# ExtremeCloud IQ (New) v25.15.0 User Guide

Comprehensive Management and Usage Instructions

9041305-00 Rev AA
October 2026

Copyright © 2026 Extreme Networks, Inc. All rights reserved.

## Legal Notice

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

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

## Trademarks

Extreme Networks and the Extreme Networks logo are trademarks or registered trademarks of Extreme Networks, Inc. in the United States and/or other countries.

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

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

## Open Source Declarations

Some software files have been licensed under certain open source or third-party licenses. End-user license agreements and open source declarations can be found at: https://www.extremenetworks.com/support/policies/open-source-declaration/



# Table of Contents


Abstract ..... xii
Preface ..... xiii
Text Conventions ..... xiii
Documentation and Training ..... xiv
Open Source Declarations ..... xv
Training ..... xv
Help and Support ..... xv
Subscribe to Product Announcements ..... xvi
Extreme Support Portal ..... xvi
Send Feedback ..... xviii

**Welcome to ExtremeCloud IQ (New) ..... 19**
Create an Extreme Platform ONE Networking Account ..... 20
Your ExtremeCloud IQ (New) Password ..... 20
Unified Login Page ..... 21
Log in to ExtremeCloud IQ (New) ..... 21
Multiple Accounts ..... 22
Forgotten Password ..... 23
Change Password ..... 23
Log in with Single Sign-On ..... 24
Unified Logout ..... 25
Browser Support and Display Settings ..... 25
Desktop Browsers ..... 25
Display Settings ..... 25
Navigation Pane ..... 26
Content Pane ..... 27
Extreme Applications and the 9-dot Menu ..... 29
CoPilot ..... 30
Common Functionality ..... 30
Pagination ..... 36
Edit Your Profile Settings ..... 37
Choose a Theme ..... 37

**Monitoring | Dashboard ..... 38**

**Monitoring | Visualize ..... 40**
View Selector ..... 40
Customize the Visualize View ..... 41
Device Icons ..... 43
Topology Legends ..... 44
Geographic View ..... 45
Heat Map View ..... 46
View Device Inventory ..... 50

Device Summary and Actions Menu 51
Create a Device Filter from the Heat Map View 62
Import a Third-Party RF Map 62
View Antenna Patterns 64
Edit a Heat Map 64
Access View 71
Device Detection 71
Device Group 72
Update Topology 72
Inspector Panel 73
View the Inspector Panel 73
View the Device Inspector Panel 74
View and Acknowledge Alerts 75
View Device 360° 76
AutoSave Device Layout and Density 76
Search an Element 77
Topology Map Settings 77
Configure the Display Options 77
Manage 78
User Roles Supported in Visualize View 78

**Monitoring | Alerts 80**
Manage Alerts 80
Alert Details 81
Use the Filter and Columns Side Bar 82
View and Acknowledge Alerts 82
Add a Site Policy 82

**Monitoring | Network Devices 83**
Supported Universal Access Points 84
AP3000 Series Radios and 6 GHz Support 85
AP4000/AP4000-1 Radios and 6 GHz Support 88
AP5000 Series Radios and 6 GHz Support 90
Fourth Radio Dedicated Sensor Support 93
Universal AP Boot and Onboarding Process 94
Boot Up Process 94
CAPWAP Connection 95
Universal/Worldwide SKU Region and Country Fingerprinting 96
Changing Operating System Persona for Onboarded APs 96
Onboarding to ExtremeCloud IQ (New) 97
AFC Overview 99
Indoor/Outdoor AFC Support 100
Anchor and Non-Anchor APs 102
6 GHz Radio Power AFC 103
6 GHz Radio — Standard Power Operation without AFC Approval 104
GeoLocation Agent 105
GeoLocation Coordinates 106
AP Placement for AFC 108
Adding Controllers and Appliances for Locally Managed Devices 110
Supported Management Options 110

The Appliances Tab ... 111
Universal Compute Platform Support ... 111
Supported Applications ... 111
Device Health ... 112
Interactive Console Access ... 112
Extreme Tunnel Concentrator Support ... 112
Network Devices | Device Status ... 112
Device List Views ... 113
Device Status Icons ... 119
Filter the Device List by Status ... 125
Network Devices | Device Health ... 125
Device Health | Wired ... 126
Device Health | Wireless ... 126
Device Health | Discovered ... 127
Network Devices | Usage & Capacity ... 127
Usage & Capacity | Wired ... 128
Usage & Capacity | Wireless ... 128
Usage & Capacity | Discovered ... 129
Network Devices | Add Devices ... 129
Add Devices Manually ... 129
Import Devices ... 132
Upgrade Network Device Firmware ... 133
Device 3-Dot Menu Actions ... 134
Enhanced Discovery ... 138
Locate Device ... 139
Perform a RADIUS Test ... 140
Upgrade Firmware Settings ... 141
Diagnostics CLI Commands ... 142
VLAN Probe ... 143
Override Supplemental CLI ... 144
AFC Geolocation Report ... 146
Delete a Device from the Network ... 148
Remove a Stack Member ... 150
Replace a Stack Member ... 151
Push Device-Level Configuration ... 152
Configuration Push Scheduling Behavior ... 154
Packet Capture ... 155
Run a Packet Capture Session ... 155
View Packet Capture Results ... 158
Configure Devices ... 159
Configure Wired Devices ... 160
Configure Fabric Settings ... 183
Configure Wireless Devices ... 187
Configure Devices ... 203
Device 360 View ... 204
Wired Device 360 View ... 204
Wireless Device 360 View ... 211
Controller Device 360 View ... 219
Site Engine Managed Device 360 View ... 221

Tunnel Concentrator Device 360 View....225
Universal Compute Platform Device 360 View....228
Discovered Device 360 View....232
Device 360 Actions Menu....235

**Monitoring | Clients....242**
Monitor Clients....242
Wireless Inspector Panel Settings....244
Client Three-dot Menu....247
Client 360 View....248
Enable Real-Time Troubleshooting....257
Monitor Users....257
User Details Panel....259
Monitor Applications....259

**Reports....261**
Filters for On-Demand Analytics and Reports....261
On-Demand Analytics....261
Generate On-Demand Analytics....262
Create a Report from On-Demand Analytics....263
Scheduled Reports....264
Create Custom Reports....265
Edit Custom Reports....266
Add or Remove Email Report Recipients....268
Delete Reports....268

**Configuration | Sites....269**
Sites....269
Import a Site Tree....270
Export a Site Tree....270
Add a Site....270
Add a Site group....271
Add a Building....271
Move a Building....272
Add a Floor....272
Upload a Floor Plan....273
Edit a Site....274
Move a Site....274
Export a Floor Plan....274
Clone a Building....274
Delete a Site....275
Delete a Building or a Floor....275

**Configuration | Network Policies....276**
Configure an Express Policy....277
Add a Network Policy....278
Configure Policy Settings....279
Configure DNS Server Policy Settings....279
Configure NTP Server Policy Settings....281
Configure SNMP Server Policy Settings....282
Configure Syslog Server Policy Settings....285
Configure Device Credentials Policy Settings....287

Configure the Device Time Zone....287
Configure Hive Policy Settings....288
Configure Management and Native VLAN Policy Settings....291
Configure IP Tracking Policy Settings....293
Configure LLDP/CDP Policy Settings....295
Configure Management Options....296
Configure Traffic Filters Policy Settings....305
Configure MGT IP Filters....306
Deploy a Network Policy....307
Configure the SSID for a Standard Wireless Network....308
Cloud User Group Settings....311
Local User Group Settings....312
Add a User Profile....315
SSIDs....316
SSID Usage in Standard Wireless Networks....316
Configure Client Mode AP Profile using Wired Connection and Device Template....328
Captive Web Portals....328
Hotspot....340
RADIUS Authentication....348
Configure VLAN Settings....362
Apply Different User Profiles to Clients and User Groups....376
Customize Advanced Access Security Controls....377
Customize Wireless Network Optional Settings....379
Settings for Multi-Link Operation....388
Electronic Shelf Labels....388
Supported APs....388
Supported Vendors....389
Important Considerations for ESL Deployments....389
Connect the ESL Communicator....389
Configure ESL in a Device Template....390
Configure ESL as a Device Override....390
ESL Settings....390
Configure Device Templates....391
Configure AP Templates....392
Configure a Switch Template....419
Configure Port Types....436
Aggregate LAG and LACP Ports....437
Configure Supplemental CLI....437
Configure Classification Rules for a Device Template....438
Add a Cloud Config Group....439
Fabric Attach....439
Configure Fabric Attach....440
Configure Device Data Collection and Monitoring Options....441
Configure the BLE Service....442
Configure Presence Analytics....445
Configure WIPS....445
WIPS Policy Settings....446
Configure a Location Server....449
Install CA Certificates....450

Configure a Layer 2 IPsec VPN Service....450
Layer 2 VPN Services Settings....451
Settings for Multi-Link Operation....453

**Configuration | Guest Access....454**

Guest Access | Splash Templates....454
Create a Splash Template....455
Clone a System Template....457
Download a System Template....457
Upload a User Template....457
Apply a Splash Template....458
Guest Access | Users....458
Create a Guest User....458
Download Guest User Details....459
Delete Guest Users....459
Create Bulk Vouchers....459
Guest Access | Settings....460
Add an Access Group....460
Add an Authorization Policy....461
Guest Access | Notification Policies....461
Add a Notification Policy....462
Guest Access | Onboarding....462
Onboarding Policy....462
Onboarding Rules....463
Add an Onboarding Policy....463

**Configuration | Common Objects....465**

Policy Configuration....466
Configure AP Templates....466
Configure Auto-Provisioning....467
Configure Bonjour Gateway Settings....470
Configure Classification Rules....472
Configure Client Monitor Profiles....474
Configure Cloud Config Groups....474
Configure Fabric Attach Profiles....475
Configure Hives....476
Configure Hotspot Profiles....479
Configure Hotspot Service Provider Profiles....479
Configure IoT Profiles....479
Manage Port Types....480
Delete Instant Secure Port Profiles....480
Delete Instant Port Profiles....480
Configure Radio Profiles....481
Configure SDR Profiles....490
Configure a Schedule....491
Configure SSIDs....492
Configure a Switch Template....492
Configure URL Filtering Detail....493
Configure URL Filtering....494
Configure User Profiles....495

Basic Configuration....495
Configure Application Sets....495
Configure Client Mode Profiles....496
Configure DHCP Servers and DHCP Relay Agents....497
Configure DNS Services....499
Configure IP Objects/Host Names....501
Configure MAC Objects/MAC OUIs....502
Configure Notification Templates....503
Configure OS Objects....504
Configure VLANs....505
Configure a VLAN Group....505
Configure Supplemental CLI Objects....506
Security Configuration....507
Configure AirDefense Policies....507
Configure Firewalls....508
Configure MAC Firewall Policies....509
Configure MGT IP Filters....510
Configure Traffic Filters....510
Configure WIPS Policies....511
QoS Configuration....512
Quality of Service....512
Classifier Maps....513
Configure Classifier Maps....514
Configure Marker Maps....517
Configure Rate Control & Queuing....518
Management Configuration....519
Configure DNS Servers....519
Configure NTP Servers....520
Configure SNMP Servers....521
Configure Syslog Servers....522
Network Configuration....522
Configure Access Consoles....523
Configure ALG Services....524
Configure LLDP/CDP Profiles....525
Configure IP Tracking Groups....526
Configure Layer 2 IPsec VPN Services....526
Configure Location Servers....532
Configure Management Options....535
Configure Tunnel Concentrator Services....535
Configure Tunnel Concentrator Address Pool (TCAP) Profiles....541
Configure Tunnel Policies....542
Configure Network Services....545
Configure a Subnetwork Space....546
Configure Firewalls....549
Configure VPN Services....550
Authentication Configuration....552
Clone AAA Server Settings....552
Configure Captive Web Portals....552
Configure External RADIUS Servers....554

Certificate Configuration....554
Certificate Management....554
Create a Certificate Bundle....560
Clone a Common Object....561
Delete a Common Object....561

**Configuration | User Management....562**
Add a User....563
User Settings....563
Bulk Create Users....564
Bulk Create Settings....565
Add a User Group....565
Add a User to a User Group....566
Bulk Add Users to a User Group....566
Configure a Private Client Group....566
Unlock Users....567
Perform a RADIUS Test....568
Unbind a Device....568
Guest User Accounts....569
PPSK....569
Captive Web Portal....569
Captive Web Portal and PPSK....569
Configure PPSK Guest User Accounts....570

**Task Center....571**
Manage Tasks in the Task Center....571
Task Details....572
Task Names....573
View Task Details and Run History....574

**Subscriptions & Services....575**

**Administration & Settings | Access Management....576**
Role-Based Access....576
Role-Mapping Between Extreme Platform ONE Networking and Other Applications....577
Security-Specific Roles and Features | ExtremeCloud IQ (New)....578
Role-Based Feature Access | ExtremeCloud IQ (New)....578
Role-Based Site Awareness....579
Users & Roles....579
Role-Based Access....580
Create a New User....580
View the List of Users....582
Edit, Disable, or Delete a User Account....583
Configure the Idle Session Timeout....584
Identity Providers | Network & Applications....584
Microsoft Entra ID....585
Google Workspace....622
Okta....652
IdP Network & Applications | Support Multiple IdPs....688
Identity Providers | Management....688
Add an IdP Profile....692
Manage IdP Profiles....697

Microsoft Entra ID | Create IdP Application 700
Okta | Create IdP Application 705
Credential Distribution Groups 712
Create a New Credential Distribution Group 712
Configure the Idle Session Timeout 713

**Administration & Settings | Alert Policies 714**
Global Policy 714
Site Policy 714
Add a Site Policy 714

**Administration & Settings | External Notifications 716**
Add Email Recipient 716
Add Webhook 717
Add ServiceNow Account 718
Add a Rule for Subscriptions 718
Add a Rule for Contracts 719

**Administration & Settings | Global Settings 720**
Service Management 720
Enable Wireless Client Tracking 720
Backup & Restore 721
VIQ Management 721
Set Default Device Password 723
Integrations 723
Create a New API Key 723

**Administration & Settings | Logs 725**
Delete KDDR (Kernel Diagnostic Data Recorder) Logs 726



# Abstract

This user guide for ExtremeCloud™ IQ (New) version 25.15.0 describes how network administrators manage wired and wireless networks through the cloud-based Extreme Platform ONE Networking interface. It covers account creation, unified login, password management, navigation, and browser requirements (latest 64-bit Chrome, Edge, Firefox, Opera, or Safari; 1280 x 1024 minimum resolution). Monitoring chapters explain the dashboard, topology, geographic, and heat map views, alerts, devices, clients, and reports. They include device onboarding, firmware upgrades, packet capture, and Device 360 views. Configuration chapters address sites, network policies, SSIDs, device templates, supplemental CLI, Fabric Attach, WIPS, BLE, presence analytics, location servers, CA certificates, guest access, and common objects for security, QoS, and authentication. Administration topics include access management, alert policies, external notifications, global settings, logs, subscriptions, and the Task Center. Universal Compute Platform and Extreme Tunnel Concentrator support and diagnostic procedures, such as KDDR log deletion, are also documented.

# 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, the product is referred to as *the switch*.

**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.<br>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.

## Extreme Support Portal

The Extreme Networks Extreme Support Portal provides access to:

- License management
- Firmware downloads
- Case management
- GTAC Knowledge base
- And more

To access the portal, you must first create an account. The Extreme Support Portal provides separate registration forms for End Customers and Partners.

Before you begin, gather the following: A valid corporate email address — required to receive the appropriate level of portal access. Your company details: company name, address, phone number (include country code if outside the US), job title, and job role. At least one supporting identifier: Sold-to number, serial number, contract number, or Purchase Order (PO) number.

*Create an End Customer Extreme Support Portal Account*

The Extreme Support Portal provides separate registration forms for End Customers and Partners. Use this task to create an End Customer account.

**Note**
If you are adding a new user to an existing account, the new user must complete and be vetted through the same registration process.

The portal registration page is at https://extreme-networks.my.site.com/.

1. Go to the Extreme Support Portal and select **Login or Signup** on the login page.
2. On the login page, select **Create a new Extreme Customer Portal Account** .
3. Complete all required fields (marked *). Use your corporate email address to ensure the appropriate access level.

**Important**
Do not register with a personal email address.

4. Read the Support Portal Terms of Use and select the acknowledgment check box to accept.

   **Important**
   You must accept the Terms of Use before you can submit the form. You can adjust or withdraw consent at any time through the Email Preference Center.

5. Select **Register**.

   A confirmation message appears on the page and a password setup email is sent to your corporate email address.
6. Open the password setup email and follow the instructions to create your portal password.

   **Tip**
   If the email does not appear in your inbox within a few minutes, check your spam or junk mail folder.

7. To log in to the support portal go to: https://extremesaas.my.site.com/.

*Create a Partner Extreme Support Portal Account*

The Extreme Support Portal provides separate registration forms for End Customers and Partners. Use this task to create a Partner account.

The portal registration page is at https://extreme-networks.my.site.com/.

1. Go to the Extreme Support Portal and select **Login or Signup** on the login page.
2. On the login page, select **Create a new Extreme Partner Portal Account**.
3. Complete all required fields (marked *). Use your corporate email address to ensure the appropriate access level.

   **Important**
   Do not register with a personal email address.

4. Read the following terms and select the required check boxes:
   - Support Portal Terms of Use
   - Extreme Networks Standard Reseller Terms and Conditions
   - Trade Compliance Terms and Conditions

   You can adjust or withdraw consent at any time through the Email Preference Center.
5. Select **Register**.

   A confirmation message appears on the page and a password setup email is sent to your corporate email address.
6. Open the password setup email and follow the instructions to create your portal password.

   **Tip**
   If the email does not appear in your inbox within a few minutes, check your spam or junk mail folder.

7. To log in to the support portal go to: https://extremesaas.my.site.com/.

## 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 Product-Documentation@extremenetworks.com.

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

# Welcome to ExtremeCloud IQ (New)

Create an Extreme Platform ONE Networking Account on page 20
Unified Login Page on page 21
Unified Logout on page 25
Browser Support and Display Settings on page 25
Navigation Pane on page 26
Content Pane on page 27
Common Functionality on page 30
Edit Your Profile Settings on page 37
Choose a Theme on page 37

ExtremeCloud IQ is an industry-leading approach to cloud-driven networking, designed to take full advantage of Extreme Networks end-to-end networking solutions.

ExtremeCloud IQ (New) offers the following:

- Unified, full-stack management of access points, switches, and SD-WAN
- Innovative ML technologies to analyze and interpret millions of network and user data points from the edge to the data center
- Network automation and intelligence to streamline operations

**Important**
For information about browser support and resolution settings, see Browser Support and Display Settings on page 25.

**Note**
During the customer onboarding process, Extreme Cloud IQ (NEW) automatically creates the **Organization** automatically creates the for sites. The **Organization** name is the same as the **Company** name that you provided for your account.

ExtremeCloud IQ (New) consists of the following major sections:

- Navigation pane
- Content pane

## Create an Extreme Platform ONE Networking Account

Use this task to create an ExtremeCloud IQ (New) account.

**Note**
With an Extreme Platform ONE Networking account, you have access to ExtremeCloud IQ. The newly created Extreme Platform ONE Networking administrator account is also an ExtremeCloud IQ administrator account.

1. Near the bottom of the **Log In** dialog, select **Register to Get Started**.
2. In the **Create an Account** dialog, type your **Business Email**, and then select **Continue**.

   The system sends an email asking you to verify your email address.
3. Follow the instructions in the email to verify your email address.
4. Provide the following information:
   a. In the fields, type the required information about you, and then select **Continue**.

      **Note**
      Only alphabetic characters (A-Z) are accepted in the fields.

   b. In the fields, type the required information about your company, and then select **Continue**.
   c. Review and accept the account notices.
5. Select **Create Account**.

   The system sends a registration email to the email address that you used to create your account. Follow the link in the email to set up your password and complete the registration process.

   Creating a new Extreme Platform ONE Networking account automatically starts the process of creating an Extreme Portal account. If you do not already have an Extreme Portal account, you will receive an email with instructions on how to set a password for your new Extreme Portal account. For information about purchasing required licenses and linking to your Extreme Portal account, see *Extreme Platform ONE Networking and ExtremeCloud IQ Subscription and Licensing Guide*.

Related Links

Your ExtremeCloud IQ (New) Password on page 20

## Your ExtremeCloud IQ (New) Password

Strong passwords provide better account security. ExtremeCloud IQ (New) requires that passwords meet the following requirements:

- Minimum 12 characters
- Maximum 64 characters (supports passphrases)
- At least one uppercase character
- At least one lowercase character

- At least one digit
- At least one special character

**Note**
To further enhance password strength, ExtremeCloud IQ (New) blocks commonly used passwords, even if they meet the requirements.

ExtremeCloud IQ (New) enforces these requirements for new password creation and for password resets.

## Unified Login Page

The Extreme Networks unified login page grants access to applications based on licenses and simplifies migration. Customers having only Extreme Platform ONE Standard Networking licensed devices or a mix of Platform ONE Standard Networking and ExtremeCloud IQ Pilot licensed devices are directed to Extreme Platform ONE Networking. From there, you can navigate to ExtremeCloud IQ (Classic) from the 9-dot application menu, ensuring access to all ExtremeCloud IQ (Classic) features.

Extreme Platform ONE Networking licenses do not provide access to ExtremeCloud IQ (New). ExtremeCloud IQ (New) is available for customers having only ExtremeCloud IQ Pilot licenses and provides a limited subset of Extreme Platform ONE Networking features. ExtremeCloud IQ (Classic) customers can open ExtremeCloud IQ (New) from the 9-dot menu.

For more information about other applications and the 9-dot menu, see Extreme Applications and the 9-dot Menu on page 29.

Related Links

Extreme Applications and the 9-dot Menu on page 29

### Log in to ExtremeCloud IQ (New)

Use this task to log in to ExtremeCloud IQ (New).

**Note**
Available widgets, menu selections, and action permissions depend on your role. For more information, see Role-Based Feature Access.

1. In a web browser, go to https://extremeplatformone.com, and enter your ExtremeCloud IQ credentials.

   **Note**
   If you don't have an existing ExtremeCloud IQ account, see Create an Extreme Platform ONE Networking Account on page 20.

2. Select **Log In**

   The **Log In** button is disabled and changes to display a loading indicator while your credentials are verified. If authentication is unsuccessful, the button is re-enabled so you can try again.

   **Note**
   If you are an ExtremeCloud IQ customer and you have only ExtremeCloud IQ Pilot licenses, ExtremeCloud IQ (New) opens. If you have a mix of Pilot and Extreme Platform ONE Standard Networking subscriptions, or all Platform ONE Standard Networking subscriptions, Extreme Platform ONE Networking opens.

3. In the **Select a Network** dialog, select the account that you want to log in to.

   This dialog appears only if you have multiple accounts. After you log in, you can switch to another account. For more information, see Switch Accounts on page 23.

## Multiple Accounts

**Note**
A tenant, also known as a Virtual IQ (VIQ), is an isolated environment that contains the data, devices, policies, users, and permissions for an organization. The terms are used interchangeably.

Every user has a *"Home"* account on their primary tenant/VIQ. You can also have multiple external accounts on other tenants, to which you have been granted access.

*Account Switcher*

You always log in with the credentials tied to your Home account. While logging in, you can select either your Home account, or an eternal account, and ExtremeCloud IQ (New) loads the context for the selected tenant. After you log in, you can use the Account Switcher feature to switch between your accounts. After each switch, you see the devices, policies, users, and settings for the selected organization.

When switching between multiple accounts, remember the following considerations for external accounts:

- Your permissions and level of access depend on your assigned role for the selected account. You might be a full administrator for your Home account, but have read-only access for another. An administrator for each tenant assigns your role for that tenant.
- If an administrator for an external organization removes your access, you cannot log into, or work in that account anymore. Your home account is unaffected.

**Important**

Because tenants are isolated instances, changes made in one tenant apply to that tenant only. As a best practice, always confirm the active account before making changes like editing policies, onboarding devices, or changing user permissions.

Related Links

Switch Accounts on page 23

*Switch Accounts*

You can have multiple accounts in ExtremeCloud IQ (New). Use this task to switch accounts after you log in.

1. On the ExtremeCloud IQ (New) banner, select .
2. (Optional) If you have previously hidden some accounts, and want to see them again, select **Show Hidden Accounts**.
3. (Optional) To search for an account by name, start typing in the **Search** bar.
4. In the **Select a Network** dialog, you can switch between accounts or VIQs that you can access using the same Identity Provider (IdP).
   - **Your Organizations**: Accounts to which you directly belong.
   - **Other Organizations**: Additional accounts or VIQs you can access using the same login credentials.
5. (Optional) To toggle visibility for an account, hover over the account and select the corresponding icon:
   - To stop hiding a previously hidden account, select .
   - To hide an account, select .
6. (Optional) To favorite an account, hover over the account and select .

Related Links

Multiple Accounts on page 22

## Forgotten Password

If you forget your password, you can reset it while logging in to ExtremeCloud IQ (New).

Use this task to reset a forgotten password.

1. In the **Log In** dialog, select **Forgot Password?**
2. In the **Forgot Password** dialog, type your **Business Email** (the email address for your account).
3. Select **Send Password Reset Link.**
4. Open your email and select the reset password link.
5. Follow the instructions to reset your password.

## Change Password

Use this task to change your password.

1. In the upper-right of the page, select **<your initials>** > **Profile**, and the select **Change Password**.

2. In the dialog, complete following steps:
   a. In the **Current Password** field, type your current password.
   b. In the **New Password** field, type the new password.
   c. In the **Confirm Password** field, retype the new password.
   d. Select **Save**.

   For information about the requirements, see Your ExtremeCloud IQ (New) Password on page 20.

## Log in with Single Sign-On

SSO simplifies the login process, so you can log in to ExtremeCloud IQ (New) using credentials from an existing SAML-enabled identity provider (IdP).

**Important**
SSO authentication is not supported in the ExtremeCloud IQ (New) mobile app. Users must log in with their standard ExtremeCloud credentials.

Key features of SSO:

- **Unified Access**: Log in once and gain access to integrated services without repeated logins.
- **Improved Security**: Use a single, strong password to reduce the risk of security breaches associated with weak or reused passwords, enforce multi-factor authentication based on your IdP policies, and deny administrative access to ExtremeCloud IQ (New) by removing users from the IdP.

Use this task to log in to ExtremeCloud IQ (New) using your SSO credentials.

1. In a web browser, go to `https://extremeplatformone.com`, and then select **Log in with SSO**.
2. Enter your email address, and then select **Log in with SSO**.

   **Note**
   When you log in with SSO for the first time, you must first select your organization from the list, and then follow the prompts. If you encounter difficulty during configuration, contact your ExtremeCloud IQ (New) administrator to determine whether your account can be configured for SSO.

3. Select your organization.
4. Enter your **Password**, and then select **Sign in**.

   The **Sign in** button is disabled and changes to display a loading indicator while your credentials are verified. If authentication is unsuccessful, the button is re-enabled so you can try again.

   **Note**
   If you can't remember your password, select **Forgot my password** to reset it.

## Unified Logout

When you log out of one application (single and multi-tab), unified logout logs you out of all applications supported by the unified login page:

- Extreme Platform ONE Networking
- ExtremeCloud IQ (New)
- ExtremeCloud IQ (Classic)
- Extreme Platform ONE Security
- ExtremeCloud SD-WAN

## Browser Support and Display Settings

**Note**
ExtremeCloud IQ (New) does not support 32-bit browsers.

### Desktop Browsers

ExtremeCloud IQ (New) supports the latest 64-bit versions of the following desktop browsers:

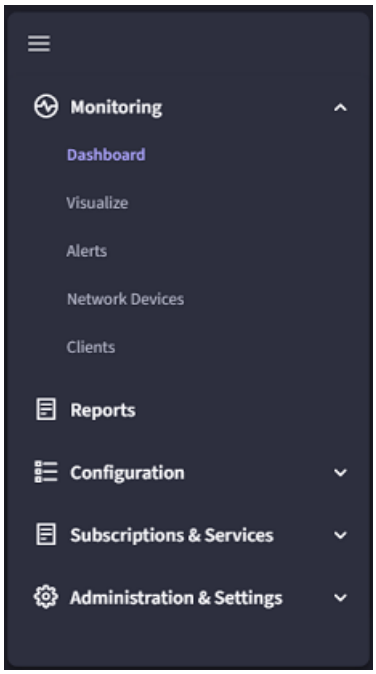
- Chrome
- Edge
- Firefox
- Opera
- Safari

Microsoft Internet Explorer is not supported.

### Display Settings

ExtremeCloud IQ (New) supports display resolutions of 1280 x 1024 or higher.

# Navigation Pane




**Note**
Select to toggle the navigation pane on and off.

Use the navigation pane to access the following work benches and content:

- **Workspace**
- **Monitoring**
  - Dashboard
  - Visualize
  - Alerts
  - Network Devices
  - Clients
- **Reports**
- **Configuration**
  - Sites
  - Network
- **Subscriptions & Services**
  - Subscriptions & Licensing
  - Contracts
  - Inventory
- **Administration and Settings**
  - Access Management
  - Alerts
  - External Notifications

- Backup and Restore
- Integrations
- Logs

## Content Pane

The ExtremeCloud IQ (New) content pane displays information related to your navigation pane selection.

Table 4 through Table 8 on page 33 describe fields and columns available in the content pane.

**Table 4: Standard Icons**

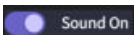
| Icon | Description |
|---|---|
| Notification Bell  | Receive notifications for device, security, performance, and operational activities.<br>When you select the bell icon, a panel displays the following:<br>• **Go to Notification Center** button<br>• **Sound On** toggle  : to hear notification alerts<br>• The following tabs:<br>◦ All: displays all notifications<br>◦ Critical: displays critical notifications<br>◦ Non-Critical: displays non-critical notifications<br>◦ Information: displays relevant information<br>• **Eye** Icon  **:** displays the total number of unread notifications<br><br>Select **Go to Notification Center** to do the following:<br>• View notifications from the last 24 hours, last week, last month and last quarter<br>• Select **Generate Report** to download a list of notifications in .csv format<br>• Use the **Search** field to quickly find notifications<br>• Select a particular notification to view the following details about that notification:<br>◦ Site<br>◦ Device<br>◦ Severity<br>◦ Category<br>◦ Description<br>◦ Aggregation count, if applicable<br>◦ Time stamp |
| Profile Icon  | Select your initials at the top right corner of the screen to view the following:<br>• Name and email address<br>• Profile icon<br>• About Extreme Platform ONE Networking displays the release version for each software component<br>• Sign Out<br><br>The **Profile** icon displays your name, login details, and multi-factor authentication (MFA).<br>You can modify your name and password from this menu.<br><br>**Note:** To show passwords on the screen, select  .<br><br>You can choose a light or dark theme for your administrative environment. |

**Table 4: Standard Icons (continued)**

| Icon | Description |
|---|---|
| Extreme Applications  | Displays all applications available in ExtremeCloud IQ (New) for trial.<br>• ExtremeCloud™ IQ<br>• Universal ZTNA<br>• ExtremeCloud SD-WAN<br>• Extreme Intuitive Insights |
| Resource Center icon  | The **Resource Center** icon expands to show the following menu options:<br>• Share Your Feedback<br>• Product Tours<br>• User Guide<br>• Release Notes<br>• Legal Summary<br>• Contact Sales Team<br>Each selection opens an external site, from which you can add feedback or obtain product-related information. |
|  Download | You can download data and export in .csv format. Use the Filter option to tailor your content to specific views. |
|  Refresh icon | Refreshes the screen and displays the latest information |

## Extreme Applications and the 9-dot Menu

ExtremeCloud IQ (New) provides access to the other applications for which you have entitlements. The menu also displays links to request trials for other Extreme Networks applications.

For access to Extreme Platform ONE Security or ExtremeCloud SD-WAN, you must have at least one subscription of that type. For more information, or to obtain a quote, contact your Extreme Networks Partner.

**Note**
To access an application from the 9-dot menu, your role must have a corresponding role in that application. For more information, see Role-Mapping Between Extreme Platform ONE Networking and Other Applications on page 577.

**Note**
CoPilot on page 30 licenses are no longer available for purchase.

Related Links

CoPilot on page 30

## CoPilot

First introduced in ExtremeCloud IQ (Classic), ExtremeCloud IQ CoPilot is an AIOps solution that leverages Explainable Machine Learning (ML).

To open CoPilot, select , and then choose **CoPilot**.

**Note**
This option is available only for customers with current CoPilot subscriptions. CoPilot subscriptions are no longer available for purchase.

CoPilot follows your ExtremeCloud IQ (New)**Theme** setting. The application includes the familiar **Anomalies** and **Connectivity Experiences** tabs. For more information, see the corresponding sections in the ExtremeCloud IQ v25.2.0 CoPilot Deployment Guide.

*ExtremeWorks and PartnerWorks*

While viewing an anomaly, ExtremeWorks or PartnerWorks customers can select **Need Help** to see relevant videos and articles and then, if needed, automatically open a support ticket.

# Common Functionality

The ExtremeCloud IQ (New) user interface offers the following common functions across the platform:

- Select the information icon for more information.
- Use the **Search** field to find and display information based on the criteria that you enter.
- **Tables:**
  - Select and drag the left or right border of the column header to adjust the column width.
  - Select and drag the column headers to change the order of the columns.[1]
  - Select a column header to sort column data in ascending or descending order.[2]
  - Select **Columns** to add, remove, and reorder the columns.[1]
  - Select **Filters** to narrow your search. You can filter by column or by selecting the **Filter** button and using check boxes.[2]
  - **Filters Applied:** indicates that the data is filtered. To remove filtered data, select **X**.[2]
  - **Page Size:** Specify the number of rows to display per page.

[1] You cannot move the primary column.

[2] Unavailable for the **Dashboard** > **Sites** table.

**Table 5: Monitoring View**

| Left Navigator Menu | Description |
|---|---|
| Dashboard | The **Dashboard** provides an overview of the network. |
| Visualize | For a description of all icons on the Visualize screen see, Visualize → Quick Navigation. |
| Alerts | The **Alerts** screen consists of the following features icons and details:<br>• Date and Time Picker: Displays alerts for up to 30 days<br>• **Refresh Alert**: Displays the most recent alerts<br>• **Export to CSV**: Downloads alerts in a CSV file<br>• **Acknowledge**: Indicates that the alert was read and understood<br>Alerts detect, record, and report details of a specific event. |
| Network Devices | The **Network Devices** page displays all devices for selected locations. You can manage the devices from this page. |
| Client & Users | The **Client & Users** screen provides an overview of clients and users. |

**Table 6: Configuration**

| Navigation pane | Description |
|---|---|
| Sites | The Sites page consists of the following features icons and details:<br>• **Import Site Tree:** Drag & Drop or browse files in xml format.<br>• **Add Site Group:** Add a site group to manage multiple sites. To add a site group see, Add a Site Group.<br>• **Add Site:** Add a site and connect site groups to the site. To add a site see, Add a Site.<br>• Select the overflow menu ⋮ at the end of each row to do one of the following:<br>◦ Add a building.<br>◦ Move a site.<br>◦ Export the plan in .xml or .tar format. |

**Table 6: Configuration (continued)**

| Navigation pane | Description |
|---|---|
| | ◦ Edit a site.<br>◦ Delete a site. |

**Table 7: Subscriptions & Services**

| Navigation pane | Description |
|---|---|
| Subscriptions | The **Subscriptions & Licenses** page includes the following features icons and details:<br>• **Customer Unique Identifier (CUID)**: Use your CUID to purchase licenses and get access to your license pool.<br>• **Linked to Extreme Portal:** A green status means you are connected to the Extreme Portal where you can access training, knowledge articles, forums, log support cases, and access to information about owned assets.<br>• **Not Linked to Extreme Portal:** A red status indicates that you have lost connection.<br>• **Unlink my Extreme Portal Account:** Removes the link to your Extreme Portal Account from Extreme Platform ONE Networking.<br>**Caution:** Do not **Unlink** your account without specific direction from Extreme Network Support personnel.<br>• **Synchronize Subscriptions:** Synchronizes information from the license management server.<br>**Note:** It can take up to 5 minutes to synchronize the license data.<br>• **Search:** Search by description, entitlement status, and product.<br>• **Status:**<br>◦ Green: Everything is good<br>◦ Yellow: A non-urgent issue<br>◦ Red: Requires immediate action<br>• **Description:** Indicates the total number of subscriptions associated with a license. This number includes all active, inactive, and expired subscriptions. To view details about individual subscriptions, select the number next to the subscription.<br>• **Entitlement:** Displays product entitlement.<br>• **Product** Displays the product name.<br>• **Total:** Displays the total number of licenses you have purchased. |

**Table 7: Subscriptions & Services (continued)**

| Navigation pane | Description |
|---|---|
| | • **Active:** Displays the total number of licenses in use.<br>• **Available:** The total number of licenses minus in use licenses. |

**Table 8: Administration and Settings**

| Navigation pane | Description |
|---|---|
| Access Management | The **Access Management** page provides the following functionality to create and view user access:<br>• Internal Users<br>• External Users<br>• Single Sign-On<br>• Credential Groups<br>Select each section to view additional details.<br>Icons and buttons:<br>• **Create New User:** Add an internal or external user to your account. To create a new user see, Create a New User.<br>• **Search:** Do searches based on column data.<br>• Select the overflow menu ⋮ at the end of the row to do one of the following:<br>◦ Edit<br>◦ Disable<br>◦ Delete<br>Single Sign-On:<br>**Note:** Only a **Super Admin** can enable SSO.<br>To add an IdP profile on the **Single Sign On Identity Provider (IdP) Profile** page, select **Add IdP Profile**. Follow the steps to create the IdP profile and configure it with an IdP provider. |
| Alert Policies | The **Alert Policies** screen provides the following functions:<br>• Configure a Global policy that impacts the full network.<br>• Configure a Site policy that impacts a specific network site. |

**Table 8: Administration and Settings (continued)**

| Navigation pane | Description |
|---|---|
| External Notifications | The **Notification Configuration** screen and the **Alert Notifications** tab consists of the following sections:<br>• Email Recipients<br>• Webhooks<br>• ServiceNow Accounts<br>Icons and buttons:<br>• **Search Recipients:** Search based on column data<br>• **Add Email Recipients:** Add new email recipients.<br>• **Refresh** icon: Refreshes the screen and displays the latest notifications .<br>• **Filters:** Filter notifications by the following:<br>◦ All<br>◦ Verified<br>◦ Not Verified<br>• **Add Webhooks:** Add a new webhook for automatic alert notifications.<br>• Select the overflow menu ⋮ at the end of the row to do one of the following:<br>◦ Edit<br>◦ Delete<br>• **Add ServiceNow Accounts:** Add a new ServiceNow Account for automatic alert notifications. |
| Backup & Restore | **Backup & Restore** provides the following functions:<br>• VIQ management<br>• Default device passwords<br>In addition, you can perform the following actions:<br>• View backup history<br>• Export VIQ settings<br>• Import VIQ settings |

**Table 8: Administration and Settings (continued)**

| Navigation pane | Description |
|---|---|
| Integration | **Integration** provides the ability to use APIs to customize ExtremeCloud IQ (New). |
| Logs | **Audit logs** contains all changes made by users and applications.<br>The **Audit Logs** screen consists of the following icons and buttons:<br>• **Search:** Search based on column data.<br>• **Date and Time Picker:** Displays activities for up to 30 days. |

| Navigation pane | Description |
|---|---|
| Access Management | The **Access Management** page provides the following functionality to create and view user access:<br>• Internal Users<br>• External Users<br>• Single Sign-On<br>• Credential Groups<br>Select each section to view additional details.<br>Icons and buttons:<br>• **Create New User:** Add an internal or external user to your account. To create a new user see, Create a New User.<br>• **Search:** Do searches based on column data.<br>• Select the overflow menu ⋮ at the end of the row to do one of the following:<br>◦ Edit<br>◦ Disable<br>◦ Delete<br>Single Sign-On:<br>**Note:** Only a **Super Admin** can enable SSO.<br>To add an IdP profile on the **Single Sign On Identity Provider (IdP) Profile** page, select **Add IdP Profile**. Follow the steps to create the IdP profile and configure it with an IdP provider. |
| Alert Policies | The **Alert Policies** screen provides the following functions:<br>• Configure a Global policy that impacts the full network.<br>• Configure a Site policy that impacts a specific network site. |

| Navigation pane | Description |
|---|---|
| External Notifications | The **Notification Configuration** screen and the **Alert Notifications** tab consists of the following sections:<br>• Email Recipients<br>• Webhooks<br>• ServiceNow Accounts<br>Icons and buttons:<br>• **Search Recipients:** Search based on column data<br>• **Add Email Recipients:** Add new email recipients.<br>• **Refresh** icon: Refreshes the screen and displays the latest notifications .<br>• **Filters:** Filter notifications by the following:<br>◦ All<br>◦ Verified<br>◦ Not Verified<br>• **Add Webhooks:** Add a new webhook for automatic alert notifications.<br>• Select the overflow menu ⋮ at the end of the row to do one of the following:<br>◦ Edit<br>◦ Delete<br>• **Add ServiceNow Accounts:** Add a new ServiceNow Account for automatic alert notifications. |
| Backup & Restore | **Backup & Restore** provides the following functions:<br>• VIQ management<br>• Default device passwords<br>In addition, you can perform the following actions:<br>• View backup history<br>• Export VIQ settings<br>• Import VIQ settings |
| Integration | **Integration** provides the ability to use APIs to customize ExtremeCloud IQ (New). |
| Logs | **Audit logs** contains all changes made by users and applications.<br>The **Audit Logs** screen consists of the following icons and buttons:<br>• **Search:** Search based on column data.<br>• **Date and Time Picker:** Displays activities for up to 30 days. |

## Pagination

ExtremeCloud IQ (New) supports pagination in all pages that show detailed data.

Select the required **Page Size** (**20**, **50**, **100**) to specify the number of entries in a table.

- The default page size is 20.

- Use the **Previous** (<) and **Next** (>) icons to scroll through the list.

Limitation:

The user interface shows incorrect data on the previous page when you scroll through list pages after applying filters.

## Edit Your Profile Settings

Use this task to change the profile settings for your account.

**Note**
You must be logged in to your account.

1. Select your **Profile** (initials), and then select **Profile**.
2. To change your display name, edit the **First Name** and **Last Name** fields, and then select **Save Changes**.
3. To change your password, select **Change Password**, type your current password, type your new password twice, and then select **Save**.

   For information about requirements, see Your ExtremeCloud IQ (New) Password on page 20.

   **Tip**
   To show passwords on the screen, select . To hide the password again, select 

4. To change your language preference, select a language from the list:
   - English
   - French
   - German
   - Italian
   - Japanese
   - Korean
   - Portuguese (Brazil)
   - Spanish (Latam)
5. To change your preferred application that displays when you first log into Extreme Platform ONE Networking, select either Networking (the default) or Security.
6. Select **Save Preferences**.

## Choose a Theme

Use this task to choose a light or dark theme for your administrative environment. This task requires you to be logged in to your account.

1. Select your **Profile** (initials), and then select **Theme**.
2. Depending on your preference, select either **Light** or **Dark**.

   You can repeat these steps to switch between light and dark themes.

# Monitoring | Dashboard

**Dashboard** uses the following widgets to provide an overview of the network performance for selected sites:

**Alerts**

The **Alerts** widget displays the number of alerts for the last three days, and the breakdown according to severity. To update the chart, select or deselect the severity categories: **Critical**, **Warning**, and **Information**. Select **Unacknowledged** to open the **Alerts** page.

**Usage & Capacity**

The **Usage & Capacity** widget displays the total number of devices that have queue congestion, and also the total affected wired and wireless devices. Select **Wired** or **Wireless** to open the **Network Devices** page, **Usage & Capacity** tab filtered for your selection.

**Device Status**

The **Device Status** widget displays the total number of managed devices, the total number of offline devices, and also the number of offline wired and wireless devices. Select **Total Offline**, **Wired**, or **Wireless**, to open the **Network Devices** page, **Device Status** tab filtered for your selection.

**Client Health**

The **Client Health** widget displays the total number of clients, the total number of clients with issues, and the numbers of wired and wireless clients with issues. Select **Wired**, or **Wireless**, to open the **Clients** page, **Clients** tab filtered for your selection.

**Device Health**

The **Device Health** widget displays the total number of managed devices, the total number of devices with issues, and the numbers of wired and wireless devices with issues. Select **Wired**, or **Wireless**, to open the **Network Devices** page, **Device Health** tab filtered for your selection.

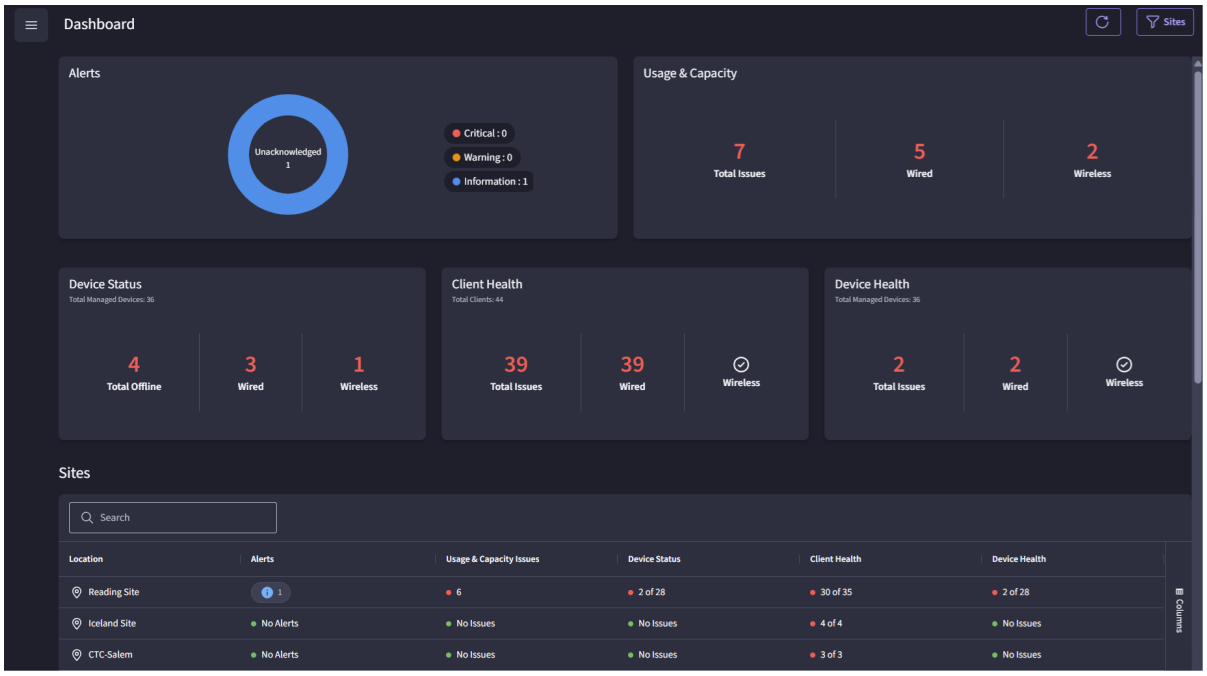



**Figure 1: Dashboard**

Use the **Sites** filter to select sites and filter the view.

**Note**
If you have access to only one site, the **Sites** filter is not present.

To display the timestamp for the last update, hover over .

To refresh the data, select .

To customize the **Sites** table view, select . You can choose which columns to display, the column order, and the number of results per page.

# Monitoring | Visualize


Customize the Visualize View on page 41
Device Icons on page 43
Topology Legends on page 44
Geographic View on page 45
Heat Map View on page 46
Access View on page 71
Device Detection on page 71
Inspector Panel on page 73
AutoSave Device Layout and Density on page 76
Search an Element on page 77
Topology Map Settings on page 77
User Roles Supported in Visualize View on page 78


Go to **Monitoring** > **Visualize**.

The Visualize canvas provides a customizable, visual overview of network performance. The default is the Geographic view. When you change the view, whether by using Quick Location Navigation, view selector, or by selecting an object in the topology map, the view focuses on your selection.

If the topology changes, ExtremeCloud IQ (New) displays a notification. These notifications do not stack. After you close the notification, the refresh icon—— displays a red dot to indicate the topology has changed. If you refresh the display and the topology changes again, the refresh icon displays the red dot again.

## View Selector

Go to **Monitoring** > **Visualize** and select 

to open the view selector and choose one of the following views:

- **Access** view
- **Heat Map** view
- **Geographic** view

**Note**
Geographic is the default view. The label for the view selector menu changes according to your selection, and ExtremeCloud IQ (New) remembers your last selection.

## Customize the Visualize View

Use **Sites** (**Quick Location Navigation**) to navigate to another level of the network hierarchy for your organization. This navigation menu displays all sites (including groups, buildings, and floors, including a device count for each level, and reopens with your last selection.

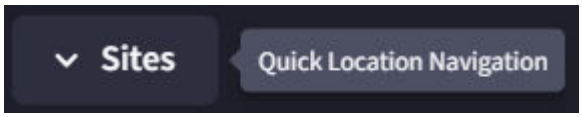



**Figure 2: Sites (Quick Location Navigation) menu**

The following table lists and describes the **Sites** (**Quick Location Navigation**) icons and other options for customizing the view.

**Table 9: Visualize icons**

| Icon | Name | Description |
|---|---|---|
| **Sites** (**Quick Location Navigation**) | | |
| Sites | Organization (Quick Location Navigation) | Displays the different levels of the network hierarchy and shows the device count for each location.<br>Use the **Sites** ( **Quick Location Navigation**) menu to customize your display by site, building, and floor.<br>To highlight the devices on the topology map for the selected location, hover over the location in the menu. |
| | Group | Indicates a group of sites. Expand this element to see the sites. |
| | Site | Indicates a site.<br>A blue icon indicates limited features and a purple icon indicates full features. Select **Unlock Full Features** to remove limitations by allocating Platform ONE licenses. |
| | Building | Indicates a building.<br>A blue icon indicates limited features. Select **Unlock Full Features** to remove limitations by allocating Platform ONE licenses. |
| | Floor | Indicates a floor. |
| | Floor plan | Indicates that a floor plan exists for the corresponding floor. |
| | Search | Indicates the search field for the **Quick Location Navigation**. To begin, start typing in the search field. |

**Table 9: Visualize icons (continued)**

| Icon | Name | Description |
|---|---|---|
|  | 3-dot menu | **Note:** The 3-dot menu options vary for different levels of the network hierarchy.<br><br>Provides the following options for the topology map:<br>• Collapse All<br>• Expand All<br>• Hide All Borders<br>• Show All Borders<br>• Floor Layouts:<br>◦ U-Shaped<br>◦ Grid<br>• Device Layouts:<br>◦ Stacked<br>◦ Spread<br>◦ Grid<br>◦ Hierarchical<br>• Density<br>◦ Very Sparse<br>◦ Sparse<br>◦ Dense<br>◦ Very Dense<br>• Update Topology (building or floor)<br>• Show Masked Devices and Links |
| **General Visualization Options** | | |
|  | Topology Locked | Indicates that the topology map is locked. Select to unlock the topology map. |
|  | Topology Unlocked | Indicates the topology map is unlocked. When the map is unlocked, you can toggle **Autosave**. Select to lock the topology map. |
|  | Zoom In | Zooms in the topology map. |
|  | Zoom Out | Zooms out the topology map. |
|  | Legend | Opens the legends used to describe the symbols used in topology maps. |
|  | Open Minimap | Opens the minimap. |
|  | Close Minimap | Closes the minimap. |

**Table 9: Visualize icons (continued)**

| Icon | Name | Description |
|---|---|---|
|  | Fit View | Adjusts the magnification for the topology map view to display the entire map. |
|  | Refresh Topology | Refreshes the topology map. |
|  | Search | Search for **Devices** by name, IP, MAC, host name, or serial number. |
|  | Filter | Filters the topology map view based on tags.<br>**Note:** Filter settings and view are persistent. |
|  | Settings | Opens the following topology map settings:<br>• Display options<br>• Manage |
|  | Inspector Panel Control Button | Displays the **Inspector** panel for more information about selected elements and services. |

## Device Icons

Extreme Platform ONE Networking uses the following icons to display devices on the **Visualize** canvas.

**Table 10: Icons on the canvas**

| Icon | Description |
|---|---|
|  | Indicates a switch managed by the application or detected through LLDP by a switch or access point |
|  | Indicates a stack of switches managed by the application |
|  | Indicates a controller |
|  | Indicates an access point (AP) managed by the application |
|  | Indicates an access point detected through LLDP by a switch or an access point |
|  | Indicates a phone detected through LLDP by a switch or an access point |
|  | Indicates a camera detected through LLDP by a switch or an access point |

**Table 10: Icons on the canvas (continued)**

| Icon | Description |
|---|---|
|  | Indicates a router detected through LLDP by a switch or an access point |
|  | Indicates a connection through SD-WAN devices |

## Topology Legends

Table 11 lists the icons that ExtremeCloud IQ (New) displays on the **Visualize** canvas and in the legends.



**Note**
ExtremeCloud IQ (New) supports only the Access, Heat Map, and Geographic layer views.

**Table 11: Topology legend icons**

| Icon | Description |
|---|---|
| **Nodes** | |
|  | Site (Geographic layer view only) |
|  | Multiple Sites (Geographic layer view only) |
|  | Building (Geographic layer view only) |
|  | Disconnected Devices |
|  | High Severity Alerts |
|  | Managed Devices |
|  | Detected Devices |
|  | Partially Connected [1] |
| **Links** | |
|  | Operational Up |
|  | Operational Down |
|  | Admin Down |

**Table 11: Topology legend icons (continued)**

| Icon | Description |
|---|---|
|  | LAG Operational Up |
|  | LAG Operational Down |
|  | LAG Degraded |
|  | LAG Admin Down |
|  | SD-WAN Internet Uplinks |
|   | AutoSense Enabled |
| **Others** | |
|  | vIST or MLAG<br>Virtual Inter-Switch Trunk or Multi-Switch Link Aggregation Group |

[1] ExtremeCloud IQ (New) indicates that a device is partially connected under the following circumstances:

- Very old firmware with no inlets support
- Old firmware with inlets support, but below the minimum firmware version
- Network issue (firewall or other solution does not allow inlets connection), a bug in the NOS, or inlets are disabled
- Device in the process of onboarding
- Extreme Networks legacy device or third-party device has not finished the full topology discovery



**Note**
For descriptions of the device icons that ExtremeCloud IQ (New) displays on the **Visualize** canvas (Access, Physical, and Fabric layers only), see Device Icons on page 43.

## Geographic View

The Geographic view is the default view in Visualize. The Geographic view supports the following functions:

- View sites.
- Zoom-in, up to the building level.



**Tip**
Use the mouse wheel, or double-click an empty space on the canvas to zoom-in and focus the view.

- Zoom-out collapses the building level into sites.



**Tip**
Use the mouse wheel, or **Shift** + double-click a space on the canvas to zoom out.

- Show links between buildings and sites.



**Note**
- Geographic view requires graphics acceleration. For more information about how to enable this feature, see the Help for your browser.
- When you select a floor, the Geographic view shows the building location and filters devices to the selected floor.
- Hover over a site on the map to view the number of sites or buildings.

## Heat Map View

From the **Heat Map** view, you can view Radio Frequency (RF) network heat maps. RF maps use a color spectrum, ranging from warm to cool, to illustrate real-time device signal strength throughout a building floor plan. Warm colors represent a stronger signal strength. Cool colors represent a weaker signal strength.

In addition to cloud-native APs, heat maps support controller-managed APs. Controller-managed APs can be matched to ExtremeCloud IQ (New) locations at the floor level and displayed on heat maps with all available heat map types across 2.4 GHz, 5 GHz, and 6 GHz frequencies.



**Note**
You can only monitor Controller-managed APs. Device configuration for locally-managed APs is not supported. For more information, see Appliances View on page 118.

ExtremeCloud IQ (New) supports the following map type views:

- Wi-Fi Map
- IoT Map



**Note**
Maps generated within the **Manage** > **Planning** section in ExtremeCloud IQ (Classic) are visible in ExtremeCloud IQ (New) RF Maps.

With ExtremeCloud IQ (New) RF Maps, you can:

- Rotate the Heat Map.
- View device details or perform actions on a selected device (including uploading installation photos).
- View the summary details of clients connected to an AP (including Client 360° details, roaming paths, and authenticating).
- Show or hide labels.

- Show or hide zones.
- View the heat map in 3D.
- Filter devices by client connection type.
- Adjust thresholds.
- Change color schemes.
- View device inventory.
- Create a device filter from the Heat Map view.
- Import a third-party RF map.
- View antenna patterns.
- Edit a Heat Map.

Use this task to view real-time network data coverage.

1. Go to **Monitoring** > **Visualize**.
2. From the Sites (**Quick Location Navigation**) menu, select a floor.

   **Note**
   Use **Search** to find a specific location in a large network. Type the first few characters to see a list of locations. The more characters you type, the more precise the search results are.

   **Note**
   The selected floor must include a floor plan. For more information, see Upload a Floor Plan on page 273.

3. From the view selector, select **Views** > **Heat Map**.
4. From the Heat Map view pane, select **Map Type**:
   a. To view the heat map for Wi-Fi devices, select **Wi-Fi**, configure the Wi-Fi map type settings in Table 12.

**Table 12: Wi-Fi Map Types**

| Map Type | Radio Frequency |
|---|---|
| RSSI | 2.4 GHz, 5 GHz, or 6 GHz |
| Coverage Overlap | 2.4 GHz, 5 GHz, or 6 GHz |
| SNR | 2.4 GHz, 5 GHz, or 6 GHz |
| Channel | All frequencies: 2.4 GHz, 5GHz, and 6 GHz |
| Interference | 2.4 GHz, 5 GHz, or 6 GHz |

**Table 12: Wi-Fi Map Types (continued)**

| Map Type | Radio Frequency |
|---|---|
| Co-channel Interference | 2.4 GHz, 5 GHz, or 6 GHz |
| Client Density | Displays client location density across the floor plan regardless of radio frequency.<br><br>**Note:** The Client Density map type is only available when **Wireless Client Tracking** is enabled. For more information, see Enable Wireless Client Tracking on page 720. |

   b. To view the heat map for IoT devices, select **IoT**, and then configure the RSSI for the 2.4 GHz radio. IoT heat maps support 2.4 GHz radio frequencies only.

5. To rotate the map, from the top left corner, select and drag the slider.
6. To view device details or perform actions, select a device on the map.

   When a rogue AP or client is detected, the following icon appears on the heat map at the reported location:

   For more information, see Rogue AP and Client Heat Map Locations on page 53.
7. To view inventory details for the clients connected to an AP, select the purple halo above the AP.
   - The purple halo shows the number of connected clients.
   - From the **Inventory** pop-up window, select a **Connected** or **Disconnected** client **Hostname** to view client **Summary** and **Actions**. For more information, see Device Summary and Actions Menu on page 51.

     **Note**
     Disconnected clients are not listed by default. Start a search to populate the Inventory list before selecting a disconnected client.

8. Right-click an AP to:
   - **Show Coverage**: Updates the heat map to show the coverage from the single AP. To reset and see coverage from all APs, select **Show Coverage** again.
   - **Hide Device**: Hides the device from the heat map without removing it from the network. To show the device, see View Device Inventory on page 50.

     **Note**
     Hiding a device from the RF Map requires administrator privileges.

9. For Channel Wi-Fi map types:
   - To view the number of connected clients per AP, select .
   - To view the number of clients per radio frequency for each AP, select .
10. To show or hide labels, select . Select a label from the list to control its visibility on the Heat Map. For information on creating labels, see Manage Heat Map Labels on page 70.

11. To show or hide zones, select . Select a zone from the list to control its visibility on the Heat Map. For information on creating zones, see Manage Heat Map Zones on page 68.
12. Select **3D** to view a three-dimensional representation of the heat map.

    This view allows users to visualize how signals propagate through different areas, including floors and walls, offering a more comprehensive understanding of network coverage and potential dead zones. This helps to optimize placement of access points and improve overall network performance.

    When viewing a heat map in 3D, you can:

    - Select to stop the rotation. Select to start the rotation.
    - Select and to zoom in and out.
    - Select and drag the slider to adjust the angle of the map.

    **Note**
    Select **2D** to return to the default map view.

13. To filter devices on the map by their connection type, select one of the following icons:
    - : All
    - : Wi-Fi
    - : Thread
14. To set Wi-Fi coverage thresholds, configure the threshold values in Table 13, select , and then select **Apply**.

    Thresholds provide a visual to see where coverage is optimal, acceptable, and where improvements are needed.

**Table 13: Wi-Fi Coverage Threshold Settings**

| Threshold | Description |
|---|---|
| Excellent | Above the set threshold, for example -30 dBm, the signal is considered excellent. |
| Good | Near the set threshold, for example -67 dBm, the signal is considered good. |
| Medium | Near the set threshold, for example 72 dBm, the signal is considered medium. |
| Poor | Below the set threshold, for example -90 dBm, the signal is considered poor. |

15. To change the color scheme, select and then select a new color scheme.

    **Note**
    The **Select Color Map** icon might display different colors, depending on the last color scheme selected.

16. To zoom in and out, select **+** and **–**, or scroll the mouse wheel. Select and drag the map to move within the window.

**Note**
When you zoom in or out, the scale of the RF Map changes in real time below the zoom icons. The scale represents the relationship between the displayed area on the RF Map and the original map scale.

Related Links

Import a Third-Party RF Map on page 62
Edit a Heat Map on page 64
Device Summary and Actions Menu on page 51
View Device Inventory on page 50
View Antenna Patterns on page 64

## View Device Inventory

**Inventory** displays a list of **Access Points**, **Switches**, or **Clients** currently being monitored on an RF Map.

The **Access Points** and **Switches** asset lists provide the following details about each device:

- **Hostname**: The name assigned to the device
- **Status**: The current operational state of the device
- **IP Address**: The unique network address assigned to the device
- **Show/Hide**: An option to toggle the visibility of the device on the heat map, allowing for a more customized and focused view of the real-time status of your network

The **Clients** asset list provides the following details about each device:

- **Hostname**: The name assigned to the device
- **MAC Address**: The unique identifier assigned to the device
- **IP Address**: The unique network address assigned to the device
- **Type**: Filter by different client types

Use this task to toggle the visibility of **Access Points** and **Switches** and filter **Client** types on a selected heat map.

1. Go to **Monitoring** > **Visualize**.
2. From the Sites (**Quick Location Navigation**) menu, select a floor.

**Note**
Use **Search** to find a specific location in a large network. Type the first few characters to see a list of locations. The more characters you type, the more precise the search results are.

**Note**
The selected floor must include a floor plan. For more information, see Upload a Floor Plan on page 273.

3. From the view selector, select **Views** > **Heat Map**.
4. Select .

   **Note**
   Use the **Search** field to find a specific device.

5. Select an Asset type:
   - Access Points
   - Switches
   - Clients
6. Select a **Hostname** to view device summary and available actions. For more information, see Device Summary and Actions Menu on page 51.
7. To show/hide device, select/deselect the check box next to the devices you want to show/hide, and then select **Apply**.

## Device Summary and Actions Menu

In a Radio Frequency (RF) Map, select a device to display device summary information and a list of available actions.

*AP Device Summary*

The AP **Summary** tab displays the following information for a selected AP device:

- Connected status: Offering the number of Days, Hours, Minutes, and Seconds a device has been connected.
- AP Name
- Model, and OS Version
- Network Policy associated with the device
- SSIDs: Network SSIDs associated with the device
- AP Orientation:
  - AP Installation Height

    **Note**
    Displays the distance unit set during floor creation. For more information, see Add a Floor on page 272.

  - Accuracy Range for Installation Height (6GHz Only)
  - Elevation
  - Azimuth
  - Height from Ground (6GHz Only)
  - Accuracy Range from Ground (6GHz Only)

**Note**
To update any AP Installation Height parameter, select the corresponding field, input the new value, and then select **Save**.

- Wi-Fi 0, Wi-Fi 1, and Wi-Fi 2 details:
  - Radio Mode
  - Power
  - Channel
  - Channel Width
  - Frequency
  - Number of Clients
  - Mode
- Installation Photos: Upload photos or videos of the device installation. For better performance, limit the image file (.png, .jpg) to less than 500 KB and limit the video file (.mp4, .mov.) to less than 5MB.

*Switch Device Summary*

The switch **Summary** tab displays the following information for a selected switch device:

- Connected status: Offering the number of Days, Hours, Minutes, and Seconds a device has been connected.
- Hostname/SysName: Select to view device details.
- Model
- Network Policy associated with the device
- IP Address, System MAC Address, OS Version, and Make of the device
- Installation Photos: Upload photos or videos of the device installation. For better performance, limit the image file (.png, .jpg) to less than 500 KB and limit the video file (.mp4, .mov.) to less than 5MB.

*Client Device Summary*

The client **Summary** tab displays the following information for a selected client:

- Host Name
- OS
- Uptime
- IP Address
- MAC Address
- Connected to
- VLAN
- SSID
- Captive Web Portal
- User
- User Profile
- Radio
- Channel

*Rogue AP and Client Heat Map Locations*

When ExtremeCloud IQ (New) detects a rogue access point or rogue client through the Wireless Intrusion Prevention System (WIPS), it plots the device on the Heat Map at its reported physical location, enabling security personnel to quickly locate and address the threat.

Rogue devices are represented on the Heat Map by a dedicated  icon that is visually distinct from the icons used for legitimate, managed access points. Select the rogue device icon to view the detected device details.

**Note**
Actions cannot be performed on rogue devices from the Heat Map. To review the WIPS alert for details, see View and Acknowledge Alerts on page 75.

*Actions*

For a selected AP or switch, from the **Actions** tab, you can perform the following actions:

- Locate a Device.
- Reboot a Device.
- Perform a VLAN Probe.
- Reset a Device to Factory Defaults.
- Upgrade Device Firmware.
- Configure AP Radio and Power Settings.

**Note**
Actions are supported only on APs directly onboarded to the cloud as cloud-native devices.

For a selected client, from the **Actions** tab, you can perform the following actions:

- **Client 360 View**: Display Client 360° information. To return to the client summary, close the pop-up window.
- **Client Roaming**: View the roaming trail of the client. For more information, see View Client Roaming Trail on page 60.
- **Deauthenticate**: Disconnect the client from the access point.

  **Note**
  Supported only on clients connected to APs directly onboarded to the cloud as cloud-native devices.

- **Show Client Location Path**: View client movement on a floor plan. View the current path of a connected client, replay a path, or locate the last known position of a disconnected client. The client path is drawn as a green line, connecting client node markers across the floor plan for the selected timeframe. To replay a path, select a **Date & Time Range**, and

then select **Play**. The icon traces the route, allowing you to follow the exact path the client took.

**Note**
The default time range for connected client paths is the last 24 hours. Path data is available for up to 90 days and can be viewed in one-day increments. To view data for a specific day, from the **Date & Time Range** calendar, select the same day twice, and then select **Done**. The last known location of a disconnected client is available for up to 90 days.

