ExtremeCloud™ Universal Zero Trust Network Access

for Version 24.1.0

9038015-00 Rev AA
May 2024

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: 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/

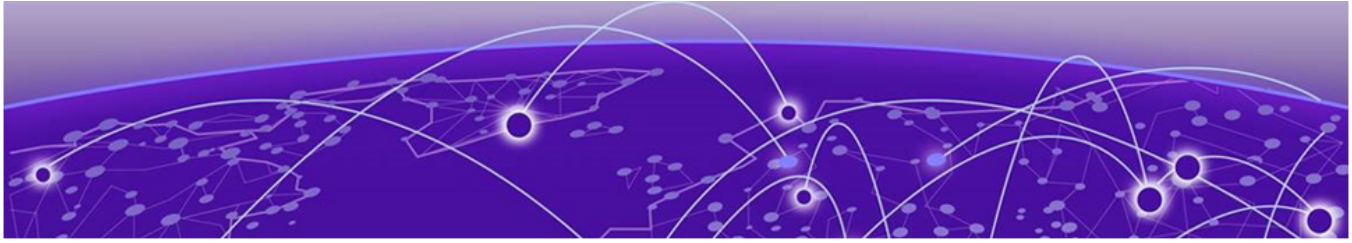


Table of Contents

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 *enter* and *type*	When you see the word *enter* 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 *type*.
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**
Words in italicized type	Italics emphasize a point or denote new terms at the place where they are defined in the text. Italics are also used when referring to publication titles.
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.
italic text	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, *member*[*member*...].
\	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.

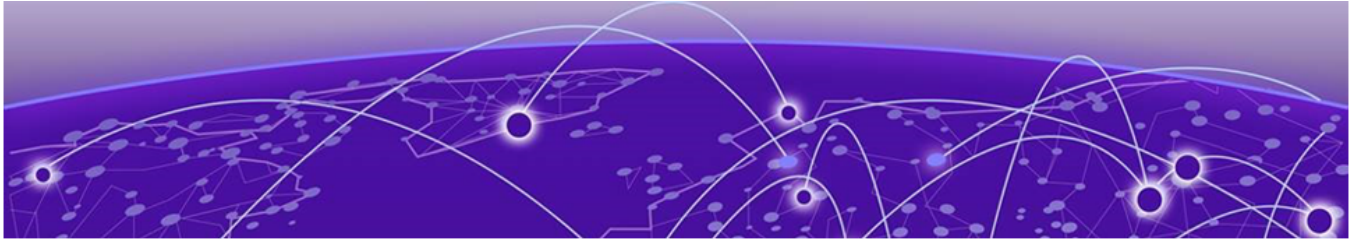
Send Feedback

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.



Introduction to the ExtremeCloud Universal ZTNA User Guide

Universal Zero Trust Network Access (Universal ZTNA) integrates network, application, and device access security within a single solution. To bolster security organization-wide, you can establish and maintain a consistent security policy across your network with a single solution to manage and enforce an identity-level zero trust policy for all users. You can also manage user networks, applications, and Internet of Things (IoT) device access independent of the user's location.

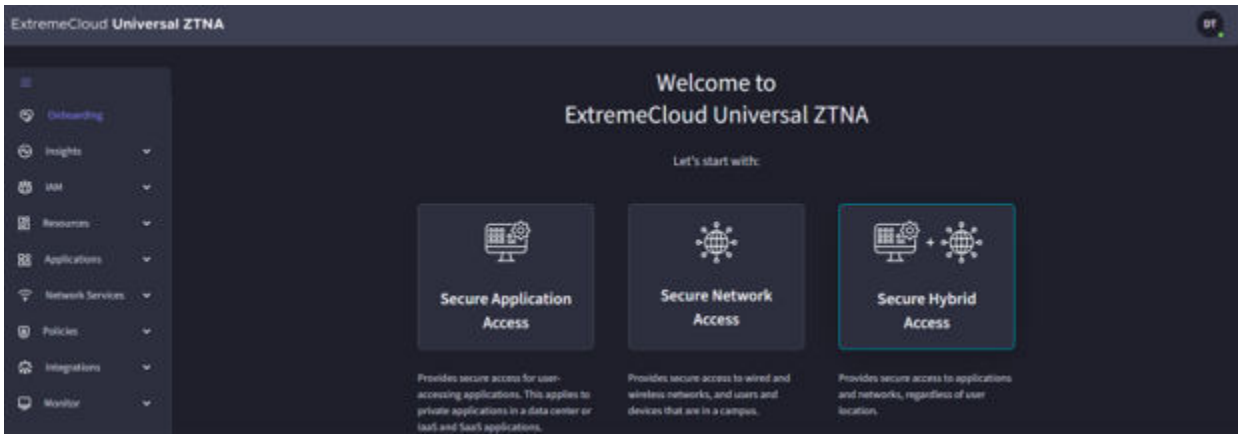
Universal ZTNA combines and enhances remote and campus access security. Remote access leverages ZTNA continuous authentication, tunneled application sessions with direct to cloud routing. On campus access combines ZTNA and NAC capabilities to control access to the network and applications for headed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

Universal ZTNA integration with mobile device solutions such as Microsoft Intune enables 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
- Setting up and preparing IoT and end user devices automatically
- Automatically configuring NAC, SSIDs, ports and VLANs on Universal APs and switches

Widgets consisting of gauges, pie charts, and line charts showing health status, applications, networks, authentication, and policies summarize your network security on the dashboard. The far-left menu allows you to:

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


ExtremeCloud Universal ZTNA
Onboarding
Insights
IAM
Resources
Applications
Network Services
Policies
Integrations
Monitor
Welcome to
ExtremeCloud Universal ZTNA
Let's start with:
Secure Application Access
Secure Network Access
Secure Hybrid Access

Universal ZTNA Onboarding

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

There are three types of secure access offered by Universal ZTNA:

- **Secure Application Access** provisions access to resources, applications at private data centers, Infrastructure as a Service (IaaS), such as Google Cloud Platform (GCP), Amazon Web Services (AWS) and Microsoft Azure or Software as a Service (SaaS) applications
- **Secure Network Access** provisions wired and wireless network access for users and devices
- **Secure Hybrid Access** combines application and network secure access

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

Each access method has three types of Identity Providers (IdP), but you can only configure one. The IdPs are:

- Microsoft Entra ID
- Google Workspace

- Microsoft Active Directory

Note
ExtremeCloud Universal ZTNA IdP is only for trialing Universal ZTNA using Secure Application Access. To complete the trial setup, see Complete a Universal ZTNA Trial Assessment.

After configuring your IdP, you must complete additional steps. Depending on the type of secure access you choose, not all steps are required.

- Create access groups
- Add resources
- Add applications and create application groups
- Define networks and network groups
- Create policies

Supported Platforms and Hardware Requirements

Minimum Supported versions for mobile agents

Android: 1l

OS: 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 later

Radsec Proxy hardware requirements and prerequisites

Minimum hardware requirements: vCPU: 2 Ram: 4 GB

Supported OS: Ubuntu 20.04, Ubuntu 22.04

Prerequisites: None

Service Connector hardware requirements and prerequisites (local and cloud)

System Requirements for Packaged Deployment:

Recommended OS - Ubuntu 20.04 or above.

Dockerized Deployment:

C-Supported Platform: amd64 Compatible with multiple operating systems; requires only Docker to be installed.

Ports Availability If connector and user are in the same network, the following ports are to be made open for the inbound requests:

WireGuard Encryption Protocol: 51820

IPSEC Encryption Protocol: 500, 4500

Minimum hardware requirements:

vCPU: 2 Ram: 4 GB

Configure UZTNA Access

This procedure explains how to onboard users, applications, and devices using:

- Secure Application Access
- Secure Network Access
- Secure Hybrid Access (combines application and network secure access)

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.

Each access method has four Identity Providers (IDP) to choose from. The network administrator needs to configure three of the four providers.

is the default. Its IDP is pre-configured at the admin level to authenticate the user's workspace, requiring no setup during the onboarding procedure and supports the following:

- Microsoft Entra ID
- Google Workspace
- Microsoft Active Directory

After you configure your IDP, there are four more major steps to complete:

- Access groups (Users/Device groups)
- Add resources
- Define applications and application groups
- Create a policy

UZTNA Wired Guidelines

Universal ZTNA supports Fabric Engine/VOSS and Switch Engine/EXOS NOSs. The minimum versions are:

- Switch Engine 32.7.1
- Fabric Engine 9.0.2

There are two management options:

- Managed Mode

- Locally Managed Mode

Managed Mode

Supported NOS: Switch Engine. Switches are onboarded directly from the cloud workflow using the **Manage your Devices** workflow.

ExtremeCloud IQ manages switch configuration. The **Instant Secure Port** workflow provisions the following components on the switch:

- Certificate for secure RadSec communication
- RADIUS/RadSec configuration to the cloud RaaS 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 the **Manage your Devices Locally** workflow.

