



ExtremeCloud™ Universal ZTNA v24.2.0 User Guide

Identity-Based Secure Access Configuration and
Integration

9039102-00 Rev AA
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.....	vi
Preface.....	7
Text Conventions.....	7
Documentation and Training.....	8
Open Source Declarations.....	9
Training.....	9
Help and Support.....	9
Subscribe to Product Announcements.....	10
Send Feedback.....	10
Welcome to ExtremeCloud Universal ZTNA.....	11
Universal ZTNA Licensing.....	12
Access Universal ZTNA.....	12
Account Profile.....	13
Universal ZTNA Onboarding.....	15
Supported Platforms and Hardware Requirements.....	16
Minimum Supported versions for mobile agents.....	16
Minimum Supported OS versions for Desktop Agents across all supported platforms	16
RadSec Proxy hardware requirements and prerequisites.....	16
Service Connector hardware requirements and prerequisites (local and cloud)	16
Universal ZTNA Wired Guidelines.....	17
Managed Mode.....	17
Locally Managed Mode.....	17
Third-party Mode.....	18
Configuration Details for Fabric Engine and Switch Engine.....	18
Configure a Switch for Instant Secure Port in ExtremeCloud IQ	18
Universal ZTNA Wireless Guidelines	21
Integrate ExtremeCloud IQ Wireless with Universal ZTNA.....	22
Configure the Network Policy in ExtremeCloud IQ.....	22
Configure SSID and Wireless.....	22
Manage SSID in Universal ZTNA	22
ExtremeCloud Universal ZTNA Common Object Management.....	23
ExtremeCloud IQ User Profiles	23
ExtremeCloud IQ VLAN Profiles	23
ExtremeCloud IQ IP Firewall Policies	23
ExtremeCloud IQ User Profile Assignment Rules.....	23
ExtremeCloud IQ Deployment	24
Insights.....	25
Dashboard.....	25
User and Device Identities.....	25

Application Discovery.....	26
Identity and Access Management.....	27
Users and Devices.....	27
Manage User Groups.....	27
Add Devices.....	28
Import Devices.....	28
Managed Device Groups.....	29
Identity Provider.....	30
Microsoft Entra ID.....	30
Google Workspace.....	36
Microsoft Active Directory Federated Services (AD FS).....	40
Change the Identity Provider.....	43
Resources.....	44
Add Sites.....	45
Add a Site Group.....	46
Deploy RadSec Proxies.....	46
Deploy Service Connectors.....	47
View RADIUS Servers.....	49
Manage Network Resources.....	49
Add a Network Device.....	50
Import a Network Device.....	51
Enable Global Timeout.....	51
Configure SSID and Wireless.....	52
Manage SSIDs.....	52
Manage RADIUS Templates.....	53
Certificate Management.....	54
CA Trusted Root Certificates.....	54
Matching Criteria for Clients.....	54
Connecting with OCSP Responder.....	54
Windows Certificate Authority: Retrieve the CA (Root) Certificate.....	54
Manage CA Trusted Root Certificates in Universal ZTNA.....	56
Configure the Server Certificate.....	56
Match Criteria for Clients.....	58
Connect with OCSP Responder.....	59
Manage DNS Servers.....	59
Add a DNS Policy.....	60
Applications and Application Groups.....	61
Add Private Web Applications.....	61
Add Multi-Cloud Web Applications.....	62
Add Custom Applications.....	62
Add Terminal Access Applications.....	63
Add Remote Desktop Applications.....	63
Manage Application Discovery.....	64
Create Application Groups.....	64
Network Services.....	66
Add Network Services.....	66
Create Network Service Groups.....	66

Policies.....	68
Create Hybrid Policy.....	68
Create Application Policy.....	70
Create Network Policies.....	71
Update Application Discovery Policy.....	73
Conditions.....	74
Add Location-Based Conditions.....	75
Add Time-Based Conditions.....	75
Create Authentication-Based Conditions.....	76
Configure Device Posture.....	77
Integrations.....	78
Integrate with the Public Cloud.....	78
Add Event Collectors.....	79
Microsoft Intune Integration.....	79
Configure Microsoft Entra ID for Universal ZTNA Microsoft Intune Integration.....	80
Configure Universal ZTNA for Microsoft Intune Integration.....	81
Monitor.....	83
View Alerts.....	83
Troubleshooting.....	83
Evaluate Network Policy.....	84
Evaluate Application Policy.....	84
Subscriptions.....	85
View Activity Logs.....	85
Appendices.....	87
Invite Users.....	87
Import Users.....	88
SAML-based Integration for Microsoft Active Directory Federated Services (AD FS).....	89
Fabric Engine Locally Managed Sample Configuration.....	91
Generate and Download the Certificate Files	91
Upload Certificate Files to the Switch Using FTP.....	91
Apply the Certificate Files to the Switch Using Default RADIUS Secure-Profile.....	92
Apply the RADIUS/RADIUS-Secure Configuration to the Switch.....	93
Optional Configuration.....	93
802.1X NEAP Basic System and Port Configuration	93
Optional Configuration	94
802.1X NEAP on Ports Enabled for Auto-sense.....	94
Optional Configuration for Auto-sense Eapol.....	94
Switch Engine Locally Managed Sample Configuration.....	95
Generate, Download, and Apply the Certificate Files to the Switch.....	95
Apply the RADIUS/RadSec configuration to the switch – RADIUS Accounting is optional but will help with immediate client disconnect notifications in Universal ZTNA..	95
Apply Netlogin/Policy Configuration to the Switch	95



Abstract

The ExtremeCloud™ Universal ZTNA User Guide for version 24.2.0 focuses on providing a robust framework for secure network, application, and device access, regardless of user location. Key features include implementing identity-based Zero Trust policies that ensure consistent, secure access across campus and remote environments. The guide details configuration steps for identity providers (IdPs) such as Microsoft Entra ID, Google Workspace, and Active Directory Federation Services (AD FS), enabling seamless integration with enterprise networks. Additional technical configurations are provided for deploying RadSec proxies, service connectors, and network policies. Universal ZTNA supports secure network application access through RADIUS, IPsec, and WireGuard encryption protocols, with extensive compatibility across various operating systems and hardware platforms like SwitchEngine and FabricEngine. Comprehensive onboarding instructions cover setting up users, devices, applications, and configuring role-based access controls. Advanced topics include monitoring, application discovery, and integration with cloud platforms for managing user identities and network security posture.



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 Ctrl or Esc . If you must press two or more keys simultaneously, the key names are linked with a plus sign (+). Example: Press Ctrl+Alt+Del
<i>Words in italicized type</i>	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.
NEW!	New information. In a PDF, this is searchable text.

Table 3: Command syntax

Convention	Description
bold text	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.
{ x y z }	A choice of required parameters is enclosed in curly brackets separated by vertical bars. You must select one of the options.
x y	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.

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.

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.



Welcome to ExtremeCloud Universal ZTNA

[Universal ZTNA Licensing](#) on page 12

[Access Universal ZTNA](#) on page 12

[Account Profile](#) on page 13

Universal ZTNA integrates network, application, and device access security within a single solution.

With Universal ZTNA:

- Establish a consistent, identity-level zero trust policy across your network for all users.
- Maintain a single policy that integrates the network, applications, and device access (including the Internet of Things (IoT) device access) independent of the client location.

Universal ZTNA combines and enhances remote and campus access security. Remote access leverages ZTNA continuous authentication and tunneled application sessions with direct to cloud routing. On campus access combines ZTNA and Network Access Control (NAC) capabilities to control access to the network and applications for headed and headless devices.

Universal ZTNA integration with mobile device solutions such as Microsoft Intune offers the following:

- Improved access by closely examining the condition of devices and their authentication features
- A single identity-based zero trust policy engine for networks and applications
- A single system for monitoring, visualizing, and reporting to gain better insights and simplify management
- Automatic set up for IoT and end user devices
- Automatic configuration for NAC, SSIDs, ports and VLANs on Universal APs and switches

For more information, see [Microsoft Intune Integration](#) on page 79.

Related Topics

[Universal ZTNA Licensing](#) on page 12

[Access Universal ZTNA](#) on page 12

[Account Profile](#) on page 13

Universal ZTNA Licensing

The current version of Universal ZTNA is 24.2.0.

Licensing for Universal ZTNA has two available options:


- Secure | Cloud NAC only
- Secure Plus | Cloud NAC & ZTNA

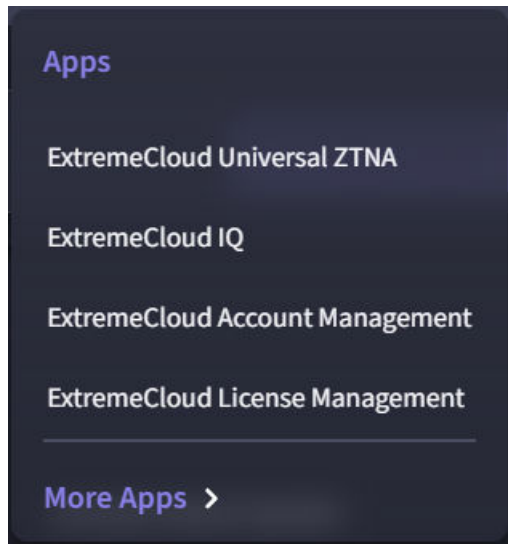
The following parameters apply to the Universal ZTNA licenses:

- The "Plus" SKU is not an add on to the "Standard" SKU.
- Minimum 50 licenses for initial order.
- Mix and match of Secure and Secure Plus tiers is permitted.
- Each user license includes 5 end devices.

Access Universal ZTNA

Log in to ExtremeCloud IQ.

To go to other Extreme apps, select the top-right menu .



To add an Administrator, Monitor, or Observer role for an administrator select, **ExtremeCloud Account Management**.

1. Select **Add User**.
2. Add a username and email address.
3. Under **Role Access Controls**, select an application and role from the drop-down lists.
4. Select **Save**.

For more information about different roles, see [Account Profile](#) on page 13.

To access Universal ZTNA, from the  top-right menu, select Universal ZTNA.

My Apps



ExtremeCloud
Universal ZTNA

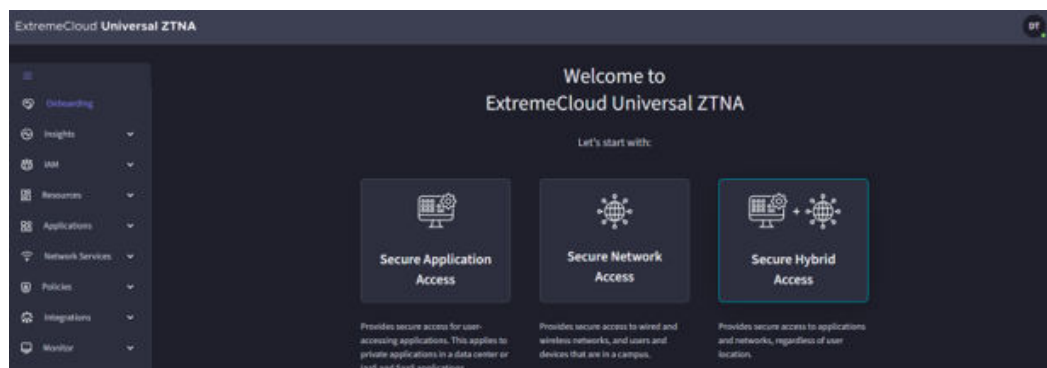


Note

If the ExtremeCloud Universal ZTNA icon is not shown, ensure a license exists in your account for Universal ZTNA.

The navigation menu allows you to:

- Onboard
- Access insights
- Add users and groups, devices and groups, and change the identity provider (IdP)
- Add resources
- Add applications
- Add network policies
- Integrate with third-party services
- Monitor (troubleshooting)



Account Profile

Your Universal ZTNA profile has information on Account Settings and your current role. In the top right corner of the application, select your profile image and **View Profile**.

Account Settings lists your Name, Email, and Owner ID.

Roles displays your role. Universal ZTNA has three access roles available. Each role will allow the admin different permissions and functionality within the application:

- Administrator - You can manage actions, including adding, updating, and removing all provided settings and resources.
- Monitor - You can view all settings and resources. Additionally, you can troubleshoot application and network policies and applications.
- Observer - You can view all settings and resources in your environment.



Universal ZTNA Onboarding

[Supported Platforms and Hardware Requirements](#) on page 16

[Universal ZTNA Wired Guidelines](#) on page 17

[Universal ZTNA Wireless Guidelines](#) on page 21

Universal ZTNA provides secure access to applications and networks from anywhere, making it easy for users to connect seamlessly to their resources.

The following types of secure access are offered by Universal ZTNA:

- **Secure Application Access** provides secure access for user-accessing applications. This applies to private applications in a data center or IaaS applications.
- **Secure Network Access** provides secure access to wired and wireless networks, and users and devices that are in a campus.
- **Secure Hybrid Access** provides secure access to applications and networks, regardless of user location.

The primary goal of a secure access method is to ensure safe access to applications and networks from anywhere, making it easy for users to connect seamlessly to their resources.



Note

This document only covers the Secure Hybrid Access onboarding method, which is the most comprehensive method. Secure Application Access and Secure Network Access are subsets of Secure Hybrid Access.

Each access method offers the following types of Identity Providers (IdPs). Universal ZTNA supports configuring one method per installation. The IdPs are:

- [Microsoft Entra ID](#)
- [Google Workspace](#)
- [Microsoft Active Directory Federated Services \(AD FS\)](#) on page 40

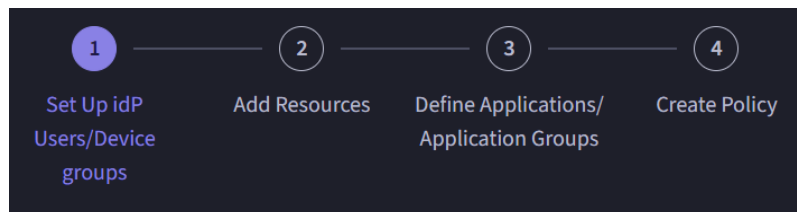
For more information, see [Identity Provider](#) on page 30.



Note

The IdP Secure Application Access is the only supported method in the ExtremeCloudUniversal ZTNA trial.

Once you configure your IdP, you can continue through the Secure Hybrid Access workflow:



Supported Platforms and Hardware Requirements

Minimum Supported versions for mobile agents

Android: 11

iOS and iPadOS: 13

Minimum Supported OS versions for Desktop Agents across all supported platforms

Mac Agent = > macOS 11 and later

Windows Agent => Windows 10 and later

Linux Agent = > Ubuntu 20.04 and 22.04

RadSec Proxy hardware requirements and prerequisites

Minimum hardware requirements: vCPU: 2 Ram: 4 GB

Supported Deployment:

VMware OVA

Ubuntu 20.04 and 22.04 Packaged Install.

Service Connector hardware requirements and prerequisites (local and cloud)

- Supported Deployments:
 - **System Requirements for Packaged Deployment** - Recommended OS - Ubuntu 20.04 and 22.04.
 - **VMware OVA**
 - **Dockerized Deployment** - C-Supported Platform: amd64 Compatible with multiple operating systems; requires only Docker to be installed.
- If the Service Connector and client device are on the same network (e.g., in the same local LAN or locally routable network), inbound requests must be allowed for the following protocols:

Wireguard Encryption Protocol: 51820

IPSEC Encryption Protocol: 500, 4500

Minimum hardware requirements:

vCPU: 2 Ram: 4 GB

Universal ZTNA Wired Guidelines

Universal ZTNA supports Fabric Engine/VOSS and Switch Engine/EXOS Network Operating Systems (NOSs). Universal ZTNA supports the minimum versions of the following products:

- Switch Engine 32.7.1
- Fabric Engine 9.0.2

There are three management options:

- [Managed Mode](#)
- [Locally Managed Mode](#) on page 17
- [Third-party Mode](#) on page 18

Managed Mode

Supported NOS: Switch Engine. Switches are onboarded directly using **Manage your Devices**.

ExtremeCloud IQ manages switch configuration. Use [Configure a Switch for Instant Secure Port in ExtremeCloud IQ](#) on page 18 to provision the following components on the switch:

- Certificate for RadSec communication
- RADIUS/RadSec configuration to the cloud RadSec server or locally deployed RadSec proxy
- 802.1X or MAC authentication

Universal ZTNA updates the policy configuration on the switch, including static policy roles and rules, based on the provisioned network policy.

Locally Managed Mode

Supported NOS: Switch Engine and Fabric Engine. Switches are onboarded using **Manage your Devices Locally**.

ExtremeCloud IQ does not configure switches in local managed mode. In local managed mode, based on the provisioned network policy, Universal ZTNA provisions policy on the switch using dynamic ACLs (dACL) conveyed using RADIUS vendor-specific attributes (VSAs) during the authentication process.

Users configure the following components manually:

- Certificate for RadSec communication
- RADIUS/RadSec configuration to the cloud RadSec server

- 802.1X or MAC authentication, along with supporting feature sets, depending on the deployment model

Third-party Mode

Universal ZTNA provisions policy on the switch using dynamic ACLs (dACL) conveyed using RADIUS vendor-specific attributes (VSAs) during the authentication process. Third-party or non-ExtremeCloud IQ devices are onboarded through **Network Resources**.

Users configure the following components manually:

- Certificate for RadSec communication
- RADIUS/RadSec configuration to the cloud RadSec server
- 802.1X or MAC authentication, along with supporting feature sets, depending on the deployment model
- Cloned and modified Extreme, Cisco, HP, and Aruba templates or newly created vendor-specific RADIUS templates. For more information, [Manage RADIUS Templates](#) on page 53.
- SSIDs for wireless devices. For more information see [Manage SSIDs](#) on page 52.
- Network devices. For more information, see [Add a Network Device](#) on page 50.