Show Client Location Path is supported only on APs directly onboarded to the cloud as cloud-native devices.

Related Links

Heat Map View on page 46

*Locate a Device*

Using a visual cue helps you quickly identify the exact position of a selected device within the mapped area. By triggering the blinking function, you can efficiently manage and troubleshoot your network, ensuring optimal performance and coverage.

Use this task to locate the physical location of a selected device.

1. Go to **Monitoring** > **Visualize**.
2. From the Sites (**Quick Location Navigation**) menu, select a floor.

**Note**
Use **Search** to find a specific location in a large network. Type the first few characters to see a list of locations. The more characters you type, the more precise the search results are.

**Note**
The selected floor must include a floor plan. For more information, see Upload a Floor Plan on page 273.

3. From the view selector, select **Views** > **Heat Map**.
4. Select a connected device from the heat map, and then select **Actions**.

5. Select **Locate AP (blinking lights)** or **Locate Switch**, and then configure the Locate Device settings in Table 14.

**Table 14: Locate Device Settings**

| Device Type | Field | Description |
|---|---|---|
| AP | LED Color | Select one of the following blinking light colors to set the color that the locator light flashes to help you find the AP:<br>• Amber<br>• White<br>• Off |
| AP | Blink Mode | Select one of the following blinking modes to set the speed at which the locator light flashes to help you find the AP:<br>• Fast<br>• Slow<br>• Steady |
| Switch | LED Timeout | Select a number of seconds between 0 (until disabled) and 604800 (one week). |

**Note**
To stop the blinking lights used for locating the device, select **Return to Standard LED operations**, and then select **Submit**.

6. Select **Submit**.

Related Links

Heat Map View on page 46
Device Summary and Actions Menu on page 51

*Reboot the Selected Device*

Use this task to restart the selected device.

**Important**
The current configuration is not automatically saved. Restarting momentarily disconnects any connected clients.

1. Go to **Monitoring** > **Visualize**.

2. From the Sites (**Quick Location Navigation**) menu, select a floor.

**Note**
Use **Search** to find a specific location in a large network. Type the first few characters to see a list of locations. The more characters you type, the more precise the search results are.

**Note**
The selected floor must include a floor plan. For more information, see Upload a Floor Plan on page 273.

3. From the view selector, select **Views** > **Heat Map**.
4. Select a connected device from the heat map, and then select **Actions** > **Reboot**.
5. Select **Yes** to confirm.

Related Links

Heat Map View on page 46
Device Summary and Actions Menu on page 51

*VLAN Probe from RF Maps*

The VLAN probe action locates available VLANs for the selected device. When the VLAN probe is complete, a table shows the host name, MAC address, available VLANs, unavailable VLANs, and their status.

**Note**
The VLAN Probe Utility is also available from the device list for a connected device.

**Note**
Performing a VLAN Probe from an RF map is supported for a single device only. To run a concurrent VLAN probe on multiple devices, go to **Monitoring** > **Network Devices** > **Device Status**, select the check box for two or more devices, and then from the **3-dot Menu** (⋮) at the end of any of the selected rows, select **Utilities** > **Initiate VLAN Probe**. For more information, see VLAN Probe on page 143.

Use this task to run a VLAN probe for a selected device on an RF Map.

1. Go to **Monitoring** > **Visualize**.
2. From the Sites (**Quick Location Navigation**) menu, select a floor.

**Note**
Use **Search** to find a specific location in a large network. Type the first few characters to see a list of locations. The more characters you type, the more precise the search results are.

**Note**
The selected floor must include a floor plan. For more information, see Upload a Floor Plan on page 273.

3. From the view selector, select **Views** > **Heat Map**.
4. Select a connected device from the heat map, and then select **Actions**.
5. Select **VLAN Probe**, and then configure the VLAN Probe settings in Table 15.

**Table 15: VLAN Probe Settings**

| Field | Description |
|---|---|
| VLAN Range | The start and end **VLAN Range** to probe.<br>You can enter up to five ranges separated by commas, up to a total range of 12. However, range numbers cannot overlap. For example, `1, 2-7, 8, 8-12`. |
| Probe Retries | The number of attempts made to send a probe to verify the status of a VLAN. |
| Timeout | The timeout from 5 to 60 seconds to specify how long to wait for a reply from each probe. |

6. Select **Start** to start a probe.
7. Select **Stop** to stop a probe before it is complete.

Related Links

Heat Map View on page 46
Device Summary and Actions Menu on page 51

*Reset a Device to Factory Defaults*

Use this task to reset the selected device to the default configuration. If you select **Yes** to acknowledge the warning message, the operation restores factory settings and reboots the device.

**Important**
This operation removes all existing settings from the selected device and resets the device to a factory default configuration state. The device reconnects to ExtremeCloud IQ (New) as a new device.

1. Go to **Monitoring** > **Visualize**.
2. From the Sites (**Quick Location Navigation**) menu, select a floor.

**Note**
Use **Search** to find a specific location in a large network. Type the first few characters to see a list of locations. The more characters you type, the more precise the search results are.

**Note**
The selected floor must include a floor plan. For more information, see Upload a Floor Plan on page 273.

3. From the view selector, select **Views** > **Heat Map**.
4. Select a connected device from the heat map, and then select **Actions** > **Reset to factory defaults**.

5. Select **Yes** to confirm.

Related Links

Heat Map View on page 46
Device Summary and Actions Menu on page 51

*Upgrade Device Firmware*

Use this task to manually upgrade firmware for a selected device from an RF Map.

**Note**
LLDP is on by default in ExtremeCloud IQ (New). With IQ Engine Release 10.7.5 and later, LLDP is on by default. If LLDP is disabled in the network policy, upgrading to 10.7.5 or later enables LLDP until after you perform a configuration update.

1. Go to **Monitoring** > **Visualize**.
2. From the Sites (**Quick Location Navigation**) menu, select a floor.

**Note**
Use **Search** to find a specific location in a large network. Type the first few characters to see a list of locations. The more characters you type, the more precise the search results are.

**Note**
The selected floor must include a floor plan. For more information, see Upload a Floor Plan on page 273.

3. From the view selector, select **Views** > **Heat Map**.
4. Select a connected device from the heat map, and then select **Actions** > **Upgrade firmware**.
5. In the **Device Update** dialog box, select an update type.

**Table 16: Update AP Device Settings**

| Field | Description |
|---|---|
| **Update Network Policy and Configuration**: | |
| Delta Configuration Update | To update only the configuration changes for the selected device, select **Delta Configuration Update**. ExtremeCloud IQ (New) only updates the device deltas. This action avoids a device reboot. |
| Complete Configuration Update | If a full update is required, select **Complete Configuration Update**. Used to reset the selected AP to ExtremeCloud IQ (New) configuration settings. For information about how the configuration push behaves with each **Activation Time** option, see Configuration Push Scheduling Behavior on page 154.<br><br>**Note:** Only supported on devices running HOS or IQE Firmware. |
| **Upgrade IQ Engine and Extreme Network Switch Images**: | |

**Table 16: Update AP Device Settings (continued)**

| Field | Description |
|---|---|
| Upgrade to the latest version | Upgrade to the latest firmware version. |
| Upgrade to the specific version | Select a **Model** to upgrade, and then select the **Version** to upgrade.<br>To add a new version (local image), select **Add/Remove**:<br>• To add a new local image, select +, and then select **Choose** to upload an image file from your computer.<br>**Note:** The format for an image file name must be *.stk, *.xos, *.voss *.tgz, *.img, or *.img.S. The file name cannot contain spaces and must not exceed 64 characters.<br>• To delete an existing local image, select an image, and then select 🗑.<br>• Select **Close**.<br>Select **View Release Notes** to access the Online Help system and see the latest release notes. |
| (Optional) Upgrade even if the versions are the same | Force an upgrade to the same version as the current version. |

**Table 17: Update Switch Device Settings**

| Field | |
|---|---|
| **Update Network Policy and Configuration**: | |
| Reboot and revert Extreme Networks switch configuration if IQAgent is unresponsive after configuration update. | **Note:** Not supported on Dell/SR. |
| Perform delta configuration update and resolve local device configuration which is out of sync with Extreme Platform ONE Networking. | |
| **Upgrade IQ Engine and Extreme Network Switch Images** | |

6. To update the selected device immediately, select **Perform Update**.
7. To save the settings for future use, select **Save as Defaults**.

Related Links

Import a Third-Party RF Map on page 62
Edit a Heat Map on page 64

*Configure AP Radio and Power Settings*

Use this task to configure AP radio and power settings.

1. Go to **Monitoring** > **Visualize**.

2. From the Sites (**Quick Location Navigation**) menu, select a floor.

**Note**
Use **Search** to find a specific location in a large network. Type the first few characters to see a list of locations. The more characters you type, the more precise the search results are.

**Note**
The selected floor must include a floor plan. For more information, see Upload a Floor Plan on page 273.

3. From the view selector, select **Views** > **Heat Map**.
4. Select a connected device from the heat map, and then select **Actions** > **Radio and Power configuration**.
5. Select a Wi-Fi interface, configure the radio and power settings in Table 18, and then select **Apply**.

**Table 18: Radio and Power Configuration Settings**

| Field | Description |
|---|---|
| Radio Status | Toggle the **Radio Status**. |
| Channel | Select a specific channel. Select **Auto** to have ExtremeCloud IQ (New) select the channel. |
| Transmission Power | Set the transmission power for the selected device (1 to 20 dBm). Select **Auto** to have ExtremeCloud IQ (New) select the transmission power. |

Related Links

Heat Map View on page 46
Device Summary and Actions Menu on page 51

*View Client Roaming Trail*

Viewing the client roaming trail to an access point (AP) on a real-time map has the following benefits:

- **Troubleshoot Connectivity Issues**: Identify areas where the client might be experiencing weak signals or frequent disconnections.
- **Optimize Network Performance**: Understand the movement patterns to adjust the placement of APs to ensure better coverage and reduce dead zones.
- **Monitor Security**: Detect any unusual or unauthorized movements within the network, which could indicate potential security threats.

Use this task to view the roaming trail of a selected AP client from a real-time map.

1. Go to **Monitoring** > **Visualize**.

2. From the Sites (**Quick Location Navigation**) menu, select a floor.

   **Note**
   Use **Search** to find a specific location in a large network. Type the first few characters to see a list of locations. The more characters you type, the more precise the search results are.

   **Note**
   The selected floor must include a floor plan. For more information, see Upload a Floor Plan on page 273.

3. From the view selector, select **Views** > **Heat Map**.
4. Select the purple halo above a device.

   The purple halo shows the number of connected clients on the device.
5. From the **Inventory** list, select an available **Hostname**, and then select **Actions** > **Client Roaming**.

   A split window opens:

   - **Left Pane**: This pane displays the map and shows how the client roamed.
   - **Right Pane**: This pane displays the roaming view details, including the Client Name, Roam Duration, RSSI, SNR, Channel, Frequency, Roam Status, Roam Type, Reason, and Surrounding APs.

     **Note**
     **Roam Status** and **Roam Type** are not shown during periods of disconnected roaming.

6. To view the roaming trail, from the right pane, select **Play**.

   **Note**
   By default, the roaming view displays client roaming details for the previous hour.

   The roaming trail plays within the top map pane, showing where the client roamed and how long it took:

   - A **green** roaming trail signifies a good roam (less than one second).
   - A **red** roaming trail signifies a slow roam (longer than one second).
7. To narrow the roaming time frame, from the right pane, select the **Date & Time Range**.
   a. Select a **Start Date** and **End Date**.
   b. Select a **Start Time** and **End Time**.
   c. Select **Done**.

   To reset to the default time frame, select **Reset to Default**.
8. To exit the roaming view and return to the heat map, select **X**.

Related Links

Heat Map View on page 46

## Create a Device Filter from the Heat Map View

The Heat Map view allows you to visually filter network devices based on their physical location. Using the filter tool, you can draw a custom perimeter directly on the map to select devices within a specific area. After a perimeter is defined, you can quickly view the corresponding devices in the network device list, automatically filtered to include only those located within the selected area.

Use this task to create a device filter from the Heat Map view:

1. Go to **Monitoring** > **Visualize**.
2. From the Sites (**Quick Location Navigation**) menu, select a floor.

   **Note**
   Use **Search** to find a specific location in a large network. Type the first few characters to see a list of locations. The more characters you type, the more precise the search results are.

   **Note**
   The selected floor must include a floor plan. For more information, see Upload a Floor Plan on page 273.

3. From the view selector, select **Views** > **Heat Map**.
4. Select .
5. Draw a perimeter: Double click to close the perimeter.
   a. Select each corner of a perimeter to select and group devices on the map.
   b. When you reach the end of the perimeter, double-click the last corner to complete the filter area.
6. To view the filtered network device list, select **View List**. To clear the filter perimeter, select **Cancel**.

   The Network Device Status list appears, filtered to show only devices within the drawn perimeter. To return to the Heat Map view, select the browser back button.

Related Links

Heat Map View on page 46

## Import a Third-Party RF Map

ExtremeCloud IQ (New) supports the following third-party RF Maps:

- Ekahau
- Hamina

Use this task to import a third-party RF Map.

1. Go to **Monitoring** > **Visualize**.

2. From the Sites (**Quick Location Navigation**) menu, select a floor.

   **Note**
   Use **Search** to find a specific location in a large network. Type the first few characters to see a list of locations. The more characters you type, the more precise the search results are.

   **Note**
   The selected floor must include a floor plan. For more information, see Upload a Floor Plan on page 273.

3. From the view selector, select **Views** > **Heat Map**.
4. Select .
5. To import a floor map from Ekahau, select **Import Ekahau**:
   a. Select **Choose**, then browse to your local folder, select a .esx floor plan, and then select **Open**.

      **Note**
      Use the **serialNumber** tag to import devices with your floor plan.

   b. Select **Next**.
   c. From **Import floors**, select a **Building** from the drop down list.

      **Note**
      With RF Maps you can only import building floors. To import a site, site folder, or a building, go to **Configuration** > **Sites**.

   d. If the configuration is custom, select the **Import Custom AP Configuration** check box.
   e. Select one or more floor plans.
   f. To move a single floor plan, double-click the selected plan.
   g. To move more than one plan, select the applicable arrow.
   h. Select **Import**.
6. To import a floor map from Hamina, select **Import Hamina**:
   a. Log in to your active Hamina account and select **Export**.
   b. Select **Extreme Networks** and follow the instructions.
   c. Select **Export**.

   Your floor map now displays APs in the correct building on the correct floor.

Related Links

Heat Map View on page 46
Edit a Heat Map on page 64

## View Antenna Patterns

**Antenna Patterns** allow users to visualize the coverage and performance of devices on the heat map. This visualization is essential for optimizing network design and troubleshooting connectivity issues.

**Note**
Antenna Patterns are not available for controller-managed APs, third-party APs, or WiNG devices.

The antenna patterns display how the antenna radiates energy in different directions and frequencies, including:

- Azimuth Plane: A top-down view of the radiation pattern, illustrating how the signal spreads out horizontally. It helps in understanding the coverage area and signal strength in different directions around the device.
- Elevation Plane: A side view of the radiation pattern, illustrating how the signal spreads out vertically. It helps in understanding the coverage area and signal strength above and below the device.
- Frequency Band: Along with Azimuth and Elevation planes, displays the radiation pattern for the 2.4 GHz, 5 GHz, and 6 GHz frequency bands for wireless devices.

These patterns help network administrators visualize and optimize device placement to ensure even and effective coverage.

Use this task to view antenna patterns.

1. Go to **Monitoring** > **Visualize**.
2. From the Sites (**Quick Location Navigation**) menu, select a floor.

   **Note**
   Use **Search** to find a specific location in a large network. Type the first few characters to see a list of locations. The more characters you type, the more precise the search results are.

   **Note**
   The selected floor must include a floor plan. For more information, see Upload a Floor Plan on page 273.

3. From the view selector, select **Views** > **Heat Map**.
4. Select .

   **Note**
   Use the **Search** field to find a specific device.

5. Select a device tab.

## Edit a Heat Map

An RF Map provides a visual representation of device signal strength across a floor plan. By editing the RF Map, you can identify areas with weak coverage, interference, and dead zones.

This information helps network administrators optimize device placement and improve overall network performance.

ExtremeCloud IQ (New) supports the following RF Map editing functions:

- Draw Inner Walls
- Manage Devices on a Heat Map
- Adjust Layer Opacity
- Resize the Heat Map

**Note**
The Recalibration tool uses the distance unit set during floor creation. For more information, see Add a Floor on page 272.

- Create and Manage Heat Map Zones
- Create and Manage Heat Map Labels

Use this task to edit an RF Map.

1. Go to **Monitoring** > **Visualize**.
2. From the Sites (**Quick Location Navigation**) menu, select a floor.

**Note**
Use **Search** to find a specific location in a large network. Type the first few characters to see a list of locations. The more characters you type, the more precise the search results are.

**Note**
The selected floor must include a floor plan. For more information, see Upload a Floor Plan on page 273.

3. From the view selector, select **Views** > **Heat Map**.
4. Select .
5. To draw inner walls, see Draw Inner Walls on a Heat Map on page 66.
6. To manage devices on the map, see Manage Devices on a Heat Map on page 67
7. To adjust the opacity of the heat map layers, select **Layers** and adjust the opacity slider bar to make a layer more or less transparent.

**Note**
As you adjust the slider bar, the layer opacity changes on the map in real time.

8. To resize the heat map:
   a. Select **Recalibrate**.
   b. Select your starting point on the map.
   c. Select again to close the line.
   d. Add a measurement (in the unit configured for this floor plan) for the line distance, and then press **Enter**.
9. To create and manage map zones, see Manage Heat Map Zones on page 68.
10. To create and manage map labels, see Manage Heat Map Labels on page 70.

11. To return to the heat map, select **Exit**.

Related Links

Heat Map View on page 46
Import a Third-Party RF Map on page 62

*Draw Inner Walls on a Heat Map*

Drawing inner walls on a Heat Map allows you to more accurately represent physical obstacles within a building or space, such as offices, conference rooms, hallways, or partitioned areas. Inner walls help the Heat Map better reflect how wireless signals propagate through the environment.

By defining inner walls, you provide the Heat Map with additional spatial context that improves the accuracy of coverage visualization, signal strength display, and performance analysis. Walls can attenuate, block, or redirect wireless signals, and modeling these structures on the Heat Map results in a more realistic representation of actual network conditions.

Use this task to draw inner walls on a Heat Map:

1. Go to **Monitoring** > **Visualize**.
2. From the Sites (**Quick Location Navigation**) menu, select a floor.

**Note**
Use **Search** to find a specific location in a large network. Type the first few characters to see a list of locations. The more characters you type, the more precise the search results are.

**Note**
The selected floor must include a floor plan. For more information, see Upload a Floor Plan on page 273.

3. From the view selector, select **Views** > **Heat Map**.
4. Select .
5. Select **Walls**.
6. Select a wall type. See Table 19 for wall type descriptions.

**Table 19: Floor Plan Wall Types**

| Wall Color | Description |
|---|---|
| | Bookshelf 5dB |
| | Cubicle 2dB |
| | Dry Wall 3dB |
| | Brick Wall 5dB |
| | Concrete 15dB |

**Table 19: Floor Plan Wall Types (continued)**

| Wall Color | Description |
|---|---|
| | Elevator Shaft 10dB |
| | Thin Door 4dB |
| | Thick Door 10dB |
| | Thin Window 1dB |
| | Thick Window 6dB |
| Add Custom Material | Create a new custom material by entering a **Name**, specifying the **Attenuation** (in dB), and selecting a **Color**. Select **Apply** to use this new material type.<br>Delete an existing custom material by selecting the material and pressing the **Delete** key on your keyboard.<br><br>**Note:** Custom materials can only be deleted after all associated references to the them have been removed. |

7. Select each corner of an inner wall on the floor plan to draw a wall boundary.
8. When you reach the end of the wall boundary, double-click the last corner to complete the wall.

   **Note**
   Right-click on a wall to change its type or delete it.

9. To disable the pen tool, press the **ESC** key on your keyboard.

Related Links

Edit a Heat Map on page 64

*Manage Devices on a Heat Map*

Managing devices on a Heat Map allows you to accurately represent where network devices are physically located within your environment. By placing devices directly on the map, you ensure that Heat Map visualizations reflect real-world deployment locations and conditions. Keeping device placement up to date helps maintain the accuracy of coverage, signal strength, and performance data displayed on the Heat Map.

Accurate device placement is especially important for troubleshooting wireless performance issues, analyzing coverage gaps, and validating network design. When device locations align with the physical layout of a site, Heat Map data becomes easier to interpret and more actionable. This also improves collaboration across teams by providing a shared visual reference for discussing device placement, planning changes, or documenting the network environment.

Use this task to add devices to specific locations, move devices as layouts change, and remove devices that are no longer relevant to the mapped area.

1. Go to **Monitoring** > **Visualize**.
2. From the Sites (**Quick Location Navigation**) menu, select a floor.

   **Note**
   Use **Search** to find a specific location in a large network. Type the first few characters to see a list of locations. The more characters you type, the more precise the search results are.

   **Note**
   The selected floor must include a floor plan. For more information, see Upload a Floor Plan on page 273.

3. From the view selector, select **Views** > **Heat Map**.
4. Select .
5. Select **Devices**:
   a. Select a device, or use the **Search** field to find a device.
   b. Hover over the floor map and select the desired location to add the device to the floor plan.

   **Note**
   Only devices that are not associated with the floor plan are displayed.

6. To move a device to a new location on the map, select a device and drag it to the desired location.
7. To remove a device from the floor plan, right-click the device, and then select **Remove Device**.

   **Note**
   The removed device displays in the **Devices** list.

Related Links

Edit a Heat Map on page 64

*Manage Heat Map Zones*

Create zones to define, organize, and visually group specific areas on a Heat Map using custom boundaries. Zones help visualize Wi-Fi coverage across different parts of a building or campus. Zones provide a way to segment a map into meaningful regions, such as departments, coverage areas, service zones, or operational spaces, making it easier to verify signal strength and manage the network at a location-based level.

Draw zone perimeters around areas of interest and assign them a name, color, and set the visibility. Naming zones helps identify their purpose, color-coding improves visual distinction between areas, and visibility controls allow you to show or hide zones as needed to reduce visual clutter or focus on specific regions.

Dividing a Heat Map into zones illustrates how radio performance and interference can vary by area. For instance, a zoned map can show that a high-density auditorium might need

a different access point plan or power configuration than a quiet office zone. In enterprise settings, zones can be tied to analytics tools that measure how users move or connect within specific regions — improving layout planning and helping businesses understand space utilization.

You can move a zone behind other zones and Heat Map elements, ensuring important data, labels, or overlapping zones remain visible and easy to interpret.

Managing zones is especially useful in large or complex environments where multiple areas must be monitored or compared.

Zones can represent high-density areas, service regions, or critical operational spaces, allowing you to quickly assess trends, troubleshoot issues, and communicate findings using clearly defined boundaries.

Use this task to manage zones on a Heat Map.

1. Go to **Monitoring** > **Visualize**.
2. From the Sites (**Quick Location Navigation**) menu, select a floor.

   **Note**
   Use **Search** to find a specific location in a large network. Type the first few characters to see a list of locations. The more characters you type, the more precise the search results are.

   **Note**
   The selected floor must include a floor plan. For more information, see Upload a Floor Plan on page 273.

3. From the view selector, select **Views** > **Heat Map**.
4. Select .
5. Select **Add New Zone**.
6. To draw a zone boundary, select each corner of an area on the heat map. To complete the zone, double-click the last corner.
7. From the **Add Zone** window, configure the following settings, and then select **Save**:
   - **Name**: The descriptive name of the zone.
   - **Visible**: Toggle to show or hide the zone on the Heat Map.
   - **Choose Color**: Select the color used to display the zone boundary on the Heat Map.

   **Note**
   To discard the new zone, select **Cancel**. The drawn boundary is removed from the Heat Map and the zone is not created.

8. To manage existing zones directly from the map, right-click a zone from the list and then perform one of the following steps:
   - **Update an existing zone**: Select **Edit**. Update the zone settings and then select **Save**.
   - **Delete an existing zone**: Select **Remove** twice to confirm.
   - **Reorder zones**: Select **Send to Back** to move the zone behind other zones and Heat Map elements. This helps ensure overlapping zones remain visible and easy to interpret.

Related Links

Edit a Heat Map on page 64

*Manage Heat Map Labels*

Create labels to add descriptive context to the Heat Map by marking important areas, locations, or points of interest. Labels help translate visual Heat Map data into meaningful, easily understood references that reflect the physical layout of your environment.

By creating and maintaining labels, you can identify specific rooms, zones, floors, buildings, or functional areas directly on the Heat Map. Editing or removing labels ensures that the map stays accurate as layouts or naming conventions change, while hiding and showing labels lets you control the level of visual detail displayed during analysis or troubleshooting.

Heat Map labels are especially useful when monitoring coverage, investigating performance issues, or collaborating across teams. Labeled locations make it easier to quickly pinpoint where issues occur, communicate findings clearly, and align Heat Map data with real-world locations. Labels also improve the usefulness of Heat Map screenshots or shared views by providing immediate context without requiring additional explanation.

Use this task to manage Heat Map labels to help keep maps organized, readable, and relevant, ensuring they remain an effective tool for analysis, troubleshooting, and operational planning.

1. Go to **Monitoring** > **Visualize**.
2. From the Sites (**Quick Location Navigation**) menu, select a floor.

   **Note**
   Use **Search** to find a specific location in a large network. Type the first few characters to see a list of locations. The more characters you type, the more precise the search results are.

   **Note**
   The selected floor must include a floor plan. For more information, see Upload a Floor Plan on page 273.

3. From the view selector, select **Views** > **Heat Map**.
4. Select .
5. Select **Labels** > **Add Label**.
6. Select the area of the Heat Map where you want to place the label.
7. Type a label name and then press **Enter**.

   The new label appears on the Heat Map and is added to the labels list.
8. To manage existing labels directly from the map, right-click a label and then perform one of the following actions:
   - **Update an existing label**: Select **Edit**. Update the label and then press **Enter** to save changes.
   - **Remove an existing label**: Select **Remove** twice to confirm.
   - **Hide a label on the map**: Select **Hide**.
   - **Show a hidden label on the map**: From the label list, right-click the hidden label and then select **Show**.

Related Links

Edit a Heat Map on page 64

## Access View

The **Access** view shows per floor view of edge devices such as access points, phones, and cameras connected to a device in a building. The view in the content pane depends on your selection in the navigation pane, as follows:

- If you select a site or group of sites, the content pane displays the first building belonging to the selected site or group of sites.
- If you select a building, the content pane displays the edge devices and connections for that building.
- If you select a floor, the content pane displays the edge devices and connections for that building, and focus is set to the selected floor.

The content pane displays the following devices (expanded) for the **Access** view:

- APs assigned to the selected floor or building
- If the LLDP Neighbors feature is enabled, the **Access** view includes the following devices:
  - LLDP-detected devices connected to switches on the selected floor or in the selected building
  - Cameras connected to switches on the selected floor or building
  - Phones connected to switches on the selected floor or building
  - Other devices connected to switches on the selected floor or building
- Existing links between switches that appear in the content pane

You can hover over an edge device or select it to view the details.

## Device Detection

**Visualize** supports managed APs, VOSS (Fabric Engine), and EXOS (Switch Engine) devices.

Use **Visualize** to view and manage all devices onboarded through common onboarding services, including switch stacks. **Visualize** view generates a topology map of all managed on-boarded devices by analyzing data from the LLDP protocols (physical) and Intermediate System to Intermediate System (IS-IS) logical tables.

Detected devices inherit the location (building and floor) from the reporting switch. If multiple switches detect a device, the device inherits the location from the first reporting switch. If the reporting switch is deleted, the device inherits the location from the next reporting switch.

If there is only one reporting switch and it is deleted, ExtremeCloud IQ (New) removes the device from the canvas.

**Table 20: Device Discovery based on LLDP**

| Adjacency | Description |
|---|---|
| Physical | Extreme Platform ONE Networking uses physical network connections to generate LLDP Neighborship from the devices. |
| Logical | Extreme Platform ONE Networking uses logical network connections to generate LLDP Neighborship, ISIS tables, and SD-WAN data. |
| Third-Party Devices | Special LLDP TLVs discover third-party devices, such as cameras, IoT devices, and sensors, and show them as attached devices on the topology map. |

## Device Group

The **Visualize** view uses site-group and site hierarchy in Extreme Platform ONE Networking for the auto-creation of groups during the device onboarding process. Sites and site groups appear in groups on topology maps.

The topology map is a persistent view. The following map characteristics persist after you log out and log back in:

- Layout changes
- Hierarchical level
- User-defined details

## Update Topology

Use this task to add devices onboarded through ExtremeCloud IQ or Extreme Platform ONE Networking to the Visualize canvas.

**Note**
The **Visualize** canvas displays devices as partially connected until the discovery process is complete and statistics have been received.

1. Go to **Monitoring** > **Visualize** and select **Sites**.
2. Select , and then select **Expand All**.
3. Locate the required building or floor.
4. Select for the building or floor, and then select **Update Topology**.

   After successful device discovery, a notification message with a **Refresh** button opens.
5. To refresh the **Visualize** canvas from the **Success** notification, select **Refresh**.

# Inspector Panel

Use the **Inspector** panel to view more information about a selected site, building, floor, or group of devices. Use the **Device Inspector** panel to view more information about a selected device.

**Table 21: Inspector panel tabs**

| Tab | Description |
|---|---|
| Summary | Lists all devices for the selected site, building, floor, device or group of devices. To open the **Device Inspector** panel for a device, select the link.<br><br>**Note:** Masked devices do not appear on the topology, and therefore do not include a link. Aggregates of devices also do not include links. However, if you select an aggregate on the topology, the **Inspector** panel displays a list of the aggregated devices with links. |
| Alerts | Lists unacknowledged critical alerts for the past 24 hours, for the selected site, building, floor, device or group of devices. For more information about an alert and to acknowledge it, select the link. To open the **Alerts** page, select **Show All**. |
| Services/VLANs | Lists VLANs and services for the selected site, building, floor, device or group of devices, divided into the following tabs:<br>• VLANs<br>• L2 Services<br>• L3 Services |
| Clients | (**Device Inspector** panel only)<br>Lists the clients for a device. For details about a client, select the corresponding link. |

Related Links

View the Inspector Panel on page 73
View the Device Inspector Panel on page 74

## View the Inspector Panel

Use this task to view the **Inspector** panel.

1. Go to **Monitoring** > **Visualize**.
2. Select  to open the view selector and choose the topology map view.
3. From  (**Quick Location Navigation**), select a site, building, floor, or group of devices.
4. To toggle the **Inspector** panel for the selected site, building, floor, or group of devices, select .

   The Inspector panel provides more information on each of the following tabs:

   - **Summary**
   - **Alerts**

- **Services/VLANs**

To display configured names on the **Services/VLANs** tab, select the **VLANs**, **L2 Services**, or **L3 Services** tab. Select , and then select . Select **Configured Names**.

## View the Device Inspector Panel

Use this task to view the **Device Inspector** panel.

1. Go to **Monitoring** > **Visualize** and select a view or layer.
2. Select to open the view selector and choose the topology map view.

   To view service mapping using topology layers, use the **View Selector** menu to select one of the following options:

   - **Views** > **Service & Fabric**
   - **Views** > **Service & Physical**
3. From Sites (**Quick Location Navigation**), select a site, building, or floor.
4. To view device-specific information, select a device on the topology map.

   To open the Device Inspector panel for a group of devices, press **Ctrl**, select multiple devices, and then select .

   A device-specific inspector panel opens. You can expand or collapse the device information for a focused view in each tab. For information about the tabs, see Inspector Panel on page 73.

   The Device Inspector panel for the Physical layer and Access views provides an **Unlock Full Features** link for devices located in buildings, floors, and sites with limited features, and for individual devices with ExtremeCloud IQ Pilot subscriptions. For a group of devices, the **Summary** tab of the panel displays the devices with ExtremeCloud IQ Pilot subscriptions, identified by a tooltip.

   If a device shows **Connected, Limited Features**, see *Extreme Platform ONE Networking and ExtremeCloud IQ Licensing Guide* for information about reassigning licenses to unlock full features.
5. (Optional) Initiate one or more of the following options from the Device Inspector panel 3-dot menu:

   - Reboot
   - VLAN Probe
   - Assign Location
   - Configure Device
   - Configure Fabric
   - Retrieve Bug Data
   - Update Device

6. To view more information about each of the **Diagnostics** widgets, select the widget.

**Table 22: Diagnostic Widgets and corresponding Device 360° pages**

| Widget | Device 360° page |
|---|---|
| Device Health | Overview |
| Usage & Capacity | Port Stats (wired device selected)<br>Wireless Interface (wireless device selected) |
| Clients Health | Clients |

7. To view more information, select the heading for each of the following sections:
   - **Device Details**
   - **Tags**
   - **Wired Interfaces**
   - **Wireless Interfaces**
8. (Optional) To add existing Manual tags, expand the **Tags** section, and do the following:
   a. In the **Manual Tags** section, select **Add Tag**.
   b. Select one or more tags from the list.

      You can start typing the name of a tag to search. Multiple tags are comma-separated.
   c. Select the search field, and then select **Done**.
9. (Optional) To add new Manual tags, expand the **Tags** section, and do the following:
   a. In the **Manual Tags** section, select **Add Tag**.
   b. Type the name of the new tag, or type the names of multiple new tags, separated by commas.
   c. Select **Add Tag**.



**Tip**
To display the new tags, refresh the page.

Related Links

Inspector Panel on page 73

## View and Acknowledge Alerts

You can use **Sites** (**Quick Location Navigation**) to navigate to critical alerts by location on the topology map.

Use this task to view and acknowledge alerts from the **Inspector** panel in **Visualize**.

1. Go to **Monitoring** > **Visualize**.
2. Use Sites (**Quick Location Navigation**) to navigate to critical alerts by site, building, or floor.
3. Select a location with critical alerts.
4. To open the **Inspector** panel, select a device.
5. To view alerts, select the **Alerts** tab in the **Inspector** panel.

6. Select an alert from the **Top 3 Alerts** list to view and acknowledge.
7. Select **Acknowledge** to mark the alert as reviewed.

## View Device 360°

Use this task to open Device 360° from the **Device Inspector** panel in **Visualize**.

1. Go to **Monitoring** > **Visualize**.
2. To open the **Device Inspector** panel, select a managed device in the topology map.
3. In the **Device Inspector** panel, select .

   Available information depends on the device selected and the connection type (wired or wireless). For more information, see the following topics:

   **Wired Devices**

   - Overview on page 205
   - Clients on page 206
   - Port Stats on page 207
   - Services/VLANs on page 208
   - Routing on page 209
   - Events on page 210

   **Wireless Devices**

   - Overview on page 205
   - Wireless Interfaces on page 216
   - Wired Interface on page 217
   - Clients on page 217
   - Alerts on page 218

# AutoSave Device Layout and Density

Use this task to enable the autosave feature for device layout and density in the Access view.

1. Select  to unlock device layout and density.
2. Enable the **AutoSave** option.
3. Go to , and select a floor.
4. Select  for the floor, and then choose the required **Device Layout** and **Density** options for the topology map:

   **Device Layout** :

   - Stacked
   - Spread
   - Grid
   - Hierarchical

**Density**:

- Very Sparse
- Sparse
- Dense
- Very Dense

## Search an Element

You can search the network for configured VLANs, L2, and L3 services. **Visualize** can display five global services on the topology map. You can select or switch between these global services to view the topology map.

Use this task to search an element in the network topology map.

1. Go to **Monitoring** > **Visualize**.
2. Select .
3. Select the required filter keyword for searching:
   - Devices
   - Services
   - VLANs
4. Type a **Device Name** in the **Search** field.

   All devices with the specified search value open in the global view.

## Topology Map Settings

Select to configure topology map settings in the **Visualize** view.

### Configure the Display Options

Use this task to configure display options for Visualize topology maps.

**Note**
The display options are user-specific.

1. Go to **Monitoring** > **Visualize** and select .
2. Select **Display Options**.
3. Select the **Access** layer options:
   - **Device Labels**: **Name**, **IP**, or **Type** (Select any two.)
   - **LLDP Neighbors** (devices with LLDP and Fabric Attach capabilities):

     You can expand or collapse **Display LLDP Options** to view and edit the list of LLDP devices:
     - Detected APs
     - Cameras

- Phones
- Others (LLDP devices without any capabilities set)

**Note**
To include all types of devices without LLDP capabilities, select **Others**. This option is disabled by default.

4. Select **Apply Settings**.

## Manage

The following capabilities are available on the **Settings** > **Manage** tab for all views and layers, except **Geographic**.

- Select **Save User Settings** to save display options, filters, expand/collapse state of **Quick Location Navigation**, topology focus, zoom level, border state, device types settings, and the breadcrumb path.
- Select **Restore Saved User Settings** to restore and apply the saved display options, filters, and border settings.
- Select **Manage Tags** to view tags.

*Tags*

Apply **Tags** to managed resources in the **Visualize** view. The tags act as labels and help in easy filtering of the devices in maps.

**Table 23: Tag types**

| Tag Type | Description |
|---|---|
| Default Tag | Default tags are auto assigned during device discovery based on predefined criteria. These tags are created based on switch type, location, model, VLAN, VRF, L2 service, and L3 service.<br>The default tags are read-only and cannot be altered or deleted.<br>The system automatically assigns **Provisional** tags to masked devices. |
| Manual Tag | Manual tags are labeled by the user. |

# User Roles Supported in Visualize View

Visualize view supports the following user roles:

**Table 24: Supported user roles**

| User Role | Description |
|---|---|
| Administrator | Administrators have read-write access to Visualize view. They can create and manage all administrator users and licenses through Visualize view. |
| BizSecOps | BizSecOps have read-write access, but cannot manage accounts and licensing. |

**Table 24: Supported user roles (continued)**

| User Role | Description |
|---|---|
| BizOps | BizOps have no access to Visualize view. |
| Observer | Observers have read-only access to Visualize view. |

For more information about roles, see Role-Based Access on page 576.

# Monitoring | Alerts

Manage Alerts on page 80

The **Alerts** view provides a comprehensive overview of network alerts, allowing operators to detect, record, and report specific events. It evaluates performance metrics and reports occurrences where specific criteria are met. Alerts can be filtered by time range, sites, alert name, severity, acknowledged, application, location, categories, source, and status.

Users can receive alert notifications through email or Webhooks.

**Note**
Extreme Platform ONE Networking offers a Client Lockout Alert. This new alert applies to cloud PPSK users only. Local PPSK authentication is handled on-device and does not go through the cloud, so local PPSK clients are not in scope for lockout detection or alerting.

Related Links

Add Email Recipient on page 716

Add Webhook on page 717

## Manage Alerts

The **Alerts** view offers widgets such as **Severity**, **Category**, **Top 3 Alerts**, and **Application** to filter the list of alerts raised during the specified time range.

Go to **Monitoring** > **Alerts**. The widgets are enabled by default. Select **Show Summary** to disable the widgets.

You can use widgets to filter the list of alerts raised during the specified time range.

The user interface filters out inactive alerts and alerts from deleted devices, so that only active, unacknowledged, and critical alerts from the last 24 hours are displayed. This applies to:

- Geographical view tooltips (**Site** and **Building** levels)
- The **Alerts** panel in the **Object Inspector**
- The **Quick Location Navigator** in the Physical and Fabric views

The alert label in the **Object Inspector** has been updated to clarify the filtering criteria (for example "Active, Last 24 hours"), providing a more accurate and actionable view of current network issues without noise from resolved or inactive alerts.

Select **Alert Policies** to view and manage global and site policies.

**Note**
Site policies take precedence over global policies.

## Alert Details

By default, the **Alerts** page displays information about active alerts raised at all sites for the last 24 hours. You can view and filter the **Alert Details** list using the following methods:

- Use the **Time Range** controls to specify a time range, within the last 30 days, for which you want to view alerts.
- Use the **Refresh Alerts** button to view the most recent alerts.
- Use the **Sites** filter to view alerts associated with a specific site.
- Select **Alert Policies** to edit and update which alerts appear in the **Alert Details** list.
- Use the **Search** field to find alerts.
- Use the **Export to CSV** button to download the alert data in `.CSV` format.
- Use **Filters Applied** to enable and disable active and inactive alerts in the **Alert Details** list.
- Use the **Clear All Filters** button to remove all the filters that have been applied to the **Alert Details** list.

The **Alert Details** list can also be filtered using the following columns. You can make multiple selections.

- Use **Alert Name** to filter alerts by the name of the alert.
- Use **Severity** to view alerts based on specific severity:
  - Critical - Red
  - Major, Minor, and Warning - Orange
  - Info - Blue
- Use **Acknowledged** to view all alerts (default), **Acknowledged**, or **Unacknowledged** alerts.
- Use **Application** to view alerts by alert rule categories:
  - **WIPS**
  - **Extreme Vendor Specific**
  - **ExtremeCloud IQ**
  - **ExtremeCloud SD-WAN**
  - **Extreme Platform ONE Security**
- Use **Location** to filter alerts further by location.
- Use **Categories** to filter alerts by category.
- Use the interactive device host name in the **Source** column for more information about the alert.
- Use **Status** to filter alerts by active alerts, inactive alert, or both.

**Note**
The column filter settings do not persist.

## Use the Filter and Columns Side Bar

Use the filter sidebar to customize the information shown in the **Devices** list and other **Alerts** view tables. You can save and reuse custom-defined filters. Saved filters are displayed in the saved filters section.

The Filter icon changes depending on whether a filter is applied.

Use the columns sidebar to customize the columns shown in the **Alert Details** list.

## View and Acknowledge Alerts

1. Go to **Monitoring** > **Alerts**.
2. Navigate to alerts by **Severity**, **Category**, **Top 3**, or **Application**.
3. Select an alert from the list to view and acknowledge.
4. Select **Acknowledge** to mark the alert as reviewed. Select **Clear Alert** to remove the alert from the **Alert Details** list.



**Note**
The Rogue AP and Rogue Client alerts have two additional available actions:

- **Mitigate**: Disconnects the AP or the client.
- **Locate**: Navigates to **Visualize** > **Heatmap** > **Floor**.

## Add a Site Policy

Use this task to add a site policy.



**Note**
The Observer role does not have access to Alert Policies.

1. Go to **Administration & Settings** > **Alert Policies**, and select **Site Policies**.
2. Select **Add Site Policy**.
3. Complete the following:
   - Provide the **Alert Policy Name**.
   - Select **Sites**.
4. Select **Next**.
5. Select an **Alert Rule** and optionally edit, enable, or disable the rule parameters.
6. Select **Apply Rules**.
7. To edit or delete the site policy, from the 3-dot menu, select **Edit** or **Delete**.

# Monitoring | Network Devices

Supported Universal Access Points on page 84
Universal AP Boot and Onboarding Process on page 94
AFC Overview on page 99
Adding Controllers and Appliances for Locally Managed Devices on page 110
Universal Compute Platform Support on page 111
Extreme Tunnel Concentrator Support on page 112
Network Devices | Device Status on page 112
Network Devices | Device Health on page 125
Network Devices | Usage & Capacity on page 127
Network Devices | Add Devices on page 129
Upgrade Network Device Firmware on page 133
Device 3-Dot Menu Actions on page 134
Packet Capture on page 155
Configure Devices on page 159
Device 360 View on page 204

**Network Devices** is a centralized location for monitoring both wired and wireless network devices. It provides detailed insights into the performance, health, and usage of each device, helping you maintain optimal network functionality. Go to **Monitoring** > **Network Devices** to display a list of devices in your network.

Extreme Cloud IQ (NEW) supports a broad range of deployment models and regulatory requirements, allowing organizations to build scalable, compliant, and flexible networks. Device capabilities vary by type, including wireless access points (APs), switches, gateways, and edge platforms. Some wireless APs support Automated Frequency Coordination (AFC) to meet regional spectrum regulations for 6 GHz operation. For more information, see Supported Universal Access Points on page 84 and AFC Overview on page 99.

From Network Devices, you can monitor the following information about a device, as well as onboard devices and upgrade device firmware.

- Device Status: Check if devices are connected, disconnected, or encountering problems.
- Device Health: Evaluate performance metrics such as CPU Usage, Memory Usage, and PoE Usage.
- Usage & Capacity: Understand bandwidth consumption, data transfer rates, and storage utilization.

- **Sites**: If you have access to multiple sites, select **Sites** to filter the network devices associated with a specific site.
- Add Devices: Add devices to the network using one of the following options:
  - Manually: Enter up to 10 serial numbers for devices of the same type.
  - Import: Add multiple devices of any type by uploading an XLSX file that contains device serial numbers.
  - **Download XLSX Template**: Download the XLSX template file to use when adding devices with the Import option.
- Upgrade Firmware: Manually upgrade firmware for selected devices.
- **Firmware Upgrade History**: Select ⋮ to view **Firmware Upgrade History**. Firmware upgrade activity is stored for a maximum of 30 days.

  **Note**
  To reschedule a scheduled firmware upgrade:
  - Select a scheduled upgrade, and then select **Reschedule Upgrade**.
  - Select a new **Date & Time**, and then select **Reschedule**.

- **Download XLSX Template**: Select ⋮ to download device list data to an XLSX spreadsheet.
- **Update Device Data**: Select ↻ to refresh and update device data.
- **Download**: Select ⬇ to download the table data as a CSV file.

## Supported Universal Access Points

Extreme Networks supports Universal APs that can operate in either ExtremeCloud IQ (New) or in an on-premises environment — one configured operating mode at a time. From the factory, Universal APs are configured for cloud management by ExtremeCloud IQ (New) and automatically engage with ExtremeCloud IQ (New) for onboarding. You have the option to deploy your devices locally — on-premises from ExtremeCloud IQ Controller — or from ExtremeCloud IQ (New). From an ExtremeCloud IQ (New) account, onboard and register the Universal AP using either Local Management or Cloud Management. To manage these APs on-premises, specify Local Management.

ExtremeCloud IQ (New) supports the following Universal APs.

**Table 25: ExtremeCloud IQ (New) Supported Universal APs**

| AP Class | Supported Universal APs |
|---|---|
| Wi-Fi 7<br>Universal World-Wide APs<br>ExtremeCloud IQ (New) | • AP3020/AP3020W/AP3020X<br>• AP4020/AP4020X/AP4020FX<br>• AP4060/X<br>• AP5020<br>• AP5022/AP5022FX/AP5022S6D*<br>• AP5060U/D* |
| Wi-Fi 6E<br>Universal World-Wide APs<br>ExtremeCloud IQ (New) | • AP3000/X<br>• AP4000<br>• AP4000-1<br>• AP5010<br>• AP5050U/D |
| Wi-Fi 6<br>Universal APs<br>ExtremeCloud IQ (New) | • AP302W<br>• AP305C/CX<br>• AP305C-1<br>• AP410C<br>• AP410C-1<br>• AP460C/S6C/S12C<br>• AP510C/CX |

* Supports **6H/5/6L** operating modes.

Related Links

AP3000 Series Radios and 6 GHz Support on page 85
AP4000/AP4000-1 Radios and 6 GHz Support on page 88
AP5000 Series Radios and 6 GHz Support on page 90

## AP3000 Series Radios and 6 GHz Support

The AP3000 series access points (APs) are Wi-Fi 6E tri-radio APs with support for multiple Extreme Networks operating systems. The AP3000 series APs include the following models:

- AP3000 — Indoor access point
- AP3000X — Indoor access point with optional external antenna.
- AP3020 — Indoor Wi-Fi 6E access point
- AP3020W — Indoor Wi-Fi 6E access point, worldwide regulatory domain
- AP3020X — Indoor Wi-Fi 6E access point with external antenna

**Note**
For all Extreme Networks APs, use the Extreme Networks certified ACC-WIFI-MICRO-USB console cable. Other MICRO-USB console cables have not been certified by Extreme Networks.

*AP3000/X*

AP3000/X APs offer two radios in three modes:

**Table 26: AP3000/X Operating Modes**

| Mode | Radio 1 (2x2) | Radio 2 (2x2) | Radio Definitions |
|---|---|---|---|
| 1 (Default) | g/n/ax | a/n/ac/ax | 2.4 GHz and 5 GHz |
| 2 | ax6 | a/n/ac/ax | 5 GHz and 6 GHz |
| 3 | Dedicated Sensor (2.4 GHz or 6GHz) | Dedicated Sensor (5 GHz) | |

Radio 1:

- sensor
- b/g
- g/n
- b/g/n
- g/n/ax (Default)
- client-bridge
- ax6

Radio 2:

- sensor
- a/n/ac
- a/n/ac/ax (Default)
- client-bridge

**Note**
When configuring sensor mode, set both Radio 1 and Radio 2 to **sensor** at the same time.

**Note**
The World-Wide Universal Access Points 6 GHz radios support only the following Wi-Fi Alliance (WFA) 6E Compliant network authentication methods:

- OWE (Opportunistic Wireless Encryption) for Open Networks
- WPA3-Personal (SAE/H2E)
- WPA3-Enterprise

ExtremeCloud IQ (New) requires that your 6 GHz radio network assignment be WFA 6E compliant. ExtremeCloud IQ (New) rejects network configuration changes that result in 6 GHz radio network assignments that are not compliant. It might be necessary to redefine your networks when configuring the 6 GHz radio on the Universal Access Points.

For the AP3000/X, before changing the Radio 1 configuration from 2.4 GHz to 6 GHz, ensure that the AP is assigned a 6E WPA compliant network.

*AP3020W*

The AP3020W is a Wi-Fi 6 dual-radio AP designed for indoor enterprise deployments and supports the following radio configuration:

- Radio 0 (WiFi0): 2.4 GHz
- Radio 1 (WiFi1): 5 GHz

- IoT radio: Bluetooth Low Energy (BLE)

**Note**
The AP3020W uses WiFi0 and WiFi1 only. Unlike tri-radio access points, AP3020W does not support a third radio interface (Wi-Fi 2). The Wi-Fi0 determines which frequency band is active.

The AP3020W includes an embedded IoT radio that supports BLE scanning for IoT applications. The following restrictions apply to AP3020W IoT configuration:

- The IoT radio is disabled by default on AP3020W models.
- When the IoT radio is enabled, only the Multiple (Bluetooth) IoT Application option is available. The Multiple option supports BLE beacon and scan applications, including iBeacon, Eddystone-url beacon scanning, and generic BLE scan reporting. The Single (Thread) option, which configures the AP as a Thread Backbone Border Router for IEEE 802.15.4 mesh networking, is not supported on the AP3020W.

**Note**
IoT Thread functionality is not supported on AP3020W models.

The AP3020 supports the following 6 GHz operating modes:

- Standard Power: Higher transmit power with Automated Frequency Coordination (AFC) authorization.
- Low Power Indoor (LPI): Lower transmit power without AFC authorization.

**Table 27: AP3020W Supported Operating Modes**

| Operating Mode | Description |
|---|---|
| 2.4/5 | Wi-Fi 0 operates on 2.4 GHz; Wi-Fi 1 operates on 5 GHz. |
| 6/5 | Wi-Fi 0 operates on 6 GHz; Wi-Fi 1 operates on 5 GHz. Select this mode to view and configure 6 GHz channel assignments. |

Standard Power allows the AP to transmit at higher power levels on the 6 GHz band compared to LPI mode, subject to regulatory authorization through AFC.

To use 6 GHz Standard Power on the AP3020W:

- The AP3020W must be deployed in a region that supports 6 GHz Standard Power (for example, the United States under FCC regulations).
- The AP must be registered with an AFC system.
- The AFC FTM policy and floor number must be configured for the AP3020W. For more information on AFC, see AFC Overview on page 99.

AP3020W 6GHz AFC certification:

- Standard Power (AFC-Controlled) requires registration of the AP3020W using the FCC ID (QXO-AP3020W) and IC ID (4141B-AP3020W) with an AFC system.

Related Links

Supported Universal Access Points on page 84

## AP4000/AP4000-1 Radios and 6 GHz Support

The AP4000 series access points (APs) are Wi-Fi 6E and Wi-Fi 7 APs with support for multiple Extreme Networks operating systems. The AP4000 series APs include the following models:

- **AP4000** — Indoor AP Wi-Fi 6E
- **AP4000-1** — Indoor AP Wi-Fi 6E
- **AP4020** — Indoor AP Wi-Fi 7
- **AP4020X** — Indoor AP Wi-Fi 7 (external antenna)
- **AP4020FX** — Indoor AP Wi-Fi 7 (external antenna)
- **AP4060** — Indoor/Outdoor AP Wi-Fi 7
- **AP4060X** — Indoor/Outdoor AP Wi-Fi 7 (external antenna)



**Note**
AP4000-1 models do not support IoT.

The AP4000/AP4000-1 access points (APs) offer the following radios:

**Table 28: AP4000/AP4000-1 Radio Modes**

| Radio | Radio Modes |
|---|---|
| Radio 1 | • b/g<br>• g/n<br>• b/g/n<br>• g/n/ax<br>• client-bridge |
| Radio 2 | • a/n/ac<br>• a/n/ac/ax<br>• client-bridge |
| Radio 3 | • 2x2 WLAN Service 6.0 GHz, Or<br>• 2x2 WLAN Tri-Band Sensor, 2.4 GHz, 5.0 GHz, 6.0 GHz |

The AP4020/AP4020X/AP4020FX and AP4060/AP4060X APs offer the following radios:

**Table 29: AP4020/AP4020X/AP4020FX Radio Modes**

| Radio | Radio Modes |
|---|---|
| Radio 1 | • b/g<br>• g/n<br>• b/g/n<br>• g/n/ax<br>• client-bridge |
| Radio 2 | • a/n/ac<br>• a/n/ac/ax<br>• client-bridge |

**Table 29: AP4020/AP4020X/AP4020FX Radio Modes (continued)**

| Radio | Radio Modes |
|---|---|
| Radio 3 | • 2x2 WLAN Service 6.0 GHz, Or<br>• 2x2 WLAN 2.4 GHz, dual 5.0 GHz, 6.0 GHz |
| Radio 4 | • Dedicated sensor mode.<br>• Performs full-time scanning and sensing across all available wireless channels (2.4 GHz, 5 GHz, and 6 GHz).<br>• Does not serve client devices.<br><br>**Note:** Supported on AP4020/AP4020X/AP4020FX and AP4060/AP4060X only. |

AP4000/AP4000-1 APs support the following:

- Out of Band discovery on the 6 GHz band. Access points that provide WLAN service on the 6 GHz band include Reduced Neighbor Report IE in all 2.4 GHz and 5 GHz beacons and probe responses. Out of Band discovery helps clients find 6 GHz SSIDs and channel information that comes from 2.4 GHz and 5 GHz beacons of co-located APs.
- Supports AirDefense Services Platform (ADSP) on 2.4 GHz, 5 GHz, and 6 GHz radios.
- 6E WFA Compliant network authentication methods.

  World-Wide Universal AP 6 GHz radios support only the following Wi-Fi Alliance (WFA) 6E Compliant network authentication methods:
  - OWE (Opportunistic Wireless Encryption) for Open Networks
  - WPA3-Personal
  - WPA3-Enterprise

  AP4000/AP4000-1 APs support downlink (DL) Orthogonal Frequency-Division Multiple Access (OFDMA) multi-user access only.

  AP4020/AP4020X/AP4020FX APs support uplink (UL) and DL OFDMA multi-user access and Multi-Link Operation (MLO). For MLO requirements and configuration, see Settings for Multi-Link Operation on page 388.

  **Note**
  When using 802.11ax radio profiles, only DL is supported.

  ExtremeCloud IQ (New) supports the following AP4020 operating modes:
  - Mode 1: 2.4 GHz / 5 GHz / 6 GHz — Service w/Sensor
  - Mode 2: 2.4 GHz / 5 GHz (Low) / 5GHz (High) — Service w/Sensor

  ExtremeCloud IQ (New) supports the following AP4020FX/AP4060/AP4060X operating modes:
  - Mode 1: 2.4 GHz / 5 GHz / 6 GHz data radios + dedicated sensor radio — All three bands are used for client connectivity, while the fourth radio performs full-time scanning for RF and security threats.

- Mode 2: 2.4 GHz + dual 5 GHz data radios + dedicated sensor radio — Optimized for environments where 6 GHz is restricted or unavailable. Provides enhanced 5 GHz performance and retains full-time sensor functionality.

ExtremeCloud IQ (New) requires that your 6 GHz radio network assignment be WFA 6E compliant. ExtremeCloud IQ (New) rejects network configuration changes that result in 6 GHz radio network assignments that are not compliant. It might be necessary to redefine your networks when configuring the 6 GHz radio on Universal APs.

Related Links

Supported Universal Access Points on page 84

## AP5000 Series Radios and 6 GHz Support

The AP5000 series access points (APs) are Wi-Fi 6E or Wi-Fi 7 APs with support for multiple Extreme Networks operating systems. The AP5000 series APs include the following models:

- AP5010 — Indoor AP Wi-Fi 6E
- AP5020 — Indoor AP Wi-Fi 7
- AP5022 — Indoor AP Wi-Fi 7 (tri-band, internal antenna)
- AP5022FX — Indoor AP Wi-Fi 7 (tri-band, external antenna on 6 GHz)
- AP5022S6D — Indoor AP Wi-Fi 7 (tri-band, sector directional 6 GHz)
- AP5050U — Indoor/Outdoor AP Wi-Fi 6E
- AP5050D — Indoor/Outdoor AP Wi-Fi 6E with selectable narrow and wide angle built in directional antennas.
- AP5060U — Indoor/Outdoor AP Wi-Fi 7
- AP5060D — Indoor/Outdoor AP Wi-Fi 7 with selectable narrow and wide angle built-in directional antennas

**Note**
The AP5022/AP5022FX/AP5022S6D and AP5060 support the same standard wireless and wired configuration options as the AP4020. Configuration is applied using the same device-level and template-level workflows.

The AP5050U/D has an Environment choice of **Indoor** or **Outdoor**, depending on the installation location. Support for 6 GHz (Wi-Fi 6E) radio (Indoor) operation depends on the compliance region. Support for 6 GHz (Wi-Fi 6E) radio (Outdoor) operation is partially supported, depending on availability indicated by the Automatic Frequency Coordination (AFC) server.

**Note**
The AP5050U/D (Outdoor) 6 GHz radio operates 6 GHz in Standard Power mode when set to Outdoor, under AFC server control in the US and Canada pending certification approval. When set to indoor mode, the AP5050U/D only offers service on 2.4 and 5 GHz. LPI 6 GHz is not permitted in weatherized enclosures.

The AP5060U is designed for environments requiring broad, omnidirectional coverage. The AP5060D provides selectable narrow and wide angle built-in directional antennas, making it

ideal for targeted coverage scenarios such as hallways, long corridors, and outdoor point-to-point deployments.

AFC certification:

- For AP5050U/D 6 GHz SP:
  - The AP is connected to a US-based Regional Data Center, which connects to an FCC-approved AFC server.
  - The FCC has approved 6 GHz standard power for the AP5050U/D in the United States. APs provide Standard Power for 6 GHz standard as permitted by AFC coordination in Canada.
- For AP4020/AP5020, Standard Power (AFC-Controlled) is supported in Canada.

The AP5020 is a universal **indoor** access point with a Wi-Fi 7 tri-radio. It is designed for high-density environments where a large number of people access your network such as schools, warehouses, healthcare facilities, and stadiums. You can operate the AP5020 across three bands - 2.4 GHz (2x2:2 or 4x4:4), 5 GHz (2x2:2 or 4x4:4), and 6 GHz (4x4:4).

For AP5020 devices, ExtremeCloud IQ (New) uses GPS-based location information when determining AFC spectrum assignments. When an AP5020 connects, ExtremeCloud IQ (New) automatically sends a GPS query to the device. After the AP reports its GPS coordinates, ExtremeCloud IQ (New) applies the standard AFC filtering criteria to determine whether spectrum can be assigned to the AP.



**Note**
The AP5020 supports operation in either Low Power or Standard Power modes with AFC.

The AP5020 supports uplink (UL) and downlink (DL) Orthogonal Frequency-Division Multiple Access (OFDMA) multi-user access for 802.11be-based radio profiles.



**Note**
When using 802.11ax radio profiles, only DL is supported.

ExtremeCloud IQ (New) supports the following AP5020 operating modes:

- Mode 1: 2.4 GHz / 5 GHz (Full) / 6 GHz — Tri-Radio
- Mode 2: Tri-Radio / 5GHz (Full) / 6 GHz — Full Band with Scan
- Mode 3: 5 GHz (Low) / 5 GHz (High) / 6 GHz — Dual 5 GHz with 6 GHz
- Mode 4: Tri-Radio / 5 GHz (Full) / 2.4 GHz — DBDC
- Mode 5: 5 GHz (Low) / 5 GHz (High) / 2.4 GHz — Dual 5 GHz with 2.4 GHz
- Mode 6: 6 GHz (Low) / 5 GHz (Full) / 6 GHz (High) — Dual 6 GHz with 5 GHz



**Note**
Dual 6 GHz radio placement differs by model. AP5022 and AP5060 use a reversed dual-6 GHz layout compared to AP5020. The AP5022/AP5060 has 6 GHz High (6H) on Wi-Fi 0 and 6 GHz Low (6L) on Wi-Fi 2 (reversed from AP5020). This configuration is identified by the 6H/5/6L operating mode label. Always refer to the operating mode label when interpreting radio assignments.

ExtremeCloud IQ (New) supports the following AP5022 and AP5060U/D operating modes under 802.3bt power:

- Mode 1: 2.4 GHz (4×4) / 5 GHz (4×4) / 6 GHz (4×4) + Tri Radio Scan (2×2)
- Mode 2: 5 GHz-Low (4×4) / 5 GHz-High (4×4) / 6 GHz (4×4) + Tri Radio Scan (2×2)
- Mode 3: 6 GHz-High (4×4) / 5 GHz (4×4) / 6 GHz-Low (4×4) + Tri Radio Scan (2×2)

Fine Timing Measurement (FTM) support is used to find (estimate) the distance between the AP (AP5010/AP5020) and the wireless client. Enabling this setting allows client devices to find their range to the AP. If the site has a Civic Address configured, or if the AP is configured with positional data (latitude/longitude/altitude), the AP advertises this information in the beacon.



**Note**
Enabling FTM (11mc) responder support results in a radio reset.

**Table 30: AP5000 Series Radio Modes**

| Radio | Radio Modes |
|---|---|
| Radio 1:<br>• 4x4 WLAN Service 2.4 GHz<br>• 2x2 WLAN Tri-Band Sensor, 2.4 GHz, 5.0 GHz, 6.0 GHz | • sensor<br>• b/g<br>• g/n<br>• b/g/n<br>• g/n/ax<br>• g/n/ax/be (AP5020 only)<br>• client-bridge<br>• 6H/5/6L (6 GHz High) |
| Radio 2:<br>• WLAN Service 5.0 GHz<br>• 4x4 WLAN Service 5.0 GHz | • a/n/ac<br>• a/n/ac/ax<br>• a/n/ac/ax/be (AP5020 only)<br>• client-bridge<br>• 6H/5/6L (5 GHz) |
| Radio 3:<br>• 4x4 WLAN Service 6.0 GHz<br>• 2x2 WLAN Service 2.4 GHz | • ax6<br>• ax6/be (AP5020 only)<br>• client-bridge<br>• 6H/5/6L (6 GHz Low) |
| Radio 4:<br>• Dedicated sensor mode<br>• Performs full-time scanning and sensing<br>• Operates on 2.4 GHz and 5 GHz<br>• Does not serve client devices<br><br>**Note:** Radio 4 is supported only on AP5020, AP5022/AP5022FX/AP5022S6D, and AP5060 access points and is available with WIPS capabilities. For more information, see Fourth Radio Dedicated Sensor Support on page 93. | |

Related Links

Supported Universal Access Points on page 84

## Fourth Radio Dedicated Sensor Support

Using the fourth radio as a dedicated sensor enables the access point (AP) to perform wireless monitoring without affecting client-serving radios in ExtremeCloud IQ (New).

In addition to wireless monitoring, the dedicated fourth radio is used to support intrusion detection and prevention capabilities. This includes continuous RF analysis, rogue AP detection, and security threat monitoring without impacting client traffic on service radios.

When enabled on supported access points, the fourth radio operates exclusively in sensor mode and does not accept client connections.

This feature is supported only on APs with WIPS capabilities, as listed in Table 31.

**Table 31: WIPS-Supported Access Points**

| AP Model | Wi-Fi | Dedicated Sensor Radio Used |
|---|---|---|
| AP4020 / AP4020X / AP4020FX | Wi-Fi 6E / Wi-Fi 7 | Yes (4th radio) |
| AP4060 / AP4060X | Wi-Fi 6E / Wi-Fi 7 | Yes (4th radio) |
| AP5020 | Wi-Fi 7 | Yes (4th radio) |
| AP5022 | Wi-Fi 7 | Yes (4th radio) |
| AP5060U / AP5060D | Wi-Fi 7 | Yes (4th radio) |
| **Note:** Dedicated sensor radios provide continuous monitoring across supported frequency bands and operate exclusively in sensor mode; they do not serve clients. | | |

**Note**
This feature is available to customers with an Essentials license tier in ExtremeCloud IQ (New). For more information, see the *Extreme Platform ONE Networking and ExtremeCloud IQ Subscription and Licensing Guide*.

Sensing is implemented as shared sensing on the following bands:

- 2.4 GHz
- 5 GHz

For shared sensing, the fourth radio timeshares between sensing operations and client-serving functions on the 2.4 GHz and 5 GHz bands. The radio allocates time for passive channel scanning and monitoring while remaining available to support client connectivity on those bands. This differs from a fully dedicated sensor, where the radio performs continuous scanning and does not serve client devices.

**Note**
Shared sensing on the AP5020, AP5022, and AP5060 is limited to the 2.4 GHz and 5 GHz bands. The fourth radio does not perform sensing on the 6 GHz band, and 6 GHz client operation is unaffected.

On supported APs, the fourth radio is dedicated exclusively to sensing operations. When enabled, this radio runs in sensor mode and passively monitors the wireless environment while the primary radios continue handling client traffic.

Using a dedicated sensor radio allows monitoring functions to run independently of client service, preserving RF efficiency and client performance.

Wireless monitoring and baseline security functions require continuous visibility into the RF environment. When sensing tasks share client radios, they may compete for airtime or reduce overall efficiency.

A dedicated radio sensor improves visibility by:

- Offloading sensing activity to a dedicated radio
- Maintaining consistent monitoring without impacting client traffic
- Eliminating the need for external sensor devices on supported hardware

## Universal AP Boot and Onboarding Process

When an access point (AP) is first powered on out of the box, it initiates a series of actions to establish a connection with the network:

- Boot Up Process: The AP starts up and performs initial checks.
- CAPWAP Connection: The AP serial number is onboarded to ExtremeCloud IQ (New).
- Universal/Worldwide SKU Region and Country Fingerprinting: The AP reports its public IP address to a STUN server, which identifies the country of connection.
- Changing Operating System Personal for Onboarded APs: The AP connects to the network controller, which may involve switching to specific operating modes, like WiNG CCC mode.
- Onboarding to ExtremeCloud IQ (New): The AP is onboarded to the cloud system, where it appears in the user interface and can be managed.

