile for each domain.

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



### Note

Select **Import From URL** to import the data from the App Federation Metadata URL.

7. From the Azure Enterprise Application, scroll down to Section 3: SAML Certificates, and select the **App Federation Metadata Url** copy to clipboard icon.

App Federation Metadata Url

<https://login.microsoftonline.com/4...>



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

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

9. Select **Continue**.

#### Related Topics

[Step 5 — Map ExtremeCloud IQ User Profile Attributes to SAML Attributes for Entra ID](#) on page 13

## Step 5 — Map ExtremeCloud IQ User Profile Attributes to SAML Attributes for Entra ID

In ExtremeCloud IQ, from the **Attribute Mapping** tab, 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.

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

**Table 4: ExtremeCloud ID - 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

### Related Topics

[Step 6 — Map ExtremeCloud IQ Group to Roles for Entra ID](#) on page 13

## Step 6 — Map ExtremeCloud IQ Group to Roles for Entra ID

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

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** ...

Enterprise Application

Overview  
Deployment Plan  
Diagnose and solve problems

Manage

Properties  
Owners  
Roles and administrators  
**Users and groups**  
Single sign-on  
Provisioning  
Application proxy  
Self-service  
Custom security attributes

Security

Conditional Access  
Permissions

+ Add user/group | Edit assignment | Remove | Update credentials | Columns | Got feedback?

The application will appear for assigned users within My Apps. Set 'visible to users?' to no in properties to prevent this. →

Assign users and groups to app-roles for your application here. To create new app-roles for this application, use the [application registration](#).

First 200 shown, to search all users & gro...

Display Name	Object Type	Role assigned
<input type="checkbox"/> XI XIQ-Administrator	Group	User
<input type="checkbox"/> XO XIQ-Application Operator	Group	User
<input type="checkbox"/> XM XIQ-Guest Management	Group	User
<input type="checkbox"/> XD XIQ-Help Desk	Group	User
<input type="checkbox"/> XI XIQ-Installer	Group	User
<input type="checkbox"/> XI XIQ-Monitor	Group	User
<input type="checkbox"/> XI XIQ-Observer	Group	User
<input type="checkbox"/> XI XIQ-Operator	Group	User

**Figure 2: 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), and then select **Operator** from the **Select an ExtremeCloud IQ group** list.
5. Build and order the rules based on First Match.

To reorder the rules, select the  icon.



#### 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.

#### Related Topics

[Step 7 — Export SP Metadata and Import into Entra ID](#) on page 14

## Step 7 — 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. In ExtremeCloud IQ, go to the main **Single Sign On** page, and then select  to edit the saved IdP configuration.
2. Select the **ExtremeCloud (SP) Connection** tab, and then select **Download SP Metadata**.

Download and keep the .xml file.

3. In the Entra ID (XIQ-SSO) Enterprise Application **SAML-based Sign-on** page, select **Upload metadata file**, navigate to the saved exported file from ExtremeCloud IQ, and then select **Add**.
4. Confirm that the imported data is correct, and then select **Save**.

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**.

#### Related Topics

[Step 8 — Map Entra ID Security Groups to ExtremeCloud IQ Roles](#) on page 15

## Step 8 — 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.

1. In Section 2: **Attributes & Claims**, select **Edit**.
2. 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

\* You must manually add to the Default Attributes and Claims created by Entra ID.

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`
3. To add a group claim, from the Attributes and Claims page, select **Add a group claim**.
  4. Select **Groups assigned to the application**.
  5. From the **Source attribute** list, select **Cloud-only group display names**.

Related Topics

[Step 9 — Entra ID Test - SP Initiated](#) on page 16

## Step 9 — Entra ID Test - SP Initiated

Use this task to log in to ExtremeCloud IQ through SP initiated.

1. Browse to the **GDC Login** page <https://sso.extremecloudiq.com/login?sso=true?sso=true>, and then select the **SSO** icon.
2. Enter the email address of the IdP account and complete the IdP login process.  
The browser is redirected to the Microsoft Login Portal. After a successful sign in, the browser redirects to the 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

ORGANIZATION	TIMESTAMP ↓	CATEGORY	ADMIN USER	DESCRIPTION
Your Organization	2023-09-13 19:06:17	ADMIN	[redacted]@[redacted].onmicrosoft.com	Logged in with privileges of admin group Administrator

**Figure 3: ExtremeCloud IQ Audit Logs**

Related Topics

[Step 10 — Entra ID Test - IdP Initiated](#) on page 16

## Step 10 — Entra ID Test - IdP Initiated

After the integration is complete, test the application.