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

Users configure the following components manually:

- Certificate for secure RadSec communication
- RADIUS/RadSec configuration to the cloud RaaS server
- 802.1x or MAC authentication, along with supporting feature sets, depending on the deployment model

Configuration Details for Fabric Engine and Switch Engine

- To configure Fabric Engine, select Fabric Engine Locally Managed Sample Configuration on page 63
- To configure Switch Engine, select Switch Engine Locally Managed Sample Configuration on page 67

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)

Identity Provider

Begin by configuring your Identity Provider (IdP). An IdP enables authentication for your workspace users. You can do this by establishing connections with one of the following identity providers:

- Microsoft Entra ID on page 14
- Google Workspace on page 19
- Microsoft Active Directory on page 22

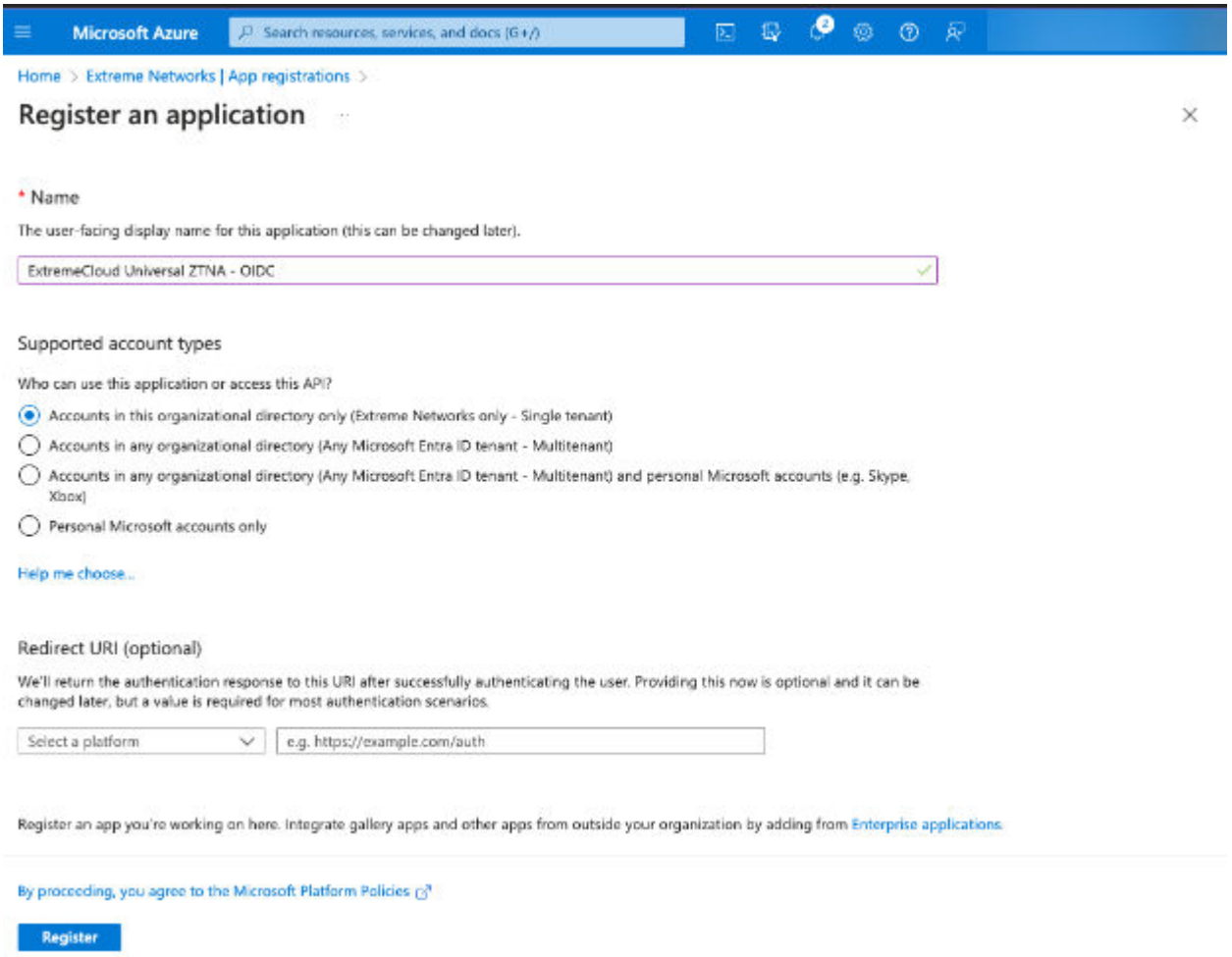
Microsoft Entra ID

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

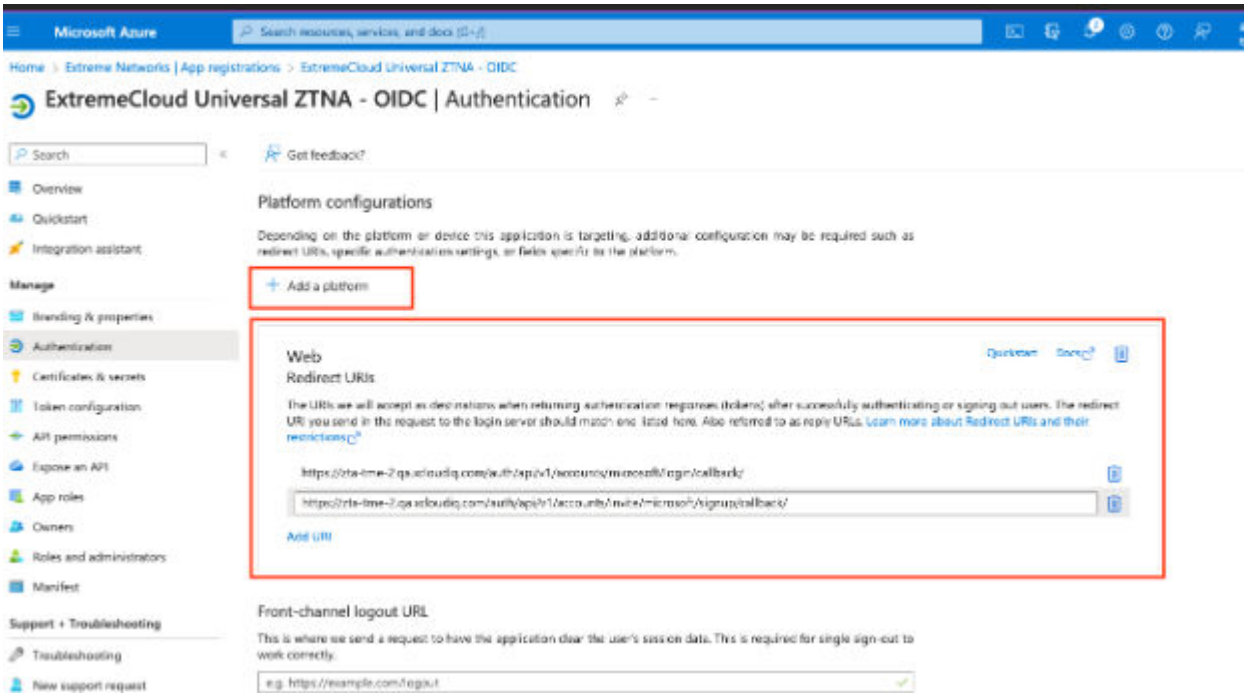
- **OpenID Connect**: This open authentication protocol works on top of the Open Authorization (OAuth) 2.0 framework.
- **Security Assertion Markup Language (SAML)**: This is an open standard for exchanging authentication and authorization data between an identity provider and a service provider.

Set up Entra ID with Open ID Connect (OIDC) Integration

1. Log into Microsoft Azure and select **Extreme Networks** > **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. Enter the following URIs:
   - https://zta-tme-2.qa.xcloudiq.com/auth/api/v1/accounts/microsoft/login/callback/
   - https://zta-tme-2.qa.xcloudiq.com/auth/api/v1/accounts/invite/microsoft/signup/callback/



5. Scroll to the bottom of the **Authentication** screen and under **Advanced Settings**, in the **Allow public client flows**, select **Yes**.
6. Return to the **Overview** screen and take note of the **Application (client) ID** and the **Directory (tenant) ID**.
7. In the **Client Credentials** field, select **Add a certificate or secret** > **New Client Secret** > **Add**.

   Note
   Keep the default expiration.

8. From the **Certificates & Secrets** screen, under the **Clients Secret** tab, in the **Value** field, copy the new token.
9. From the **API Permissions** screen, select **Grant admin consent for** [company name].
10. From the **ExtremeCloud Universal ZTNA Onboarding** screen, enter the noted **Application (client) ID**, **Client Secret**, and **Directory (tenant) ID**.
11. Select **Validate Information**.
12. When validation is complete, select **Update** > **Confirm**.

Configure Microsoft Entra ID - OpenID Connect

Before You Begin

There are two prerequisites to complete before configuring the Identity Provider in ExtremeCloud Universal ZTNA.

- Create **ClientID**, **Client Secret**, and **Discovery URL** in Azure under **App Registration**. Save a copy of each to use in this procedure.

- Your organization's AD-synced users must have administrative privileges in Azure so Microsoft can authorize the user during log in. To set the permission, navigate to **App Registrations** > **[Your Application]** > **API Permissions**.

About This Task

Follow this procedure to configure a Microsoft Entra ID - OpenID Connect Identity Provider.

Procedure

1. Select **Onboarding**.

   The welcome window displays.
2. Select **Secure Hybrid Access** [**Secure Application Access** or **Secure Network Access**].
3. On the **Identity Provider** window, select **Microsoft Entra ID**
4. Select **Continue**.

   The **Identity Provider** window displays.
5. Enter **Client ID**.
6. Enter **Client Secret**.
7. Enter **Tenant ID**.