### Boot Up Process

1. **Initial Boot**: The AP powers on and attempts to obtain an IP address and gateway from the DHCP server on the native VLAN. The DHCP process can also specify DNS and NTP addresses.
2. **Time Synchronization**: The AP tries to synchronize its device time using NTP.
   - If an NTP server is assigned using DHCP, the AP connects to that server using UDP port 123.
   - If no NTP server is assigned, the AP connects to the default NTP server using UDP port 123.
3. **DNS Configuration**: The AP may need to use DNS to look up the NTP server hostname.
   - If a DNS server is defined using DHCP, the AP uses that server.
   - If no DNS server is defined, the AP uses its default DNS servers: 208.67.222.222 and 208.67.220.220.



**Note**
Both DNS and NTP are required. If traffic is not allowed to the default NTP and DNS entries, accessible internal DNS and NTP must be defined using DHCP.

## CAPWAP Connection

1. The AP discovers ExtremeCloud IQ (New) through one of four mechanisms, executed in the following sequence:
   - DHCP option 43
   - DNS
   - Local subnet discovery
   - Redirector

   **Note**
   The Redirector is the primary mechanism for ExtremeCloud IQ (New). The AP will use DNS to find the Redirector IP address.

2. The AP automatically discovers and CAPWAP connects to the redirector.

   **Note**
   Outbound UDP 12222 or TCP 80 is required.

   - By default, all CAPWAP connections first attempt to connect using UDP 12222. If unable to connect, the AP attempts to connect using TCP 80 instead.
   - Refer to the firewall guide to identify the IP address ports needed to permit traffic to the Redirector.

3. If the AP serial number is onboarded to ExtremeCloud IQ (New):
   - The Redirector directs the AP to connect to the RDC master CAPWAP server by setting the command `capwap client server name <CAPWAPMASTERHOSTNAME>`.
   - The AP disconnects from the Redirector and CAPWAP to connect to the RDC master CAPWAP server.

     **Note**
     Outbound UDP 12222 or TCP 80 is required.

   - The RDC master CAPWAP server directs the AP to connect to the CAPWAP server designated as the primary management instance for the device by setting the command `capwap client server name <CAPWAPSERVERHOSTNAME>`.

4. If the AP is not onboarded to customer account, it continues to cycle through the AP discovery methods defined above.

**Tip**
**CAPWAP Connection troubleshooting**:

- Ensure the AP can resolve hostnames using DNS.
- Ensure firewall ports are open on UDP 12222 or TCP 80 to the IP addresses defined in the Global Data Center Services and Regional Data Center Services sections of your firewall configuration guide.
- If using TCP 80, CAPWAP connection times will increase.
- To locate the firewall configuration guide specific to your installation, select your Profile (initials), and then select About ExtremeCloud IQ (New) > App Info to find the link to your **Firewall Configuration Guide**.

## Universal/Worldwide SKU Region and Country Fingerprinting

1. ExtremeCloud IQ (New) informs Universal and Worldwide SKU APs to begin the country discovery process that assigns region and country compliance tables.
2. Universal and Worldwide SKU APs are initially configured for the WORLD region, with an ISO Country Code of 998.
3. When a Universal or Worldwide SKU AP is onboarded:
   - The AP contacts stun.extremenetworks.com on outbound UDP 12222.

     **Important**
     The AP must have the correct time to validate the certificate provided by the STUN server.

   - The AP communicates its configured Region and ISO Country Code to the STUN server.
   - The STUN server gathers the AP's reported public IP address, a process known as fingerprinting, and cross-references it with a database to identify the country where the device is connected.
   - If fingerprinting is successful:
     - The STUN server informs the AP of its region and country.
     - The AP reconfigures itself to comply with the appropriate region and country compliance tables.
     - The AP is released to appear connected to ExtremeCloud IQ (New) in the UI.
   - If fingerprinting fails, ExtremeCloud IQ (New) initiates a new region/country fingerprinting attempt every 5 minutes until fingerprinting succeeds.
4. If the AP is not a Universal or Worldwide SKU, fingerprinting is skipped.

**Tip**
**Region and Country Fingerprinting Troubleshooting**:

- The AP must have the correct time (from NTP) to validate the certificate and establish connection to the STUN server.
- Ensure firewall ports are open for outbound UDP 12222 to all of the STUN servers defined in the firewall configuration guide.
- To locate the firewall configuration guide specific to your installation, select your Profile (initials), and then select About ExtremeCloud IQ (New) > App Info to find the link to your **Firewall Configuration Guide**.
- If the previous steps are unsuccessful and your AP is operating on a code version earlier than 10.6.1, use TFTP to sideload IQ Engine 10.6.1 or a later version onto your AP.
- If a newly onboarded Universal or Worldwide AP has already been assigned to the FCC (US) or Canada regions, the fingerprinting process cannot change to a different country. Please contact GTAC for options.

## Changing Operating System Persona for Onboarded APs

From the factory, Universal APs are configured for management by ExtremeCloud IQ (New) and always engage with ExtremeCloud IQ (New) for onboarding. You have the option to deploy your

devices locally — on-premise from an ExtremeCloud IQ Controller (or a WiNG controller) — or to deploy your devices from ExtremeCloud IQ (New).

From ExtremeCloud IQ (New), onboard and register the Universal AP.

If local network configuration (DHCP or DNS) is not available to assist the AP to find ExtremeCloud IQ Controller, Enhanced Discovery from ExtremeCloud IQ (New) is supported. The AP takes the IP address or FQDN of ExtremeCloud IQ Controller. For more information, see Enhanced Discovery on page 138.

If locally onboarded, ExtremeCloud IQ (New) issues a command to the AP to switch to the WiNG operating system and then issues a delayed reboot command:

- For most Universal APs:
  - The AP boots into WiNG in discovery mode.
  - The AP searches for the controller's DHCP or DNS address, or performs local discovery within the subnet.
  - Depending on the controller instance's configuration, the device reboots into either Campus mode or WiNG Distributed mode and then connects to the controller instance.
- WiNG Distributed mode is not supported on AP4000 devices. These devices boot directly into WiNG Campus mode for use with ExtremeCloud IQ Controller.
- For AP3000/AP4020/AP5020 devices, administrators can set up two controller URLs in ExtremeCloud IQ (New) during onboarding. Once the device switches to WiNG, the device contacts ExtremeCloud IQ to retrieve the controller address assignments.



**Tip**
**Troubleshooting connectivity to ExtremeCloud IQ Controller after switching OS**:

- The AP must complete a region and country check before OS conversion. If the AP reports Region as World with Country as 998, offboard the AP and re-onboard it to retrigger the region check.
- If the AP region and country does not match your Site region and country defined in ExtremeCloud IQ Controller, the AP may not be able to onboard. Place the AP in the site with the correct region and country defined on the AP.

## Onboarding to ExtremeCloud IQ (New)

If onboarded to ExtremeCloud IQ (New) (and assigned a location and network policy), the AP begins a firmware upgrade and config push process.



**Note**
Outbound TCP 443 and either outbound UDP 12222 or TCP 80 are required, as defined in the Firewall Configuration Guide. To locate the firewall configuration guide specific to your installation, select your Profile (initials), and then select About ExtremeCloud IQ (New) > App Info to find the link to your **Firewall Configuration Guide**.

1. If the AP is running .0 code (factory code), the AP automatically upgrades to the firmware revision defined in the model-specific device template. If no device template for the given

model is configured, the AP automatically upgrades to the latest available version for that model.

2. If the AP is running non-.0 code, the AP automatically upgrades to the firmware revision defined in the model-specific device template. If no template is defined for that model, the AP will not upgrade.
3. After firmware upgrade, but prior to a device reboot, a complete configuration push writes the network policy settings to the AP in a startup configuration file.



**Note**
Outbound TCP 443 is required.

4. When the firmware upgrade and configuration push are complete, the AP reboots and uses the new startup configuration file.
5. The AP comes back online after the reboot and re-establishes a connection to its CAPWAP server on either outbound UDP 12222 or TCP 80.



**Note**
Outbound TCP 443 is required for ongoing statistics reporting and other file transfer activities (for example, firmware management).

6. If the AP cannot connect to its defined CAPWAP server after configuration and reboot within a 15-minute window, the AP rolls back to the previous configuration and reboots again. This resets the configuration to the previous state.



**Tip**
**Troubleshooting**:

- If AP is unable to connect to your account:
  - Ensure the correct device serial number is entered into ExtremeCloud IQ (New).
  - Ensure UDP 12222 or TCP 80 firewall ports are open to all IP addresses defined in the **Regional Data Center Services** section of the firewall configuration guide.
  - Ensure the AP completes Country and Region Fingerprinting steps defined in Universal/Worldwide SKU Region and Country Fingerprinting on page 96.
- If the AP is unable to complete a firmware upgrade or complete configuration, ensure port TCP 443 in open outbound for all the IP ranges defined in the **Regional Data Center Services** section of the firewall configuration guide.
- After the configuration push and reboot, if the AP stays unconnected for 15 minutes and rolls back to the default configuration, check to ensure the IP address, native VLAN, and management VLAN settings are correct for your network. Use VLAN probe to test whether native and management VLAN are available with DHCP services to your AP. For more information, see VLAN Probe on page 143.

# AFC Overview

Automatic Frequency Coordination (AFC) is a system that enables unlicensed Wi-Fi users to operate in the same frequency spectrum as licensed users, specifically in the 5.925–6.425 GHz (U-NII-5) and 6.525–6.875 GHz (U-NII-7) frequency spans.

In ExtremeCloud IQ (New), access points (APs) that support 6 GHz Standard Power (SP) operation and require AFC authorization are displayed in the **Monitoring** > **Network Devices** > **Device Status** > **AFC Wireless** tab. This tab provides a centralized view of APs whose 6 GHz operation depends on spectrum approval from an external AFC service. Only eligible APs configured for SP operation appear in this view, as their channel and power usage must be coordinated with licensed incumbents to ensure regulatory compliance. For more information, see AFC Wireless View on page 116.

Approved AFC cloud-based operators have access to a regulator's database which stores geolocation coordinates and associated power levels of licensed users operating in the 6 GHz spectrum.

The AFC server responds to requests made by ExtremeCloud IQ (New) on behalf of eligible ExtremeCloud IQ (New) APs for access to 6 GHz Standard Power spectrum based on the geo-location coordinates of the APs. The AFC server responds by querying its database to verify whether there is an existing licensed 6 GHz service in that geo-location. If there is no conflict with licensed users in the AP's geo-location, the AFC server sends a response to ExtremeCloud IQ (New) specifying over which channels and at which power levels the AP can operate.

ExtremeCloud IQ (New) Smart-RF automatically selects the AP 6 GHz radio channel and power level after the AFC server allocates 6 GHz Standard Power spectrum.

Here are some key points about AFC:

- Increased Range and Performance: AFC deployments enable increased range and performance for indoor Access Points (APs) by allowing them to operate in the 6 GHz band up to the same power limits that APs are allowed to use in non-DFS 5 GHz channels.
- Outdoor APs: AFC deployment enables outdoor APs to operate in the 6 GHz U-NII-5 & U-NII-7 bands in countries where regulatory bodies allow the use of 6 GHz for Wi-Fi, such as the United States.

ExtremeCloud IQ (New) supports AFC with the AP5050, AP5020, AP5022, and AP5060U/D. The AP5050 supports 6 GHz Standard Power based on geo-location coordinates provided by an integral GPS module. For APs that do not have an integral GPS module, ExtremeCloud IQ (New) offers AFC with Geo-Location Agent support. The AP5020, AP5022, and AP5060U/D support 6 GHz Standard Power based on geo-location coordinates assigned by the Geo-Location Agent.

The AP5050, with its integral GPS module, does not require additional configuration, but it does require a GPS signal. The AP5020 with the Geo-Location Agent support does require a configuration update before the assigned AP can receive the geo-location from the Geo-Location Agent.

For AP5020 devices, ExtremeCloud IQ (New) uses GPS-based location information when determining AFC spectrum assignments. When an AP5020 connects, ExtremeCloud IQ (New)

automatically sends a GPS query to the device. After the AP reports its GPS coordinates, ExtremeCloud IQ (New) applies the standard AFC filtering criteria to determine whether spectrum can be assigned to the AP.

**Table 32: AFC Terminology Definitions**

| Term | Definition |
|---|---|
| LPI | 6 GHz Radio Low Power Indoor. |
| Standard Power (SP) | 6 GHz Radio Standard Power Indoor or Outdoor, which matches the 5 GHz Power level. |
| 6 GHz Power Mode | The AP5020 6 GHz radio can be configured to LPI or SP/LPI. The SP spectrum is based on the geo-location. The SP/LPI option is standard power with a fallback option to low power. If the agent can not determine the allowable SP spectrum for the area, or if the SP spectrum is not allowed in the area, the AP5020 6GHz radio will revert to LPI, and the AP5050 6GHz radio reverts to zero power. If one or more radios are configured to SP, the AP consumes an AFC AP-license. |
| 6 GHz Power Level | The 6 GHz radios configured to SP operate with SP power level only if the AP is assigned the AFC spectrum based on the AP geo-location coordinates. If the AP5020 is not assigned the AFC spectrum, it can be configured to operate with LPI power level. If the AP5050 is not assigned an AFC spectrum, it reverts to zero power. |

Related Links

Indoor/Outdoor AFC Support on page 100
Anchor and Non-Anchor APs on page 102
6 GHz Radio Power AFC on page 103
6 GHz Radio — Standard Power Operation without AFC Approval on page 104
GeoLocation Agent on page 105
GeoLocation Coordinates on page 106
AP Placement for AFC on page 108

## Indoor/Outdoor AFC Support

With the introduction of Wi-Fi 6E and Wi-Fi 7, wireless networks can now operate in the 6 GHz frequency band, offering greater capacity, reduced interference, and improved performance. To ensure safe and compliant use of this spectrum, regulatory bodies such as the FCC require the use of Automated Frequency Coordination (AFC) for standard power operation.

AFC enables access points to dynamically request and receive permission to operate on specific 6 GHz frequencies based on their physical location, ensuring they do not interfere with licensed incumbent users.

The following sections provide an overview of AFC for both indoor and outdoor environments:

- Indoor AFC: AFC requirements for indoor access points, including supported models, key features, and configuration requirements.

- Outdoor AFC: AFC requirements for outdoor access points, including supported models, key features, and configuration requirements.

*Indoor AFC*

Indoor AFC enables ExtremeCloud IQ (New) access points to operate at standard power levels in the 6 GHz band, beyond the limitations of Low Power Indoor (LPI) mode. This allows for greater coverage and improved performance in enterprise environments while maintaining compliance with regulatory requirements.

ExtremeCloud IQ (New) supports the following indoor AFC devices:

- AP3020W
- AP4020/AP4020X/AP4020FX
- AP4060/AP4060X
- AP5020
- AP5022
- AP5060U/D
- AP5050U/D

Key features include:

- **Standard Power Operation**: Enables higher transmit power for improved range and throughput.
- **Geolocation-Based Coordination**: Indoor APs must use Geolocation and elevation data, even when a civic address is provided.
- **Dynamic Frequency Assignment**: Frequencies are assigned based on location and environmental factors to avoid interference with licensed incumbents.
- **Cloud-Managed AFC**: Configuration and AFC registration are managed through ExtremeCloud IQ (New).

Configuration requirements:

- Ensure the AP is installed in a fixed indoor location.
- Provide accurate location data (civic address or GPS).
- Enable AFC in the device configuration settings.
- Verify that the AP is connected to the internet to communicate with the AFC system.

*Outdoor AFC*

Outdoor AFC is mandatory for all standard power 6 GHz outdoor access points. It ensures that ExtremeCloud IQ (New) outdoor APs operate safely and legally by coordinating spectrum use with licensed incumbents in the 6 GHz band.

ExtremeCloud IQ (New) supports the following outdoor AFC devices:

- AP4060/AP4060X
- AP5050U/AP5050D

Key features include:

- **Mandatory AFC Use**: Outdoor APs must use AFC to operate in the 6 GHz band.
- **GPS-Based Location Services**: Outdoor APs are equipped with GPS modules or require manual input of precise coordinates.
- **Real-Time Frequency Coordination**: Outdoor APs query certified AFC databases to receive approved frequency and power settings.
- **Environmental Awareness**: AFC considers terrain, nearby structures, and incumbent systems when assigning channels. AFC also considers AP antenna coverage patterns; antenna changes can affect AFC calculations and channel allocation.
- **Radio Frequency (RF) Coverage Pattern**: AFC uses more than just geolocation, elevation, civic address, and device model to determine frequency and power levels. It also relies on the RF coverage pattern, which includes the antenna system characteristics. Providing accurate and complete information is critical. Any modification to the antenna—such as adding or replacing it—changes the coverage shape and size. This can result in the device operating outside the AFC-approved parameters, leading to regulatory non-compliance and potential interference.



**Important**
If any of the parameters used by the AFC system to determine available frequencies or power levels change, the access point must obtain a new or updated authorization from the AFC system prior to operating.

Configuration requirements:

- Install the AP in a fixed outdoor location with a clear view of the sky (for GPS).
- Ensure GPS is enabled and functioning, or manually input accurate coordinates.
- Enable AFC in the device configuration.
- Maintain a stable internet connection for ongoing AFC communication.

Related Links

AFC Overview on page 99

## Anchor and Non-Anchor APs

All 6 GHz Standard Power AFC with Geo-Location Agent Support deployments require anchor and non-anchor APs.

**Anchor APs**

An integral GPS module supplies geo-location coordinates to anchor APs. The AP5050D/U is currently the only supported anchor AP.

The 6GHz SP APs with integral GPS module bring up SP spectrum based on geo coordinates derived from one of the following sources, according to the listed priority:

1. Geo coordinates derived by the Geo-Location Agent.
2. Geo coordinates provided by the integral AP GPS module.

If an anchor AP is unable to derive geo coordinates from the Geo-Location Agent, the AP uses coordinates from its integral GPS module. This ensures a high degree of certainty

that the anchor AP does not have sufficient connectivity to complete a subgraph before it switches to using coordinates from its GPS module. This is optimal in cases where many APs in a subgraph lock on to the anchor AP GPS coordinates, and there is a subset of APs that must derive coordinates from the Geo-Location Agent.

**Non-Anchor APs**

The Geo-Location Agent running on ExtremeCloud IQ (New) assigns geo-location coordinates to all APs under its control.

- The AP4020, AP5020, AP5022, and AP5060U/D are non-anchor APs that support SP and require an anchor for AFC Geo-Location Agent support (because they do not include their own GPS module).
- The AP5050 has an integral GPS module, supports SP, and can be used as an anchor or a non-anchor AP depending on your deployment needs.
- The AP5010 and AP3000 can be configured to support FTM AP-to-AP ranging and participate as non-anchor APs in providing higher geo-location density for the construction and extension of AFC subgraphs. These APs do not support SP and are not required for AFC.

Related Links

AFC Overview on page 99

## 6 GHz Radio Power AFC

When the 6 GHz SP Spectrum cannot be obtained from the AFC server, the AP behavior depends on the AP model and its configuration.

**AP3020W**

You can configure the AP3020W to fall back to LPI if obtaining the SP Spectrum channel plan from the AFC server fails.

- Low Power Indoor (Default):

  In low power indoor (LPI) mode, 6 GHz radios use a predefined compliance table and the AP does not require AFC spectrum. The AP goes into service immediately after it boots. LPI operates over U-NII 5, 6, 7, and 8. A radio that is configured with LPI mode is not an AFC AP, and does not appear on the AFC tab.

- Standard Power (with fallback to LPI):

  In standard power (SP) mode, AP3020W 6 GHz radios can operate at SP or LPI. The SP power level depends on geo-location coordinates of the AP and on receiving AFC spectrum from the AFC server. If AFC spectrum is not available, the radio falls back to the LPI power level. In SP mode the channel list is limited to U-NII 5, and 7 (in the US). Once ExtremeCloud IQ (New) determines the geo-location for the AP and receives AFC spectrum from the server, the 6 GHz radio transitions to the SP power level. If the AFC spectrum cannot be renewed, the 6 GHz radio falls back to the LPI power level.

  The list of supported channels in LPI fallback mode is limited to the channels supported by SP mode. This way, the AP does not have to change channels when switching between SP and LPI modes.

**AP4020/AP5020/AP5022/AP5060U/AP5060D**

You can configure the AP4020, AP5020, AP5022, and AP5060U/D to fall back to LPI if obtaining the SP Spectrum channel plan from the AFC server fails.

- **Low Power Indoor (Default)**

  In low power indoor (LPI) mode, 6 GHz radios use a predefined compliance table and the AP does not require AFC spectrum. The AP goes into service immediately after it boots. LPI operates over U-NII 5,6,7, and 8. A radio that is configured with LPI mode is not an AFC AP, and does not appear on the **AFC** tab.

- **Standard Power (with fallback to LPI)**

  In standard power (SP) mode, AP4020/AP5020 6 GHz radios can operate at SP or LPI. The SP power level depends on geo-location coordinates of the AP and on receiving AFC spectrum from the AFC server. If AFC spectrum is not available, the radio falls back to the LPI power level. In SP mode the channel list is limited to U-NII 5, and 7 (in the US). As soon as ExtremeCloud IQ (New) determines the geo-location for the AP and receives AFC spectrum from the server, the 6 GHz radio transitions to the SP power level. If the AFC spectrum cannot be renewed, the 6 GHz radio falls back to the LPI power level.

  The list of supported channels in LPI fallback mode is limited to the channels supported by SP mode. This way, the AP will not have to change channels when switching between SP and LPI modes.

**AP5050**

The AP5050 tries first to derive geo-location coordinates from the AFC indoor group of APs in order to query the AFC server in the 6 GHz spectrum. If it is unable to derive coordinates, the AP5050 uses its integral GPS coordinates to present to the AFC server. After the AFC server responds by allocating SP spectrum, Smart-RF automatically selects the channel and power level and the AP5050 starts the 6 GHz radio in SP mode.

Related Links

AFC Overview on page 99

## 6 GHz Radio — Standard Power Operation without AFC Approval

When a 6 GHz radio is configured for Standard Power (SP) operation but does not receive mandatory power and channel confirmation from the Automated Frequency Coordination (AFC) server, ExtremeCloud IQ (New) automatically implements fallback behavior to maintain service availability while ensuring regulatory compliance. This behavior applies to all APs that support both (SP) and Lower Power Indoor (LPI) operation.



**Note**
The AP4020FX is an SP-only device and does not support LPI fallback. If AFC confirmation is unavailable, the AP4020FX cannot operate and will remain offline until AFC approval is restored.

If the SP-configured 6 GHz radio does not receive AFC approval, the following actions occurs:

- **Automatic Fallback to LPI Mode**: The radio automatically transitions from SP to LPI mode to maintain operational capability until AFC confirmation is received.

- **Channel Selection in LPI Mode**: While operating in LPI mode, the radio attempts to select a channel that was previously available in SP mode, preserving service continuity on familiar spectrum when possible.
- **Automatic Return to SP Mode**: The radio continuously monitors for AFC responses. Once a positive response is received (including permitted power levels and channel assignment), the radio automatically returns to SP mode.

If AFC spectrum approval expires while the radio is operating in SP mode:

- The radio transitions immediately to LPI mode.
- The AP attempts to select LPI-permitted channels that were previously available in SP mode.
- The system generates alarms and event notifications to notify administrators of operational changes related to AFC status. For more information, see Table 33.

**Table 33: AFC-Related Radio State Change Event Notifications**

| Event | Description | Trigger Condition |
|---|---|---|
| AFC Approval Failure – LPI Fallback | Radio transitioned from SP to LPI mode due to lack of AFC confirmation. | AFC server does not provide required power and channel approval. |
| AFC Approval Received – SP Restored | Radio returned to SP mode following a successful AFC response. | AFC server provides positive response with power and channel information. |

**Note**

- The fallback to LPI mode ensures continuous wireless service whenever AFC approval is unavailable.
- Radios automatically return to SP mode once AFC confirmation resumes—no manual action required.
- Channel availability in LPI mode may differ from SP mode due to regulatory restrictions.

Related Links

AFC Overview on page 99

## GeoLocation Agent

The GeoLocation Agent within ExtremeCloud IQ (New) provides geo-location coordinates for AP consumption. The AP5020 uses the geo-location coordinates to query the AFC server in the 6 GHz spectrum.

The following steps outline how the Geo-Location Agent derives the AP coordinates:

1. The APs use 802.11mc Fine Time Measurement (FTM) technology to determine the distance between two APs, referred to as AP-to-AP ranging. The GeoLocation Agent collects the

ranging results and builds one or more graphs (subgraphs) of APs on the floor. The graph borders are the estimated distances between the APs.

**Note**
The AP3000/AP3020W/AP4020/AP5010/AP5020/AP5022/AP5050/AP5060U/AP5060D participate in building out AFC subgraphs on floor plans by performing FTM AP-to-AP ranging and deriving their geo-location coordinates from the Geo-Location Agent.

2. Anchor APs are access points equipped with GPS modules. The GeoLocation Agent collects the GPS coordinates of the anchor APs and combines them with the FTM graph to derive the geo-location coordinates. For an AP to be part of the graph, it has to have an equivalent range of at least three other APs. Anchor and non-anchor APs must be placed on the graph. A minimum of four anchor APs must provide GeoLocation coordinates in order to place the graph on the geographic map from which the geo-location coordinates of each AP can be derived.

**Tip**
To lock on GPS signals, install anchor APs close to the building perimeter or outdoors. The indoor anchor AP location must be chosen based on the GPS signal availability. Building properties determine the degree of shielding of the GPS signal. It is recommended to survey the GPS signal with a smart phone application such as GNSSLogger to determine the best anchor AP position.

Related Links

AFC Overview on page 99

## GeoLocation Coordinates

The GeoLocation Agent builds one or more AP graphs (subgraphs) for each floor plan to which APs are assigned, based on the FTM AP-to-AP ranging results. The graph boundaries are created from the measured distance between the APs, using the 802.11mc protocol. Where the AP graph is located on the map depends on the GeoLocation reported by the anchor APs.

**Note**
For APs that are eligible for use in an AFC indoor configuration (AP3000/AP4020/AP4060/AP5010/AP5020/AP5022/AP5050/AP5060U/AP5060D), do not use the 5 GHz radio for MESH connection, since this radio is reserved for performing FTM AP-to-AP ranging.

The following conditions must be met before the GeoLocation Agent can derive coordinates for APs on the floor:

- **AP graph connectivity**: Each AP on the floor must be able to determine the FTM distance to a minimum of three neighboring APs.

  If the AP graph connectivity requirement is not met for all the APs on the floor, the GeoLocation Agent creates several subgraphs. Each subgraph includes a subgroup of APs.
- **Number of anchor APs**: The AP graph must be connected to a minimum of four anchor APs, with multiple subgraphs per floor supported.

The APs belonging to subgraphs might have geo-location coordinates assigned. See the following scenarios and recommendations for corrective actions.

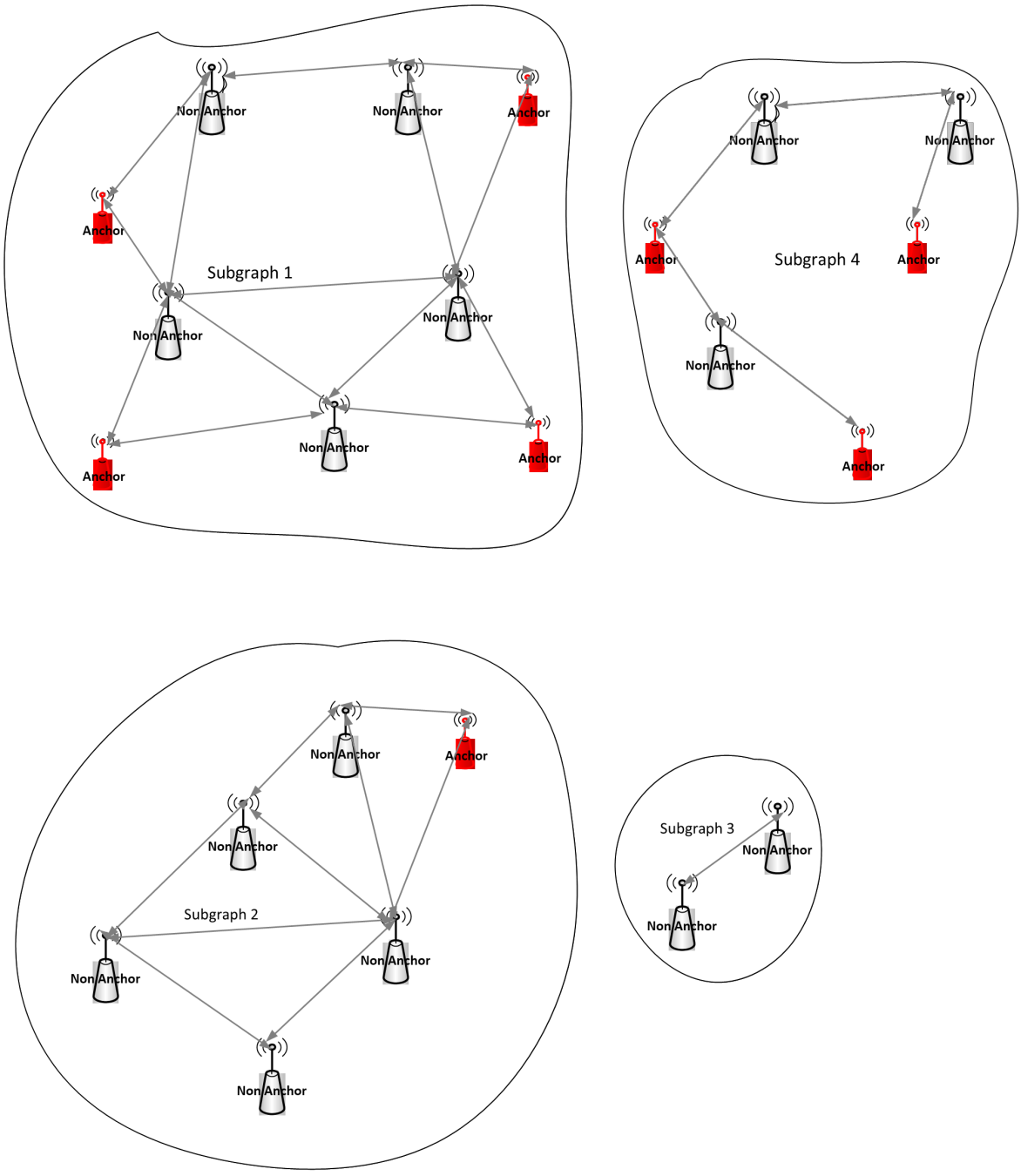



**Figure 3: Example Subgraph Scenarios**

**Subgraph 1**

The group of APs belonging to Subgraph 1 satisfy the AP graph connectivity and the number of anchor AP requirements. As a result, the geolocation agent derived coordinates for each of them.

No corrective action required.

**Subgraph 2**

The group of APs belonging to Subgraph 2 satisfy the AP graph connectivity rules, but not the number of anchor AP requirements. As a result, the geolocation agent did not derive coordinates for these APs.

**Corrective action**: Install more APs between Subgraph 1 and Subgraph 2 to add more connections between the subgraphs and merge them.

**Subgraph 3**

When the AP graph connectivity rule is not met, but the number of anchor APs requirement is met, geolocation coordinates are not derived.

**Corrective action**: Reposition the APs, or install more APs, to achieve connectivity with the rest of the APs on the floor.

**Subgraph 4**

When neither requirement is met, geo-location coordinates are not derived. Take the following corrective actions:

**Corrective action**: Reposition the APs or install more APs to achieve connectivity with the rest of the APs on the floor.

Related Links

AFC Overview on page 99

## AP Placement for AFC

Consider the following when selecting a location:

- Install Anchor APs where they can receive a GPS signal. The anchor AP needs a minimum 11mc FTM range to non-anchor APs. Before installing anchor APs outdoors make sure the outer wall of the building is penetrable by Wi-Fi signals used for ranging.
- To ensure GPS signal reception, place a minimum of four anchor APs on each floor, strategically located near windows, on each side of the floor. Four, or more, anchor APs provide good location accuracy.

- To provide FTM AP-to-AP ranging connectivity, create a grid of anchor APs placed less than 20m apart to cover the interior floor area.
- Typical existing Indoor AP deployments for Wi-Fi Service on 5 GHz have the required AP density to satisfy the ranging requirements. In cases where the requirements are not satisfied, add more APs.

**Note**
A best practice is to conduct a GPS survey to determine a location with adequate GPS reception. For more information, see Conduct a GPS Survey with a Smart Phone for AFC on page 109.

*Anchor AP Requirements*

Indoor 6 GHz SP deployments depend on the availability of the geo location coordinates of the anchor APs provided by GPS signal. Every deployment will have to be evaluated for indoor GPS signal reception before final commitment. The AP5050 is the supported anchor AP.

Anchor AP placement must meet the following requirements:

- GPS signal reception is sufficient for the AP GPS module to lock.
- Minimum of four anchor APs per floor.
- The AP5050 with Integral GPS module anchor APs can be mounted outdoors, provided that Wi-Fi FTM 11mc AP-to-AP ranging with three or more indoor APs is possible.

**Important**
Before final commitment and installation, evaluate your deployment for indoor GPS signal reception. For more information, see Conduct a GPS Survey with a Smart Phone for AFC on page 109.

*Non-Anchor AP Requirements*

Place non-anchor APs in the range of at least three other anchor or non-anchor APs. The range of each AP must be able to reach a minimum of three other APs on the same floor. The AP3000, AP4020, AP4060, AP5010, AP5020, AP5022, AP5050, and AP5060U/D can be used as a non-anchor AP.

Related Links

AFC Overview on page 99

*Conduct a GPS Survey with a Smart Phone for AFC*

The cell phone must be running an application that can report GPS-only derived geo-locations. The following are possible applications:

- GPS Status
- GnssLoger

Anchor APs must have sufficient exposure to GPS signals. To evaluate the feasibility of potential installation locations for anchor APs, conduct a GPS survey.

Use this task to conduct a GPS survey.

1. Position the phone at the proposed AP placement area and wait up to 30 minutes for GPS lock.

   If the phone does not report a GPS coordinate, the location has poor GPS signal and is not recommended for an anchor AP.
2. Repeat Step 1 for each anchor AP.

Related Links

AP Placement for AFC on page 108

# Adding Controllers and Appliances for Locally Managed Devices

You can add controllers and appliances to monitor their locally managed devices from Extreme Platform ONE Networking. The locally-managed devices also display in the Extreme Platform ONE **Network Devices** list.

**Important**
You cannot use Extreme Platform ONE Networking to adjust the device configuration for locally managed devices. Device support for locally managed devices is limited to monitoring only.

## Supported Management Options

Extreme Platform ONE Networking supports adding the following local management options to monitor their local devices:

**ExtremeCloud IQ Controller**

An on-premises management platform. It is represented in Extreme Platform ONE Networking by the controller model number. For more information, see the ExtremeCloud IQ Controller documentation.

**ExtremeCloud Site Engine**

An on-premises management appliance. It is represented in Extreme Platform ONE Networking as **XIQ-SE**. Use GUI (OneView) from ExtremeCloud Site Engine to connect the appliance to Extreme Platform ONE. You do not add the device from the **Add Devices** option in Extreme Platform ONE. For more information about ExtremeCloud Site Engine Connected mode, see Logging into ExtremeCloud IQ Site Engine. For the full documentation set, refer to ExtremeCloud IQ - Site Engine documentation.

An on-premises appliance cluster or stand-alone appliance designed to host ExtremeCloud Edge self-managed orchestration and container-based applications. It provides an on-premises framework for running distributed edge services, such as tunnel concentrators and local network controllers. It is represented in Extreme Platform ONE Networking as **APPLIANCE CLUSTER**. For more information, see the Universal Compute Platform documentation.

A centralized software appliance that terminates thousands of GRE or IPSec tunnels from remote wireless access points, simplifying branch network management and

improving resilience. It is represented in Extreme Platform ONE Networking as **TUNNEL CONCENTRATOR**. For more information, see Extreme Tunnel Concentrator documentation.

### The Appliances Tab

After the appliance, controller, or tunnel concentrator is added to Extreme Platform ONE Networking, it is displayed on the **Appliances** tab.

- Go to **Monitor** > **Network Devices** > **Device Status** > **Appliances**.
- Go to **Subscription & Services** > **Inventory** > **Appliances**.

Related Links

Network Devices | Add Devices on page 129
Device 360 View on page 204

## Universal Compute Platform Support

ExtremeCloud IQ (New) supports onboarding of the Universal Compute Platform (UCP). The UCP serves as a service platform for an on-premises application offering. UCP provides a performance-validated hosting platform that supports advanced orchestration of a catalog of applications. It provides a container-based orchestration framework in an Extreme Networks qualified and validated high-performance hardware configuration. The framework natively supports clustering, a distributed file system, and orchestration through Kubernetes, providing a highly resilient application operational base.

UCP appliances support the following deployment configurations:

- Standalone — A single node that operates as an independent appliance.
- Appliance Cluster — Multiple nodes configured in a multi-node cluster for redundancy and scalability.

ExtremeCloud IQ (New) supports UCP management through the UCP Device 360 view. The UCP Device 360 view provides Device Health information, Events, and Alerts for each UCP appliance, giving you visibility into appliance performance and operational status without leaving ExtremeCloud IQ (New).

Go to **Monitor** > **Network Devices** > **Device Status** > **Appliances** and select a UCP device name from the table to open the UCP Device 360 view. For more information, see Universal Compute Platform Device 360 View on page 228.

For more information about UCP, see the Universal Compute Platform documentation.

### Supported Applications

Each UCP device supports one installed application at a time. The following applications can be installed on a UCP device:

- ExtremeCloud IQ Controller
- Extreme Tunnel Concentrator

The **Application** column on the **Appliances** tab identifies the application hosted on each UCP device. To add the **Application** column to the **Appliances** tab view, go to **Monitor** > **Network Devices** > **Device Status** > **Appliances**, select Columns, and then under **Additional Columns**, select **Application**. For more information, see Appliances View on page 118.

### Device Health

ExtremeCloud IQ (New) provides **Device Health** information for each UCP appliance on the **Overview** tab of the UCP Device 360 view. By default, the data time frame for **Device Health** widgets is 24 hours. To customize the time period, select a Date & Time Range in the graph controls. For more information, see Universal Compute Platform Device 360 View on page 228.

### Interactive Console Access

ExtremeCloud IQ (New) provides an interactive console pane for each application installed on a UCP device in Running state. The console session opens in a dedicated interactive pane, providing CLI access to the appliance. Communications tunnel through Inlets over the existing management connection. For more information, see Open the UCP Console on page 241.

## Extreme Tunnel Concentrator Support

configures point-to-point tunneling between wireless access points and the Tunnel Concentrator application, which runs on the . Tunnel Concentrator serves as the tunnel termination point and forwards received traffic to the data center, where the traffic can be aggregated. To provision tunneling, administrators use their chosen management application to configure tunneling settings for a given VLAN, then they map the VLAN across the WLAN network.

ExtremeCloud IQ (New) supports Tunnel Concentrator management through the Tunnel Concentrator Device 360 view. The Tunnel Concentrator Device 360 view provides appliance-level device details, a topology overview, and tunnel MTU status for each Tunnel Concentrator appliance. Tunnel Concentrator appliances are represented in ExtremeCloud IQ (New) as TUNNEL CONCENTRATOR.

Go to **Monitor** > **Network Devices** > **Device Status** > **Appliances** and select a Tunnel Concentrator device name from the table to open the Tunnel Concentrator Device 360 view. For more information, see Tunnel Concentrator Device 360 View on page 225.

## Network Devices | Device Status

Go to **Monitoring** > **Network Devices** > **Device Status** to manage your network devices. The following information is provided on the Device Status window:

- **Device Status Indicators**: Under the **Status** column in the device list, icons appear that are designed to provide useful device status information. Multiple status icons can be associated with a device. Hover over any icon to view a label indicating what the icon

represents. For a description of each icon that can appear in the device list, see Device Status Icons.

- Device List Views: Select a view option to filter the list of devices. Device list views allow you to filter the device table by interface type, making it easier to focus on the devices relevant to your task:
  - **All**: Displays all devices.
  - Wired: Displays wired devices managed by ExtremeCloud IQ (New).
  - Wireless: Displays wireless access points and associated devices.
  - AFC Wireless: Displays wireless devices operating in Automated Frequency Coordination (AFC) mode.
  - Appliances: Displays ExtremeCloud Site Engine devices, ExtremeCloud IQ Controller, and Tunnel Concentrator.
  - Discovered: Displays devices managed through ExtremeCloud Site Engine.
- **Packet Capture Results**: After one or more packet capture sessions have completed, you can view the available results and download capture files. For more information, see Packet Capture on page 155.
- To download the table data as a CSV file, select .
- **Device Actions**: Select  at the end of a row in the device list to perform actions on a device. For more information about the available actions, see Device 3-Dot Menu Actions on page 134.

  **Note**
  To perform actions on multiple devices, select more than one device, and then select **Actions** from the toolbar at the top of the page.

- To refine the device list:
  - Select and drag the left or right border of the column header to adjust the column width.
  - Select and drag the column headers to change the order of the columns.

    **Note**
    Once columns are reordered, the layout is saved and persistent until it is manually changed.

  - Select a column header to sort column data in ascending or descending order.
  - Select **Columns** to add, remove, and reorder the columns.
  - To refine the list, select **Filter**. The filter sidebar lets you customize what information is displayed in the device list. Available filters vary depending on the window you are in. The **Status** filter lets you select one or more device status icons to display only devices that have those status conditions. For more information, see Filter the Device List by Status on page 125. To see all available options, in the filter area, select a section heading to see more or less items. To clear all active filters, select **Clear all filters** above the **Filters** panel.

## Device List Views

The device list displays in tabular format, with device provisioning details arranged under various columns.

Select **Columns** to add, remove, and reorder the columns. The columns that appear in the device list by default depends on which of the following views is selected:

- All: Select **All** to filter a list of all devices.
- Wired: Select **Wired** to filter a list of wired devices. This view provides an overview of your physical network connections. Use this view to verify connectivity, identify performance bottlenecks, and troubleshoot issues affecting wired infrastructure.
- Wireless: Select **Wireless** to filter a list of wireless devices. This view provides insight into standard wireless connections. Use this view to help optimize wireless coverage, manage network load, and resolve connectivity issues.
- AFC Wireless: Select **AFC Wireless** to filter a list of AFC wireless devices. This view provides real-time insights into the status and performance of AFC wireless connections across the network. Use this view to monitor AFC compliance, troubleshoot connectivity issues, and ensure optimal wireless spectrum usage.
- Appliances: Select **Appliances** to filter a list of network appliances, includingExtremeCloud Site Engine (XIQ-SE) appliances, cloud onboarded controllers, and devices managed by XIQ-SE. This view provides operational status and connectivity information for appliance-type devices in your network. Use this view to monitor appliance health, manage device status, and access native management interfaces for the appliances in your environment.
- Discovered: Select **Discovered** to filter a list of devices that are natively connected to the cloud. These devices are discovered through ExtremeCloud Site Engine. This view provides basic operational insight for devices with limited telemetry support, allowing you to quickly assess overall device presence and connectivity. Use this view to monitor mixed-vendor environments, verify operational status, and support networks transitioning toward cloud-managed deployments.

Related Links

Network Devices | Device Status on page 112

*All View*

The **ALL** view provides a list of all devices.

Go to **Monitoring** > **Network Devices** > **Device Status** > **All Devices** to display the following information:

- Status
- Device *
- Management IP
- Serial Number
- Location
- Model
- Firmware
- Uptime
- Network Policy *
- State
- Clients **
- Cloud Config Group **
- Network Policy Template **
- Description **
- MAC **
- Default Gateway **
- OS **
- IPv6 **

* Select to view additional details.

** You must enable **Additional Columns** to display the field in **Columns**, and then select **Columns** to add, remove, and reorder the columns.

For status icon descriptions, see Device Status Icons on page 119. For details on performing actions on a device, see Device 3-Dot Menu Actions on page 134.

*Wired View*

The **Wired** view provides a list of wired devices.

Go to **Monitoring** > **Network Devices** > **Device Status** > **Wired** to display the following information:

- Status
- Clients **
- Cloud Config Group **
- Network Policy Template **
- Device *
- Location
- Uptime
- MAC Address *
- Serial Number
- CoPilot ***
- Management IP
- Default Gateway
- FW Upgrade On
- Operating System
- Firmware
- Model
- Network Policy
- IPv6

* Select to view additional details.

** You must enable **Additional Columns** to display the field in **Columns**, and then select **Columns** to add, remove, and reorder the columns.

The **Clients** column shows the number of clients currently connected to the device. To check client health status, select the client count to open **Monitoring** > **Clients** filtered for the selected device. For more information, see Monitor Clients on page 242.

*** Requires an active CoPilot license.

For status icon descriptions, see Device Status Icons on page 119. For details on performing actions on a device, see Device 3-Dot Menu Actions on page 134.

*Wireless View*

The **Wireless** view provides a list of wireless devices.

Select **Monitoring** > **Network Devices** > **Device Status** > **Wireless** to display the following information:

- Status
- Device *
- Location
- Clients *
- Uptime
- Uplink Speed
- MAC *
- Serial Number
- CoPilot
- Management IP
- Country Code
- Managed By
- Network Policy Template **
- Wi-Fi 0 **
  - Channel
  - Power
  - Radio
- Wi-Fi 1 **
  - Channel
  - Power

- Primary Controller IP ***
- Secondary Controller IP ***
- Default Gateway
- FW Upgrade On
- Cloud Config Group
- Firmware Version
- Model
- Network Policy
- IPv6
    - Radio
- Wi-Fi 2 **
    - Channel
    - Power
    - Radio

* Select to view additional details.

The **Clients** column shows the number of clients currently connected to the device. To check client health status, select the client count to open **Monitoring** > **Clients** filtered for the selected device. For more information, see Monitor Clients on page 242.

** You must enable **Additional Columns** to display the field in **Columns**, and then select **Columns** to add, remove, and reorder the columns.

*** Available for locally managed devices only. These devices are identified by the  status icon.

For status icon descriptions, see Device Status Icons on page 119. For details on performing actions on a device, see Device 3-Dot Menu Actions on page 134.

*AFC Wireless View*

Go to **Monitoring** > **Network Devices** > **Device Status** > **AFC Wireless** to display AFC device information.



**Note**
AFC is supported on AP4020/4020X/AP4020FX (indoor), AP4060/AP4060X (indoor/outdoor), AP5020 (indoor), AP5022 (indoor), AP5050 (indoor/outdoor), and AP5060U/D (indoor) devices.

The **AFC Wireless** view provides a list of wireless devices that are required to use AFC (6 GHz standard power). This view displays information to help ensure compliance with spectrum regulations and optimize wireless performance.

#### AFC Service

The AFC Service widget displays configuration and operational status information for the AFC service used for 6 GHz standard power operation. This AFC service is provided by a third-party provider and is not managed by ExtremeCloud IQ (New). This widget allows administrators to monitor the availability and responsiveness of the AFC service and to identify potential service availability issues.

Select a **Country** from the drop-down list to filter the details for a specific region. The **Mode** and **Address** fields display service-related information. The **Time Range** graph displays AFC service activity over the last 24 hours. You can zoom in and out of the graph to view shorter

time intervals for more detailed analysis. Select **Reset Zoom** to reset the graph to return to the default time range.

#### AFC Wireless View Summary Widgets

The widgets in the AFC Wireless view provide critical insights into device status and AFC operations. They help administrators monitor spectrum compliance, validate device location data, and identify potential issues with frequency coordination. Understanding these widgets ensures efficient troubleshooting and optimal wireless performance.

**Total APs**

Displays the total number of 6 GHz Standard Power Powered APs managed in the AFC Wireless view. Use this count to understand the overall scale of your AFC deployment. Select the widget to add a filter the AFC device table.

**Geolocation**

Displays the geolocation status of AFC-enabled devices as a percentage, showing the proportion of devices with geolocation **Available** and **Not Available**, helping you confirm which AFC-enabled devices have valid location data for frequency coordination. Select the widget to add a filter the AFC device table.

**AFC Spectrum Status**

Displays the spectrum coordination status of AFC-enabled devices as a percentage, giving you a visual overview of spectrum authorization progress across your device fleet. Select the widget to add a filter the AFC device table.

**AFC Radio Operational Status**

Displays counts of AFC radios in the following operational states:

- **Radios Off**: Provides a count of devices that are not transmitting because the approved AFC spectrum does not permit operation on the configured channel or power level.
- **Radios Reduced**: Provides a count of devices operating at reduced power levels due to AFC-imposed spectrum or power limitations.

This information helps you quickly identify and address compliance or performance issues related to AFC frequency coordination.

#### AFC Device Table

The AFC device table displays the following information:

- Status
- Serial Number
- Model
- Device
- Geolocation
- Wi-Fi Radio
- AFC Status
- Power Mode
- Channel
- Requested Channel
- Power
- Requested Power
- AFC Expires

The AFC Status and Geolocation of an AP indicate the regional RF compliance of the AP, not the AP's current connection status. If an AP is no longer connected, the AFC Status and Geolocation are not erased. Both the AFC Status and Geolocation remain unchanged until the

expiration time is reached. When the expiration time is reached, the AFC Status changes to "Grace Period" and the Geolocation changes to "Not Available".

For status icon descriptions, see Device Status Icons on page 119. For details on performing actions on a device, see Device 3-Dot Menu Actions on page 134.

*Appliances View*

The **Appliances** view displays all appliance-type devices onboarded to Extreme Platform ONE Networking, both cloud-onboarded controllers and locally managed appliances, including:

- ExtremeCloud Site Engine
- ExtremeCloud IQ Controller
- Extreme Tunnel Concentrator
-

Go to **Monitoring** > **Network Devices** > **Device Status** > **Appliances** to display the following information:

- Status
- Device*
- Management IP
- Serial Number
- Location
- Model
- Firmware
- Clients**
- Uptime
- MAC*
- OS
- IPv6
- Network Policy
- Application***

* Select to view additional details.

** Select the number of wireless clients reported by this controller to view a filtered list of clients on the **Wireless** tab.



**Important**
The **Clients** column is not filterable.

*** The **Application** column displays:

- The full application name for the installed application (for example, `Third Party Management Engine`, `Tunnel Concentrator`, or `ExtremeCloud IQ Controller`).
- No value (blank) if UCP has no application installed.



**Note**
Each UCP row represents the UCP host itself. The **Application** column shows the application hosted on that UCP device. UCP supports one installed application at a time.
The 4120C supports multiple instances of the Tunnel Concentrator application.

To add the **Application** column to the **Appliances** tab view, select **Columns**, under **Additional Columns**, select **Application**.

For status icon descriptions, see Device Status Icons on page 119. For details on performing actions on a device, see Device 3-Dot Menu Actions on page 134.

*Discovered View*

The **Discovered** view provides a list of devices managed through ExtremeCloud Site Engine (XIQ-SE).

Go to **Monitoring** > **Network Devices** > **Device Status** > **Discovered** to display the following information:

- Status
- Device*
- Management IP
- Serial Number
- Location
- Model
- Firmware
- Uptime
- OS
- MAC*
- IPv6

* Select to view additional details.

For status icon descriptions, see Device Status Icons on page 119. For details on performing actions on a device, see Device 3-Dot Menu Actions on page 134.

## Device Status Icons

**Table 34: Device Status Icons**

| Icon | Icon Name | Description |
|---|---|---|
|  | AFC Status | Indicates an AFC issue with the selected device. Status options include **Pending**, **Grace Period**, and **Spectrum Mismatch**. |
|  | Anchor AP | Device is set as an anchor. |
|  | Configuration Audit Match | The network policy configuration matches the current running configuration.<br>Select the icon to open a pop-up window detailing the configuration changes that occurred since the last **Update Devices** operation.<br>• Audit tab — lists any modifications made since the previous configuration update.<br>• Delta tab — shows CLI commands that have changed since the previous update.<br>• Complete tab — shows all CLI commands (including the CLI commands in the Delta tab) that form a configuration file. ExtremeCloud IQ uses this file for the next configuration update. After a successful configuration update, the configuration in the Complete tab matches the running configuration.<br>**Note:** Not applicable for locally managed switches. |

**Table 34: Device Status Icons (continued)**

| Icon | Icon Name | Description |
|---|---|---|
|  | Configuration Audit Mismatch | The network policy configuration does not match the current running configuration.<br>Cause: The Configuration Audit Mismatch icon is visible on devices between the time that network policy changes are saved and the time that the altered network policy is uploaded to the device.<br>Action: Upload the network policy to the device.<br>Select the icon to open a pop-up window detailing the configuration changes that occurred since the last **Update Devices** operation. See the Configuration Audit Match icon description for details.<br>**Note:** Not applicable for locally managed switches. |
|  | Configured at Device Level | Device possesses a device-level configuration that is different from the configuration defined in the network policy. This is not an error condition, but this information can be useful when troubleshooting network behavior because device-level configurations supersede device templates and network policy configurations. |
|  | Configuration Pending | Device is currently offline and will receive its latest assigned configuration once it reconnects to the network. |
|  | Configuration Rollback | Device could not establish a connection to ExtremeCloud IQ after the configuration update. Device configuration rolled back to the last known good connection and the **Updated** status column displays `Device update failed`. |
|  | Connected Device | Device is actively communicating with ExtremeCloud IQ (New). |
|  | Device Update Unsuccessful | Device did not accept the OS or configuration upload.<br>Cause: There are many reasons for an unsuccessful update, but the most common include network connectivity or connection status changes, or the device rejected the command it received.<br>Action: Hover over the update message in the Updated column to view the reason message describing the likely error condition. Ensure that the device is properly powered, that there is appropriate network connectivity, and that common causes listed here are not the issue. |
|  | Digital Twin | Device is a simulated device. |

**Table 34: Device Status Icons (continued)**

| Icon | Icon Name | Description |
|---|---|---|
|  | Disconnected Device | Device is not actively communicating with ExtremeCloud IQ (New).<br>Cause: The device might be physically disconnected from the network or powered off. This condition also occurs if there are interruptions in the network between the device and ExtremeCloud IQ (New) or when there are misconfigured firewalls or ACL rules.<br>Action: Ensure the device is connected to the network and powered on and ensure that communication can occur through logical barriers such as firewalls. |
|  | ExtremeCloud Appliance Cluster (Closed) | Device is a logical cluster of appliances, but the cluster is collapsed visually to appear as a single device. |
|  | ExtremeCloud Appliance Cluster (Open) | Device is a logical cluster of appliances, but the cluster is expanded visually to reveal the cluster members. |
|  | Fabric Attach | Device is a member of the Fabric Attach Connect Automation environment and is functioning properly in that context. |
|  | Fabric Attach Issue | Device is Fabric Attach capable, but the Fabric Attach (FA) session to the FA server is not established.<br>Cause: This can occur if the communication link between the FA device and server is disrupted or if FA is disabled on the peer switch.<br>Action: Ensure that there is connectivity between FA device and server, and that FA server functionality is enabled on the peer switch. |
|  | Locally Managed (ExtremeCloud IQ (New)) | Device is managed locally but monitored in ExtremeCloud IQ (New). For example, devices can be managed locally by ExtremeCloud IQ Controller or ExtremeCloud Site Engine. |

**Table 34: Device Status Icons (continued)**

| Icon | Icon Name | Description |
|---|---|---|
|  | Locally Managed (No Cloud Management) | Device or its management appliance are not visible to ExtremeCloud IQ (New).<br>Cause: This is not always an error condition, but it can indicate a status communication problem. In this case, the device is functioning properly, so there is no disruption in network performance; instead, the status communication is disrupted so that ExtremeCloud IQ (New) is unaware of the status.<br>Action: First, ensure that the device is functioning properly to rule out problems with the device. Next, ensure that there are no logical barriers between the device and ExtremeCloud IQ (New). Afterward, ensure that any applications that lie in the communication path are receiving, processing, and sending data appropriately. |
|  | Managed by ExtremeIoT | Device is provisioned to function with ExtremeIoT. |
|  | Monitoring Unassociated Clients | Device is using presence analytics to monitor client devices that are not associated to the network, such as passersby. |
|  | No Connection | This device has not yet made a connection with ExtremeCloud IQ (New). It can take up to 10 minutes for a device to appear after the initial onboarding process. |
|  | Old OS Personality Inactive | Device formerly used another OS persona, which is no longer active. The information in this record pertains to the device when it ran using this OS persona. |
|  | Provisioned Device | An administrator has provisioned the device, but the device has not yet communicated with ExtremeCloud IQ (New).<br>This is an administrative state and does not reflect the actual connection status. To view the actual connection status, you must manually change the management state using the **Actions** > **Change Management Status** menu option. |
|  | RadSec Proxy Server | Device is acting as a RadSec proxy server. This service optimizes some authentication functions, especially for cloud authentication, such as cloud PPSK and cloud RADIUS. |
|  | Rogue AP Mitigation | Device is actively mitigating a rogue access point. Refer to the information provided by your security management platform. |
|  | Sensor Mode - Interface Active | Device is functioning as a sensor and the monitoring interface is active and monitoring the RF environment. |

**Table 34: Device Status Icons (continued)**

| Icon | Icon Name | Description |
|---|---|---|
|  | Sensor Mode - Interface Inactive | Device is functioning as a sensor, but the monitoring interface is not active and is not monitoring the RF environment. |
|  | Simulated Device | Device is a simulated device, which possesses only simulated configurations, conditions, and traffic. By contrast, a real device has a physical presence on the network and consumes power and network resources. |
|  | Spectrum Intelligence | Device is functioning as a Spectrum Intelligence monitor, which monitors the RF environment and provides frequency and time domain graphs and heat maps. |
|  | Swap for Real Device | Device is a simulated device that you can exchange for a real device. |
|  | Switch Stack | Device is a switch stack. |
|  | Switch Stack Warning | One or more stack member switches is not associated to the master stack node.<br>Cause: One or more member switches within a stack has lost connectivity to the master stack node. This can happen if the member switch is powered off, physically disconnected from the stack, or if there is an issue with the switch itself.<br>Action: Ensure that the switch slot has power and that the stacking cables are properly connected. |
|  | Thread Commissioner Running | The AP is a designated Commissioner in the IoT Thread network. |
|  | Undetermined | Device status is undetermined.<br>Cause: This condition can arise when the indicators are ambiguous, unknown, or appear contradictory due to other factors. If the device is owned by ExtremeCloud Site Engine, an *Undetermined* status typically indicates that the device is orphaned. Site Engine does not recognize the device, while the cloud identifies it as Site Engine–owned. Investigate this discrepancy; in most cases, the device should be removed from the cloud.<br>Action: Begin general troubleshooting procedures to ensure that the device is powered, connected, and is responding to traffic and CLI commands. Ensure that the device is communicating appropriately with network services, such as NTP, DHCP, etc. |

**Table 34: Device Status Icons (continued)**

| Icon | Icon Name | Description |
|---|---|---|
|  | VPN Client Server Tunnels Down | Device is functioning as a VPN client, but the VPN tunnel is down. If the tunnel is administratively down, then this is not an error condition.<br>Cause: If not administratively down, issues on the server side can cause the tunnel to go down. Additionally, if the client- and server-side configuration do not agree, then a tunnel cannot be built.<br>Action: Consult the VPN troubleshooting tools in ExtremeCloud IQ (New). You can also ensure that the server device is connected to the network and that the tunnel configurations agree on both ends of the tunnel. |
|  | VPN Client Server Tunnels Up | Device is functioning as a VPN client and the VPN tunnel is up, healthy, and operating properly. |
|  | VPN Client Server Tunnels Up and Down | Some of the VPN client tunnels are administratively up but operationally down.<br>Cause: VPN server might be down, or unreachable.<br>Action: Ensure that the VPN server is powered on, connected to the network, and communicating with ExtremeCloud IQ (New). In addition, ensure that there is connectivity and communication between the VPN server and client. |
|  | VPN Server Turned Down | Device is functioning as a VPN server, but the VPN tunnel is down. If the tunnel is administratively down, then this is not an error condition.<br>Cause: If not administratively down, issues on the client side can cause the tunnel to go down. Additionally, if the client- and server-side configuration do not agree, then a tunnel cannot be built.<br>Action: Consult the VPN troubleshooting tools in ExtremeCloud IQ (New). You can also ensure that the client device is connected to the network and that the tunnel configurations agree on both ends of the tunnel. |
|  | VPN Server Turned Up | Device is functioning as a VPN server and the VPN tunnel is up, healthy, and operating properly. |
|  | VPN Server Turned Up and Down | Some of the VPN server tunnels are administratively up but operationally down.<br>Cause: VPN client might be down, or unreachable.<br>Action: Ensure that the VPN clients are powered on, connected to the network, and communicating with ExtremeCloud IQ (New). In addition, ensure that there is connectivity and communication between the VPN server and clients. |

## Filter the Device List by Status

From **Monitoring** > **Network Devices** > **Device Status**, you can use the **Filters** panel to narrow the device list to only those devices that are associated with specific statuses. You can select multiple statuses to display only the devices that have any of the selected status conditions. For a description of each status icon, see Device Status Icons on page 119.

**Note**
The **Status** filter displays only the status icon options that are present in the current device table.

Use this task to apply the **Status** filter in the **Filters** panel to display only devices that have one or more selected device statuses.

1. Go to **Monitoring** > **Network Devices** > **Device Status**.
2. If needed, select a view tab: **All Devices**, **Wired**, **Wireless**, **AFC Wireless**, **Appliances**, or **Discovered**.
3. Select **Filter**.

   The **Filters** panel opens on the right side of the page.
4. In the **Filters** panel, select the **Status** section heading to expand the status filter options.

   A list of statuses appears with a **Search** field and a check box next to each status icon name. Only the status icons names currently represented in the device table are listed.
5. Select the check box next to each status you want to filter by.

   You can select more than one status at a time. To locate a specific status quickly, type part of its name in the **Search** field.

   The device list updates automatically to display only devices that are associated with at least one of the selected statuses.

The device list is filtered to show only devices with the selected status conditions. An active filter is indicated by the icon in the column header.

**Note**
To remove the status filter and restore the default view, select **Reset** in the **Status** filter section. To clear all active filters, select **Clear all filters** at the top of the **Filters** panel.

# Network Devices | Device Health

Go to **Monitoring** > **Network Devices** > **Device Health** to view real-time device metrics. **Device Health** provides key performance metrics to help monitor and maintain the stability of your network devices. Alternatively, select the device host name to display System and Connectivity information for the selected device, including the management status of the device.

To refine the device list:

- Select and drag the left or right border of the column header to adjust the column width.
- Select and drag the column headers to change the order of the columns.

**Note**
Once columns are reordered, the layout is saved and persistent until it is manually changed.

- Select a column header to sort column data in ascending or descending order.
- Select **Columns** to add, remove, and reorder the columns.
- To refine the list, select **Filter**. The filter sidebar lets you customize what information is displayed in the device list. Available filters vary depending on the window you are in. To see all available options, in the filter area, select a section heading to see more or less items. To clear all active filters, select **Clear all filters** above the **Filters** panel.

**Note**
To download the table data as a CSV file, select .

## Device Health | Wired

Go to **Monitoring** > **Network Devices** > **Device Health** > **Wired** to filter a list of wired devices.

When **Show Summary** is enabled, health widgets display CPU Usage Issues, Memory Usage Issues, PoE Usage Issues, Temperature Issues, Fan Issues, and Power Supply Issues. By default, the data capture time frame is 24 hours.

**Note**
Widgets provide interactive functionality. Selecting a widget may either filter the device table or open the widget for modification, depending on the widget type.

The Wired table displays the following information:

- Device *
- Location
- CPU Usage %
- Memory Usage %
- PoE Usage %
- Temperature°C
- Fan Status *
- Power Supply *

* Select to view additional details. You can expand a switch stack to view individual switches. Select a switch to view its health metrics, including model, uptime, location, IP address, CPU usage, memory usage, temperature, and PoE consumption.

## Device Health | Wireless

Go to **Monitoring** > **Network Devices** > **Device Health** > **Wireless** to filter a list of wireless devices.

When **Show Summary** is enabled, health widgets display CPU Usage Issues, Memory Usage Issues, and PoE Usage Issues. By default, the data capture time frame is 24 hours.

**Note**
Widgets provide interactive functionality. Selecting a widget may either filter the device table or open the widget for modification, depending on the widget type.

The Wireless table displays the following information:

- Device *
- Location
- CPU Usage %
- Memory Usage %
- PoE Usage
- Channel Change
- WiFi Reboots
- Unicast/Multicast/Broadcast:
  - Eth 0%
  - Eth 1%

* Select to view additional details.

### Device Health | Discovered

Go to **Monitoring** > **Network Devices** > **Device Health** > **Discovered** to filter a list of devices managed through ExtremeCloud Site Engine.

The table displays the following information:

- Device *
- Location
- CPU Usage %
- Memory Usage %
- Temperature °C
- Fan Status
- Power Supply

* Select to view additional details.

## Network Devices | Usage & Capacity

Go to **Monitoring** > **Network Devices** > **Usage & Capacity** to monitor bandwidth usage and capacity trends to ensure optimal network performance and resource planning.

To refine the device list:

- Select and drag the left or right border of the column header to adjust the column width.
- Select and drag the column headers to change the order of the columns.

**Note**
Once columns are reordered, the layout is saved and persistent until it is manually changed.

- Select a column header to sort column data in ascending or descending order.
- Select **Columns** to add, remove, and reorder the columns.
- To refine the list, select **Filter**. The filter sidebar lets you customize what information is displayed in the device list. Available filters vary depending on the window you are in. To see

all available options, in the filter area, select a section heading to see more or less items. To clear all active filters, select **Clear all filters** above the **Filters** panel.

**Note**
To download the table data as a CSV file, select .

## Usage & Capacity | Wired

Go to **Monitoring** > **Network Devices** > **Usage & Capacity** > **Wired** to filter a list of wired devices.

When **Show Summary** is enabled, usage and capacity widgets display Usage Utilization, Throughput (Billions of Packets), and Congestion. When you select **Total Congestion in Packets**, the wired device table is filtered to display only devices associated with packet-based congestion. By default, the data capture time frame is 24 hours.

The Wired device table displays the following information:

- Device *
- Location
- Clients
- Total Bandwidth Utilized (Bytes)
- Total Throughput (Rx Packets per Second)
- Total Throughput (Tx Packets per Second)
- Total Unicast (Packets %)
- Total Multicast (Packets %)
- Total Broadcast (Packets %)
- Total Queue Congestion (# of Packets)

* Select to view additional details.

## Usage & Capacity | Wireless

Go to **Monitoring** > **Network Devices** > **Usage & Capacity** > **Wireless** to filter a list of wireless devices.

When **Show Summary** is enabled, usage and capacity widgets display Excessive Channel Utilization, Excessive Retries, and Excessive Packet Loss. By default, the data capture time frame is 24 hours.