Use this task to start an IdP initiated test.

1. Go to the Azure main Single Sign On page for the XIQ-SSO application.
2. Scroll down to the **Test single sign-on with XIQ-SSO** section, and then select **Test**.
3. Select **Test sign in**, and then sign in to the Microsoft Login Portal.

After a successful login, you are redirected to the 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

ORGANIZATION	TIMESTAMP ↓	CATEGORY	ADMIN USER	DESCRIPTION
Your Organization	2023-09-13 19:06:17	ADMIN	[redacted]@[redacted].onmicrosoft.com	Logged in with privileges of admin group Administrator

**Figure 4: ExtremeCloud IQ Audit Logs**





# Integration with Okta

[Step 1 — Navigate to the Okta Admin Portal on page 17](#)

[Step 2 — Create a New SAML Application and Define User Group Mappings in Okta on page 18](#)

[Step 3 — Assign Users and Groups in Okta on page 18](#)

[Step 4 — Create New Password Authentication Policy in Okta on page 19](#)

[Step 5 — Export Metadata for your Okta SAML Application on page 20](#)

[Step 6 — For Okta: Create IdP Profile, Import Metadata, and Edit Settings in ExtremeCloud IQ on page 20](#)

[Step 7 — Modify Okta SAML Application Metadata with ExtremeCloud IQ Settings on page 22](#)

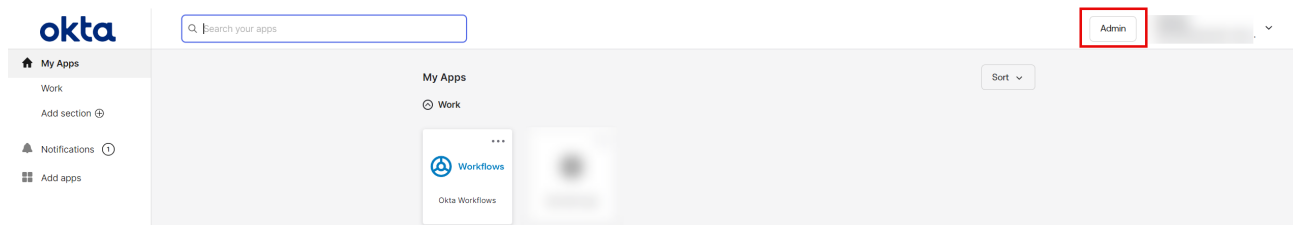
[Step 8 — Okta Test - SP Initiated on page 24](#)

[Step 9 — Okta Test - IdP Initiated on page 25](#)

## Step 1 — Navigate to the Okta Admin Portal

Use this task to navigate to the Admin Portal (Okta).

1. Browse to <https://login.okta.com>, and then log in to your Okta Organization with an account with the necessary Administrator permissions to create user, groups, SAML applications, and Authentication Policies.
2. From the Okta Dashboard page, select **Admin**.



**Figure 5: Okta - Dashboard and Link to the Admin Portal**

### Related Topics

[Step 2 — Create a New SAML Application and Define User Group Mappings in Okta on page 18](#)

## Step 2 — Create a New SAML Application and Define User Group Mappings in Okta

---



### Note

You must create the user groups in the IdP before you can map the user roles in ExtremeCloud IQ.

1. From Okta, navigate to **Applications > Applications**, and then select **Create App Integration**.
2. Select **SAML 2.0**, and then select **Next**.
3. Enter an **App name**, and then select **Next**.
4. In the **SAML Settings** section, enter temporary URLs as a placeholder that will be updated later for the following fields:
  - **Single sign-on URL**: `https://replaceme`
  - **Audience URI (SP Entity ID)**: `https://replaceme`
5. Scroll down to the **Attribute Statements** section.
6. Set **Name** to `user.email` and the corresponding **Value** to `user.email`, and then select **Add Another**.
7. Set **Name** to `user.firstName` and the corresponding **Value** to `user.firstName`, and then select **Add Another**.
8. Set **Name** to `user.lastname` and the corresponding **Value** to `user.lastname`.
9. Scroll down to the **Group Attributes** section:
  - a. Set **Name** to `user.group`.
  - b. Set the corresponding **Filter** to `Matches regex`, and then set the **Value** to `.*` (a period followed by an asterisk).
10. Select **Next**.
11. On the **Help Okta Support understand how you configured this application** page, set **App Type**, and then select **This is an internal app that we have created**.
12. Select **Finish**.