   Note
   Redirect URLs are on the IdP set up page on the UI. You can copy and update redirect URLs in Azure. In Azure, specify the following URLs under the URI section. These URLs redirect the user to the portal after a successful authorization by Microsoft during log-in and sign-up.
   - https://*server URL*/auth/api/v1/accounts/microsoft/login/callback/
   - https://*server URL*/auth/api/v1/accounts/invite/microsoft/signup/callback/

8. (*Optional*) Select **Secure Network Access** if you want to allow Multi-Factor Authentication (MFA) enabled users to authenticate with ExtremeCloud Universal ZTNAservers.

   If the **Secure Network Access** check box is checked, the administrator must create a separate Entra ID Application in Azure and provide the Client ID, Client Secret and Tenant ID.
9. (*Optional*) To provision users and user groups in Azure and then sync them with Universal ZTNA, follow these steps:

   a. Follow the **Setup Guidelines** instructions.

      Note
      AD Syncing automatically updates Azure users and user groups and UZTNA users and user groups when users are removed or added.

   b. Select **Sync AD Users and User Groups**.

      Confirm AD Syncing pop-up window displays. This message cautions the user that they can no longer change the IdP settings if they proceed with syncing.

c. (*Optional*) Select **Send Invitations to synced users automatically**.

d. Select **Confirm**.

10. (*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.

11. Select **Validate Information**.

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

12. Select **Update**.

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

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

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

15. Configure Access Groups on page 24.
16. Configure Resources on page 28.
17. Configure Applications and Application Groups on page 32.

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

18. Configure Policies on page 38.

Results

Your onboarding is complete. Your users, applications, and devices can now access the network securely.

Configure Microsoft Entra ID - SAML

About This Task

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

Procedure

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 ZTNAselected.

3. Select **Next**.

   The **Onboarding** window displays.

4. Select the link to review the comprehensive tutorial on creating a SAML-based SSO in Microsoft Azure Entra ID.
5. Copy and paste the **Identifier** link and **Reply URL** link in Azure per the instructions in the tutorial.

   Azure 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 Azure.

   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 workspace users.
11. If you decide to continue, select **Confirm**.
12. Select **Next**.

    The **Onboarding - Access Groups** window displays.
13. Configure Access Groups on page 24.
14. Configure Resources on page 28.
15. Configure Applications and Application Groups on page 32.

    You can skip this step if you are using Secure Network Access.
16. Configure Policies on page 38.

Results

Your onboarding is complete. Your users, applications, and devices can now access the network securely.

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

Configure Google Workspace - OpenID Connect

Before You Begin

Retrieve the **ClientID** and **Client Secret** from Azure.

About This Task

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

Procedure

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 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.

   a. Follow the instructions on the UI.
   b. 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 workspace users.
12. If you decide to continue, select **Confirm**.
13. Select **Next**.

    The **Onboarding - Access Groups** window displays.
14. Configure Access Groups on page 24.
15. Configure Resources on page 28.
16. Configure Applications and Application Groups on page 32.

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

17. Configure Policies on page 38.

Results

Your onboarding is complete. Your users, applications, and devices can now access the network securely.

Google Workspace - SAML

Before You Begin

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

About This Task

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

Procedure

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 Azure.

   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 workspace users.
15. If you decide to continue, select **Confirm**.
16. Select **Next**.

    The **Onboarding - Access Groups** window displays.
17. Configure Access Groups on page 24.

18. Configure Resources on page 28.
19. Configure Applications and Application Groups on page 32.

    You can skip this step if you are using Secure Network Access.
20. Configure Policies on page 38.

Results

Your onboarding is complete. Your users, applications, and devices can now access the network securely.

Microsoft Active Directory

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

Microsoft Active Directory offers two types of 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.

Configure Microsoft Active Directory - OpenID Connect

Before You Begin

There are two prerequisites to complete before configuring the Identity Provider in ExtremeCloud Universal ZTNA.

- Create **ClientID**, **Client Secret**, and **Discovery URL** in Azure under **App Registration**. Save a copy of each to use in this procedure.
- Your organization's AD-synced users must have administrative privileges in Azure so Microsoft can authorize the user during log in. To set the permission, navigate to **App Registrations** > **[Your Application]** > **API Permissions**.

About This Task

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

Procedure

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 ZTNAselected.
3. Select **Microsoft Active Directory** and **Continue**.

   Microsoft Active Directory 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 Azure 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 workspace users.
11. If you decide to continue, select **Confirm**.
12. Select **Next**.

    The **Onboarding - Access Groups** window displays.
13. Configure Access Groups on page 24.
14. Configure Resources on page 28.
15. Configure Applications and Application Groups on page 32.

    You can skip this step if you are using Secure Network Access.
16. Configure Policies on page 38.

Results

Your onboarding is complete. Your users, applications, and devices can now access the network securely.

Configure Microsoft Active Directory - SAML

About This Task

This task shows you how to configure your identity provider using Microsoft Active Directory - SAML.

Procedure

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 ZTNAselected.

3. Select **Next**.

   The **Onboarding** window displays.
4. Select the Link to review the comprehensive tutorial on creating a SAML-based SSO in Microsoft Active Directory.
5. Copy and paste the **Identifier** and **Reply URL** links in Azure as per instructions in the tutorial.

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

   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 workspace users.
11. If you decide to continue, select **Confirm**.
12. Select **Next**.

    The **Onboarding - Access Groups** window displays.
13. Configure Access Groups on page 24.
14. Configure Resources on page 28.
15. Configure Applications and Application Groups on page 32.

    You can skip this step if you are using Secure Network Access.
16. Configure Policies on page 38.

Results

Your onboarding is complete. Your users, applications, and devices can now access the network securely.

Access Groups

Access groups enable you to manage individual users and devices or groups of users and devices by controlling their access to enterprise applications and the network.

Invite Users

About This Task

This task shows you how to manually invite users.

Procedure

1. (*Default*) Select the **Users** tab under **Access Groups**.
2. Select **Invite Users** (default).

   The **Invite Users** pop-up window displays.

3. For **User Email Addresses**, 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.

4. For **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.

5. Select **Send Invitation**.

Results

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 workspace.

Imports Users

About This Task

This task shows you how to import users in bulk.

Procedure

1. Select **Import Users**

   The **Import Users** pop-up window displays.
2. From **File Format**, select one of the following:
   - **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 UZTNA template.
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 Bulkpop-up window displays.
5. Select the users to invite.

   Note
   If any of your imported users appear disabled in the list, it could be because you 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.

Results

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 workspace.

Add Devices

About This Task

This task shows you how to manually add devices.

Procedure

1. Select **Add Devices**
   The **Add Devices** pop-up window displays.
2. For **MAC Address**, enter one or more MAC addresses.
3. Select **Add**

Results

Your device displays in the device list.

Import Devices

About This Task

This task shows you how to import devices in bulk.

Procedure

1. Select **Import Devices**
   The **Import Devices** pop-up window displays.
2. 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.
3. Select **Proceed**
   A confirmation pop-up window displays: **File uploaded and validated successfully. You can now continue.**
4. Select **Proceed**
   The list of devices from the .csv file displays.
5. Select specific MAC addresses to import or all addresses to import.
6. Select **Confirm**
   The **Select Device Group** pop-up window displays.

7. (*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.
8. Select **Import**

Results

Your devices display in the device list.

Create User Groups

About This Task

This task shows you how to create user groups.

Procedure

1. Select **User Groups**
2. Select **Create User Group**

   The **Create User Group** pop-up window displays.
3. For the **Name of User Group**, enter at least three alphanumeric characters of the integration group.
4. (*Optional*) Enter a description.
5. (*Optional*) Select one or multiple users.
6. Select **Create**

Results

Your group displays in the group list.

Create Device Groups

About This Task

This task shows you how to create device groups.

Procedure

1. Select **Device Groups.**
2. Select **Create Device Group.**

   The **Create Device Group** pop-up window displays. .
3. For the **Name of Device Group** , enter at least three alphanumeric characters for the device group name.
4. (*Optional*) Enter a description.
5. (*Optional*) Select one or multiple devices.
6. Select **Create.**

Results

Your device displays in the device list.

Resources

These are the required resources if you are onboarding using Secure Hybrid Access:

- **Sites** enable you to define your virtual or physical network boundaries
- **Deploy Service Connector** enables you to add secure application access over encrypted protocols
  - 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 datacenter or public cloud such as AWS, Azure, and GCP
- **Deploy RadSec Proxy** ensures RADIUS communications over untrusted networks

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, Azure, GCP)) managed by tenant admin.

These resources are optional if you are 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 UZTNA 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
  - The switch or access point does not support the RADSEC protocol by the secure TLS tunnel

Add Sites

Before You Begin

About This Task

This task shows you how to add and mange network sites by defining virtual or physical network boundaries.

Note
Sites created in ExtremeCloud IQ UZTNA are added to ExtremeCloud Universal ZTNA.

Procedure

1. (*Default*) Select the **Sites** > **Resources**.

2. Select **Add Site**.
   a. Provide the following Site information:
      - Site Name
      - Address
   b. Select **Add**.

Results
Your site displays in the site list.

Deploy Service Connectors

Before You Begin
Follow these recommendations:

Note
If Secure Socket Layer(SSL) decryption is in use, the traffic will not pass through the service connector.