Configuration Details for Fabric Engine and Switch Engine


- To configure Fabric Engine, select [Fabric Engine Locally Managed Sample Configuration](#) on page 91.
- To configure Switch Engine, select [Switch Engine Locally Managed Sample Configuration](#) on page 95.

Fabric Engine and Switch Engine Reference Guides

- [Switch Engine OnePolicy](#)
- [Switch Engine Netlogin](#)
- [Fabric Engine Auto-sense/Zero-Touch Capabilities](#)
- [Fabric Engine - EAP \(Extensible Authentication Protocol over LAN\)](#)

Configure a Switch for Instant Secure Port in ExtremeCloud IQ

Use this task to configure a switch for Instant Secure Port in ExtremeCloud IQ.

1. Go to **Configure > Network Policies**.
2. On an existing network policy, select  to edit.
3. Select the Switching section of the configuration. Go to **Switch Settings > Instant Secure Port Profiles**.

4. Select **+** to create a new profile and configure the settings.
 - a. In the **Create Instant Secure Port Profile** dialog, enter a name.
 - b. To assign a VLAN on an authentication failure, an unreachable server, or other non-authenticated conditions, select the **Enable Unauthenticated VLAN** check box and select or create an **Unauthenticated VLAN**. Otherwise, any unauthenticated session will be rejected.
 - c. Leave the option for **UZTNA RADIUS Cloud configuration** enabled. This ensures the switch automatically installs the RadSec certificates and authentication configuration.
 - d. Select **SAVE**.

Create Instant Secure Port Profile
✕

An Instant Secure Port Profile authenticates devices attached to switch ports and allows for dynamic configuration to be applied based on RADIUS authentication.

Name *

Description

Enable Unauthenticated VLAN Enable and define an untagged VLAN when the device is unauthenticated. Authentication mode is optional when the Unauthenticated VLAN is enabled.

Unauthenticated VLAN * +

Set authentication options for switches that will have Instant Secure Port enabled within the switch template. The port type also requires User or MAC auth to be enabled.

Authentication	Order
User Authentication – Enable 802.1x authentication for ports connected to individual hosts.	↑ ↓
MAC Authentication – MAC authentication uses the MAC address as the username and password to authentication clients. Typically used to support legacy clients.	↑ ↓

Define the RADIUS server configuration. If a DHCP assigned IP address is utilized, the DHCP IP address will be used for the RADIUS client IP configuration. If the DHCP assigned IP address changes, then a device update will be required to update the RADIUS client IP configuration.

Use UZTNA RADIUS Cloud configuration ← [here](#). If UZTNA settings or license is not properly configured, then device authorization may fail.

Use UZTNA RADIUS Proxy Servers

CANCEL
SAVE

5. Select **Switch Templates** and add or edit a switch template for the relevant device types.



Note

Instant Secure Port **only** works on Universal switches running Switch Engine and the X435 switch models.

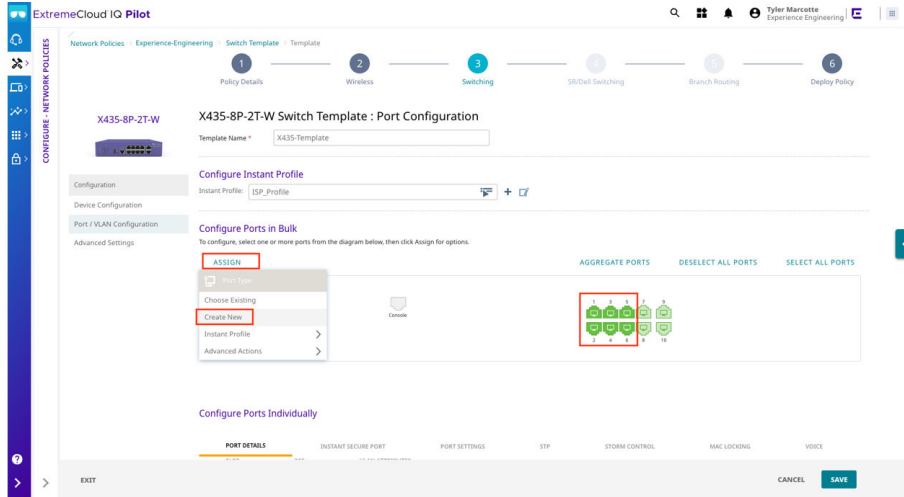
6. Select **Port / VLAN Configuration**. Under **Configure Instant Profile**, select the previously created profile.

- Click and drag a box around multiple ports or select an individual port to enable. Select **Create New** from the **Assign > Port Type** drop-down menu.



Note

Default port types cannot be edited.



The system displays the **Create Port Type** dialog.

- Configure the port type settings.
 - Enter a name for the new port type.
 - Select **NEXT** until the Instant Secure Port Settings section is selected.

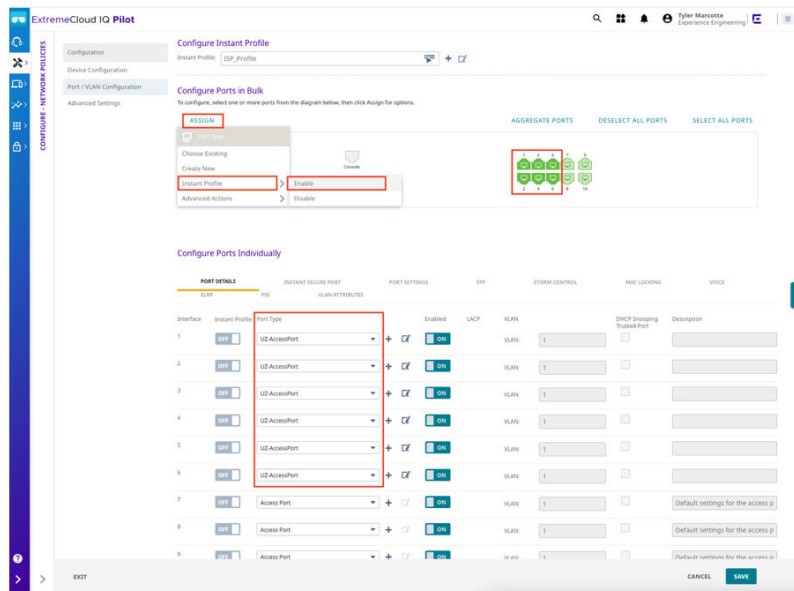


Note

The VLAN doesn't require configuration in ExtremeCloud IQ. It is assigned in Universal ZTNA.

- On the **Instant Secure Port Settings** tab, enable the desired authentication types on the switch port.
- Continue selecting **NEXT** until the system displays the Summary screen.
- Select **SAVE**.

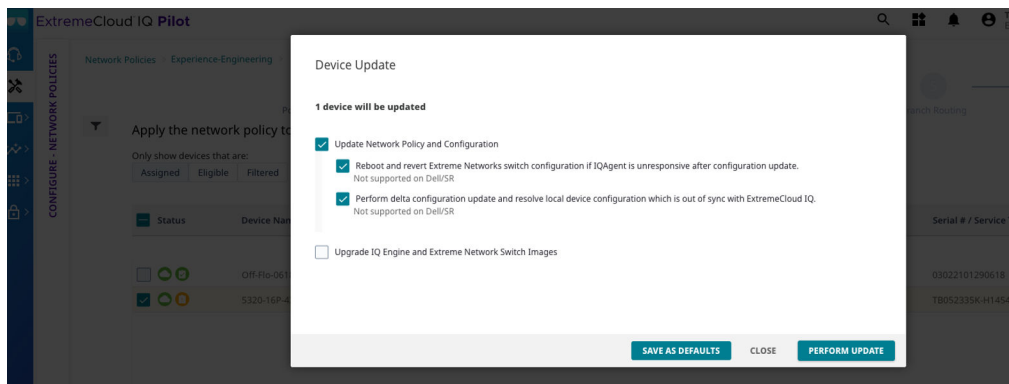
9. Select the ports again from the switch picture, and select **Assign > Instant Profile > Enable**. Alternatively, enable the slider for each port that Instant Profiles should be enabled.



Note

The port types are now assigned to the ports; however Instant Profiles are not enabled for those ports.

10. With the Instant Secure Port enabled, select **SAVE**.
11. Select the **Deploy Policy** workflow menu.
12. Update the relevant devices.



Universal ZTNA Wireless Guidelines

This chapter describes how Universal ZTNA can be used for mapping policies based on Universal ZTNA conditions and returning a filter ID that matches an automatically provisioned policy using ExtremeCloud IQ Wireless.

Integrate ExtremeCloud IQ Wireless with Universal ZTNA

Use this task to integrate ExtremeCloud IQ Wireless with Universal ZTNA.

1. From the ExtremeCloud IQ portal main navigation, select **Configure > Common Objects > Policy > SSIDs**.
2. Select your SSID and select the edit (pencil) icon.
3. Under **SSID Usage**, ensure the **SSID Authentication** and **Enterprise** tabs are selected.
4. Under **Authentication Settings**, enable **Authentication with ExtremeCloud Universal ZTNA**.

Configure the Network Policy in ExtremeCloud IQ

Use this task to configure the network policy in ExtremeCloud IQ.

1. From ExtremeCloud IQ, go to **Configure > Network Policies** and select **Add Network Policy**.
2. Select **Wireless**.
3. Enter a name for the policy and optional description.
4. Select **Save**.
5. Select **Next**.

Go to [Configure SSID and Wireless](#) on page 22.

Configure SSID and Wireless

Service Set Identifier (SSID) configuration in ExtremeCloud IQ depends on the type of authentication (802.1X or MAC) and the type of RadSec deployed.

Universal ZTNA RadSec is supported in all SSID types except for Private Pre-Shared Key SSIDs.


Use this task to configure SSID and wireless in ExtremeCloud IQ.

1. Go to **Configure > Common Objects > Policies > SSIDs**.
2. Select **+** to create a new SSID.
3. Enter a username and broadcast name.
4. Under **SSID Usage**, ensure the **SSID Authentication** and **Enterprise** tabs are selected.
5. (Optional) To enable MAC authentication toggle to **ON**.
6. Under **Authentication Settings**, enable **Authentication with ExtremeCloud Universal ZTNA**.

Manage SSID in Universal ZTNA

ExtremeCloud Universal ZTNA automatically creates and deletes common objects in ExtremeCloud IQ and associates them with managed SSIDs to integrate with the ExtremeCloud IQ wireless solution.

Use this task to enable SSID management for ExtremeCloud Universal ZTNA.

1. Log in to Universal ZTNA.
2. Select **Resources** > **Network Resources** > **SSID**.
3. Select .
4. Select **Managed SSID** > **UZTNA Managed** > **Confirm**.

ExtremeCloud Universal ZTNA Common Object Management

Common objects created by ExtremeCloud Universal ZTNA are named with a UZTNA_ prefix. The administrator must not use these objects to modify or associate them with other common objects. Universal ZTNA automatically deletes or modifies their configuration when changes are made through the ExtremeCloud Universal ZTNA portal.

ExtremeCloud IQ User Profiles

Universal ZTNA creates a user profile for each hybrid or network policy created in Universal ZTNA. User profiles are visible to the administrator in ExtremeCloud IQ. Go to **Configure** > **Common Objects** > **Policy** > **User Profiles**.

ExtremeCloud IQ VLAN Profiles

Universal ZTNA creates a VLAN Profile for each VLAN ID selected for use in a hybrid or network policy created in Universal ZTNA.

ExtremeCloud Universal ZTNA automatically associates the VLAN Profile to the corresponding user profile.

ExtremeCloud IQ IP Firewall Policies

When you configure a network service group for a Universal ZTNA policy, Universal ZTNA creates an IP firewall policy.

The IP Firewall Rules uses other common objects such as IP address and network services which are also created by Universal ZTNA when network service groups are configured for a policy.

The IP Firewall Policy is automatically associated to the outbound traffic policy for the corresponding user profile in ExtremeCloud IQ.

ExtremeCloud IQ User Profile Assignment Rules

Universal ZTNA creates user profile assignment rules for each hybrid or network policy created in Universal ZTNA and automatically attaches them to managed SSIDs in Universal ZTNA.

The user profile assignment rules map user profiles to the corresponding Filter-ID RADIUS Attribute to ensure that users are assigned the appropriate policy when authenticating to an SSID.

The administrator can control which user profile assignment rules are attached to an SSID by configuring an SSID location condition in the hybrid or network policy in Universal ZTNA.

ExtremeCloud IQ Deployment

Universal ZTNA automatically deploys configuration updates to ExtremeCloud IQ Access Points which are assigned a network policy in ExtremeCloud IQ that contains SSIDs managed by Universal ZTNA.

Changes to hybrid, network policies or managed SSIDs in Universal ZTNA triggers an automatic configuration deployment.



Note

Universal ZTNA will deploy automatically to ExtremeCloud IQ if there is no staged configuration from ExtremeCloud IQ.

If there is staged configuration, you can manually trigger this deployment by (Re)-Syncing the configuration. Go to **Resources > Network Resources > Network Devices**.



Insights

- [Dashboard](#) on page 25
- [User and Device Identities](#) on page 25
- [Application Discovery](#) on page 26

Use Insights to view user identities and device identities.

You can also use Insights to manage linked devices to ensure secure application access. Devices can be re-authenticated, allowed access, have access revoked, or deleted.

Dashboard

Go to **Insights > Dashboard** for a summary of network security with a focus on health status, applications, networks, authentication, and policies.

User and Device Identities

Go to **Insights > Identities**. When you expand an identity on the list, you can view Device Information, Network Information, and ZTNA Agent Access Information.

The following actions are available for user and device identities:

- View History
- Add to Device Group
- Add to User Group
- Re-Authenticate



Note

Re-Authenticate is not available for third-party or non-ExtremeCloud IQ devices.

- Restore Access
- Revoke Access
- Delete
- Network Policy Evaluation



Note

When viewing **Device Information**, Hostname, Model Name, Operating System are not available for third-party or non-ExtremeCloud IQ devices,

The filter options are Auth State, ZTNA Agent, Policy, Device Type, Compliance Status, NAS IP, NAS Port ID, SSID, OS Name, and Auth Type.

Application Discovery

Go to **Insights > Application Discovery**, you can view the following application analytic information:

- Most Used Applications by Users
- Least Used Application by Users
- Total Applications Discovered
- Total Users
- Total Apps
- Policy Recommendation



Note

Application Discovery will allow all users, all subnets, on all ports effectively acting as a wide-open VPN.

To enable, extend, and end application discovery, see [Manage Application Discovery](#) on page 64.



Identity and Access Management

[Users and Devices](#) on page 27

[Identity Provider](#) on page 30

Go to Identity and Access Management (**IAM**) to configure [users](#), [user groups](#), [devices](#), [device groups](#), or update an identity provider.

Users and Devices

Manage individual users and devices or groups of users and devices by controlling their access to enterprise applications and the network.

The **Users** page contains a list of users. For more information, see [Manage User Groups](#) on page 27.



Note

When an IdP is not being synchronized, you can also [Invite Users](#) on page 87 and [Import Users](#) on page 88.

The **Devices** page contains a list of devices. You can [Add Devices](#) on page 28 and [Import Devices](#) on page 28.

The **Devices Groups** page contains a list of device groups. For more information, see [Managed Device Groups](#) on page 29.

Manage User Groups

Use this task to create, manage, and review user groups synchronized from the IdP.

1. Go to **IAM > User Groups**.
2. To create a user group, select **Create User Group** and configure the settings.

Table 4: User Group Creation Settings

Field	Description
User Group Name	Enter at least three alphanumeric characters.
Description (Optional)	Enter a description.
Select Users (Optional)	Select or search for one or multiple users.



3. Select **Create**.

The **User Groups** page contains a list of user groups.



Note

List displays user groups synchronized from the IdP. When an IdP is not being synchronized, you can also [Invite Users](#) on page 87 and [Import Users](#) on page 88.

4. To add users or make an update to an existing group, select  within the table and select **Update**.
 - a. You can update the **User Group Name** or **Description**.
 - b. To add users to the user group, select users you would like to add.
 - c. Select **Update**.
5. To remove an existing group, select  within the table and select **Remove**.


Add Devices

Use this task to manually add devices.

1. Go to **IAM > Devices**.
2. Select **Add Devices** and configure the settings.

Table 5: Device Configuration Settings

Field	Description
MAC Address	Enter one or more MAC addresses.
Alias (Optional)	Enter an alias for your device.
Description (Optional)	Enter a description.

3. Select **Add**.
Your device displays in the device list.
4. To remove a device, select  within the table and select **Remove** devices.

Import Devices

Use this task to import devices in bulk.

1. Go to **IAM > Devices**.
2. Select **Import Devices**.
3. Select one of the following:
 - **Browse** to locate your .csv file.
 - **Download the cvs** template to create your device list to import.

When you finish creating your template, then repeat the **Browse** step.

4. Select **Proceed**.
A confirmation pop-up window displays: **File uploaded and validated successfully. You can now continue.**

5. Select **Proceed**.

The list of devices from the .csv file displays.

6. Select specific MAC addresses to import or all addresses to import.

7. Select **Confirm**.

The **Select Device Group** pop-up window displays.

8. (Optional) Select a device group from **Add to Device Group**.

If no device groups are available, select **Create New Device Group** and follow the instructions.

9. Select **Import**.

Your devices display in the device list.