### Related Topics

[Step 3 — Assign Users and Groups in Okta](#) on page 18

## Step 3 — Assign Users and Groups in Okta

---

Your new application is now created, and we will assign users and groups to be able to use the application.

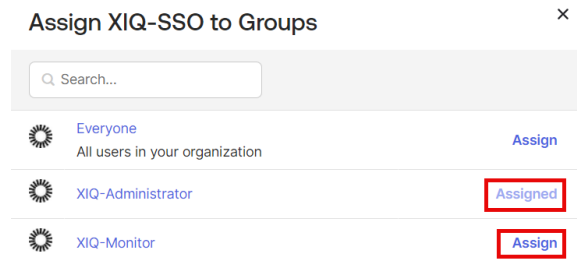
1. From within your new application, select the **Assignments** tab.
2. Select **Assign**, and then select **Assign to Groups**.

- For each group you want to permit authentication to ExtremeCloud IQ with SSO login, select **Assign** next to the Group Name.



#### Note

For each group that you permit, ensure the Group is set to **Assigned**.



**Figure 6: Okta - Group Assignment Continued**

- Select **Done**.

#### Related Topics

[Step 4 — Create New Password Authentication Policy in Okta](#) on page 19

## Step 4 — Create New Password Authentication Policy in Okta

When a user logs in to ExtremeCloud IQ using SSO with Okta, the user must follow the rules defined in the Okta Authentication Policy. You can assign your new SAML application to use one of Okta's out-of-the box Authentication policies. By default, your SAML application uses the **Any Two Factors** Authentication Policy, which has been successfully tested with ExtremeCloud IQ.

Use this task to create and assign a new Password-only Authentication Policy, which can be used with ExtremeCloud IQ if you do not need Okta to enforce Multi-Factor Authentication.

- From the left navigation bar, navigate to **Security > Authentication Policies**, and then select **Add a policy**.
- Enter a **Name**, and then select **Save**.  
You will be directed to the Rules tab of your new Authentication Policy, where we will modify the rules associated with the existing Catch-all Rule policy.
- For the **Catch-all Rule**, select **Actions**, and then select **Edit**.

4. Scroll down to the **Then** section, for **AND User must authenticate with**, select **Password** from the list.
5. For **Prompt for authentication**, select **Every time user signs in to resource**.
6. Select **Save**.
7. Select the **Applications** tab, and then select **Add app**.
8. Find the SAML Application you created in [Step 2](#), and then select **Add** for the associated row.
9. Select **Done** to close the app assignment dialog box.

Related Topics

[Step 5 — Export Metadata for your Okta SAML Application](#) on page 20

---

## Step 5 — Export Metadata for your Okta SAML Application

1. From the left navigation bar, go to **Applications > Applications**.
2. Select the SAML Application you created in [Step 2](#), and then select the **Sign On** tab.
3. In the **Metadata Details** section, you will see the **Metadata URL**. Select **Copy** and retain the URL for use in the next step.

Related Topics

[Step 6 — For Okta: Create IdP Profile, Import Metadata, and Edit Settings in ExtremeCloud IQ](#) on page 20

---

## Step 6 — For Okta: Create IdP Profile, Import Metadata, and Edit Settings in ExtremeCloud IQ

To see the Enable SSO Global Settings option, log in to ExtremeCloud IQ using the SSO URL, <https://sso.extremecloudiq.com/login?sso=true>.



**Note**

Single Sign-on integration can only be configured by ExtremeCloud IQ users with Administrator permissions in their home account (VIQ). External administrators cannot access the SSO configuration page when administering other customer accounts.