- **Packaged deployment:** Recommended OS - Ubuntu 20.04 or higher
- **Dockerized deployment:** Compatible with multiple operating systems; requires only Docker to be installed.
- **Port availability:** If the connector and user are not in the same network, open the following ports for the inbound requests:
  - **WireGuard Encryption Protocol:** 51820
  - **IPSEC Encryption Protocol:** 500, 4500
  - **Default Radius UDP Port:** 1812, 1813
  - **Default RADSEC Port:** 2083
- **System Requirements for Packaged Deployment:**Recommended OS - Ubuntu 20.04 or above
- **Dockerized Deployment:**C-Supported Platform: amd64 compatible with multiple operating systems; requires only Docker to be installed. Ports Availability - If the connector and the user are in the same network, open the following ports for inbound requests:
  - **WireGuard Encryption Protocol:** 51820
  - **IPSEC Encryption Protocol:** 500, 4500
  - **Default Radius UDP Port:** 1812, 1813
  - **Default RADSEC Port:** 2083
- **Minimum hardware requirements:** vCPU: 2 Ram: 4 GB

About This Task
This task shows you how to deploy service connectors.

Procedure

1. Select the **Deploy Service Connector** tab.

   If deploying a Service Connector out of onboarding, select **Resources** > **Service Connectors** from the navigation pain on the left.

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**.

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

Note
Alternatively, you can verify the deployment status on your host machine.
`sudo systemctl status servicename`

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

Deploy RadSec Proxies

Before You Begin
Follow these recommendations:

- **Packaged deployment:** Recommended OS - Ubuntu 20.04 or higher
- **Dockerized deployment:** Compatible with multiple operating systems; requires only Docker to be installed.
- **Port availability:** If the connector and user are not in the same network, open the following ports for the inbound requests:
  - **WireGuard Encryption Protocol:** 51820
  - **IPSEC Encryption Protocol:** 500, 4500
  - **Default Radius UDP Port:** 1812, 1813
  - **Default RADSEC Port:** 2083
- **System Requirements for Packaged Deployment:**Recommended OS - Ubuntu 20.04 or above
- **Dockerized Deployment:**C-Supported Platform: amd64 compatible with multiple operating systems; requires only Docker to be installed. Ports Availability - If the

connector and the user are in the same network, open the following ports for inbound requests:
  - **WireGuard Encryption Protocol:** 51820
  - **IPSEC Encryption Protocol:** 500, 4500
  - **Default Radius UDP Port:** 1812, 1813
  - **Default RADSEC Port:** 2083
- **Minimum hardware requirements:** vCPU: 2 Ram: 4 GB

About This Task

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

Procedure

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 pain on the left.
2. Select **Deploy RadSec Proxy**.
   a. Read the Guidelines.
   b. Select **Next**.

      The **Configure** pop-up window displays.
   c. For **RadSec Proxy Name**, enter at least three alphanumeric characters.
   d. For **Associate Site**, select an existing site or create one.
   e. For **Certificate Rotation Time**, enter the number of days until the next rotation.
   f. Select **Deploy**.
   g. Read the information and follow the installation procedure for the host machine.
   h. Select **Close**.

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

   Note
   If you installed the host machine before sub-step 2.f on page 31, you will not need to perform the installation procedure after you return to the main proxy window. Instead, after waiting a short period, your proxy should come into service and display the **UP** status. Therefore, you can skip step 3.
3. Go to your host machine and perform the installation using the guidelines provided.

Results

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

Applications and Application Groups

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

- Add Private Web Applications on page 32
- Add Multi-Cloud Web Applications on page 33
- Add Custom Applications on page 33
- Public Software as a Service (SaaS)
- Terminal Access
- Remote Desktop

You can also create application groups and combine all the applications with the same policies and rules into one group. Therefore, any policy added to the application group automatically applies to all the applications within the group.

Add Private Web Applications

About This Task

This task shows you how to add web applications.

Procedure

1. Under the **Applications** tab, select **Web**.
2. Under **Add Application**, select **Private Web App**.

   Add Application - General Settings pop-up window displays.
3. For **Application Name**, enter at least three alphanumeric characters.
4. For **Associate Site**, select a site or create a new one.
5. For **Associate Service Connector**, select a connector or create a new one.
6. Select **Next**.

   The **Add Application - Application Info**pop-up window displays.
7. For the **Application URL**, select either **HTTPS** or **HTTP**.
8. Enter the **Application URL**.

   Note
   If your service is accessible through SSO, you should clear the **Hide my URL** option.

9. Select **Next**.

   The **Add Application - Review & Test Connectivity** pop-up window displays.
10. After you review your information, select **Test Connectivity**.

    This test checks if the associated service connector can access your enterprise application.

    If the test passes, the **Add** button becomes available.

11. Select **Add**.

    This step can take up to a minute to complete. When it does, the application's status is **CONNECTED**.
12. When you finish adding applications, select **Next** to Create Application Groups.

Related Topics

Add Public SaaS Applications on page 34
Add Terminal Access Applications on page 35
Add Remote Desktop Applications on page 36

Add Multi-Cloud Web Applications

Before You Begin

About This Task

Use this procedure to add multi-cloud web applications.

Procedure

1. Login to UZTNA.
2. Select **Applications** > **Private Hosted Applications** > **Add applications.**
3. Use this table to populate required fields.

Table 4: Add Custom Cloud Web Applications

Field	Action
Application Name	Enter a name for the application
Application Type	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: • AWS • Azure • GCP
Load balancer	Select a load balancer

4. Select **Add**.

Add Custom Applications

Before You Begin

Custom applications provide support for adding applications with Transmission Control Protocol(TCP) and User Datagram Protocols (UDP).

About This Task

Use this procedure to add custom applications.

Procedure

1. Login to UZTNA.
2. Select **Applications** > **Private Hosted Applications** > **Add Applications**.
3. Use this table to populate required fields.

Table 5: Add Custom Applications

Field	Action
Application Name	Enter a name for the application
Application Type	Select Custom Application
Associated Site	Select an associated site or create a new site
Protocol	Select UDT or TCP
Hostname	Enter a hostname
Port	Enter a port name

4. Select **Test Connectivity**.
5. Select **Add**.

Add Public SaaS Applications

About This Task

With Universal ZTNA, you can add Software as a Service (SaaS) applications and control your organization's access to those applications. There are eight applications you can add:

- Mulesoft
- Salesforce
- Slack
- G Suite
- Splunk
- Github
- Atlassian
- Dropbox
- Zoom

Procedure

1. Select **Applications** > **Applications** > **SaaS Applications.**
2. Find the application you want to add and select **Add**.

   Integrate - Service Provider Settings application pop-up window displays.
3. For the integration **Name**, enter at least three alphanumeric characters.
4. Enter the **Application URL**.
5. Enter the **Entity ID**.

6. Enter the **ACS URL**.
7. Enter the **Digest Method** and the **Signature Method**.
8. Select **Next**.

   Integration - Service Provider SSO pop-up window displays..
9. Select **Add.**

Related Topics

Add Private Web Applications on page 32
Terminal Access Applications on page 35
Remote Desktop Applications on page 36

Add Terminal Access Applications

About This Task

This task shows you how to add terminal access applications:

Procedure

1. Under the **Applications** tab, select **Terminal Access**.
2. Select **Add Applications**.

   Add Application - General Settings pop-up window displays.
3. For **Application Name**, enter at least three alphanumeric characters.
4. Select an **Associate Site**.
5. Select an **Associate Service Connector**.
6. Select Secure Shell (SSH) or Telnet protocols.
7. Select a **Hostname (or IP Address)**.
8. Enter a port number.
9. Select **Next**.

   The **Add Application - Review & Test Connectivity** pop-up window displays.
10. After you review your information, select **Test Connectivity**.

    This test checks if the associated service connector can access your enterprise application.

    If the test passes, the **Add** button becomes available.
11. Select **Add**.

    The step can take up to a minute to complete. The application will be displayed in the list when the procedure finishes showing the **UP** status.
12. When you finish adding applications, select **Next** to Create Application Groups.

Related Topics

Add Private Web Applications on page 32
Add Public SaaS Applications on page 34
Add Remote desktop applications on page 36

Add Remote Desktop Applications

About This Task

This task shows you how to add remote desktop applications.

Procedure

1. Under the **Applications** tab, select **Remote Desktop**
2. Select **Add Applications**.

   Add Application - General Settings pop-up window displays.
3. For **Application Name**, enter at least three alphanumeric characters.
4. Select an **Associate Site**.
5. Select an **Associate Service Connector**.
6. For **Hostname (or IP Address)**, select **VNC** or **RDP**.
7. Enter a **Hostname (or IP Address)**.

   Note
   If your service is accessible through SSO, you should clear the **Hide my URL** option.
8. Enter a port number.
9. Select **Next**.

   The **Add Application - Review & Test Connectivity** pop-up window displays.
10. After you review your information, select **Test Connectivity**.

    This test checks if the associated service connector can access your enterprise application.

    If the test passes, the **Add** button becomes available.
11. Select **Add**.

    The step can take up to a minute to complete. The application will be displayed in the list when the procedure finishes showing the **UP** status.
12. When you finish adding applications, select **Next** to Create Application Groups.

Related Topics

Add Private Web Applications on page 32
Add Public SaaS Applications on page 34
Add Terminal Access Applications on page 35

Create Application Groups

About This Task

This task shows you how to create applications groups.