The Wireless table displays the following information:

- Device *
- Location
- Clients
- MAC Address *
- Packet Loss %
- Channel Utilization %
- Retries
- Unicast/Multicast/Broadcast
- Noise (dBm)
- Interference %

* Select to view additional details.

## Usage & Capacity | Discovered

Go to **Monitoring** > **Network Devices** > **Usage & Capacity** > **Discovered** to filter a list of devices managed through ExtremeCloud Site Engine.

The table displays the following information:

- Device *
- Site Name
- Total Bandwidth Utilized (Bytes)
- Total Throughput (Rx Packets per Second)
- Total Throughput (Tx Packets per Second)
- Total Unicast (Packets %)
- Total Multicast (Packets %)
- Total Broadcast (Packets %)

* Select to view additional details.

# Network Devices | Add Devices

Add devices to the network using one of the following methods:

- Manually: Manually enter up to 10 serial numbers for devices of the same type.
- Import: Bulk import multiple devices of any type using a CSV file that contains device serial numbers.
- **Download XLSX Template**: Download device list data to an XLSX spreadsheet.



**Note**
When adding a device, you have the option to assign the device to a site. If you do not initiate the site assignment, ExtremeCloud IQ (New) assigns the device to the default site. This assignment is visible under **Inventory**, and you can reassign the device to another site.

## Add Devices Manually

Use this task to manually add devices to ExtremeCloud IQ (New) by entering device serial numbers.

From **Add Devices**, you can add access points that are managed from ExtremeCloud IQ (New) or specify that devices are managed locally by a controller. You can also add local controllers and appliances, then monitor their local devices through Extreme Platform ONE.



**Note**
You can add a maximum of 10 serial numbers per session. All serial numbers entered must be from the same device type.

1. Go to **Monitoring** > **Network Devices**.
2. Select **Add Devices** > **Manually**.

   The **Manually Add Devices** dialog opens.

3. Select how the device will be managed.
   - **Cloud Managed**: Select this option to add and manage the device directly through ExtremeCloud IQ (New). Select the device type you want to add and enter one or more device serial numbers.

     **Note**
     When adding controllers and appliances, select **Cloud** management. The devices that are managed by the local-controller or appliance automatically display in the **Network Devices** list.

     **Important**
     Cloud management is not supported for AP3020, AP3020X, and AP3020W. They can only be onboarded as controller-managed (locally managed) devices.

   - **Controller Managed**: Select this option to add a device for controller-based management. This option is used for supported devices intended to be managed by an on-premises controller instead of being managed directly through ExtremeCloud IQ (New). After adding the device, it connects to an external controller and is managed from the controller. Enter one or more device serial numbers.
     - **Enhanced Discovery**: For deployments that do not have a local network configuration for discovery, we offer an enhanced AP onboarding experience that provides indication of the specific IP address or Fully-Qualified Domain Name (FQDN) of the controllers to which the AP connects. Enable this option if the controller is not detected using standard DHCP or DNS mechanisms, or if the network environment restricts direct discovery.
       - **Primary Controller**: Enter the IP address or fully qualified domain name (FQDN) of the primary controller. The device attempts to connect to this controller first.
       - **Backup Controller** (Optional): Enter the IP address or FQDN of a secondary controller. The device connects to this controller if the primary controller is unreachable.

     **Note**
     Devices added in controller-managed mode are managed from the controller for configuration, firmware updates, and policy enforcement. ExtremeCloud IQ (New) provides visibility, monitoring, and inventory tracking.

4. From the **Device Type** drop-down, select the type of device you are adding.

**Table 35: Device Type Options**

| Device Type | Description |
|---|---|
| Switch Engine/ EXOS | Extreme Networks switches running Switch Engine (EXOS) firmware. |
| Fabric Engine/ VOSS | Extreme Networks switches running Fabric Engine (VOSS) firmware. |

**Table 35: Device Type Options (continued)**

| Device Type | Description |
|---|---|
| IQ Engine | Extreme Networks wireless access points running IQ Engine firmware and managed directly through ExtremeCloud IQ (New).<br><br>**Note:** For AP3020W, AP3020, and AP3020X APs, select **IQ Engine** as the device type. These APs support both Cloud Managed and Controller Managed onboarding modes. |
| Universal Compute Platform | Extreme Networks Universal Compute Platform clustered or stand-alone appliances. |
| Tunnel Concentrator | appliances that aggregate and route wireless traffic from access points to the wired network.<br>support requires the following configuration:<br>• Configure a Tunnel Concentrator service<br>• Configure a Tunnel Policy |
| Controller | Extreme Networks wireless LAN controllers that manage access point associations, authentication, and network policy enforcement.<br>Controller considerations:<br>• The controller serial number and MAC address are required for onboarding. The serial number is the Lock ID from the controller.<br>• Devices that have already discovered the local controller will display in the Extreme Platform ONE Networking **Network Devices** list. |

5. In the **Serial No.** field, enter the device serial number.
   To add more serial numbers, select the add icon (**+**) to display an additional serial number field. You can enter a maximum of 10 serial numbers.

   **Note**
   When adding one or more serial numbers, any device model that does not support the selected device type is identified with a visual indicator and a warning message. You can choose to **Cancel** or **Continue**. If you choose to continue, the unsupported devices are skipped and only compatible devices are onboarded.

6. Select a **Network Policy** for the devices.
   A network policy definition does not apply to the onboarding workflow for controllers, appliances, or tunnel concentrators.
7. Select a **Location** for the devices.
   Location indicates where the device will be installed. Valid locations include a floor or outdoor site. When location is not provided, the default site is automatically assigned. The default site is predefined and auto-created per customer account.
8. Select **Add Device(s)**.
   The devices are added to ExtremeCloud IQ (New) and appear in the **Network Devices** list.

Related Links

Adding Controllers and Appliances for Locally Managed Devices on page 110

## Import Devices

Before you begin, download the XLSX template file. Select **Add Devices** > **Download XLSX Template** and populate it with the device information. The tabbed XLSX file indicates the required and optional fields for each device type. The file must be in XLSX format.

**Note**
AP3020W, AP3020, and AP3020X support bulk onboarding using the XLSX import method. Use the **IQ Engine** device type when adding these models.

Use this task to add multiple devices to ExtremeCloud IQ (New) at one time by uploading an XLSX file that contains the device information.

**Note**
The upload supports XLSX files only. Ensure your file uses the downloaded template format.

1. Go to **Monitoring** > **Network Devices**.
2. Select **Add Devices** > **Import**.

   The **Import** dialog opens.
3. Under **Managed By**, select how the devices will be managed.
   - **Cloud**: Select this option to add and manage the device directly throughExtremeCloud IQ (New).

     **Note**
     When adding controllers and appliances, select **Cloud** management. The devices that are managed by the local-controller or appliance automatically display in the **Network Devices** list.

     **Important**
     Cloud is not supported for AP3020, AP3020X, and AP3020W. They can only be onboarded as controller (locally managed) devices.

   - **Controller**: Select this option to add the device for controller-based management. This option is used for supported devices intended to be managed by an on-premises controller instead of being managed directly through ExtremeCloud IQ (New). After adding the device, it connects to an external controller and is managed from the controller. Enter one or more device serial numbers.
     - **Enhanced Discovery**: Enable Enhanced Discovery to assist the device in locating the controller, or to manually specify controller details. Enable this option if the controller is not detected using standard DHCP or DNS mechanisms, or if the network environment restricts direct discovery.
       - **Primary Controller**: Enter the IP address or fully qualified domain name (FQDN) of the primary controller. The device attempts to connect to this controller first.

- **Backup Controller** (Optional): Enter the IP address or FQDN of a secondary controller. The device connects to this controller if the primary controller is unreachable.

**Note**
Devices added in controller-managed mode are managed from the controller for configuration, firmware updates, and policy enforcement. ExtremeCloud IQ (New) provides visibility, monitoring, and inventory tracking.

4. Select **Browse Files** or drag and drop your completed XLSX file into the upload area.
5. Select a **Network Policy** for the devices
6. Select a **Location** for the devices.
7. Select **Add Device(s)**.

   The devices from the XLSX file are added to ExtremeCloud IQ (New) and appear in the **Network Devices** list.

## Upgrade Network Device Firmware

You can upgrade device firmware for one or more devices on demand or you can schedule the upgrade.

Use this task to upgrade firmware for selected devices.

1. Go to **Monitor** > **Network Devices**.
2. Select **Upgrade Firmware**.
3. Select a **Device Type** and **Device Management** (Cloud Managed is the default).

**Note**
You can filter the device list by using the **Search** field to quickly locate specific devices.

4. Select the devices for firmware upgrade, and then select **Next**.
5. Select a **Firmware Version** for each device, and then select **Next**.

**Note**
- Firmware upgrades are available only for connected and managed devices.
- The **Vulnerabilities Fixed** column displays all fixed security vulnerabilities data associated with your selection.

6. Confirm the **Review Summary**, and then select a **Firmware Update Schedule**:
   - To update immediately, select **Upgrade Now**, and then select **Upgrade Firmware**.
   - To update at a later time, select **Upgrade Later**, select a **Date & Time** , and then select **Schedule Firmware Update**.

**Note**
Firmware upgrades can be scheduled up to 30 days in advance.

7. Select ⋮ to view **Firmware Upgrade History**. Firmware upgrade activity is stored for a maximum of 30 days.

   **Note**
   To reschedule a scheduled firmware upgrade:
   - Select a scheduled upgrade, and then select **Reschedule Upgrade**.
   - Select a new **Date & Time**, and then select **Reschedule**.

## Device 3-Dot Menu Actions

To manage devices in ExtremeCloud IQ (New), go to **Monitoring** > **Network Devices** > **Device Status**. From the **3-dot Menu** (⋮) at the end of a device row, you can perform a number of actions on the device.

**Note**
- Not all actions are available for all device types. Most device options are unavailable for an unmanaged device. To change the management status of your device, select **Change Management Status** > **Manage**.
- To perform actions on multiple devices, select the devices to configure, and then select **Actions**. The Actions menu displays on the upper toolbar only after multiple devices are selected. When you select multiple devices, the action is available if at least one selected device supports the action. The action will not apply to unsupported devices.

The actions that are available depend on the device model. The following is a list of possible actions:

- **Advanced**:
  - **Change Device Mode**: Change the device mode from AP device to Router.

    **Note**
    - To configure an AP device as a router, the associated network policy must have both wireless and routing activated.
    - The following features are not supported: SDWAN, URL filtering, USB modem, private client group, and client mode.
    - The device must complete a full configuration update for the mode change to take effect.

  - **Change OS to WiNG**: Change the operating system of the selected devices to WiNG.

    **Important**
    Changing the OS reboots the device and permanently erases the existing configuration. The new OS reverts to factory default settings.

    **Note**
    This action is not available for AP5022, AP5022FX, or AP5022S6D devices when managed as cloud devices.

- **SSH Access**: Select an available runtime to temporarily access your network remotely to troubleshoot the selected device. Select **Start** to begin an SSH session.

  **Note**
  SSH must be enabled to run an SSH session on the selected device. For more information, see Configure SSH on page 202.

- **AFC Geolocation Report** (AFC Wireless Only): Generate and view the AFC Geolocation Report for the selected device. The report displays geolocation data, radio parameters, and ranging measurements to support AFC compliance analysis. For more information, see AFC Geolocation Report on page 146.
- **Assign Country Code**: Select a country code for a managed device from the drop-down list. The country code defines the device radio channels and power limitations for the country in which the device operates. For devices used in the United States, the region code is reset to **FCC** and the country code is preset to **United States**. Select **Save** to reboot the selected devices.
- **Assign to Cloud Config Group**: Add the selected devices to an existing **Cloud Config Group** (CCG). In the **Assign to a Cloud Config Group** panel, select a CCG to assign to the selected devices, and then select **Assign**. To create a new CCG, see Add a Cloud Config Group on page 439.
- **Assign Location**: Assign a location to the selected devices.
- **Assign Network Policy**: Assign an existing network policy to the device.

  **Note**
  This action replaces existing associated policies with the newly selected policy.

- **Change Management Status**: Indicates the management status of the selected devices. Select **Manage** or **Unmanage**.

  **Note**
  The **Change Management Status** menu option is now available for Site Engine and devices managed by Site Engine. If Site Engine status is **Unmanaged**, the status for both Site Engine and devices managed by Site Engine is **Unmanaged**.

- **Change CoPilot License Status**: Activate (use) a CoPilot license for the selected device, or revoke the license for a device currently using a license. These actions are available only if your deployment has an active CoPilot subscription.
- **Change OS to Fabric Engine / Change OS to Switch Engine**: Change the operating system of the selected devices to Fabric Engine or Switch Engine.

  **Important**
  Changing the OS reboots the device and permanently erases the existing configuration. The new OS reverts to factory default settings.

- **Clear Audit Mismatch**: Occasionally, there can be a mismatch between the configuration database and the device-level configuration database. If this occurs, perform this action.
- **Configure** > **Device**: Perform device-level configuration tasks and update devices. Settings made at this level apply only to the individual device and overrides the template settings configured for the network policy. For wired devices, see Configure Wired Devices. For wireless devices, see Configure Wireless Devices.

- **Delete**: Delete the selected devices from the network. See Delete a Device from the Network on page 148.
- **Diagnostics** (AFC Wireless Only): Select a diagnostic method to run CLI commands on the selected devices. For a full list of CLI commands, see Diagnostics CLI Commands on page 142.

  **Note**
  Each time you run a CLI command, the diagnostic results are added to the log. To resize the log window, select and drag any corner of the window to view more of the results on the screen. Select **Export Results** to download all diagnostic results as a .txt file.

- **Enhanced Discovery**: Configure the primary and backup controllers for locally managed (controller-managed) devices. You can use this action for a single device or for multiple devices selected from the device list. For more information, see Enhanced Discovery on page 138.

  **Note**
  This action is available on locally managed devices only. Locally managed devices are identified by the  status icon.

- **Locate Device**: Trigger a visual cue to quickly identify the exact position of a selected device. For more information, see Locate Device on page 139.
- **Manage Feature License**: Add or revoke a Premier or MACsec switch license to a currently managed device. Toggle **Premier License** and **MACsec License** on or off, and then select **Save**.

  **Note**
  The ability to apply or revoke licenses depends on the selected hardware model and license availability.

  **Important**
  When managing multiple selected devices, some devices may need to be managed separately when performing license actions due to differences in hardware compatibility or license type.

- **Open Application UI** (UCP Only): Open the local web-based management interface of an application running on the Universal Compute Platform. The application interface opens in a separate browser tab. ExtremeCloud IQ (New) uses the appliance connection to proxy access to the application's local user interface.

  **Note**
  This action is available only when the target UCP appliance has a supported application and the application can be reached through the appliance connection. If the application is stopped, unavailable, or the UCP appliance cannot be reached, the action is unavailable and the application user interface will not open.

- **Ping** (Tunnel Concentrator Only): Sends a ping request from the Tunnel Concentrator to verify network connectivity.
- **Reboot Device**: Reboot devices after uploading a configuration. Rebooting momentarily disconnects any associated clients from the SSID, which could be disruptive.

- **Remove Stack Members** (Wired Stack Only): Remove one or more member switches from a stack. This action removes the selected members from ExtremeCloud IQ (New) but does not physically disconnect them from the stack. For more information, see Remove a Stack Member on page 150.
- **Replace Stack Members** (Wired Stack Only): Replace a failed or decommissioned switch in a stack with a new switch of the same model. For more information, see Replace a Stack Member on page 151.
- **Reset to Default**: Reset the device to factory defaults.

  **Important**
  This operation removes existing settings from the selected device and returns it to factory settings. It then reconnects to the cloud as a new device.

- **Retrieve Debug Data**: Collect diagnostic information for the selected devices from the network to help with troubleshooting and support. Use this data to analyze issues, identify root causes, and improve system performance. Select a **Debug Data Type**, and then select **Retrieve Data**. Once the process is complete, select **Download** to save a .tar.gz file containing the collected debug files.
- **Revert Device to Template**: Returns the device settings to the network policy template. This removes any device-level configuration settings.
- **Show AFC Spectrum** (AFC Wireless Only): View the current AFC-authorized channels and power limits assigned to the selected devices.

  **Note**
  If the AFC status of the selected AP is **Pending**, the spectrum results do not display because the AP is awaiting spectrum authorization from the AFC server. This status occurs during startup or after configuration changes and resolves automatically once a response is received.

- **Show GRE Tunnel** (Tunnel Concentrator Only): Display the current GRE tunnel status and configuration details.
- **Show Log** (Tunnel Concentrator Only): Display the current system log for the Tunnel Concentrator.
- **Show Tunnel Clients** (Tunnel Concentrator Only): Display a list of clients currently connected through this Tunnel Concentrator.
- **Thread Commissioner** (AP5010/AP5020 only): Enter a runtime to temporarily access your network remotely, and then select **Start**. The Thread Commissioner securely screens endpoint devices attempting to join the Thread network. To define the behavior of the Thread Commissioner, see Configure the Thread Commissioner on page 414.

  **Note**
  If another AP is already running as the Commissioner on this Thread network, a warning message displays prompting the user to stop the current Commissioner or wait for it to automatically shutdown. If Thread is not enabled on the AP, or if configuration changes have not been deployed, the operation fails and a related error message displays.

- **Tools**:
  - **Derive GPS Location** (AFC Wireless Only): Recalculate the GPS coordinates for the selected devices.

  - **Send AP Range Info** (AFC Wireless Only): Send location and antenna range data to the AFC server for the selected devices.
- **Update AFC Spectrum** (AFC Wireless Only): Request updated channel and power assignments from the AFC server based on current AP configuration and location of the selected devices.
- **Update Devices**: Update network policy and configuration for the selected devices. Select the type of update (**Delta** or **Complete**), and then select **Update**:
  - **Delta Configuration Update**: Perform delta configuration update and resolve local device configuration which is out of sync.
  - **Complete Configuration Update**: Perform a complete configuration update. Select to activate now or at a later date and time. For information about how the configuration push behaves with each **Activation Time** option, see Configuration Push Scheduling Behavior on page 154.
- **Upgrade Firmware**: Upgrade firmware to a selected version. Select **Upgrade Now** to upgrade immediately, or select **Upgrade Later** to upgrade at a specific date and time.
- **Utilities**:
  - **Diagnostics**: Select a diagnostic method to run CLI commands on the device for basic network connectivity checks, status monitoring, and function diagnostics. For a full list of CLI commands, see Diagnostics CLI Commands on page 142.

    **Note**
    Each time you run a CLI command, the diagnostic results are added to the log. To resize the log window, select and drag any corner of the window to view more of the results on the screen. Select **Export Results** to download all diagnostic results as a .txt file.

  - **RADIUS Test**: Send a RADIUS request from the device to an authentication or accounting server. For more information, see Perform a RADIUS Test on page 140.
  - **VLAN Probe**: Locates available VLANs for one or more selected devices concurrently. Select the check boxes multiple devices in the device list. When the probe completes, the results grid displays the host name, MAC address, available VLANs, unavailable VLANs, and status for each probed device. For more information, see VLAN Probe on page 143.
  - **Packet Capture**: Captures wireless and wired traffic for advanced troubleshooting. For more information, see Packet Capture on page 155.

## Enhanced Discovery

Use Enhanced Discovery to enhance onboarding support for locally managed access points in Extreme Platform ONE Networking by configuring primary and secondary ExtremeCloud IQ Controller addresses for AP discovery and adoption.

Enhanced Discovery is commonly used in deployments where local network discovery methods are unavailable or restricted. In these environments, administrators can configure the IP address or Fully Qualified Domain Name (FQDN) of the controllers that locally managed APs connect to during onboarding.

With Enhanced Discovery, selected APs are assigned to a specific controller or high-availability controller pair during conversion to the local operating system. After the AP boots

into the local WiNG operating system, the AP connects directly to the configured controller, bypassing traditional discovery mechanisms.

Universal APs are configured for cloud management by default. To manage these APs locally, select **Controller** when onboarding APs in Extreme Platform ONE Networking.

In remote deployment scenarios, administrators can configure the primary and secondary controller IP addresses or FQDNs used for local management. During onboarding, the AP first connects to Extreme Platform ONE Networking through a REST API call. The API response includes the configured controller information. After the AP successfully adopts to ExtremeCloud IQ Controller, the AP reboots into the local management persona.

Enhanced Discovery is supported for:

- Manual device onboarding
- Bulk onboarding using a .csv file

Use this task to configure controller settings for locally managed devices.

1. Go to **Monitoring** > **Network Devices** > **Device Status** > **Wireless**.
2. Select one or more locally managed devices.

**Note**

Locally managed devices are identified by the status icon.

3. From the **3-dot Menu** ( ) at the end of a device row, select **Enhanced Discovery**.
4. Configure the settings in Table 36.

**Table 36: Enhanced Discovery Settings**

| Field | Description |
|---|---|
| Primary Controller | The IP address or FQDN of the primary controller for the selected device(s). |
| Backup Controller (optional) | The IP address or FQDN of the backup controller for the selected device(s). |

5. Select **OK** to apply the settings, or **Cancel** to exit without saving.

## Locate Device

Using a visual cue helps you quickly identify the exact position of a connected device. By triggering the blinking function, you can efficiently manage and troubleshoot your network, ensuring optimal performance and coverage.

Use this task to locate the physical location of a connected device.

1. Go to **Monitoring** > **Network Devices** > **Device Status**.

2. Select ⋮ at the end of a connected device row, select **Locate Device**, and then configure the Locate Device settings in Table 37.

**Table 37: Locate Device Settings**

| Device Type | Field | Description |
|---|---|---|
| AP | LED Color | Select one of the following blinking light colors to set the color that the locator light flashes to help you find the AP:<br>• Amber<br>• White<br>• Off |
| AP | Blink Mode | Select one of the following blinking modes to set the speed at which the locator light flashes to help you find the AP:<br>• Fast<br>• Slow<br>• Steady |
| Switch | LED Timeout | Select a number of seconds between 0 (until disabled) and 604800 (one week). |

**Note**
To stop the blinking lights used for locating the device, select **Return to Standard LED operations**, and then select **Submit**.

3. Select **Submit**.

## Perform a RADIUS Test

The RADIUS Test tool tests network connectivity between a device acting as a RADIUS authenticator (RADIUS client) and RADIUS authentication server, which can be an Extreme Networks RADIUS server, or an external RADIUS authentication or accounting server.

Use this task to test the connectivity between a RADIUS authenticator and a RADIUS server.

1. Go to **Monitoring** > **Network Devices** > **Device Status**.
2. Select ⋮ at the end of a connected device row, and then select **Utilities** > **Initiate RADIUS Test**.
3. Select a **RADIUS Client** from the drop-down list.

   This is the device from which the **RADIUS Access-Request** or **Accounting-Request** message is sent.
4. Select the type of RADIUS server that you want to test.
   - To test connectivity to an Extreme Networks RADIUS server, choose **Local Server**, and then select a server from the drop-down list.
   - To test connectivity to an external RADIUS authentication or accounting server, select **External Server**, and enter the IP address of the server.

5. Select either **RADIUS Authentication Server** or **RADIUS Accounting Server**.

   If you select an authentication server, you must also enter supplicant credentials (a user name or barcode, and a password or PIN) for a valid user account on the RADIUS authentication server. You can also enter a user name and password that do not match an account on the RADIUS server.
6. Select **Test**.

Results appear under **Test Result**. A successful test result is shown below.

```
RADIUS server is reachable. Get attributes from RADIUS server: User-
Group-ID:0=13; VLAN-ID:1=1; Session-Timeout=1800
```

## Upgrade Firmware Settings

**Table 38: Upgrade Firmware Settings**

| Field | Description |
|---|---|
| **Upgrade IQ Engine and Extreme Networks Switch Engines** | |
| Upgrade to the latest version | Upgrade to the latest firmware version. |
| Upgrade to a specific version | Select a **Model** to upgrade, and then select the **Version** to upgrade.<br>To add a new version (local image), select **Local Image Management**:<br>• To add a new local image, select , and then select **Choose** to upload an image file from your computer.<br>**Note:** The format for an image file name must be *.stk, *.xos, *.voss *.tgz, *.img, or *.img.S. The file name cannot contain spaces and must not exceed 64 characters.<br>• Select **Close**.<br>Select **View Release Notes** to access the Online Help system and see the latest release notes. |
| (Optional) Upgrade even if the versions are the same | Enforce an upgrade to the same version as the current version. |
| (Optional) Enable distributed image upgrade (APs only) | Designate the AP as the server to download the firmware image. This AP then distributes the firmware to other APs in the network. |

## Diagnostics CLI Commands

To open a command window to run CLI commands, go to **Monitoring** > **Network Devices** > **Device Status** > **3-dot Menu** (⋮), select **Utilities** > **Diagnostics**.

**Note**
For Tunnel Concentrator devices, only the following subset of diagnostics is available:

- Ping
- Show GRE Tunnel
- Show Tunnel Clients
- Show Log

**Table 39: CLI Commands**

| CLI Command | Description |
|---|---|
| Ping | Ping the IP address of the device management interface (default) or any IP address, such as pinging the IP address of its own mgt0 interface (default). You can change the target to any IP address, such as the default gateway, or an address beyond the gateway, such as a DNS server. |
| Show AFC Data Exchange | Display details of the last data exchange between the AP and the AFC system, including request parameters, response channels, power limits, and status.<br><br>**Note:** Available only for AFC Wireless devices. |
| Show AMRP Tunnel | Display information about DNXP, INXP, and VPN tunnels, including tunnel type, the peer IP address, and how long the tunnel has been up. |
| Show ARP Cache | Display the ARP cache. |
| Show CPU | Display total, per user, and per system CPU utilization. |
| Show DNXP Cache | The DNXP cache stores information about client associations, allowing the network to quickly identify and re-authenticate devices as they move between access points. |
| Show DNXP Neighbors | Display neighboring hive members in the same or different subnets. This is the equivalent of entering the **`show amrp dnxp neighbor`** command. Hive members use AMRP to support roaming clients. DNXP is a component of AMRP that supports Layer 3 roaming. Hive members in different subnets use DNXP to create tunnels on an as-needed basis between themselves, allowing clients to seamlessly roam between subnets, while preserving their IP address settings, authentication state, encryption keys, firewall sessions, and QoS enforcement settings. Tunnels are not required for clients roaming among members in the same subnet. |
| Show GRE Tunnel | Display packet statistics for client traffic that members send through GRE tunnels between themselves. Extreme Networks devices use GRE tunnels for DNXP, INXP, and wireless VPN. |

**Table 39: CLI Commands (continued)**

| CLI Command | Description |
|---|---|
| Show IKE Event | Display up to 12 recent events during IKE phase 1 and phase 2 negotiations between a VPN client device and VPN server device. |
| Show IKE SA | Display the cookies and creation times of SAs (security associations) established during IKE phase 1 negotiations between a VPN client and VPN server. If there are no SAs, the negotiations were either incomplete or unsuccessful. Use this option to check the log messages for more details. |
| Show IP Routes | Display the IP routing table. |
| Show IPsec SA | Display the SAs established during IKE phase 2 negotiations between a VPN client and VPN server. |
| Show IPsec Tunnel | View details about the IPsec tunnel including the amount of traffic between the VPN client and servers. |
| Show Log | Display the event log for the device. |
| Show MAC Routes | Display the MAC routes table. |
| Show Memory | Display total, free, used, buffered, and cached memory. |
| Show Roaming Cache | Display the roaming cache, which contains MAC addresses and PMKs (pairwise master keys) for wireless clients and MAC addresses for the authenticating devices. This table also includes the user profile ID number of the client and details about the PMK. |
| Show Running Config | Display the configuration running on the device. |
| Show Startup Config | Display the configuration used by the device on reboot. |
| Show Version | Display the version running on the device. |

## VLAN Probe

The VLAN probe action locates available VLANs for the selected device. When the VLAN probe is complete, a table shows the host name, MAC address, available VLANs, unavailable VLANs, and their status.

**Note**
The VLAN Probe Utility is also available from the device list for a connected device.

Use this task to verify the VLAN probe results and status of VLAN for selected device.

1. Go to **Monitoring** > **Network Devices** > **Device Status**.
2. Select the check boxes for the devices you want to probe.

**Note**
You can select a single device or multiple devices to run the probe concurrently.

3. From the **3-dot Menu** (⋮) at the end of a device row, select **Utilities** > **VLAN Probe**.

4. Configure the VLAN Probe settings in Table 40.

**Table 40: VLAN Probe Settings**

| Field | Description |
|---|---|
| VLAN Range | The range of VLAN IDs to probe (1-4094). You can enter a single value or a range (for example, 1-100).<br>You can enter up to five ranges separated by commas. However, range numbers cannot overlap. For example, `1, 2-7, 8, 9-20`. |
| Timeout (optional) | The number of seconds to wait for a reply from each probe, from 1 to 60 seconds. Default is 5 seconds. |
| Probe Retries (optional) | The number of retry attempts for each probe, from 1 to 10. Default is 1. |

5. Select **Start** to start a probe.

   A progress bar indicates the status of the probe.
6. (Optional) Select **Stop** to stop a probe before it completes.

When the probe completes, the VLAN Probe Results appear. A timestamp indicates when they were last updated. A summary includes Status, Start Time, Duration, and device counts for Total, Passed, Failed, Stopped, and Running.

The results table lists all devices included in the VLAN probe and provides the Host Name, MAC Address, Available VLANs, Unavailable VLANs, and Status. To view detailed VLAN results for a specific device, expand its row in the Status column. A sub-table opens, showing the VLAN ID, Availability status, and IP Address for each probed VLAN.

## Override Supplemental CLI

Before you can configure Supplemental CLI access on a device, you must first enable Supplemental CLI. Go to **Administration & Settings** > **Global Settings** > **Backup & Restore**, and then enable **Supplemental CLI**.

You can save supplemental CLI objects that contain CLI commands and then automatically update devices each time you update the network policy. On the **Device** page, you can keep the supplemental CLI object in the network policy and append another supplemental CLI object to the end of the running configuration list. If the supplemental CLI is appended to the delta configuration and the supplemental CLI portion fails device update, only the supplemental CLI regenerates for subsequent device updates.

If you use CLI to manage features that are not configured in the user interface, you can choose to override the user interface (or to override the CLI), benefiting deployments that rely on overly complex CLI objects.

Use this task to override supplement CLI from network policy supplement CLI.

1. Go to **Monitoring** > **Network Devices** > **Device Status**.
2. Select ⋮ at the end of a device row, and then select **Configure** > **Device**.
3. Select **Override Supplement CLI from network policy Supplement CLI**.

4. Select an existing supplemental CLI object, or select to add, or to edit a supplemental CLI object. For more information, see Add a Supplemental CLI Object on page 145.
5. Select **Save Configuration**.

   For more information about how to push updated configuration to the device, see Push Device-Level Configuration on page 152.

**Note**
To avoid an unnecessary system reboot, select **Delta Configuration Update**. ExtremeCloud IQ (New) attempts to update only the configuration deltas. If a full update is required, the system prompts you to select **Complete Configuration Update**. For information about how the configuration push behaves with each **Activation Time** option, see Configuration Push Scheduling Behavior on page 154. Examples of CLI commands that require a full configuration update are: **`system antenna-type`** and **`system environment`**.

Related Links

Add a Supplemental CLI Object on page 145

*Add a Supplemental CLI Object*

Before you can use the supplemental CLI tool, you must first enable Supplemental CLI. Go to **Administration & Settings** > **Global Settings** > **Backup & Restore**, and then enable **Supplemental CLI**.

You can save supplemental CLI objects containing CLI commands, and ExtremeCloud IQ (New) can then automatically update them for devices, each time you update the network policy.

**Note**
- Limit CLI commands to configuration commands. Exclude **`Show`** or other commands used to display information.
- Do not use supplemental CLI commands to configure any settings set via the ExtremeCloud IQ (New) GUI as that creates a configuration sync conflict that results in future **`Device Update Failed`** errors.
- These commands work as a delta mechanism. Every new supplemental CLI update must only include new commands that you want to run, not ALL commands that you want to have present on the device at start up. Re-running some commands after already applied can cause future **`Device Update Failed`** errors.

Use the following task to create CLI objects.

1. Go to **Monitoring** > **Network Devices** > **Device Status**.
2. Select at the end of a device row, and then select **Configure** > **Device**.
3. Go to **Configure** > **Common Objects** > **Basic** > **Supplemental CLI Objects**.
4. Select **Override Supplement CLI from network policy Supplement CLI**.
5. To add or modify a supplemental CLI object, select to add, or to edit.
6. Enter a **Name** and an optional **Description**.

7. Enter the CLI commands.
   - Enter multiple CLI commands, one command per line, not exceeding a maximum total of 8192 characters. Limit CLI commands to configuration commands. Exclude Show or other commands used to display information.
   - You can use CLI commands that contain IP and VLAN objects: **`${ip:ip_object_name}`** and **`${vlan:vlan_object_name}`**.
   - You must perform a complete configuration update each time commands are appended to device configurations.
   - If supplemental CLI is added to device-level configuration, then device-level supplemental CLI takes precedence.
8. Select **SAVE** and perform a configuration update each time you append commands to device configurations.



**Note**
To avoid an unnecessary system reboot, select **Delta Configuration Update**. ExtremeCloud IQ (New) attempts to update only the configuration deltas. If a full update is required, the system prompts you to select **Complete Configuration Update**. For information about how the configuration push behaves with each **Activation Time** option, see Configuration Push Scheduling Behavior on page 154. Examples of CLI commands that require a full configuration update are: **`system antenna-type`** and **`system environment`**.

Related Links

Override Supplemental CLI on page 144

## AFC Geolocation Report

Generate and view the **AFC Geolocation Floor Report** to analyze anchor geolocation coordinates, per-AP location data, and ranging measurements for AFC-enabled access points.



**Note**
If the device has an AFC status of Pending, the AFC spectrum data may be incomplete.

Use this task to generate an AFC Gelocation Report for the selected device.

1. Go to **Monitoring** > **Network Devices** > **Device Status** > **AFC Wireless**.
2. Locate the target device in the device list and from the 3-dot menu (⋮) select **AFC Geolocation Report**.

   The **AFC Geolocation Floor Report** opens with the **Anchors** tab selected by default.
3. Select a subgraph from the **Subgraph** drop-down list to filter the report data for a specific subgraph.

   The selected subgraph applies to all three report tabs.

4. Navigate the report sections to view geolocation and ranging data:
   - Select **Anchors** to view geolocation coordinate data for anchor APs.

| Column | Description |
|---|---|
| **AP Hostname** | The hostname of the anchor AP. |
| **Status*** | The geolocation status of the anchor AP. |
| **Latitude** | The latitude coordinate of the anchor AP location. |
| **Longitude** | The longitude coordinate of the anchor AP location. |
| **Elevation Height** | The elevation height of the anchor AP, in meters. |
| **GPS Source*** | The source used to determine the GPS coordinates of the anchor AP. |

   * Select the filter icon (☰) in a column header to filter by available values.
   - Select **APs** to view per-AP geolocation data.

     The APs section displays the following information:

| Column | Description |
|---|---|
| **AP Hostname** | The hostname of the AP. |
| **Status** | The geolocation status of the AP.<br>* Select the filter icon (☰) next to the column header to filter by available values. |
| **Latidute** | The latitude coordinate of the AP location. |
| **Longitude** | The longitude coordinate of the AP location. |
| **Elevation Height** | The elevation height of the AP, in meters. |

   - Select **Ranging** to view ranging measurement data.

     The Ranging section displays the following columns:

| Column | Description |
|---|---|
| **Initiator** | The hostname of the device that initiated the ranging exchange. |
| **Responder** | The hostname of the device that responded to the ranging request. |
| **Distance** | The measured distance between the Initiator and Responder devices. |
| **Standard Deviation** | The standard deviation of the distance measurement, indicating measurement precision. |
| **Channel Width*** | The channel width used during the ranging exchange, displayed as a width value only (for example: 20 MHz or 89 MHz). |
| **Band*** | The radio frequency band used during the ranging exchange, displayed as a frequency value: 2.4 GHz, 5 GHz, or 6 GHz. |

* Select the filter icon ( ) in a column header to filter by available values.

To update the geolocation data used in the report, select **Derive GPS location** from the device 3-dot menu to recalculate the GPS coordinates for the device. For more information, see Device 3-Dot Menu Actions on page 134.

## Delete a Device from the Network

You can delete one or more devices from ExtremeCloud IQ (New). For wireless APs, you can optionally reset the device to its factory settings before deletion. Deletion is processed asynchronously; the inventory updates automatically when the operation completes.

**Note**
Devices that are disconnected from ExtremeCloud IQ Site Engine are considered orphaned devices. Extreme Cloud IQ (NEW) detects orphaned devices, displays them on the **Discovered** tab, and notifies Site Engine. You can remove orphaned devices from ExtremeCloud IQ (New) Inventory.

Use this task to delete one or more devices from the network.

1. Go to **Monitor** > **Network Devices**.
2. Select one or more devices from the device list.
3. To delete a single device, select the 3-dot overflow menu in the device row. To delete multiple devices, select the check box for each device, then select the **Actions** menu.
4. Select **Delete**.

   The **Delete Device(s)** dialog opens, showing the number of devices selected for deletion.
5. (Optional) To erase the device configuration before deleting it, select the **Delete Configuration** check box.

   **Note**
   The behavior of **Delete Configuration** varies by device type:
   - **Wireless AP—online (connected, not simulated)**: The system sends an erase configuration command to the device before deleting it. If the erase succeeds, the operation is reported as completed. If the erase fails but the deletion succeeds, the result is reported as partially completed.
   - **Wireless AP—offline or simulated**: The device is removed from inventory without erasing the configuration. The physical device may retain its configuration after deletion. The operation is reported as partially completed.
   - **Switches, routers, and other non-AP devices**: The device is removed from inventory. Erase configuration is not performed. The operation is reported as completed if the deletion succeeds.

6. Select **Delete** to confirm the deletion.

   **Note**
   To delete multiple devices, the **Delete Device(s)** dialog displays a 6-digit confirmation code. Enter the code in the fields provided, then select **Delete**. This step ensures that large bulk deletions are intentional and secure.

The deletion request is submitted. The system processes the deletion asynchronously. The **Network Devices** inventory list updates automatically when the operation completes. A notification appears to confirm the result. For more information, see Delete Device Status and Error Code Definitions on page 149.

**Note**
For bulk operations, the system processes devices in batches. The inventory refreshes progressively as each batch completes. If a deletion is only partially successful (for example, an AP was offline and could not be factory-reset), a notification indicates the partial result. The device is removed from the inventory even if the factory reset did not occur.

**Important**

- "Accepted" is not "Deleted": An ACCEPTED response means the platform received your request and will process it. The device is not yet removed. Wait for the final status to indicate deletion is complete.
- Delete Configuration does not guaranteed factory wipe: If an AP is offline, the platform cannot reach it to perform a reset. The device is still removed from cloud inventory, but the physical hardware may retain its configuration.
- Bulk deletes can have mixed results: In a batch of devices, some will succeed, while others may fail. Each device is processed independently within its batch.
- Progress is visible: For large bulk operations, you will see incremental progress updates as each batch of devices is processed, rather than waiting for the entire operation to finish.
- User interface refresh is automatic: After the final delete status is reached, the device inventory refreshes automatically. If a device still appears, allow a few seconds for the user interface to update.
- Timeouts are eliminated: The batch processing architecture uses a sliding timeout window (default 10 minutes), to prevent device operations from timing out.

*Delete Device Status and Error Code Definitions*

**Table 41: Delete Device Status Definitions**

| Status | Meaning | Customer Action |
|---|---|---|
| ACCEPTED | Request received and queued for processing. Deletion has **not** started yet. | Wait for the final status to indicate deletion is complete. |
| IN_PROGRESS | The deletion process is underway. | Monitor progress—no action needed yet. |
| COMPLETED | All selected devices were deleted successfully. | No action needed. |

**Table 41: Delete Device Status Definitions (continued)**

| Status | Meaning | Customer Action |
|---|---|---|
| PARTIALLY_COMPLETED | Devices were deleted with caveats (for example, AP deleted without erasing the configuration because it was offline). | Review per-device details. |
| FAILED | All delete actions failed (possible causes: devices not found, in active use, or insufficient permissions). | Review error codes and retry after resolving the issue. |

**Table 42: Delete Device Error Code Definitions**

| Error Code | Meaning | Customer Action |
|---|---|---|
| DELETE_FAILED | Device deletion failed. | Retry the operation. If persistent, contact support. |
| DEVICE_NOT_FOUND | The device does not exist in inventory. | Verify the device ID and check if it was already deleted. |
| DEVICE_IN_USE | The device has active connections. | Disconnect or decommission the device before retrying. |
| DEPENDENCY_EXISTS | The device has dependencies, such as policies or templates. | Remove dependent resources first, then retry. |
| RESET_FAILED | Factory reset command failed, but the device was deleted. | The device was removed from inventory. Manually factory-reset the physical device if needed. |
| INSUFFICIENT_PERMISSIONS | User does not have permission to delete. | Contact your administrator for elevated access. |

## Remove a Stack Member

Ensure the following before you begin:

- Your network includes at least one switch stack with two or more members.
- The stack parent (virtual device) row is visible in **Network Devices** > **Wired**.

Use this task to remove one or more member switches from a switch stack. Removing a member removes it from ExtremeCloud IQ (New) but does not physically disconnect it from the stack.

**Important**
You cannot remove the master switch using this action. The master switch row is not selectable in the **Remove Stack Member** dialog.

1. Go to **Monitoring** > **Network Devices** > **Device Status** > **Wired**.

2. Locate the stack parent device row in the device list.

   Stack devices are identified by the **Switch Stack** icon ( ) in the **Device Type** column. Select the expand arrow to view the individual stack member rows within the parent.

3. Select the **3-dot Menu** ( ) at the end of the stack parent device row, and then select **Remove Stack Member**.

   The **Remove Stack Member** dialog opens. The dialog displays a list of the stack member switches, including their slot/unit number, hostname, serial number, role, and status.

4. Select the check box for each stack member that you want to remove from the stack.
   - You can select one or more non-master members.
   - The master switch is not selectable.

5. Select **Remove**.

   The selected stack members are removed from ExtremeCloud IQ (New). A success message confirms that the operation is complete.

The removed switches are no longer managed by ExtremeCloud IQ (New). They remain physically connected to the stack but appear as unmanaged devices. To re-add a removed switch to ExtremeCloud IQ (New), onboard it as a new device. For more information, see Network Devices | Add Devices on page 129.

**Note**
If you remove a member accidentally, you can onboard it again without affecting the physical stack functionality.

## Replace a Stack Member

Ensure the following before you begin:

- The replacement switch is the same model as the switch being replaced.
- You have the serial number of the replacement switch available.

**Important**
Replacing a stack member may affect your licensing. Contact your account team to confirm whether a license transfer is required for the replacement switch.

Use this task to replace a failed or decommissioned switch in a stack with a new switch of the same model type.

1. Go to **Monitoring** > **Network Devices** > **Device Status** > **Wired**.
2. Locate the stack parent device row in the device list.

   Stack devices are identified by the **Switch Stack** icon ( ) in the **Device Type** column.

3. Select the **3-dot menu** ( ) at the end of the stack parent device row, and then select **Replace Stack Member**.

   The **Replace Stack Member** dialog opens.

4. From the **Member to Replace** list, select the stack member that you want to replace.

   After you make a selection, the **Current Serial Number** field populates automatically with the serial number of the selected member.

5. In the **New Serial Number** field, type the serial number of the replacement switch.

   The serial number is validated against the model of the switch being replaced. If the serial number is invalid or the model does not match, an inline error message displays.
6. Select **Replace**.

   A confirmation dialog opens, prompting you to confirm the replacement.
7. In the confirmation dialog, select **Replace** to confirm the replacement, or select **Cancel** to return to the previous dialog without making changes.

   ExtremeCloud IQ (New) updates the stack record to associate the new switch serial number with the slot. A success message confirms that the replacement is complete.

The stack member record in ExtremeCloud IQ (New) is updated to reflect the replacement switch. Verify that the new switch appears correctly in the stack member list under the stack parent device.

**Note**
After the replacement is complete, verify the licensing status of the replacement switch with your account team.

## Push Device-Level Configuration

Use this task to update configuration settings to an individual network device. This process allows device-specific update parameters to be configured and pushed directly from the **Device Status** page.

1. Go to **Monitoring** > **Network Devices** > **Device Status**.
2. Select ⋮ at the end of a device row, and then select **Configure** > **Device**.
3. Select **Update** and configure the **Device Update** settings for the selected device.

**Note**
Update is only available when there are changes available to push to the device.
When you select **Activate/reboot on this schedule** under **Activation Time**, the configuration push and device reboot are deferred until the scheduled date and time. The device status displays **Scheduled** until the push completes. For more information, see Configuration Push Scheduling Behavior on page 154.

**Table 43: Update Wired Device Settings**

| Field |
|---|
| **Update Network Policy and Configuration** |
| Reboot and revert Extreme Networks switch configuration if IQAgent is unresponsive after configuration update. |
| Perform delta configuration update and resolve local device configuration which is out of sync with ExtremeCloud IQ (New). |

**Table 44: Update Wireless Device Settings**

| Field | |
|---|---|
| **Update Network Policy and Configuration** | |
| Delta Configuration Update | Updates only the device delta configuration changes for the selected device. This action avoids a device reboot. |
| Complete Configuration Update | Performs a full configuration push for the selected device, replacing its entire configuration with the settings defined in ExtremeCloud IQ (New) (including the assigned Network Policy and device-level overrides). This action requires a device reboot. For information about how the configuration push behaves with each **Activation Time** option, see Configuration Push Scheduling Behavior on page 154.<br><br>**Note:** Only supported on devices running HOS or IQ Engine Firmware.<br><br>**Note:** ExtremeCloud IQ (New) automatically forces a Complete Configuration Update when the tunnel destination assigned to an access point changes to a different destination. A **Complete Configuration Update** purges and reboots the device. |
| **Activation Time for Extreme Networks Devices Running Images:** | |
| Activate at next reboot (requires rebooting manually) | The configuration is pushed to the device immediately. The device status displays **Pending** until the device is manually rebooted. After the reboot, the device status changes to **Complete**. |

**Table 44: Update Wireless Device Settings (continued)**

| Field | |
|---|---|
| Activate after xx seconds | The configuration is pushed to the device immediately. The device reboots automatically after the specified delay in seconds. The device status displays **Pending** until the reboot completes. |
| Activate/reboot on this schedule based on your local system time | The configuration push and device reboot are deferred until the specified date and time. The device status displays **Scheduled**. Hover over **Scheduled** to view the date and time. After the scheduled push and reboot complete, the device status changes to **Complete**. |

4. To update the selected device immediately, select **Perform Update**. To keep these settings for future use, select **Save as Defaults**.

   The device status in the device list updates based on the selected activation time:

   - **Pending**: The configuration is pushed and awaiting a device reboot.
   - **Scheduled**: The push is deferred to the scheduled date and time. Hover to view the schedule.
   - **Complete**: The push and reboot are complete.

## *NEW!* Configuration Push Scheduling Behavior

When you select **Complete Configuration Update** and choose an **Activation Time** option, the configuration push and device reboot occur according to the schedule you specify.

The **Activation Time** option controls when the configuration is pushed to the device and when the device reboots to activate the new configuration. The configuration status in the device list reflects the current state of the scheduled push.

**Activate at next reboot (requires rebooting manually)**

The configuration push completes immediately. The device status displays **Pending** until the device is manually rebooted and the configuration is activated.

**Activate after *xx* seconds**

The configuration push completes immediately. The device reboots automatically after the specified delay. The device status displays **Pending** until the reboot completes and the configuration is activated.

**Activate/reboot on this schedule based on your local system time**

The configuration push and device reboot are both deferred until the specified date and time. The device status displays **Scheduled**. Hovering over the **Scheduled** status displays

the scheduled date and time. After the scheduled push and reboot complete, the device status changes to **Complete**.

**Note**
The configuration status column in the device list displays one of the following values:

- **Pending**: The configuration has been pushed and is waiting for the device to reboot.
- **Scheduled**: The configuration push is scheduled for a future date and time. Hover over the status to view the scheduled date and time.
- **Complete**: The configuration push and device reboot are complete.

## Packet Capture

The Packet Capture utility enables you to capture wireless and wired traffic on a per-AP basis for advanced troubleshooting. You can configure capture filters by band, SSID, interface, VLAN, client, protocol, and traffic direction, and save the resulting capture file to ExtremeCloud IQ (New) or upload it directly to CloudShark for analysis. Packet Capture is accessible from the Utilities menu in the device 3-dot menu.

**Note**
Packet Capture is only available for wireless AP devices. The Packet Capture dialog window displays the AP name as a subtitle to confirm which device the capture is running on.

After one or more packet capture sessions have completed, you can view the available results and download capture files from the Device Status page. For more information, see View Packet Capture Results on page 158.

### Run a Packet Capture Session

Use this task to configure and start a new packet capture session on a selected AP.

1. Go to **Monitoring** > **Network Devices** > **Device Status** > **Wireless**.
2. At the end of a device row, select the 3-dot menu, and then select **Utilities** > **Packet Capture**.
3. Select a tab to configure the type of capture:
   - **General**: Configure wireless and wired capture settings, traffic filters, capture duration, and CloudShark upload option.
   - **Security**: Configure a security-focused capture with MAC address filtering, network location scope, and a shorter time duration.
4. Configure the capture settings:
   - General Packet Capture Settings
   - Security Packet Capture Settings

5. Select **Run**.

**Note**
To close the dialog without starting a capture, select **Cancel**.

After a capture session completes, you can view the results and download the capture file. Selecting **View Results** from the Packet Capture dialog, or re-opening **Utilities** > **Packet Capture** on an AP that has an existing capture, opens the results view.

The results view displays the following information:

- **Last captured at**: The date and time the most recent capture completed (for example, December 18, 2023 4:32PM).
- **Packet Capture**: A card showing the capture status and a message confirming whether the capture was successful and data is available for export.

From the results view, you can:

- Select **Download** to download the capture file.

**Note**
If you selected the `Upload to CloudShark` option when starting the capture, the file is also available directly in CloudShark after the capture completes.

- Select the **delete icon** to delete the capture session and its associated file. Confirm the deletion when prompted.

**Important**
Deletion is permanent. Deleted packet capture sessions and their files cannot be recovered.

- Select **Cancel** to close the dialog.

*Packet Capture Settings*

**Table 45: General Packet Capture Settings**

| Field | Description |
|---|---|
| **Wireless**<br>Select to enable wireless traffic capture. When the check box is selected (enabled by default), the wireless packet capture settings are active. Clear the check box to disable wireless packet capture. | |
| Band / Interface | Select the capture scope for the wireless interface:<br>• **Band**: Captures traffic across a selected wireless band. When selected, the **Select Bands** and **SSID** fields are available.<br>• **Interface**: Captures traffic on a specific wireless interface (for example, Wi-Fi0, Wi-Fi1, Wi-Fi2, or Wi-Fi3). When selected, an interface selector replaces the Band and SSID fields. |

**Table 45: General Packet Capture Settings (continued)**

| Field | Description |
|---|---|
| Select Bands | Select the wireless band to capture:<br>• All (default)<br>• 2.4 GHz<br>• 5 GHz<br>• 6 GHz<br><br>**Note:** Available when **Band** is selected. |
| SSID | Select the SSID to filter captured wireless traffic:<br>• **All** (default): Captures traffic across all SSIDs.<br>• **Specific SSID**: Select from the available SSIDs on the AP.<br><br>**Note:** Available when **Band** is selected. |
| Filters | Select the types of wireless frames to include in the capture (multiple filter types can be selected):<br>• Management<br>• Data<br>• Control<br><br>If no filter is selected, all frame types are captured. |
| Direction | Select the direction of wireless traffic to capture:<br>• Both (default)<br>• Rx (inbound)<br>• Tx (outbound) |
| Clients | Select specific client MAC addresses to filter the wireless capture. Multiple clients can be selected. If no clients are selected, traffic from all clients is captured. |
| VLANs | Enter one or more VLAN IDs to filter captured wireless traffic to specific VLANs. Supports ranges and lists (for example: 2,4,5-10). |
| Protocol | Select the network protocol to filter captured wireless traffic:<br>• **Any** (default): Captures all protocols.<br>• **Specific protocol**: Select from the available protocols. |
| **Wired**<br>Select to enable wired traffic capture. When the check box is selected (enabled by default), the wired capture fields are active. Clear the check box to disable wired capture. | |
| Interface | Select the wired interface on the AP to capture traffic from:<br>• eth0 (default)<br>• Additional interfaces if available on the AP |
| Filters | Select the types of wired traffic to include in the capture. Multiple filter types can be selected. If no filter is selected, all traffic types are captured. |

**Table 45: General Packet Capture Settings (continued)**

| Field | Description |
|---|---|
| Direction | Select the direction of wired traffic to capture:<br>• Both (default)<br>• Rx (inbound)<br>• Tx (outbound) |
| Clients | Select specific client MAC addresses to filter the wired capture. Multiple clients can be selected. If no clients are selected, traffic from all clients is captured. |
| VLANs | Enter one or more VLAN IDs to filter captured wired traffic to specific VLANs. Supports ranges and lists (for example: 2,4,5-10). |
| Protocol | Select the network protocol to filter captured wired traffic:<br>• **Any** (default): Captures all protocols.<br>• **Specific protocol**: Select from the available protocols. |
| **Capture Settings** | |
| Duration | Enter the maximum duration for the capture session in seconds. The minimum value is 5 seconds and the maximum is 604800 seconds (7 days). The default value is 60 seconds. The capture stops automatically when the duration expires. |
| Upload to CloudShark | Select this check box to automatically upload the completed capture file to CloudShark for analysis. |

**Table 46: Security Packet Capture Settings**

| Field | Description |
|---|---|
| Any MAC Address | Select this check box to capture traffic from any MAC address. When selected (default), no MAC address filter is applied. Clear the check box to restrict the capture to specific MAC addresses. |
| Network Location(s) (optional) | Select one or more network locations to filter the capture to traffic associated with those locations. If no location is selected, the capture is not filtered by location. |
| Sites | Select one or more sites to associate with the capture session. Multiple sites can be selected. This field works in conjunction with the Network Location(s) field to further scope the capture. |
| Time Duration (5-30 minutes) | Enter the duration for the Security capture in minutes. The minimum value is 5 minutes and the maximum is 30 minutes. The default value is 5 minutes. |

## View Packet Capture Results

After one or more packet capture sessions have completed, you can view the available results and download capture files from the Device Status page.

Use this task to view available packet capture results.

1. Go to **Monitoring** > **Network Devices** > **Device Status**.
2. Select **Packet Capture Results** on the content pane on the right.

   The **Packet Capture Results** window displays a list of available capture sessions. Packet capture result details include:

   - **Session Name**: The name assigned to the capture session.
   - **Status**: The current status of the capture session.
   - **Host Name**: The host name of the AP on which the capture was run.
   - **Interface**: The AP interface(s) targeted by the capture session.
   - **Location**: The physical location of the AP.
   - **Start Time**: The date and time the capture session started.
   - **End Time**: The date and time the capture session ended.
3. To download one or more capture files, select the check box next to one or more sessions, and then select **Download**.

## Configure Devices

To configure a device:

1. Go to **Monitoring** > **Network Devices** > **Device Status** page. Select **All Devices** or one of the following tabs:

   - **Wired** — Displays wired devices managed by ExtremeCloud IQ (New).
   - **Wireless** — Displays wireless access points and associated devices.
   - **AFC Wireless** — Displays wireless devices operating in Automated Frequency Coordination (AFC) mode.
   - **Appliances** — Displays ExtremeCloud Site Engine devices, ExtremeCloud IQ Controller, and Tunnel Concentrator.
   - **Discovered** — Displays devices managed through ExtremeCloud Site Engine.

   **Note**
   To configure Tunnel Concentrator device settings, select the **Appliances** tab.
2. At the end of a device row, select the **3-dot Menu**(⋮), and then select **Configure** > **Device**.

   **Note**
   To configure fabric settings for devices running Fabric Engine, select **Configure** > **Fabric**.

For more information, see Configure Wired Devices, Configure Fabric Settings, Configure Wireless Devices, and Configure Tunnel Concentrator Devices.

**Note**
Configuration actions are available only for connected devices. Devices that are not connected cannot be configured.

## Configure Wired Devices

The following configuration options are offered on the 3-dot menu for each wired device.

Select ⋮ > **Configure** > **Device**.

- Device Configuration: Edit device details such as the host name, the description, the device function, IP addresses, and VLAN assignments.
- Device Management Servers: Edit management server settings for a device associated with a network policy.
- Port/VLAN Configuration: Edit switch ports, STP, Storm Control, PSE, and VLAN attributes.

  **Note**
  Fabric Engine devices support EAPoL, SLPP, and VLAN/ISID configuration with VLAN attributes.

- Device Credentials: Assign or change network administrator credentials and administrator assignments.
- Interface Configuration: Add, edit, or delete interface configurations.
- Routing Configuration: Configure IP4 Static Routes.

After you make changes to the configuration, you must push the configuration changes to the device.

*Wired Device Configuration*

Making device configuration changes at the wired device level overrides the equivalent settings in the network policy assigned to the device, after you push the updated configuration to the device.

Use this task to make device configuration changes at the device level.

1. Go to **Monitoring** > **Network Devices** > **Device Status**.
2. Select ⋮ at the end of a device row, and then select **Configure** > **Device**.
3. Under the **Configuration** menu, select **Device Configuration**.
4. Configure the **Device Details**:
   - **Host Name**: Enter a unique host name for the device. It can contain up to 32 characters and can include spaces.
   - **SNMP Location**: Enter a location name, for example `headquarters, building 1`.
5. Configure the **Network Details**:
   - **Network Policy**: Select a network policy from the drop-down list of existing policies.
   - **Device Template**: Select a device template from the drop-down list of existing templates, or clone an existing template.

     **Note**
     Fabric Engine devices do not support device templates.

6. Toggle **Management Interface Settings** to **On** or **Off**.

   When enabled, management interface settings specified below are applied and override template-level management interface settings. If disabled, you can apply template settings, or the device will use manually configured management interface settings. Leave disabled when using **Out-Of-Band Management**.

   - **VLAN Interface**: Select when the management interface is to be supplied by the management VLAN.
     - **Management VLAN**: Enter the VLAN to be used by the switch.
     - **Management IP Settings**: Select **Static Address** or **Dynamic Address Configuration (DHCP) Client** to enable DHCP on this interface.
7. (Optional) Configure **Supplemental CLI**:
   a. **Apply Supplement CLI from network policy switch template**: Include the supplemental CLI object in the network policy and append the selected CLI object from the list. If you select a supplemental CLI object from the list, or create a new one, it is appended to the end of the configuration list, after the supplemental CLI object in the network policy.
   b. **Override Supplement CLI from network policy Supplement CLI**: Enable the network policy to override supplemental CLI objects for the device. For more information, see Override Supplemental CLI on page 144.

   **Note**
   Fabric Engine only supports Supplemental CLI from device-level configuration.

   **Important**
   Before you can configure Supplemental CLI access on a device, you must first enable Supplemental CLI. Go to **Administration & Settings** > **Global Settings** > **Backup & Restore**, and then enable **Supplemental CLI**.

8. Select **Save Configuration**.

   For more information about how to push updated configuration to the device, see Push Device-Level Configuration on page 152.

Related Links

Device Management Servers on page 161
Configure Wired Devices on page 160

*Device Management Servers*

The **Device Management Servers** page does not appear until you apply a network policy to the device.

Use this task to override a network policy and make device-level changes to management server settings for a device. The changes affect only the specific device, not all devices associated with the network policy. You must **Unlock** before you can configure and save a device level management server configuration. You can use **Revert** to restore the network policy configuration and overwrite any changes made at the device level.

For stacks, the unlock and revert action applies to all units/slots within the page. This enables the full stack to revert to the currently assigned network policy. Also, the **Device Management Servers** is not available until you apply the network policy to both single switches and stacks.

1. Go to **Monitoring** > **Network Devices** > **Device Status**.
2. Select ⋮ at the end of a device row, and then select **Configure** > **Device**.

   **Note**
   This action is available only for managed devices. If the device is not currently managed, to change the management status of the device, select **Change Management Status** > **Manage**.

3. Under the **Configuration** menu, select **Device Management Servers**.
4. Select **Unlock** from the top banner.
   Changes saved after you unlock the device override the associated network policy.
5. Select each server tab to make any necessary changes to the server settings:
   - DNS Server
   - NTP Server
   - SNMP Server
   - Syslog Server
   - RADIUS Server (Fabric Engine devices only)

   **Note**
   DNS Server, NTP Server, SNMP Server, and Syslog Server configurations can be managed at the device level for Switch Engine/EXOS and Fabric Engine/VOSS after unlock. Not all management server tabs are available for all device types. EXTREME PLATFORM ONE RADIUS and EXTREME PLATFORM ONE RADIUS Proxy Servers are supported only for Fabric Engine devices under device management servers. The **RADIUS Server** tab provides a **Use Extreme Platform ONE Security RADIUS Cloud Configuration** toggle.

6. Select **SAVE CONFIGURATION**.
   The changes only apply at the device level.

   For more information about how to push updated configuration to the device, see Push Device-Level Configuration on page 152.

Related Links

Configure Switch Ports and VLAN on page 165
Configure Wired Devices on page 160

#### Device Management Server Settings

1. Go to **Monitoring** > **Network Devices** > **Device Status**.
2. Select ⋮ at the end of a device row, and then select **Configure** > **Device**.
3. Under the **Configuration** menu, select **Device Management Servers**.
4. Select **Unlock** to enable switch-level configuration changes.

**DNS Server Settings**

5. Select **DNS Server**.
6. Toggle **DNS Server** to **ON**.

   **Note**
   Use DNS Server for domain name-to-IP address resolution. Extreme Networks devices that are DHCP clients can receive a domain name and DNS Server IP Address through DHCP, although any DNS settings that you enter here override those dynamically applied.

7. Enter a **Domain Name** for the default DNS server.
8. To add a new DNS server, select , and then:
   a. Enter an **IP Address** for the DNS server.
   b. Select a **Routing Instance**.
   c. Select **ADD**.

   You can add up to three servers. The first entry is the primary server. The secondary entry is the secondary server, and the third entry is the tertiary server. Use the arrows in the **Order** column to change the order.
9. To delete a DNS server from the list, select the DNS servers, and then select (delete).

**NTP Server Settings**

10. Select **NTP Server**.
11. Toggle **NTP Server** to **ON**.

    **Note**
    When enabled, Extreme Networks devices synchronize their time with specified servers. Devices use a manually set time if synchronization is disabled. Fastpath and X435 switches support SNTP, but do not support NTP. Use an NTP server with an IP Address instead of a Fully Qualified Domain Name for VOSS platforms.

12. To add a new NTP server to the list, select .
    a. Enter an **NTP Server**.
    b. Select a **Routing Instance**.
    c. Select **ADD**.
13. To delete an NTP server from the list, select the NTP servers, and then select (delete).

**SNMP Server Settings**

14. Select **SNMP Server**.
15. Toggle **SNMP Server** to **ON**.
16. Enter an **SNMP Contact** for the default SNMP server.
17. Select an existing SNMP server, and then select , or to add a new one, select .

18. Configure the following SNMP server settings, and then select **ADD SNMP SERVER**:

**Table 47: Settings for SNMP servers**

| Setting | Description |
|---|---|
| SNMP Server | Type a name for the server. |
| Version | From the drop-down list, select the version of SNMP that is running on the management station that you intend to use. |
| Operation | Select the type of activity to permit between the specified SNMP management station and the devices in the network policy to which you will assign this profile. Options include:<br>• **None**: Disable all SNMP activity for the specified management station.<br>• **Get**: Permit GET commands sent from the management station to a device to retrieve MIBs.<br>• **Get and Trap**: Permit the reception of GET commands from the management station and the transmission of traps to the management station.<br>• **Trap**: Permit devices to send messages notifying the management system of events of interest. |
| Community | For SNMP V2C and V1, enter a text string that must accompany queries from the management station. The community string acts similarly to a password, such that devices accept queries only from management stations that send the correct community string. |
| Routing Instance | Select the SNMP server routing instance. |

**Note**
Use the arrows in the **Order** column to change the order.

19. To delete an SNMP server from the list, select the SNMP servers, and then select (delete).

**Syslog Server Settings**

20. Select **Syslog Server**.
21. Toggle **Syslog Server** to **ON**.

**Note**
When enabled, Extreme Networks devices save the event log entries to the Syslog servers specified.

22. Select a **Syslog Facility**.
23. To add a new Syslog server, select , and then:
    a. Enter a **Syslog IP Address** for the Syslog server.
    b. Select a **Severity** level.
    c. Type the **Port** number.

d. Select a **Virtual Routing** instance.
e. Select **ADD**.

**Note**
Use the arrows in the **Order** column to change the order.

24. To delete a Syslog server from the list, select the Syslog servers, and then select (delete).

**RADIUS Server Settings**

25. Select **RADIUS Server**.
26. Toggle **RADIUS Server** to **ON**.
27. Select one of the following options:

- **Use Extreme Platform ONE RADIUS Cloud Configuration**: Enables the device to use the cloud-based RADIUS configuration provided by UZTNA for authentication.

  **Note**
  UZTNA is provisioned through the UZTNA application. If UZTNA settings or license is not properly configured, then device authorization may fail.

- **Use UZTNA RADIUS Proxy Servers**: Enables the device to route RADIUS authentication requests through UZTNA proxy servers for secure handling and centralized control. Select the **Primary RADSEC Proxy Server** and the **Secondary RADSEC Proxy Server**.

Related Links

Device Management Servers on page 161

*Configure Switch Ports and VLAN*

You can configure switch port configuration details and settings at the device level. Switch-level settings always override any port configuration settings that were made in the device template for a network policy. You must first **Unlock** this page to change the switch-specific port configuration. You can also return to the original template configuration with the **Revert** option.

**Note**

- Only the options available to the specific switch are displayed.
- For 5520/5720 Universal Switches, VIM and partition mode are configurable at the device level.
- LLDP/CDP, MAC locking, STP Priority, BPDU Restrict, BPDU Restrict Recovery, Forwarding Delay, VLAN Attributes, and Max Age are configurable at the device level.
- BPDU Restrict and BPDU Recovery settings are found within the STP tab.

1. Go to **Monitoring** > **Network Devices** > **Device Status**.
2. Select at the end of a device row, and then select **Configure** > **Device**.
3. Under the **Configuration** menu, select **Port / VLAN Configuration**.

4. Select **Unlock** to enable switch-level configuration changes.

   **Note**
   Changes made after unlocking the device will override network policy and switch template configuration.

5. Select each tab, and edit any accessible field.
   - Port Details
   - Port Settings & Aggregation
   - Instant Secure Port Settings
   - STP
   - Storm Control
   - MAC Locking
   - Voice
   - PSE - Power Sourcing Equipment
   - ELRP - Extreme Loop Recovery Protocol
   - VLAN Attributes
   - SLPP - Simple Loop Prevention Protocol (Fabric Engine only)
   - EAPoL - Extensible Authentication Protocol over LAN (Fabric Engine only)
6. Select **Save Port Configuration**.