1. In ExtremeCloud IQ, select your name in the top right corner, and then select **Global Settings**.
2. Select **Enable Single Sign On (SSO)**.
3. Select **Add IdP Profile**.
4. On the **Type** tab, select **Okta**.
5. On the **Profile** tab, enter the fully qualified **Domain** name for which you want to provide single-sign on, and then select **Continue**.



**Note**

You can only define a single domain name per integration. If your IdP supports multiple domains, you must create a separate IdP profile for each domain.

6. On the **IdP Connection** tab, select **Import from URL**.
7. In the **ISP Metadata URL** field, paste the URL captured in [Step 5](#), and then select **Import**.

After successful import, metadata from Okta displays.



#### Note

There might be some critical elements not included in the Okta metadata. If the SLO URL and SLO Response URL fields are blank, enter placeholder values in each field, which we can update in a subsequent step.

8. To supply the placeholder values, copy the **SSO URL** and paste the value into the **SLO URL** and **SLO Response URL** fields.
9. From the **Choose Certificates** list, ensure the certificate that was included in the Metadata import is selected, and then select **Continue**.

The screenshot displays the configuration interface for an IdP profile. Key elements include:

- IdP Entity ID\***: A text field containing a placeholder URL with a red arrow pointing to it labeled "Copy This".
- SSO Binding**: Radio buttons for "HTTP POST" (selected) and "HTTP Redirect".
- SSO URL\***: A text field containing a placeholder URL with a red arrow pointing to it labeled "Paste Here".
- SSO Sign Request**: An unchecked checkbox.
- SLO Binding**: Radio buttons for "HTTP POST" and "HTTP Redirect" (selected).
- SLO URL\***: A text field containing a placeholder URL with a red arrow pointing to it labeled "Paste Here".
- SLO Response URL\***: A text field containing a placeholder URL with a red arrow pointing to it labeled "Paste Here".
- Verification Certificate**: A section showing a certificate with a valid date of "2024-09-16 - 2034-09-16" and a "Choose Certificates\*" dropdown menu with "trial" selected.

**Figure 7: ExtremeCloud IQ - Placeholder Values for Single Logout**

10. On the **Attribute Mapping** page, enter the following values:
  - **First Name:** `user.firstName`
  - **Last Name:** `user.lastName`
11. Select **Add a group name mapping** for each Okta group to map to an ExtremeCloud IQ role.

12. In the **IdP group** field, enter the name of your Okta group, and then select the ExtremeCloud IQ role to map any users in the group.

Add additional mappings as needed.



**Note**

Each of the values for First Name, Last Name, and Group Name are case sensitive. Ensure that what you enter here exactly matches the information in Okta. The list is applied from top to bottom, with the first match taking precedence. If a user belongs to multiple groups listed here, they will be assigned the XIQ role based on the order you specify.


13. Select a Default RBAC role assignment to assign a default permission for users that log into ExtremeCloud IQ, but are not a member of an explicitly defined group.
  - If you select **Deny User Login**, a user that successfully logs into ExtremeCloud IQ with their Okta credentials, but is not in an Okta group mapped to XIQ RBAC role, is denied access to the application.
  - If you select **Allow User Login and assign default user group**, a user that successfully logs into ExtremeCloud IQ with their Okta credentials, but is not in an Okta group mapped to XIQ RBAC role, is mapped to the role defined here.
14. Select **Save & Finish**.