Procedure

1. Select the **Application Groups** tab.

   The **Application Group** window displays.

2. Select **Create Application Group**.
   The **Create Application Group** pop-up window displays.
3. For the **Name of Application Group**, enter at least three alphanumeric characters.
4. (*Optional*) Enter a group description
5. Select the applications you want to combine in your group from the **Applications** drop-down list.
6. Select **Create**.

Results

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

Add Applications to Groups

About This Task

This task shows you hot to add applications to groups.

Procedure

1. Select the **Applications** tab (default).
2. Select the applications you want to group from the **Name** column.
3. Select **Combine Selected into Group**.
   The **Create Application Group** window displays.
4. For the **Name of Application Group**, enter at least three alphanumeric characters.
5. (*Optional*) Enter a group description.
6. Select **Create**.

Results

The **Application Groups** tab displays your group in the list.

Networks and Network Groups

We create Networks and Network Groups to enable or deny access. Networks can be grouped and applied to policies.

Add Network Services

About This Task

This task shows you how to add network services.

Procedure

1. Select **Networks Services** > **Network Services**
   The **Network Services** window displays.
2. Select **Add Network Service**.
   The **Add Network Service** pop-up window displays.

3. For **Network Service Name**, enter at least three alphanumeric characters
4. For **Protocol/IP Address**:
   a. Select a protocol.
   b. Enter an IP address.
5. (*Optional*) Enter one or multiple ports separated by commas.
6. Select **Add**.

Results

Your network displays in the network services list.

Create Network Services Groups

About This Task

Creating network groups aims to group a set of networks that share the same policy or rules. Therefore, any policy added to the network group automatically applies to all the networks within the group. Conversely, a network group should not include any network that requires a unique policy.

This task shows you how to create network services groups.

Procedure

1. Select **Network Services** > **Network Service Groups**.
   The **Network Service Groups** window displays.
2. Select **Create Network Service Group**.
   The **Create Network Service Group** pop-up window displays.
3. For the **Network Group Name**, enter at least three alphanumeric characters.
4. (*Optional*) Enter a group description.
5. Under **Add Network Service**, select **Create New** or **Select Existing**.
6. Select **Create**.

Results

Your network displays in the group list.

Policies

Policies contain distinct conditions that provide different levels of authorization to your infrastructure. There are three types of policies:

- Create Hybrid Policies on page 39 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.

Create Hybrid Policies

About This Task

This task shows you how to create a hybrid policy.

Procedure

1. Select **Add Hybrid Policy**.

   Create New Policy displays.
2. For **Policy Name**, enter at least three alphanumeric characters
3. (*Optional*) Enter a description.
4. For **User Groups**, select **Any User** or select a user group from the drop-down menu or create one, for details, see Create User Groups on page 27.
5. For **Device Groups**, select **Any Device** or select a device group from the drop-down menu or create one, for details, see Create Device Groups on page 27.

   Note
   If user and device groups are configured in the policy, for the policy to match for network access both access conditions must pass.

6. (*Optional*) For **Location Based Condition**, select a location condition from the drop-down menu or create a new condition, for details, see Add Location Based Conditions on page 42.
7. (*Optional*) For **Time Based Condition**, select a time condition from the drop-down menu or create a new condition, for details, see Add Time Based Conditions on page 42.
8. (*Optional*) For **Authentication Based Condition**, select an authentication condition from the drop-down menu or create a new condition, for details, see Create Authentication Based Conditions on page 43
9. For **Application Groups**, select one from the drop-down menu or create one, for details, see Add Applications to Groups on page 37
10. Select Agent-based or Agentless access mode.

    Note
    By default Agent-based or Agentless are checked when creating new policies.

11. If you do not want to use a secure network access, change the **Default Network Access** to **Allow**.
12. For the **Select VLAN from** ExtremeCloud IQ options, you can use your own VLAN or a VLAN from ExtremeCloud IQ .
    - 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
13. (*Optional*) Select a **VLAN** from the drop-down menu.
14. (*Optional*) Fabric Service Identified (ISID) .

15. Select *(Optional)* **Network Service Group** and continue as follows:
    a. Select **Add Network Service Group**.
    b. Select **Allowed** or **Denied**
16. Select **Add**.

Create Application Policies

About This Task

This task shows you how to create an application policy.

Procedure

1. Select **Create Policy**.
2. Select **Add Application Policy**.

   Create New Policy displays.
3. For **Policy Name**, enter at least three alphanumeric characters
4. (*Optional*) Enter a description.
5. For **User Groups**, select **Any User** or select a user group from the drop-down menu or create one.
6. (*Optional*) For **Location Based Condition**, select a location condition from the drop-down menu or create a new condition to use.
7. (*Optional*) For **Time Based Condition**, select a time condition from the drop-down menu or create a new condition to use.
8. (*Optional*) For **Authentication Based Condition**, select an authentication condition from the drop-down menu or create a new condition.
9. For **Application Groups**, select one from the drop-down menu or create one.
10. Select Agent-based or Agentless access mode.

    Note
    By default, Agent-based or Agentless are checked when creating new policies.

11. Select **Add**.

Results

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

Related Topics

Create Network Policies on page 40
Create Hybrid Policies on page 39

Create Network Policies

About This Task

This task shows you how to create a network policy.

Procedure

1. Select **Create Policy**.
2. Select **Add Network Policy**

   Create New Policy pop-up window displays.
3. For **Policy Name**, enter at least three alphanumeric characters
4. (*Optional*) Enter a description.
5. For **User Groups**, select **Any User** or select a user group from the drop-down menu or create one.
6. For **Device Groups**, select **Any Device** or select a device group from the drop-down menu or create one.

   Note
   If user and device groups are configured in the policy, for the policy to match for network access both access conditions must pass.

7. (*Optional*) For **Location Based Condition**, select a location condition from the drop-down menu or create a new condition to use.
8. (*Optional*) For **Time Based Condition**, select a time condition from the drop-down menu or create a new condition to use.
9. (*Optional*) For **Authentication Based Condition**, select an authentication condition from the drop-down menu or create a new condition.
10. If you do not want to use a secure network access, change the **Default Network Access** to **Allow.**
11. For the **Select VLAN from ExtremeCloud IQ** options, you can use your own VLAN or a VLAN from ExtremeCloud IQ.
    a. To use your own VLAN, ensure Select **VLAN from ExtremeCloud IQ** is deactivated (default) and enter a VLAN ID.
    b. To use a VLAN from ExtremeCloud IQ, activate **Select VLAN from ExtremeCloud IQ** and select a VLAN from the list.
12. *(Optional)* Select a VLAN from the drop-down menu.
13. (Optional) ISID - this is a fabric service identifier.
14. (Optional) Select **Network Service Group** and continue as follows:
    a. Select **Add Network Service Group**.
    b. Select Allowed or Denied.
15. Select **Add**.

Results

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

Related Topics

Create Application Policies on page 40
Create Hybrid Policies on page 39

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

About This Task

This task shows you how to create location based conditions.

Procedure

1. Select **Policies** > **Conditions**

   The **Location Based Conditions** window displays.
2. Select **Add Condition**.
3. For **Condition Name**, enter at least three alphanumeric characters.
4. (*Optional*) Enter a description.
5. (*Optional*) For **User Geographic Location(s)**, select one or multiple locations.
6. (*Optional*) For **Network Location**, select **SSID** or **Switch** from the drop-down and enter their respective information.
7. Select **Add**.

Results

Your location condition displays in the list.

Related Topics

Add Time Based Conditions on page 42
Add Authentication Based Conditions on page 43

Add Time Based Conditions

About This Task

This task shows you how to create time based conditions.

Procedure

1. Select **Policies** > **Conditions**.

   The **Location Based Conditions** window displays.
2. Select the **Time** tab at the top of the window.

   The **Time Based Conditions** window displays.
3. Select **Add Condition**.

4. For **Condition Name**, enter at least three alphanumeric characters.
5. (*Optional*) Enter a description.
6. (*Optional*) To enable access anytime, select **All Time Access**.
7. Select a start date and time for **Start Date & Time**.
8. Select an end date and time for **End Date & Time**.
9. Select how often you want the condition to repeat or not repeat.
10. (*Optional*) Select a repeat frequency.
11. Select **Add**.

Results

Your time condition displays in the list.

Related Topics

Add Location Based Conditions on page 42
Add Authentication Based Conditions on page 43

Create Authentication Based Conditions

About This Task

This task shows you how to create authentication based conditions.

Procedure

1. Select **Policies** > **Conditions**
   The **Location Based Conditions** window displays.
2. Select the **Authentication** tab at the top of the window.
   The **Authentication Based Conditions** window displays.
3. For **Condition Name**, enter at least three alphanumeric characters.
4. (*Optional*) Enter a description.
5. For the **Authentication Method**, select a method from the drop-down.
6. Select **Add**.

Results

Your authentication condition displays in the list.