Managed Device Groups

Use this task to create device groups.


1. Go to **IAM > Device Groups**.
2. Select **Create Device Group** and configure the settings.

Table 6: Device Group Configuration Settings


Field	Description
Name of Device Group	Enter at least three alphanumeric characters for the device group name.
Description (Optional)	Enter a description.
Select Type	Select one of the following: <ul style="list-style-type: none"> • Devices • MAC OUI - To add a new MAC OUI, select Add MAC OUI and configure the settings: <ul style="list-style-type: none"> ◦ Alias (Optional) - Add an optional alias. ◦ Search - Select MAC OUIs can be tagged and searched by any given name mentioned as the alias. ◦ Select Add. • Custom MAC - Any MAC address starting with the entered hex value will be matched.

3. Select **Create**.

Your device displays in the device list.

4. To add devices or make an update to an existing group, select  within the table and select **Update**.

- a. You can update the **Device Group Name** or **Description**.
- b. To change the type, select a new option.

- c. To add devices to the device group, select **Existing Devices** or **New Device** from the **Add device**.
 - d. Select **Update**.
5. To remove an existing group, select  within the table and select **Remove**.

Once you have onboarded your initial users and devices, continue to [Resources](#) on page 44.

Identity Provider

An Identity Provider (IdP) is the source of your users' identities for your organization. Begin by configuring your IdP. You can do this by establishing connections with one of the following IdPs:

- [Microsoft Entra ID](#) on page 30
- [Google Workspace](#) on page 36
- [Microsoft Active Directory Federated Services \(AD FS\)](#) on page 40

Once you have established your initial IdP during onboarding, to make changes to your selection, see [Change the Identity Provider](#) on page 43.

Microsoft Entra ID

Microsoft Entra ID offers two types of Single Sign-on (SSO) methods.

- **OpenID Connect (OIDC)**: This open authentication protocol works on top of the Open Authorization (OAuth) 2.0 framework.

For more information on OIDC SSO, see [Set up Microsoft Entra ID with Open ID Connect Integration](#) on page 30.

- **Security Assertion Markup Language (SAML)**: This is an open standard for exchanging authentication and authorization data between an identity provider and a service provider.



Note

Secure Network Authentication is not supported with SAML 2.0.

For more information on SAML Connect SSO, see [Configure Microsoft Entra ID - SAML](#) on page 35.

Set up Microsoft Entra ID with Open ID Connect Integration

There are multiple applications that may be needed when creating the application in Entra ID.

1. Secure Application Access authentication – Used for logging into the Universal ZTNA Agent or the End User web portal.
2. Secure Network Access authentication
3. User and User Group Synchronization

Use this task to set up Microsoft Entra with Open ID Connect (OIDC).

1. Log in to Microsoft Entra ID and select **Applications > App Registrations**.
2. To create a new registration, in the **Name** field, enter **ExtremeCloud Universal ZTNA – OIDC** and select **Register**.
3. Select **Redirect URIs > Add a platform**.
4. Copy the current URIs listed under **Web > Redirect URIs**.
The format of the URIs will be similar to this example:
 - <https://va2-uz.extremecloudiq.com/auth/api/v1/accounts/invite/microsoft/signup/callback/>
 - <https://va2-uz.extremecloudiq.com/auth/api/v1/accounts/microsoft/login/callback/>
5. Return to the **Overview** screen and take note of the **Application (client) ID** and the **Directory (tenant) ID**.
6. In the **Client Credentials** field, select **Add a certificate or secret > New Client Secret > Add**.



Note

Take note of the expiration date as the application will not be functional after the secret expires.

7. From the **Certificates & Secrets** screen, under the **Clients Secret** tab, in the **Value** field, copy the new token.
8. From the **API Permissions** screen, select **Grant admin consent for** [company name].
9. From the **ExtremeCloud Universal ZTNA Identity Provider - Microsoft Entra ID** screen, enter the noted **Application (client) ID**, **Client Secret**, and **Directory (tenant) ID**.
10. (Optional) Select **Secure Network Access** if the Network Access functionality will be used. If so, the same application can be leveraged as Application access. However, if Multi-Factor Authentication is enabled in Entra ID, a separate application must be created, and a conditional access policy must be leveraged to disable MFA on this specific application.

If the **Secure Network Access** check box is checked, you can create separate Entra ID Application in Entra ID and provide the Client ID, Client Secret and Tenant ID or select **Use Settings Above for Network Access** to use same IDP credentials entered for app access for network access.
11. (Optional) To provision users and user groups in Entra ID and then sync them with Universal ZTNA, [Synchronize Users and Groups with Microsoft Entra ID](#) on page 31.
12. Select **Validate Information**.
13. When validation is complete, select **Update > Confirm**.

Synchronize Users and Groups with Microsoft Entra ID

Synchronizing Users and User Groups from Entra ID is best way to ensure user groups can be properly leveraged in Universal ZTNA policies. There are two methods to synchronize users with Universal ZTNA:

1. Just in Time (JIT) Synchronization – this method has Universal ZTNA reach into Entra ID and pull users and user groups on a polled basis. This method leverages the Secure Application Access OIDC Application to integrate with Entra ID APIs.

2. System for Cross-Domain Identity Management (SCIM) Synchronization – this method had Microsoft Entra ID push users and user groups from Entra ID into Universal ZTNA. This method requires an enterprise application to be set up in Entra ID so that automatic provisioning can be enabled.

Synchronizing Users and User Groups using JIT Provisioning

JIT User and User Group synchronization leverages the Entra ID application that is entered for Secure Application Access. There are additional items that need to be configured to enable the correct APIs.

Use this task to synchronize users and user groups using Just-In-Time (JIT) provisioning.

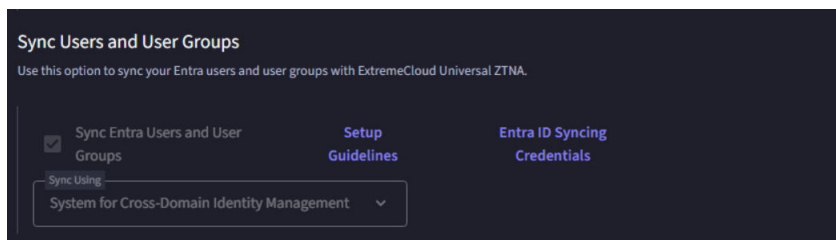
1. In the registered application, go to the **Authentication** section. Select **ID tokens** under **Implicit grant and hybrid flows**.
2. Select **Save**.
3. Under **Token configuration** select **Add optional claim** and select **upn, family_name,** and **given_name**.
4. Select **Add**.
5. If prompted, select the check box to turn on the Microsoft Graph profile permission and select **Add**.
6. Select **Add groups claim** followed by **Groups assigned to the application**.
7. Under **ID section**, select **Group ID** and select **Add**.
8. Under **API permissions** select **Add a permission**.
9. Select **Microsoft Graph**.
10. Next, choose **Application permissions**. Under **Select permissions**:
 - a. Filter on Group and select **Group.Read.All**.
 - b. Filter on GroupMember and select **GroupMember.Read.All**.
 - c. Filter on User and select **User.Read.All**.
 - d. Click **Add permissions** to add them to the API permissions list.
11. On the **API permissions** page, select **Grant admin consent for <Company Name>**.
12. Under **Overview**, scroll to the bottom and select the **Go to Enterprise Applications**.
13. Under Manage select **Properties** and set the **Assignment Required** option to **Yes**.
14. Select **Save**.
15. The final step in Entra ID is to assign Users and groups. Under **Users and groups** assign all groups that should be leveraged in Universal ZTNA.
16. In Universal ZTNA, go to **IAM > Identity Providers**.
17. Select the **Sync Entra ID Users and User Groups** option.
18. Under **Sync Users and User Groups** select **JIT (Just-in-time)** from the **Sync Using** drop-down list.
19. Select **Validate**.

Synchronize Users and User Groups using SCIM Provisioning

Using SCIM to push Users and User Groups into Universal ZTNA requires the creation of an Enterprise Application in Entra ID. Use this task to configure System for Cross-domain Identity Management (SCIM) provisioning in Microsoft Entra ID.

1. Log in to Microsoft Entra ID and go to **Enterprise application > New application**.

2. Select **Create your own application**. Name the application with Provisioning in the title so that it can be easily located. Select the **Non-gallery** option.
3. Select **Properties** for the application and toggle **Assignment Required** to **Yes** and **Visible to Users** to **No** then select **Save**.
4. Select **Users and groups** and assign the User groups that should be included in Universal ZTNA.
5. Select **Manage > Provisioning**.
6. Select **Automatic** from the **Provisioning Mode** drop-down list.
7. In Universal ZTNA go to **IAM > Identity Providers**.
8. Under **Provisioning**, select **Entra ID Syncing credentials** and copy the **Tenant URL** and **Secret Token**.
9. Under **Sync Users and User Groups** select the **Sync Entra ID Users and User Groups** check box.
10. Under **Sync** select **System for Cross-Domain Identity Management (SCIM)** from the drop-down list.



11. Select **Validate** and **Update** to save the changes.
12. In Microsoft Entra ID, under **Admin Credentials**, paste the **Tenant URL** and **Secret Token** and select **Test Connection**.
13. Select **Provision Microsoft Entra ID Users**.
14. On the **Attributes Mapping** page and complete the following:
 - a. Under **Source Object Scope**, select **All records**.
 - b. Select **Add new filter group**.
 - c. In **Add Scoping Filter**, select **mail** as the source attribute. The mail attribute needs to exist for the user to be imported into Universal ZTNA. If the desire is to only have corporate email accounts imported into Universal ZTNA, matching on the email extension for the organization will work. For this example, select **INCLUDES** as the operator and the email domain as the clause value.
 - d. Name the scoping filter and select **Apply**.
 - e. In the resulting screens, select **Apply** and **Save** to save the filter to the provisioning profile.
15. (Optional) Under **Settings**, there is a section for **Scope now**. If there is not, refresh the webpage. The default action is to only synchronize groups that are assigned to this application. To synchronize all groups in the Entra ID, change the **Scope** to **Sync all users and groups**.
16. Go to **Provisioning** and set **Provisioning Status** to **On**.
17. Provisioning can take up to an hour to start. If desired **Provision on Demand** can be selected from the Provisioning Overview to immediately start a provisioning cycle.
18. Select the group or users to provision at that moment.

19. Once provisioning is complete, the logs can be reviewed in case there were issues provisioning.

Disable MFA using a Conditional Access Policy for Microsoft Entra ID

Currently, the Secure Network Authentication requires that multi-factor authentication (MFA) be disabled for the app when using EAP-TTLS.

If you use Microsoft Entra ID premium, you can create a rule to exclude this only for the Universal ZTNA application. For more information, see [Disable MFA using Microsoft Entra ID Premium](#) on page 34.

If you don't use Microsoft Entra ID premium, this must be disabled for all users. For more information, see [Disable MFA without Entra ID Premium](#) on page 34.

Disable MFA using Microsoft Entra ID Premium

Use this task to disable multi-factor authentication (MFA) with Microsoft Entra ID Premium.

If you do not have Microsoft Entra ID Premium, see [Disable MFA without Entra ID Premium](#) on page 34.

1. Log in to Microsoft Entra ID.
2. Go to **Manage > Properties** and configure the settings.
 - a. Select **Manage Security defaults**.
 - b. Disable the toggle **Enable Security defaults** and select **Save**.
3. Go to **Manage > Security > Conditional Access**.
4. Select **New Policy** and configure the settings.
 - a. In the **Name** field, enter 2FA policy.
 - b. Under **Users and groups**, select **All Users**.
 - c. Under **Cloud apps or actions**, in the **Exclude** section and select the **Universal ZTNA** app you created earlier in **Select excluded cloud apps**.
 - d. Under **Grant**, select **Grant access**.
 - e. Select the **Require multi-factor authentication** check box and any other settings your organization requires.
 - f. At the bottom, ensure **Enable policy** is set to **On** and select **Save**.

Disable MFA without Entra ID Premium



Note

Using Microsoft Entra ID premium is the correct way to perform this. This option is only suggested for testing or when its impossible to have access to Microsoft Entra ID premium. To use Microsoft Entra ID premium, see [Disable MFA using Microsoft Entra ID Premium](#) on page 34.

Use this task to disable common recommended settings from Microsoft.

1. Log in to Microsoft Entra ID.

2. Go to **Manage > Properties** and configure the settings.
 - a. Select **Manage Security defaults**.
 - b. Disable the toggle **Enable Security defaults** and select **Save**.

Configure Microsoft Entra ID - SAML

This task shows you how to configure your identity provider using Microsoft Entra ID - SAML.



Note

Secure Network Access is not supported with SAML.

1. Select **Onboarding**.

The **Welcome** window displays.
2. Select **Secure Hybrid Access** [**Secure Application Access** or **Secure Network Access**].

The **Identity Provider** window displays with ExtremeCloud Universal ZTNA selected.
3. Select **Next**.

The **Onboarding** window displays.
4. Select the [link](#) to review the comprehensive tutorial on creating a SAML-based SSO in Microsoft Entra ID.
5. Copy and paste the **Identifier** link and **Reply URL** link in Entra ID per the instructions in the tutorial.

Entra ID creates a Login URL and Microsoft Entra ID Identifier.
6. Paste the **Login URL** and **Microsoft Entra ID Identifier** into their Universal ZTNA fields.
7. Upload the **SAML Signing Certificate** you downloaded from Entra ID.

The UI instructions explain how to upload the certificate.
8. (Optional) Select **All Domains** or **Custom** and enter the domain.

If you select **Custom**, fill in the approved domains. Applicable for network and application access.
9. Select **Validate Information**.

A message in the upper right corner confirms the validation test passed.
10. Select **Update**.

Update Identity Provider pop-up window displays. This message cautions you that the Identity Provider change logs out current users.
11. If you decide to continue, select **Confirm**.
12. Select **Next**.

The **Onboarding - Access Groups** window displays.
13. Configure [Users and Devices](#) on page 27.
14. Configure [Resources](#) on page 44.
15. Configure [Applications and Application Groups](#) on page 61.

You can skip this step if you are using Secure Network Access.
16. Configure [Policies](#) on page 68.

Google Workspace

Google Workspace is a collection of identity and access management tools. It allows companies to allocate and manage user accounts efficiently, enforce multi-factor authentication, enable single sign-on and OAuth 2.0, and govern access to applications and services under one platform.

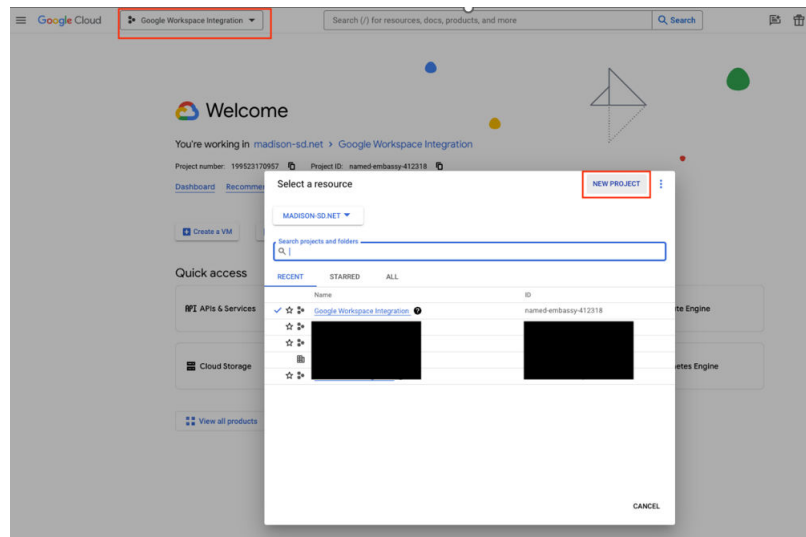
Google Workspace offers two types of Single Sign-on (SSO) methods:

- **OpenID Connect:** This open authentication protocol works on top of the Open Authorization (OAuth) 2.0 framework
- **Security Assertion Markup Language (SAML):** This is an open standard for exchanging authentication and authorization data between an identity provider and a service provider

Set up Google Workspace with Open ID Connect

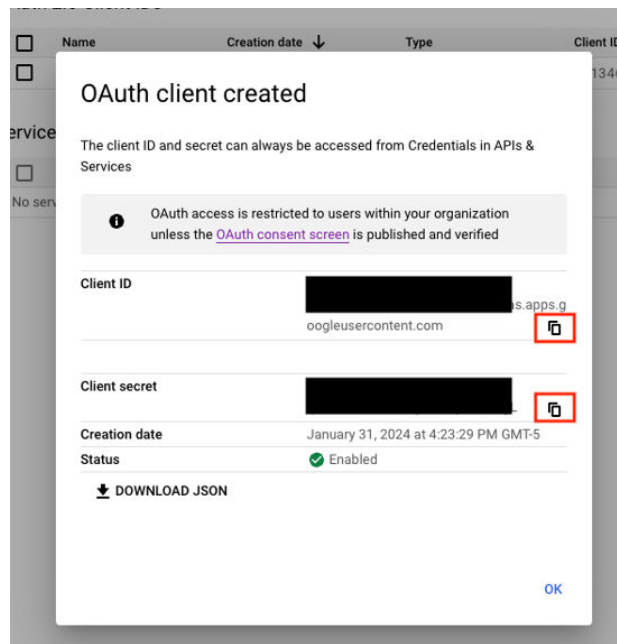
Use this task set up Google Workspace with Open ID Connect (OIDC) in Google Cloud (GCP).