   **Note**
   BPDU Restrict and BPDU Restrict Recovery Timeout settings are found within the STP settings.

   For more information about how to push updated configuration to the device, see Push Device-Level Configuration on page 152.
7. To revert back to the network policy switch template, select **Revert to Network Policy**.

Related Links

Configure Wired Device Credentials on page 181
Configure Wired Devices on page 160

**Port/VLAN Configuration Settings**

**Table 48: Port Details**

| Field | Description |
|---|---|
| EDIT | Edit multiple ports at once. Select the ports, then select **EDIT** to apply bulk changes. |
| Instant Profile | 1. Select  to choose an existing instant profile.<br>2. To create a new instant profile, select , and then select Instant Port Profile or Instant Secure Port Profile.<br>3. Select **SAVE**.<br><br>**Note:** Not supported on Fabric Engine devices. |
| IGMP Settings | Toggle to **ON** to enable the switch to identify ports to which multicast group member hosts are attached to optimize the distribution of multicast traffic.<br>When enabled, the following options are available (not supported on Fabric Engine devices):<br>• **Enable immediate leave**: Instructs the switch to remove a multicast host from the multicast forwarding table immediately upon receipt of a leave-group-membership message.<br>• **Suppress redundant IGMP membership reports to optimize traffic**: Suppresses redundant IGMP membership reports from multiple hosts on a subnet. The switch sends a single report to the IGMP router, reducing traffic. |
| DHCP Snooping (non-Fabric Devices) | Toggle **DHCP Snooping** to **ON**, to enable snooping of DHCP packets and create a DHCP bindings database of IP to MAC addresses for static and dynamic VLANs.<br>Optionally, select **Enable drop rogue DHCP Packets action for static and dynamic VLANs**. Ports configured as trusted will not apply drop action. By default, port types configured as Trunk Port will be trusted.<br><br>**Note:** If VLAN attributes has enabled DHCP Snooping settings, then the VLAN attributes will override the switch template. |

**Table 48: Port Details (continued)**

| Field | Description |
|---|---|
| DHCP Snooping Global Enable (Fabric Device Only) | Toggle to **ON** to enable DHCP Snooping.<br><br>**Important:** When DHCP Snooping is enabled, it may disrupt connectivity for authorized DHCP servers connected to a switch port or an uplink port currently in use. Select **YES** to confirm. |
| Interface | The port or interface identifier on the switch. |
| Instant Profile Status | Indicates if an instant profile is applied to the port. |
| Port State | Indicates the current operational state of the port (ON or OFF). |
| LACP | Indicates if Link Aggregation Control Protocol (LACP) is enabled for the port. |
| Auto-Sense (Fabric Engine only) | Indicates whether Auto-Sense is enabled, allowing the port to automatically detect and configure its role based on the connected device type. |
| Port Type & VLAN | Specifies the port type (access or trunk) and associated VLAN configuration.<br><br>To create a new port type, select . For more information, see Create a New Port Type on page 427. |
| VLAN | Lists the VLAN assigned to the port. |
| DHCP Snooping Trusted Port | Indicates if the port is trusted for DHCP snooping to allow DHCP server responses. |
| Description | A description or label for the port. |

**Table 49: Port Settings & Aggregation**

| Field | Description |
|---|---|
| EDIT | Edit multiple ports at once. Select the ports, then select **EDIT** to apply bulk changes. |
| MTU Settings | Set the maximum transmission unit value for Ethernet interfaces. The MTU value determines the largest packet size that can be transmitted through your system. |

**Table 49: Port Settings & Aggregation (continued)**

| Field | Description |
|---|---|
| LLDP Settings | Set the following LLDP settings:<br>• **Advertisements Interval**: The number of seconds between LLDP advertisements sent to neighboring network devices.<br>• **Timer Hold**: Specifies how long neighboring devices retain LLDP information. The value is multiplied by the advertisement interval to determine the LLDP time-to-live (TTL). (EXOS/ Switch Engine, VOSS/Fabric Engine, SR22XX/23XX, Dell)<br>• **LLDP Initialization Delay Time**: The length of time that you want the interface to wait before initializing LLDP.<br>• **Fast start repeat count**: The number of advertisement LLDP frames to send when the connected device is detected. |
| Aggregate Selected Ports | Select two or more ports of the same type that you want to aggregate, and then select **Aggregate Selected Ports**. For more information, see Aggregate LAG and LACP Ports on page 437.<br><br>**Note:** You can only aggregate ports when you configure in bulk. |
| Interface | The port or interface identifier on the switch. |
| Transmission Type | Set the **Transmission Type**:<br>• **Auto**: Selecting Auto causes the switch to negotiate the best possible duplex mode possible with the connected device.<br>• **Full-Duplex**: Selecting Full-Duplex forces the switch to communicate with the connected device using full-duplex communication.<br>• **Half-Duplex**: Selecting Half-Duplex forces the switch to communicate with the connected device using half-duplex communication. |
| Speed | Select the speed the port uses to communicate with the connected device. |
| Flow Control | Select how to manage the receive transmission speed, which enables a feedback mechanism between a transmitting port and the receiving port on the switch. |
| LLDP—Transmit | Enables the switch to transmit Link Layer Discovery Protocol Data Unit (LLDPDU) frames. |

**Table 49: Port Settings & Aggregation (continued)**

| Field | Description |
|---|---|
| LLDP—Receive | Enables the switch to receive LLDPDU frames. |
| LLDP MED Capabilities | Enables LLDP-Media Endpoint Discovery. |
| CDP | Enables the switch to receive and parse the information within Cisco CDP frames. |
| Client Reporting | Enables collection and reporting of learned MAC addresses for the port. |

**Table 50: Instant Secure Port Settings**

| Field | Description |
|---|---|
| EDIT | Edit multiple ports at once. Select the ports, then select **EDIT** to apply bulk changes. |
| Interface | The port or interface identifier on the switch. |
| User Auth | Toggle to **ON** to enable user authentication. |
| MAC Auth | Toggle to **ON** to enable MAC authentication. |

**Table 51: STP**

| Field | Description |
|---|---|
| Enable STP | Toggle to **ON** to enable STP and configure the settings for the device.<br><br>**Note:** Not applicable to Auto-Sense ports on Fabric Engine devices. |
| EDIT | Edit multiple ports at once. Select the ports, then select **EDIT** to apply bulk changes. |
| STP for Device | Configure STP settings for the device. For more information, see Configure STP Settings on page 433.<br><br>**Note:** If Spanning Tree Mode is set to STP, then port priority should be set to either 0 or 16. Any greater value will be ignored and the default STP (802.1D) port priority of 16 will be used. |
| Interface | The port or interface identifier on the switch. |
| STP Status | Toggle **ON** to enable STP for the port. |
| Edge Port | Connects to a user terminal or server, instead of other switches or shared network segments. A port configured as an edge port will not cause a loop upon network topology changes. |

**Table 51: STP (continued)**

| Field | Description |
|---|---|
| BPDU Protection | Use the drop-down list to change BPDU protection to guard or filter status:<br>• **Guard**: Controls whether a port explicitly configured as Edge will disable itself upon reception of a BPDU. The port will enter the error-disabled state, and will be removed from the active topology.<br>• **Disabled**: Turns off BPDU Protection. |
| BPDU Restrict | Toggle the switch to **ON** to enable BPDU Restrict.<br><br>**Note:** Not supported on Fabric Engine devices. |
| BPDU Recovery Timeout | Input a BPDU recovery timeout time between 60-600 seconds. |
| Priority | When this port is an STP edge port, select a port priority for STP from the drop-down list. |
| Path Cost | Enter the Path Cost (bandwidth) for this port. |

**Table 52: Storm Control**

| Field | Description |
|---|---|
| EDIT | Edit multiple ports at once. Select the ports, then select **EDIT** to apply bulk changes. |
| Interface | The port or interface identifier on the switch. |
| Broadcast | Select to include traffic that is forwarded to all destinations simultaneously. |
| Unknown Unicast | Select to include traffic whose destination address does not appear in the forwarding database. |
| Multicast | Select to include traffic whose destination is a multicast address. |
| Rate Limit Type | PPS (packets per second) is the default rate limit type. |
| Value | Enter when the switch should discard traffic of the selected types. |

**Table 53: MAC Locking**

| Field | Description |
|---|---|
| Enable MAC Locking | Toggle to **ON** to enable MAC locking. |
| EDIT | Edit multiple ports at once. Select the ports, then select **EDIT** to apply bulk changes. |

**Table 53: MAC Locking (continued)**

| Field | Description |
|---|---|
| Interface | The port or interface identifier on the switch. |
| MAC Locking | Toggle **ON** to enable MAC locking for the port. |
| Max First Arrival Limit | Set the Maximum First Arrival Limit for the port. Select  to revert to the original network policy settings. |
| Disable Port | Toggle **ON** to disable the port. |
| Link Down Action | Specify the Link Down Action for the port.<br>By default, Link Down Action is set to clear first arrival MACs, with the option to retain MACs. |
| Remove Aged MACs | Toggle **ON** to remove MACs when they are aged out for the port. |

**Table 54: Voice**

| Field | Description |
|---|---|
| EDIT | Edit multiple ports at once. Select the ports, then select **EDIT** to apply bulk changes. |
| Interface | The port or interface identifier on the switch. |
| LLDP Voice Advertisements | Toggle to **ON** to enable LLDP to advertise voice VLAN information to connected devices for VoIP configuration. |
| 802.1 VLAN and Port Protocol | Select to configure IEEE 802.1 standards for VLAN tagging and port protocol identification for voice traffic. |
| Med Voice VLAN DSCP Value | Type the DSCP (Differentiated Services Code Point) value for voice media traffic to prioritize audio streams. |
| Med Voice Signaling DSCP Value | Type the DSCP value for voice signaling traffic to ensure call setup and control messages are prioritized. |
| CDP Advertisements | Toggle to **ON** to enable Cisco Discovery Protocol advertisements to share voice VLAN and device information with connected endpoints. |

**Table 54: Voice (continued)**

| Field | Description |
|---|---|
| CDP Voice VLAN | Specifies the voice VLAN ID communicated through CDP for VoIP devices. |
| CDP Power Available | Indicates the amount of PoE (Power over Ethernet) available on the port, advertised via CDP for powered devices. |

**Table 55: PSE**

| Field | Description |
|---|---|
| EDIT | Edit multiple ports at once. Select the ports, then select **EDIT** to apply bulk changes. |
| PSE Settings for Device | Select to set maximum power thresholds to send alerts to ExtremeCloud IQ (New) when exceeding maximum power levels. |
| Interface | The port or interface identifier on the switch. |
| POE | Toggle to **ON** to enable POE on the port. |
| PSE Profile | Select  to choose an existing PSE profile.<br>To create a new PSE profile, select . For more information, see Configure PSE on page 435. |
| Power Mode | The POE power mode.<br>802.3af (PoE) can deliver 15.4 watts over Cat5 cables. 802.3at (PoE+) can deliver up to 30 watts over Cat 5 cables with 25.5 watts available to devices. |

**Table 55: PSE (continued)**

| Field | Description |
|---|---|
| Power Limit (mW) | The available PoE power limit. |
| Priority | The power output priority:<br>• **Low**: If the total powered device (PD) power consumption exceeds the PSE power budget, power output is modified to bring the total consumption back to within the PSE power budget.<br>• **High**: When the total PD power consumption exceeds the PSE power budget, power output is modified only after ports with low priority PSE profiles are regulated.<br>• **Critical**: When the total PD power consumption exceeds the PSE power budget, power output is shut down last. |

**Table 56: ELRP**

| Field | Description |
|---|---|
| EDIT | Edit multiple ports at once. Select the ports, then select **EDIT** to apply bulk changes. |
| ELRP Settings | Configure ELRP settings for the device:<br>• Toggle **Enable ELRP**.<br>• Select the **Enable ELRP for dynamically created VLAN(s)** check box.<br>• Toggle **Configure ELRP Port Duration** and enter the duration in seconds. |
| Interface | The port or interface identifier on the switch. |
| ELRP | Toggle to **ON** to enable ELRP on the port. |
| ELRP Exclude | Toggle to **ON** to exclude ELRP on the port. |

**Table 57: VLAN Attributes**

| Field | Description |
|---|---|
| To create a new, edit, clone, or delete VLAN attributes, see VLAN Attributes on page 179. | |
| VLAN ID | The VLAN ID for the VLAN attribute. |
| VLAN Name | The name of the VLAN. |
| ISID | The unique service identifier for the VLAN attribute. |
| IGMP Snooping VLAN Settings | Specifies if IGMP Snooping is enabled for the VLAN attribute. |

**Table 57: VLAN Attributes (continued)**

| Field | Description |
|---|---|
| DHCP Snooping VLAN Settings | Specifies if DHCP Snooping is enabled for the VLAN attribute. |
| VLAN Deployment | Specifies if VLAN Deployment is enabled for the VLAN attribute. |

**Table 58: SLPP**

| Field | Description |
|---|---|
| EDIT | Edit multiple ports at once. Select the ports, then select **EDIT** to apply bulk changes. |
| Interface | The port or interface identifier on the switch. |
| SLPP | Toggle to **ON** to enable Simple Loop Prevention Protocol (SLPP) to detect and prevent Layer 2 loops within the fabric by monitoring packets on VLANs. |
| Guard Timeout | Specify the time interval (in seconds) before the system re-enables a port after a loop protection event, helping maintain network stability. |

**Table 59: EAPoL**

| Field | Description |
|---|---|
| Enable EAPoL | Toggle to **ON** to enable EAPoL on the device.<br><br>**Note:** Modifying user authentication port settings will disconnect authenticated clients when a configuration update is performed. |
| EDIT | Edit multiple ports at once. Select the ports, then select **EDIT** to apply bulk changes. |
| Interface | The port or interface identifier on the switch. |
| User Auth | Toggle to **ON** to enable user authentication. |
| MAC Auth | Toggle to **ON** to enable MAC authentication. |
| Any Auth MAC MAX | Set the maximum number of authenticated MAC addresses allowed on the port for any authentication method. |
| 802.1X Auth MAC MAX | Set the maximum number of MAC addresses that can be authenticated using 802.1x on the port. |
| MAC Auth MAC MAX | Set the maximum number of MAC addresses permitted for MAC-based authentication on the port. |

**Table 59: EAPoL (continued)**

| Field | Description |
|---|---|
| EAPoL Re-Authentication—Status | Toggle to **ON** to enable periodic EAPoL re-authentication on the port. |
| EAPoL Re-Authentication—Period | Set the time interval (in seconds) for performing EAPoL re-authentication when enabled. |

#### Configure Instant Port Profiles

Use this task to configure Instant Port Profiles (IPP) from Network Devices or Network Policies:

**Network Devices**

1. Go to **Monitoring** > **Network Devices** > **Device Status**.
2. Select at the end of a device row, and then select **Configure** > **Device**.
3. Under the **Configuration** menu, select **Port / VLAN Configuration**.
4. From **Port Details**, select **INSTANT PROFILE**.
5. To add a new IPP, select , and then select **Instant Port Profile**.
6. Configure the IPP settings in Table 60 on page 176.
7. Select **Save** to apply the IPP to the device.

**Network Policies**

8. Go to **Configuration** > **Network**.
9. Select an existing switching/routing network policy.
10. On the **3 Switching/Routing** page, select **Configuration Settings** > **Switch Templates**.
11. In the switch template, select **Configuration** > **Port/VLAN Configuration**.
12. Choose one of the following actions:
    - To add a new IPP, select .
    - To edit an existing IPP, select , choose the IPP object, and then select .
13. Configure the IPP settings in Table 60 on page 176.
14. Select **Save** to apply the IPP to the device template.

**IPP Settings**

15. Configure IPP settings.

**Table 60: Instant Port Profile Settings**

| Field | Description |
|---|---|
| Name | Type a **Name** for the IPP. |
| Description | Type a **Description** for the IPP. |

**Table 60: Instant Port Profile Settings (continued)**

| Field | Description |
|---|---|
| Non-Forwarding VLAN | Select to choose a VLAN to detect attached devices; this VLAN does not forward traffic.<br>To add a new non-forwarding VLAN, select , to edit an existing choose a VLAN and then select , enter a **Name** and **VLAN ID**, and then select **SAVE VLAN**.<br>The non-forwarding VLAN cannot be utilized within a port type assigned to the switch. |
| Default Port Type | From the menu, select the default port type:<br>• **Access Port** - Use for a port connected to an individual host.<br>• **Trunk Port** - Use for a port connected to a forwarding device such as an AP and switch that supports multiple VLANs.<br>Ports assigned to an IPP inherit the selected port type settings, such as type, speed, STP, MAC locking, ELRP, and PSE port settings.<br>To add a new port type, select . |
| Non-Match Action | Select one of the options:<br>• **Non-Forwarding VLAN**: Does not forward traffic for devices that do not match an assignment rule.<br>• **Use Default Port Type VLAN**: Assigns the VLANs associated with the port type.<br>Storm control settings are inherited when the non-match action is set to use the default port type and the device does not match a defined device type. |
| Device Types | Add a new **Device Type**, edit or delete an existing **Device Type**.<br>Configure the IPP Device Type Settings on page 422.<br>**Note:** For a device type to match based on MAC learning, the rule must be ordered above any LLDP-based assignment rules. This ensures that MAC learning takes precedence, irrespective of LLDP information. |

### Configure Instant Secure Port Profiles

Use this task to configure Instant Secure Port Profiles (ISPP) from Network Devices or Network Policies:

#### Network Devices

1. Go to **Monitoring** > **Network Devices** > **Device Status**.
2. Select at the end of a device row, and then select **Configure** > **Device**.
3. Under the **Configuration** menu, select **Port / VLAN Configuration**.
4. From **Port Details**, select **INSTANT PROFILE**.

5. Select , and then select **Instant Secure Port Profile**.
6. Configure the Instant Secure Port Profile settings in Table 61 on page 179.
7. Select **Save** to apply the ISPP to the device.
8. Choose whether to use Unauthenticated VLAN. Unauthenticated VLAN is either a common object or can be created when the profile is created. If the Enable Unauthenticated VLAN is selected, then this VLAN will override the untagged VLAN in the port type and will be used as the Unauthenticated VLAN on the device when the configuration is pushed.
9. Specify the order in which to execute authentication. The order is per profile; therefore the same order is used for the entire device once the configuration is pushed. Use the arrows to change the default order.

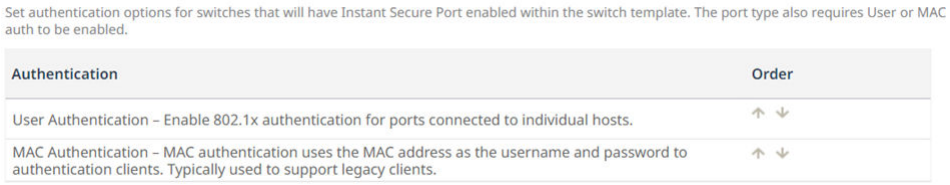



**Figure 4: ISPP Authentication Order**

10. Pick the RADIUS server for the Instant Secure Profile. Selecting **Use Extreme Platform ONE Security RADIUS Cloud configuration** uses either the free cloud RADIUS server set up per RDC, or configured proxy RADIUS servers in the Extreme Platform ONE Security application. Select one of the radio buttons to decide which type to use. Further, in the case of proxy RADIUS, you can select up to two proxy RADIUS servers; it is assumed that the ones selected have reached a deployed state after being configured in Extreme Platform ONE Security.
11. Select **Save**.

**Network Policies**

12. Go to **Configuration** > **Network**.
13. Select an existing switching/routing network policy.
14. On the **3 Switching/Routing** page, select **Configuration Settings** > **Switch Templates**.
15. In the switch template, select **Configuration** > **Port/VLAN Configuration**.
16. Choose one of the following actions:
    - To add a new ISPP, select .
    - To edit an existing ISPP, select , choose the ISPP object, and then select .
17. Configure the Instant Secure Port Profile settings in Table 61 on page 179.
18. Select **Save** to apply the IPP to the device template.

**ISPP Settings**

19. Configure ISPP settings.

**Table 61: Instant Secure Port Profile Settings**

| Field | Description |
|---|---|
| Name | Enter a profile name. |
| Description | Enter a profile description. |
| Enable Unauthenticated VLAN | Enable and define an untagged VLAN when the device is unauthenticated. Authentication mode is optional when the Unauthenticated VLAN is enabled. |
| Authentication | Set authentication options for switches that will have Instant Secure Port enabled within the switch template. The port type also requires User or MAC auth to be enabled. Enabling Instant Secure Port will also enable node alias. Node alias will provide additional data for wired client information such as IP address of the wired client device. |
| Use Extreme Platform ONE Security RADIUS Cloud Configuration | Define the RADIUS server configuration. If a DHCP assigned IP address is utilized, the DHCP IP address will be used for the RADIUS client IP configuration. If the DHCP assigned IP address changes, then a device update will be required to update the RADIUS client IP configuration.<br><br>**Note:** If Extreme Platform ONE Security settings or license is not properly configured, then device authorization may fail. |
| Use Extreme Platform ONE Security RADIUS Proxy Servers | |

20.Select **SAVE**.

#### VLAN Attributes

Use the VLAN attributes page to define additional configurations on a per-VLAN basis on a switch. VLAN attributes are applied when the VLAN is defined within an assigned port type or when the VLAN deployment option is enabled. If dynamic VLANs are utilized, then the VLAN deployment option can be enabled within the VLAN attributes page to apply VLAN settings.

**Note**
A VLAN defined within Instant Port Profiles as Non-Forwarding will not apply VLAN attributes.

To configure VLAN Attributes on a switch:

1. Go to **Monitoring** > **Network Devices** > **Device Status**.
2. Select ⋮ at the end of a device row, and then select **Configure** > **Device**.
3. Under the **Configuration** menu, select **Port / VLAN Configuration**.

4. Select **Unlock** to enable switch-level configuration changes.

**Note**
Changes made after unlocking the device will override network policy and switch template configuration.

5. Select **VLAN Attributes**.
6. To create a new VLAN attribute, select . To edit an existing VLAN attribute, select .
7. Configure the settings in Table 62.

**Table 62: VLAN Attributes**

| Setting | Description |
|---|---|
| Use VLAN common object | Select **Use VLAN common object** to automatically update the VLAN NAME and VLAN ID. |
| Manual | Select **Manual** to customize the following fields:<br>• VLAN Name: The name of the VLAN.<br>• VLAN ID: The numerical identification number of the VLAN. This can be any currently unused number. |
| ISID (Fabric Engine only) | Specifies the service identifier used to map the VLAN to a unique service instance within the fabric.<br><br>**Note:** The ISID is autogenerated if not set. |
| IGMP Snooping | Toggle to **ON** to enable **IGMP Snooping** for switches to identify ports to which multicast group member hosts are attached to optimize the distribution of multicast traffic.<br><br>**Note:** Enable **Immediate Leave** to remove multicast host immediately when it leaves the group. |
| DHCP Snooping | Enable snooping of DHCP packets and create a DHCP bindings database of IP to MAC addresses for this VLAN. Toggle to **ON** to enable DHCP Snooping. Optional: Select the action **Enable drop rogue DHCP packets action for this VLAN**.<br><br>**Note:** Ports configured as trusted will not apply drop action. By default, port types configured as Trunk Port will be trusted. |
| VLAN Deployment | With VLAN Deployment, VLAN and VLAN attributes can be created on switches when no port types are assigned with the defined VLAN. Toggle to **ON** to enable VLAN deployment. |

8. To create a copy, select an existing VLAN ID, select , and then type a name for the new VLAN attribute.
9. To delete VLAN attributes, select the VLAN IDs, and then select .
10. Select **Save**.

*Configure Wired Device Credentials*

You must select **Enable Device Management Settings for Switch Engine/EXOS Switches** under **Global Settings**. To do this, under your admin name at the top right of the ExtremeCloud IQ window, select **Global Settings** > **Administration** > **Device Management Settings**.

For Switch Engine devices only, use device credentials to set up log in information for root or read-only administrators, change the name and password of the root admin, or add a read-only admin to a switch. Device-level credentials offer access to devices through Telnet, SSH, or console connections.

**Note**
At this level, you are making changes to the selected device only. These changes always override the network policy configurations. To revert to the settings in the network policy, from the device list, select the device host name, and use the **Actions** button.

A root admin has complete privileges, which include the ability to add, modify, and delete other administrators, and to reset the configuration. A read-only admin can view settings but cannot add, modify, or delete them. You can require that an admin be prompted for a password before accessing high-level privileged CLI commands. To configure a root admin with full capability, follow these steps:

1. Go to **Monitoring** > **Network Devices** > **Device Status**.
2. Select ⋮ at the end of a device row, and then select **Configure** > **Device**.
3. Under the **Configuration** menu, select **Device Credentials**.
4. For an **Administrator Account**, enter the **Admin Name** and **Password**.

   Passwords should contain at least 8 characters, including at least one number, one special character, and one uppercase character.
5. For a **Read Only Administrator**, enter the **Admin Name** and **Password**.

   Passwords should contain at least 8 characters, including at least one number, one special character, and one uppercase character.
6. Select **Save Configuration**.

   For more information about how to push updated configuration to the device, see Push Device-Level Configuration on page 152.

Related Links

Configure Wired Devices on page 160

*Interface Configuration*

On the **Interface Configuration** page, you can add, edit, or delete Interface configurations. The table includes the following parameters:

- IP Address
- IPv4 Subnetwork Allocation Name
- VLAN Name
- VLAN ID
- DHCP Relay

- IPv4 Forwarding
- Routing Instance

Use this task to configure the device interface.

1. Go to **Monitoring** > **Network Devices** > **Device Status**.
2. Select at the end of a device row, and then select **Configure** > **Device**.
3. Under **Network Allocation**, select **Interface Configuration**.
4. Select a port icon on the template graphic to view port details, if available.
5. Select to add, or to edit an Interface.
6. Enter the interface attributes according to the table below:

**Table 63: Interface Configuration Attributes**

| Field | Description |
|---|---|
| Network Allocation | An IP subnetwork configuration. |
| VLAN Attribute | A VLAN attribute, which can be created from within the **Network Policy Switching** > **VLAN Attribute** Section. |
| IPv4 Address / Subnet Mask | The assigned device IP Address. |
| Routing Instance | The device routing instance. |
| IPv4 Forwarding | Toggle **ON** to enable IPv4 forwarding. |
| VLAN Loopback Enable | Select the check box to enable VLAN loopback. |
| DHCP Relay | To override DHCP Relay, toggle **ON Enable DHCP Relay**. If enabled, enter a **Primary DHCP Server** and an optional **Secondary DHCP Server**. |

7. Select **Next**.
8. Confirm **Summary** details, and then select **Save**.

   To go back and make changes, select **Previous**.
9. To delete Interfaces, select the Interface(s) and then select .
10. For more information about how to push updated configuration to the device, see Push Device-Level Configuration on page 152.

Related Links

Routing Configuration on page 182
Configure Wired Devices on page 160

*Routing Configuration*

The device must have an IPv4 interface configured. For more information, see Interface Configuration on page 181.

Use this task to configure IP4 Static Routes for the selected device.

1. Go to **Monitoring** > **Network Devices** > **Device Status**..
2. Select at the end of a device row, and then select **Configure** > **Device**.
3. Under the **Network Allocation** menu, select **Routing Configuration**.

4. Select to add or to edit, and then configure the static route settings in Table 64.

**Table 64: Static Route Settings**

| Field | Description |
|---|---|
| Static Route Name | The name of the Static Route. |
| Destination Subnet | The desired subnet, such as `10.1.0.0/16`. |
| Next Hop IP | The desired IP Address for the next Hop, such as `123.321.132.312`. |
| Next Hop IP Ping Protection | **Enable** or **Disable** Next Hop IP Ping Protection.<br><br>**Note:** Enabling Ping Protection will generate a Ping Protection Status tool tip when viewing your device within **Monitoring** > **Visualize** > **Wired** > **Routing**<br><br>**Note:** Not supported for Fabric Engine/VOSS. |
| Metric | The desired metric value. |
| Routing Instance | Shows the Routing Instance. |

5. Select **Save**.
6. To delete a static route, select the check box next to the Static Route Name and then select .
7. For more information about how to push updated configuration to the device, see Push Device-Level Configuration on page 152.

Related Links

Configure Wired Devices on page 160

## Configure Fabric Settings

Shortest Path Bridging MAC (SPBM) is a next generation virtualization technology that revolutionizes the design, deployment, and operations of carriers and service providers, along with enterprise campus core networks and the enterprise data center. SPBM provides massive scalability while at the same time reducing the complexity of the network.

Auto-sense is a port-based functionality that supports zero touch capabilities on the switch. Auto-sense dynamically configures the port to act as an IS-IS network-to-network interface (NNI), Fabric UNI (Flex-UNI), Fabric Attach (FA), Fabric Extend, or voice (IP phone) interface, based on the Link Layer Discovery Protocol (LLDP) events. Auto-sense provides global

configuration options for IS-IS authentication, FA authentication, Fabric Extend tunnel creation, and voice configuration for IP phones on the switch.

**Note**
This feature is available only if the device is in an ExtremeCloud IQ (New)-compatible building or outdoor site with full features unlocked. For more information, see *Extreme Platform ONE Networking and ExtremeCloud IQ Subscription and Licensing Guide*.

Use this task to configure fabric settings for devices running Fabric Engine.

1. Go to **Monitoring** > **Network Devices** > **Device Status**.
2. Select ⋮ at the end of a device row, and then select **Configure** > **Fabric**.
3. Configure the following fabric settings:
   - Global SPBM Settings
   - Auto Sense Settings

   **Note**
   Toggle **Advanced** to **ON** to view advanced options.
4. To save device fabric settings, see Push Device-Level Configuration on page 152.

Related Links

Device 3-Dot Menu Actions on page 134

*Global SPBM Settings*

**Table 65: Global SPBM Settings**

| Field | Description |
|---|---|
| **SPBM** | |
| Hostname | Specifies the SPBM system name. Enter a string length from 1 to 255. |
| System ID | Specifies the SPBM instance ID.<br><br>**Note:** System ID and Nickname can only be changed together. |
| Nickname | Specifies a nickname for the SPBM instance globally. Valid value is 2.5 bytes in the format <x.xx.xx>.<br><br>**Note:** System ID and Nickname can only be changed together. |
| ISIS Manual Area ID | Specifies the IS-IS manual area. Valid value is 1-26 bytes in the format <xx.xxxx.xxxx...xxxx>. Only one manual area is supported. Use the same manual area across the entire SPBM cloud. For IS-IS to operate, you must configure at least one manual area. |
| Primary BVLAN | Specifies the primary SPBM B-VLAN to add to the SPBM instance. |

**Table 65: Global SPBM Settings (continued)**

| Field | Description |
|---|---|
| Secondary BVLAN | Specifies the secondary SPBM B-VLAN to add to the SPBM instance. |
| IP Shortcuts | Toggle **IP Shortcuts** to **ON** to enable the SPBM IP shortcut state. The default is disable. In **IP Source Address**, specify the CLIP interface to use as the source address for SBPM IP shortcuts. |
| Multicast | Toggle **Multicast** to **ON** to enable IP multicast over SPBM. The default is disabled. |
| Auto ISID Assignment | Toggle **Auto ISID Assignment** to **ON** to enable automatic allocation to assign and manage ISIDs. In **L2 ISID Offset**, specify the starting index for SID allocation for Level 2 IS-IS routers. |
| **Nickname Server** (Advanced Option) | |
| Nickname Prefix | Specifies the nickname server allocation prefix. x.xx.xx uses the form X.X0.00 from 0.00.00 to F.F0.00. A group, X.X0.00 to X.XF.FF, can provide up to 4,096 nicknames. The default is A.00.00. |

Related Links

Auto Sense Settings on page 185

Configure Fabric Settings on page 183

*Auto Sense Settings*

**Table 66: Auto Sense Settings**

| Field | Description |
|---|---|
| **General Assignments** | |
| Onboarding ISID | Specifies the onboarding I-SID used by the auto-sense ports.<br><br>**Note:** This is an **Advanced** option. |
| Data ISID | Specifies the data I-SID used by the auto-sense ports. |
| Wait Interval | Specifies the wait interval, in seconds, for Auto sense to wait for a Link Layer Discovery Protocol (LLDP) neighbor to be detected in the auto-sense wait state before transitioning to the auto sense onboarding state. This configuration is a global configuration that applies to all auto-sense ports. The default value is 35.<br><br>**Note:** This is an **Advanced** option. |
| Voice ISID | Specifies the voice I-SID used by auto sense ports. |

**Table 66: Auto Sense Settings (continued)**

| Field | Description |
|---|---|
| Voice CVID | Specifies the customer VLAN ID associated with the voice I-SID used by auto-sense ports. Voice C-Vid is configured for tagged voice traffic only.<br><br>**Important:** You must configure the Auto-sense voice customer VLAN ID along with the auto sense voice I-SID. |
| EAPoL Voice LLDP Authentication Bypass | Select to enable the EAPoL LLDP authentication bypass for voice auto sense ports.<br><br>**Note:** This is an **Advanced** option. |
| **Fabric Attach Assignments** | |
| FA Proxy Management ISID | Specifies the FA proxy management I-SID used by auto sense ports. |
| FA Proxy Management CVID | Specifies the proxy management client-VLAN ID (C-VID) used by auto sense ports. |
| FA Proxy No Auth Management ISID | Specifies the proxy no-auth I-SID used by auto sense ports.<br><br>**Note:** This is an **Advanced** option. |
| FA WAP Type1 ISID | Specifies the FA WAP type-1 I-SID used by auto sense ports. |
| FA Camera ISID | Specifies the FA camera I-SID used by auto sense ports. |
| EAPoL FA WAP Type1 Authentication Bypass | Select to enable the FA EAPoL authentication bypass for Wap-type-1 I-SID used by auto sense ports. |
| EAPoL FA Camera Authentication Bypass | Select to enable the FA EAPoL authentication bypass for camera I-SID used by auto sense ports. |
| **FA Message Authentication** | |
| FA Message Authentication | Select to enable FA message authentication. |
| FA Auth Key | Specifies the FA authentication key for the auto sense ports. |
| **Message Authentication IS-IS** (Advanced Options) | |
| ISIS Hello Auth Type | Select an IS-IS hello authentication type. |
| ISIS Hello Auth Key ID | Specifies the IS-IS authentication key ID for auto sense ports. |
| ISIS Hello Auth Key | Specifies the IS-IS authentication key for auto sense ports. |

Related Links

Global SPBM Settings on page 184

Configure Fabric Settings on page 183

## Configure Wireless Devices

After you select a **Wireless** device from the device list, you can create or modify the following:

- Wireless Device Configuration: Edit device details such as the host name, the description, the device function, IP addresses, and VLAN assignments.
- Wireless Interface Settings: View the default template settings and control actions for the Wireless (Wi-Fi) and Wired (Ethernet) ports. You can edit any field that is selectable.
- Wireless Device Credentials: Assign or change network administrator credentials and administrator assignments, and configure CAPWAP and Shared Key settings.
- Configure Netdump: Enable an unresponsive AP to automatically save a core dump file to a TFTP server on the network the next time it boots.
- DHCP Server and Relay: For a small network, configure and enable a DHCP server on a device to provide network settings dynamically to clients.
- Neighboring Devices: Define a list of neighbor access points that will collaborate in the Layer 3 roam process.
- Bonjour Gateway Settings: Choose the AP you want to act as your Bonjour Gateway Designated Device (BDD) at the device level.
- Troubleshooting: Enable Client Monitor so devices can detect client issues, and report client connection activities and problems to ExtremeCloud IQ (New).

After you make changes to the configuration, you must push the configuration changes to the device.

*Wireless Device Configuration*

It is a best practice to configure devices using a device template. However, you can override the device template settings for a specific device.

Use this task to configure the settings for a specific wireless device.

1. Go to **Monitoring** > **Network Devices** > **Device Status**.
2. Select ⋮ at the end of a device row, and then select **Configure** > **Device**.
3. Under the **Configuration** menu, select **Device Configuration**.
4. Configure **Device Details** settings in Table 67.

**Table 67: Device Details Settings**

| Field | Description |
|---|---|
| Host Name | Type a unique host name for the device. It can contain up to 32 characters and can include spaces. |
| Description | Optional description for the device. |
| Mgt0 MAC Address | This is the Node ID and is listed on the printed label located on each device. |
| Device Model | The hardware model of the configured device. |
| Device Function | This describes the main function of the device. For example, AP. |

**Table 67: Device Details Settings (continued)**

| Field | Description |
|---|---|
| IQ Engine | Lists the IQ Engine firmware version currently installed on the AP. |
| SNMP Location | The SNMP location name, for example `headquarters, building 1`. |

5. Configure **Network Details** settings:
   - **Network Policy**: Select a network policy from the drop-down list of existing policies.
   - **Device Template**: Select a device template from the drop-down list of existing templates, or clone an existing template.

6. Configure **Management Interface (Mgt0)** settings:
   a. Select **Static Address** to enter a static address for this interface, and then configure the settings in Table 68.

**Table 68: Static Address Settings**

| Field | Description |
|---|---|
| IPv4 Address | The IPv4 address you want the device to use for the mgt0 interface. |
| Subnet Mask | The appropriate netmask for the subnet to which the mgt0 interface connects. |
| Default Gateway | The address through which the device (and its connected hosts) can reach the Internet. |

   b. Select **Dynamic Address Configuration (DHCP) Client** to have an address automatically assigned by DHCP, and then configure the settings in Table 69.

**Table 69: Dynamic Address Configuration (DHCP) Settings**

| Field | Decription |
|---|---|
| Use DHCP only to set IP Address (IPv4 only) | Enable or disable this function. |
| Advanced DHCP Options (IPv4 only) | Select to display or hide this section. Configure the following settings:<br>• **DHCP Timeout**: Enter the amount of time (in seconds) that the device waits for a response from the DHCP server before assigning itself a static IP address. By default, the timeout for reverting to a static address is 20 seconds. You can change the timeout from 0 to 3600 seconds (1 hour). A timeout of 0 means that the device continues trying to obtain network settings through DHCP indefinitely.<br>• **Automatically Generate Interface IP Settings**:<br>◦ **IP Prefix**: The Extreme Networks device automatically switches to this IP address if it cannot obtain settings through DHCP. You can also enter an IPv6 address.<br>◦ **Subnet Mask**: Enter the netmask for the subnet to which the mgt0 interface connects.<br>• **Static Fallback IP Settings**:<br>◦ **Static IP Address**: Enter the IP address you want the device to use if it cannot contact the DHCP server. You can also enter an IPv6 address.<br>◦ **Subnet Mask**: Enter the appropriate netmask for the subnet to which the mgt0 interface connects.<br>◦ **Default Gateway**: The address through which the device (and its connected hosts) can reach the Internet. |

   c. Enter the **Management VLAN** for this interface.
   d. Enter the **Native VLAN** for this interface.
   e. Select **Override MGT0 MTU** to manually enter an MTU, ranging from 100-1500 Bytes (the default value is 1500 Bytes).

7. (Optional) Configure **Supplemental CLI**:
   a. **Apply Supplement CLI from network policy switch template**: Include the supplemental CLI object in the network policy and append the selected CLI object from the list. If you select a supplemental CLI object from the list, or create a new one, it is appended to the end of the configuration list, after the supplemental CLI object in the network policy.
   b. **Override Supplement CLI from network policy Supplement CLI**: Enable the network policy to override supplemental CLI objects for the device. For more information, see Override Supplemental CLI on page 144.

   **Important**
   Before you can configure Supplemental CLI access on a device, you must first enable Supplemental CLI. Go to **Administration & Settings** > **Global Settings** > **Backup & Restore**, and then enable **Supplemental CLI**.

8. Select **Override Disable WebUI in the network policy** to disable the local web user interface on an IQ Engine device to improve system security, without disabling the associated captive web portal.

   If you configured **WebUI** in the network policy, you can disable it for this device here.
9. For **Deployment Mode**, select **Pre-Provisioned** or **Production** to indicate whether the device has been pre-provisioned.
10. (AP5010 only) Enable **POE Profile Override**, select the override option from the drop-down menu, and hover over the **i** icon to view the corresponding override table.
11. (AP4060/AP4060X and AP5060U/D only) For **Antenna Location Type**, select a location from the drop-down list.

    **Note**
    You must have IQ Engine Version 10.8r4 or higher.

12. Select **Save Device Configuration**.

    For more information about how to push updated configuration to the device, see Push Device-Level Configuration on page 152.

Related Links

Wireless Interface Settings on page 190
Configure Wireless Devices on page 187

*Wireless Interface Settings*

Use this task to view **Device Template Default Settings** and control actions for Wireless (Wi-Fi) and Wired (Ethernet) ports.

**Note**
Changes made here are at the device level, which overrides the network policy template for the device only. The Network Policy remains unchanged.

1. Go to **Monitoring** > **Network Devices** > **Device Status**.
2. Select ⋮ at the end of a device row, and then select **Configure** > **Device**.
3. Under the **Configuration** menu, select **Interface Settings**.

4. For **Wireless Interfaces**:
   a. Select an **Operating Mode**.
   b. Select either the **WiFi0**, **WiFi1**, **WiFi2**, **BLE**, or **IoT0** tab.

      **Note**
      The **IoT0** tab is supported on AP5010/AP5020 models.

   c. To configure **WiFi0**, **WiFi1**, **WiFi2**, or **IoT0**, see Wi-Fi Settings on page 191.
   d. To configure **BLE**, go to **Configuration** > **Network** > **Network Policy** > **Wireless** > **Application Management** > **BLE Service**.
5. For **Wired Interfaces**, see Configure Wired Interfaces Settings on page 193.

   **Note**
   To enable LLDP/CDP for a port, ensure LLDP/CDP is enabled under both the policy level and port level configuration.

6. To configure **Electronic Shelf Label**, toggle **Enable ESL** to **ON**, and then Configure Electronic Shelf Label Settings.
7. Select **Save Interface Settings**.

   For more information about how to push updated configuration to the device, see Push Device-Level Configuration on page 152.

Related Links

Configure Wireless Device Credentials on page 194
Configure Wireless Devices on page 187

Wi-Fi **Settings**

**Table 70: Radio Status Settings**

| Field | Description |
|---|---|
| Radio Status | Set to **On**. |
| Radio Profile—or IoT Profile, if applicable | Select a profile from the drop-down list. You can also add a new Radio Profile or IoT Profile here, or clone and modify an existing profile.<br><br>**Note:** Only the AP510C, AP510CX, AP550, AP650, AP650X, AP305C, AP305CX, AP302W, AP4000, AP5010, AP3000/X, AP410C, AP460C, AP460S6C, and AP460S12C models support MU-MIMO on its Wi-Fi0 interface. |

**Table 70: Radio Status Settings (continued)**

| Field | Description |
|---|---|
| Radio Usage | Select the usage type:<br>• **Client Mode**: Select to configure a device for AP client mode radio usage, and to configure advanced features such as **Port Forwarding Rules** and **DHCP Server** settings. Select a **Client Mode Profile**. If required, you can configure a new Client Mode Profile, or edit an existing profile.<br>• **Client Access**: Select for normal client operation.<br>• **Backhaul Mesh Link**: Select for wireless portal and mesh backhaul operation.<br>• **Sensor**: Select for presence operation. |
| Enable SDR (Software Defined Radio) | Enable and then select an **SDR Profile** from the drop-down list. You can also add a new profile here or modify an existing profile. |
| Channel | Select a channel. If you select **Auto**, ExtremeCloud IQ (New) selects the channel for you. |
| Override channel exclusion setting in radio profile | Enable, and then select activated channels to manually exclude them from the radio profile. |
| Transmission Power | Activate to manually set the transmission power. Select **Manual**, and then use the slider to select a dBm setting. |
| Enable client transmission power control (802.11h) | Activate to manually enable client transmission power control (802.11h). Select **Manual** and use the slider to select a dBm setting. |

**Table 71: Enable Presence Analytics Settings**

| Field | Description |
|---|---|
| Enable Presence Analytics | Toggle to **On** to modify device presence analytics settings. |
| Name | Automatically populates with the name of the Network Policy. |
| Trap Interval | The interval (in seconds) that the presence sensor reports data to ExtremeCloud IQ (New). |
| Aggregate Time | The interval (in seconds) for the period during which aggregation occurs for the presence profile. |
| Aging Time | The aging time (in seconds) for a given presence profile. |

**Table 72: SSID Settings**

| Field | Description |
|---|---|
| SSID Name (Policy) | The current SSID name. |
| Status | Toggle the SSID status to **On** or **Off**. |
| Override SSID Broadcast Name | Change the SSID broadcast name for the device. |

**Table 72: SSID Settings (continued)**

| Field | Description |
|---|---|
| Override PSK Password | Change the PSK password for the device. |
| Reassign CWP | Select a new CWP from the drop-down list. |
|  | Hover and select **Revert** to revert device-specific SSID settings to their default values. |

Related Links

Wireless Interface Settings on page 190

#### Configure Wired Interfaces Settings

**Table 73: Wired Interfaces Settings**

| Field | Description |
|---|---|
| Interface | The software representation of the physical port. |
| State | Indicates if the port is enabled or disabled. |
| Port Type | The interface port type. This field is read only. |
| Native VLAN | The native (untagged) VLAN assigned to frames that do not have any 802.1Q VLAN tags in their headers. |
| Allowed VLANs | The VLANs, including the native VLAN, that you want the trunk port to permit.<br>You can list the VLANs individually, separated by commas, or as a range of VLANs using a hyphen. Alternatively, you can enter the word **all** in this field to support all existing VLANs previously configured in the network policy (the default). |
| Fabric Attach | 1. Select , and then enter a **Name** and **Description** for the Fabric Attach.<br>2. For each VLAN, select , and then enter the device's associated **VLAN ID** and **I-SID**.<br>3. Select a VLAN from the list, and then select  to remove the VLAN from the Fabric Attach.<br>4. Select **Save**. |
| Transmission Type | Select one of the following options:<br>• **Auto**: The switch negotiates the best common duplex mode with the connected device.<br>• **Full-Duplex**: Forces the switch to communicate with the connected device using full duplex communication.<br>• **Half-Duplex**: Forces the switch to use half duplex communication. |
| Speed | The speed the Ethernet port uses to communicate with the connected device. |

**Table 73: Wired Interfaces Settings (continued)**

| Field | Description |
|---|---|
| Green Ethernet | Select to allow physical layer transmitters to consume less power when they are in a state of idleness or low data activity.<br><br>**Note:** Supported on AP4020, AP5020, AP5060U/D, AP_410C, AP_305C/CX, AP_510C/CX, AP_460C/S6C/S12C, AP_4000/4000U devices only. |
| LLDP | Select for devices to advertise identities, status, and capabilities to each other.<br>Devices can transmit data about themselves and receive transmitted data from other devices, but they cannot solicit and retrieve data from other devices. |
| CDP | Select for devices to advertise an IP address that can send and receive SNMP traps. |
| MCast Filter | Select to enable Multicast Rate Limiting on the interface for multicast/ broadcast traffic. |
| Multicast Rate Limit | Set the maximum rate (in Kbs) for incoming multicast traffic for the interface. |

Related Links

Wireless Interface Settings on page 190

**Configure Electronic Shelf Label Settings**

**Table 74: Electronic Shelf Label Settings**

| Field | Description |
|---|---|
| Server | The name of the server that manages Electronic Shelf Label (ESL) communication and data updates. |
| State | The current operational status of the ELS device. |
| Port Type | The network port type used for communication. |
| Native VLAN | The assigned VLAN ID. |

Related Links

Wireless Interface Settings on page 190

*Configure Wireless Device Credentials*

Use device credentials to set up log in information for root or read-only administrators, change the name and password of the root admin, or add a read-only admin to an AP. Device-level credentials offer access to APs through Telnet, SSH, or console connections.

**Note**
At this level, you are making changes to the selected AP only. These changes always override the network policy configurations.

A root admin has complete privileges, which include the ability to add, modify, and delete other administrators, and to reset the configuration. A read-only admin can view settings but cannot add, modify, or delete them. You can require that an admin be prompted for a password before accessing high-level privileged CLI commands.

Use this task to configure wireless device credentials.

1. Go to **Monitoring** > **Network Devices** > **Device Status**.
2. Select ⋮ at the end of a device row, and then select **Configure** > **Device**.
3. Under the **Configuration** menu, select **Device Credentials**.
4. For an **Administrator Account**, enter the **Admin Name** and **Password**.

   Passwords should contain at least 8 characters, including at least one number, one special character, and one uppercase character.
5. For a **Read Only Administrator**, enter the **Admin Name** and **Password**.

   Passwords should contain at least 8 characters, including at least one number, one special character, and one uppercase character.
6. Configure the **Primary CAPWAP Server** and **Secondary CAPWAP Server** connections.

   You can select an existing CAPWAP server from the drop-down list, or select the add icon to define a new server.
7. Configure a **Shared Key for Authentication Passphrase**.
8. Select **Save Device Credentials**.

   For more information about how to push updated configuration to the device, see Push Device-Level Configuration on page 152.

Related Links

Configure Netdump on page 195
Configure Wireless Devices on page 187

*Configure Netdump*

You must perform a full configuration update for each device on which you want to enable netdump.

If an AP or switch becomes non-responsive, you can enable it to automatically save a core dump file to a TFTP server on the network the next time it boots. You can provide this file to Support to assist in diagnosing the issue. To configure a device to save a core dump file to a TFTP server, complete the following steps:

1. Go to **Monitoring** > **Network Devices** > **Device Status**.
2. Select ⋮ at the end of a device row, and then select **Configure** > **Device**.
3. Under the **Configuration** menu, select **Configure Netdump**.
4. Select the check box to **Enable Netdump**.

5. Configure the **Update Settings** in Table 75.

**Table 75: Netdump Update Settings**

| Field | Description |
|---|---|
| TFTP server for saving netdump files | The IP address of the TFTP server where you want the device to send the core file. |
| Netdump filename to save | The name of the netdump file. |
| VLAN for reaching the TFTP server | The VLAN of the interface the device will use to send the netdump file to the TFTP server. |
| Native VLAN of the local Extreme Networks device | The native VLAN of the device. |

6. Select **DHCP** to have the device bootloader use DHCP to obtain an IP address at startup.
7. Select **Static** to use a static IP and configure the network settings in Table 76 that the bootloader must use to connect to the network:

**Table 76: Update Static IP Settings**

| Field | Description |
|---|---|
| Address of local Extreme Networks device | The IP address of the reporting device. |
| Netmask of local Extreme Networks device | The netmask for the reporting device. |
| Gateway for reaching the TFTP server | The IP address of the TFTP server. |

8. Select **SAVE NETDUMP CONFIGURATION**.

   For more information about how to push updated configuration to the device, see Push Device-Level Configuration on page 152.

The device will send a core dump file to the TFTP server the next time it reboots.

Related Links

Configure DHCP Server and Relay Settings on page 196
Configure Wireless Devices on page 187

*Configure DHCP Server and Relay Settings*

For small networks that do not already have a DHCP server, you can configure and enable a DHCP server on an Extreme Networks device to provide network settings dynamically to clients. After you configure one hive member as a DHCP server, the other hive members forward the DHCPDISCOVERY and DHCPREQUEST messages to their neighbors. The device you use as the DHCP server must be a portal.

When all hive members are in the same subnet and all devices in that subnet are on a single VLAN, you only need to configure the DHCP server device with a pool of IP addresses it can draw from when responding to DHCP client requests. When some hive members are in a different subnet from the DHCP server, you must also configure those devices to forward DHCP traffic to the IP address of the DHCP server. In this case, the other devices act as DHCP relay agents.

Use this task to configure both DHCP servers and relay agents.

1. Go to **Monitoring** > **Network Devices** > **Device Status**.
2. Select at the end of a device row, and then select **Configure** > **Device**.
3. Under the **Additional Settings** menu, select **DHCP Server and Relay**.
4. Select to add or to edit, and then configure the settings in Table 77.

**Table 77: DHCP Server and Relay Settings**

| Field | Description |
|---|---|
| Name | A unique identifier for the DHCP configuration profile. |
| Description | A brief summary for the configuration profile. |
| Platform Supported | The device models or operating systems the configuration is compatible with. |
| Interface | The network interface through which DHCP services are provided or relayed. |
| Service | Defines whether the device acts as a DHCP Server or Relay Agent.<br>The DHCP relay enhancement supports deployments when a centralized DHCP server (for example, at corporate headquarters) is used. When you enable DHCP Relay, the DHCP server feature on devices is disabled so that routers redirect DHCP service requests to the centralized DHCP server |

5. Enable or disable **Set the DHCP server as authoritative**.

   If this DHCP server is the only one on your network, it contains a record of the valid IP numbers on the network. If a client tries to register with an invalid IP address (for example, if a client device still has an active lease with another network), an authoritative DHCP server denies access to that client.
6. Enable **Use ARP to check for IP address conflicts** when this DHCP server uses ARP to check for IP address conflicts on the network before assigning an IP address to a DHCP client.
7. Select **Enable NAT Support** if this DHCP server uses NAT.
8. For **IP Pool**, define the IP address pool from which the DHCP server draws IP addresses when making assignments.
   a. Select to add a new IP pool.
   b. Enter the **Start IP Address** and **End IP Address**.
   c. Select **Add**.
9. For **IP Binding**
   a. Select to add a new IP Binding.
   b. Enter the**IP Address** and **MAC Address**.
   c. Select **Add**.
10. To configure each of the required parameters that the DHCP server returns to clients along with an IP address, configure the DHCP Server Options Settings on page 198.

11. To define custom DHCP options to provide additional network settings to connected clients, see Configure Custom DHCP Options on page 198.
12. Select **Save**.

    For more information about how to push updated configuration to the device, see Push Device-Level Configuration on page 152.

Related Links

Configure Neighboring Devices on page 199
Configure Wireless Devices on page 187

#### DHCP Server Options Settings

**Table 78: DHCP Server Options Settings**

| Field | Description |
|---|---|
| Default Gateway | The IP address of the default gateway for the subnet to which the address in the IP pool belong. |
| DNS Server1 IP | The primary DNS server IP address for the clients to contact when resolving domain names to IP addresses. |
| DNS Server2 IP | The secondary DNS server IP address for clients to contact when resolving domain names to IP addresses. |
| DNS Server3 IP | The tertiary IP address for clients to contact when resolving domain names to IP addresses. |
| POP3 Server IP | The POP3 server IP address. |
| SMTP Server IP | The SMTP server IP address. |
| WINS Server1 IP | The primary WINS server IP address. |
| WINS Server2 IP | The secondary WINS server IP address |
| Lease Time | The length of time for the DHCP lease to last. |
| Netmask | The subnet to which the addresses in the IP pool belong. |
| Domain Name | The DNS name resolution domain name to assign to DHCP clients. |
| MTU | The path MTU aging timeout in seconds. |
| NTP Server1 IP | The primary NTP server IP address for DHCP client clock synchronization. |
| NTP Server2 IP | The secondary NTP server IP address for DHCP client clock synchronization. |
| Log Server IP | The log server IP address for DHCP clients. |

Related Links

Configure DHCP Server and Relay Settings on page 196

#### Configure Custom DHCP Options

Create or modify **DHCP Server and Relay settings**.

Use this task to define custom DHCP options to provide additional network settings to connected clients.

1. Select .
2. Enter a custom **Number** from 2 to 5, 8 to 14, 16 to 25, 27 to 41, 43, 45 to 50, 52 to 57, 60 to 68, 71 to 224, 227, 228, or 232 to 254.
3. Select the **Type** of data that the option provides:
   - **Integer**: (0-2,147,483,547)
   - **IP Address**: (Four octets for an IP address or eight groups of two octets each for an IPv6 address.)
   - **String**: (1-255 characters)
   - **Hex**: (1-254 hexadecimal digits)
4. Enter the **Value** for the data.
5. Select **Add**.

Related Links

Configure DHCP Server and Relay Settings on page 196

*Configure Neighboring Devices*

**Roaming Threshold** helps control the number of tunnels an AP can accept during layer 3 roaming operations.

Manually add a **Neighbor** to define a Hive neighbor in the case where the APs cannot hear over the air and they are in different management subnets (which is how they ordinarily learn of each other.) Bonjour Gateway piggybacks on this functionality to learn of APs in other management subnets that cannot be heard over the air.

1. Go to **Monitoring** > **Network Devices** > **Device Status**.
2. Select  at the end of a device row, and then select **Configure** > **Device**.
3. Under the **Additional Settings** menu, select **Neighboring Devices**.
4. Select a **Roaming Threshold** value from the drop-down list to set the volume of traffic that the selected neighbors will accept through GRE (Generic Routing Encapsulation) tunnels to support Layer 3 roaming.

   This option gives hive members the ability to push tunnels to other members for better tunnel load balancing. For example, if one AP near an entrance gets overloaded with tunnels, you can lower its threshold to medium or low so that more tunnels terminate on other APs.

   **Note**
   This setting only takes effect when the APs function as portals and Layer 3 roaming is enabled.

5. Select  to manually add a Layer 3 roaming or Bonjour gateway neighboring Extreme Networks device.

6. Select an **Available Neighbor** device from the drop-down list and select **Add**.

   **Note**
   You can add any or all of the Layer 3 roaming and Bonjour gateway neighboring Extreme Networks devices by repeating the previous two steps.

7. To remove a manually configured neighboring device, select a device, and then select .
8. Select **Save Neighboring Devices**.

   For more information about how to push updated configuration to the device, see Push Device-Level Configuration on page 152.

Related Links

Configure Bonjour Gateway Settings on page 200
Configure Wireless Devices on page 187

*Configure Bonjour Gateway Settings*

Define Bonjour Gateway settings in the network policy.

Use this task to choose the wireless device you want to act as your Bonjour Gateway Designated Device (BDD) at the device level. If possible, use the newest model device you have in a low traffic area.

1. Go to **Monitoring** > **Network Devices** > **Device Status**.
2. Select at the end of a device row, and then select **Configure** > **Device**.
3. Under the **Additional Settings** menu, select **Bonjour Gateway Settings**.
4. Set the **Priority** for the wireless device you want to use as your BDD to around 250.

   By default, every AP is set an automatic priority level (10-20) for the Bonjour service. The AP with the highest priority setting acts as the Bonjour Gateway. The MAC address is used if the priority is the same on all APs.
5. To modify the realm name, select **Override the default real name** and set the **Realm Name**.

   **Note**
   A realm name is automatically generated by placing this device on a map (the auto-generated name is the building name). Modifying the realm name here overwrites the auto-generated realm name.

6. Select **Save Bonjour Gateway Settings**.

   For more information about how to push updated configuration to the device, see Push Device-Level Configuration on page 152.

Push a complete configuration to the BDD, followed by a **Delta** update to all other APs.

Related Links

Troubleshooting on page 201
Configure Wireless Devices on page 187

*Troubleshooting*

Use this task to enable Client Monitor so devices can detect client issues, and report client connection activities and problems to ExtremeCloud IQ (New).

1. Go to **Monitoring** > **Network Devices** > **Device Status**.
2. Select at the end of a device row, and then select **Configure** > **Device**.
3. Under the **Additional Settings** menu, select **Troubleshooting**.
4. Toggle **Enable Client Monitor** to **On**.
5. Select to configure a new Client Monitor Policy, see Client Monitor Profile Settings on page 201, and then click **Save**.

   **Note**
   Select the client monitor profile name to edit the profile.

6. Select to select an existing client monitor policy.
7. Select **X** to use the SSID client monitor policy.
8. For wireless devices that support Dynamic Packet Capture, toggle **Enable Packet Capture** to **On**.

   **Note**
   If the AP model supports Dynamic Packet Capture, a small packet capture of the event is appended to the client monitor record. Dynamic Packet Capture is supported on the following models:
   - AP3000, AP3000X, or AP5010 running 10.6.7 or higher
   - AP5020 running 10.7.1 or higher
   - AP4020 running 10.8.1 or higher

9. Select **Save Troubleshooting**.

   For more information about how to push updated configuration to the device, see Push Device-Level Configuration on page 152.

Related Links

Configure SSH on page 202
Configure Wireless Devices on page 187

**Client Monitor Profile Settings**

**Table 79: Client Monitor Profile Settings**

| Field | Description |
|---|---|
| Name | Type a name to identify the Client Monitor Profile policy. |
| **Association Problem** | |
| Trigger Times | Set the number of times an association problem can be triggered, between 1 and 10. |
| Report Interval | Set the interval between reporting an association problem, between 30 and 3600 seconds. |

**Table 79: Client Monitor Profile Settings (continued)**

| Field | Description |
|---|---|
| **Authentication Problem** | |
| Trigger Times | Set the number of times an authentication problem can be triggered, between 1 and 10. |
| Report Interval | Set the interval between reporting an authentication problem, between 30 and 3600 seconds. |
| **Networking Problem** | |
| Trigger Times | Set the number of times a network problem can be triggered, between 1 and 10. |
| Report Interval | Set the interval between reporting a network problem, between 30 and 3600 seconds. |

Related Links

Configure Client Mode Profiles on page 496

*Configure SSH*

Before you can configure SSH access on a device, you must first enable **SSH Availability**. Go to **Administration & Settings** > **Global Settings** > **Backup & Restore** > **VIQ Management** and toggle **SSH Availability** to **ON**.

ExtremeCloud IQ (New) provides a way to access devices remotely using the SSH protocol by using an SSH proxy server.

**Note**
It is important to remember that while SSH access is available, your device is exposed to public access through an SSH proxy. The device is protected only by the device administrator credentials, because SSH FTP assumes that it is run over a secure channel.

Use this task to enable SSH on a wireless device.

1. Go to **Monitoring** > **Network Devices** > **Device Status**.
2. Select at the end of a device row, and then select **Configure** > **Device**.
3. Under the **Additional Settings** menu, select **SSH**.
4. Under **Run Time**, select the length of time that you want SSH to be available for the device.

   Extreme Platform ONE Networking creates an SSH session for the specified length of time between the SSH proxy server and the device.
5. Select **Enable SSH**.

   Provide assisting technicians with the onscreen instructions and device log in credentials so they can open a session from their external SSH client to the specified IP address and port number of the proxy server.
6. When they are finished, select **Disable SSH**.

   The SSH session remains active for another minute or so and then automatically closes. If more time is required, enable a new SSH session.

Related Links

Configure Wireless Devices on page 187

## Configure Devices

terminates incoming GRE and GRE-over-IPsec tunnels from remote access points, enabling centralized routing for wireless client data as well as AP-originated RADIUS authentication and accounting traffic.

To configure the Tunnel Concentrator settings:

1. Go to **Monitoring** > **Network Devices** > **Device Status** > **Appliances**.
2. At the end of a device row, select the 3-dot menu (⋮).
3. Select **Configure** > **Device**.
4. Configure the device settings in Table 80.
5. Select **SAVE DEVICE CONFIGURATION**.



**Warning**
Making configuration changes at the device level overrides settings inherited from the assigned network policy template.

**Table 80: Device Details Settings**

| Field / Element | Description |
|---|---|
| Host Name (required) | A unique host name used to identify the Tunnel Concentrator on the network (for example, `1130C_1-TC1-V8KD2`). |
| Serial Number | The factory-assigned serial number of the Tunnel Concentrator instance. This field is read-only. |
| License Status | The current activation status of the Tunnel Concentrator license (for example, **Valid** or **Invalid**).<br>Select **SELECT FILE** to browse to and upload a license file (`.xlc`) to activate or renew the Tunnel Concentrator. |
| Mgt0 MAC Address | The hardware MAC address assigned to the primary management interface (`mgt0`) of the Tunnel Concentrator. This field is read-only. |
| Device Model | The hardware or virtual platform Tunnel Concentrator model. This field is read-only. |
| Device Function | The active software role or function assigned to the Tunnel Concentrator. This field is read-only. |
| Tunnel Concentrator Service | The name of the assigned Tunnel Concentrator Service profile bound to this Tunnel Concentrator. Select the service name link to open and view the corresponding Tunnel Concentrator Service configuration dialog. For more information, see Configure Tunnel Concentrator Services on page 535. |

# Device 360 View

The Device 360 view provides a comprehensive overview of the specifications and current status for the selected device.

Go to **Monitor** > **Network Devices** > **Device Status** and then select a **Device** name from the table. The **Device Details** window displays detailed information for the Wired, Wireless, Controller, Site Engine Managed, Tunnel Concentrator or UCP device.

Select **Actions** to perform specific tasks on the selected device. For more information, see Device 360 Actions Menu on page 235.

## Wired Device 360 View

The **Wired** Device 360 view provides a streamlined interface for reviewing device details. Allowing quick access to essential device-specific information.

Go to **Monitor** > **Network Devices** > **Device Status** > **Wired** and select a **Device** name from the table. The **Device Details** window displays the following detailed information for the wired device:

- Connection Status: The current network connectivity status of the device.
- Device Image: A visual representation or model image of the device.
- Device Location: The physical or configured location of the device.
- From the **Actions** menu you can perform actions for the selected device. For more information, see Device 360 Actions Menu on page 235.

  **Note**
  Not all actions are available for all devices.

- Installation Media Gallery: Select to upload an image (.png or .jpg less than 500KB) or video (.mp4 or .mov less than 5MB) file.
- Device Details: Key device information.
- Tags: Assigned tags for device categorization. Select **Add Tag** to manually add tags. Tags act as labels and help in easy filtering of the devices.
- Overview: Displays general device information.
- Clients: Lists device client details.
- Port Stats: Displays statistics for all device ports.
- Services/VLANs: Displays configured services and VLAN assignments.
- Routing: Provides routing configuration and status.
- Events: Lists system and device events.
- Alerts: Displays alerts and notifications triggered on the device.

To narrow the time frame, select the **Date & Time Range**, select a **Start Date** and **End Date**, select a **Start Time** and **End Time**, and then select **Done**. Select **Reset to Default** to reset back to the default time frame.

To refine the device list:

- Select and drag the left or right border of the column header to adjust the column width.
- Select and drag the column headers to change the order of the columns.

  **Note**
  Once columns are reordered, the layout is saved and persistent until it is manually changed.

- Select a column header to sort column data in ascending or descending order.
- Select **Columns** to add, remove, and reorder the columns.
- To refine the list, select **Filter**. The filter sidebar lets you customize what information is displayed in the device list. Available filters vary depending on the window you are in. To see all available options, in the filter area, select a section heading to see more or less items. To clear all active filters, select **Clear all filters** above the **Filters** panel.

*Overview*

**Overview** displays the following information about the selected device:

- **Device Health** widgets display:
  - CPU Usage
  - Memory Usage
  - Resource Utilization
  - PoE Usage
  - Temperature
  - Fan Status
  - Power Status

  By default, the data capture time frame is 24 hours.

  **Note**
  To view more information, select a widget.

- From the Port Configuration diagram, select individual ports or enable **Select All Ports** to reveal the following options:
  - Port Bounce
  - PoE Bounce
  - Cable Test
- From the interactive timeline graph:
  - View and filter:
    - Total CPU Utilized
    - Total Memory Utilized
    - Total MAC Table Utilized %
    - Temperature
    - PoE Usage Consumed
    - Fan Status
    - Power Supply Status

- Select any point along the timeline in the graphic to display details only for that precise time. To customize the time period for graphs, drag inside the timeline. The chart lines are interactive—hover over a line to see more data.
- Select ☰ to:
  - View in full screen
  - Print chart
  - Download PNG image
  - Download JPEG image
  - Download PDF document
  - Download SVG vector image

- Device widgets display **Usage Utilization**, **Client Health**, and **Throughput (Millions of Packets)**.