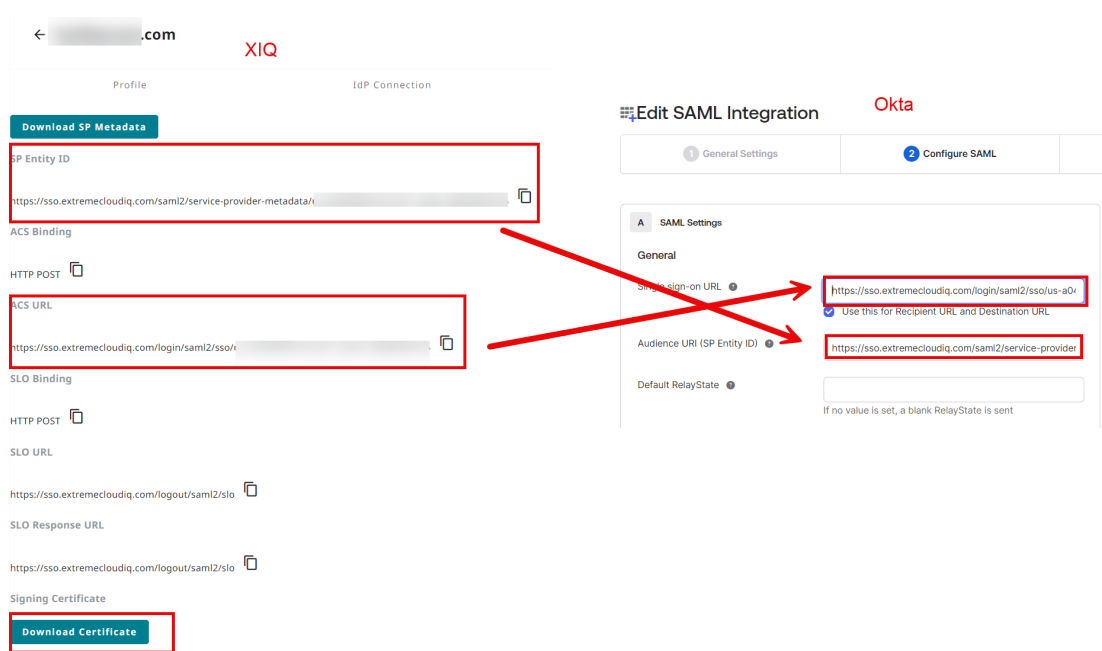
Related Topics

[Step 7 — Modify Okta SAML Application Metadata with ExtremeCloud IQ Settings](#) on page 22

## Step 7 — Modify Okta SAML Application Metadata with ExtremeCloud IQ Settings

For this step, we recommend having ExtremeCloud IQ and Okta open in separate tabs, as you will select data from your new IdP profile in ExtremeCloud IQ and copy it over to your SAML application in Okta.

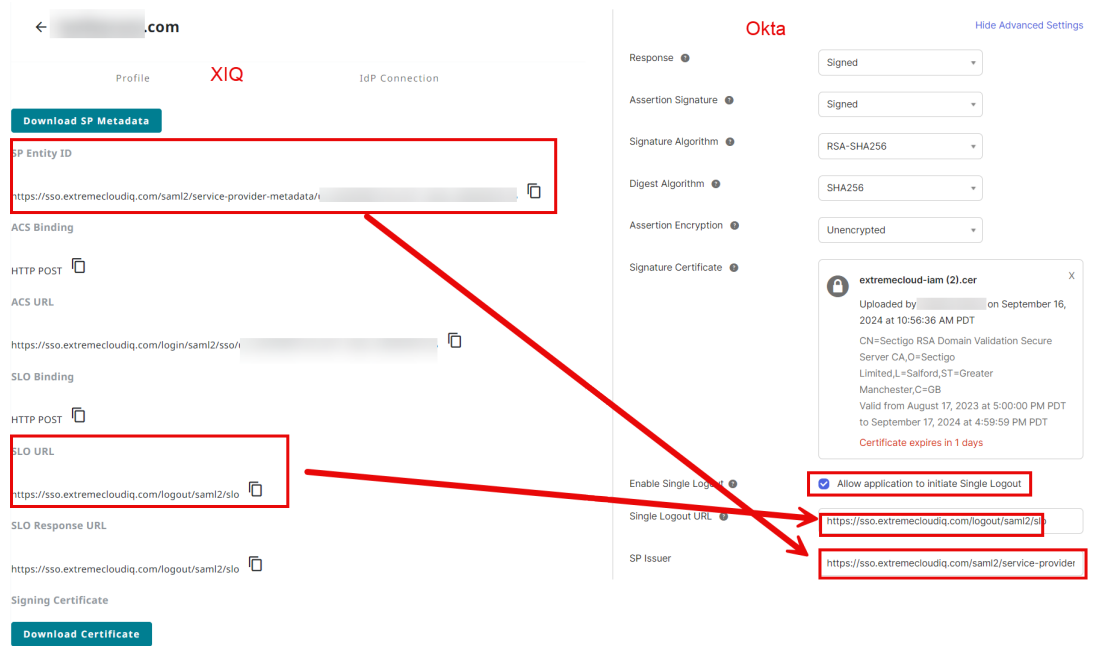
1. In **Okta**:
  - a. Browse to your Admin Portal, navigate to **Applications > Applications**, and then select your SAML application.
  - b. From the **General** tab, scroll down to **SAML Settings**, and then select **Edit**.
  - c. Select **Next**, and then select the **Configure SAML** tab.
2. In **ExtremeCloud IQ**:
  - a. Navigate to **General Settings > Enable Single Sign-on**, in the row for your IdP profile completed in [Step 6](#), select , and then select **Edit**.
  - b. Select the **ExtremeCloud (SP) Connection** tab.
  - c. Select **Download Certificate**, and save the file to your computer.
  - d. Copy the **SP Entity ID** value from ExtremeCloud IQ and copy it to the **Audience URI (SP Entity ID)** field in Okta.
  - e. Copy the **ACS URL** value from ExtremeCloud IQ and copy it to the **Single Sign-On URL** field in Okta.