1. Log in to Google Cloud using <https://console.cloud.google.com>.
2. To create a new project:
 - a. From the drop-down menu at the top of the screen, select **NEW PROJECT**.



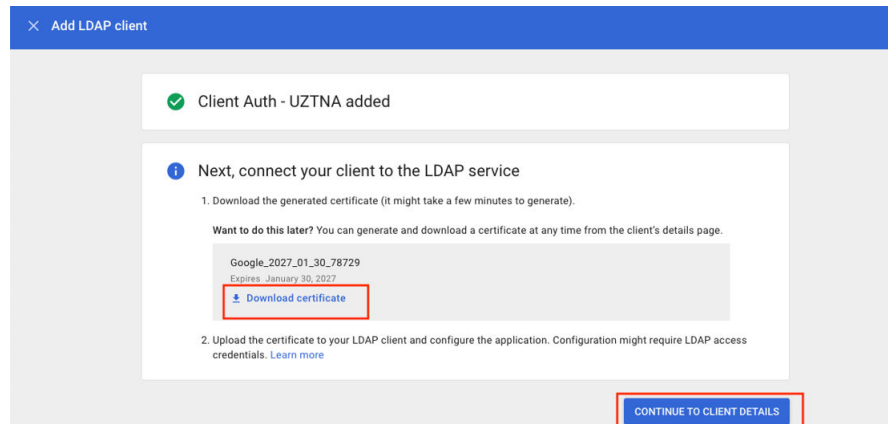
- b. Enter a name in the **Project Name** field and select **CREATE**.
- c. Select the newly created Project and under the **Quick Access** menu, select **APIs & Services**.
- d. Go to **OAuth consent screen**.
- e. Under **User Types**, select the **Internal** radio button and select **CREATE**.
- f. In the **App Information** section, enter the App Name, select a User support email from the drop-down list.
- g. In the **Developer contact information** section, enter an email address and select **SAVE AND CONTINUE**.
- h. On the **Scopes** screen, make no updates and select **SAVE AND CONTINUE**.
- i. On the **Summary** screen, to complete the configuration, select **BACK TO DASHBOARD**.

3. To create new API credentials:
 - a. Go to **Credentials**, and select **CREATE CREDENTIALS**.
 - b. Select **OAuth client ID** from the available options.
 - c. On the **Create OAuth client ID** screen, select **Web application** from the Application type drop-down list, and enter a name for the OAuth client.
 - d. From the **Universal ZTNA Identity Provider** screen, copy the two Redirect URIs from the **Set up Redirect URIs** section and enter them in the **Authorized redirect URIs** section in Google Workspace.
 - e. Select **CREATE**.
The system displays and **OAuth client created** dialog.
 - f. Copy the Client ID and Client secret to use in Universal ZTNA.



- g. On the **Universal ZTNA IDP Configuration** screen, in the **Setup Extreme Cloud ZTNA** section, enter in the saved Client ID and Client Secret.
- h. Select **Validate Information** to check to confirm that the information is valid.
- i. Once the information is successfully validated, select **Update** to apply the integration.
To configure the integration to be able to authenticate users against Google Workspace, a Secure LDAP Configuration must be added to Google.
4. To add a secure LDAP configuration to Google:
 - a. Log in to the admin portal for Google workspace.
 - b. Go to **APPS > LDAP**.
 - c. Select **ADD CLIENT**.
The system displays the **Client Details** page.
 - d. Enter the LDAP client name and select **CONTINUE**.
The system displays the **Access Permissions** page.
 - e. Under **Verify user credentials**, select the **Entire domain** option.

- f. Under **Read user information**, select the **Entire domain** option.
- g. Select **ADD LDAP CLIENT**.
- h. Once the certificate is generated, select **Download certificate** and save it for use in Universal ZTNA.



- i. Select **CONTINUE TO CLIENT DETAILS**.
- j. By default, the LDAP client is not enabled. Under **Service Status**, select the drop-down option.
 The system displays the **Service Status** screen.
- k. To enable the LDAP client, select the **ON for everyone** option and select **SAVE**.
- l. On the **Identity Provider** page in Universal ZTNA, select the **Secure Access to Networks** check box and upload the previously saved certificate bundle (zip file).
- m. Select **Validate Information**.

Configure Google Workspace - OpenID Connect

Retrieve the **ClientID** and **Client Secret** from Entra ID.

Use this task to configure your identity provider (IdP) using Google Workspace - OpenID Connect.

1. Select **Onboarding**.
 The **Welcome** window displays.
2. Select **Secure Hybrid Access** [**Secure Application Access** or **Secure Network Access**].
 The **Secure Provider** window displays with ExtremeCloud Universal ZTNA.
3. Select **Next**.
 The **Onboarding** window displays.
4. Select **OpenID Connect** from the **Single Sign-On Method** drop-down list.
5. Follow the instructions under **Setup Redirect URI**.
6. Enter the **ClientID**.

7. Enter the **Client Secret**.**Note**

Redirect URLs are on the IdP set up page on the Universal ZTNA UI. You can copy and update redirect URLs in Google Workspace. In Google Workspace, specify the following URLs under the URI section. These URLs redirect the user to the Google Workspace portal after a successful authorization by Google Workspace during log-in and sign-up.

- `https://server URL/auth/api/v1/accounts/google/login/callback/`
- `https://server URL/auth/api/v1/accounts/invite/google/signup/callback/`

8. (Optional) Select **All Domains** or **Custom** and enter the domain.

If you select **Custom**, fill in the approved domains. Applicable for network and application access.

9. (Optional) Select **Secure Network Access**.**Note**

This option uses Secure LDAP with Google Workspace to enable secure network access in Universal ZTNA.

- Follow the instructions on the UI.
- Upload the certificate.

10. Select **Validate Information**.

A message in the upper right corner confirms the validation test passed.

11. Select **Update**.

Update Identity Provider pop-up window displays. This message cautions you that the Identity Provider change logs out current users.

12. If you decide to continue, select **Confirm**.13. Select **Next**.

The **Onboarding - Access Groups** window displays.

14. Configure [Users and Devices](#) on page 27.15. Configure [Resources](#) on page 44.16. Configure [Applications and Application Groups](#) on page 61.

You can skip this step if you are using Secure Network Access.

17. Configure [Policies](#) on page 68.*Google Workspace - SAML*

Retrieve the **SSO URL** and **Entity ID Identifier** from Google Workspace.

This task shows you how to configure your identity provider using Google Workspace - SAML.

1. Select **Onboarding**.

The **Welcome** window displays.

2. Select **Secure Hybrid Access** [**Secure Application Access** or **Secure Network Access**].

The **Identity Provider** window displays with ExtremeCloud Universal ZTNA.

3. Select **Next**.
The **Onboarding** window displays.
4. Select [link](#) to review the comprehensive tutorial on creating a SAML-based SSO in Google Workspace.
5. Follow the ExtremeCloud Universal ZTNA instructions.
6. Enter the **SSO URL**.
7. Enter the **Entity ID Identifier**.
8. Upload the **SAML Signing Certificate** you downloaded from Entra ID.
The UI instructions explain how to upload the certificate.
9. Follow the **Configure Service Provider Details** instructions.
10. Follow the **Attribute Mapping** instructions.
11. Select **Secure Network Access > Sync Users > User Groups**.
12. (Optional) Select **All Domains** or **Custom** and enter the domain.
If you select **Custom**, fill in the approved domains. Applicable for network and application access.
13. Select **Validate Information**.
A message in the upper right corner confirms the validation test passed.
14. Select **Update**.
Update Identity Provider pop-up window displays. This message cautions you that the Identity Provider change logs out current users.
15. If you decide to continue, select **Confirm**.
16. Select **Next**.
The **Onboarding - Access Groups** window displays.
17. Configure [Users and Devices](#) on page 27.
18. Configure [Resources](#) on page 44.
19. Configure [Applications and Application Groups](#) on page 61.
You can skip this step if you are using Secure Network Access.
20. Configure [Policies](#) on page 68.

Microsoft Active Directory Federated Services (AD FS)

Network administrators manage permissions and control access to network resources using the Microsoft Active Directory Federated Services directory service. Active Directory uses objects categorized by their names and attributes to store users, groups, applications, and device data.



Note

Synchronizing Users and User Groups is not supported with AD FS.



Note

Inbound web access through the firewall to the AD FS server is required for application and network authentication to function.

Microsoft AD FS offers two types of SSO methods.

- **OpenID Connect (OIDC):** This open authentication protocol works on top of the Open Authorization (OAuth) 2.0 framework.

For more information on OIDC SSO, see [Set up Microsoft Entra ID with Open ID Connect Integration](#) on page 30.

- **Security Assertion Markup Language (SAML):** This is an open standard for exchanging authentication and authorization data between an identity provider and a service provider.



Note

Secure Network Access is not supported with SAML 2.0.



Note

Secure Network Authentication is not supported with SAML 2.0.

For more information on SAML Connect SSO, see [Configure Microsoft Entra ID - SAML](#) on page 35.

Configure Microsoft AD FS - OpenID Connect

Follow this procedure to configure a Microsoft Active Directory Federated Services - OpenID Connect Identity Provider.

1. Select **Onboarding**.

The **Welcome** window displays.

2. Select **Secure Hybrid Access** [**Secure Application Access** or **Secure Network Access**].

The **Identity Provider** window displays with ExtremeCloud Universal ZTNA selected.

3. Select **Microsoft Active Directory Federated Services** and **Continue**.

Microsoft Active Directory Federated Services window displays.

4. [Default] Confirm that **OpenID Connect** is selected for the **Single Sign-on Method**.

5. Follow the **Setup Redirect URIs** instructions.

6. Enter the data you created in Entra ID into the following fields:

- a. Enter the **Client ID**.
- b. Enter the **Client Secret**.
- c. Enter the **Discovery URL**.

7. (Optional) Select **All Domains** or **Custom** and enter the domain.

If you select **Custom**, fill in the approved domains. Applicable for network and application access.

8. Select **Secure Network Access**.



Note

Specify the **Client ID**, **Client Secret** and **Discovery URL**.

9. Select **Validate Information**.

A message in the upper right corner confirms the validation test passed.

10. Select **Update**.

Update Identity Provider pop-up window displays. This message cautions you that the Identity Provider change logs out current users.

11. If you decide to continue, select **Confirm**.

12. Select **Next**.

The **Onboarding - Access Groups** window displays.

13. Configure [Users and Devices](#) on page 27.

14. Configure [Resources](#) on page 44.

15. Configure [Applications and Application Groups](#) on page 61.

You can skip this step if you are using Secure Network Access.

16. Configure [Policies](#) on page 68.

Configure Microsoft AD FS - SAML

Use this task to configure your identity provider (IdP) with Microsoft Active Directory Federated Services (AD FS) - SAML.

1. Select **Onboarding**.

The **Welcome** window displays.

2. Select **Secure Hybrid Access** [**Secure Application Access** or **Secure Network Access**].

The system displays the **Identity Provider** window with ExtremeCloud Universal ZTNA selected.

3. Select **Next**.

The **Onboarding** window displays.

4. Select the [Link](#) to review the comprehensive tutorial on creating a SAML-based SSO in Microsoft AD FS.

5. Copy and paste the **Identifier** and **Reply URL** links in Entra ID as per instructions in the tutorial.

Entra ID creates a Login URL and Microsoft AD FS Identifier.

6. Paste the **Login URL** and **Microsoft AD FS Identifier** into their Universal ZTNA fields.

7. Upload the **SAML Signing Certificate** you downloaded from Entra ID

The UI instructions explain how to upload the certificate.

8. (Optional) Select **All Domains** or **Custom** and enter the domain.

If you select **Custom**, fill in the approved domains. Applicable for network and application access.

9. Select Secure Network Access network.

10. Select **Update**.

Update Identity Provider pop-up window displays. This message cautions you that the Identity Provider change logs out current users.

11. If you decide to continue, select **Confirm**.

12. Select **Next**.

The **Onboarding - Access Groups** window displays.

13. Configure [Users and Devices](#) on page 27.

14. Configure [Resources](#) on page 44.
15. Configure [Applications and Application Groups](#) on page 61.
You can skip this step if you are using Secure Network Access.
16. Configure [Policies](#) on page 68.

Change the Identity Provider

Use this task to change your Identity Provider (IdP) once onboarding is complete.

1. Go to **IAM > Identity Provider**.
2. Select **Disconnect Identity Provider**.
The **Disconnect Identity Provider** pop-up window displays.
3. (Optional) Clear **Re-authenticate all the environment users** if you do not want to re-authenticate users accessing applications or networks.
When users are not re-authenticated before disconnecting the IdP, they are active until the re-authentication interval times out.
4. Select **Initiate Assessment**.



Caution

Failure to address the recommendation could lead to instability in your network.

5. Select **Update Policy** or **Remove Policy**.
Updating a policy means you are changing the user group to local.
The **Disconnect IdP: Cleaning Assessment** pop-up window displays.
6. Select **Cleanup & Disconnect**.

The **Identity Provider** window displays. This is the confirmation that the Identity Provider was successfully disconnected. See [Identity Provider](#) to add a new one.



Resources

- [Add Sites](#) on page 45
- [Add a Site Group](#) on page 46
- [Deploy RadSec Proxies](#) on page 46
- [Deploy Service Connectors](#) on page 47
- [View RADIUS Servers](#) on page 49
- [Manage Network Resources](#) on page 49
- [Certificate Management](#) on page 54
- [Manage DNS Servers](#) on page 59
- [Add a DNS Policy](#) on page 60

Use these required resources for onboarding using Secure Hybrid Access:

- **Sites** enable you to define your virtual or physical network boundaries. Sites are synchronized using ExtremeCloud IQ and in general should be created and managed using that interface. To manage a site, see [Add Sites](#) on page 45.
- **Deploy Service Connector** enables you to add secure application access over encrypted protocols. For more information on Service Connectors, see [Deploy Service Connectors](#) on page 47.
- **Deploy RadSec Proxy** ensures RADIUS communications over untrusted networks. For more information on RadSec Proxies, see [Deploy RadSec Proxies](#) on page 46.

These are two required tasks to set up resources for Secure Application Access:

- **Service Connector Location** enables you to add and manage network sites by defining your virtual and physical network boundaries. A site can contain one or more service connectors. The same site is global and can be used for other places in Universal ZTNA to define boundaries
- **Deploy Service Connector** allows you to select an encryption protocol such as IPsec or WireGuard and deploy a service connector on the customer premises such as private data center or public cloud (AWS, Entra ID, GCP) managed by tenant admin.

Use these optional resources for onboarding using Secure Network Access:

- **RadSec Proxy Location:** A site can contain none, one, or more RadSec proxies. The same site is global and can be used for other places in Universal ZTNA to define boundaries
- **Deploy RadSec Proxy:**
 - For network devices (switches/AP) that cannot do RadSec, the RadSec Proxy secures RADIUS traffic into a secure Transport Layer Security (TLS) tunnel

- The RadSec Proxy server forwards an auth-request to the RADIUS server and another auth-request back to the switch or access point

Once the onboarding is complete, you can access additional resources:

- **RADIUS Server** enables authentication for remote access. For more information, see [View RADIUS Servers](#) on page 49.
- **Network Resources** enables you to manage Network Devices, SSIDs, and RADIUS Template. For more information, see [Manage Network Resources](#) on page 49.
- **Certificate Management** enables you to manage Trusted Root, RADIUS server, and intermediate certificates. For more information, see [Certificate Management](#) on page 54.
- **DNS** enables you to manage DNS servers and policies. For more information, see [Manage DNS Servers](#) on page 59 or [Add a DNS Policy](#) on page 60.

Add Sites

Use this task to add and manage network sites by defining virtual or physical network boundaries.





Note

Sites created in ExtremeCloud IQ are leveraged in ExtremeCloudUniversal ZTNA. Sites should be managed from ExtremeCloud IQ whenever possible.

1. Go to **Resources > Sites**.
2. Select **Add Site** and configure the settings.

Table 7: Site Configuration Settings

Field	Description
Site Name	Enter a name for the site.
Description (Optional)	Enter a description.
Associations (Optional)	Select an association from the drop-down list.
Country	Select a country from the drop-down list.

3. Select **Add**.
The system displays a list of sites.
4. To edit an existing site, select  within the table and select **Edit**.
 - a. Update the **Site Name**, **Description**, **Associations**, **Country**, or **Address**.
 - b. Select **Update**.
5. To delete an existing site, select  within the table and select **Delete**.

Add a Site Group

Use this task to add a site group.



Note

Site groups created in ExtremeCloud IQ are leveraged in ExtremeCloudUniversal ZTNA. Site groups should be managed from ExtremeCloud IQ whenever possible.

1. Go to **Resources > Sites**.
2. Select **Add Site Group** and configure the settings.

Table 8: Site Group Configuration Settings

Field	Description
Site Group Name	Enter at least three alphanumeric characters.
Description (Optional)	Enter a description.
Associations (Optional)	Select an association from the drop-down list.

3. Select **Add**.
The system displays a list of site groups.

Deploy RadSec Proxies

A RadSec Proxy is only required when the network switch or AP does not support native RadSec. This is specifically applicable to 3rd party devices. Any Extreme Universal switch or ExtremeCloud IQ Access Point supports native RadSec and should be connected in that way as a best practice.

Follow these recommendations:

- **Packaged deployment:**
Recommended OS
Ubuntu 20.04 or 22.04
VMware OVA
- **Port availability:** The following ports need to be allowed outbound from the RadSec proxy:
 - **RadSec Port:** 2083, 443
- **Minimum hardware requirements:** CPU: 2 Ram: 4 GB

This task shows you how to deploy RadSec Proxies to implement secure authentication on non-RadSec protocol compatible devices.