*Clients*

**Clients** displays the following information about the selected device:

- From the Port Configuration diagram, select individual ports or enable **Select All Ports** to reveal the following options:
  - Port Bounce
  - PoE Bounce
  - Cable Test
- From the interactive timeline graph:
  - View and filter:
    - Clients with Issues
    - Port Congestion
    - Unicast TX/RX
    - Broadcast TX/RX
    - Multicast TX/RX
    - Port Errors TX/RX
  - To narrow the time frame, select the **Date & Time Range**, select a **Start Date** and **End Date**, select a **Start Time** and **End Time**, and then select **Done**. Select **Reset to Default** to reset back to the default time frame.
  - Select any point along the timeline in the graphic to display details only for that precise time. To customize the time period for graphs, drag inside the timeline. The chart lines are interactive—hover over a line to see more data.
- Device widgets display **IP Connectivity Issues**, **Port Congestion**, **Traffic Anomalies**, and **Port Errors**.
- Select **Client Details** to display the following information:
  - Port Number
  - Client
  - MAC
  - Operating System
  - Connection Status

- IPv4
- IPv6
- VLAN

- Select **Client Traffic** to display the following information:
  - Connection Status
  - Client
  - VLAN
  - Port Number
  - Total Congestion (# of Packets)
  - Total Unicast (Packets%)
  - Total Multicast Packets
  - Total Broadcast (Packets%)
  - Total Port Errors

*Port Stats*

**Port Stats** displays the following information about the selected device:

- From the Port Configuration diagram, select individual ports or enable **Select All Ports** to reveal the following options:
  - Port Bounce
  - PoE Bounce
  - Cable Test
- From the interactive timeline graph:
  - View and filter:
    - Total TX/RX Bytes
    - Total TX/RX Unicast Pkts
    - Total TX/RX Broadcast Pkts
    - Total TX/RX Multicast Pkts
    - Total Errors
    - Total Queue Congestion
  - Narrow the time frame. Select the **Date & Time Range**, select a **Start Date** and **End Date**, select a **Start Time** and **End Time**, and then select **Done**. Select **Reset to Default** to reset back to the default time frame.
  - Select any point along the timeline in the graphic to display details only for that precise time. To customize the time period for graphs, drag inside the timeline. The chart lines are interactive—hover over a line to see more data.
- Device widgets display **Usage Utilization**, **Throughput (Millions of Packets)**, and **Congestion**.
- The description table lists the following details:



**Note**
You can use the **Search** field to filter the table view.

**Ports Description**:

- Port Number
- LLDP Neighbor
- MAC Locking
- Media Type
- Operational Status
- STP Port State
- Transmission Mode
- Link Speed

**Port Stats Summary** lists the following details:

- **% Utilization**
  - Port Number
  - % Utilization Rx
  - % Utilization Tx
  - % Utilization MaxRx
  - % Utlization MaxTx
- **In/Out Statistics**:
  - Port Number
  - InOctets
  - OutOctets
  - InUcastPkts
  - OutUcastPkts
  - InBroadcastPkts
  - OutBroadcastPkts
  - InMulticastPkts
  - OutMulticastPkts
  - Port Queue Congestion Count
- **Error**:
  - Port Number
  - Total Aggregated Port Errors Counter
- **Queue**:
  - Port Number
  - QP0 Pkt Cong | Xmts
  - QP1 Pkt Cong | Xmts
  - QP2 Pkt Cong | Xmts
  - QP3 Pkt Cong | Xmts
  - QP4 Pkt Cong | Xmts
  - QP5 Pkt Cong | Xmts
  - QP6 Pkt Cong | Xmts
  - QP7 Pkt Cong | Xmts
  - QP8 Pkt Cong | Xmts

**Link PoE**:

- Port Number
- Power Consumed per port, mW

*Services/VLANs*

**Services/VLANs** displays the following information about the selected device:

- From the Port Configuration diagram, select individual ports or enable **Select All Ports** to reveal the following options:
  - Port Bounce
  - PoE Bounce
  - Cable Test
- A table lists the following details about the clients that are connected during the specified time range:
  - VLAN Id
  - VLAN Name
  - Total Active Ports

- Total Tagged Ports
- STP Instance

**Note**
You can use the **Search** field to filter the table view.

*Routing*

**Routing** displays the following information about the selected device:

- From the Port Configuration diagram, select individual ports or enable **Select All Ports** to reveal the following options:
  - Port Bounce
  - PoE Bounce
  - Cable Test
- From the interactive timeline graph:
  - View and filter:
    - Total Routes
    - Direct Routes
    - Static Routes
    - OSPF Routes
    - IS-IS Routes
    - BGP Routes
  - Narrow the time frame. Select the **Date & Time Range**, select a **Start Date** and **End Date**, select a **Start Time** and **End Time**, and then select **Done**. Select **Reset to Default** to reset back to the default time frame.
  - Select any point along the timeline in the graphic to display details only for that precise time. To customize the time period for graphs, drag inside the timeline. The chart lines are interactive—hover over a line to see more data.
- The **IPv4/IPv6 Routing Table** lists the following details:
  - Destination
  - Next Hop
  - VLAN Name
  - VLAN Id
  - Service Name
  - Service ID
  - Route Origin
  - Status
  - Metric
  - Route Type Priority
  - Routing Instance

**Note**
- Select **Refresh Routing Table** to update the table with the most current data.
- Use the **Search** field to filter the table view.

*Events*

**Events** displays the following information about the selected device:

- From the **Events** interactive timeline graph:
  - View and filter by **Critical**, **Major**, **Minor**, **info**, and **Clear** events.
  - Select any point along the timeline in the graphic to display details only for that precise time. To customize the time period for graphs, drag inside the timeline. The chart lines are interactive—hover over a line to see more data.
  - Select ☰ to:
    - View in full screen
    - Print chart
    - Download PNG image
    - Download JPEG image
    - Download PDF document
    - Download SVG vector image
- The **Events** table lists the following details:
  - Timestamp
  - Severity
  - Component
  - Description



**Note**
You can use the **Search** field to filter the table view.

*Alerts*

**Alerts** provides the following information about the selected wireless device:

- An interactive graph shows the number of alerts raised on the current device, for the specified time frame. By default, the data capture time frame is 24 hours.
  - To customize the graph, select any **Filter by** option from the list (Critical Alerts, Warning Alerts, and Information Alerts).
  - To narrow the time frame, select the **Date & Time Range**, select a **Start Date** and **End Date**, select a **Start Time** and **End Time**, and then select **Done**. Select **Reset to Default** to reset back to the default time frame.
- The **Alerts by Severity** widget displays the total number of **Alerts Raised** for the specified time range, with the colored bands of the arch and color-matched beads below it representing refinements on the basis of **Severity**, as follows:
  - Critical
  - Warning
  - Information

  By default, the data capture time frame is 24 hours.
- A table lists the following alert details during the specified time range:
  - Alert Name
  - Summary
  - Location
  - Category

- Severity
- Status
- Application
- Source
- Timestamp

To view alert details, select an **Alert Name**. The **Alert Details** pane displays the following information:

- Severity
- Description
- Detected
- Source:
  - Name
  - Type
- Details:
  - Model
  - MAC Address
  - Application
  - Serial Number
  - Admin State
  - IP Address
  - Location

**Note**
Select **Acknowledge** to mark the alert as reviewed. Acknowledging an alert does not resolve the issue, but it signals that the alert has been reviewed. This helps reduce duplicate investigations and allows teams to track which alerts are actively being addressed or have already been acknowledged.

- Select to export filtered alerts.
- You can use the **Search** field to filter the table view.

## Wireless Device 360 View

The **Wireless** Device 360 view provides a streamlined interface for reviewing device details. Allowing quick access to essential device-specific information.

Select a **Device** name from the **Wireless** table. The **Device Details** window displays the following detailed information for the wireless device:

- Connection Status
- Device Image
- Floor Map (if available)
- Device Location
- Installation Reports
- Installation Media Gallery: Select to upload an image (.png or .jpg less than 500KB) or video (.mp4 or .mov less than 5MB) file.
- From the **Actions** menu you can perform actions for the selected device. For more information, see Device 360 Actions Menu on page 235.

**Note**
Not all actions are available for all devices.

- Overview
- Wireless Interfaces

- Wired Interfaces
- Clients
- Events
- Alerts

To narrow the time frame, select the **Date & Time Range**, select a **Start Date** and **End Date**, select a **Start Time** and **End Time**, and then select **Done**. Select **Reset to Default** to reset back to the default time frame.

To refine the device list:

- Select and drag the left or right border of the column header to adjust the column width.
- Select and drag the column headers to change the order of the columns.

  **Note**
  Once columns are reordered, the layout is saved and persistent until it is manually changed.

- Select a column header to sort column data in ascending or descending order.
- Select **Columns** to add, remove, and reorder the columns.
- To refine the list, select **Filter**. The filter sidebar lets you customize what information is displayed in the device list. Available filters vary depending on the window you are in. To see all available options, in the filter area, select a section heading to see more or less items. To clear all active filters, select **Clear all filters** above the **Filters** panel.

*Actions*

From the **Actions** menu you can perform the following actions for the selected device:

- Reboot on page 212
- Reset Factory Settings on page 212
- Upgrade Firmware on page 213
- Locate on page 213
- VLAN Probe on page 143

**Reboot**

To restart a connected device, select **Reboot**, and then select **Yes** to confirm. Restarting momentarily disconnects any connected clients.

**Note**
The current configuration will not be saved before the reboot.

**Reset Factory Settings**

To reset the selected device to their default configuration, select **Reset Factory Settings**, and then select **Yes** to confirm.

**Important**
This operation removes existing settings from the selected device and returns it to factory settings. It then reconnects to the cloud as a new device.

### Upgrade Firmware

Use this task to manually upgrade firmware for a selected device.

1. Go to **Network Devices** > **Device Status**, and then select a device name from the **Device** column.
2. From the **Actions** menu, select **Upgrade firmware**.
3. Select a **Firmware Version**.
4. Select a **Firmware Upgrade Schedule**:
   - To update immediately, select **Upgrade Now**, and then select **Upgrade Firmware**.
   - To update at a later time, select **Upgrade Later**, select a **Date & Time** , and then select **Schedule Firmware Update**.

   **Note**
   Firmware upgrades can be scheduled up to 30 days in advance.

5. Select ⋮ to view **Firmware Upgrade History**. Firmware upgrade activity is stored for a maximum of 30 days.

   **Note**
   To reschedule a scheduled firmware upgrade:
   - Select a scheduled upgrade, and then select **Reschedule Upgrade**.
   - Select a new **Date & Time**, and then select **Reschedule**.

### Locate

Use this task to locate the physical location of a selected device.

1. Select **Locate**, and then configure the **Locate Device** settings in Table 81.

**Table 81: Locate Device Settings**

| Field | Description |
|---|---|
| LED Color | Select one of the following blinking light colors to set the color that the locator light will flash to help you find the AP:<br>• Amber<br>• White<br>• Off |
| Blink Mode | Select one of the following blinking modes to set the speed at which the locator light will flash to help you find the AP:<br>• Fast<br>• Slow<br>• Steady |

**Note**
Select **Return to Standard LED operations**, and then select **Submit**, to stop the blinking lights used for locating the device.

2. Select **Submit**.

### VLAN Probe

The VLAN probe action locates available VLANs for the selected device. When the VLAN probe is complete, a table shows the host name, MAC address, available VLANs, unavailable VLANs, and their status.

**Note**
The VLAN Probe Utility is also available from the device list for a connected device.

Use this task to verify the VLAN probe results and status of VLAN for selected device.

1. Go to **Monitoring** > **Network Devices** > **Device Status**.
2. Select the check boxes for the devices you want to probe.

**Note**
You can select a single device or multiple devices to run the probe concurrently.

3. From the **3-dot Menu** (⋮) at the end of a device row, select **Utilities** > **VLAN Probe**.
4. Configure the VLAN Probe settings in Table 82.

**Table 82: VLAN Probe Settings**

| Field | Description |
|---|---|
| VLAN Range | The range of VLAN IDs to probe (1-4094). You can enter a single value or a range (for example, 1-100).<br>You can enter up to five ranges separated by commas. However, range numbers cannot overlap. For example, `1, 2-7, 8, 9-20`. |
| Timeout (optional) | The number of seconds to wait for a reply from each probe, from 1 to 60 seconds. Default is 5 seconds. |
| Probe Retries (optional) | The number of retry attempts for each probe, from 1 to 10. Default is 1. |

5. Select **Start** to start a probe.

   A progress bar indicates the status of the probe.
6. (Optional) Select **Stop** to stop a probe before it completes.

When the probe completes, the VLAN Probe Results appear. A timestamp indicates when they were last updated. A summary includes Status, Start Time, Duration, and device counts for Total, Passed, Failed, Stopped, and Running.

The results table lists all devices included in the VLAN probe and provides the Host Name, MAC Address, Available VLANs, Unavailable VLANs, and Status. To view detailed VLAN results for a specific device, expand its row in the Status column. A sub-table opens, showing the VLAN ID, Availability status, and IP Address for each probed VLAN.

*Overview*

**Overview** displays the following information about the selected device:

- The **Connection Chain** diagram shows how the device connects to the internet and to ExtremeCloud IQ (New).
- The following widgets appear below the connection chain diagram:
  - Device Health
  - Connectivity Issues
  - Excessive Packet Loss

  By default, the data capture time frame is 24 hours.

  **Note**
  The selected time period applies to the widgets as well as the connection chain diagram.

- System Information for the selected device.
- Tunnel Concentrator Status: Displays AP-reported tunnel health, endpoint states, and tunneled client counts for APs associated with a Tunnel Policy.

#### Tunnel Concentrator Status

When an AP is configured with a Tunnel Policy, the **Tunnel Concentrator Status** section appears in the AP's Wireless Device 360 View. The status data is reported directly by the AP and reflects the current operational state of each configured Tunnel Concentrator (TC) endpoint.

The section groups tunnel status entries by **Tunnel Policy Name**. Each group lists the configured TC endpoints (Primary, Secondary, and Tertiary) and shows whether each endpoint is active or on standby. This visibility allows network administrators to quickly assess tunnel health and AP-level failover state from a single view.

**Note**
**Tunnel Concentrator Status** is only visible for APs that have a Tunnel Policy assigned. APs without a Tunnel Policy do not display this section. For more information, see Configure Tunnel Policies on page 542.

Tunnel Concentrators support two levels of high availability:

- Appliance-level HA: Two TC appliances can be paired in an primary/backup relationship using VRRP. The **State** column in the Tunnel Concentrator Status table reflects which appliance is currently active and which is standby.
- AP-level HA: Each AP can be configured with up to three TC endpoint pairs—**Primary**, **Secondary**, and **Tertiary**. If connectivity to the Primary endpoint is lost, the AP automatically fails over to the Secondary, then to the Tertiary. The Tunnel Concentrator Status table shows the current operational state for all configured endpoint tiers.

For information about monitoring the Tunnel Concentrator appliance itself—including system metrics, licensing, and appliance-level configuration—see Tunnel Concentrator Device 360 View on page 225.

**Table 83: Tunnel Concentrator Status Fields**

| Field | Description |
|---|---|
| Tunnel Policy | The name of the Tunnel Policy configured on the AP. Tunnel status entries are grouped by Tunnel Policy Name. Select **›** to reveal detailed endpoint breakdown. For more information, see Detailed Endpoint Breakdown (Expanded View) on page 216. |
| Service Name | The name of the associated Tunnel Concentrator service. |
| Status | Operational tunnel connectivity state. |
| MTU Status | Health status of tunnel Maximum Transmission Unit (MTU) detection across the tunnel path. |
| Configured MTU | The configured MTU value on the tunnel interface (0 = auto/ default). |

#### Detailed Endpoint Breakdown (Expanded View)

Selecting the expand icon (**›**) next to a Tunnel Policy row displays child details for individual Tunnel Concentrator endpoints, including:

- **TC Endpoints**: Primary, Secondary, and Tertiary endpoints configured for High Availability.
- **Endpoint IP Address**: IPv4 address of each TC endpoint node.
- **Endpoint State**: Role and state (`ACTIVE` or `STANDBY`).
- **Tunneled Client Count**: Number of active wireless clients routed through each TC endpoint.

*Wireless Interfaces*

**Wireless Interface** provides the following information about the selected wireless device's radios and their performance:

- An interactive timeline graph displaying channel utilization and connected clients. Select a **Radio** (Wi-Fi 0, Wi-Fi 1, or Wi-Fi 2) and **Filter by** Channel Utilization % and Connected Clients.
- Summary tables for **Wi-Fi 0**, **Wi-Fi 1**, and **Wi-Fi 2**, including **Channel Utilization Details** widgets. Each widget provides key performance metrics, including percentages for Interference, Tx Retries, and Rx Retries, helping you assess channel quality and identify potential issues.

  **Note**
  The **Wi-Fi 2** tab does not display for AP3020W devices. To view 6 GHz channel availability, set the operating mode to **6/5**.

- The **Surrounding Access Points** table provides the following details about surrounding APs:
  - **Device**: The name or identifier of the AP.
  - **MAC (BSSID)**: The host name of the surrounding AP. If the host name is not known, the BSSID displays instead.

- **SSID**: The network name broadcast by the AP. If multiple SSIDs are available, you can select the SSID value to open a detail pane listing all SSIDs for that AP.
- **Channel**: The RF channel currently used by the AP.
- **Width (MHz)**: The channel width in megahertz, indicating bandwidth allocation.
- **Band (GHz)**: The APs frequency band (2.4 GHz, 5 GHz, or 6 Hz).
- **RSSI**: The Received Signal Strength Indicator (RSSI), showing signal strength from the AP.
- **Mode**: The wireless mode or standard in use.
- **Rogue AP/Friendly AP**: Indicates whether the AP is classified as rogue or friendly.
- **Extreme Device**: Identifies if the AP is an Extreme Networks device.
- **Channel Utilization (%)**: The percentage of channel usage, reflecting congestion level.
- **Cyclical Redundancy Check** (CRC): CRC error count, indicating potential data integrity issues.
- **Clients**: The number of client devices currently connected to the AP.

*Wired Interface*

**Wired Interface** provides the following interface details about the selected wireless device:

- State
- Admin State
- Interface
- Power Draw *
- Port
- Speed
- Tx Bytes
- Rx Bytes
- Tx Errors
- Rx Errors
- Tx Drops
- Rx Drops

* Reports the actual Power over Ethernet (PoE) power consumed by the access point on its primary eth0 interface in Watts (W), rounded to the nearest whole integer.

**Note**
PoE Power Draw reporting supports AP3000, AP5000, AP5020, AP4020, AP302W, AP305C, and AP4000 series access points.

*Clients*

**Clients** provides the following information about the selected wireless device:

- An interactive timeline graph shows the number of clients connected to the current device, for the specified time frame. By default, the data capture time frame is 24 hours.

  You can select any point along the timeline in the graphic to display details only for connected clients at that precise time. To customize the time period for graphs, drag inside the timeline. The chart lines are interactive. Hover over a line to see more data.
- **Client Statics** displays the following widgets:
  - Total Clients within selected time range: Displays the number of clients.
  - Clients with poor health: Displays the number of clients.
  - Total Unique Clients: Displays

  By default, the data capture time frame is 24 hours.

- A table lists the following details about the clients that are connected during the specified time range:
  - Connection Status
  - Client
  - Site
  - SNR
  - RSSI
  - Frequency
  - Channel Utilization %
  - Association Issues
  - Authentication Issues

**Note**
You can use the **Search** field to filter the table view.

*Events*

**Events** displays the following information about the selected device:

- An interactive timeline graph, from which you can:
  - View and filter **Critical**, **Major**, **Minor**, **info**, and **Clear**.
  - Select any point along the timeline in the graphic to display details only for that precise time. To customize the time period for graphs, drag inside the timeline. The chart lines are interactive—hover over a line to see more data.
  - Select ≡ to:
    - View in full screen
    - Print chart
    - Download PNG image
    - Download JPEG image
    - Download PDF document
    - Download SVG vector image
- A table lists the following details:
  - **Timestamp**: The time that the event occurred.
  - **Severity**: Identifies the event as major, informational, or cleared.
  - **Category**: The type of event, for example, status or threshold changes.
  - **Description**: A brief explanation of the event.
  - **Host Name**: The host name of the device on which the event occurred.
  - **Device MAC**: The MAC address of the device that reported the event.
  - **Client MAC**: The MAC address of the client that reported the event.

*Alerts*

**Alerts** provides the following information about the selected wireless device:

- An interactive graph shows the number of alerts raised on the current device, for the specified time frame. By default, the data capture time frame is 24 hours.

To customize the graph, select any **Source** from the list (Critical Alerts, Warning Alerts, and Information Alerts).

- The **Alerts by Severity** widget displays the total number of **Alerts Raised** for the specified time range, with the colored bands of the arch and color-matched beads below it representing refinements on the basis of **Severity**, as follows:
  - Critical
  - Warning
  - Info

  By default, the data capture time frame is 24 hours.
- A table lists the following alert details during the specified time range:
  - Alert Name
  - Summary
  - Severity
  - Status
  - Category
  - Source
  - Timestamp

  To view alert details, select an **Alert Name**. The **Alert Details** pane displays the following information:
  - Severity
  - Description
  - Source:
    - Name
    - Type
  - Details:
    - Model
    - MAC Address
    - Application
    - Serial Number
    - Admin State
    - IP Address
    - Location

  **Note**
  Select **Acknowledge** to mark the alert as reviewed. Acknowledging an alert does not resolve the issue, but it signals that the alert has been reviewed. This helps reduce duplicate investigations and allows teams to track which alerts are actively being addressed or have already been acknowledged.
- Select to export filtered alerts.
- You can use the **Search** field to filter the table view.

## Controller Device 360 View

The **Controller** Device 360 view provides a streamlined interface for reviewing controller details. Allowing quick access to essential controller-specific information.

Go to **Monitoring** > **Network Devices** > **Device Status** > **Appliances** and select a controller **Device** name from the **Appliances** table. The **Device Details** window displays the following detailed information for the controller:

- Connection Status
- Appliance Image

- Installation Media Gallery: Select to upload an image (.png or .jpg less than 500KB) or video (.mp4 or .mov less than 5MB) file.
- Device Details: Hostname, Controller Type, SSID, Model, Function, Device Template, Configuration Type, Serial Number, Device Status, Mgt0 Addresses, IPv Subnet Masks, IPv Default Gateways, Mgt0 MAC Address, DNS, and NTP.
- Wired Interfaces
- Clients

To narrow the time frame, select the **Date & Time Range**, select a **Start Date** and **End Date**, select a **Start Time** and **End Time**, and then select **Done**. Select **Reset to Default** to reset back to the default time frame.

To refine the device list:

- Select and drag the left or right border of the column header to adjust the column width.
- Select and drag the column headers to change the order of the columns.



**Note**
Once columns are reordered, the layout is saved and persistent until it is manually changed.

- Select a column header to sort column data in ascending or descending order.
- Select **Columns** to add, remove, and reorder the columns.
- To refine the list, select **Filter**. The filter sidebar lets you customize what information is displayed in the device list. Available filters vary depending on the window you are in. To see all available options, in the filter area, select a section heading to see more or less items. To clear all active filters, select **Clear all filters** above the **Filters** panel.

*Controller Device 360 View | Wired Interface*

**Wired Interface** provides the following interface details about the selected controller:

- Status
- Interface
- Speed

*Controller Device 360 View | Clients*

**Clients** provides the following information about the clients that are connected to the selected controller during the specified time range:

- Connection Status
- Type
- Operating System
- Health Status
- Client*
- MAC Address*
- IPv4 Address
- IPv6 Address
- User Name
- VLAN
- SSID
- RSSI
- SNR

* Select to view client details.

**Note**
You can use the **Search** field to filter the table view.

## Site Engine Managed Device 360 View

The Site Engine Managed Device 360 view provides detailed monitoring information for devices managed byExtremeCloud Site Engine (XIQ-SE), including port statistics, health data, events, and diagnostics.

Go to **Monitor** > **Network Devices** > **Device Status** > **Appliances** and select an XIQ-SE **Device** name from the table.

The **Device Details** window displays the following detailed information for the wired device:

- Connection Status: The current network connectivity status of the device.
- Device Image: A visual representation or model image of the device.
- From the **Actions** menu you can perform actions for the selected device. For more information, see Device 360 Actions Menu on page 235.

  **Note**
  Not all actions are available for all devices.

- Device Details: Key device information.
- Overview: Displays general device information.
- Port Stats: Displays statistics for all device ports.
- Events: Lists system and device events.
- Alerts: Displays alerts and notifications triggered on the device.

To narrow the time frame, select the **Date & Time Range**, select a **Start Date** and **End Date**, select a **Start Time** and **End Time**, and then select **Done**. Select **Reset to Default** to reset back to the default time frame.

To refine the device list:

- Select and drag the left or right border of the column header to adjust the column width.
- Select and drag the column headers to change the order of the columns.

  **Note**
  Once columns are reordered, the layout is saved and persistent until it is manually changed.

- Select a column header to sort column data in ascending or descending order.
- Select **Columns** to add, remove, and reorder the columns.
- To refine the list, select **Filter**. The filter sidebar lets you customize what information is displayed in the device list. Available filters vary depending on the window you are in. To see all available options, in the filter area, select a section heading to see more or less items. To clear all active filters, select **Clear all filters** above the **Filters** panel.

*Site Engine Managed Device 360 View | Overview*

**Overview** displays the following information about the selected device:

- **Device Health** widgets display:
  - CPU Usage
  - Memory Usage
  - Resource Utilization
  - Temperature
  - Fan Status
  - Power Status

  By default, the data capture time frame is 24 hours.

  **Note**
  To view more information, select a widget.

- From the interactive timeline graph:
  - View and filter:
    - Total CPU Utilized
    - Total Memory Utilized
    - Temperature
    - Fan Status
    - Power Supply Status
  - Select any point along the timeline in the graphic to display details only for that precise time. To customize the time period for graphs, drag inside the timeline. The chart lines are interactive—hover over a line to see more data.
  - Select ☰ to:
    - View in full screen
    - Print chart
    - Download PNG image
    - Download JPEG image
    - Download PDF document
    - Download SVG vector image
- Device widgets display **Wired Utilization** and **Throughput**.

*Site Engine Managed Device 360 View | Port Stats*

**Port Stats** displays the following information about the selected device:

- From the interactive timeline graph:
  - View and filter:
    - Total TX/RX Utilization %
    - Total TX/RX Throughput Bbps
    - Total TX/RX Unicast Pkts
    - Total TX/RX Broadcast Pkts

        - Total TX/RX Multicast Pkts
        - Total Errors
    - Narrow the time frame. Select the **Date & Time Range**, select a **Start Date** and **End Date**, select a **Start Time** and **End Time**, and then select **Done**. Select **Reset to Default** to reset back to the default time frame.
    - Select any point along the timeline in the graphic to display details only for that precise time. To customize the time period for graphs, drag inside the timeline. The chart lines are interactive—hover over a line to see more data.
- Device widgets display **Wired Utilization** and **Throughput**.
- The description table lists the following details:

  **Note**
  You can use the **Search** field to filter the table view.

  **Ports Description**:

    - Port Number
    - LLDP Neighbor
    - Media Type
    - Operational Status
    - Transmission Mode
    - Default Port Mode
    - Link Speed

  **Port Stats Summary**:
    - **% Utilization**
        - Port Number
        - % Utilization Rx
        - % Utilization Tx
        - % Utilization MaxRx
        - % Utlization MaxTx
    - **In/Out Statistics**:
        - Port Number
        - InOctets
        - OutOctets
        - InUcastPkts
        - OutUcastPkts
        - InBroadcastPkts
        - OutBroadcastPkts
        - InMulticastPkts
        - OutMulticastPkts
        - InFlowCtrlPkts
        - OutFlorCtrlPkts
        - Port Queue Congestion Count
    - **Error**:
        - Port Number
        - Total Aggregated Port Errors Counter

*Site Engine Managed Device 360 View | Events*

**Events** table displays the following information about the selected device:

- Timestamp
- Severity

- Category
- Description

**Note**
You can use the **Search** field to filter the table view.

*Site Engine Managed Device 360 View | Alerts*

**Alerts** provides the following information about the selected wireless device:

- An interactive graph shows the number of alerts raised on the current device, for the specified time frame. By default, the data capture time frame is 24 hours.
  - To customize the graph, select any **Filter by** option from the list (Critical Alerts, Warning Alerts, and Information Alerts).
  - To narrow the time frame, select the **Date & Time Range**, select a **Start Date** and **End Date**, select a **Start Time** and **End Time**, and then select **Done**. Select **Reset to Default** to reset back to the default time frame.
- The **Alerts by Severity** widget displays the total number of **Alerts Raised** for the specified time range, with the colored bands of the arch and color-matched beads below it representing refinements on the basis of **Severity**, as follows:
  - Critical
  - Warning
  - Information

  By default, the data capture time frame is 24 hours.
- A table lists the following alert details during the specified time range:
  - Alert Name
  - Summary
  - Severity
  - Status
  - Category
  - Source
  - Timestamp

  To view alert details, select an **Alert Name**. The **Alert Details** pane displays the following information:
  - Severity
  - Description
  - Detected
  - Source:
    - Name
    - Type
  - Details:
    - Model
    - MAC Address
    - Application
    - Serial Number
    - Admin State
    - IP Address
    - Location

**Note**
Select **Acknowledge** to mark the alert as reviewed. Acknowledging an alert does not resolve the issue, but it signals that the alert has been reviewed. This helps reduce duplicate investigations and allows teams to track which alerts are actively being addressed or have already been acknowledged.

- Select to export filtered alerts.
- You can use the **Search** field to filter the table view.

## Tunnel Concentrator Device 360 View

The **Tunnel Concentrator** Device 360 view provides a streamlined interface for reviewing device details. Allowing quick access to essential device-specific information.

Go to **Monitor** > **Network Devices** > **Device Status** > **Appliances** and select a **Device** name from the table. The details window displays the following detailed information for the wired device:

- Connection Status: The current network connectivity status of the Tunnel Concentrator appliance.
- Device Image: A visual representation or model image of the device.
- From the **Actions** menu you can perform actions for the selected device. For more information, see Device 360 Actions Menu on page 235.

  **Note**
  Not all actions are available for all devices.

- Installation Media Gallery: Select to upload an image (.png or .jpg less than 500KB) or video (.mp4 or .mov less than 5MB) file.
- **Device Details**: Key appliance information, including hostname, network policy, model, function, configuration type, serial number, firmware version, device status, Tunnel Concentrator Service, tunnel IP address, and management interface address, as defined in Table 84 on page 227.
- **Overview**: A topology diagram showing the Tunnel Concentrator's connection paths to ExtremeCloud IQ (New) and the Internet.

  The topology diagram includes the following nodes:
  - ExtremeCloud IQ: Represents the cloud management platform. A connection line between the Tunnel Concentrator appliance and this node indicates the appliance is actively managed and connected.
  - Tunnel Concentrator Appliance: Displayed centrally in the topology view, identified by its hostname and device type icon.
  - Internet: Represents the upstream internet path. A connection line indicates the appliance has a routable upstream internet path available.

**Note**
The **Tunnel Concentrator** Device 360 view displays system-level metrics, licensing, and configuration for the Tunnel Concentrator appliance itself.

To monitor AP-reported tunnel health—including per-AP tunnel endpoint state (ACTIVE/STANDBY), client counts, and direct appliance access—see Tunnel Concentrator Status on page 215 in the Wireless Device 360 View.

For more information, see the Extreme Tunnel Concentrator Documentation.

*Tunnel MTU Status and Mismatches*

ExtremeCloud IQ (New) displays tunnel MTU status in the Tunnel Concentrator Device 360 view, providing visibility into active tunnel health and MTU consistency across connected access points. The following MTU information is available:

- Configured MTU vs. Measured MTU: Compares the maximum configured payload size with the active data-plane MTU discovered by ICMP keep-alive probes.
- MTU Mismatch Warning: A status indicator appears when an intermediate hop reduces the available path MTU below the configured tunnel threshold.

When an MTU mismatch alert is flagged, adjust the MTU threshold under the assigned Tunnel Policy or adjust intermediate switch/router MTU settings accordingly.

*High Availability*

Tunnel Concentrators support two levels of high availability:

- Appliance-level HA: Two Tunnel Concentrator appliances can be paired in an active/backup relationship using VRRP. The State column in the Tunnel Concentrator Status table reflects which appliance is currently ACTIVE and which is STANDBY.
- AP-level HA: Each access point can be configured with up to three Tunnel Concentrator endpoint pairs: Primary, Secondary, and Tertiary. If connectivity to the Primary endpoint is lost, the access point automatically fails over to the Secondary, then the Tertiary.

*Tunnel Concentrator Status*

ExtremeCloud IQ (New) displays Tunnel Concentrator Status in the Wireless Device 360 view for access points that have a Tunnel Policy assigned. The status data is reported directly by the access point and reflects the current operational state of each configured Tunnel Concentrator endpoint.

The Tunnel Concentrator Status section groups tunnel status entries by Tunnel Policy Name and provides the following information:

- Tunnel Policy: The name of the Tunnel Policy configured on the access point.
- Service Name: The name of the associated Tunnel Concentrator service.
- Status: The operational tunnel connectivity state.
- MTU Status: The health status of tunnel MTU detection across the tunnel path.
- Configured MTU: The configured MTU value on the tunnel interface.

Selecting the expand icon next to a Tunnel Policy row displays endpoint details, including the endpoint IP address, endpoint state (ACTIVE or STANDBY), and the number of active wireless clients routed through each endpoint.

For more information, see Tunnel Concentrator Status on page 215 in the Wireless Device 360 view.

*Configuration*

ExtremeCloud IQ (New) provides configuration options for Tunnel Concentrator services and tunnel policies. The following configuration tasks are available:

- Configure Tunnel Concentrator Services: Define the Tunnel Concentrator service profile bound to a Tunnel Concentrator appliance. See Configure Tunnel Concentrator Services on page 535.
- Configure Tunnel Concentrator Address Pool (TCAP) Profiles: Define address pools for tunnel termination. See Configure Tunnel Concentrator Address Pool (TCAP) Profiles on page 541.
- Configure Tunnel Policies: Define tunnel policy settings for access points, including Primary, Secondary, and Tertiary Tunnel Concentrator endpoint assignments. See Configure Tunnel Policies on page 542.

*Network Connectivity Verification*

ExtremeCloud IQ (New) provides a Ping action for Tunnel Concentrator appliances. From the Tunnel Concentrator Device 360 view, select **Actions**, and then select **Ping** to send a ping request from the Tunnel Concentrator to verify network connectivity.

*Tunnel Concentrator Details*

**Table 84: Tunnel Concentrator — Device 360 Device Details**

| Field | Description |
|---|---|
| Hostname | The configured hostname of the Tunnel Concentrator. |
| Network Policy | The network policy assigned to this device. |
| Model | The device model identifier. Always displays *TUNNELCONCENTRATOR* for Tunnel Concentrator devices. |
| Function | The device function role. Always displays *XIQTC*. |
| Configuration Type | The IP address configuration method. |
| Serial Number | The device serial number in the format *TC01NNNNE-VXXXX*. |
| Version | The firmware version currently running on the device. |
| Device Status | The current management state of the device. |
| Tunnel Concentrator Service | The Tunnel Concentrator service configured for this device. Displays N/A if no service is assigned. |
| Tunnel IP Address | The IP address of the GRE tunnel interface. |
| IPv4 Subnet Mask | The subnet mask of the tunnel interface. Displays N/A if not configured. |
| IPv4 Default Gateway | The default gateway for the management interface. Displays N/A if not configured. |
| Mgt0 IPv4 Address | The MAC address of the management interface (Mgt0). |

## Universal Compute Platform Device 360 View

The **UCP Device 360 view** provides a comprehensive overview of the selected UCP appliance, including device health metrics, port status, network throughput, installed applications, and device management actions.

Go to **Monitor** > **Network Devices** > **Device Status** > **Appliances** and select a UCP **Device** name from the table.

The details window displays the following detailed information for the wired device:

- Connection Status: The current network connectivity status of the device.
- Device Image: A visual representation or model image of the device.
- From the **Actions** menu you can perform actions for the selected device. For more information, see Device 360 Actions Menu on page 235.

  **Note**
  Not all actions are available for all devices.

- Installation Media Gallery: Select to upload an image (.png or .jpg less than 500KB) or video (.mp4 or .mov less than 5MB) file.
- **Device Details**: Key information about the device, as defined in Table 85 on page 228.
- Overview: Provides a real-time summary of appliance performance, port status, and installed applications.
- Events: Lists system and device events.
- Alerts: Displays alerts and notifications triggered on the device.

**Table 85: UCP Device 360 — Device Details**

| Field | Description |
|---|---|
| System Name | The configured hostname of the device. |
| IP Address | The management IP address of the device. |
| MAC | The MAC address of the device. |
| Model | The UCP model designation (for example, *4120C*). |
| Serial Number | The unique serial number of the device. UCP serial numbers follow the format *PPPPYYWWM-MXXXX*, where the first four characters (prefix) identify the UCP model. For example, *XC01* identifies a UCP 4120C. |
| Make | The hardware category. Displays *Appliance* for UCP devices. |
| Firmware Version | The firmware version currently installed on the appliance. |
| OpenAPI Version | The OpenAPI version supported by the appliance. Displays N/A if not applicable. |
| System Description | A system description string for the appliance (for example, *UCP1211-00ABC-Default(0.0.0.0_A0) (Private)*). |

*UCP Device 360 View | Overview*

The **Overview** tab provides a real-time summary of appliance performance, port status, and installed applications.

- **Device Health**: The Device Health widgets display the information as described in Table 86 on page 229. By default, the data time frame is 24 hours.
- The port diagram displays the logical connectivity status for the ports on the selected UCP appliance. Active ports are displayed with a highlighted indicator; inactive ports are dimmed. Select individual ports or enable **Select All Ports** to reveal the following options:
  - Port Bounce
  - PoE Bounce
  - Cable Test
- From the interactive timeline graph:
  - View and filter:
  - Select any point along the timeline in the graphic to display details only for that precise time. To customize the time period for graphs, drag inside the timeline. The chart lines are interactive—hover over a line to see more data.
  - To narrow the time frame, select the **Date & Time Range**, select a **Start Date** and **End Date**, select a **Start Time** and **End Time**, and then select **Done**. Select **Reset to Default** to reset back to the default time frame.
- Installed Applications: Lists all applications installed on UCP.

**Table 86: UCP Health Widgets**

| Widget | Description |
|---|---|
| CPU Usage | Current CPU utilization as a percentage. |
| Memory Usage | Current memory utilization as a percentage. |
| Resource Utilization | Aggregate resource utilization for the appliance. |
| Temperature | Current thermal status. Displays *No Issues* when operating within normal range. |
| Fan Status | Current fan health. Displays *No Issues* when all fans operate normally. |
| Power Status | Current power supply status. Displays *No Issues* when power supplies are operating normally, or indicates the number of issues detected. |

#### Installed Applications

The **Installed Applications** table lists all applications installed on UCP, including:

- **Status**: Indicates whether the application is running, stopped, or the installation progress.
- **Application Name**: The name of the installed application.

- **Instances**: The running instances for the application.

**Note**
If UCP has no installed applications, the message `No installed applications found` displays. To install an application, go to **Supported Applications**, and then from the 3-dot (⋮) menu, select **Install**. The selected application is then installed on UCP.

#### Installed Application Actions

The following actions are available from the 3-dot (⋮) menu, depending on the application status.

**Table 87: Installed Application Actions by Status**

| Action | Status | Description |
|---|---|---|
| **Open Application UI** | Running | Opens the local web-based management interface of the application installed on a UCP node. The interface opens in a separate browser tab and is accessed through UCP connection. |
| **Open Console** | Running | Opens an interactive SSH console session for the selected UCP in a dedicated pane. For more information, see Open the UCP Console on page 241. |
| **Stop** | Running | Stops the running application. The application transitions to `Stopped` state. Use **Start** to restart the application without reinstalling it. For more information, see Start or Stop a UCP Application on page 240. |
| **Start** | Stopped | Launches a stopped application. The status transitions from `Stopped` to `Starting` to `Running`. For more information, see Start or Stop a UCP Application on page 240. |
| **Uninstall** | Running or Stopped | Removes the application from UCP and returns the device to a clean state. After uninstalling, you can install a different application. For more information, see Uninstall an Application from UCP on page 240. |

- For **Running** applications:
  - **Open Console**: Opens an interactive console session for the application.
  - **Stop**: Stops the running application.
  - **Uninstall**: Removes the application from the device.
- For **Stopped** applications:
  - **Start**: Launches the application.
  - **Uninstall**: Removes the application from the device.

*UCP Device 360 View | Events*

The **Events** tab displays system and device events for the selected UCP appliance.

The **Events** table lists the following details:

- Timestamp
- Severity
- Component
- Description

**Note**
You can use the **Search** field to filter the table view.

*UCP Device 360 View | Alerts*

**Alerts** provides the following information about the selected UCP appliance:

- An interactive graph shows the number of alerts raised on the current device, for the specified time frame. By default, the data capture time frame is 24 hours.
  - To customize the graph, select any **Filter by** option from the list (Critical Alerts, Warning Alerts, and Information Alerts).
  - To narrow the time frame, select the **Date & Time Range**, select a **Start Date** and **End Date**, select a **Start Time** and **End Time**, and then select **Done**. Select **Reset to Default** to reset back to the default time frame.
- The **Alerts by Severity** widget displays the total number of **Alerts Raised** for the specified time range, with the colored bands of the arch and color-matched beads below it representing refinements on the basis of **Severity**, as follows:
  - Critical
  - Warning
  - Information

  By default, the data capture time frame is 24 hours.
- A table lists the following alert details during the specified time range:
  - Alert Name
  - Summary
  - Severity
  - Application
  - Location
  - Status
  - Category
  - Source
  - Timestamp

  To view alert details, select an **Alert Name**. The **Alert Details** pane displays the following information:
  - Severity
  - Description
  - Detected
  - Source:
    - Name
    - Type
  - Details:
    - Model
    - MAC Address
    - Application
    - Serial Number
    - Admin State
    - IP Address
    - Location

**Note**
Select **Acknowledge** to mark the alert as reviewed. Acknowledging an alert does not resolve the issue, but it signals that the alert has been reviewed. This helps reduce duplicate investigations and allows teams to track which alerts are actively being addressed or have already been acknowledged.

- Select to export filtered alerts.
- You can use the **Search** field to filter the table view.

## Discovered Device 360 View

The **Discovered** Device 360 view provides a streamlined interface for reviewing device details for devices managed through ExtremeCloud Site Engine.

Select a **Device** name from the table to view the following information for the device:

- Connection Status
- From the **Actions** menu you can perform actions for the selected device. For more information, see Device 360 Actions Menu on page 235.

**Note**
Not all actions are available for all devices.

- Installation Media Gallery: Select to upload an image (.png or .jpg less than 500KB) or video (.mp4 or .mov less than 5MB) file.
- Device Details:
  - System Name
  - IP Address
  - Model
  - Sys Up Time
  - OS Version
  - Location
  - System MAC
  - Serial Number
  - Last Backup: Displays the result of the most recent configuration backup attempt for the third-party device.
    - **Success**: The latest configuration backup completed successfully.
    - **Failure**: The latest configuration backup operation failed. Inspect the managing appliance logs in **Task Center** for failure details.
    - **Not Performed**: No configuration backup has been executed for this device.
  - Backup Schedule: Displays the active configuration backup schedule assigned to the device:
    - **Daily**: Backs up device configuration once per day.
    - **Weekly**: Backs up device configuration once per week.
    - **Monthly**: Backs up device configuration once per month.
    - **None**: Scheduled configuration backups are disabled.

- Backup History: Select **Backup History** to open **Task Center** > **Backup and Restore**. This view lists all historical backup records, timestamps, file sizes, and status details for the selected device. For more information, see Task Center on page 571.
- Managed By: Select to view the details of the Third-Party Management Engine associated with the selected device.

- Overview on page 233
- Devices on page 234 (Third-Party Management Engine only)

To refine the device list:

- Select and drag the left or right border of the column header to adjust the column width.
- Select and drag the column headers to change the order of the columns.

**Note**
Once columns are reordered, the layout is saved and persistent until it is manually changed.

- Select a column header to sort column data in ascending or descending order.
- Select **Columns** to add, remove, and reorder the columns.
- To refine the list, select **Filter**. The filter sidebar lets you customize what information is displayed in the device list. Available filters vary depending on the window you are in. To see all available options, in the filter area, select a section heading to see more or less items. To clear all active filters, select **Clear all filters** above the **Filters** panel.

*Overview*

**Overview** displays the following information about the selected device:

- The **Device Health** widgets display the following information:
  - CPU Usage
  - Memory Usage
  - Temperature

  By default, the data capture time frame is 24 hours.
- The Port Configuration diagram is an interactive visual representation of the device's physical port layout showing link state and port orientation. Select individual ports or enable **Select All Ports**.
- The diagram shows how the device connects to the internet and to ExtremeCloud IQ (New).
- Status (Third-Party Management Engine only): Displays the Third-Party Management Engine discovery status, including whether discovery is in progress or complete, and the completion date.

**Note**
Changes to the discovery status are not reflected in real time. Refresh the browser window to display the updated status.

- From the interactive timeline graph (Third-Party Management Engine managed devices only):
  - View and filter:
    - CPU Stats

    - Memory Stats
  - To narrow the time frame, select the **Date & Time Range**, select a **Start Date** and **End Date**, select a **Start Time** and **End Time**, and then select **Done**.

    **Note**
    The selected time period applies to the widgets as well as the diagram.

  - Select any point along the timeline in the graphic to display details only for that precise time. To customize the time period for graphs, drag inside the timeline. The chart lines are interactive—hover over a line to see more data.
  - To reset back to the default time frame, select **Reset to Default**.

*Devices*

**Devices** provides a consolidated view of all devices associated with the selected ExtremeCloud Site Engine. and displays the following information for each associated device:

- Status
- State
- Location
- Hostname
- Model
- MAC
- Firmware
- Subscription
- Serial Number
- MGT IP Address

*Port Stats*

**Port Stats** includes an interactive Port Configuration diagram alongside the **Ports Description** table detailing operational states for all physical interfaces.

**Table 88: Ports Description Definitions**

| Column | Description |
|---|---|
| Port Number | Displays the physical port designation or identifier on the device. |
| LLDP Neighbor | Displays the system name of the connected LLDP neighbor device, with a hyperlink to view neighbor details if available. |
| Operational Status | Indicates whether the port link state is currently `Up` or `Down`. |
| Transmission Mode | Displays the duplex transmission mode configured on the port (for example, Full Duplex or Half Duplex). |
| Link Speed | Displays the negotiated operational speed of the port interface (for example, 100 Mbps, 1 Gbps, or 10 Gbps). |

## Device 360 Actions Menu

In **Network Devices** > **Device Status**, select a device name from the **Device** column to display a list of available actions within the Device 360 view.

From the **Actions** menu, you can perform the following tasks on a selected device:

- Common actions
- UCP only
- Tunnel Concentrator only

*Common Actions*

- **Assign Country Code**: Select a country code for a managed device from the drop-down list. The country code defines the device radio channels and power limitations for the country in which the device operates. For devices used in the United States, the region code is reset to **FCC** and the country code is preset to **United States**. Select **Save** to reboot the selected devices.
- **Assign to Cloud Config Group**: Add the selected devices to an existing **Cloud Config Group** (CCG). In the **Assign to a Cloud Config Group** panel, select a CCG to assign to the selected devices, and then select **Assign**. To create a new CCG, see Add a Cloud Config Group on page 439.
- **Assign Location**: Assign a location to the selected device. Select a location, and then select **Submit**.
- **Assign Network Policy**: Assign an existing network policy to the device.

  **Note**
  This action replaces existing associated policies with the newly selected policy.

- **Change Device Mode**: Change the device mode from AP device to Router.

  **Note**
  - To configure an AP device as a router, the associated network policy must have both wireless and routing activated.
  - The following features are not supported: SDWAN, URL filtering, USB modem, private client group, and client mode.
  - The device must complete a full configuration update for the mode change to take effect.

- **Change Management Status**: Indicates the management status of the selected devices. Select **Manage** or **Unmanage**.

  **Note**
  The **Change Management Status** menu option is now available for Site Engine and devices managed by Site Engine. If Site Engine status is **Unmanaged**, the status for both Site Engine and devices managed by Site Engine is **Unmanaged**.

- **Change OS to Fabric Engine / Change OS to Switch Engine**: Change the operating system of the selected devices to Fabric Engine or Switch Engine.

  **Important**
  Changing the OS reboots the device and permanently erases the existing configuration. The new OS reverts to factory default settings.

- **Change OS to WiNG**: Change the operating system of the selected devices to WiNG.

  **Important**
  Changing the OS reboots the device and permanently erases the existing configuration. The new OS reverts to factory default settings.

  **Note**
  This action is not available for AP5022, AP5022FX, or AP5022S6D devices when managed as cloud devices.

- **Clear Audit Mismatch**: Occasionally, there can be a mismatch between the configuration database and the device-level configuration database. If this occurs, perform this action.
- **Configure Fabric**: Configure the minimum required Global SPBM and Auto Sense settings to enable SPBM to operate on a wired device.

  **Note**
  This feature is available only if the device is in an ExtremeCloud IQ (New)-compatible building or outdoor site.

- **Configure Device**: Perform device-level configuration tasks and update devices. Settings made at this level apply only to the individual device and overrides the template settings configured for the network policy. For wired devices, see Configure Wired Devices. For wireless devices, see Configure Wireless Devices.
- **Diagnostics**: Select a diagnostic method to run CLI commands on the device for basic network connectivity checks, status monitoring, and function diagnostics. For a full list of CLI commands, see Diagnostics CLI Commands on page 142.

  **Note**
  Each time you run a CLI command, the diagnostic results are added to the log. To resize the log window, select and drag any corner of the window to view more of the results on the screen. Select **Export Results** to download all diagnostic results as a .txt file.

- **Locate Device**: Locate the physical location of the selected device. Set an **LED Timeout**, and then select **Submit**.

  **Note**
  To stop the blinking lights used for locating the device, select **Return to Standard LED operations**, and then select **Submit**.

- **Manage/Unmanage**: Select **Manage** or **Unmanage** to indicate the management status of the selected device.

  **Note**
  The **Change Management Status** menu option is now available for Site Engine and devices managed by Site Engine. If Site Engine status is **Unmanaged**, the status for both Site Engine and devices managed by Site Engine is **Unmanaged**.

- **Packet Capture**: Captures wireless and wired traffic for advanced troubleshooting. For more information, see Packet Capture on page 155.
- **RADIUS Test**: Send a RADIUS request from the device to an authentication or accounting server. For more information, see Perform a RADIUS Test on page 140.
- **Reboot Device**: Restart the selected device. Select **Yes** to confirm.
- **Reset to Default/Reset Factory Setting**: Reset the device to factory defaults. Select **Yes** to confirm.

  **Important**
  This operation removes existing settings from the selected device and returns it to factory settings. It then reconnects to the cloud as a new device.

- **Revert Device to Template Defaults**: Returns the device settings to the network policy template. This removes any device-level configuration settings.
- **Retrieve Debug Data**: Collect diagnostic information for the selected devices from the network to help with troubleshooting and support. Use this data to analyze issues, identify root causes, and improve system performance. Select a **Debug Data Type**, and then select **Retrieve Data**. Once the process is complete, select **Download** to save a .tar.gz file containing the collected debug files.
- **Show GRE Tunnel**: Display the current GRE tunnel status and configuration details.

  **Note**
  This action is supported only on Tunnel Concentrator.

- **Show Log**: Display the current system log for the Tunnel Concentrator.

  **Note**
  This action is supported only on Tunnel Concentrator.

- **SSH Access**: Select an available runtime to temporarily access your network remotely to troubleshoot the selected device. Select **Start** to begin an SSH session.

  **Note**
  SSH must be enabled to run an SSH session on the selected device. For more information, see Configure SSH on page 202.

- **Thread Commissioner** (AP5010/AP5020 only): Enter a runtime to temporarily access your network remotely, and then select **Start**. The Thread Commissioner securely screens

endpoint devices attempting to join the Thread network. To define the behavior of the Thread Commissioner, see Configure the Thread Commissioner on page 414.

**Note**
If another AP is already running as the Commissioner on this Thread network, a warning message displays prompting the user to stop the current Commissioner or wait for it to automatically shutdown. If Thread is not enabled on the AP, or if configuration changes have not been deployed, the operation fails and a related error message displays.

- **Update Devices**: Update network policy and configuration for the device. Select any of the following options, and then select **Update**:
  - Reboot & revert Extreme Networks switch configuration if IQ Agent is unresponsive after configuration update.
  - Perform delta configuration update and resolve local device configuration which is out of sync.
  - Save as default.
- **Upgrade Firmware**: Upgrade device firmware. Select a **Firmware Version**, and then select **Upgrade Firmware**.
- **VLAN Probe**: Locates available VLANs for the selected device. When the VLAN probe completes, a table displays the client name, MAC address, available VLANs, unavailable VLANs, and their status.

*UCP only*

- **Application** > **Add**: Add an application to a UCP. The application is downloaded from the Extreme Application File Server (AFS), installed on the UCP, and deployed automatically. The process is monitored in three stages: Downloading, Installing, and Deploying. For more information, see Add an Application to UCP on page 239.

**Note**
The **Application** > **Add** action is only available for UCP with no currently installed applications. If the action does not appear, the selected device has at least one application installed.

- **Open Appliance UI**: Opens the local web-based management interface of the application installed on a UCP node. The interface opens in a separate browser tab and is accessed through the UCP connection.

**Note**
This action is available only when the target UCP has a supported application and the application can be reached through the appliance connection. If the application is stopped, unavailable, or the UCP cannot be reached, the action might be unavailable or the application UI might not open.

- **Open Console**: Open a virtual remote console for a UCP. For more information, see Open the UCP Console on page 241.

- **Start/Stop**: Starts and stops an application on UCP. Starting and stopping an application does not remove it from the UCP. For more information, see Start or Stop a UCP Application on page 240.
- **Uninstall**: Remove an installed application from UCP. For more information, see Uninstall an Application from UCP on page 240.

*Tunnel Concentrator only*

- **Ping**: Sends a ping request from ExtremeCloud IQ (New) to verify network connectivity.
- **Show Tunnel Clients**: Display a list of clients currently connected through this Tunnel Concentrator.

*Add an Application to UCP*

Before you begin:

- UCP must be running firmware version 5.14.01 or later.
- UCP must have no application currently installed. If an application is installed, uninstall it before proceeding.

Use this task to add an application to UCP. The application is downloaded from the Extreme Application File Server (AFS), installed on the UCP, and deployed automatically. The process is monitored in three stages: Downloading, Installing, and Deploying.

1. Go to **Monitor** > **Network Devices** > **Device Status** > **Appliances** and select a UCP from the table.

   The UCP Device 360 view opens.
2. From the **Actions** menu, select **Application** > **Add**.

   **Note**
   The **Application** > **Add** action is only available for UCP with no currently installed application. If the action does not appear, the selected device already has an application installed.

   The **Add Application** dialog opens, displaying a list of applications supported by the selected UCP model.
3. From the application list, select the application you want to install.

   The list is populated dynamically from the UCP and shows only applications supported for the specific UCP model. If no applications appear, verify that the UCP firmware version meets the minimum requirement.
4. Select **Confirm** to begin the installation.

   The installation begins and the progress is displayed in the **Installed Applications** table:

   - `Downloading`: The application image is being downloaded to the UCP from AFS.
   - `Installing`: The application image is being installed on the device.
   - `Deploying`: The application is being deployed.

   After deployment completes, the application status changes to `Running` and the install image is automatically removed from the device.

The application is installed and running on the UCP. The **Applications** column in the **Network Devices** > **Appliances** table and the **Installed Applications** section in Device 360 are automatically updated to show the installed application and its status.

This action is recorded in the audit log. To review the action, go to **Administration and Settings** > **Logs** > **Audit Logs**.

*Uninstall an Application from UCP*

An application must be installed on UCP (in Running or Stopped state).

Use this task to remove an installed application from UCP. After the application is uninstalled, UCP returns to a clean state and you can install a different application using Add Application.

1. Go to **Monitor** > **Network Devices** > **Device Status** > **Appliances** and select a UCP from the table.

   The UCP Device 360 view opens.
2. In the **Installed Applications** table, from the 3-dot (⋮) menu for the application you want to remove, select **Uninstall**.

   The **Uninstall** option is available in both application states: running or stopped.

   A confirmation dialog opens.
3. Review the application and instance details, and then select **Confirm**.

   **Note**
   If the device has multiple instances of the same application installed, the dialog lists all instances. Select one ore more instances to remove before confirming.

   The uninstall process begins. The application status transitions to `Uninstalling` while the operation is in progress.

The application is removed from the UCP device. The device returns to a clean state with no installed applications. The **Installed Applications** section displays the message `No installed applications found`, and the **Application** > **Add** action becomes available. For more information, see Add an Application to UCP on page 239.

*Start or Stop a UCP Application*

An application must be installed on the UCP.

Use this task to start a stopped application or to stop a running application on UCP. Starting and stopping an application does not remove it from UCP; use Uninstall to permanently remove an application.

1. Go to **Monitor** > **Network Devices** > **Device Status** > **Appliances** and select a UCP from the table.

   The UCP Device 360 view opens.
2. In the **Installed Applications** table, select the 3-dot (⋮) menu for the application, and then select one of the following actions:
   - **Start**: Launches the application. Available only when the application status is `Stopped`.
   - **Stop**: Stops the application. Available only when the application status is `Running`.

The application status updates in real time:

- **Start**: Status transitions from `Stopped` → `Starting` → `Running`. The Actions menu updates to show **Stop**, **Open Console**, and **Uninstall**.
- **Stop**: Status transitions from `Running` → `Stopping` → `Stopped`. The Actions menu updates to show **Start** and **Uninstall**.

*Open the UCP Console*

An application must be installed on UCP and must be in `Running` state.

Use this task to open a virtual remote console for UCP. The console session opens in a dedicated interactive pane, providing CLI access to UCP. Communications tunnel through Inlets over the existing management connection.

1. Go to **Monitor** > **Network Devices** > **Device Status** > **Appliances** and select a UCP from the table.

   The UCP Device 360 view opens.

2. In the **Installed Applications** table, select the 3-dot (⋮) menu for a Running application, and then select **Open Console**.

   An interactive console pane opens for the selected UCP. You can type CLI commands directly in the console window. To close the console, select **Close** in the console pane header, or navigate away from the Device 360 view.

*Upgrade Firmware*

Use this task to manually upgrade firmware for a selected device.

1. Go to **Network Devices** > **Device Status**, and then select a device name from the **Device** column.
2. From the **Actions** menu, select **Upgrade firmware**.
3. Select a **Firmware Version**.
4. Select a **Firmware Upgrade Schedule**:
   - To update immediately, select **Upgrade Now**, and then select **Upgrade Firmware**.
   - To update at a later time, select **Upgrade Later**, select a **Date & Time** , and then select **Schedule Firmware Update**.

   **Note**
   Firmware upgrades can be scheduled up to 30 days in advance.

5. Select ⋮ to view **Firmware Upgrade History**. Firmware upgrade activity is stored for a maximum of 30 days.

   **Note**
   To reschedule a scheduled firmware upgrade:
   - Select a scheduled upgrade, and then select **Reschedule Upgrade**.
   - Select a new **Date & Time**, and then select **Reschedule**.

# Monitoring | Clients

Monitor Clients on page 242
Monitor Users on page 257
Monitor Applications on page 259

The **Clients** page provides a list of wired and wireless clients, users, and applications.

## Monitor Clients

The **Clients & Users** tab provides list of wired, wireless, and discovered devices. You can filter the client list for the selected site.

For more information on performing actions on the clients from the 3-dot menu, see Client Three-dot Menu on page 247.

For device details, select the client within the table column. See Client 360 View on page 248.

From the **Wired** tab, enable **Show Summary** to display the following widgets:

- IP Connectivity Issues
- Port Congestion
- Traffic Anomalies
- Port Errors

**Note**
Widgets provide interactive functionality. Selecting a widget may either filter the device table or open the widget for modification, depending on the widget type.

The Wired table displays the following information:

- Connection Status
- Client
- Location
- IPv4
- Port Number/Switch Name
- VLAN
- Operating System
- MAC
- Username
- Instant Port Profile
- Total Congestion
- Total Unicast
- Total Multicast
- Total Broadcast
- Total Port Errors
- IPv6

From the **Wireless** tab, enable **Show Summary** to display the following widgets:

- Connectivity Issues
  - Association Failures
  - Authentication Failures
  - Network Issues
- Roaming Issues
- Frequency Distribution - Select Frequency Distribution to filter table data.
- ICA Clients- Select **More Details** to access the XVS inspector panel, see Table 93 on page 245.

To enable Real-time Troubleshooting, see Enable Real-Time Troubleshooting on page 257.

The Wireless table displays the following information:

- Connection Status
- Client
- Location
- SNR
- RSSI
- Frequency
- Airtime %
- Association Issues
- Authentication Issues
- IP Address Issues
- Network Issues
- Roaming Issues
- IPv4
- Connected To
- SSID
- VLAN
- Last Session Start Time
- Operating System
- MAC
- User Name
- Authentication
- Encryption
- User Profile
- Alias
- Category Assignment
- IPv6
- Client Retries
  - Tx Retries
  - Rx Retries
- Wireless Client Type
  - Wi-Fi
  - Thread
  - BLE
  - ZigBee
  - Wi-Fi - MLO

## Wireless Inspector Panel Settings

**Table 89: Association Issues Panel Settings**

| Field | Actions |
|---|---|
| Search | To search a specific associated issue, enter the AP name, reason code, or description in the **Search** field. |
| Issue Details | View the following details:<br>• Date & Time<br>• Association Duration<br>• Reason code & Description<br>• AP Name |

**Table 90: Authentication Issues Panel Settings**

| Field | Actions |
|---|---|
| Search | To search a specific authentication issue, enter the AP name, reason code, or description in the **Search** field. |
| Issue Details | View the following details:<br>• Date & Time<br>• Association Duration<br>• Reason code & Description<br>• AP Name |

**Table 91: IP Address Issues Panel Settings**

| Field | Actions |
|---|---|
| Search | To search a specific IP address issue, enter the AP name, or description in the **Search** field. |
| Issue Details | View the following details:<br>• Date & Time<br>• Issue Type<br>• AP Name |

**Table 92: Roaming Issues Settings**

| Field | Actions |
|---|---|
| Search | To search a specific roaming issue, enter the AP name, issue type, or description in the **Search** field. |
| Issue Details | View the following details:<br>• Date & Time<br>• Issue Type<br>• Roaming Time<br>• AP Name |

**Table 93: XVS Clients Settings**

| Field | Actions |
|---|---|
| Search | To search a specific roaming issue, enter the AP name, issue type, or description in the **Search** field. |
| Make and Model | Select the Make and Model of a client to open the inspector panel for that specific client.<br>The following actions are available from the 3-dot menu on the **Clients** panel, see Run Web Response Analysis on page 256 and Delete Clients from Inspector Panel on page 256. |
| Connection Details | View how many clients are connected and how many are disconnected. |

The **Discovered** table displays the following information:

- Status*
- Client
- Location
- IPv4
- Port Number/Switch Name
- VLAN
- Operating System
- MAC
- User Name
- IPv6

* This column can be filtered by **Connected** and **Disconnected** clients.

To refine the client list:

- Select and drag the left or right border of the column header to adjust the column width.
- Select **Columns** to add, remove, and reorder the columns.
- Select and drag the column headers to change the order of the columns.

  **Note**
  Once columns are reordered, the layout is saved and persistent until it is manually changed.

- Select a column header or the associated 3-dot menu to sort column data in ascending or descending order.
- Select the column header 3-dot menu to do the following:
  - Sort the columns in Ascending or Descending order.
  - Pin a column to the left or the right to move it out of the way. You can subsequently unpin the column to display it in it's original location.
  - Autosize the select column or all columns.
  - Choose the columns to display.
  - Reset the columns.

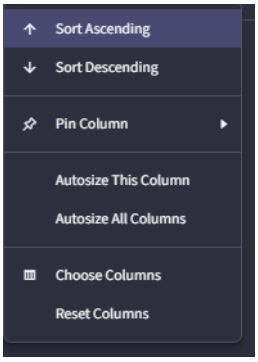



**Figure 5: Column Header Menu**

- To refine the list, select **Filter** in the column header or the filter sidebar. The filter sidebar lets you customize what information is displayed in the device list. Available filters vary depending on the window you are in. To see all available options, in the filter area, select a section heading to see more or less items. To clear all active filters, select **Clear all filters** above the **Filters** panel.

## Client Three-dot Menu

From the three-dot menu on the **Client** tab, you can complete the following actions:

- Wireless:
  - Change Client Alias on page 247
  - Disconnect Client on page 252 or Clients (Bulk)
  - Manage Real Time Statistics on page 247
  - GDPR Export or Delete
- Wired:
  - Show Endpoint to Endpoint
  - Port Bounce
  - Cable Test

*Change Client Alias*

Use this task to change a client alias.

1. Go to **Monitoring** > **Clients**.
2. Select one or several clients and select the three dot menu and select **Change Client Alias** .
3. Add a new client alias in the field and select **Save**.
4. For bulk client alias changes, add a new client alias and select **Yes**.

*Manage Real Time Statistics*

Use this task to manage Real Time Statistics for wireless clients.

1. Go to **Monitoring** > **Clients**.
2. Select one or several clients and select the three dot menu and select **Real Time Statistics** and configure the settings in Table 94.

**Table 94: Real Time Statistics Configuration Settings**

| Field | Descriptions |
|---|---|
| Client | Select a client. |
| Select **Start** or **Stop**. | |
| Select an AP from the drop-down list. | |
| Packet Stream | Select one of the three options:<br>• All<br>• Data Frames<br>• Management Frames |

3. Select **Close**.

*Delete and Export Client Data (GDPR)*

The General Data Protection Regulation (GDPR) Delete action permanently deletes all personal data for the selected client across all Extreme Platform ONE Networking data sources, including Extreme Platform ONE Security, SD-WAN, AI, and network data. You can select GDPR

Export first to download the client's data as a CSV file before deletion begins. If the export fails, deletion does not proceed.

All GDPR Delete and GDPR Export actions are recorded in the GDPR Logs, see Administration & Settings | Logs on page 725.

1. Go to **Monitoring** > **Clients**.

**GDPR Export**

2. Select one or more clients, select the three-dot menu, and select **GDPR Export**.

   When the export completes, the client data CSV file is available to download from the **GDPR Logs** page, see Administration & Settings | Logs on page 725.