**Figure 8: Okta - Replace Temporary Data for Single Sign-On URL and Audience URI**

3. In Okta:
  - a. Under **SAML Settings > General**, select **Show Advanced Settings**.
  - b. For **Signature Certificate**, select **Browse files**.
  - c. Select **All Files**, navigate to find the certificate file you downloaded in the previous step, select the certificate, and then select **Open** to upload the ExtremeCloud IQ certificate.
  - d. Select **Enable Single Logout**.
  - e. Copy the **SLO URL** value from **ExtremeCloud IQ** and copy it to the **Single Logout URL** field in Okta.

- f. Copy the **SP Entity ID** value from **ExtremeCloud IQ** and copy it to the **SP Issuer** field in Okta.



**Figure 9: Okta - Single Logout Setting Definition**

- g. Select **Next**, and then select **Finish**. Click to view your SAML application again.
- h. Select the **Sign On** tab, and in the **SAML 2.0** section, select **More Details**.
- i. Next to the **Single Logout URL** field, select **Copy**.  
Use this URL to replace the placeholder text we submitted earlier.
4. In **ExtremeCloud IQ**:
- Return to the **IdP Connection** tab of your IdP profile and paste that value into the **SLO URL** and **SLO Response URL** fields, replacing your placeholder values.
  - Select **Save**.

The integration is now complete.

#### Related Topics

[Step 8 — Okta Test - SP Initiated](#) on page 24

## Step 8 — Okta Test - SP Initiated

Use this task to log in to ExtremeCloud IQ through SP initiated.

- Browse to the GDC Login page, and then select **SSO**.  
`https://sso.extremecloudiq.com/login?sso=true`
- Enter the email address of the IdP account and complete the IdP login process.  
The browser is redirected to the Okta Login Portal. After a successful sign in, the browser redirects to the ExtremeCloud IQ default view.

#### Related Topics

[Step 9 — Okta Test - IdP Initiated](#) on page 25



## Step 9 — Okta Test - IdP Initiated

---

After the integration is complete, test the application.

Use this task to start an IdP initiated test.

1. Log in to your Okta Organization at <https://login.okta.com> with a user account that has been granted access to the SAML application.
2. From the Okta Dashboard page, select your SAML application, and then from the right pane select **Launch App**.

The browser redirects to the Okta Login Portal.

3. Enter your **Username** and **Password**, and then select **Verify**.

After a successful login, you are redirected to the ExtremeCloud IQ default view.



## 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 Admin Account defined in the following figure.

### Admin Accounts

<input type="checkbox"/>	User Name	Email Address	Role
<input type="checkbox"/>	Test User <span style="background-color: #0070C0; color: white; padding: 2px;">SSO</span>	test.user@...	Monitor

**Figure 10: Admin Accounts List Shows User and Assigned Role**

- The **Username** field is created only if the User object is provisioned with the First Name/Last Name field and the Attributes are added in ExtremeCloud IQ.
- Most roles (Operator, Monitor, Installer, etc) require a location be defined for the user to see managed devices. SSO-created accounts do not automatically get assigned locations, so an Administrator must assign each SSP-created account to a location manually in ExtremeCloud IQ.
- A single IdP SSO domain can 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. Certificates can be managed for an IdP Profile by selecting , and then selecting **Manage Certificates**.