1. If deploying a RadSec Proxy during onboarding, select the **Deploy RadSec Proxy** tab.
If deploying a RadSec Proxy outside of onboarding, select **Resources > RadSec Proxy** from the navigation pane on the left.

2. Select **Deploy RadSec Proxy**.
 - a. Read the Guidelines and configure the settings.

Table 9: RadSec Proxy Configuration Settings

Field	Description
RadSec Proxy Name	Enter at least three alphanumeric characters.
Associate Site	Select an existing site or create one.
Certificate Rotation Time	Enter the number of days until the next rotation.
Shared Secret	You can update the text field with a value between 3 and 32 characters in length. This shared secret will be used with network devices authenticating via RADIUS to the RadSec Proxy.

- b. Select **Next**.
- c. Select the deployment mode and follow the installation procedure shown.
- d. Read the information and follow the installation procedure for the host machine.
- e. Select **Done**.

The new proxy displays in the RadSec Proxy list with the **Ready to Install** status.

3. Go to your host machine and perform the installation using the guidelines provided.

Your proxy should come into service after waiting a short period, and display the **UP** status.

To update an existing RadSec Proxy, select . From this menu you can do the following:

- Connect Devices
- Update Now
- Sync Now
- Remove

Deploy Service Connectors

Follow these recommendations:



Note

When Secure Socket Layer (SSL) decryption is in use, the traffic does not pass through the service connector.

- **Packaged deployment:**

Recommended OS

Ubuntu 20.04 or 22.04

VMware OVA

- **Dockerized deployment:** Compatible with multiple operating systems; requires only Docker to be installed.

- **Port availability:** The following ports need to be allowed outbound from the RadSec proxy:
 - **WireGuard Encryption Protocol:** 51820
 - **IPsec Encryption Protocol:** 500, 4500
- **Dockerized deployment:** compatible with multiple operating systems; requires only Docker to be installed.
- **Port Availability** - If the connector and the user are in the same network, open the following ports for outbound requests:

**Note**

ARM based installations are not supported.

- **WireGuard Encryption Protocol:** 51820
- **IPsec Encryption Protocol:** 500, 4500
- **Minimum hardware requirements:** CPU: 2 Ram: 4 GB

Use this task to deploy a service connector which:

- Connects to private, cloud-hosted application services and facilitates secure data exchange between the user and these application services
 - Performs data transformation and routing between the user and application services
 - Can be hosted in private data center or public cloud such as AWS, Entra ID, and GCP
1. If deploying a Service Connector outside of the onboarding process, go to **Resources > Service Connectors** from the navigation pane on the left, if not go to the **Deploy Service Connector** tab.
 2. Select **Deploy Service Connector > Private Hosted** from the drop-down on the right.
 - a. Read the Guidelines.
 - b. Select **Next** to configure the connector.

The **Deploy Private Hosted Service Connector** pop-up window displays.
 - c. For the **Connector Name**, enter at least three alphanumeric characters
 - d. Select an existing site or add a site for **Associate Site**.
 - e. Enter a size for **Set MTU** (Maximum Transmission Unit).

The MTU value is the maximum size of a data packet that an internet-connected device can accept in bytes. The MTU size ranges from 1300 to 1500 bytes.
 - f. Select **Next**.
 - g. Review your configuration.
 - h. Select **Deploy**.
 - i. Read the information and follow the deployment procedure for the service connector.
 - j. Select **Close**.

When deployment finishes, the service connector status turns green and displays **Up**.

Your enterprise applications and networks are now securely accessible to the service connector.

Once you have completed the resources part of the onboarding, you can continue to [Applications and Application Groups](#) on page 61.

View RADIUS Servers

Use this task to view RADIUS servers in your environment.



Note

To manage RADIUS servers for ExtremeCloud IQ Controller or ExtremeCloud IQ Site Engine, see the associated user guides from <https://supportdocs.extremenetworks.com/support/documentation/>.

1. Select **Resources** > **RADIUS Server**.
The following displays:
 - Fully Qualified domain Name (FQDN)
 - IP Address
 - Port
 - Secret
 - Region
2. To display more pages, select the right arrow at the bottom of the screen.
3. To refresh the screen, select

Manage Network Resources

Go to **Resources** > **Network Resources** to manage Network Resources which consists of three sections, Network Devices, SSIDs, and RADIUS Template.

The Network Devices section contains a list of your network devices, their current policy, and sync status.



Note

This list will include all devices currently in ExtremeCloud IQ.

From the top-right menu, you can select:

- [Import Devices](#)
- Resync All Devices
- [Global Timeout](#)

Within the Network Device table, you can select to perform actions depending on how the device was added to Universal ZTNA. The actions include:

- Download Certificate Bundle
- Sync Device
- Update
- Remove

To add a network device, see [Add a Network Device](#) on page 50.

The SSIDs section contains a list of all SSIDs known to ExtremeCloud Universal ZTNA. SSID are automatically added from ExtremeCloud IQ or can be manually added.

When enabling an ExtremeCloud IQ SSID to be managed, policies will be pushed to all Access Points that are broadcasting that SSID based on the location conditions defined.

When enabling BYOD on an SSID, an option appears in the Universal ZTNA Agent to automatically provision the wireless network profile for a client device. To add, manage, or remove an SSID, see [Manage SSIDs](#) on page 52.

The RADIUS Template section contains a list of RADIUS templates. You can add, clone, export, or import Radius templates. For more information, see [Manage RADIUS Templates](#) on page 53.

Add a Network Device

Use this task to add a network device to your resources.

1. Go to **Resources > Network Resources** and click **Add Network Device**.
2. Configure the settings for the new device:

Table 10: Network Device Configuration Settings

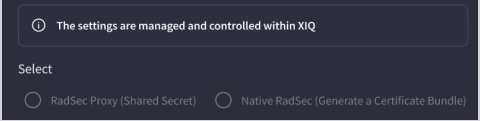
Field	Description
IP Address	Enter an IP address for your network device in the text field.
Alias (Optional)	Enter a network device alias.
RADIUS Template	Search for and select an existing RADIUS template from the drop-down menu.
Select	<ul style="list-style-type: none"> • RadSec Proxy (Shared Secret) - If you select RadSec Proxy (Shared Secret), enter the Shared Secret into the associated text field. • Native RadSec (Generate a Certificate bundle) - If you select Native RadSec (Generate a Certificate bundle), the Create a certificate bundle check box appears pre-selected. 
Type	Select Wired or Wireless from the network device Type drop-down list.
Sites	Search and select an existing site from the Sites drop-down menu.

Table 10: Network Device Configuration Settings (continued)

Field	Description
Session Timeout for Device (Optional)	If 'Use Global Timeout' is selected, this option is disabled. If an individual session timeout for the device is required, disable 'Use Global Timeout'.
Use Global Timeout	To set an individual session time out for this device, de-select this option and set the desired session timeout in the above field.

3. Click **Add**.

Import a Network Device

Use this task to import a list of network devices.


1. Go to **Resources > Network Resources**.
2. Select , and select **Import Devices** and configure the settings.

Table 11: Configuration Settings for Importing Network Devices

Field	Description
RADIUS Template	Select a RADIUS template from the drop-down list.
Shared Secret (Optional)	For RadSec Proxy, provide a Shared Secret in the field. For Native RadSec, download the certificate from the device menu by navigating to network devices.
Sites	Select a site from the drop-down list that is associated with the imported devices.
Template Upload	Download the csv template and fill in your network device information. Drag and drop or browse to your csv file.

3. Select **Import**.

Enable Global Timeout

Use this task to enable global timeout for network devices. Modifying the Global Timeout will apply to all network resources using Global Timeout.

1. Go to **Resources > Network Resources**.

2. Select , and select **Global Timeout** and configure the settings.

Table 12: Global Timeout Configuration Settings

Field	Description
Seconds	Enter the number of seconds for global timeout. Note: Recommended session timeout is 3600 seconds.
Override and apply to all custom/individually set timeouts.	Select this check box to apply to all.


3. Select **Update**.

Configure SSID and Wireless

Service Set Identifier (SSID) configuration in ExtremeCloud IQ depends on the type of authentication (802.1X or MAC) and the type of RadSec deployed.

Universal ZTNA RadSec is supported in all SSID types except for Private Pre-Shared Key SSIDs.

Use this task to configure SSID and wireless in ExtremeCloud IQ.

1. Go to **Configure > Common Objects > Policies > SSIDs**.
2. Select  to create a new SSID.
3. Enter a username and broadcast name.
4. Under **SSID Usage**, ensure the **SSID Authentication** and **Enterprise** tabs are selected.
5. (Optional) To enable MAC authentication toggle to **ON**.
6. Under **Authentication Settings**, enable **Authentication with ExtremeCloud Universal ZTNA**.

Manage SSIDs



Use this task to add, manage, or remove an SSID.

1. Go to **Resources > Network Resources**.
2. Select the **SSID** tab.
3. Select **Add SSID** and configure the settings.

Table 13: SSID Configuration Settings

Field	Description
Name	Enter at least three alphanumeric characters.
Broadcast Name	Enter a broadcast name.

4. Select **Add**.
The system displays existing SSIDs.

5. To manage preferences for an existing SSID, select  within the table and select **Manage SSID**.
6. To remove an existing SSID, select  within the table and select **Remove**.

Manage RADIUS Templates



Note

It is recommended that a RADIUS Template be created by cloning (step 3) an existing template and adjusting the necessary values. However, if a new template is desired it can be added using steps 4-5.

Use this task to add or clone a RADIUS template. To import an existing template, see [Import a RADIUS Template](#) on page 54.


1. Go to **Resources > Network Resources**.
2. Select the **RADIUS Template** tab.
3. To clone an existing RADIUS template, within the column associated with the template to clone, select  and select **Clone**.
 - a. Enter a **Name** and **Description** for the cloned template.
 - b. Select RADIUS VSA's from the drop-down list.
 - c. Variables in the drop-down list correspond to the elements of a network policy. Select the matching variables to assign to the RADIUS VSA.
 - d. Select **Clone**.
4. To add a new template, select **Add RADIUS Template** and configure the settings.

Table 14: RADIUS Template Configuration Settings

Field	Description
Name	Enter at least three alphanumeric characters.
Description	Enter a description.
RADIUS VSA'S	Select RADIUS VSA's from the drop-down list.
Variables	Variables in the drop-down list correspond to the elements of a network policy. Select the matching variables to assign to the RADIUS VSA.


5. Select **Add**.

Import a RADIUS Template

Use this task to import a RADIUS template.



Note

Export an existing RADIUS Template to retrieve the proper format. To export an existing RADIUS template, within the column associated with the template to clone, select  and select **Export**.

1. Go to **Resources** > **Network Resources** and select the **RADIUS Template** tab.
2. Select **Import**.
3. Drag and drop your template or select **Browse Files**.
4. Once you have chosen or added a file, select **Import**.

Certificate Management

Go to **Resources** > **Certificate Management**. The **Certificate Management** page is divided into four sections CA Trusted Root Certificates, Server and Intermediate Certificates, Matching Criteria for Clients, and Connecting with OSCP Responder.

CA Trusted Root Certificates

Within this section update and download CA Trusted Root and Intermediate Certificates. For more information, see [Manage CA Trusted Root Certificates in Universal ZTNA](#) on page 56.

Matching Criteria for Clients

Select the client certificate attribute that Universal ZTNA should examine to detect the username (an email address). For more information, see [Match Criteria for Clients](#) on page 58.

Connecting with OSCP Responder

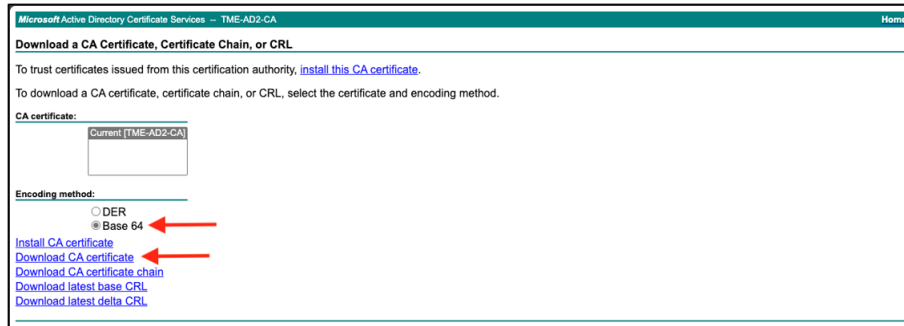
Provide the OSCP responder server's URL or endpoint for checking the validity or revocation status of a specific digital certificate. For more information, see [Connect with OSCP Responder](#) on page 59.

Windows Certificate Authority: Retrieve the CA (Root) Certificate

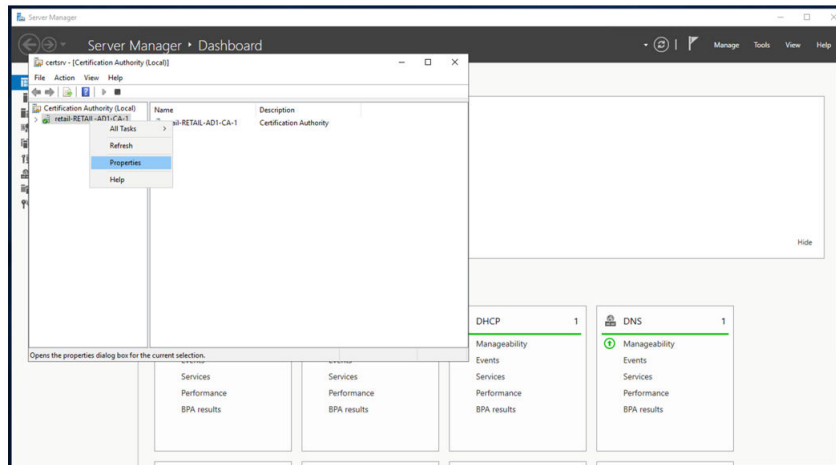
When setting up certificates in Universal ZTNA you must download the CA certificate also known as the root certificate from the certificate authority so that it can be uploaded into Universal ZTNA. Navigate to the domain controller certificate services site.

1. Go to Microsoft Active Directory Certificate Services: **https://<certificatedomain>/certsrv**.
2. Select **Download a CA certificate, certificate chain, or CRL**.

- Under **Encoding method**, select the **Base 64** option and select **Download CA certificate**.



- If web-based certificate services are not enabled, you can open the Certification Authority window from Server Manager on the Active Directory machine, right-click on the CA and select **Properties**.



- Under the **General** tab, select **View Certificate**.
- Under the **Details** tab, select **Copy to File**.
The system displays the **Certificates Export Wizard**.
- In the **Export File Format** section, select the **Base-64 encoded X.509** option and select **Next**.
- In the **File to Export** section, under **File name**, select **Browse**.
- Navigate to a directory where the file will be saved, enter an appropriate name, and select **Save**.
- To complete the process, select **Next**.

The file will be downloaded with a **.cer** extension.



Note


Before the file can be uploaded you must rename the file with a **.pem** extension.

To upload the certificate to Universal ZTNA, go to [Manage CA Trusted Root Certificates in Universal ZTNA](#) on page 56.

Manage CA Trusted Root Certificates in Universal ZTNA

Retrieve the CA certificate also known as the root certificate from the certificate authority to upload into Universal ZTNA. For more information, see [Windows Certificate Authority: Retrieve the CA \(Root\) Certificate](#) on page 54.

Use this task to update or download certificates.

1. Go to **Resources > Certificate Management**.
2. To update a CA Trusted Root & Intermediate certificate, select  and select **Update Certificate** from the drop-down menu.



Note

After a successful validation and update of the CA certificate, active authentication sessions will continue to function. However, for all new connections, the handshake process will occur using the new CA certificate.

3. Drag and drop or browse for your file.
4. Select **Update**.

The system will validate the certificate format and show that it has been updated successfully.

5. To download a CA Trusted Root certificate, select  and select **Download Certificate** from the drop-down menu.

Once you have added the certificate within Universal ZTNA, go to [Configure the Server Certificate](#) on page 56.

Configure the Server Certificate

. Before you configure the Server Certificate, you must [Manage CA Trusted Root Certificates in Universal ZTNA](#) on page 56.

Before a Server Certificate can be requested, a Certificate Signing Request (CSR) needs to be generated on behalf of Universal ZTNA to be signed by the Certificate Authority or Intermediate Certificate Authority.

Use this task to create a SAN configuration file, and execute a command against that file to create a new certificate file as well as a new private key file with no password.

1. Access any Linux environment using SSH.
2. After accessing the machine, generate a key file using the following comment.

```
openssl genrsa -out serverkey.pem 2048
```
3. Use vi, vim, or another editor to create a file named **san.cnf**.

4. Edit the file and then copy in the text below.

Edit the **[dn]** and **[alt_names]** fields to reflect the current environment. Ensure that the FQDN and DNS name is reflective of the values shown in the **Resources > RADIUS Server** field section.

```
[ req ]
default_bits = 2048
prompt = no
default_md = sha256
distinguished_name = dn
req_extensions = req_ext

[ dn ]
CN = radius.va2-uz.extremecloudiq
emailAddress = remote_demo@extremenetworks.com
O = Extreme Networks
OU = Solutions Engineering
L = Salem
ST = New Hampshire
C = US

[ req_ext ]
subjectAltName = @alt_names

[ alt_names ]
DNS.1=radius.va2-uz.extremecloudiq.com
```

5. Save the file and then run the following command:

```
openssl req -new -key -serverkey.pem -out va2-uz-server.csr -config san.cnf
```

This command will create a **.csr** file to be used to create a new server certificate to be used along with the **serverkey.pem** file to update the server certificate in Universal ZTNA.