**GDPR Delete**

3. Select one or more clients, select the three-dot menu, and select **GDPR Delete** .

   **Important**
   Deletion is permanent and cannot be undone. All client data is removed from Extreme Platform ONE Networking, including Extreme Platform ONE Security, SD-WAN, AI, and network data sources.

4. In the confirmation dialog, select **Delete**.

   A toast notification confirms if the deletion was successful.

## Client 360 View

The Client 360 view provides a comprehensive overview of the selected client specifications and current status. Go to **Monitoring** > **Clients** and then select a Client name from the table. The Client Details window displays detailed information for the Wired, Wireless, or Discovered Client.

Within Client 360, the following tabs and options are available:

- Location on page 248
- Overview on page 249
- Client Trail on page 250
- Troubleshooting Connectivity on page 251
- Real-Time Troubleshooting on page 251

Select **Actions** to perform specific tasks on the selected client. For more information, see Client 360 Actions Menu on page 252.

*Location*

The Location tab displays the topology information in a mini map that displays the physical location of connected clients on a floor plan. This feature enhances troubleshooting capabilities by providing visual context for client connectivity and roaming behavior.

To use the location functionality, ensure the following requirements are met:

- Presence Analytics is enabled on the network policy. See Configure Presence Analytics on page 445.
- Floor plans are uploaded for locations where clients are connected. See Upload a Floor Plan on page 273.
- Access points have known locations on the floor plan.

The map displays the current client location. Use Zoom to change the view, click and drag to pan the map, and select the center icon to reset the map.

*Overview*

Within the **Client Details** section you can view the following information pertaining to the selected client:

- Hostname
- Username
- OS Type
- IP Address
  - IPv4 Address
  - IPv6 Address
- MAC
- Location
- Connected to Switch (Link to the physical access view.)
- Connected to Port
- VLAN & IP
- ISID
- Fabric Attach Client Type
- Instant Port Device Type
- LLDP Information
  - System Capability
  - System Description
- DHCP Snooping
  - DHCP Lease Time
  - Server Port Number
- Encryption
- Authentication method
- User Profile
- Client Auth Information
- Policy Assigned
- Username Identity
- Type
- NAC Details
- NAC Profile

Select from the graph options:

- RSSI
- RSSI from Network
- SNR
- Noise Floor
- Roaming

View the following widgets:

- Roaming Report
- Voice Calls - Select the segment for more details.
- Voice Performance
- Least Speed Test Results - Server, Distance, Latency, Average Jitter, Download Speed, Upload Speed

View the following graphs:

- Status and Events - Online, Offline, Voice, Web Response
- Battery Level
- Device Unlocks
- Download and Upload

*Client Trail*

The **Client Trail** tab on the **Wireless Clients** page provides a view of the following:

- Roaming Trail - Displays how many roams completed and how many roams failed.
  - Timestamp
  - From
  - To
  - Roam Duration
  - Status
- Connectivity Experience
  - Timestamp
  - AP Name
  - SSID
  - Association
  - Authentication
  - DHCP
  - DNS
  - Default Gateway ARP

The **Connectivity Experience** view displays SSID information for each connection event, enabling users to track which SSID the client was connected to at each point in time.

**Note**
The **Roaming Trail** displays **Roams Completed** and **Roams with Issues** counters. Only transitions exceeding 3000 ms are counted as roaming issues, consistent with the Dashboard health widget. Disconnected events are listed separately and are not counted as roaming issues.

The **Client Trail** tab on the **Wired Clients** page provides an view of the following:

- Timestamp From
- Timestamp To
- Duration
- Device Name
- Port
- Speed
- Duplex

*Troubleshooting Connectivity*

The **Troubleshooting** tab on the **Clients** page provides an view of the **Troubleshooting Sessions**. The table displays the Timestamp, Description, Initiated by, and Status.

The **Client Issues** table provides the following:

- Status - To troubleshoot your status immediately select the linked status and see Troubleshoot Now on page 255.
- Issue Type
- Summary
- User Profile
- Location
- Detected On

*Real-Time Troubleshooting*

To view real-time client and packet stream statistics, select one or more Access Points in the **Select AP** drop-down list, and select **Start**.

**Client Statistics** displays the following:

- RSS, SNR, Usage (per 5 sec)
- Tx and Rx
- Tx and Rx Retries

**Packet Stream** displays the following:

- Options All, Data Frames, Management Frames
- RSS, SNR, Usage (per 5 sec)
- Tx and Rx Retries
- Packet Stream - No., Time, Serial Number, Source, Destination, Protocol, Length

Select **Stop** to complete the process.

*Client 360 Actions Menu*

From the **Actions** menu on the **Client Overview** tab, you can complete the following actions:

- Wireless:
  - **VLAN Probe** - See VLAN Probe on page 143.
  - **Troubleshoot Connectivity** - See Troubleshoot Connectivity on page 252.
  - **Disconnect Client** - See Disconnect Client on page 252.
  - **Active Analysis** - See Run Active Analysis on page 253.
  - **Packet Capture** - Select a **Duration** from the drop-down list, select **Mgmt Frames Only** or **All Frames**, and select **Take Action.**
  - **Ping** - Add an IP/Hostname and select **Ping**.
  - **Run Speed Test** - Once complete and details of test are displayed, select **Run Again** or **Close**.
  - **GDPR Export** and **GDPR Delete** - See Delete and Export Client Data (GDPR).
- Wired:
  - **Show Endpoint to Endpoint** - See Show Endpoint to Endpoint on page 253.
  - **VLAN Probe** - See VLAN Probe on page 143.
  - **Port Bounce**
  - **Cable Test**

#### Troubleshoot Connectivity

Use this task to troubleshoot client connectivity.

1. Go to **Actions** > **Troubleshoot Connectivity** and configure the settings in Table 95.

**Table 95: Troubleshooting Settings**

| Field | Description |
|---|---|
| Selected Client | Shows selected client. |
| Description (Optional) | You can add a description. |
| Select APs from the list below | Search for a specific client or select a client from the list. |

2. Select **Start**.

#### Disconnect Client

Use this task to disconnect a client.

1. Go to **Actions** > **Disconnect Client**.
2. To temporarily disconnect the select client, select **Yes**.

#### Run Active Analysis

1. Go to **Actions** > **Active Analysis** and configure the settings for Table 96 or Table 97 on page 253.

**Table 96: Zebra WI Voice Analysis Configuration Settings**

| Field | Description |
|---|---|
| Start Date and Time | Select a start date and time from the drop-down list. |
| Duration | Select a duration from the drop-down list. |
| Never Ends | Enable the **Never Ends** toggle on for the analysis to repeat indefinitely or select en **End Date and Time** from the drop-down list. |
| Default Gateway | Enable the **Default Gateway** toggle on for the analysis to use the default gateway. |

**Table 97: Web Response Analysis Configuration Settings**

| Field | Description |
|---|---|
| Start Date and Time | Select a start date and time from the drop-down list. |
| Duration | Select a duration from the drop-down list. |
| Repeat | Select if you would like the analysis to run once or repeat. |
| Never Ends | Enable the **Never Ends** toggle on for the analysis to repeat indefinitely or select en **End Date and Time** from the drop-down list. |
| URL 1 | Enter a URL in the associated field. |

2. Select **Submit**.



**Note**
Web Response analysis can have a 1-2 minute delay. Retry if it does not start.

#### Show Endpoint to Endpoint

Use this task to show endpoint to endpoint.

1. Go to **Actions** > **Show endpoint to endpoint** and configure the settings.
2. Select the **Physical** or **Fabric** layer as required.
3. Right-click a device in the topology map and select **Show Endpoint-to-Endpoint Service/VLAN**.
4. Select the second device from the list of devices to view the endpoint-to-endpoint service mapping.

5. Select **Select End Point**.
   The lists of services available on the selected endpoints opens.

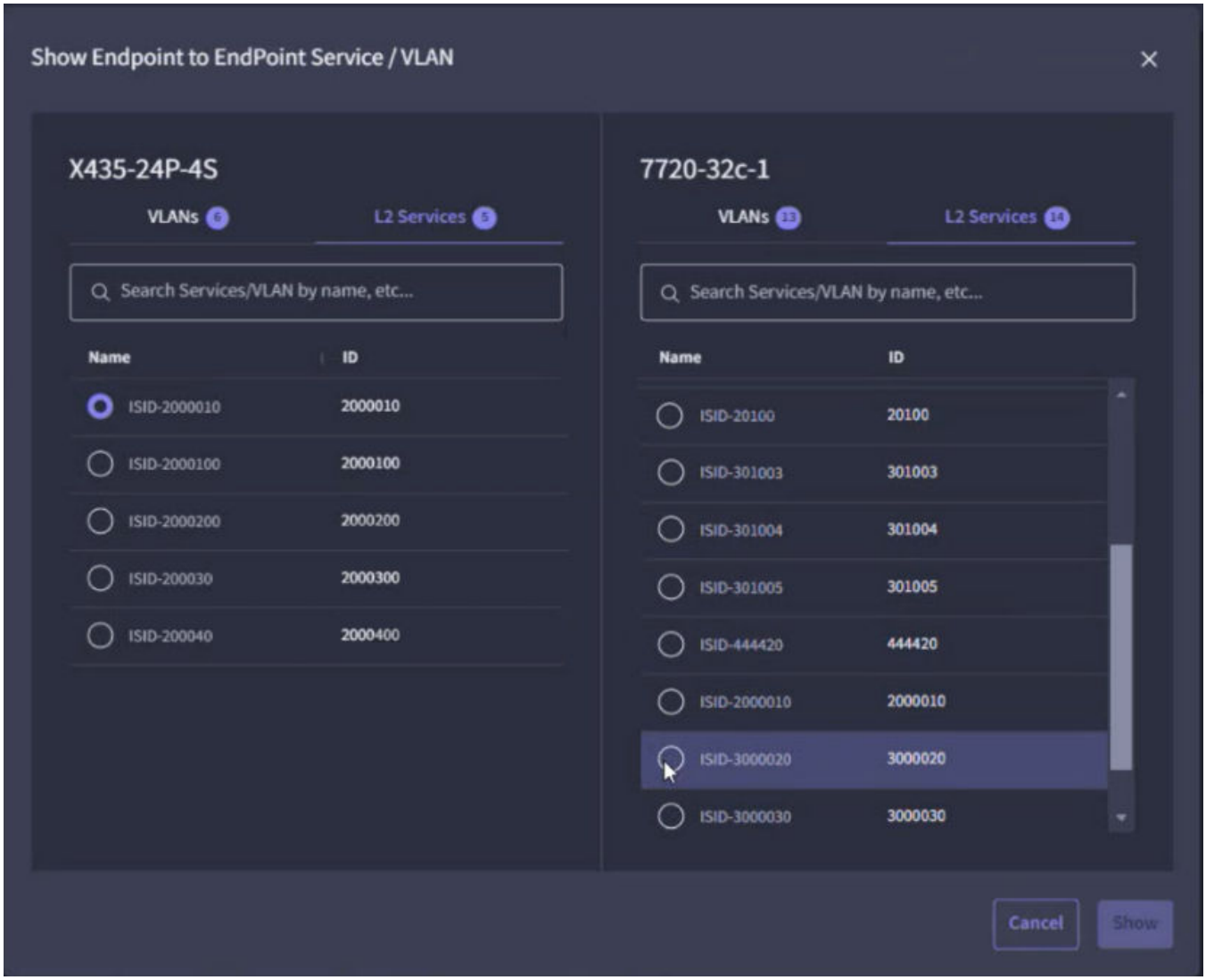



**Figure 6: Endpoint Services**

6. Select a service from each of the lists.

7. Select **Show**.

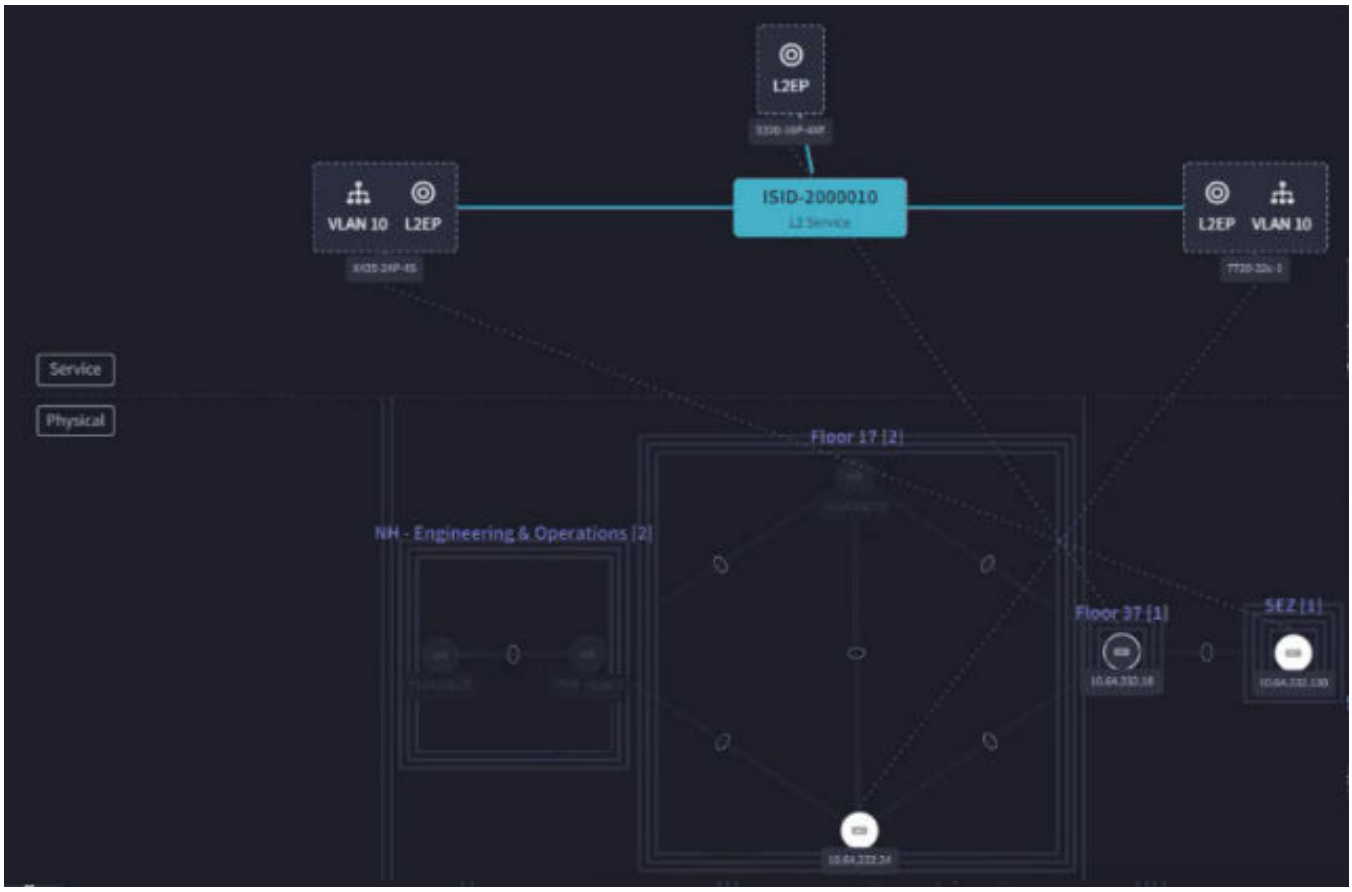



**Figure 7: Endpoint to Endpoint Configuration Path**

ExtremeCloud IQ (New) displays the Endpoint to Endpoint configuration path for the selected device.

8. Select the highlighted service on the topology map to view the endpoint-to-endpoint summary in the inspector panel.
9. In the inspector panel, select **Close ETE Service View** to exit the endpoint-to-endpoint service view.

*Troubleshoot Now*

Use this task to resolve or escalate status client issues.

1. Go to **Monitoring** > **Clients**, select the **Clients** tab and then **Wireless**.
2. Select an existing client and in the Client details page, select the **Troubleshooting** tab.
3. Select a status to display the following information:
   - Device Name
   - User Profile
   - Client MAC
   - Problem type
   - Description

- Location
- Case Number (Optional)
- Detected On
- Last successful connection
- Suggested Remedy

4. Select **Take Action**.
5. Select **Escalate** or **Resolve** from the **Select Action** drop-down list.
6. (Optional) Enter comments in to the **Comments (Optional)** field.
7. Enter an email address, select the associated check box, and select **Submit**.

*Run Web Response Analysis*

Use this task to run web response analysis.

1. Go to **Monitoring** > **Clients**, select the **Clients** tab and then **Wireless**.
2. In the **ICA Clients** widget, select **More Details**.
3. In the **XVS Clients** inspector panel, select one of the options within the **Make and Model** column.
4. In the resulting **Clients** inspector panel, select one or more clients and from the 3-dot menu, select **Run Web Response Analysis**.
5. Configure the settings in Table 98.

**Table 98: Web Response Analysis Configuration Settings**

| Field | Description |
|---|---|
| Start Date and Time | Select a start date and time from the drop-down list. |
| Duration | Select a duration from the drop-down list. |
| Repeat | Select if you would like the analysis to run once or repeat. |
| Never Ends | Enable the **Never Ends** toggle on for the analysis to repeat indefinitely or select en **End Date and Time** from the drop-down list. |
| URL 1 | Enter a URL in the associated field. |

6. Select **Submit**.

**Note**
Web Response analysis can have a 1-2 minute delay. Retry if it does not start.

*Delete Clients from Inspector Panel*

Use this task to run web response analysis.

1. Go to **Monitoring** > **Clients**, select the **Clients** tab and then **Wireless**.
2. In the **XVS Clients** widget, select **More Details**.
3. In the **XVS Clients** inspector panel, select one of the options within the **Make and Model** column.

4. In the resulting **Clients** inspector panel, select one or more clients and from the 3-dot menu, select **Delete Client (s)**.
5. To confirm, select **Delete**.

## Enable Real-Time Troubleshooting

Use is task to enable Real-time Troubleshooting.

1. Go to **Monitoring** > **Clients**.
2. Under **Wireless**, select **Real-Time Troubleshooting** and configure the settings in Table 99.

**Table 99: Real-Time Troubleshooting Configuration Settings**

| Field | Descriptions |
|---|---|
| Client | Select a client. |
| Select **Start** or **Stop**. | |
| Select an AP from the drop-down list. | |
| Packet Stream | Select one of the three options:<br>• All<br>• Data Frames<br>• Management Frames<br>The **Client Statistics** tab displays the following:<br>• RSS, SNR, Usage (per 5 sec)<br>• Tx and Rx<br>• Tx, Tx Retries, Rx, Rx Retries (per 5 sec)<br>The **Packet Stream** tab displays the following:<br>• Time<br>• Serial Number<br>• Source<br>• Destination<br>• Protocol |

3. Select **Close**.

# Monitor Users

The **Users** tab provides list of users. You can filter the user list for the selected site or a date and time range. To select date and time range, select the drop-down picker, select a **Start Time** and an **End Time** and select **Done**.

Enable **Show Summary** to display the following widgets:

- User Type
  - PPSK
  - Radius
  - Others
- Data Usage

- Connected Users

To refine the client list:

- Select and drag the left or right border of the column header to adjust the column width.
- Select and drag the column headers to change the order of the columns.



**Note**
Once columns are reordered, the layout is saved and persistent until it is manually changed.

- Select a column header to sort column data in ascending or descending order.
- Select **Columns** to add, remove, and reorder the columns.
- To refine the list, select **Filter**. The filter sidebar lets you customize what information is displayed in the device list. Available filters vary depending on the window you are in. To see all available options, in the filter area, select a section heading to see more or less items. To clear all active filters, select **Clear all filters** above the **Filters** panel.

The following actions are available from the user table:

- **Search –** Search for a user with the User Name, Email, or User Group.
- **Sort –** Sort users by User Name, Email, User Group, Client Devices, Data Usage, or Session Duration.
- **Download (Individual and bulk) –** Select and existing user or users and select the download icon to download the details for one or multiple users.
- **Access User Details Panel –** Select User Name or Email address to open the User Details Panel. For more information, see User Details Panel on page 259.

The Users table displays the following information:

- Status
- Location
- User Name
- Email Address
- User Group
- Clients
  - Wired
  - Wireless



**Note**
Select a specific client to navigate to the associated Client page.

- Data Usage (in GB)
- Source
- Session Duration
- Expires

## User Details Panel

The **User Details Panel** provides list of clients and applications. You can filter the list for the selected date and time range.

The following widgets are available:

- Top Clients
  - Status
  - SSID
  - User Profile
  - Access Point
- Top Applications
- Top Network Usage

The following actions are available from the user table:

- **Search -** Search for specific clients and applications.
- **Group -** Select the **Group by** drop-down list to group by **Clients** or **Applications**.
- **Applications by Client -** Select **Applications** to open the **Applications by Client** inspector panel to view the details, see Table 100 on page 259.

The Clients & Applications table displays the following information:

- Status
- Client
- Location
- Model
- OS
- Network Usage
  - Tx
  - Rx
- Applications

**Table 100: Applications by Client Panel Settings**

| Field | Actions |
|---|---|
| Application Details | View the following details:<br>• Name<br>• Network Usage |

# Monitor Applications

The Applications table displays the following information:

- Application
- Category

- Data Usage
  - Generated Traffic - The following filters can be applied to this column:
    - Bytes
    - KB
    - MB
    - GB
  - %Used
- #Clients
- #Users

To refine the client list:

- Select and drag the left or right border of the column header to adjust the column width.
- Select and drag the column headers to change the order of the columns.



**Note**
Once columns are reordered, the layout is saved and persistent until it is manually changed.

- Select a column header to sort column data in ascending or descending order.
- Select **Columns** to add, remove, and reorder the columns.
- To refine the list, select **Filter**. The filter sidebar lets you customize what information is displayed in the device list. Available filters vary depending on the window you are in. To see all available options, in the filter area, select a section heading to see more or less items. To clear all active filters, select **Clear all filters** above the **Filters** panel.

# Reports

Filters for On-Demand Analytics and Reports on page 261
On-Demand Analytics on page 261
Scheduled Reports on page 264

The **Reports** page provides details about your network that can indicate how well it is functioning. In the navigation pane, select **Reports** and then select one of the following options:

- **On-Demand Analytics**: Information that is generated on-the-fly using criteria selected on-demand and displayed in the **On-Demand Analytics** tab.
- **Scheduled Reports**: Information that is generated at predetermined times using predefined criteria. Reports are emailed as either PDFs, HTML, or a URL link.

## Filters for On-Demand Analytics and Reports

You can filter on-demand analytics and scheduled reports according to the following criteria:

- **Sites:** Select multiple sites that are defined on the system. The default selection is all sites. Search for sites in the **Search** field in the **Sites** drop-down list.
- **Date and Time Range:** Select an extended date and time range up to 90 days in the past.
- **Radio Bands:** Select multiple radio bands that are in use on the system (2.4GHz, 5GHz, and 6GHz). The default selection is all radio bands.
- **SSID:** Select multiple SSIDs that are defined on the system. The default selection is all SSIDs. You can search for SSIDs in the **Search** field in the **SSID** drop-down list.

## On-Demand Analytics

The **On-Demand Analytics** tab provides access to the following analytics:

- **Clients**
  - **Max Concurrent Clients Over Time**: Measures the peak number of devices connected at the same time, tracked across time intervals
  - **Client Quality Score Over Time**: Snapshot of overall client quality (poor: 0–49 | good: 50–79 | Excellent: 80–100)
  - **Wireless Clients By OS**: A breakdown of connected wireless client devices grouped by their operating system
  - **Unique Clients Over Time By SSID**: The number of distinct client devices connecting to each SSID during a selected time period, tracked over time

- **Client Sessions Over Time**: The number of connection sessions initiated by clients over a selected time period
- **Unique Clients By OS**: A breakdown of the unique operating systems detected
- **Unique Wi-Fi Clients Over Time**: Measures the number of distinct devices that connected to Wi-Fi over a period of time
- **Client Airtime Usage Over Time**: Measures how much wireless channel time clients are consuming on the network over a period of time

- **Application Usage**

  **Whole App Traffic Volume**: The amount of data consumed on the wireless network, broken down by application type

- **Device**

  **Devices By Clients Over Time**: The relationship between clients (users/devices connecting to Wi-Fi) and the devices those clients represent, tracked over time

Related Links

Generate On-Demand Analytics on page 262
Create a Report from On-Demand Analytics on page 263

## Generate On-Demand Analytics

Use this task to generate **On-Demand Analytics** for one or more analytics types.

1. Go to **Reports** > **On-Demand Analytics**.
2. Select one or more of the analytics.
3. Select **Generate Analytics**.
   **On-demand Analytics** generates a table or graph for each selected analytic.
4. Mouseover a line on a graph to see the value and timestamp for a particular point on the timeline.
5. Use the filter menus to further customize the report data.
   See Filters for On-Demand Analytics and Reports on page 261 for more information.
6. To update the graphs and tables in the display, select **Apply**.
7. To reset the filters, select **Clear**.
8. (Optional) To add or remove analytics select .
   - To add additional analytics select them from the list.
   - To search for analytics, enter search terms in the **Search** field and select "search".
   - To remove all additionally selected analytics select **Reset**.
   - To remove a previously selected analytic select the highlighted analytic.
   - To save and display your changes select **Save**.
   - To exit without saving your changes select **Cancel**.
9. To download the generated analytics as a report, select  and choose the file format (PDF or XLSX).

Related Links

Create a Report from On-Demand Analytics on page 263

## Create a Report from On-Demand Analytics

Use this task to create a report from generated on-demand analytics.

1. Select **Create Report** after generating on-demand analytics.
2. Configure the following settings.

**Table 101: On-Demand Analytics Report Settings**

| Field | Description |
|---|---|
| Name | Enter the name for the report. |
| (Optional) Description | Enter an optional description of the report. |
| Report Format | Select the format for the report. Valid options are:<br>• PDF<br>• SXLS<br><br>**Note:** You can select both PDF and SXLS. |
| Recurrence | Select the report frequency.<br>• **Monthly**: Select one or more days of the month to run the report. The default is on the first day of the month. You can select "Last Day of Month" to run the report on the last day of the month.<br>• **Weekly:** Select the one or more days of the week to run the report.<br>• **Daily:** Select one or more dayswhen the report will run.<br><br>(Optional) Select the time of day and the time zone to run the report. |
| (Optional) Add Recipient Email(s) | Add optional recipient email addresses.<br>Select  in the **Add Recipient** field and select recipients.<br>If the recipient email address is not found, add the email address. . Select the check box next to the added email address.<br><br>a. Select **Add New Recipient Email**.<br>b. Enter the email address.<br>c. Select **Save**.<br>d. Select the check box next to the added email address.<br><br>**Note:** Recipient email addresses are optional and can be added to the report at a later time. |

3. Select **Create Report Schedule** to create the report and add it to the list of scheduled reports. Select **Cancel** to exit without saving.

Related Links

Generate On-Demand Analytics on page 262
Add or Remove Email Report Recipients on page 268

# Scheduled Reports

The **Scheduled Reports** tab provides access to a pre-configured Network Summary report and custom reports that you can modify for your needs.

**Network Summary Report**

The Network Summary Report is available out-of-the-box and provides system health, usage and capacity information. The report is generated monthly on the first of each month and contains data from the previous month. It can be automatically emailed to a list of recipients after it has been generated. The report is disabled by default. PDF and SXLS files can be created with report information and can be downloaded. The PDF and SLXS files are stored for 12 months. After 12 months the files are deleted.

From the **Network Summary Report** tab you can:

- Search for Network Summary Reports and email report recipients by entering search terms in **Search**.
- Enable and disable the Network Summary Report by selecting **Enable/Disable**.
- Refresh reports by selecting .
- Add or remove email report recipients by selecting **Add/Remove Report Recipients**.

The table includes columns for:

- **Report Month:** The month of the reporting period.
- **Recipients:** The email addresses of the recipients who are sent the report.
- **Report PDF:** The downloadable PDF of the report.

**Custom Reports**

Custom reports are user created. Report frequency can be monthly, weekly, or daily. Custom reports can be automatically emailed to a list of recipients after they have been generated. PDF and SXLS files can be created with report information and can be downloaded. Daily reports are saved for 14 days, weekly reports are saved for four weeks, and monthly reports are saved for 13 months. The reports are disabled by default.

From the **Custom Reports** tab you can:

- Select either the monthly, weekly, or daily tab to view a list of custom reports of that frequency.
- Search for reports or report recipients by entering search terms in **Search**.
- Create reports by selecting **Create Report**.
- Refresh reports by selecting .
- Add or remove email report recipients by selecting **Add/Remove Report Recipients** after selecting a report from the list.
- Select **On/Off** to enable or disable individual reports.

The table includes columns for:

- **Recipients:** The email addresses of the recipients who are sent the report.
- **On-Off:** Select the box in this column to enable a report to automatically run.
- **Report Schedules:** The next time the report is scheduled to run.

To refine the report list:

- Select and drag the left or right border of the column header to adjust the column width.
- Select and drag the column headers to change the order of the columns.

**Note**
Once columns are reordered, the layout is saved and persistent until it is manually changed.

- Select a column header to sort column data in ascending or descending order.
- Select **Columns** to add, remove, and reorder the columns.
- To refine the list, select **Filter**. The filter sidebar lets you customize what information is displayed in the device list. Available filters vary depending on the window you are in. To see all available options, in the filter area, select a section heading to see more or less items. To clear all active filters, select **Clear all filters** above the **Filters** panel.

Related Links

Create Custom Reports on page 265
Add or Remove Email Report Recipients on page 268

## Create Custom Reports

Use this task to create custom reports.

1. Go to **Reports** > **Scheduled Reports** and select either the Monthly, Weekly, or Daily Custom Reports tab.
2. Select **Create Report**.
3. Configure the following settings.

**Table 102: Custom Report Settings**

| Field | Description |
|---|---|
| **Analytics & Filters** | |
| Type of Analytics | Select one or more of the analytics to be used in the report. |
| Filters | Select filters from the filter menus to further customize the report data.<br>See Filters for On-Demand Analytics and Reports on page 261 for more information. |
| **Report Details** | |
| Name | Enter the name for the report. |
| (Optional) Description | Enter an optional description of the report. |
| Report Format | Select the format for the report. Valid options are:<br>• PDF<br>• SXLS<br><br>**Note:** You can select both PDF and SXLS. |
| **Schedule & Recipients** | |

**Table 102: Custom Report Settings (continued)**

| Field | Description |
|---|---|
| Recurrence | Select the report frequency.<br>• **Monthly**: Select one or more days of the month to run the report. The default is on the first day of the month. You can select "Last Day of Month" to run the report on the last day of the month.<br>• **Weekly:** Select the one or more days of the week to run the report.<br>• **Daily:** Select one or more dayswhen the report will run.<br>(Optional) Select the time of day and the time zone to run the report. |
| (Optional) Add Recipient Email(s) | Add optional recipient email addresses.<br>Select in the **Add Recipient** field and select recipients.<br>If the recipient email address is not found, add the email address. . Select the check box next to the added email address.<br>a. Select **Add New Recipient Email**.<br>b. Enter the email address.<br>c. Select **Save**.<br>d. Select the check box next to the added email address.<br>**Note:** Recipient email addresses are optional and can be added to the report at a later time. |

4. Select **Create Report Schedule** to create the report and add it to the list of scheduled reports. Select **Cancel** to exit without saving.

Related Links

Add or Remove Email Report Recipients on page 268

## Edit Custom Reports

Use this task to edit custom reports.

**Note**
You cannot edit the pre-configured Network Summary Report.

1. Go to **Reports** > **Scheduled Reports** and select either the Monthly, Weekly, or Daily Custom Reports tab.
2. Select the report to edit, select the corresponding , and select **Edit**.

3. Configure the settings in Table 103:

**Table 103: Custom Report Settings**

| Field | Description |
|---|---|
| **Analytics & Filters** | |
| Type of Analytics | Select one or more of the analytics to be used in the report. |
| Filters | Select filters from the filter menus to further customize the report data.<br>See Filters for On-Demand Analytics and Reports on page 261 for more information. |
| **Report Details** | |
| Name | Enter the name for the report. |
| (Optional) Description | Enter an optional description of the report. |
| Report Format | Select the format for the report. Valid options are:<br>• PDF<br>• SXLS<br><br>**Note:** You can select both PDF and SXLS. |
| **Schedule & Recipients** | |
| Recurrence | Select the report frequency.<br>• **Monthly**: Select one or more days of the month to run the report. The default is on the first day of the month. You can select "Last Day of Month" to run the report on the last day of the month.<br>• **Weekly:** Select the one or more days of the week to run the report.<br>• **Daily:** Select one or more dayswhen the report will run.<br><br>(Optional) Select the time of day and the time zone to run the report. |
| (Optional) Add Recipient Email(s) | Add optional recipient email addresses.<br>Select  in the **Add Recipient** field and select recipients.<br>If the recipient email address is not found, add the email address. . Select the check box next to the added email address.<br><br>a. Select **Add New Recipient Email**.<br>b. Enter the email address.<br>c. Select **Save**.<br>d. Select the check box next to the added email address.<br><br>**Note:** Recipient email addresses are optional and can be added to the report at a later time. |

4. Select **Create Report Schedule** to create the report and add it to the list of scheduled reports. Select **Cancel** to exit without saving.

## Add or Remove Email Report Recipients

Use this task to add or remove email recipients from reports.

1. Go to **Reports** > **Scheduled Reports** and select a report.
2. Select **Add/Remove Report Recipients**.
3. Add or remove email recipients.
   - To add email report recipients, select  in **Add Recipient Email(s)** and select the check box next to the recipient email . You can select multiple emails.
   - To remove email report recipients, select  next to the recipient email. You can remove all email recipients.
4. Select **Done**.

## Delete Reports

Use this task to delete reports.

1. Go to **Reports** > **Scheduled Reports** and select a report.
2. Select the corresponding  button for the report and select **Delete**.
3. Select **Delete** and select **Delete** again to confirm the deletion of the Access Profile.

   Select **Cancel** to abandon the operation.

# Configuration | Sites

Sites on page 269

Use **Sites** to plan your network by adding locations. Place simulated devices to determine where you might need to add or redistribute devices for optimal wireless network performance.



**Note**
During the customer onboarding process, Extreme Cloud IQ (NEW) automatically creates the **Organization** automatically creates the for sites. The **Organization** name is the same as the **Company** name that you provided for your account.

## Sites

To configure and manage the network hierarchy for your organization, go to **Configuration** > **Sites**.



**Note**
ExtremeCloud IQ (New) automatically adds devices that are not mapped to a specific site or floor to the **Default Site**. You can assign locations to these devices or keep them in the **Default Site**.

The location indicates where the device is installed. Valid locations include a floor or outdoor site. When location is not provided for a device, ExtremeCloud IQ (New) automatically assigns it to the default site. The default site is predefined and auto-created per customer account.

ExtremeCloud IQ (New) supports the following location hierarchy:

**Site Group**

Site groups are optional folders into which you can organize sites. Two levels of site groups are permitted. Site group names must be unique within the organization.

**Site**

Sites are a mandatory component of the location hierarchy. A site is the parent container for buildings and can include multiple buildings.

Site names must be unique within the organization. A site cannot belong to more than one site group.

**Building**

Buildings are physical premises with addresses. A building is the parent container for floors and must be associated with a site.

Building names must be unique within the parent site.

**Floor**

Floors are physical subdivisions of buildings.

Floor names must be unique within the parent building.

You can use the **Search** field to find specific sites, buildings, or floors within the network hierarchy.

## Import a Site Tree

Use this task to import a site tree to your network plan.

**Note**
This feature is available only when the site tree is empty.

1. Navigate to **Configuration** > **Sites** > **More options (three-dot) menu** and select **Import Site Tree**.
2. Select **Browse Files** or drag and drop the the site tree file.

   The files must be in .xml format.
3. Select **Import**.

## Export a Site Tree

Use this task to export site information.

1. Navigate to **Configuration** > **Sites** > **More options (three-dot) menu** and select **Export Site Tree**.
2. Locate the site that you want to export.
3. Select **More options (three-dot) menu** > **Export Site Tree** and select **Export**.

The site plan is exported as an XML/TAR file.

## Add a Site

Use this task to add a new site to your network plan.

1. Go to **Configuration** > **Sites** and select **Add Site**.

   Alternatively, to add a site to an existing site group, select and choose **Add Site**.
2. Type a **Name** for the new site.
3. Select the **Country**.
4. To add the new site group to an existing group, select an existing parent site group from the **Association** list.

5. (Optional) Type a **Description**.

   Although optional, descriptions can be helpful when you are configuring or troubleshooting your network.
6. Specify the time zone for the site.

   You can scroll through the list, or use the **Search** feature to find it.
7. Type GPS coordinates or the address manually, or select the location on the map.

   Use the **Search** function for the map to zoom in to the general location. You can manually move the location marker to the exact location.
8. For an outdoor site, toggle **Outdoor Location?** to **Yes** and configure the following settings.

**Table 104: Outdoor Settings**

| Setting | Description |
|---|---|
| Environment | Select a specific environment to apply a static, well-defined propagation model. Auto Estimate is more adaptive but might be less predictable for planning purposes.<br>Select **Auto Estimate** to have ExtremeCloud IQ (New) infer the best-fit propagation environment dynamically. This is useful when the deployment environment is mixed or not clearly defined |
| AP Installation Height | Specify the AP installation height in feet or meters above the ground. |
| AFC Schedule Update | Schedule when ExtremeCloud IQ (New) automatically refreshes Automated Frequency Coordination (AFC) spectrum data for APs operating on the 6 GHz band. |
| Upload Floor Plan | A floor plan at the site level serves as the placement canvas for outdoor APs. See Upload a Floor Plan on page 273. |

9. Select **Save**.

## Add a Site group

Use this task to add a new site group folder to your network plan.

1. Go to **Configuration** > **Sites** and select **Add Site Group**.

   Alternatively, select ⋮ for the corresponding parent group, and then choose **Add Site Group**.
2. Type a **Name** for the new site group.
3. (Optional) Add the **Description** text.
4. To add the new site group to an existing group, select an existing parent site group from the **Association** list.
5. Select **Save**.

## Add a Building

Your network hierarchy must contain at least one site with the country code defined, before you can add buildings and floors.

Use this task to add a new building to your network plan, and to upload building perimeters and floor plan images. Visualize view stores the images in the image library for future use.

1. Go to **Configuration** > **Sites**, and select the corresponding ⋮ button for a site.
2. Select **Add Building**.
3. Type a **Name** for the building.
4. Type the building **Address**.

   Alternatively, to automatically populate the address, use Google Maps search. If you manually adjust the marker on the map, the address updates automatically.

   While sites do not require addresses, buildings must have addresses.
5. Select **Save**.

## Move a Building

Use this task to move a building from one site, to another indoor site.

1. Go to **Configuration** > **Sites**.
2. Locate and expand the site that includes the building that you want to move.
3. Locate the building and select ⋮ > **Move**.
4. In the dialog, from the **Associated With** menu, select the destination site.

   **Note**
   Moving a building to an outdoor site is not supported.
   Building names must be unique. If a building with the same name exists in the target site, ExtremeCloud IQ (New) prompts you to rename the building before the move.
5. Select **Move**.

## Add a Floor

Use this task to add a floor to a building.

1. Go to **Configuration** > **Sites**, and select the corresponding ⋮ button for a building.
2. Select **Add Floor**.
3. Type a **Name** for the floor.
4. From the **Environment** menu, choose the environment type that most closely matches your installation.
5. For **Floor Attenuation (in dB)** menu, type or use the arrows to select the noise level for the floor.
6. Specify the **AP Installation Height** (distance from the floor to the mounting point) of the APs on the floor.

   If the height varies from AP to AP, enter the average height. This setting has a minimal effect on location estimates except for sites such as warehouses where the height of ceilings or high crossbeams is substantial.

7. Specify the unit of measurement: feet or meters.

   **Note**
   The unit defined when the floor is created is retained with the floor plan, and it is used for all measurements for that floor.

8. To provide more information for AFC, turn on **Additional 6 GHz Settings** and do the following:
   a. For **AP Installation Height**, specify the **Accuracy Range % (+/-)**.
   b. Specify the **Height from Ground** (distance from the ground to the mounting point) of the APs on the floor.
   c. For **Height from Ground**, specify the **Accuracy Range % (+/-)**.
9. Select **Upload Floor Plan** and choose an image from the Library, or upload a new image.

   For more information, see Upload a Floor Plan on page 273.
10. Verify the name of the building in the **Association** list.
11. Select **Save**.

Related Links

Upload a Floor Plan on page 273

## Upload a Floor Plan

You can upload a floor plan to an existing floor or a new floor. You can also upload a floor plan to an outdoor site.

Use this task to upload a floor plan.

Extreme Platform ONE Networking supports the jpg and png image formats with an image resolution of 8K.

1. Go to **Configuration** > **Sites** and expand the **Site** and the **Building**, to which you want to add a floor plan.
2. For an existing floor, select .

   If you're adding a new floor, select **Upload Floor Plan**.
3. Choose **Upload New**.

   Alternatively, select **Choose from Library**, select an image, and then click **Select**.
4. Drag and drop image files into the window, or select **Browse Files** to locate and select the image files.
5. To overwrite files with duplicate names, select **Override floor plan images with same names**.
6. Select **Next**.
7. Select and drag the image border to crop the image.

   To zoom in and out on the floor plan image, select **+** and **-**, or use the mouse scroll wheel. The floor plan image adjusts as you scroll, allowing more precise cropping.
8. Select **Next**.
9. Select Point A and drag to Point B to set the scale for the floor plan.
10. Select **Done**.

## Edit a Site

Use this task to edit a site, site group, building, or floor in your network plan.

**Note**
For sites created before implementation of the mandatory time zone setting, ExtremeCloud IQ (New) derives the time zone from the site address. If the site address is not specified, the system uses GMT. Edit the site to specify the time zone.

1. Go to **Configuration** > **Sites**.
2. Select for the site, and then select **Edit**.
3. Change the fields as needed.
4. Select **Save**.

## Move a Site

Use this task to move a site to a new location.

1. Go to **Configuration** > **Sites**.
2. Select associated with the site to move it.
3. Select **Move**.
4. To move the site to an existing group, select an existing parent site group from the Association list.
5. Select **Move**.

## Export a Floor Plan

Use this task to export a floor plan.

1. Go to **Configuration** > **Sites**.
2. Select associated with the floor to export it.
3. Select **Export**.

   The floor plan is exported into .xml or .tar format.
4. Select **Export**.

## Clone a Building

Use this task to clone a building.

1. Go to **Configuration** > **Sites**.
2. Select associated with the building to clone it.
3. Select **Clone**.
4. Type a **Name** for the new building.
5. To add the new building an existing group, select an existing parent site group from the Association list.

## Delete a Site

Use this task to delete a site.

1. Go to **Configuration** > **Sites**
2. Select for the site.
3. Select **Delete**.

   If an object is in use, a pop-up window asks you to delete the references first. The default response is **Cancel**. To delete the object anyway, provide the randomly generated code to delete the location object.

**Warning**
Deleting objects with references can result in orphaned objects and other issues.

Related Links

Delete a Building or a Floor on page 275

## Delete a Building or a Floor

Use this task to delete a building or a floor.

1. Go to **Configuration** > **Sites**.
2. Expand the site for which you want to delete a building or floor.
3. Select for the building or floor.

   You can select multiple buildings or floors to delete at once.
4. 
5. Select **Delete**.

   If an object is in use, a pop-up window asks you to delete the references first. The default response is **Cancel**. To delete the object anyway, provide the randomly generated code to delete the location object.

**Warning**
Deleting objects with references can result in orphaned objects and other issues.

Related Links

Delete a Site on page 275

# Configuration | Network Policies


Configure an Express Policy on page 277
Add a Network Policy on page 278
Configure Policy Settings on page 279
Deploy a Network Policy on page 307
Configure the SSID for a Standard Wireless Network on page 308
Electronic Shelf Labels on page 388
Configure Device Templates on page 391
Configure Supplemental CLI on page 437
Configure Classification Rules for a Device Template on page 438
Fabric Attach on page 439
Configure Device Data Collection and Monitoring Options on page 441
Configure the BLE Service on page 442
Configure Presence Analytics on page 445
Configure WIPS on page 445
Configure a Location Server on page 449
Install CA Certificates on page 450
Configure a Layer 2 IPsec VPN Service on page 450
Settings for Multi-Link Operation on page 453


A network policy is a combination of configuration settings that can be applied to multiple APs, switches, and routers that share a common characteristic, such as being located at the same site or working together to connect multiple remote sites through VPN tunnels. The type of network policy depends on whether your deployment consists of only wireless AP devices, only switches, only routers, or a combination of these devices. One of the strengths of creating a single policy for multiple device types is that you might only need one unified policy for all your devices. The policy can include one or more SSIDs, device templates, and port types, as well as other configuration elements for networking, including management services such as QoS and VPN tunneling. The policy items are as follows:

- **Policy Details**: Select the policy type: **Wireless** (APs), **Switching** (Universal switches), or both. See Configure Policy Settings on page 279.
- Standard Wireless Networks: Define the wireless network (SSID) and the bands on which to broadcast each SSID, plus SSID usage (authentication, including RADIUS configuration), user access, and additional settings.

- Device Templates: Configure Access Point and Switch device templates.
- Deploy Policy: Push the configuration to your network devices.

**Note**

- The assigned **Access Scope** determines an administrator's access to **Common Objects**. Administrators without global access can see and work only with policy objects created for the sites to which they are assigned.
- Only Switch Engine/EXOS devices support common switch settings, templates, and port types.

Related Links

Add a Network Policy on page 278
Configure Policy Settings on page 279
Configure the SSID for a Standard Wireless Network on page 308
Configure Device Templates on page 391
Deploy a Network Policy on page 307

## Configure an Express Policy

**Express Policy Setup** is a streamlined workflow used to quickly create standard network policies using reliable default settings. With this feature, you can:

- Configure the network policy name and wireless SSID.
- Specify essential security types for the SSID (such as Open or PSK).
- Toggle basic Captive Web Portal (CWP) or Guest access settings without needing complex policy architecture.

**Express Policy Setup** is ideal for branch offices, retail locations, guest networks, or quick lab setups where standard default settings are sufficient.

1. Go to **Configuration** > **Network Policies**.
2. Select **Express Policy Setup**, and configure the settings:

**Table 105: Express Policy Setup settings**

| Setting | Description |
|---|---|
| Policy Name | Type a name to identify the policy. |
| Create Wireless Network | To create a wireless network (SSID), select the check box. |
| | Select the authentication method for the SSID:<br>• PPSK<br>• Open<br>• PSK<br>• WEP<br>• Enterprise |
| | Type a name to identify the SSID. |

**Table 105: Express Policy Setup settings (continued)**

| Setting | Description |
|---|---|
| Create CWP | To create a CWP, select the check box. |
| | Type a name to identify the CWP. |
| Use existing User Group | To specify an existing user group, select the checkbox. |
| | From the menu, select a user group. |

3. Select **Create**.

## Add a Network Policy

This topic guides you through the basic steps to provide clients with network access via Extreme Networks devices. This process assumes that APs and routers have been deployed and have established secure CAPWAP connections with Extreme Cloud IQ (NEW). Switches do not use CAPWAP connections. Extreme Networks routers and APs run IQ Engine and communicate with ExtremeCloud IQ (New) using CAPWAP on UDP port 12222 or CAPWAP-over-HTTP on TCP port 80. This is true whether they communicate with ExtremeCloud IQ (New) on-premises or in the cloud. Other supported devices communicate with ExtremeCloud IQ (New) using HTTPS on TCP port 443.

Sequential workflow tabs at the top of the page define the network policy configuration process. These tabs are: **1 Policy Details**, **2 Wireless**, **3 Switching/Routing**, and **4 Deploy Policy**. The selected tab is highlighted.

Use this task to add a new network policy.

1. Go to **Configuration** > **Network Policies**.

   You can display network policies in a list ( ) or in a thumbnail ( ) format.
2. Select  from the list view, or select **Add Network Policy** from the thumbnail view.
3. In the **New Policy** window, select a policy type: (Wireless, Switching/Routing, SR/Dell Switching, Branch Routing, or a combination, including all them).
4. Type a **Policy Name**.
5. (Optional) Type a **Description**.
6. Enable or disable **Presence Analytics**.

   Enable this option to collect customer behavior data. After you enable it, go to the **2 Wireless** workflow step, and from the left navigation bar, under **Application Management**, select **Presence Analytics**. This is where you configure analytics settings, such as trap interval, aging time, and aggregate time.
7. Select **SAVE**.
8. Configure Policy Settings on page 279, as required.
9. Select **NEXT**.

   The highlighted tab changes from **1 Policy Details** to **2 Wireless**, **3 Switching/Routing**, **4 SR/Dell Switching**, **5 Branch Routing** and **6 Deploy Policy**, depending on your configuration choices.

After you have configured the network policy, Deploy a Network Policy on page 307.

Related Links

Configure Policy Settings on page 279
Deploy a Network Policy on page 307

## Configure Policy Settings

The network policy settings that you configure depend on your requirements. For example, determine which default routing instance to use for NTP, DNS, Syslog, and SNMP for a switch.

This task is part of the network policy configuration workflow. Use this task to configure policy settings.

1. Go to **Configuration** > **Network Policies**.
2. Select an existing network policy, and then select , or to add a new one, select . to create a new policy.
3. Configure the **Policy Settings**.
   a. Configure DNS Server Policy Settings on page 279.
   b. Configure NTP Server Policy Settings on page 281.
   c. Configure SNMP Server Policy Settings on page 282.
   d. Configure Syslog Server Policy Settings on page 285.
   e. Configure Device Credentials Policy Settings on page 287.
   f. Configure the Device Time Zone on page 287.
   g. Configure Hive Policy Settings on page 288.
   h. Configure Management and Native VLAN Policy Settings on page 291.
   i. Configure IP Tracking Policy Settings on page 293.
   j. Configure LLDP/CDP Policy Settings on page 295.

   **Note**
   To configure LLDP port configurations on SR22XX, 23XX, VOSS, and EXOS devices, go to the device template or device configuration page. Configuring LLDP from this page can affect APs, XR, and 20XX/21XX switches, along with certain EXOS, VOSS, SR22XX, and 23XX Global LLDP parameters.

4. Configure the **Management Settings**.
   a. Configure Management Options on page 296.
   b. Configure Traffic Filters Policy Settings on page 305.
   c. Configure MGT IP Filters on page 306.
5. Select **SAVE**.
6. Select **Policy**, and then select **NEXT**.

Related Links

Configure Classification Rules for a Device Template on page 438

### Configure DNS Server Policy Settings

DNS is a critical service for ExtremeCloud managed devices and is required to permit each device to connect to and communicate with ExtremeCloud IQ (New) and related services.

Out of the box, and by default, unconfigured APs and switches find the DNS server to use from your DHCP server.

**Note**
For APs — If your DHCP server does not advertise a DNS server, the AP will instead use the following DNS servers from OpenDNS:

- 208.67.222.222
- 208.67.220.220

The usability of OpenDNS servers can vary depending on the country. Consult OpenDNS documentation for information on excluded countries.

Either your DHCP-defined DNS server or the two default DNS servers must be reachable outbound on UDP port 53 by each device connecting to ExtremeCloud IQ (New).

The DNS server settings defined in this part of the network policy configuration workflow are written to the configuration of your managed device after initial connection.

**Note**
If enabled, these DNS server settings will override the default DNS behaviors of your managed device. The DNS servers defined here must be reachable from your managed devices on outbound UDP port 53.

This task is part of the network policy configuration workflow. Use this task to configure **DNS Server Policy Settings** for a network policy.

1. Go to **Configuration** > **Network Policies**.
2. Select an existing network policy, and then select , or to add a new one, select . to create a new policy.
3. From the **Policy Settings** menu, select **DNS Server**.
4. Toggle the **DNS Server** setting to **ON**.
5. (Optional) To use existing DNS server settings, choose a DNS object from the menu.
6. Configure the DNS Server Settings on page 281.
7. To add a new DNS server, select .
   a. Type the IP address of the new DNS server.
   b. Select **ADD**.

   You can add up to three servers. The first entry is the primary server. The secondary entry is the secondary server, and the third entry is the tertiary server. Use the arrows in the **Order** column to change the order.
8. If you want to use classification, select **Apply DNS servers to devices via classification**.
   a. To add a classification rule, select .
   b. To specify an existing classification rule, select .

   For more information, see Configure Classification Rules on page 291
9. Select **SAVE DNS SERVER**.

Related Links

DNS Server Settings on page 281

Configure Policy Settings on page 279

*DNS Server Settings*

**Table 106: Settings for DNS server profiles**

| Setting | Description |
|---|---|
| Name | (Required)<br>Type a **Name** for the default DNS server. |
| Domain Name | Type a **Domain Name** for the default DNS server. |
| Description | Type a description for the default DNS server. Although optional, entering a description is helpful for troubleshooting and for identifying the DNS server. |

Related Links

Configure DNS Server Policy Settings on page 279

## Configure NTP Server Policy Settings

NTP is a critical service for ExtremeCloud managed devices and is required to permit each device to securely connect with ExtremeCloud IQ (New) and related services and to ensure alerts and events have the correct timestamp.

By default, Extreme Networks access points (APs) and switches try to contact the NTP server assigned by your DHCP server. If your DHCP server does not advertise an NTP server, the device automatically attempts to resolve and connect to the NTP server at `0.aerohive.pool.ntp.org`. Device DNS must be functioning correctly to contact the NTP server.

Either your DHCP-defined NTP server or the default NTP server must be reachable outbound on UDP port 123 by each device connecting to ExtremeCloud IQ (New).

**Note**
If using a Windows server as your NTP server, your Windows server must synchronize with an upstream NTP server for Extreme APs to trust and accept responses from the Windows NTP server.

This task is part of the network policy configuration workflow. Use this task to configure NTP Server policy settings.

**Note**
If enabled, these NTP server settings override the default NTP behaviors of your managed devices. The NTP servers defined here must be reachable from your managed devices on outbound UDP port 123.

1. Go to **Configuration** > **Network Policies**
2. Select an existing network policy, and then select , or to add a new one, select .
3. For **Policy Settings**, select **NTP Server**.
4. Toggle **NTP Server** to **ON**.

5. To use existing NTP server settings, select , and choose an NTP object.
6. Configure NTP Server Settings on page 282.
7. To add a new NTP server to the list, select .
   a. To use an existing NTP, select , and choose a server.
   b. To add a new NTP server, select , and then select **IP Address** or **Host Name**.
   c. Type a **Name** for the new object.

      You can use the menu to change your previous selection (**IP Address** or **Host Name**).
   d. Select **SAVE IP OBJECT**.
   e. Select **ADD**.

      ExtremeCloud IQ (New) accesses NTP servers in order, from the top down. Use the arrows to rearrange them.
8. If you want to use classification, select **Apply NTP servers to devices via classification**.
   a. To add a classification rule, select .
   b. To specify an existing classification rule, select .

   For more information, see Configure Classification Rules on page 291.
9. Select **SAVE NTP SERVER**.

Related Links

NTP Server Settings on page 282
Configure Policy Settings on page 279

*NTP Server Settings*

**Table 107: Settings for NTP server profiles**

| Setting | Description |
|---|---|
| Name | Type a **Name** for the NTP server. |
| Domain Name | (Optional)<br>Type a **Domain Name** for the NTP server. |
| Synchronize the device clock with the NTP servers. | 1. Type the **HiveOS Device Sync Interval** value (in minutes).<br>2. From the **Switch Sync Interval**, select a value. |

Related Links

Configure NTP Server Policy Settings on page 281

## Configure SNMP Server Policy Settings

SNMP (Simple Network Management Protocol) exchanges information between network devices and one or more central network management stations (referred to in ExtremeCloud IQ as an SNMP server). The devices send traps, which are unsolicited messages, to the management stations on UDP port 162 when events of note occur. Management stations also query monitored devices to check their operational status. The queries are in the form of get commands that management stations send on UDP port 161.

This task is part of the network policy configuration workflow. Use this task to configure **SNMP Server Policy Settings** for a network policy.

1. Go to **Configuration** > **Network Policies**
2. Select an existing network policy, and then select , or to add a new one, select .
3. For **Policy Settings**, select **SNMP Server**.
4. Toggle **SNMP Server** to **ON**.
5. To use existing SNMP server settings, select , and choose an SNMP server.
6. Configure the SNMP Server Settings on page 284.
7. To add a new SNMP server, select , and then select **IP Address** or **Host Name**.

   You can add up to three SNMP servers to the profile.
8. To use an existing SNMP server, select it from the menu.
9. Type a **Name** for the new IP object.

   You can use the menu to change your previous selection (**IP Address** or **Host Name**).
10. Select **SAVE IP OBJECT**.
11. For **Version**, select the version of SNMP that is running on the management station you intend to use.
12. For **Operation**, select the type of activity to permit between the specified SNMP management station and the devices assigned to this profile in the network policy.
    - **None**: Disable all SNMP activity for the specified management station.
    - **Get**: Permit GET commands sent from the management station to a device to retrieve MIBs.
    - **Get and Trap**: Permit reception of GET commands from the management station and transmission of traps to the management station.
    - **Trap**: Permit devices to send messages notifying the management system about events of interest.
13. In the Community field (for SNMP V2C and V1), type a text string that must accompany queries from the management station.

    The community string acts similarly to a password, in that devices accept queries only from the management stations that send the correct community string.
14. Select **ADD SNMP SERVER**.
15. (Optional) Select **Apply SNMP servers to devices via classification**.

    a. To add a classification rule, select .

    b. To specify an existing classification rule, select .

    For more information, see Configure Classification Rules on page 291.
16. Select **SAVE SNMP SERVER**.

Related Links

SNMP Server Settings on page 284
Configure Policy Settings on page 279

*SNMP Server Settings*

**Table 108: Settings for SNMP servers**

| Setting | Description |
|---|---|
| Name | Type a **Name** for the server. |
| Description | (Optional)<br>Type a brief **Description** for the server. Although optional, entering a description is helpful for troubleshooting and for identifying the server. |
| SNMP Contact | Type the **SNMP Contact** information for the SNMP server administrator, so they can be contacted if necessary. This can be an email address, telephone number, physical location, or a combination. |
| Disable to Send traps over CAPWAP | Clear the check box for **Disable to Send traps over CAPWAP** to enable devices to send trap information (events and alarms) to ExtremeCloud IQ over a CAPWAP connection, or leave the box checked to disable this action. |
| SNMP Server | Select an SNMP server from the drop-down list.<br>Choose the IP address or host name object for the SNMP server or servers that will access the devices. To permit management access from a single SNMP server, choose an IP address or host name that defines only that server. To permit management access from an entire subnet, choose an IP address or host name that defines that subnet. If you do not see the IP address or host name that you need, select **+** and define one. |
| Version | From the drop-down list, select the version of SNMP that is running on the management station that you intend to use. |
| Operation | Select the type of activity to permit between the specified SNMP management station and the devices in the network policy to which you will assign this profile. Options include:<br>• **None**: Disable all SNMP activity for the specified management station.<br>• **Get**: Permit GET commands sent from the management station to a device to retrieve MIBs.<br>• **Get and Trap**: Permit the reception of GET commands from the management station and the transmission of traps to the management station.<br>• **Trap**: Permit devices to send messages notifying the management system of events of interest. |
| Community | For SNMP V2C and V1, enter a text string that must accompany queries from the management station. The community string acts similarly to a password, such that devices accept queries only from management stations that send the correct community string. |

Related Links

Configure SNMP Server Policy Settings on page 282

## Configure Syslog Server Policy Settings

You can configure syslog server profiles for device log entry storage. The syslog administrator can then sort messages by facility and see all the ones relating to Extreme Networks devices. The administrator can further sort the messages by IP address and by severity. Syslog server settings can be configured as common objects, from within the network policy workflow, and at the device level. Device-level settings override network policy settings.

**Note**
Using NTP to synchronize the time stamp on messages from all syslog clients can ensure that all messages reported to the syslog server appear in their proper chronological order. Otherwise, it can be very difficult to interpret a series of events affecting multiple network devices, such as reconnaissance probes and network intrusion exploits. To further ensure synchronicity, as a best practice, have all syslog clients use the same NTP time server. See Configure NTP Server Policy Settings on page 281.

This task is part of the network policy configuration workflow. Use this task to configure the **Policy Settings** for a Syslog server.

1. Go to **Configuration** > **Network Policies**
2. Select an existing network policy, and then select , or to add a new one, select .
3. For **Policy Settings**, select **Syslog Server**.
4. Toggle **Syslog Server** to **ON**.
5. To use existing syslog server settings, select , and choose a syslog server.
6. Configure the Syslog Server Settings on page 286.
7. To add a new syslog server to the table, select .

   Use the up or down arrows to reorder the list of syslog servers in the table.
8. Select , and choose an existing syslog IP address or host name, or select .
9. For **Severity**, select the log level.
10. Type the **Port** number.
11. Select **ADD**.
12. Select **Assign Syslog servers via Classification**.
    a. To add a classification rule, select .
    b. To specify an existing classification rule, select .

    For more information, see Configure Classification Rules on page 291
13. Select **SAVE SYSLOG SERVER**.

Related Links

Syslog Server Settings on page 286
Configure Policy Settings on page 279

*Syslog Server Settings*

**Table 109: Settings for Syslog servers**

| Setting | Description |
|---|---|
| Name | Type a **Name** for the syslog server. |
| Description | (Optional)<br>Type a **Description** for the syslog server. Although optional, entering a description is helpful for troubleshooting and for identifying the server. |
| **Syslog Facility** | |
| IQ Engine Syslog Facility | Select an **IQ Engine Syslog Facility** to categorize messages sent to syslog from IQ Engine devices.<br>Because syslog servers can receive messages from many types of network devices, such as routers, firewalls, mail servers, you can designate one of the twelve syslog facilities reserved for local use—Auth, Authpriv, Security, User, and Local0 to Local7—to mark messages from all the devices to which you apply this management service set. |
| Non-IQ Syslog Facility | Select a **Non-IQ Syslog Facility** to categorize messages sent to syslog from non-IQ Engine devices. |
| Syslog Group | Select the arrow to expand the **Syslog Group** section, and use the menus to select the log level for each category.<br>• Emergency<br>• Alert<br>• Critical<br>• Error<br>• Warning<br>• Notification<br>• Info<br>• Debug<br>Syslog groups organize messages by category and limit the number of messages sent based on severity level. APs do not send messages that are below the assigned level to the syslog server. |
| Syslog servers are on the same internal network as the reporting Extreme Networks devices (for PCI DSS compliance) | If you must make PCI DSS compliance reports, select the check box. If the servers are on an external network outside the firewall, clear the check box. |
| Enable hostname in syslog headers | To add the hostname to the headers for all syslog messages, select the check box. |

Related Links

Configure Syslog Server Policy Settings on page 285

## Configure Device Credentials Policy Settings

ExtremeCloud IQ (New) uses device credentials for remote access to devices through Telnet, SSH, or console connections. If you do not configure the Administrator and Read Only Administrator accounts, global device management settings apply.

**Note**
If you configure a new administrator account, the new account replaces the default account.

This task is part of the network policy configuration workflow. Use this task to configure **NTP Server Policy Settings** for a network policy.

1. Go to **Configuration** > **Network Policies**.
2. Select an existing network policy, and then select , or to add a new one, select ..
3. For **Policy Settings**, select **Device Credentials**.
4. Configure the following settings:

**Table 110: Device Credentials**

| Setting | Description |
|---|---|
| **Administrator Account** | |
| Admin Name | Type the name of the **Administrator** account. |
| Password | Type the password for the **Administrator** account. |
| Show Password | Select the check box to show the password. |
| **Read Only Administrator** | |
| Admin Name | Type the name of the **Read Only Administrator** account. |
| Password | Type the password for the **Read Only Administrator** account. |
| Show Password | Select the check box to show the password. |

5. Select **SAVE**.

Related Links

Configure Policy Settings on page 279

## Configure the Device Time Zone

This task is part of the network policy configuration workflow. Use this task to configure the **Device Time Zone** for a network policy.

1. Go to **Configuration** > **Network Policies**.
2. Select an existing network policy, and then select , or to add a new one, select ..
3. From the **Policy Settings** menu, select **Device Time Zone**.
4. From the **Time Zone** menu, select a time zone.
5. If you want to use classification, select the **Apply time zone to devices via classification** check box.
6. Select **SAVE**.

Related Links

Configure Policy Settings on page 279

## Configure Hive Policy Settings

This task is part of the network policy configuration workflow. Use this task to configure **Hive** policy settings for a network policy.

1. Go to **Configuration** > **Network Policies**.
2. Select an existing network policy, and then select , or to add a new one, select . to create a new policy.
3. From the **Policy Settings** menu, select **HIVE**.
4. (Optional) To use existing Hive settings, choose a Hive object from the menu.
5. Configure the Hive Profile Settings on page 288.
6. Apply MAC filters to restrict devices that can join the hive.

   You can select existing filters from the table or add new filters.
7. From the menu, choose the default action (**Permit** or **Deny**) for devices that have a MAC address or OUI that does not match the selected MAC filter.
8. Select **SAVE**.