Related Topics

Add Location Based Conditions on page 42
Add Time Based Conditions on page 42

Configure Microsoft Entra ID - Microsoft Azure - Intune Integration

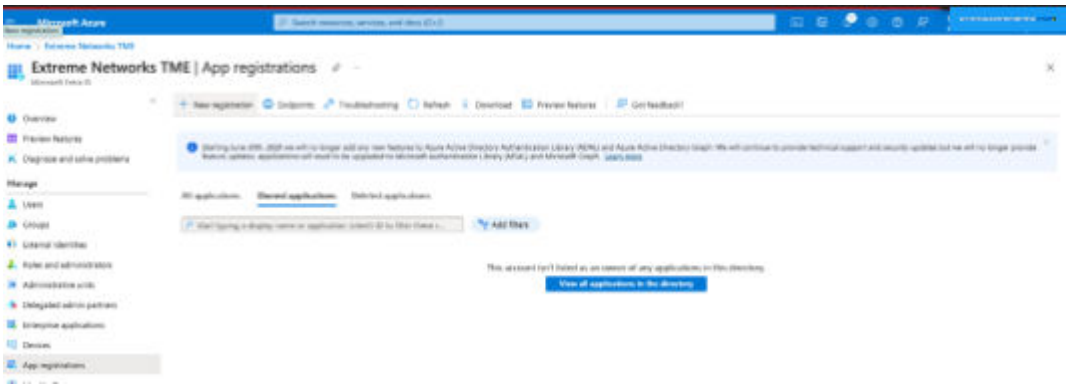
Before You Begin

About This Task

Use this procedure to configure Entra ID.

Procedure

1. In Entra ID, go to **App Registrations** and start a new registration.



2. Enter a name for the app and leave as **Single Tenant.**
3. Select **API Permissions** > **Microsoft Graph** > **Applications Permissions**.
4. Search for and enable the following items:
   - AIpplication: Application.Read.All
   - DeviceManagementManagedDevices:
     - DeviceManagementManagedDevices.PrivilegedOperations.All
     - DeviceManagementManagedDevices.Read.All
     - DeviceManagementServiceConfig
     - DeviceManagementServiceConfig.Read.All
   - Group: Group.Read.All
   - User: User.Read.All
5. Select **Update Permissions.**
6. To enable permissions, select **Grant Admin Consent for <domain>**.

   API permissions display.

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...

7. Select **Certificates & Secrets** > **New Client Secret.**
8. Select **New Client Secret** and enter a name for the secret.
9. Select the expiration time.
10. Select **Add**.

11. Save the generated value of the Secret in a secure place.

Note
After leaving this screen, you will not see the value of the secret.

12. Select **Overview.**
13. Copy the Application(client) ID and the Directory(tenant) ID.
14. Go to Integrate with Mobile Device Management on page 52.

Complete Universal ZTNA Identity Provider Access Onboarding

About This Task

This task shows you how to complete onboarding using ExtremeCloud Universal ZTNA.

Procedure

1. Select **Onboarding**.

   The welcome window displays.
2. Select **Secure Application Access**.

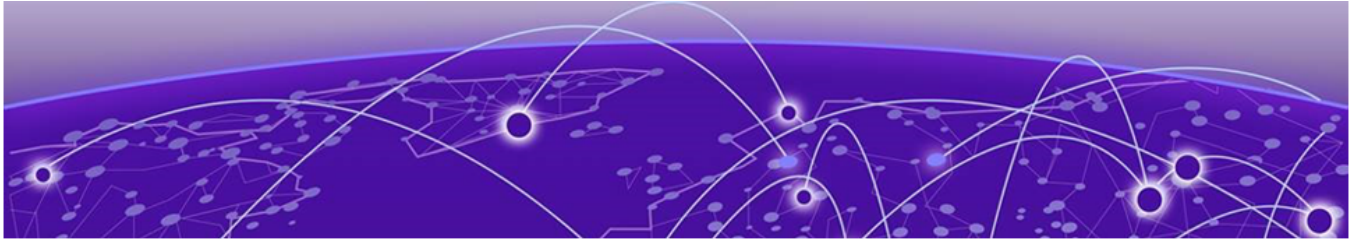
   The **Identity Provider** window displays with the ExtremeCloud Universal ZTNA IdP selected.
3. Select **Next**.

   The **Onboarding** window displays.
4. Configure Access Groups on page 24.
5. Configure Resources on page 28.
6. Configure Applications and Application Groups on page 32.

   You can skip this step if you are using Secure Network Access.
7. Configure Policies on page 38.

Results

Your onboarding is complete. Your users, applications, and devices can now access the network securely.



Additional Features

Insights

Insights allows you to view user identities, device identities and activity logs.

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.

User and Device Identities

Go to **Insights** > **Identities**. The following are a list of actions to take for user and device identities:

- View History
- Add to Device Group
- Add to User Group
- Re-Authenticate
- Allow Device Access
- Revoke Access
- Delete

View Activity Logs

About This Task

Activity Logs lets you 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

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

Procedure

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

The **Activity Logs** window displays.

What to Do Next

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.

Identity and Access Management

Add additional users, user groups, devices, device groups, and change the identity provider.

Changing the Identity Provider

Before You Begin

About This Task

If you want to change your Identity Provider after onboarding, follow this procedure.

Procedure

Select **Disconnect Identity Provider**,

The **Disconnect Identity Provider** pop-up window displays.

a. (*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.

b. Select **Initiate Assessment**.

   The **Disconnect IdP: Cleanup Assessment** pop-up window displays the list of policies. The assessment informs you of user groups synced in an IdP application and tells you to update or delete the policy.

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

c. 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.

d. Select **Cleanup & Disconnect**.

Results

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

Example

Additional Resources

Add additional sites, Deploy RadSec Proxies on page 30 deploy service connectors, manage RADIUS Servers, view network resources, and management certificates.

View Network Resources

Before You Begin

Network Resources consists of two sections, Network Devices and SSIDs.

The Network Devices section contains a list of your network devices, their current policy, and sync status. You can trigger a resync on the devices.

The SSIDs section contains a list of all SSIDs configured in XIQ. You can mark certain SSIDs as Universal ZTNA managed or Bring Your Own Devices (BYOD) managed.

About This Task

Manage and review certificates for the RadSec connection between network devices and ExtremeCloud Universal ZTNA.

Procedure

Select **Resources** > **Network Resources**.

Results

What to Do Next

Use the search function to find your device.

Manage Certificates

Before You Begin

From the **Certificate Management** screen, you can do the following:

- Update and download CA Trusted Root & Intermediate Certificates
- Manage RADIUS Server Certificates

- Match policies
- Verify the Online Certificate Status Protocol (OCSP) Responder certificate

About This Task

Use this procedure to manage certificates.

Procedure

1. Select **Resources** > **Certificate Management.**
2. To update or download CA Trusted Root & Intermediate Certificates, select  .
3. To update or invalidated RADIUS server certificates, select  .
4. To specify the certificate attribute to match a policy:
   a. In the **Certificate Attribute for Username** field, enter an email address.
   b. In the **Pattern to Match Device Name** field, enter a name.
5. To validate certificates, put a check mark in the **Validate Certificate via OCSP** check box.
6. In the **Enter URL** field, enter the responder server's URL or endpoint.
7. Select **Update.**

RADIUS Server

About This Task

Use this procedure to view RADIUS servers in your environment.

Procedure

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

Additional Policy Management

Add additional policies, conditions, device posture, and DNS servers.

Configure Device Posture

Before You Begin

About This Task

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

Procedure

1. Select a **Matching Criteria**.
2. Select a **Posture Check Frequency**.
3. Select the **Attributes** you want to use.
   - 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.
4. Select **Save**.

Results

Example

What to Do Next

Add DNS Servers

Before You Begin

About This Task

Procedure

1. Select **Policies** > **DNS**

   The **DNS** window displays.
2. Select **Add DNS Server**

   The **Add DNS Server** pop-up window displays.

   a. For the **Server Name**, enter at least three alphanumeric characters
   b. Enter an **IP Address**.
   c. Select a **Service Connector**.
   d. Select **Add**.

Results

Next, you will see a sequence of screen updates while UZTNA works to bring the DNS server up.

1. A connectivity test runs.
2. If the test passes, a confirmation message displays at the top of the window.
3. Your server displays in the server list.

4. The **Status** column displays **Activating**.
5. The **Status** changes to **Up** when the server is in service.

Example

What to Do Next

Integrations

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

Integrate with the Public Cloud

Before You Begin

There are three public cloud integration options:

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

About This Task

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

Procedure

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

Before You Begin

There are two options to add event connectors:

- Splunk
- API-based Log Collection

About This Task

This procedure allows you to add Splunk and use API to filter activity logs.

Procedure

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.**

Integrate with Mobile Device Management

Before You Begin

About This Task

Use this procedure to create a Microsoft Intune integration.

Procedure

1. From the **Mobile Management Device (MDM)** screen, select **Add Integration.**
2. Update the following fields:
   - Client ID
   - Client Secret
   - Tenant ID
3. Select **Validate Information**.
4. If the configuration is valid, select **Add Integration.**

   Intune synchronization happens in the background and devices display.

   Note
   If there are integration errors, check the application permissions that was created in Entra ID.

Monitor

Alerts

Before You Begin

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

About This Task

Use this procedure to view, filter and export alerts.

Procedure

1. Select **Monitor** > **Alerts.**
2. Select the time period for which you wish to display alerts.
3. To refresh the screen, select .
4. To sort alerts, use the **Filter** icon.
5. To download alerts, select **Export to CSV** .

Troubleshooting

About This Task

Use this procedure to evaluate the network policy.