6. Go back to Microsoft Active Directory Certificate Services: <https://<domain name>/certsrv>.
7. Select **Request a Certificate** and **advanced certificate request**.
8. Copy the contents of the CSR file and paste it into the **Save Request** field.

9. Select **Web Server** from the template drop-down and select **Submit**.
10. Once complete, select **Base 64 encoded** and **Download Certificate**.

- The certificate request can also be made using powershell by issuing the following command:

```
certreq -submit -attrib "CertificateTemplate: WebServer" va2-uz-server.csr
```

- Go to Universal ZTNA, select **Resources > Certificate Management**.

- Within the **Server & Intermediate Certificates** section, select  and select **Update Certificate**.



Note


Both certificate and key files must be renamed be renamed using a **.pem** extension before being uploaded.

- Select **Certificate with Embedded Key** or **Certificate with Separate Key**.

- To upload the newly created certificate as well as the key file drag and drop or browse for the file.

- Select **Update**.

Validation of the certificate will take upwards of two minutes to complete. Once this is accomplished, clients should be able to connect using 802.1X EAP-TLS.

- To invalidate RADIUS server certificates, select  and select **Invalidate Certificate** from the drop-down menu.

Match Criteria for Clients

Before you match criteria for clients, go to [Configure the Server Certificate](#) on page 56.

Currently Universal ZTNA will authenticate user certificates using one of two specific formats. Use this task to select the client certificate attribute that Universal ZTNA should examine to detect the username (an email address).

- Go to **Resources > Certificate Management**.
- From the **Certificate Attribute for Username** field, select one of the three options:



Note

Universal ZTNA expects the Username to be an email address or a User Principal Name (UPN). Other values will be rejected.

- Subject Distinguished Name | Common Name - The **Subject** field of the certificate the **CN** or **Common Name** must contain the full email address of the client.
 - SAN | Email Address - The **SAN** or **Subject Alternative Name** must contain either an email attribute, or that attribute must contain the full email address of the client.
 - SAN | User Principal Name - The UPN must be the user's complete email address.
- If the username cannot be determined by the Matching Criteria, define the action to be performed. In Universal ZTNA you can select the **Reject Authentication Request** or leverage the username value from the RADIUS Request and select **Match with RADIUS Username**.

4. Select **Update**.

Once you have matched the client criteria, go to [Connect with OCSP Responder](#) on page 59.

Connect with OCSP Responder

Use this provide the OCSP responder server's URL or endpoint for checking the validity or revocation status of a specific digital certificate.

1. Go to **Resources > Certificate Management**.
2. To validate certificates, put a check mark in the **Validate Certificate via OCSP** check box.
3. In the **Enter URL** field, enter the responder server's URL or endpoint.
4. Select **Update**.


Manage DNS Servers


Use this task to add, update, or remove Domain Name Systems (DNS) servers.

1. Select **Resources > Domain Name Systems**.
The **DNS** window displays.
2. Select **Add DNS Server** and configure the settings.

Table 15: DNS Configuration Settings

Field	Description
Server Name	Enter at least three alphanumeric characters.
IP Address	Enter an IP address.
Service Connector	Select a service connector from the drop-down list.

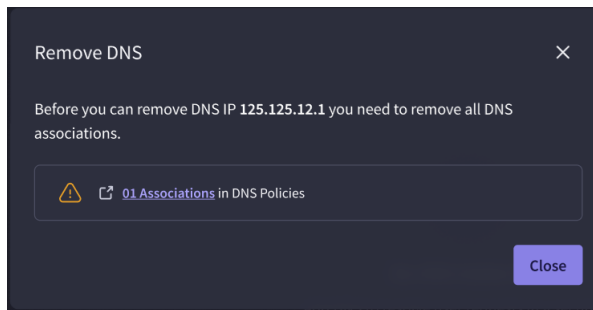
3. Select **Add**.
Next, you will see a sequence of screen updates while Universal ZTNA works to bring the DNS server up.
 - a. A connectivity test runs.
 - b. If the test passes, a confirmation message displays at the top of the window.
 - c. Your server displays in the server list.
 - d. The **Status** column displays **Activating**.
 - e. The **Status** changes to **Up** when the server is in service.
4. To update an existing DNS server, select  and select **Update** from the drop-down list.

- To remove an existing DNS server, select  and select **Remove** from the drop-down list.



Note

Before removing a DNS server, you must remove all associations.



Once you have onboarded your resources, go to [Applications and Application Groups](#) on page 61.

Add a DNS Policy

Use this task to add a DNS policy.

- Go to **Resources > Domain Name System**.
The **DNS** window displays.
- Select the **DNS Policies** tab.
- Select **Add DNS Policy** and configure the settings.

Table 16: DNS Policy Configuration Settings

Field	Description
Policy Name	Enter at least three alphanumeric characters.
Location-Based Conditions	Select a location-based conditions from the drop-down list.
Primary DNS	Select a DNS Type, Public or Private and enter an IP Address.
Secondary DNS (Optional)	Select a DNS Type, Public or Private and enter an IP Address.

- Select **Add**.



Applications and Application Groups

- [Add Private Web Applications](#) on page 61
- [Add Multi-Cloud Web Applications](#) on page 62
- [Add Custom Applications](#) on page 62
- [Add Terminal Access Applications](#) on page 63
- [Add Remote Desktop Applications](#) on page 63
- [Manage Application Discovery](#) on page 64
- [Create Application Groups](#) on page 64

Integrating your site infrastructure with ExtremeCloud Universal ZTNA ensures secure access to your enterprise applications. There are five application categories. Each one is optional, and you can add them in any order. The application types are:

- [Add Private Web Applications](#) on page 61
- [Add Multi-Cloud Web Applications](#) on page 62
- [Add Custom Applications](#) on page 62
- [Add Terminal Access Applications](#) on page 63
- [Add Remote Desktop Applications](#) on page 63

Application groups are created that combine similar applications policies to be leveraged within a single application or hybrid policy. Therefore, any policy added to the application group automatically applies to all the applications within the group.


Add Private Web Applications

Use this task to add web applications.

1. Go to **Applications > Applications**.
2. Select **Add Application** and configure the settings. select **Private Web App**.

Field	Description
Application Name	Enter at least three alphanumeric characters.
Application Type	Select Private Web App from the drop-down list.
Associated Site	Select a site or create a new one.
Associate Service Connector	Select a connector or create a new one.

3. Select **Next** if you are in the onboarding workflow, if not select **Add**.
The **Add Application - Application Info** pop-up window displays.

4. Enter the complete URL (e.g., <https://<website>.com>).
5. Select **Add**.
This step can take up to a minute to complete as it tests the application connectivity. When it does, the application's status is **Up**.
6. To remove an existing application, select  and select **Remove**.

Related Topics

[Add Terminal Access Applications](#) on page 63

[Add Remote Desktop Applications](#) on page 63

Add Multi-Cloud Web Applications

Use this task to add multi-cloud web applications.

1. Go to **Applications > Private Hosted Applications**
2. Select **Add Application**, and configure the settings.

Table 17: Multi-cloud Web Application Configuration Settings

Field	Action
Application Name	Enter a name for the application.
Application Type	Select Multi-Cloud Web App .
Associated Site	Select an associated site or create a new site.
Associated Connector	Select an associated connector.
Cloud Hosting Provider	Select one of the following options: <ul style="list-style-type: none"> • AWS • AZURE • GCP
Load balancer	Select a load balancer.

3. Select **Add**.

Add Custom Applications

Custom applications provide support for adding applications using customized TCP or UDP ports.

Use this task to add custom applications.

1. Select **Applications > Private Hosted Applications**.
2. Select **Add Applications** and configure the settings.

Table 18: Custom Applications Configuration Settings

Field	Action
Application Name	Enter a name for the application.
Application Type	Select Custom Application .

Table 18: Custom Applications Configuration Settings (continued)

Field	Action
Associated Site	Select an associated site or create a new site.
Protocol	Select UDP or TCP.
Hostname	Enter a hostname or IP address.
Port	Enter a port.

3. Select **Add**.

Add Terminal Access Applications

Use this task to add terminal access applications:

1. Go to **Applications > Applications**.
2. Select **Add Applications** and configure the settings.

Table 19: Terminal Access Configuration Settings

Field	Descriptions
Application Name	Enter at least three alphanumeric characters.
Application Type	Select Terminal Access from the drop-down list.
Associate Site	Select an existing site from the drop-down list or create a new site.
Associate Service Connector	Enter an associate service connector.
Application Info	<ul style="list-style-type: none"> • Under Protocol, select Secure Shell (SSH) or Telnet protocols. • Enter a Hostname (or IP Address). • Enter a port number.

3. Select **Add**.

The step can take up to a minute to complete as the application is tested for connectivity. The application will be displayed in the list when the procedure finishes showing the **UP** status.

Related Topics

[Add Private Web Applications](#) on page 61

[Add Remote desktop applications](#) on page 63

Add Remote Desktop Applications

Use this task to add remote desktop applications.

1. Under the **Applications** tab, select **Remote Desktop**.

2. Select **Add Applications** and configure the settings.

Table 20: Remote Desktop Configuration Settings

Field	Description
Application Name	Enter at least three alphanumeric characters.
Application Type	Select Remote Desktop from the drop-down list.
Associate Site	Select an existing site from the drop-down list or create a new site.
Associate Service Connector	Enter an associate service connector.
Application Info	<ul style="list-style-type: none"> • Under Protocol, select RDP or VNC. • For Hostname (or IP Address), enter the hostname or IP address. • Enter a port number.

3. Select **Add**.

The step can take up to a minute to complete as the application is tested for connectivity. The application will be displayed in the list when the procedure finishes showing the **UP** status.

Related Topics

[Add Private Web Applications](#) on page 61

[Add Terminal Access Applications](#) on page 63

Manage Application Discovery

Application Discovery allows access to all applications and can be used temporarily to help determine what application policies are needed for specific user groups. Use this task to enable application discovery.

1. Go to **Applications > Applications**.
2. Select **Enable Application Discovery** and enter a **Domain Name**.
3. Select **Enable Application Discovery**.



Note

This will allow all users, all subnets, on all ports effectively acting as a wide-open VPN.

4. Discovery will run for 30 days, to extend an additional 30 days up to a maximum of 90 days, select **Extend Application Discovery**, read the message, and select **Extend**.
5. To end Application Discovery, select **End Application Discovery**, read the message, and select **End Now**.

Create Application Groups

Use this task to create applications groups.

1. Go to **Application > Application Groups**.

2. Select **Create Application Group** and configure the settings.

Table 21: Application Groups Configuration Settings

Field	Description
Name of Application Group	Enter at least three alphanumeric characters.
Description (Optional)	Enter a group description.
Select Application	Select all the applications you want to add to your group.

3. Select **Create**.

Your application group displays in the list. You can also see the number of applications in your group.



Network Services

[Add Network Services](#) on page 66

[Create Network Service Groups](#) on page 66

Network Services are leveraged in Network and Hybrid policies to define network resources that should be allowed or denied via the policy. These are installed via ACL or firewall rules in the network device depending upon its capabilities.

Add Network Services

Use this task to add network services.

1. Go to **Networks Services > Network Services**.
2. Select **Add Network Service** and configure the settings.

Field	Description
Service Name	Enter at least three alphanumeric characters.
Protocol/IP Address	a. Select a protocol. b. Enter an IP address.
Ports (Optional)	Enter one or multiple ports separated by commas.

3. Select **Add**.

Your network displays in the network services list.

Create Network Service Groups

Use this task to create network service groups to share policies or rules with a set group of network services. A policy using this group applies to all network services defined in the group.

1. Go to **Network Services > Network Service Groups**.

2. Select **Create Network Service Group** and configure the settings.

Field	Description
Network Group Name	Enter at least three alphanumeric characters.
Description (Optional)	Enter a group description.
Add Network Service	Under Add Network Service , select Create New or Select Existing from the drop-down list.

3. Select **Create**.
4. To update or remove an existing Network Service Group, select  and select **Update** or **Remove** from the drop-down list.

Your network displays in the group list.



Policies

- [Create Hybrid Policy](#) on page 68
- [Create Application Policy](#) on page 70
- [Create Network Policies](#) on page 71
- [Update Application Discovery Policy](#) on page 73
- [Conditions](#) on page 74
- [Configure Device Posture](#) on page 77

Policies contain distinct conditions that provide different levels of authorization to your infrastructure.

You can search for or create the following three types of policies:

- [Hybrid Policy](#) allows you to manage your applications and network access.
- [Application Policy](#) allows you to manage only your applications.
- [Network Policy](#) allows you to manage only your network.



Note

To update the order of existing network policies, select and drag the policy into the desired order.

Create Hybrid Policy

Use this task to create a hybrid policy.

1. Go to **Policies > Policies**.
2. Select **Add Policy** and select **Hybrid** drop the drop-down list and configure the settings.

Table 22: Hybrid Policy Settings

Field	Description
Policy Name	Enter at least 3 alphanumeric characters.
Description (Optional)	Enter a description.
User Groups	Select Any User or select a user group from the drop-down list or create one. For more information, see Manage User Groups on page 27.

Table 22: Hybrid Policy Settings (continued)

Field	Description
Device Groups	<p>Select Any Device or select a device group from the drop-down menu or create one, for details, see Managed Device Groups on page 29.</p> <p>Note: If user and device groups are configured in the policy, for the policy to match for network access both access conditions must pass.</p>
Location Based Condition (Optional)	<p>Select a location condition from the drop-down menu or create a new condition.</p> <p>Note: Location group is also used to scope the network policies to only those network devices included in the location condition.</p> <p>For more information, see Add Location-Based Conditions on page 75</p>
Time Based Condition (Optional)	<p>Select a time condition from the drop-down menu or create a new condition, for details, see Add Time-Based Conditions on page 75.</p>
Authentication Based Condition (Optional)	<p>Select an authentication condition from the drop-down menu or create a new condition, for details, see Create Authentication-Based Conditions on page 76.</p>
Applications Groups	<p>Select one from the drop-down menu or create one, for details, see Create Application Groups on page 64.</p>
Access Mode	<p>Select Agent-based or Agentless to determine whether the applications defined in the application group should be available via the agent, the agentless web portal, or both.</p>
AP Aware	<p>Ability to determine AP attachment to port to prevent auth for wireless clients when Auth for wireless clients is handled via AP.</p>
Default Network Access	<p>Select the default access for the network. By default, all network access is dropped except for agent-based traffic.</p>

Table 22: Hybrid Policy Settings (continued)

Field	Description
Select VLAN from ExtremeCloud IQ	You can use your own VLAN or a VLAN defined in ExtremeCloud IQ . <ul style="list-style-type: none"> To use your own VLAN, ensure Select VLAN from ExtremeCloud IQ is deactivated (default) and enter a VLAN ID. To use a VLAN from ExtremeCloud IQ, activate Select VLAN from ExtremeCloud IQ and select a VLAN from the list
VLAN ID (Optional)	Select a VLAN from the drop-down menu.
ISID (Optional)	Fabric Service Identifier (ISID) .
Network Service Group (Optional)	Select Network Service Group and continue as follows: <ol style="list-style-type: none"> Select Add Network Service Group. Select Allowed or Denied. <p>Note: The Network Service groups, and their associated actions are ordered. To re-arrange the order, drag the network service group up or down.</p>
Advanced Settings (Optional)	<ul style="list-style-type: none"> Radius VSA's - Select from the drop-down menu. Variables - Select from the drop-down menu.

3. Select **Add**.

4. To update or remove an existing Hybrid policy, select  and select **Update** or **Remove** from the drop-down list.

Create Application Policy

Use this task to create an application policy.

- Go to **Policies > Policies**.
- Select **Create Policy**.
- Select **Add Policy** and select **Application** from the drop-down list and configure the settings.

Table 23: Application Policy Settings

Field	Description
Policy Name	Enter at least 3 alphanumeric characters.
Description (Optional)	Enter a description.

Table 23: Application Policy Settings (continued)

Field	Description
User Groups	Select Any User or select a user group from the drop-down list or create one. For more information, see Manage User Groups on page 27.
Location Based Condition (Optional)	Select a location condition from the drop-down menu or create a new condition, for details, see Add Location-Based Conditions on page 75.
Time Based Condition (Optional)	Select a time condition from the drop-down menu or create a new condition, for details, see Add Time-Based Conditions on page 75.
Applications Groups	Select one from the drop-down menu or create one, for details, see Create Application Groups on page 64.
Access Mode	Select Agent-based or Agentless to determine whether the applications defined in the application group should be available via the agent, the agentless web portal, or both.

4. Select **Add**.

Your application policy displays in the list showing the **Application Access** status as **Active**.

To update or remove an existing Application policy, select  and select **Update** or **Remove** from the drop-down list.

Related Topics

[Create Network Policies](#) on page 71

[Create Hybrid Policy](#) on page 68

Create Network Policies

Use this task to create a network policy.

1. Go to **Policies > Policies** and in the Network Policies tab, select **Add Policy > Network**.
2. Configure the following network policy settings:

Table 24: Network Policy Settings

Field	Description
Policy Name	Enter at least three alphanumeric characters for the name of the new network policy.
Description (Optional)	Enter a policy description.