Procedure

1. Select **Monitor** > **Troubleshooting.**

2. Update the following fields:
   - MAC address
   - Authentication Type
3. Include optional fields to run an authentication test.
4. The following fields are optional:
   - Username
   - Password
   - Service Set Identifier (SSID)
   - AP/Switch IP
   - Switch Port
   - Date
   - Time
5. Select **Run Test.**

   If you entered a username and password, the matching policy and authorization status displays. You can expand the policy results to see the order that each policy was checked and why a policy was not a match.

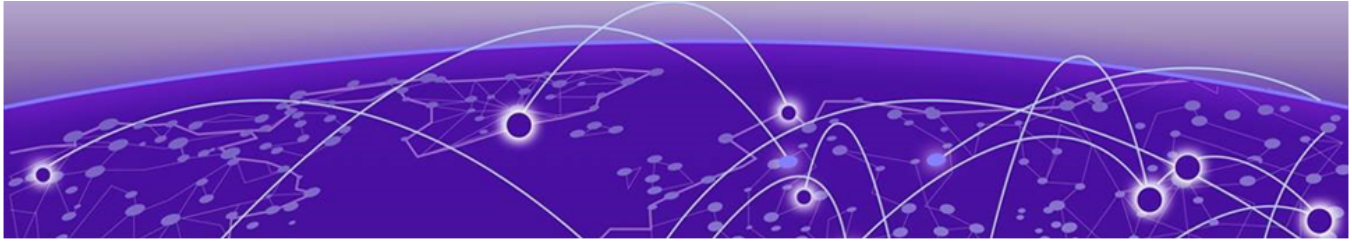
Subscriptions

About This Task

Use this procedure to view and filter subscriptions.

Procedure

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  .



ExtremeCloud IQ Wireless Integration

This chapter desribes how Universal ZTNA can be used for mapping policies based on Universal ZTNA conditions and returning a filter ID that matches a pre-provisioned policy using ExtremeCloud IQ Wireless. RADIUS and Policy must be configured using ExtremeCloud IQ Wireless.

Integrate ExtremeCloud IQ Wireless with Universal ZTNA

Before You Begin

Complete the onboarding steps found in Configure UZTNA Access on page 12, specifically Deploy RadSec Proxies on page 30.

About This Task

To integrate ExtremeCloud IQ Wireless with Universal ZTNA, do the following:

Procedure

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**, create an external RADIUS Server Group with your Radsec proxy IP address by selecting + under **Authenticate via RADIUS Server**. This is the same IP address used for the Radsec proxy deployment in Deploy RadSec Proxies on page 30.

5. In the **Configure RADIUS Servers** window, configure the server details and select **Save**.
6. Identify the required filter-ID value needed.

   You will use this filter-ID in the assignment rule for the name of the Universal ZTNA policy in the next step. You can find the filter-ID in the **User Profile Assignment Rule** section of the SSID configuration under the **Value** column heading.
7. Create Universal ZTNA policies using the ExtremeCloud IQ filter-IDs as the policy name.

   The policy name is used in the RADIUS response for user authentication: as follows:

   - Select**Add Policy** > **Network Policy**
   - Set the name of the policy to the filter-ID from the assignment rule and add access groups and conditions. The network section is ignored for ExtremeCloud IQ policies; only the name, access groups (user groups or device groups), and conditions are used. If this policy is being used with another operating system,complete the network sections..
8. (Optional) You can force a reauthorization in ExtremeCloud IQ wireless by doing the following:
   a. From the ExtremeCloud IQ main navigation, select **ML Insights** > **Network 360 Monitor**
   b. Select the floor map where the client access point is located.
   c. Select the access point and select **Disconnect** next to your client's station address.

Configure the Network Policy

Before You Begin

About This Task

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

Procedure

1. Log into ExtremeCloud IQ
2. Select **ConfigureNetwork Policy**
3. Select **Add Network Policy**.
4. Select **Wireless.**
5. Enter a name for the policy.
6. *(Optional)* enter a description.
7. Select **Save**.
8. Select **Next** to configure Wireless.

Example

What to Do Next

Go to Configure SSID and Wireless on page 57.

Configure SSID and Wireless

Before You Begin

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

ExtremeCloud IQ supports the following configurations:

- Enterprise 802.1X Authentication with Universal ZTNA RadSec
- Enterprise 802.1X AutheExtremeCloud IQntication with Universal ZTNA RadSec Proxy
- Enterprise MAC Authentication with Universal ZTNA RadSec
- Open MAC Authentication with Universal ZTNA RadSec Proxy

Note
Universal ZTNA RADSEC and ExtremeCloud IQ cloud authentication services cannot co-exist. If any cloud authentication objects are in the virtual IQ, you must use the RADSEC Proxy.

About This Task

Use this procedure to configure SSID and wireless.

Procedure

1. Select + to create a new SSID.
2. In the **Wireless Network** section, **Name (SSID)** field, enter the SSID name.
3. In the **Broadcast Name** field, enter the broadcast name.
4. Configure SSID usage as follows:
   a. For Enterprise access, select **SSID Usage** > **SSID AUTHENTICATION** > **Enterprise WPA / WPA2 / WPA3**.
   b. For Open access (MAC with RadSec Proxy Only), select **SSID Usage** > **SSID AUTHENTICATION** > **Open**.
5. *(Optional)* Enable MAC authentication as follows:
   a. In **SSID Usage** select **MAC AUTHENTICATION**.
   b. Select the **MAC AUTHENTICATION** slider and toggle it **ON**.
6. Configure SSID authentication settings as follows:
   a. For Universal ZTNA RadSec, in the **Authentication Settings** section, select the **Authentication with ExtremeCloud Universal ZTNA** slider and toggle it **ON.**
   b. For Enterprise 802.1X with Universal ZTNA RadSec Proxy, to add a Default RADIUS Server Group, select **Authentication Settings** > **Authenticate via RADIUS Server** > + .
   c. For Open MAC with Universal ZTNA RadSec Proxy, to add a Default RADIUS Server Group, select **SSID Usage** > **MAC AUTHENTICATION** > **Authenticate via RADIUS Server** > + .
7. From the Configure RADIUS Server screen, configure a RADIUS server as follows:
   a. In the **RADIUS Server Group Name** field, enter the group name for a RADIUS server.

b. Add or select an existing external RADIUS Server.
c. Select **Save RADIUS**.

Manage SSID in Universal ZTNA

Before You Begin

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.

About This Task

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

Procedure

1. Log into UZTNA.
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 is named as 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 by selecting **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

Universal ZTNA creates an IP Firewall Policy for a hybrid or network policy created in Universal ZTNA when network service groups are configured for that 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 Engines (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
Configuration changes on ExtremeCloud IQ that are not yet applied are applied along with automatic updates from Universal ZTNA.

The administrator can also manually trigger this deployment by (Re)-Syncing the configuration from the Resources > Network Resources > Network Devices portal.

Appendices

SAML-based SSO in Microsoft Server 2016 AD

Before You Begin

About This Task

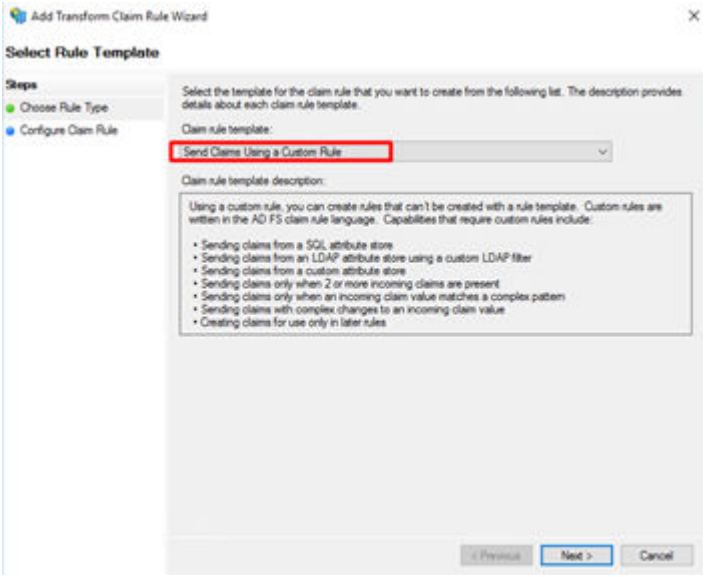
Use this procedure to set up SAML-based SSO in Microsoft Server 2016 AD.