Table 24: Network Policy Settings (continued)

Field	Description
<p>Conditions</p> <p>Note: All conditions are mutually exclusive.</p>	<p>Select desired conditions:</p> <ul style="list-style-type: none"> • Any User (Default) - If the default is not selected, search and select from the User Group(s) drop-down menu or create a new user group. • Any Device (Default) - If the default is not selected, search and select from the Device Group(s) drop-down menu or create a new device group. • Any Location (Default) - If the default is not selected, you can search, select, and edit from the optional Location-based Condition drop-down menu or create a new condition. • Any Time (Default) - If the default is not selected, search, select, and edit from the optional Time-based Condition drop-down menu or create a new condition. • Any Authentication Type (Default) - If the default is not select and edit from the optional Authentication-based Condition drop-down menu or create a new condition.

Table 24: Network Policy Settings (continued)

Field	Description
Network Access	<ul style="list-style-type: none"> • Default Access - Select the default access for the network. By default, all network access is dropped. • AP Aware - Enable this option to only authenticate the first MAC address connecting to the port of an Extreme Networks switch. The primary use case for this is an access point. All other MAC addresses will be authenticated by the access point. • Enter a VLAN ID or enable the switch to select an existing VLAN ID from ExtremeCloud IQ. Enter a Fabric Service Identifier if one is needed. • Network Service Group (Optional): <ul style="list-style-type: none"> ◦ Select Add Network Service Group. <p style="margin-left: 20px;">Note: Drag Network Service Groups in the order to respond within the RADIUS response.</p> <ul style="list-style-type: none"> ◦ Select Allow or Deny. <p>Note: In the Network Group table, select Revert Policy Order to reorder the columns.</p>
Advanced Settings (Optional)	<ul style="list-style-type: none"> • RADIUS VSA's - Select from the drop-down menu. • Variables - Select from the drop-down menu.

3. Select **Add**.

Your network policy displays in the list showing the **Network Access** status as **Active**.

To update or remove an existing Network policy, select  and select **Update** or **Remove** from the drop-down list.

Related Topics

[Create Application Policies](#) on page 70

[Create Hybrid Policy](#) on page 68

Update Application Discovery Policy

Application Discovery has been enabled in the system.

Use this task to update an Application Discovery policy.

1. Go to **Policies > Policies**.

2. Select **Add Policy** and select **Application Discovery Policy** from the drop-down list and configure the settings.

Table 25: Application Discovery Policy Configuration Settings

Field	Description
Policy Name	This will be automatically filled with App Discovery (temp policy) .
Description (Optional)	Enter a description.
User Groups	Select Any User or select a user group from the drop-down list or create one. For more information, see Manage User Groups on page 27.
Location Based Condition (Optional)	Select a location condition from the drop-down menu or create a new condition, for details, see Add Location-Based Conditions on page 75.
Time Based Condition (Optional)	Select a time condition from the drop-down menu or create a new condition, for details, see Add Time-Based Conditions on page 75.
Authentication Based Condition (Optional)	Select an authentication condition from the drop-down menu or create a new condition, for details, see Create Authentication-Based Conditions on page 76.
Application Groups	This drop-down list will default to Discovery (All Apps) .
Application Access	Select Agent-based or Agentless access mode. Note: By default, Agent-based or Agentless are checked when creating new policies.

3. Select **Update**.

Conditions

Conditions provide a distinct level of authorization to your infrastructure. Policy requirements regulate secure access to your enterprise applications and networks. There are three types of conditions:

- Location
- Time
- Authentication


Add Location-Based Conditions

Use this task to create location based conditions.

1. Select **Policies > Conditions**.
2. Select **Add Condition** and configure the settings.

Table 26: Location-Based Conditions Settings

Field	Descriptions
Condition Name	Enter at least three alphanumeric characters.
Description (Optional)	Enter a description of the condition.
User Geographic Location(s) (Optional)	Select one or more geographic locations from the drop-down list. Note: Geographic Location conditions are only applicable to Application Based Policies.
Network Location (Optional)	Select one of the following: If you select Site , select the existing sites from the drop-down list. <ul style="list-style-type: none"> • SSID - select the existing SSID from the drop-down list. Only SSIDs that are currently managed in the Network Resources > SSID view are listed. • Sites - select a site from the drop-down list. • Access Point - select the existing APs from the drop-down list. • Access Point & SSID - select the existing SSIDs and AP from the associated drop-down lists. • Switch - select the existing switches from the drop-down list.

3. Select **Add**.
4. To update or remove an existing location-based condition, select  and select **Update** or **Remove** from the drop-down list.

Your location condition displays in the list.

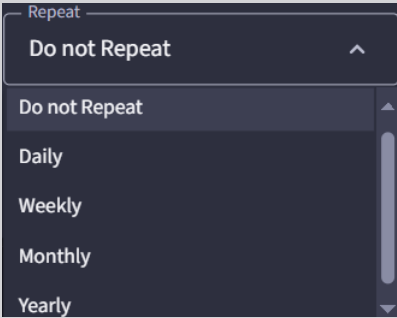
Add Time-Based Conditions


Use this task to create time-based conditions.

1. Select **Policies > Conditions**.
2. Select the **Time** tab at the top of the window.
The **Time Based Conditions** window displays.

3. Select **Add Condition** and configure the settings.

Table 27: Time-Based Conditions Settings

Field	Descriptions
Condition Name	Enter at least three alphanumeric characters.
Description (Optional)	Enter a description of the condition.
Select Time Zone	Select a time zone from the drop-down list.
Start Date	Select a start date with the Start Date calendar.
End Date	Select an end date with the End Date calendar.
Start Time	Select a start time with the Start Time clock.
End Time	Select an end time with the End Time clock.
Repeat	Under the Repeat drop-down list, select how often you want the condition to repeat. 

4. Select **Add**.
5. To update or remove an existing time-based condition, select  and select **Update** or **Remove** from the drop-down list.

Your time condition displays in the list.


Create Authentication-Based Conditions

Use this task to create authentication-based conditions.

1. Select **Policies > Conditions**.
2. Select the **Authentication** tab at the top of the window.
The **Authentication-Based Conditions** window displays.

3. Select **Add Condition** and configure the settings.

Field	Description
Condition Name	Enter at least three alphanumeric characters.
Description (Optional)	Enter a description of the condition.
Authentication Method	Select a method from the drop-down list or search for a method.

4. Select **Add**.
5. To update or remove an existing authentication-based condition, select  and select **Update** or **Remove** from the drop-down list.

Your authentication condition displays in the list.

Configure Device Posture

Device Posture checks the security data of connected devices and reduces the devices' cybersecurity risks by enforcing access controls and policies on those devices.

1. Go to **Policies > Device Posture** and configure settings.

Field	Description
Matching Criteria	Select a Matching Criteria from the drop-down list: <ul style="list-style-type: none"> • Allow when all match • Allow when some match
Posture Check Frequency	Select a Posture Check Frequency : <ul style="list-style-type: none"> • At the time of login • At the time of login and every <select the amount of time from the Select Time drop-down list.
Attributes	Select the Attributes you want to use: <ul style="list-style-type: none"> • Anti-virus and Anti-malware — For desktop agents installed on Windows OS only. • Screen Lock — For mobile agents only. • Operating System Check — For all user agents (mobile and desktop). • Browser Check — For the end user portal only.

2. Select **Save**.



Integrations

[Integrate with the Public Cloud](#) on page 78

[Add Event Collectors](#) on page 79

[Microsoft Intune Integration](#) on page 79

Integrate with the public cloud, add event collectors, and integrate with mobile device management.

Integrate with the Public Cloud

There are three public cloud integration options:

- Amazon Workspace (AWS)
- Microsoft Azure
- Google Cloud Platform (GCP)

Use this task to add an integration to deploy and manage cloud service connectors.

1. Select **Integrations > Public Cloud**.

2. To add an AWS integration:

- a. Select the **AWS Integration** tab.
- b. Select **Add Integration**.
- c. Update the following fields:
 - Integration Name
 - AWS Account ID
 - AWS Access Key ID
 - AWS Secret
 - Session Token

d. Select **Add**.

3. To add an Azure integration:

- a. Select the **Azure Integration** tab.
- b. Select **Add Integration**.
- c. Update the following fields:
 - Integration Name
 - Subscription ID
 - Tenant ID
 - Application Client ID

- Object ID
 - Application Client Secret
 - d. Select **Add**.
4. To add a GCP integration:
 - a. Select the **GCP Integration** tab.
 - b. Select **Add Integration**.
 - c. Follow instructions on the screen to update the following fields:
 - Integration Name
 - Project ID
 - Upload the JSON key file
 - d. Select **Add**.

Add Event Collectors

There are two options to add event connectors:

- Splunk
- API-based Log Collection

Use this task to add Splunk and use API to filter activity logs.

1. Select **Integrations > Event Collector**.
2. To integrate Splunk:
 - a. Follow instructions on the screen and update the following fields:
 - HTTP Event Collector Host
 - Port
 - Protocol
 - Authentication Token
 - b. Select **Validate**.
3. To use an API-based log collection:
 - a. Follow instructions on the screen.
 - b. Copy the API endpoint.
 - c. Select **Generate Token**.

Microsoft Intune Integration

To integrate Universal ZTNA and Microsoft Intune configurations are required in both Microsoft Entra ID and Universal ZTNA.

To proceed with the integration, complete the following tasks:

- [Configure Microsoft Entra ID for Universal ZTNA Microsoft Intune Integration](#) on page 80
- [Configure Universal ZTNA for Microsoft Intune Integration](#) on page 81

Configure Microsoft Entra ID for Universal ZTNA Microsoft Intune Integration


Use this task to configure the Microsoft Entra ID piece of a Universal ZTNA and Microsoft Intune integration.

1. Log in to Microsoft Entra ID.
2. Go to **Manage > App Registrations**.
3. Select **New registration**.

The system displays the **Register an application** page.

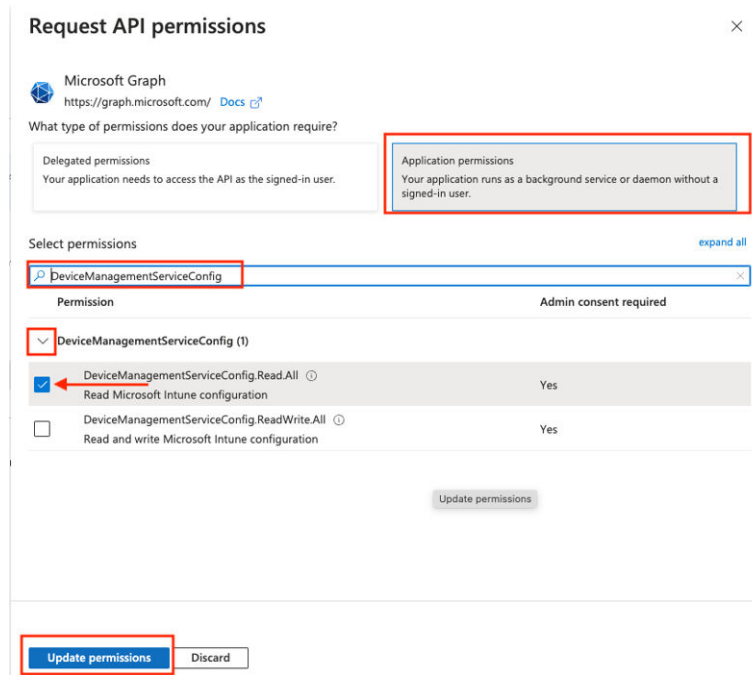
4. Enter an app name and ensure the **Single Tenant** option is selected under **Supported account types**.
5. Go to **Manage > API Permissions**.
6. Select **Microsoft Graph (1)**.

The system displays the **Request API permissions** page.

7.  **Note**
Application permissions must be granted.

Select the **Applications permissions** block.

8. Search for and select the following items:



Request API permissions

Microsoft Graph
https://graph.microsoft.com/ Docs

What type of permissions does your application require?

Delegated permissions
Your application needs to access the API as the signed-in user.

Application permissions
Your application runs as a background service or daemon without a signed-in user.

Select permissions expand all

DeviceManagementServiceConfig

Permission	Admin consent required
<input checked="" type="checkbox"/> DeviceManagementServiceConfig (1)	
<input checked="" type="checkbox"/> DeviceManagementServiceConfig.Read.All Read Microsoft Intune configuration	Yes
<input type="checkbox"/> DeviceManagementServiceConfig.ReadWrite.All Read and write Microsoft Intune configuration	Yes

Update permissions

Update permissions Discard

Main search	Specific permission
Application	• Application.Read.All
DeviceManagementManagedDevices	• DeviceManagementManagedDevices.PrivilegedOperations.All • DeviceManagementManagedDevices.Read.All
DeviceManagementServiceConfig	• DeviceManagementServiceConfig.Read.All

Main search	Specific permission
Group	• Group.Read.All
User	• User.Read.All

- Once they are all enabled, select **Update permissions**.
- To enable permissions, select **Grant admin consent for <domain>**.

API / Permissions name	Type	Description	Admin consent req...	Status
▼ Microsoft Graph (7) ...				
Application.Read.All	Application	Read all applications	Yes	✔ Granted for Extreme Ne... ...
DeviceManagementManagedDevices.PrivilegedOperations.All	Application	Perform user-impacting remo...	Yes	✔ Granted for Extreme Ne... ...
DeviceManagementManagedDevices.Read.All	Application	Read Microsoft Intune devices	Yes	✔ Granted for Extreme Ne... ...
DeviceManagementServiceConfig.Read.All	Application	Read Microsoft Intune config...	Yes	✔ Granted for Extreme Ne... ...
Group.Read.All	Application	Read all groups	Yes	✔ Granted for Extreme Ne... ...
User.Read	Delegated	Sign in and read user profile	No	✔ Granted for Extreme Ne... ...
User.Read.All	Application	Read all users' full profiles	Yes	✔ Granted for Extreme Ne... ...

Once complete the system displays the API permissions.

- Go to **Manage > Certificates & secrets**.
- Select **New client secret**. The system displays the **Add a client secret** page.
 - Enter a description and select an expiry time from the drop-down list.
 - Select **Add**.

In the Value column the secret value is revealed.

- Copy the secret value and store it in a secure place.



Note

The secret value can only be viewed from this screen. If you navigate from this screen, the value will no longer be accessible.

- Select **Overview** and copy the **Application (client) ID** and the **Directory (tenant) ID**.

[Configure Universal ZTNA for Microsoft Intune Integration](#) on page 81

Configure Universal ZTNA for Microsoft Intune Integration

You must complete [Configure Microsoft Entra ID for Universal ZTNA Microsoft Intune Integration](#) on page 80.

Use this task to configure the Universal ZTNA piece of a and Microsoft Intune integration.

- Log in to Universal ZTNA.
- Go to **Integrations > Mobile Device Mgmt**.
- For the Microsoft Intune option, select **Add Integration**.
The system displays the **Add Microsoft Intune Integration** dialog.
- Enter the saved Client ID, Secret, and Tenant ID from [Configure Microsoft Entra ID for Universal ZTNA Microsoft Intune Integration](#) on page 80.
- Select **Validate Information**.

6. If the configuration is valid, select **Add Integration**.
Synchronization with Microsoft Intune occurs in the background. If the integration is successful, the system displays all compliant devices.
7. If there are any errors with the integration, check the permissions for the application that was created in Microsoft Entra ID.
8. Go to **Insights > End Systems**.
9. The Compliance column can now be added to the End Systems table.



Note

Column order can be updated.



Monitor

[View Alerts](#) on page 83

[Troubleshooting](#) on page 83

[Subscriptions](#) on page 85



[View Activity Logs](#) on page 85

Go to **Monitor** to search for and view system alerts, to run tests, view subscriptions, and activity logs.

View Alerts

The **Alerts** screen displays a list of alerts, their severity, status, description, and source.

Use this task to view, filter, and export alerts.

1. Go to **Monitor > Alerts**.
2. Select the time period for which you wish to display alerts.
3. To refresh the screen, select .
4. Hover over the alert for a summary.
5. To sort alerts, use the **Filter** icon.
6. To download alerts, select **Export to CSV**.
7. To acknowledge an existing alert, select  and select **Acknowledge** from the drop-down list.

Troubleshooting

Within the Troubleshooting section to troubleshoot the Universal ZTNA configuration or operational state.

- Network Policy Evaluation - This process will evaluate a combination of input fields for an authentication request. Based on the Hybrid and Network policy configuration a test of authentication success or failure and expected policy assignment will be displayed. For more information, see [Evaluate Network Policy](#) on page 84.
- Application Policy Evaluation - This process will evaluate whether a specific user should have access to an application. If they should have access but are experiencing issues, a troubleshooting workflow can be started to gather logs and troubleshooting data to share with Extreme Networks Support. For more information, see [Evaluate Application Policy](#) on page 84.

Evaluate Network Policy

Use this task to evaluate the network policy.

1. Go to **Monitor > Troubleshooting**.
The **Network Policy Evaluation** tab displays.
2. Configure the settings.

Table 28: Settings for Network Policy Evaluation

Field	Description
MAC Address	Enter the MAC address.
Authentication Type	Select an authentication type from the drop-down list.
Optional options	You can update optional fields: <ul style="list-style-type: none"> • Username • Password • Service Set Identifier (SSID) • AP/Switch IP • Switch Port • Date • Time

3. Select **Run Test**.

If you entered a username and password, Universal ZTNA will attempt to authenticate against the Identity Provider using 802.1X EAP-TTLS to validate a successful configuration.

Evaluate Application Policy

Use this task to evaluate application policy.