Procedure

1. Go to your **MS 2016 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.

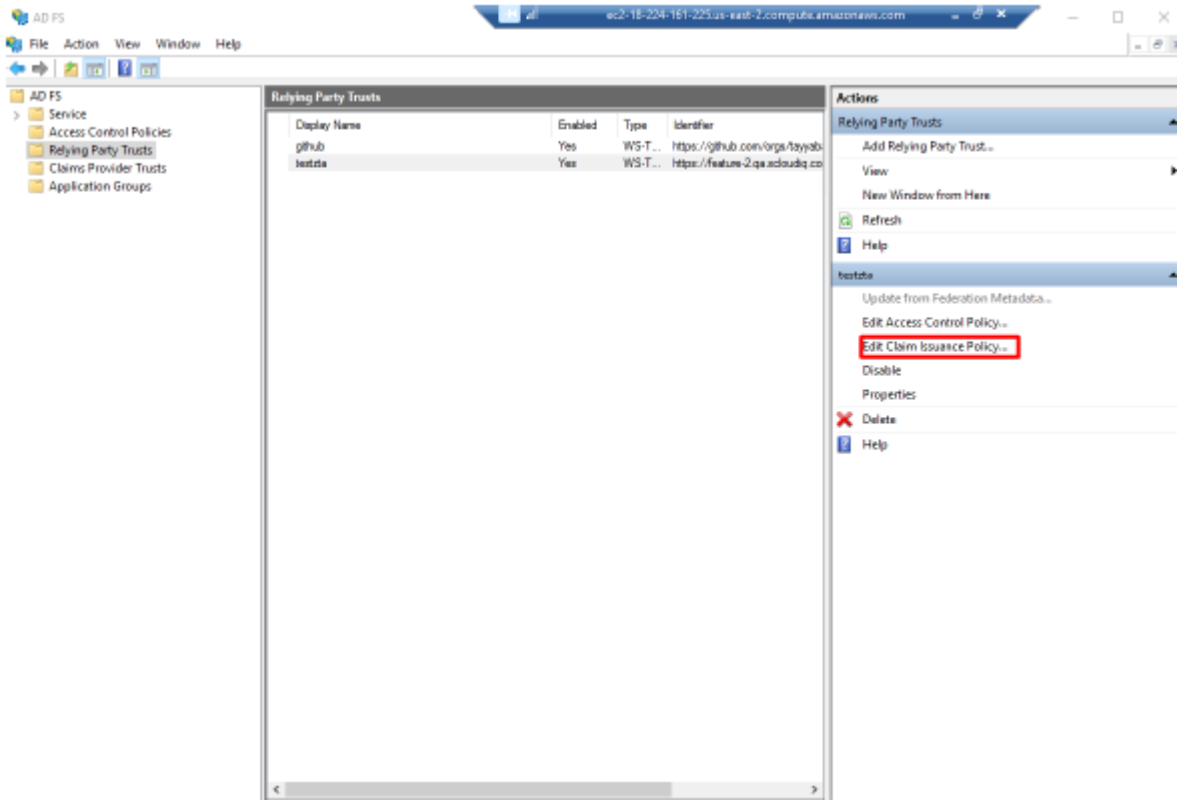
a. Go to **ADFS Manager** > **Relying party trust add claim issuance policy** > **Add Rule.**
b. From the **Select Rule Template** screen, in the **Claim Rule Template** field, select **Send Claim Using a Custom Rule.**



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. From the **Select Rule Template** screen, in the **Claim Rule Template** field, select **Send LDAP Attributes as Claims.**

h. Select **Next.**

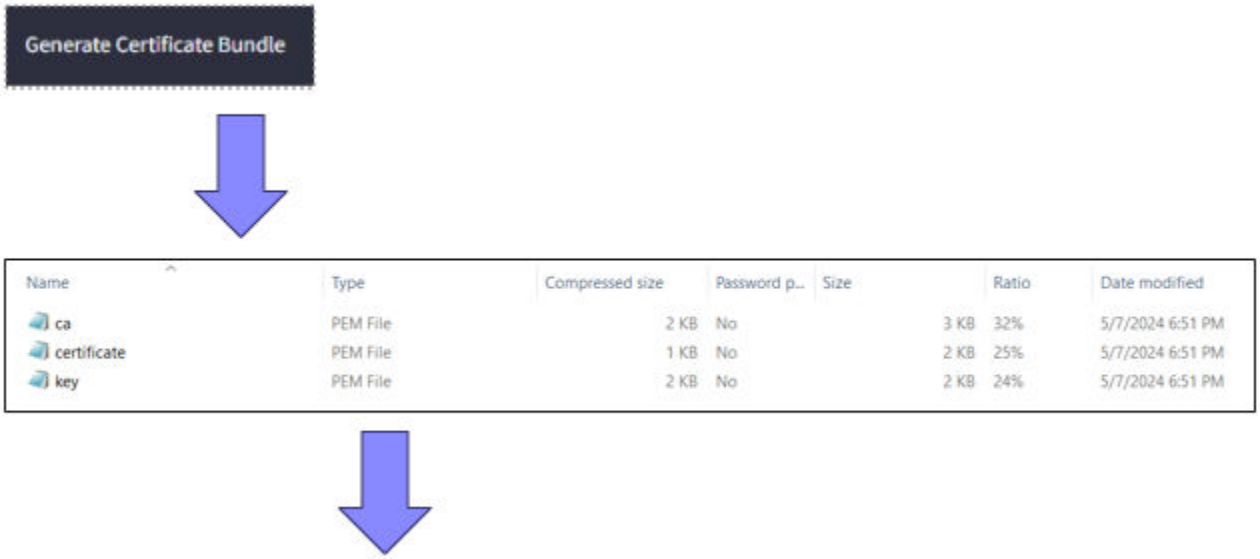
i. Add a Rule.

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

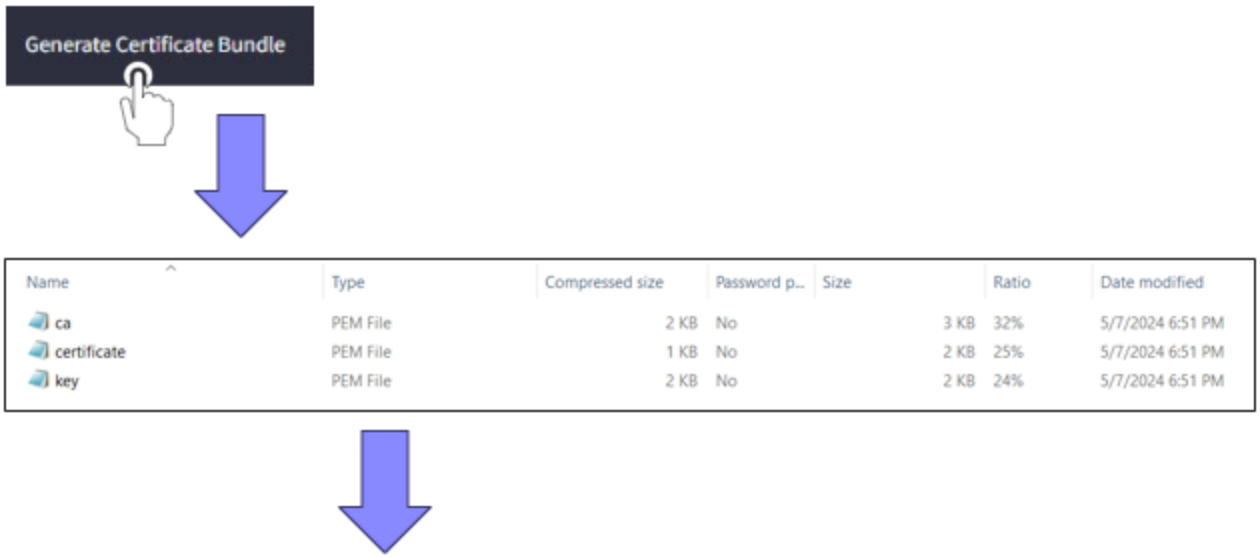
Optional Configuration for Auto-sense Eapol

```
#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




```
# 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 UZTNA


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

Apply Netlogin/Policy Configuration to the Switch

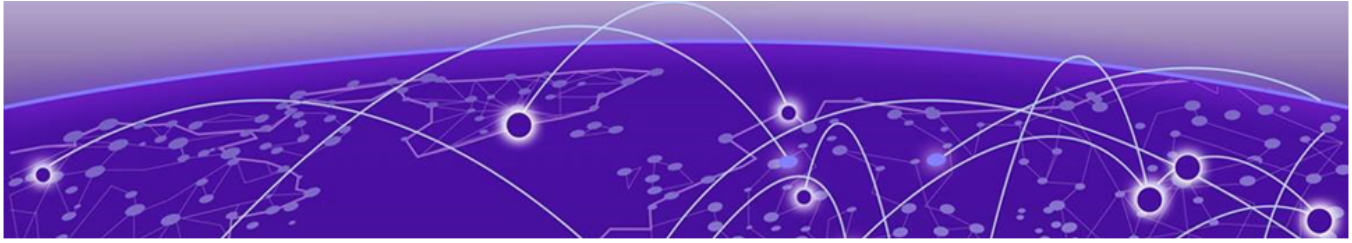
1. Configure the policy for dACL and VLAN authorization.

```
# configure policy rule-model access-list

# config policy vlanauth enable
```

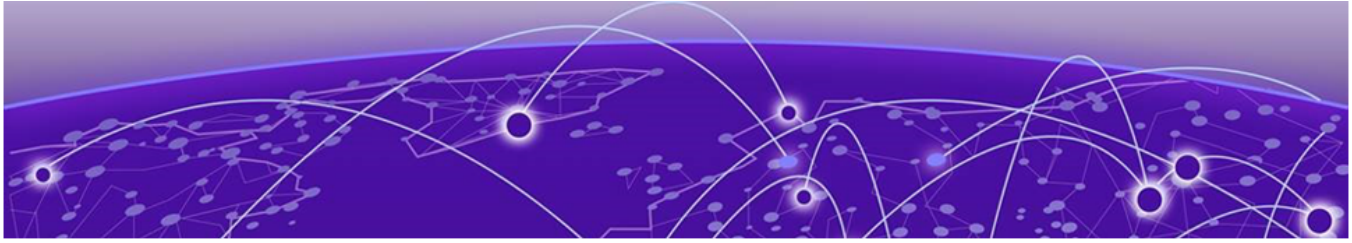
```
# config policy maptable response both

# 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
```



Glossary



Index