1. Go to **Monitor > Troubleshooting** and select the **Application Policy Evaluation** tab.
2. Configure the settings.

Table 29: Settings for Application Policy Evaluation

Field	Description
User	Select a user from the drop-down list.
Application	Select an application from the drop-down list.
Access Mode	Select the Agentless or Agent-Based option.
Location-Based Condition	Select a location-based condition from the drop-down list.

Table 29: Settings for Application Policy Evaluation (continued)

Field	Description
Device	If testing agent-based, a device must be selected. If agentless is being tested, no device is required.
Time-Based Condition	Select a time zone from the drop-down list. You can also select a start time and end time.

3. Select **Evaluate**.

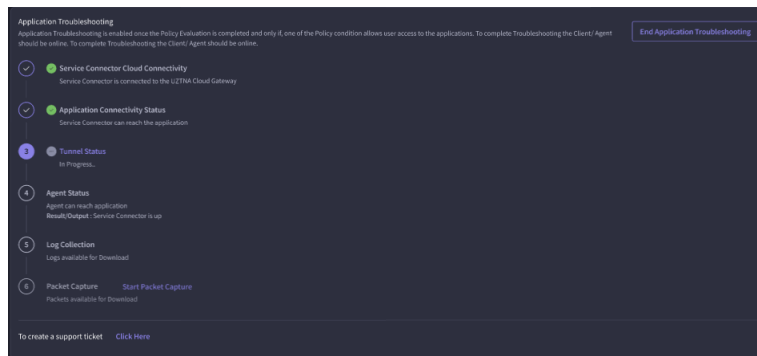
The **Evaluation Results** and **Application Troubleshooting** sections display. To enable troubleshooting, select **Start Application Troubleshooting**.



Note


The client/agent must be online.

To end the process before all items have been analyzed, select **End Application Troubleshooting**.



Subscriptions

Use this task to view and filter subscriptions.

1. Select **Monitor > Subscriptions**.
2. On the **Subscriptions** screen, you can view subscription status, availability, quantity used, and the total number of subscriptions.
3. To refresh the screen, select .

View Activity Logs

Use Activity Logs to view the last 30 days of your environment users' interaction with Universal ZTNA. There are 14 categories of logs.

- Log in and Registration
- Applications
- Relay
- Service Connector

- Network and Network Groups
- Device and Device Groups
- Policy
- Users
- DNS
- Conditions
- IdP
- Workspace

Select **Monitor** > **Activity Logs**.

The **Activity Logs** window displays.

You can view the logs for that day, the last hour or two hours, seven days, or thirty days. The filter options are User Identity, Event Source, Event Name, or Event Status.



Appendices

[Invite Users](#) on page 87

[Import Users](#) on page 88

[SAML-based Integration for Microsoft Active Directory Federated Services \(AD FS\)](#) on page 89

[Fabric Engine Locally Managed Sample Configuration](#) on page 91

[Switch Engine Locally Managed Sample Configuration](#) on page 95

Invite Users

Use this task to manually invite users.

1. Go to **IAM > Users**.
2. Select **Invite Users** and configure the settings.

Table 30: Invite User Configuration Settings

Field	Description
User Email Address	Enter one or more email addresses. Note: Use the Invite Users option for five or less users. For more than five users, use the import option.
Add to User Group	Select the user group from the drop-down menu to add the user to an existing user group. User groups assign your enterprise applications and networks to those users. Note: If no user groups exist at this step, select IAM > User Groups to create one.

3. Select **Send Invitation**.

The user receives an email asking them to accept the invitation. The user's status shows **Awaiting Acceptance** while waiting for the invitation to be accepted. When the user accepts the invitation, the status changes to **Active**, indicating the user is now a member of your environment.

Import Users

Use this task to import users in bulk.

1. Go to **IAM > Users**.
2. Select **Import Users** and configure the settings.

Table 31: Import User Configuration Settings

Field	Description
File Format	<p>From File Format, select one of the following:</p> <ul style="list-style-type: none"> • Single G-Suite: Uses a list exported from G-Suite. • Entra ID: Uses a list exported from Microsoft. • Custom: Uses a list created from the .csv Universal ZTNA template.
Add to User Group	<p>Select the user group from the drop-down menu to add the user to an existing user group. User groups assign your enterprise applications and networks to those users.</p> <p>Note: If no user groups exist at this step, select IAM > User Groups to create one.</p>

3. Select **Proceed** to upload and validate the import file format.



Note

Depending on the number of users to import, the import can take several minutes.

4. Select **Proceed**.
Invite users in Bulk pop-up window displays.
5. Select the users to invite.



Note

If any of your imported users appear disabled in the list, you may have restricted user access to approved domains only. To update these settings, go to **IAM > Identity Providers**.

6. Select **Proceed**.
The **Select User Group** pop-up window displays.
7. Select a group from **Add to User Group**.
The users now have access to the same applications and network settings.
8. Select **Add Users** to send the invitations.

The user receives an email asking them to accept the invitation. The user's status shows **Awaiting Acceptance** while waiting for the invitation to be accepted. When the user accepts the invitation, the status changes to **Active**, indicating the user is now a member of your environment.

SAML-based Integration for Microsoft Active Directory Federated Services (AD FS)

Use this task to set up SAML-based integration for Microsoft Active Directory Federated Services (AD FS)

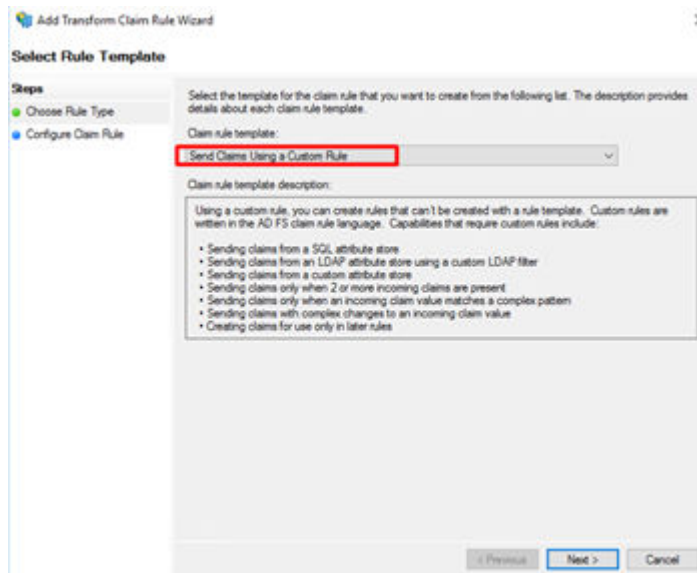
1. Go to your **MS AD Server Manager**.
2. To create a relying party trust as part of configuring partner organizations, select [Relying Party Trust](#) and follow the instructions.
3. To create a rule to send Lightweight Directory Access Protocol (LDAP) attributes as claims, select [Create a Rule to Send LDAP Attributes as Claims](#) and follow the instructions.
4. Follow these steps to create claim rules for Zero Trust Access (ZTA) applications as a service provider.



Note

Add claim rules for ZTA as a service provider in Identity Provider (IdP) windows server 2016.

- a. Go to **ADFS Manager > Relying party trust add claim issuance policy > Add Rule**.
- b. In **Select Rule Template**, in the **Claim Rule Template** field, select **Send Claim Using a Custom Rule**.



- c. Select **Next**.

- d. Add this attribute rule as a custom rule:

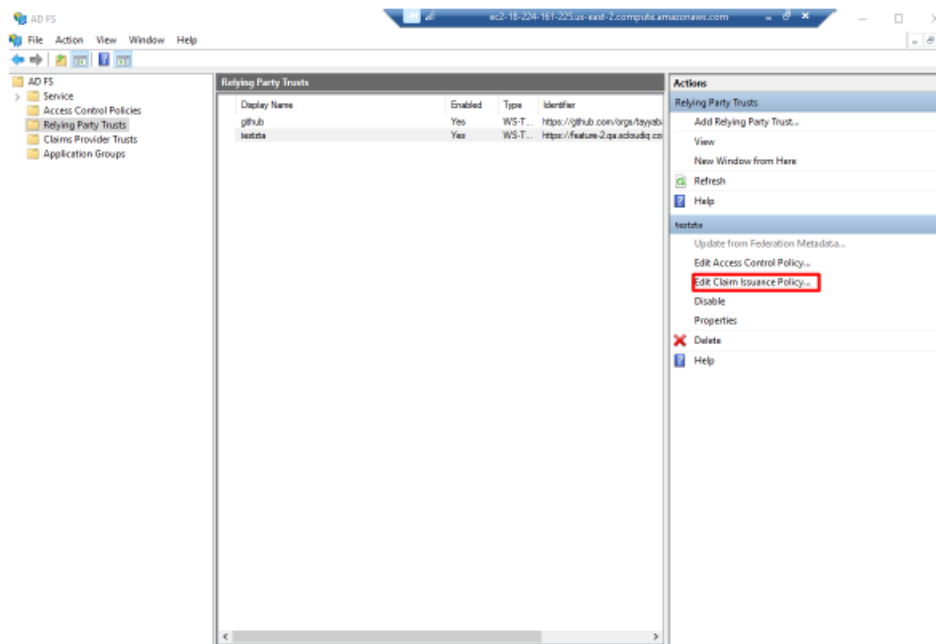
```
c:[Type == "http://schemas.xmlsoap.org/ws/2005/05/identity/claims/upn"]  
=> issue(Type = "http://schemas.xmlsoap.org/ws/2005/05/identity/claims/  
nameidentifier", Issuer = c.Issuer, OriginalIssuer = c.OriginalIssuer, Value  
= c.Value, ValueType = c.ValueType, Properties["http://schemas.xmlsoap.org/ws/  
2005/05/identity/claimproperties/format"] = "urn:oasis:names:tc:SAML:2.0:nameid-  
format:unspecified");
```



Note

If you applied the rule successfully, you will receive a successful status.

- e. Select **ADFS > Service > Relying Party Trust > Edit Claim Insurance Policy.**



- f. Select **Add Rule > OK.**
- g. In **Select Rule Template**, in the **Claim Rule Template** field, select **Send LDAP Attributes as Claims.**
- h. Select **Next.**
- i. Add a Rule.



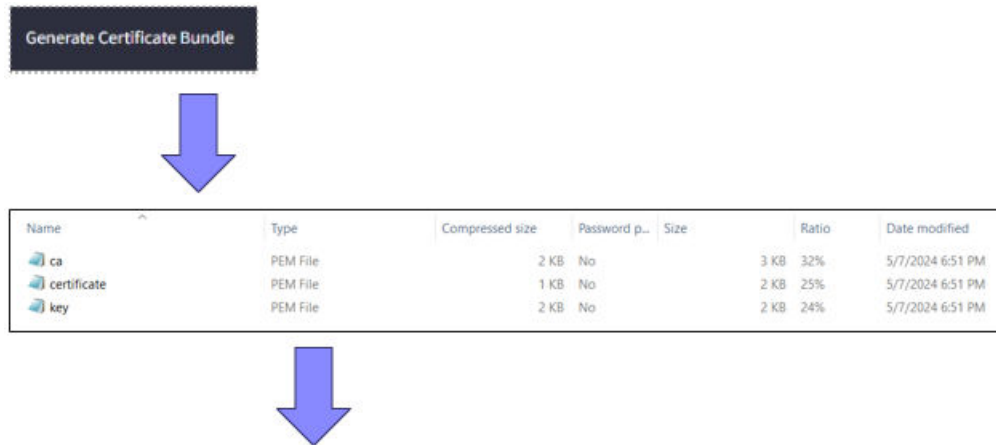
Note

If you applied the rule successfully, you will receive a successful status.

- j. Select **OK > Close.**

Fabric Engine Locally Managed Sample Configuration

Generate and Download the Certificate Files



Directory of C:\Users\Radsec\Downloads\certificate-file-extreme

```

05/15/2024 10:06 AM <DIR> .
05/15/2024 10:06 AM <DIR> ..
05/13/2024 02:04 PM 2,427 ca.pem
05/13/2024 02:04 PM 1,244 certificate.pem
05/13/2024 02:04 PM 1,678 key.pem
3 File(s) 5,349 bytes
2 Dir(s) 43,057,008,640 bytes free

```

Upload Certificate Files to the Switch Using FTP

```

C:\Users\Radsec\Downloads\certificate-file-extreme>ftp 10.68.16.150

Connected to 10.68.16.150.

220 FTP server ready

530 USER and PASS required

User (10.68.16.150:(none)): rwa

331 Password required

Password:

```

```
230 User logged in

ftp> binary

200 Type set to I, binary mode

ftp> put ca.pem

200 Port set okay

150 Opening BINARY mode data connection

226 Transfer complete

ftp: 2427 bytes sent in 0.00Seconds 2427000.00Kbytes/sec.

ftp> put certificate.pem

200 Port set okay

150 Opening BINARY mode data connection

226 Transfer complete

ftp: 1244 bytes sent in 0.00Seconds 1244000.00Kbytes/sec.

ftp> put key.pem

200 Port set okay

150 Opening BINARY mode data connection

226 Transfer complete

ftp: 1678 bytes sent in 0.00Seconds 1678000.00Kbytes/sec.

ftp> quit

221 Bye...see you later
```



Note

files are uploaded in the default location **/intflash**

When running Enhanced Secure Mode (ESM) default location will be
/intflash/shared directory

Apply the Certificate Files to the Switch Using Default RADIUS Secure-Profile

```
#radius secure-profile default ca-cert-file ca.pem

#radius secure-profile default cert-file certificate.pem
```

```
#radius secure-profile default key-file key.pem
#radius secure-profile default key-pwd radsec
```

Apply the RADIUS/RADIUS-Secure Configuration to the Switch

```
#radius server host 3.72.170.112 key radsec used-by eapol
#radius server host 3.72.170.112 used-by eapol secure-enable
#radius secure-flag
#radius enable
```

Optional Configuration

```
#radius secure-profile TestProfile -to use create custom Radius secure-profile
```

```
#radius server host 3.72.170.112 used-by eapol secure-profile TestProfile -to link the
custom profile to a specific Radius
server
```

```
#radius server host 3.72.170.112 used-by eapol acct-enable -to enable accounting for a
specific Radius
server
```

```
#radius accounting enable -to enable the accounting globally
```

```
#radius server host 3.72.170.112 used-by eapol secure-log-level -to change log level for
the TCP/TLS
session
```

```
#radius server host 3.72.170.112 used-by eapol secure-mode -to switch
between TLS and DTLS
```

802.1X NEAP Basic System and Port Configuration

```
#eapol enable

#interface gigabitEthernet 1/1

#(config-if)#eapol multihost radius-non-eap-enable

#(config-if)#eapol status auto
```

Optional Configuration

```
#interface gigabitEthernet 1/1
```

```
 #(config-if)#eapol multihost non-eap-mac-max 10 -to change the max number of NEAP clients
  allowed on that
    port
```

```
 #(config-if)#eapol multihost mac-max 10 -to change the max Mac clients allowed on 802.1x
  enabled
    ports
```

```
 #(config-if)#eapol re-authentication enable -to enable
  re-authentication
```

802.1X NEAP on Ports Enabled for Auto-sense

Auto-sense is a port-based functionality to support zero touch capabilities on the VOSS switches. When you enable Auto-sense on a port, the system dynamically configures the port based on the Link Layer Discovery Protocol (LLDP) events .

```
#interface gigabitEthernet 1/1
```

```
 #(config-if)#auto-sense
```

Optional Configuration for Auto-sense Eapol

```
 #auto-sense eapol multihost non-eap-mac-max 10 -to change the max number of NEAP clients
  allowed on that
    port
```

```
 #auto-sense eapol multihost mac-max 10 -to change maximum MAC clients supported on
  an Eapol enabled port
```

Switch Engine Locally Managed Sample Configuration

Generate, Download, and Apply the Certificate Files to the Switch

Generate Certificate Bundle

Name	Type	Compressed size	Password p...	Size	Ratio	Date modified
ca	PEM File	2 KB	No	3 KB	32%	5/7/2024 6:51 PM
certificate	PEM File	1 KB	No	2 KB	25%	5/7/2024 6:51 PM
key	PEM File	2 KB	No	2 KB	24%	5/7/2024 6:51 PM

↓

```
# download ssl <ip address> certificate trusted-ca ca.pem
# download ssl <ip address> certificate certificate.pem
# download ssl <ip address> privkey key.pem
```

Apply the RADIUS/RadSec configuration to the switch – RADIUS Accounting is optional but will help with immediate client disconnect notifications in Universal ZTNA

FQDN	IP Address	Port	Secret	Region
radius.zta-qa.qa.xcloudiq.com	3.72.170.112	2083	radsec	Frankfurt (Europe)

↓

```
# config radius rls ocap off
# configure radius netlogin 1 server 3.72.170.112 rls 2083 client-ip <switch ip> shared-secret radsec vr VR-Mgmt
# enable radius netlogin
# configure radius-accounting netlogin 1 server 3.72.170.112 rls 2083 client-ip <switch ip> shared-secret radsec vr VR-Mgmt
# enable radius-accounting netlogin
```

Apply Netlogin/Policy Configuration to the Switch

1. Configure the policy for dACL and VLAN authorization.

```
# configure policy rule-model access-list
# config policy vlanauth enable
# config policy mactable response both
# enable policy
```

2. Configure netlogin for dot1x or mac authentication/reauth (example on ports 1-5).

```
# enable netlogin dot1x mac

# configure netlogin authentication protocol-order dot1x mac web-based
  cep

# enable netlogin ports 1-5 dot1x mac

# configure netlogin add mac-list ff:ff:ff:ff:ff:ff 48

# configure netlogin mac ports 1-5 timers reauthentication on
```