Related Links

Configure Policy Settings on page 279
Hive Profile Settings on page 288

*Hive Profile Settings*

**Table 111: Hive profile settings**

| Setting | Description |
|---|---|
| Name | Type a **Name** for the new profile. |
| Hive Control Traffic Port | Type the port number for Hive traffic control.<br>Hive communications operate at Layers 2 and 3. The default port number for Layer 3 hive communications and for roaming-related traffic is UDP 3000. If a different service on your network is already using port 3000, you can change this to a number from 1024 to 65535, as long as the new setting is at least 50 greater or less than the current setting. For example, if the current port number is 3000, you can set a new port number higher than 3050. |
| Description | (Optional)<br>Type a description for the new profile. Although optional, entering a description is helpful for troubleshooting and for identifying the profile. |
| **Alarms** | |
| CAPWAP Delay Alarms | Toggle the setting **ON** or **OFF**. |
| **Security** | |

**Table 111: Hive profile settings (continued)**

| Setting | Description |
|---|---|
| Encryption Protection | Toggle the setting **ON** or **OFF**.<br>Disable **Encryption Protection** to have ExtremeCloud IQ derive a default password from the hive name. |
| Encryption Password | Choose between **Auto Generate** and **Manual**.<br>Hive members use this password to authenticate to each other over the wireless backhaul link using WPA-PSK CCMP (AES). To see the password that you entered, clear the **Shared Secret** > **Show Password** check box. |
| MAC-based DoS Prevention Rules | Select **Hive** or **Client**, and modify the settings in the dialog box.<br>Extreme Networks devices ship with default hive- and SSID-level DoS detection settings for some frame types commonly used in DoS attacks. You can raise the thresholds to reduce false alarms or lower them to receive more alarms indicative of spikes in certain types of traffic.<br>• **DoS prevention rules for hives** apply to wireless traffic from all radios that might reach the backhaul or access channel from wireless clients or nearby access points broadcasting on the same channel. You can define settings to detect DoS attacks on the radio channels that a device uses for hive communications and for SSID access traffic.<br>• **DoS prevention rules for clients** apply to traffic originating from a single neighboring radio. The source might be a neighbor member or a nearby device outside the network that is broadcasting on the same channel the Extreme Networks device is using for its wireless backhaul communications, or for SSID access traffic.<br>For both types of rules, you can change the alarm thresholds and enable or disable settings for each DoS Detection type: Probe Requests and Responses, (Re) Associations, Association and Disassociation Requests and Responses, Authentication and Deauthentication, and EAP over LAN (EAPoL). Wireless clients periodically send probe requests to determine whether access points are within range. The threshold determines the number of messages per minute required to trigger an alarm about a possible DoS attack. The alarm interval determines the length between repeated alarms when the number of messages continues to exceed the threshold. |
| **Wireless Mesh Settings** | |
| Request to Send Threshold | Type the maximum frame size that triggers the device to send a request to send (RTS) message, before sending a large frame. The default setting is 2346 bytes. |
| Fragment Threshold | Type the maximum IEEE 802.11 frame size for control traffic sent over the wireless backhaul. The device sends larger frames in fragments. The default setting is 2346 bytes. |
| Require minimum wireless signal strength for creating wireless mesh | Select the check box to require a minimum wireless signal strength for creating wireless mesh, and configure the related settings. |

**Table 111: Hive profile settings (continued)**

| Setting | Description |
|---|---|
| Signal Strength Threshold | Use the slider to specify a signal strength between 90 dBm and - 55 dBm.<br>This value is the minimum signal strength required to enable members to form a wireless backhaul link. The default is -80 dBm. |
| Polling Interval | Type the number of minutes (1 to 60) between polling for the signal strength of neighboring members.<br>A lower interval increases traffic on the network slightly, especially in dense environments. However, a lower interval also increases the responsiveness to changes in signal strength. A higher interval reduces responsiveness to signal strength changes, which can be preferable in environments where severe and frequent signal strength fluctuations cause members to drop and re-establish connections. The default is every 60 seconds. |
| **Client Roaming > Detect neighbor devices** | |
| Devices send keepalive heartbeats every | Set the interval between keepalive heartbeats.<br>The default is 10 seconds, and the range is 5 to 360,000 seconds (100 hours). To calculate the length of time, multiply the keepalive interval by the number of missed keepalives. For example, 10 seconds (interval) x 5 (missed keepalives) results in a neighbor aging out after 50 seconds. |
| Remove neighbor if the number of missed keepalive heartbeats exceeds | Specify the number of missed heartbeats before ExtremeCloud IQ (New) removes a neighbor. |
| **Client Roaming > Share connected client information (Roaming cache)** | |
| Devices send client information every | Specify how often devices send client information. The default is 60 seconds. |
| Remove cached client information when absent from updates after | Specify the number of missed updates, after which ExtremeCloud IQ (New) deletes cached client information for the affected client. |
| Update all hive members within radio range, including Layer 3 neighbors | Select the check box to update all hive members within radio range, including Layer 3 neighbors. |
| Update hive members in the same subnet and VLAN. | Select the check box to update hive members in the same subnet and VLAN. |
| **IP Address Preference** | |
| Use IP address type first with | (Required)<br>Choose the IP address version **IPv4** or **IPv6**. |

Related Links

Configure Hive Policy Settings on page 288

## Configure Management and Native VLAN Policy Settings

This task is part of the network policy configuration workflow. Use this task to configure **Management and Native VLAN** policy settings for a network policy.

1. Go to **Configuration** > **Network Policies**.
2. Select an existing network policy, and then select , or to add a new one, select ..
3. From the **Policy Settings** menu, select **Management and Native VLAN**.
4. Select an **MGT Interface VLAN** and choose an existing object, or to add a new one, select ..
5. For a new **MGT Interface VLAN**, configure the settings.
   a. Type a **Name** for the new VLAN object.
   b. Type a **VLAN ID** for the new VLAN object.
   c. (Optional) If you want to use classification, select **Apply VLANs to devices using classification**.

      See Configure Classification Rules on page 291.
   d. To add a classification rule, select .
   e. To specify an existing classification rule, select .
6. Select an **Native (Untagged) VLAN***For IQ Engine devices only* and choose an existing object, or to add a new one, select ..
7. For a new **Native (Untagged) VLAN**, configure the settings.
   a. Type a **Name** for the new VLAN object.
   b. Type a **VLAN ID** for the new VLAN object.
   c. (Optional) If you want to use classification, select **Apply VLANs to devices using classification**.

      See Configure Classification Rules on page 291.
   d. To add a classification rule, select .
   e. To specify an existing classification rule, select .
8. Select **SAVE VLAN**.

Related Links

Configure Classification Rules on page 291
Configure Policy Settings on page 279

*Configure Classification Rules*

Before you can use classification rules, you must create a network location, along with cloud config groups, IP addresses, and IP subnets.

ExtremeCloud IQ (New) supports multiple classification rules for DNS servers, VLANs, RADIUS servers, device templates, user groups, and private client groups (PCGs). You can create classification rules as part of a network policy or as a common object.

**Important**
Classification rules for IP objects are supported only when IP objects are used to create firewall rules.

- Configure **Device Location** rules to assign different DNS and RADIUS servers and different time zones to different physical locations.
- Configure **Cloud Config Groups** (CCGs) to create user passwords which restrict access to private and personal network devices.
- Configure **IP Address** classification rules to associate user groups so they can communicate using their own private networks.
- Configure **IP Subnet** classification rules to support multiple user-group private networks.
- Configure **IP Range** classification rules for multiple user-group private networks.

Use this task to configure classification rules when you configure Management and Native VLAN policy settings, or as part of another task flow.

1. Select , choose an existing rule, and then select , or to add a new one, select .
2. Enter a **Name** for the rule.
3. (Optional) Enter a **Description** for the rule.
4. Select , and then choose the rule type to configure.

   Choose from the following rule types:

**Table 112: Rule types**

| Selected rule type | Do this |
|---|---|
| Device Location | a. Drill down until you reach the location level at which the device resides.<br>b. Select **Select**.<br>The location appears in the **Classification Rules** table. |
| Cloud Config Group | a. Select the **Match Type**.<br>b. Select and choose an existing group, or select .<br>c. Select **CLOUD CONFIG GROUP**.<br>d. Select **CONTINUE**. |
| IP Address | a. From the **Match Type** menu, select **Contains** or **Does Not Contain**.<br>b. Select and choose an existing IP address, or select .<br>If you do not see the IP address that you want, select **New** to create a new IP address.<br>c. Select **SAVE IP**.<br>d. Select **CONTINUE**. |

**Table 112: Rule types (continued)**

| Selected rule type | Do this |
|---|---|
| IP Subnet | a. From the **Match Type** menu, select **Contains** or **Does Not Contain**.<br>b. Select and choose an existing IP subnet, or select menu.<br>If you do not see the IP subnet that you want, select **New** to create a new IP subnet.<br>c. Select **SAVE SUBNET**.<br>d. Select **CONTINUE**. |
| IP Range | a. From the **Match Type** menu, select **Contains** or **Does Not Contain**.<br>b. Select and choose an existing IP range, or select .<br>If you do not see the IP range that you want, select **New** to create a new IP range.<br>c. Select **SAVE IP**.<br>d. Select **CONTINUE**. |

5. Select **SAVE RULE**.
6. Use the up and down arrows in the **Order** column to define the order in which the location, cloud config group, IP address, IP subnet, and IP range objects appear.
   ExtremeCloud IQ (New) uses a top-down, first-match, stop-on-match processing method for these objects. Therefore, if a device is a member of more than one matching object for an element, only the first match applies.

## Configure IP Tracking Policy Settings

This task is part of the network policy configuration workflow. Use this task to configure **IP Tracking** policy settings for a network policy.

1. Go to **Configuration** > **Network Policies**.
2. Select an existing network policy, and then select , or to add a new one, select . to create a new policy.
3. From the **Policy Settings** menu, select **IP Tracking**.
4. Toggle the **IP Tracking** setting to **ON**.
5. Select a tracking group and use the single-arrow controls to move it from **Available IP Tracking Groups** to **Selected IP Tracking Groups**, or vice versa.
   Use the double-arrow controls to move all of the tracking groups.
6. To add a new IP tracking group, select **ADD ANOTHER IP TRACKING GROUP**, and then configure the IP Tracking Group Settings on page 294.
7. Select **SAVE**.

Related Links

IP Tracking Group Settings on page 294
Configure Policy Settings on page 279

*IP Tracking Group Settings*

**Table 113: Settings for IP Tracking Groups**

| Setting | Description |
|---|---|
| Name | Type a **Name** for the group. |
| Description | (Optional)<br>Type a **Description** for the group. Although optional, entering a description is helpful for troubleshooting and for identifying the group. |
| Connectivity | Select either **Backhaul Connectivity Tracking for APs** or **WAN Interface Connectivity Tracking for APs**. |
| Enable IP Tracking | To activate this IP tracking group, select the check box. Clear the check box to exclude the group from **Available IP Tracking Groups**. |
| **Track the Following Targets** | |
| IP Addresses | Enter up to four IP addresses, separated by commas. If you are also tracking the default gateway, enter up to three IP addresses. |
| Default Gateway | If the IP addresses use the default gateway, select **Default Gateway**. Otherwise, clear the check box. |
| Take action when | From the menu, select a condition for which to take action. Choose between **All targets become unresponsive** and **A single target becomes unresponsive**. |
| Tracking Interval | (Required)<br>Type the tracking interval for this group. Default: 6 |
| Tracking Retries | (Required)<br>Type the number of retries before taking action for an IP address failure. Default: 3 |
| **Actions to take when target becomes unresponsive** | |
| Enable the virtual access console | Select the check box to take this action when the target is unresponsive. |
| Disable all active SSIDs | Select the check box to take this action when the target is unresponsive. |
| Start the backhaul (mesh) failover procedure | Select the check box to take this action when the target is unresponsive. |

Related Links

Configure IP Tracking Policy Settings on page 293

## Configure LLDP/CDP Policy Settings

This task is part of the network policy configuration workflow. Use this task to configure LLDP/CDP policy settings for a network policy.

**Note**

LLDP is on by default in ExtremeCloud IQ (New). With IQ Engine Release 10.7.5 and later, LLDP is on by default. This is the new default behavior for all new devices running 10.7.5 and later.

If LLDP is disabled in the network policy, upgrading to 10.7.5 enables LLDP until after you perform a configuration update.

1. Go to **Configuration** > **Network Policies**.
2. Select an existing network policy, and then select , or to add a new one, select .
3. For **Policy Settings**, select **LLDP/CDP**.
4. Toggle **LLDP/CDP** to **ON**.
5. To use existing LLDP/CDP settings, select , and choose an LLDP/CDP object.
6. Configure the LLDP and CDP Settings on page 295.

Related Links

Configure Policy Settings on page 279
LLDP and CDP Settings on page 295

*LLDP and CDP Settings*

**Table 114: Settings for LLDP and CDP**

| Setting | Description |
|---|---|
| Name | Type a **Name** for the new LLDP/CDP object. |
| Description | (Optional)<br>Type a **Description** for the new LLDP/CDP object. Although optional, entering a description is helpful for troubleshooting and for identifying the LLDP/CDP object. |
| Enable LLDP on access ports | Select the check box to permit LLDP on access ports.<br><br>**Note:** LLDP is enabled on other port types by default. |
| Enable receive only mode. | Select the check box to permit devices to receive, cache, and display LLDP advertisements from other devices, but to not advertise their own data. |
| LLDP entries to cache | (IQ Engine Only)<br>Type the maximum number of LLDP entries from neighboring network devices that a device can store in its cache. |
| Neighbors keep Extreme Networks advertisements for | Type the number of seconds for which neighboring devices retain LLDP advertisements.<br>Increase the time while troubleshooting a network issue and decrease it if you need to reduce overall network traffic. |
| Advertisements Interval | Type the number of seconds between LLDP advertisements sent to neighboring network devices. |

**Table 114: Settings for LLDP and CDP (continued)**

| Setting | Description |
|---|---|
| Timer Hold | Type a multiple of the advertisements interval. (EXOS/Switch Engine, VOSS/Fabric Engine, SR22XX/23XX, Dell) |
| Max power for LLDP advertisements | Select **Use the default max power in IQ Engine** to use the maximum power level that devices can request in LLDP advertisements. |
| LLDP Initialization Delay Time | Type the length of time that you want the interface to wait before initializing LLDP. |
| Fast start repeat count | Type the number of advertisement LLDP frames to send when the connected device (such as an IP phone) starts up or is detected. |
| CDP (Cisco Discovery Protocol) | Toggle CDP **ON** to enable devices to receive and cache CDP advertisements.<br><br>**Note:** You can enable LLDP and CDP concurrently.<br><br>CDP is a proprietary Data Link Layer protocol developed by Cisco Systems. |
| Enable CDP on access ports. | Select the check box to permit CDP on access ports. By default, CDP is enabled on other port types. |
| CDP entries to cache | Type the maximum number of CDP entries that a device can store in its cache. |

Related Links

Configure LLDP/CDP Policy Settings on page 295

## Configure Management Options

After you enable **Management Options** in the network policy, you can re-use an existing **Management Options** object, or configure the settings manually.

This task is part of the network policy configuration workflow. Use this task to configure **Management Options** for a network policy.

1. Go to **Configuration** > **Network Policies**.
2. Select an existing network policy, and then select , or to add a new one, select . to create a new policy.
3. From the **Management Settings** menu, select **Management Options**.
4. Toggle the **Management Options** setting to **ON**.
5. To reuse existing management options settings, select **Re-use MGT IP Filter**, and then select an existing **Management Option**.
6. Enter a **Name**.
7. (Optional) Enter a **Description**.

   Although optional, entering a description is helpful for troubleshooting and for identifying the **Management Options** object.
8. Configure the settings for Management Options on page 297.

9. Select **SAVE**.

Related Links

Management Options on page 297
Configure Policy Settings on page 279

*Management Options*

Use these settings to control how administrators authenticate and how they access the devices they manage. You can configure global and device-level settings. For example, you can enable or disable the reset button and console port, enable or disable proxy ARP requests and replies, enable APs and routers to forward broadcasts and multicasts between SSIDs, and a variety of other options such as adjusting LED brightness, and setting temperature alarms.

#### Forwarding Engine Control Management Options

The forwarding engine controls the type of traffic being forwarded between interfaces, between GRE tunnels, and sets logging features.

**Table 115: Forwarding Engine Control Settings**

| Setting | Description |
|---|---|
| **Forwarding Engine Control** | |
| GRE Tunneling Selective Multicast Forwarding | Select one of the following options:<br>• **Block All**—Prohibits forwarding multicast and broadcast traffic through tunnels.<br>• **Allow All**—Enables forwarding multicast and broadcast traffic through tunnels.<br>ExtremeCloud IQ (New) devices can selectively block or permit broadcast and multicast traffic through GRE tunnels to reduce traffic congestion. You can filter using a blocked list that blocks the forwarding of all broadcast and multicast traffic through GRE tunnels (or blocks all except to a few select destinations) or using an allow list that permits all broadcast and multicast traffic through GRE tunnels (or allows all, except to a few destinations). |
| Exception IP List | Add an entry (destination IP Address and Netmask) to the **Exception IP List**. Type the values, and then select **ADD**. |
| **Service Control** | |
| Limit MAC Sessions per Station | Select **Limit MAC Sessions per Station** to enable the feature, and then type the maximum number of (Layer 2 sessions) that can be created to or from a station.<br>By default, devices do not enforce MAC or IP session limits per station. By default, devices do not enforce IP session limits per station. |

**Table 115: Forwarding Engine Control Settings (continued)**

| Setting | Description |
|---|---|
| Limit IP Sessions per Station | Select **Limit IP Sessions per Station** to enable the feature, and type the maximum number of sessions per station.<br>This feature enables a device to monitor the TCP MSS (maximum segment size) option in TCP SYN and SYN-ACK messages for traffic that the device is going to pass through GRE tunnels (for Layer 3 roaming and static identity-based tunnels) and GRE-over-IPsec tunnels (for IPsec VPN tunnels). The device can then notify the sender to adjust the TCP MSS value if it exceeds a maximum threshold. |
| Enable TCP Maximum Segment Size | Select **Enable TCP Maximum Segment Size** to enable the feature, and then type the maximum segment size.<br>When establishing a TCP connection, neither end is aware of the packet processing done by network forwarding equipment in between. For example, if a device has to send traffic through an IPsec VPN tunnel, then it adds a GRE header, IPsec header, and possibly a UDP header for NAT-Traversal to each packet. Since the additional headers expand packet size, the device is forced to fragment them, which increases packet processing and slows down throughput. To avoid fragmentation, the device can adjust the MSS (maximum segment size) value inside the initial SYN packet to provide room for the additional headers.<br>The default thresholds are 1414 bytes for GRE tunnels and 1336 bytes for GRE-over-IPsec tunnels and are based on encapsulation overhead of the corresponding tunnel type and the maximum transmission unit (MTU) for the mgt0 interface, which is 1500 bytes by default. If you change the MTU and use "auto" for the TCP MSS option, the device automatically readjusts the TCP MSS thresholds. |
| DHCP Option 82: Replace MAC Address with Hostname | To switch between MAC address and Hostname for DHCP option 82,enable **DHCP Option 82: Replace MAC Address with Hostname**. The default is MAC address. |
| ARP Shield | Enable **ARP Shield** to prevent Man-In-the-Middle attacks by client devices attempting to impersonate critical network resources on the network such as a network gateway or DNS server through an ARP poisoning attack.<br>ARP Shield should not be used if any clients on the network are assigned static IP addresses. ARP Shield is disabled by default and can only be enabled on access points running IQ Engine 6.8.1 and above. Enabling ARP Shield is not enforced on access points running IQ Engine 6.5, switches, routers, or Virtual Gateway appliances. |

**Table 115: Forwarding Engine Control Settings (continued)**

| Setting | Description |
|---|---|
| DHCP Shield | Disable **DHCP Shield** to turn off the built-in ability for IQ Engine to prevent attached clients from impersonating a DHCP server.<br>In the default enabled state, connected clients are blocked from responding to DHCP server discovery or IP lease requests. When disabled, connected clients can respond to DHCP discovery or IP lease requests. DHCP Shield is enabled by default on access points running IQ Engine 6.8.1 and above.<br>Disabling DHCP Shield results in no changes to access points running IQ Engine 6.5, switches, routers, or Virtual Gateway appliances. |
| Proxy ARP | **Proxy ARP** requests enable learning MAC addresses and proxy replies to ARP requests. Select one of the following slider bar options:<br>• **Disabled**: Not recommended. Disabling turns off all proxy ARP handling capabilities. It increases air time utilization by having to send ARPs to clients in the roaming cache. Use for troubleshooting only. When diagnosing a network issue, you might need to permit ARP requests and replies between wireless clients and network devices (such as the default gateway) to flow directly across the device without proxy.<br>• **Legacy**: Not recommended, but is available for legacy Wi-Fi 4 APs.<br>• **Enhanced**: Preferred and is the highest level of adoption. Supported on Wi-Fi 5 APs and newer. Does not support ARP suppression for devices not in the roaming cache. Wired clients can flood the air with ARPs.<br>• **ARP Suppression**: Recommended, but support is limited to AP3000, AP5010, and AP5050. Protects airtime from overuse by unneeded ARP traffic. |
| Disable Inter SSID Flooding | Select **Disable Inter SSID Flooding** to prohibit a device from forwarding traffic that it receives from clients in one SSID to clients associated with the same device in another SSID.<br>Instead, such traffic must first cross the device from an interface in access mode to an interface in backhaul mode. From there, the traffic might pass through an internal firewall that performs deep-packet inspection, URL filtering, or antivirus checking, and other operations, before sending the traffic back across the device to reach the clients in the destination SSID. |
| Disable WebUI Without Disabling CWP | Select **Disable WebUI Without Disabling CWP** to disable the local web user interface on a device to improve system security without disabling the associated captive web portal. |

**Table 115: Forwarding Engine Control Settings (continued)**

| Setting | Description |
|---|---|
| Enable legacy HTTP redirect | Select **Enable legacy HTTP redirect** to enable redirects to legacy HTTP sites.<br><br>**Note:** Extreme Networks recommends HTTPS for best security. This option is provided for legacy clients, for which HTTPS is not suitable. |
| **Global Logging Options for Firewall Policies** | |
| Log | Select the corresponding check boxes to enable the generation of logs for the following scenarios:<br>• **Drop packets that are denied by IP or MAC firewall policies**<br>• **The first packets of the session destined for the Extreme Networks device itself** |
| Drop | Select the corresponding check boxes to enable the generation of logs for the following scenarios:<br>• **Fragmented IP Packets**<br>• **All non-management traffic destined for the Extreme Networks device itself** |

#### System Settings Management Options

Use the settings in this section to adjust various device-level functions, including device health alarm thresholds, VoIP features, and client OS detection types. Miscellaneous settings cover reset, console, PoE, and data collection features.

**Table 116: System Settings**

| Setting | Description |
|---|---|
| LED Brightness | Set the device status LED brightness level. Select an option from the menu: **Bright**, **Soft**, **Dim**, or **Off**. |
| Temperature Alarm Threshold | Specify the ambient celsius temperature threshold that triggers an alarm. |
| Fans Underspeed Alarm Threshold | Specify the minimum RPM operating speed for fans. Speeds below this value trigger an alarm. |
| Call Admission Control | To enable **Call Admission Control**, toggle the setting to **ON**. If enabled, devices monitor VoIP traffic to determine if there is enough available airtime for new VoIP calls. |

**Table 116: System Settings (continued)**

| Setting | Description |
|---|---|
| Airtime per Second | Set the amount of airtime reserved for VoIP traffic. Decreasing the amount of reserved airtime for VoIP traffic frees more airtime for traffic other than VoIP. This can be useful if there are only a few VoIP users on the WLAN. For a high number of VoIP users, increase the amount of reserved airtime. Type a value in microseconds.<br>By default, a device reserves 500 milliseconds of airtime per second for all VoIP calls. You can change the reserved airtime per second for VoIP from 100 to 1000 milliseconds per second. |
| Guaranteed Airtime for Roaming Clients | Set the percentage of airtime that a device reserves on the access interface for receiving VoIP calls from roaming clients. Type a value as a percentage (%).<br>By default, a device guarantees 20% of the reserved VoIP airtime for VoIP calls from roaming clients. You can change the percent of guaranteed airtime for roaming clients from 0% to 100%. Consider lowering the percent if VoIP users rarely roam, and raising the setting if roaming often occurs. Because VoIP traffic from a roaming client belongs to an existing session, the device to which the client roams always accepts it. If there is not enough airtime available in the guaranteed roaming reserve, the device deducts available airtime from the relevant user profile. |
| OS Detection | Enable devices to detect the OS of client devices based on a combination of DHCP option 55 contents and the contents of the HTTP headers. To enable, set the toggle to **ON**.<br>The following detection methods are available:<br>• **Use DHCP option 55 contents**: Select to use the DHCP option 55 parameter list.<br>• **Use HTTP user agent IDs**: Select to use the contents of the HTTP user agent ID within the HTTP headers.<br>• **Use both detection methods (DHCP=primary method, HTTP=secondary method)**: Select to use both the DHCP option 55 parameter list and the HTTP user agent information to identify the client operating system. When you select this option, devices first check the contents of the DHCP option 55 parameter list. If it finds no match, then the device examines the HTTP header for the HTTP user agent ID to determine the operating system. If no match is found in either pass, then ExtremeCloud IQ displays **unknown** as the client OS. |
| Disable Reset Button | Disable the reset button on the front panel of the chassis to prevent non-administrators from using it to reset the device to its default settings or to a bootstrap configuration. Select the check box. |

**Table 116: System Settings (continued)**

| Setting | Description |
|---|---|
| Disable Console Port | Disable the functionality of the console port on a device to block all administrative access through that port. Select the check box.<br>Disabling the console port on a device that is deployed in a publicly accessibly location is a good security precaution.<br><br>**Note:** If you disable the console port, all administrative access flows over the network, and can be affected by network connectivity issues. When a device configured to use only DHCP cannot get an IP address, you cannot log in to the device. |
| Enable Smart PoE | To enable Smart PoE, select the check box.<br>Smart PoE lets an AP230, AP320 or AP340 adjust power consumption automatically based on the current power supply. The AP230 and AP320 support PoE on the ETH0 interface. The AP340 supports PoE on both its ETH0 or ETH1 interfaces, and can simultaneously draw power through either one or both.<br>Using Smart PoE, an AP can detect if there are power injectors connected to one or both of its Ethernet ports and how many watts are available for each PoE channel. The AP uses this information to manage its internal use of power resources based on the currently available power level as follows:<br>• 20 W or higher: No adjustments are needed when the power level is 20 W or higher.<br>• 18 - 20 W: The device disables the ETH1 interface.<br>• 15 – 18 W: The device switches from 3x3 MIMO (Multiple In, Multiple Out) to 2x3.<br>• 13.6 - 15 W: In rare cases when the power drops between 13.6 and 15 W and further power conservation is necessary, the device reduces the speed on its active Ethernet interface from 10/100/1000 Mbps to 10/100 Mbps.<br>• 0 - 13.6 W: If there is a problem with the PoE switch or Ethernet cable and the power falls between 0 and 13.6 W, the device disables its wireless interfaces and returns its ETH0 and ETH1 interfaces to 10/100/1000 Mbps speeds.<br><br>**Note:** When using smart PoE, the maximum power consumption setting must be set to **No limitation** (the default). Manually setting the PoE maximum power consumption level to anything else overrides Smart PoE and essentially disables it. |
| Enable PCI Wireless Control Data Collection | Enable this feature to collect data about MAC DoS, IP DoS, and MAC filter violations in PCI compliance reports. Select the check box. |

**Table 116: System Settings (continued)**

| Setting | Description |
|---|---|
| Accept ICMP Redirect Message | Enable this feature to accept ICMP redirect messages from routers on their subnet. Select the check box.<br>Enable this feature to allow multiple routers on a subnet to update the device routing table. By default, devices reject ICMP redirects because redircted messages can be used to direct malicious traffic. Enable this feature with care. |
| Report client information gathered from captive web portals | Enable this feature to require devices to forward client information (such as name and email address) to ExtremeCloud IQ (New), where the information is logged as an event and in the syslog records. Select the check box. |
| Hostname in Beacon | Activate iBeacon for or APs that have internal iBeacon transmitters and that belong to a network policy. Slide the toggle to **ON**.<br>To use this setting, you must first define the iBeacon service in the associated network policy and then turn it on from the **Device Management** page. |

#### Authentication Settings Management Options

Authentication settings specify the database location for storing administrator accounts and control authentication for administrators.

**Table 117: Authentication Settings**

| Setting | Description |
|---|---|
| Extreme Networks Device Admin Authentication | Specify the location of the database storing administrator accounts with which the AP authenticates administrators when they log in. Choose one of the following options:<br>• **Local**—Stores admin accounts locally on the APs.<br>• **RADIUS**—Stores admin accounts remotely on RADIUS authentication servers.<br>• **Both**—Stores admin accounts both locally and remotely.<br>If one or more RADIUS servers are already in place, for convenience and security, you can keep all the accounts there and configure the AP to look up administrators on those servers.<br>**Note:** Be careful about using the RADIUS option. If all the AP admin accounts are on a RADIUS server and the device cannot connect to it, attempts by administrators to log in to the device fail.<br>If there is no central RADIUS server containing a user database, or if you prefer to keep the admin accounts locally on the AP, select **Local**. To use accounts located on an external RADIUS server and locally on the device, select **Both**. In this case, the device authenticates administrators by first checking accounts on the external RADIUS servers specified in the RADIUS profile, and then by checking accounts stored on the local database second. |
| Private PSK Server Auto-Save Interval | Type the length of time that a device acting as a private PSK server automatically saves its list of private PSK-to-client MAC address bindings to flash memory.<br>Depending on how frequently the server is binding private PSKs to client MAC addresses, you can make the interval as short as 60 seconds or as long as 3600 seconds (1 hour). |
| MAC Address Format | Define the **MAC Address Format**:<br>• **Delimiter**—Choose the type of delimiter: Colon (:), Dash (-), or Dot (.).<br>• **Style**—Choose **No delimiters**, **Two delimiters**, or **Five delimiters**.<br>• **Case Sensitivity**—Choose between **Lower Case** and **Upper Case**.<br>Some servers only accept MAC addresses in a particular format. These parameters control MAC authentication for local users on an Extreme Networks RADIUS server. For example, if you set case sensitivity as lower case and store local users with upper case MAC addresses for their user names and passwords, MAC authentication checks fail. |

**Table 117: Authentication Settings (continued)**

| Setting | Description |
|---|---|
| | By default, a device formats MAC addresses using lower case without any delimiter; for example: 0016cF8d55bc. You can reformat this address by making the following selections:<br>Colon, no delimiter, upper case: 0016CF8D55BC<br>Colon, two-delimiter, upper case: 0016:CF8D:55BC<br>Colon, five-delimiter, upper case: 00:16:CF:8D:55:BC<br>Dash, five-delimiter, upper case: 00-16-CF-8D-55-BC<br>Dot, five-delimiter, upper case: 00.16.CF.8D.55.BC |

Related Links

Configure Management Options on page 296

## Configure Traffic Filters Policy Settings

After you enable **Traffic Filter** in the network policy, you can reuse an existing Traffic Filter object, or configure the settings manually.

This task is part of the network policy configuration workflow. Use this task to configure **Traffic Filter** policy settings for a network policy.

1. Go to **Configuration** > **Network Policies**.
2. Select an existing network policy, and then select , or to add a new one, select ..
3. From the **Management Settings** menu, select **Traffic Filter**.
4. Toggle the **Traffic Filter** setting to **ON**, and configure the settings.
5. (Optional) To use an existing filter, select **Re-use Traffic Filter Settings**, , and then choose an existing filter.
6. Configure the Traffic Filter Settings on page 305.
7. Select **SAVE**.

Related Links

Traffic Filter Settings on page 305
Configure Policy Settings on page 279

*Traffic Filter Settings*

**Table 118: Settings for Traffic Filters**

| Setting | Description |
|---|---|
| Name | Type a **Name** for the new Traffic Filters object. |
| Description | Type a **Description** for the new Traffic Filters object. |
| **IQ Engine APs, Routers and Switches** | |

**Table 118: Settings for Traffic Filters (continued)**

| Setting | Description |
|---|---|
| Control the following types of traffic to devices | Select the corresponding check boxes to enable the selected types of traffic.<br>• **Enable SSH**: Permit an SSH connection to the mgt0 interface. By default, SSH is enabled.<br>• **Enable Telnet**: Permit a Telnet connection to the mgt0 interface. By default, Telnet traffic is disabled.<br>• **Enable Ping**: Permit ICMP echo requests (pings) to reach the mgt0 interface. By default, pinging mgt0 is allowed.<br>• **Enable SNMP**: Permit an SNMP connection to the mgt0 interface. By default, SNMP is disabled.<br>• **Enable Inter-station Traffic**: (Only for APs) Permit inter-station traffic between APs. |
| **Non-IQ Engine Switches (Dell & Extreme Networks)** | |
| Control the following types of traffic to devices | Select the corresponding check boxes to enable the selected types of traffic.<br>• **Enable Telnet**: Permit a Telnet connection to the mgt0 interface. By default, Telnet traffic is disabled.<br>• **Enable Ping**: Permit ICMP echo requests (pings) to reach the mgt0 interface. By default, pinging mgt0 is allowed.<br>Does not apply to N1100 series devices. |

Related Links

Configure Traffic Filters Policy Settings on page 305

## Configure MGT IP Filters

After you enable MGT IP Filter in the network policy, you can reuse an existing MGT IP Filter object, or configure the settings manually.

This task is part of the network policy configuration workflow. Use this task to configure **MGT IP Filter** policy settings for a network policy.

1. Go to **Configuration** > **Network Policies**.
2. Select an existing network policy, and then select , or to add a new one, select ..
3. From the **Management Settings** menu, select **MGT IP Filter**.
4. Toggle the **MGT IP Filter** setting to **ON**.
5. To use an existing filter, select **Re-use MGT IP Filter** and then select an existing filter.
6. Configure the MGT IP Filter Settings on page 307.
7. To add a new IP Object, select **Add Another IP Object**, configure the settings, and then select **SAVE SUBNET**.

   See MGT IP Filter Settings on page 307.
8. Select **SAVE MGT IP FILTER**.

Related Links

MGT IP Filter Settings on page 307

Configure Policy Settings on page 279

*MGT IP Filter Settings*

**Table 119: Settings for MGT IP Filters**

| Setting | Description |
|---|---|
| Name | Type a **Name** for the filter. |
| Description | (Optional)<br>Type a **Description** for the filter. Although optional, entering a description is helpful for troubleshooting and for identifying the filter. |
| **Permitted Management Traffic Source** | |
| Available IP Objects | IP objects in this list are preconfigured. To add to the list, select **ADD ANOTHER IP OBJECT**. See Table 120 on page 307.<br>Select an IP address in the **Available IP Objects** column, and then select the single arrow ( **›** ) to move it to the **Selected IP Objects** column.<br>Use the double arrow **››** to move all available IP addresses. |
| Selected IP Objects | IP objects in this list are the IP addresses from which administrators can access the devices.<br>Select an IP address in the **Selected IP Object** column, and then select the single arrow ( **›** ) to move it to the **Available IP Objects** column.<br>Use the double arrow **››** to move all available IP addresses. |

**Table 120: Settings for IP Objects**

| Setting | Description |
|---|---|
| Name | (Required)<br>Type a **Name** for the new IP object. |
| Subnet | (Required)<br>Type the new **IP Address** and **Subnet**. |

## Deploy a Network Policy

When you create a new network policy or make changes to an existing policy, the final step is to push the policy to the devices. ExtremeCloud IQ (New) pushes all configuration uploads as complete uploads. This action requires devices to reboot and activate the new configurations. Network policies can only be pushed to real devices (not simulated devices).

This task is part of the network policy configuration workflow. Use this task to deploy a network policy.

1. Go to **Configuration** > **Network Policies**.
2. Select an existing policy, and then select , or to add a new one, select .

3. After you configure the network policy, select the devices to which you want to upload the policy.
   - To automatically select the check boxes for all of the devices, select the check box in the top left of the table header.
   - To upload your network policy to specific devices only, select the corresponding check boxes for those devices.

     Use the **Assigned**, **Eligible**, and **Filtered** controls to customize your view of the devices that appear in the table.
4. Select **UPLOAD**.
5. In the **Device Update** window, select the type of update (**Delta** or **Complete**), whether to update IQ Engine and Extreme Networks switch images, and the activation times for the updated devices.

   **Note**
   The **Activation Time** option controls when the configuration is pushed to the device. When you select **Activate/reboot on this schedule**, both the configuration push and the device reboot are deferred until the scheduled date and time. For more information, see Configuration Push Scheduling Behavior on page 154.
6. Select **Enable Distributed Image Upgrade** when WAN speed and traffic usage are concerns.

   Select this option to revert the switch configuration if the device update causes a disconnect between the switch and ExtremeCloud IQ (New). The switch reboots and reverts to its previous configuration, which enables you to correct any configuration issues and perform a new device update.
7. Select **PERFORM UPDATE**.

   The device **Status** column in the device list updates to one of the following values:
   - **Pending**: The configuration has been pushed and is waiting for the device to reboot.
   - **Scheduled**: The configuration push is scheduled for a future date and time.
   - **Complete**: The configuration push and device reboot are complete.

## Configure the SSID for a Standard Wireless Network

A network policy can include one or more wireless networks, commonly referred to as SSIDs. A wireless network SSID is an alphanumeric string that identifies a wireless network, including the set of authentication and encryption services that wireless clients and access point devices use to communicate with each other over the network.

This task is part of the network policy configuration workflow. Use this task to configure an SSID for a standard wireless network.

1. Go to **Configuration** > **Network Policies**.
2. Select an existing network policy, and then select , or to add a new one, select .
3. Select **2 Wireless**.
4. (Optional) Select **Assign SSIDs using Classification Rules**.
   a. To add a classification rule, select .

b. To specify an existing classification rule, select .

For more information, see Configure Classification Rules on page 291

**Note**
If you have more than 16 SSIDs, the check box appears dimmed. To enable the check box, reduce the number of SSIDs to fewer than 16.

5. Select an existing SSID and then select , or to add a new one, select ..
6. Type a **Name** for the wireless network SSID.

   ExtremeCloud IQ (New) and IQ Engine use this name to group all the settings related to this wireless network, such as required and optional data rates, DoS policies, MAC filters, and the broadcast SSID.
7. Type a **Broadcast Name** for this wireless network, or accept the one automatically derived from the SSID name.

   Clients discover this broadcast name from beacons and probe responses.
8. Select SSID radio broadcast bands:
   - **Wi-Fi 0 Radio (2.4 GHz or 5 GHz)**: Broadcast the SSID based on the configuration of the Wi-Fi 0 radio.
   - **Wi-Fi 1 Radio (5 GHz only)**: Broadcast the SSID on the Wi-Fi 1 radio operating in the 5 GHz band. Most Extreme Networks devices have two radios: radio 1 is bound to Wi-Fi 0 and radio 2 is bound to Wi-Fi 1. Radio 1 generally operates in the 2.4 GHz band but can also operate in the 5 GHz band on some models. Radio 2 operates in the 5 GHz band.

     **Note**
     Mapping an SSID to both radio types is a good approach if the devices need to work with some wireless clients that only support 802.11n/b/g, and others that only support 802.11ac/n/a/ac/x. In this case, both Wi-Fi 0 and Wi-Fi 1 must be in access mode or dual mode. If hive members need to support wireless backhaul communications with each other and you want both interfaces to provide client access, then one of the wireless interfaces must be able to provide both access and backhaul links.

   - **Wi-Fi 2 Radio (6 GHz only)**: This option currently supports only Enterprise WPA3, Personal WPA3, and Open Enhanced. After you select this check box, a message reminds you that WiFi2 supports only 6Ghz band for client access. The configuration menu shows only options applicable to 6Ghz.

9. Select an authentication method and configure the settings.

**Table 121: Authentication methods**

| Method | Configuration |
|---|---|
| SSID Authentication | • Select **Enterprise WPA/WPA2/WPA3** to require users to authenticate by using a certificate or entering a username and password, and validating against a RADIUS server. Only WPA3 is supported for 6 GHz devices. See Configure Enterprise SSID Authentication on page 319.<br>• Select **Personal WPA/WPA2/WPA3** to require users to enter a shared passphrase to authenticate. Only Personal WPA3 is supported for 6 GHz devices. See Configure Personal SSID Authentication on page 321.<br>• Select **Private Pre-Shared Key** to allow the use of multiple passphrases on a single SSID. See Configure Private Pre-Shared Key SSID Authentication on page 326.<br>• Select **Open** (not available for 6 GHz) so users do not use any form of authentication, but can be directed to a captive web portal before they can access other network resources.<br><br>To create a captive web portal for open authentication, see:<br>◦ Customize and Preview Cloud-based Captive Portal Settings on page 338<br>◦ Customize and Preview Device-based Captive Web Portal Settings on page 331<br>◦ Import Captive Web Portal HTML Files on page 339<br>• Select **Enhanced Open** (available only for 6 GHz devices) to provide improved data privacy in open Wi-Fi networks, such as Wifi hotspots and guest WLANs.<br><br>**Note:** For security reasons, WEP configuration is no longer available in the UI. If you require WEP for business continuity purposes, you can enable it via Supplemental CLI. |
| MAC Authentication | See Configure MAC Authentication on page 318. |

Continue configuring the network policy.

Related Links

Configure Classification Rules on page 291
Configure Enterprise SSID Authentication on page 319
Configure Personal SSID Authentication on page 321
Configure Private Pre-Shared Key SSID Authentication on page 326
Customize and Preview Cloud-based Captive Portal Settings on page 338
Customize and Preview Device-based Captive Web Portal Settings on page 331
Import Captive Web Portal HTML Files on page 339
Configure MAC Authentication on page 318

## Cloud User Group Settings

When you configure a user group for an Enterprise 802.1X SSID, the password database always resides in the cloud. For a user group for a Private Pre-Shared Key (PPSK) SSID, the password database can reside in the cloud or on all SSID APs. The following settings are available when you configure a cloud-based user group.

**Table 122: Settings for Cloud User Groups**

| Setting | Description |
|---|---|
| User Group Name | Type a name for the user group. |
| Password DB Location | Select **Cloud** for a cloud-resident password database. |
| Password Type | Select **PPSK** or **RADIUS**. |
| Description | Type an optional **Description** for the user group. |
| Enable CWP Register | Select **Enable CWP Register** to require users in this user group to log in using a captive web portal.<br>Available only if a captive web portal is enabled for this SSID. |
| PCG Use | (Optional) Available only for the PPSK password type.<br>Select **Enable use for Private Client Group**. |
| **Password Settings** | |
| Generate Password Using | (Required)<br>Select any combination of characters that you want to include in the password: **Letters**, **Numbers**, and **Special Characters**. |
| Enforce the use of | Select one of the password enforcement options from the menu:<br>• **All selected character types**<br>• **Any selected character types**<br>• **Only one character type** |
| PSK Generation Method | Available only for the PPSK password type.<br>Select **Password Only** or **User String Password** from the menu. With the **User String Password** option, you can include the user name and a string of characters in front of the generated Private PSKs.<br>If the password generation method is **Password Only**, then the PPSK password can be between eight and 63 characters. If the generation method is **User + String + Password**, the maximum passphrase for the Private PSK can be between eight and 31 characters. |
| Generated Password Length | Select the length for automatically-generated passwords for this user group. Range: 8–63 |
| Concatenating String | Available only for the **User String Password** PSK Generation Method. Range: 0–8<br>Use this string to generate PPSKs as User name + Character String + Password. For example, if you enter `Extreme`, as the string, then the generated PPSKs are **<User name>Extreme<Password>**. |
| **Expiration Settings** | |

**Table 122: Settings for Cloud User Groups (continued)**

| Setting | Description |
|---|---|
| Account Expiration | Select one of the options from the menu:<br>• **Never Expire**<br>• **Valid During Dates**<br>Use the calendar and time controls to specify the **Start** and **End** dates and times.<br>• **Valid For Time Period**<br>Specify the time period for which the password is valid after **ID Creation** or **First Login**. Type the number of **hours**, **days**, or **weeks**. Select the unit of time and the **after**-condition from the menus.<br>Optionally, select **Renew user credentials**. To delete credentials after a specific time period, select **Delete credentials after**, type a value, and then select the unit of time from the menu.<br>• **Daily**<br>Use the **Start** and **End** controls to specify the daily time period. |
| Action at Expiration | Not available for accounts set to never expire.<br>Select **Access Rejected** to have ExtremeCloud IQ (New) block users from renewing their credentials.<br>Select **Show Expiration Message** to have ExtremeCloud IQ (New) present to users an on-screen prompt that they can use to renew their credentials. |
| **Delivery Settings** | |
| Deliver Access Key by | Select the methods for delivery of the access key. Select one or both:<br>• **Text Messages (SMS)**<br>• **Email**<br>Use the menus to select an email template for each method. |

Related Links

Configure the SSID for a Standard Wireless Network on page 308

## Local User Group Settings

When you configure a user group for an Enterprise 802.1X SSID, the password database always resides in the cloud. For a user group for a Private Pre-Shared Key (PPSK) SSID, the password

database can reside in the cloud or locally on all APs that connect to the SSID. The following settings are available when you configure a cloud-based user group.

**Table 123: Settings for Local User Groups**

| Setting | Description |
|---|---|
| User Group Name | Type a name for the user group. |
| Password DB Location | Select **Local** to store login credentials on all APs using this SSID. You must select **Local** to create a private client group in this user group.<br>See Classification Rules Overview. |
| Password Type | Select **PPSK** or **RADIUS**. |
| Description | Type an optional **Description** for the user group. |
| Set the maximum number of clients per private PSK | (Optional) Available only for the PPSK password type.<br>Select **Set the maximum number of clients per private PSK** to set per-user PPSK limits for different users in the same wireless network (SSID). Because you can set per-user PPSK limits for different users in the same SSID, you no longer need to configure an SSID for each user group (for instance, with three devices per employee). You can set multiple per-user PPSK limits can be set in the same (SSID).<br>Range: 0-15, 0 = no limit |
| PCG Use | (Optional) Available only for the PPSK password type.<br>Select **Enable use for Private Client Group**. |
| PPSK Classification Use | (Optional) Available only for the PPSK password type.<br>Select **Enable user for PPSK Classification only** to create a single SSID and distribute unique guest passwords for each location.<br>Use this option with a **Private Pre-Shared Key** SSID Authentication network policy. See Configure Private Pre-Shared Key SSID Authentication on page 326 for more information. |
| **Password Settings** | |
| Generate Password Using | (Required)<br>Select any combination of characters that you want to include in the password: **Letters**, **Numbers**, and **Special Characters**. |
| Enforce the use of | Select one of the password enforcement options from the menu:<br>• **All selected character types**<br>• **Any selected character types**<br>• **Only one character type** |

**Table 123: Settings for Local User Groups (continued)**

| Setting | Description |
|---|---|
| PSK Generation Method | Available only for the PPSK password type.<br>Select **Password Only** or **User String Password** from the menu. With the **User String Password** option, you can include the user name and a string of characters in front of the generated Private PSKs.<br>If the password generation method is **Password Only**, then the PPSK password can be between eight and 63 characters. If the generation method is **User + String + Password**, the maximum passphrase for the Private PSK can be between eight and 31 characters. |
| Generated Password Length | Select the length for automatically-generated passwords for this user group. Range: 8–63 |
| Concatenating String | Available only for the **User String Password** PSK Generation Method. Range: 0–8<br>Use this string to generate PPSKs as User name + Character String + Password. For example, if you enter `Extreme`, as the string, then the generated PPSKs are **<User name>Extreme<Password>**. |
| **Expiration Settings** | |
| Require Authentication After | To force re-authentication after a session is inactive for some time, select **Require Authentication After** and enter a time in the minutes field. |
| Account Expiration | Select an option from the menu:<br>• **Never Expire**<br>• **Valid During Dates** (Available only for PPSK.)<br>Use the calendar and time controls to specify the **Start** and **End** dates and times. |
| Action at Expiration | Not available for accounts set to never expire.<br>Select **Access Rejected** to have ExtremeCloud IQ (New) block users from renewing their credentials.<br>Select **Show Expiration Message** to have ExtremeCloud IQ (New) present to users an on-screen prompt that they can use to renew their credentials. |
| **Delivery Settings** | |
| Deliver Access Key by | Select the methods for delivery of the access key. Select one or both:<br>• **Text Messages (SMS)**<br>• **Email**<br>Use the menus to select an email template for each method. |

Related Links

Configure the SSID for a Standard Wireless Network on page 308

## Add a User Profile

Configure an SSID for a standard wireless network. See Configure the SSID for a Standard Wireless Network on page 308.

User profiles define user traffic settings on APs. After a user associates with a device, the device assigns the user to a user profile. The device can make this assignment dynamically from attributes returned by a RADIUS authentication server or statically by using the default user profile set.

This task is part of the SSID configuration workflow. Use this task to add a user profile for an SSID, as part of a network policy.

1. While configuring an SSID, go to **User Access Settings** > **Default User Profile**.
2. To add a new user profile, select  and configure the settings.
3. Select **Save User Profile**.

Related Links

User Profile Settings on page 315
Configure the SSID for a Standard Wireless Network on page 308

*User Profile Settings*

Configure the following settings for user profiles.

**Table 124: User profile settings**

| Setting | Description |
|---|---|
| User Profile Name | Type a **User Profile Name**. |
| Connect to | 1. Select **VLAN** or **VLAN Group**.<br>2. To select an existing VLAN or VLAN group, select  and choose an existing object, or to add a new one, select .<br>Typically, the default VLAN is 1.<br>**Note:** The user profile **default-profile** cannot be edited directly. If this profile is assigned to your wireless network, you must either select a different profile or create a new one to configure the settings.<br>For more information, see VLAN Object Settings on page 363 and VLAN Group Object Settings on page 363.<br>To edit an existing VLAN object, select it and then select . |
| SECURITY | See Configure User Profile Security on page 363. |
| TRAFFIC TUNNELING | See Configure User Profile Traffic Tunneling on page 367. |
| QOS | See Configure User Profile QoS on page 371. |
| AVAILABILITY SCHEDULE | See Configure an Availability Schedule on page 373. |

**Table 124: User profile settings (continued)**

| Setting | Description |
|---|---|
| CLIENT SLA | See Configure User Profile Client SLA on page 375. |
| DATA/TIME LIMIT | See Configure User Profile Access Restrictions on page 375. |

Related Links

Add a User Profile on page 315
Configure User Profiles on page 495
Configure VLAN Settings on page 362

## SSIDs

An SSID is an alphanumeric string that identifies a wireless or guest network. For information about adding wireless networks, see Configure the SSID for a Standard Wireless Network on page 308.

To view the list of configured SSIDs, go to Go to **Configuration** > **Network Policies**, choose an existing network policy, and then select **2 Wireless**.

The SSID table displays the following information about your network SSIDs:

- **SSID Name**: The name assigned to an SSID when it was created. This is the name that APs advertise in beacons (unless the SSID is in stealth mode) and respond to during client probes.
- **SSID Broadcast Name**: This name can be the same as the SSID Name.
- **Access Security**: The method that the SSID uses to secure network access.
- **VLAN**: The VLAN to which this SSID is assigned.
- **Default User Profile**: The user profile that is assigned to this SSID.
- **Used By**: Displays the number of APs and network policies that use this SSID. Hover over any non-zero number to see details.

Related Links

Configure the SSID for a Standard Wireless Network on page 308

## SSID Usage in Standard Wireless Networks

As part of configuring a standard wireless network, you must determine how authentication takes place. You can choose SSID authentication or MAC authentication. MAC Authentication is typically used to support legacy clients.

**Note**
Client mode radios use only PSK or Open SSID authentication.

*SSID Authentication*

SSID Authentication offers the following types of access security methods:

- **Enterprise WPA/WPA2/WPA3** requires users to authenticate by entering a user name and password, validated against a RADIUS server. Only WPA3 is supported for 6 GHz devices. See Configure Enterprise SSID Authentication on page 319.
- **Personal WPA/WPA2/WPA3** requires users to enter a shared PPSK to authenticate. Only Personal WPA3 is supported for 6 GHz devices. See Configure Personal SSID Authentication on page 321.
- **Private Pre-Shared Key** requires users to authenticate by entering a PPSK unique to each user (not available for 6 GHz). See Configure Private Pre-Shared Key SSID Authentication on page 326.
- **OPEN** (not available for 6 GHz) or **Enhanced Open** does not require users to use any form of authentication, but can direct them to a captive web portal before they can access other network resources. **Enhanced Open** is available only for 6 GHz devices.

*MAC Authentication*

In Extreme Networks, MAC authentication works by checking a client MAC address against a RADIUS server. The RADIUS server, or an external database with which the RADIUS server communicates, must have an entry with the client MAC address as both user name and password. If the client MAC address matches the entry, it is authenticated, and the AP allows it to access the network as determined by the user profile.

MAC authentication can provide an additional or sole means of authentication. If an SSID employs MAC authentication with another type of access control—PPSK or a captive web portal—MAC authentication occurs first. If it is successful, the AP continues with the rest of the authentication procedure. Otherwise, the authentication process stops, the AP denies network access to the client, and the AP disassociates the client. If you enable MAC authentication and use an open SSID, then MAC authentication becomes the sole means of access control. See Configure MAC Authentication on page 318.

Related Links

Configure the SSID for a Standard Wireless Network on page 308

*Configure Private Client Group Options*

First, Configure Private Pre-Shared Key SSID Authentication on page 326.

This task is part of the network policy configuration workflow. Use this task to to configure the options for Private Client Groups.

1. On the **2 Wireless** page for the policy, under **SSID Usage**, select **Private Pre-Shared Key**.
2. Select **Private Group Options**.
3. Select **AP-Based** or **Key-Based**.

   **AP-Based** PCG mode requires a unique user and shared keys. This mode supports common shared devices within personal network spaces. It also requires room assignments for AP anchoring and traffic tunneling.

   **Key-Based** PCG requires one password used by the entire device group. Key-based PCG does not require room assignments for AP anchoring and traffic tunneling.

4. If you selected **Key-Based**, select the following **Private Client Groups Traffic Filtering** options as required.
   - **Enable Broadcast Filtering**: When selected, broadcast frames are not propagated beyond the current PCG domain.
   - **Enable Multicast Filtering**: When selected, multicast frames are not propagated beyond the current PCG domain.
     - **Enable MDNS** (multicast DNS) Filtering—When applied, multicast DNS frames are not forwarded outside the PCG domain.
     - **Enable SSDP** (Simple Service Discovery Protocol)—When enabled, SSDP frames are not forwarded outside of the PCG domain.

   When you select **Multicast Filtering**, both mDNS and SSDP filtering are auto-selected. If you do not select **Multicast Filtering**, you can independently select mDNS and SSDP filtering. This capability depends solely on site requirements.

Related Links

Configure Private Pre-Shared Key SSID Authentication on page 326
Configure the SSID for a Standard Wireless Network on page 308

*Configure MAC Authentication*

Create a standard wireless network (SSID).

MAC authentication checks a client MAC address against a RADIUS server, and can provide an additional, or sole means of authentication. If an SSID employs MAC authentication with another type of access control, such as PPSK, PSK, or a captive web portal, MAC authentication occurs first. If it is successful, the AP continues the authentication procedure. Otherwise, the authentication process stops, the AP denies network access to the client, and the AP disassociates the client. If you enable MAC authentication and use an OPEN SSID, then MAC authentication becomes the sole means of access control.

This task is part of creating or editing a network policy. Use this task to configure an MAC authentication as part of a network policy, or if you are configuring an AP template object.

1. Go to Go to **Configuration** > **Network Policies**.
2. Select **MAC Authentication**, and then toggle the setting to **On**.
3. Select an **Authentication Protocol** to determine how the AP forwards authentication requests from users to an external RADIUS or Active Directory server:

   **PAP**: The AP sends an unencrypted password to the RADIUS server.

   **Note**
   When **Authentication with ExtremeCloud Universal ZTNA** is enabled in the SSID authentication settings, PAP is the only option. For more information, see Configure the SSID for a Standard Wireless Network on page 308.

   **CHAP or MS CHAP V2**: The AP sends the result of an operation it performs on the password, instead of the password itself, to the RADIUS or Active Directory authentication server. The authentication server performs the same operation, and then compares the results to see if they match.

4. Select , and choose an existing RADIUS Server Group, or to add a new one, select .
   For more information, see Configure an AAA Server Profile on page 355

Continue configuring a standard wireless network.

Related Links

Configure an AAA Server Profile on page 355

*Configure Enterprise SSID Authentication*

First, create a standard wireless network policy. For more information, see Configure the SSID for a Standard Wireless Network on page 308.

This task is part of the network policy configuration workflow. Use this task to configure the **SSID AUTHENTICATION** options for Enterprise SSID authentication.

1. On the **2 Wireless** page for the policy, select to add a new one.
   Alternatively, select an existing Enterprise SSID to edit.
2. Under **SSID Usage** > **SSID Authentication**, select **Enterprise**.
   This option requires users to authenticate by entering a user name and password, which the system checks against a RADIUS authentication server.
3. (Optional) Enable Hotspot 2.0 support.
   IQ Engine v10.7.4 is required. For more information, see Configure a Hotspot on page 341.
4. Select the required **Key Management** from the menu, or keep the default value.
   **Key Management** options:
   - **WPA3-802.1X** uses 128-bit encryption and automatically enables 802.11w Protected Management Frames, found in the **Advanced Access Security Settings** section of the Wireless Network configuration. If all wireless clients support WPA3, it is a better choice than WPA2.
   - **WPA3-802.1X (192-bit)** uses GCMP256 encryption, offering stronger protection than standard WPA2 or WPA3-Enterprise (128-bit). Requires IQ Engine version 10.8r5, or higher.

     **Note**
     Selecting WPA3-802.1X (1920bit) automatically selects GCMP256 encryption.

   - **WPA2-802.1X** supports PMK caching and preauthentication (WPA does not). If the wireless clients support WPA2, it is the better choice over WPA. If you have a lot of legacy clients connecting to the network, WPA2 is a good choice.
   - **WPA-802.1X** does not support PMK caching or preauthentication. However, if you know that all the clients that are going to use this SSID were released before IEEE 802.11i was ratified in 2004 and only support WPA (not WPA2), this option allows the Extreme Networks devices to support them.
5. For an Enterprise or Personal SSID, configure the **Protected Management Frames** settings.

   **Note**
   Available settings depend on the **Key Management** selection (WPA, WPA2, or WPA3).

**Table 125: Protected Management Frames Settings**

| Setting | Description |
|---|---|
| 802.11w | Toggle **802.11w** to **ON** to prevent forgery and retransmission of management frames. |
| Use of 802.11w is | If you select a WPA3 level of security, 802.11w is enabled by default at a Mandatory level. The menu and check box appear dimmed. If you select a WPA3 level of security with Transition Mode enabled, 802.11w will be enabled as Optional.<br>If you select WPA2 level of security, 802.11w is disabled by default, with option to enable. |
| Use 802.11w protection for broadcasts/ multicasts | |
| Enable Beacon Protection | Enhances Wi-Fi security by safeguarding beacon frames against tampering.<br>**Note: Enable Beacon Protection** is supported on AP4020/AP5020 only. |

6. Select an **Encryption Method**:
   - **CCMP (AES)**: Counter Mode-Cipher Block Chaining Message Authentication Code Protocol (CCMP) uses AES (Advanced Encryption Standard) encryption. CCMP provides message integrity by combining counter mode with CBC (cipher block chaining) to produce a MAC (message authentication code).
   - **GCMP256**: Galois/Counter Mode Protocol with 256-bit keys is an advanced encryption algorithm that uses 256-bit AES-GCMP encryption. GCMP256 offers stronger encryption and better performance in high-security wireless networks, particularly in WPA3-Enterprise (192-bit mode). GCMP256 provides message integrity by using a GMAC (Galois Message Authentication Code).
7. Toggle **Transition Mode if Applicable** on.

   802.11w settings might have been changed. See Customize Advanced Access Security Controls on page 377 to confirm.

   **Important**
   Transmission mode with Auto Protected Frame Management across all radios (including 6 GHz) requires IQ Engine 10.7.3. If you push the Auto setting to an AP with IQ Engine below 10.7.3, the AP defaults to the best available 802.11w setting available, and Protected Management Frames is set to **Mandatory**.

   For more information, see Transition Mode Overview on page 325.
8. To enable Multi-Link Operation (MLO), turn on **Enable MLO**. See Settings for Multi-Link Operation on page 388.
9. To create a captive web portal, select **Enable Captive Web Portal**.
10. To enable authentication using user groups, select **Authentication with ExtremeCloud IQ Authentication Service**.

11. If you intend to authenticate via RADIUS servers, either select an existing **Default RADIUS Server Group** from the current list or select the plus sign to add a new group.

    See Configure RADIUS Server Settings on page 350 to add a wireless network (SSID)-specific RADIUS object. See Configure an External RADIUS Server on page 352 to add an external RADIUS common object.

    To use classification, select **Apply RADIUS server groups to devices via classification**.
12. Select an existing user group from the list, or select  and configure the settings.

    See Cloud User Group Settings on page 311 and Local User Group Settings on page 312.
13. Use the existing **Default User Profile**, select a profile from the list, or select  and configure the settings..

    See Add a User Profile on page 315.
14. (Optional) Under **User Access Settings**, select the **Apply a different user profile to various clients and user groups** check box.

    See Apply Different User Profiles to Clients and User Groups on page 376.
15. To customize the **SSID Availability Schedule**, select the **Restrict the availability of this SSID to selected schedules** check box to enable SSID schedules.
16. Select **Customize**.

    To create a new schedule, select , and see Schedule Settings on page 374.
17. To customize **Advanced Access Security Controls**, see Customize Advanced Access Security Controls on page 377.
18. To customize **Optional Settings** (not available for 6 GHz), see Customize Wireless Network Optional Settings on page 379.
19. Toggle **Client Monitor ON** (default) to enable devices to detect client issues and report client connection activities and problems to ExtremeCloud IQ (New).
20. Select **SAVE**.

Related Links

Settings for Multi-Link Operation on page 388

Configure RADIUS Server Settings on page 350
Configure an External RADIUS Server on page 352
Cloud User Group Settings on page 311
Local User Group Settings on page 312
Apply Different User Profiles to Clients and User Groups on page 376
Schedule Settings on page 374
Customize Advanced Access Security Controls on page 377
Customize Wireless Network Optional Settings on page 379
Configure the SSID for a Standard Wireless Network on page 308

*Configure Personal SSID Authentication*

First, create a standard wireless network policy. For more information, see Configure the SSID for a Standard Wireless Network on page 308.

This task is part of the network policy configuration workflow. Use this task to configure the **SSID AUTHENTICATION** options for Personal SSID authentication.

1. On the **2 Wireless** page for the policy, select **Personal** SSID Authentication.

   This option requires all users to authenticate by entering the same pre-shared key.
2. Choose one of the following **Key Management** options:
   - Select **WPA3 (SAE)** to negotiate using WPA3 with clients. If all the wireless clients support WPA3, it is a better choice than WPA2.
   - Select **WPA2-(WPA2 Personal)-PSK** to use WPA2 for key management.
   - Select **WPA-PSK** to use WPA for key management. WPA does not support PMK caching or pre-authentication, but if the clients were released before IEEE 802.11i was ratified and they support WPA (not WPA2), this option allows the Extreme Networks devices to support them.

   **Note**
   For more information, see Transition Mode Overview on page 325.
3. For an Enterprise or Personal SSID, configure the **Protected Management Frames** settings.

   **Note**
   Available settings depend on the **Key Management** selection (WPA, WPA2, or WPA3).

**Table 126: Protected Management Frames Settings**

| Setting | Description |
|---|---|
| 802.11w | Toggle **802.11w** to **ON** to prevent forgery and retransmission of management frames. |
| Use of 802.11w is | If you select a WPA3 level of security, 802.11w is enabled by default at a Mandatory level. The menu and check box appear dimmed. If you select a WPA3 level of security with Transition Mode enabled, 802.11w will be enabled as Optional.<br>If you select WPA2 level of security, 802.11w is disabled by default, with option to enable. |
| Use 802.11w protection for broadcasts/ multicasts | |
| Enable Beacon Protection | Enhances Wi-Fi security by safeguarding beacon frames against tampering.<br>**Note: Enable Beacon Protection** is supported on AP4020/AP5020 only. |

4. Choose one of the following **Method** options:
   - **HNP/H2E** (default): Enable both Hunting and Pecking (HNP) and Hash to Element (H2E).
   - **H2E**: Set the H2E method as the privacy method for the WLAN on all radios (2.4 GHz, 5 GHz and 6 GHz). This option applies only to 6E capable devices (AP4000, AP5010, AP5020, AP5050, AP3000, and 11ax portfolio).

     **Note**
     Ensure that networks defined with the option **H2E** are assigned to configuration Profiles of supported devices (AP4000, AP5010, AP5020, AP5050, AP3000, and 11ax portfolio).

   - **HNP**: Set the HNP method as the privacy method for the WLAN on all radios (2.4 GHz, 5 GHz and 6 GHz).
   - Select the **Enable AKM-24 (WiFi 7 Only)** check box to ensure compatibility and compliance with 802.11be.

     **Note**
     Applies only to AP4020, AP4060, and AP5020 devices.

5. Select an **Encryption Method**.

   Encryption methods for WPA3 and WPA2 include:
   - **CCMP (AES)**: Counter Mode-Cipher Block Chaining Message Authentication Code Protocol (CCMP) uses AES (Advanced Encryption Standard) encryption. CCMP provides message integrity by combining counter mode with CBC (cipher block chaining) to produce a MAC (message authentication code).
   - **CCMP (AES)/GCMP256**: Supports both encryption protocols. Allows the network to dynamically select the strongest encryption method supported by the client. This ensures maximum compatibility while offering strong security. Ideal for mixed environments with both legacy and modern devices.
   - **GCMP256**: Galois/Counter Mode Protocol with 256-bit keys is an advanced encryption algorithm that uses 256-bit AES-GCMP encryption. GCMP256 offers stronger encryption and better performance in high-security wireless networks, particularly in WPA3-Enterprise (192-bit mode). GCMP256 provides message integrity by using a GMAC (Galois Message Authentication Code).

   The **Encryption Method** for WPA-PSK is **TKIP**. Temporal Key Integrity Protocol (TKIP), uses RC4 as its cipher and provides a rekeying mechanism. TKIP ensures that every data packet is sent with a unique encryption key, which is a combination of an Interim Key/Temporal Key and a Packet Sequence Counter. TKIP provides more secure encryption than Wired Equivalent Privacy (WEP), and works on older or legacy WEP hardware with minor upgrades.

   **Note**
   ExtremeCloud IQ (New) supports TKIP only for AP3000, AP3000X, AP4000, AP5010, AP5050D, AP5050U models.

6. Select an **SAE Group**.

7. Toggle **Transition Mode if Applicable** on.

   **Note**
   When enabled with 6 GHz: PMF is optional for 2.4 GHz and 5 GHz, but mandatory for 6 GHz. Requires IQ Engine version 10.8r4 or higher.

   For more information, see Transition Mode Overview on page 325.
8. For **Key Value**, enter the pre-shared key and **Confirm** it.

   The **Key Type** is **ASCII Key**.
9. (Optional) To show the **Key Value**, select **Show Password**.
10. To enable Multi-Link Operation (MLO), turn on **Enable MLO**.

    See Settings for Multi-Link Operation on page 388.
11. To create a captive web portal, select **Enable Captive Web Portal**.
12. Use the existing **Default User Profile**, select a profile from the list, or select  and configure the settings..

    See Add a User Profile on page 315.
13. (Optional) Under **User Access Settings**, select the **Apply a different user profile to various clients and user groups** check box.

    See Apply Different User Profiles to Clients and User Groups on page 376.
14. To customize the **SSID Availability Schedule**, select the **Restrict the availability of this SSID to selected schedules** check box to enable SSID schedules.
15. Select **Customize**.

    To create a new schedule, select , and see Schedule Settings on page 374.
16. To customize **Advanced Access Security Controls**, see Customize Advanced Access Security Controls on page 377.
17. To customize **Optional Settings** (not available for 6 GHz), see Customize Wireless Network Optional Settings on page 379.
18. Toggle **Client Monitor ON** (default) to enable devices to detect client issues and report client connection activities and problems to ExtremeCloud IQ (New).
19. Select **SAVE**.

Related Links

Settings for Multi-Link Operation on page 388

Apply Different User Profiles to Clients and User Groups on page 376
Schedule Settings on page 374
Customize Advanced Access Security Controls on page 377
Customize Wireless Network Optional Settings on page 379
Configure the SSID for a Standard Wireless Network on page 308

*Transition Mode Overview*

Transition Mode eases the transition from WPA2 to WPA3 Wi-Fi security by connecting newer client hardware with the latest security standards, and permitting legacy client devices to access the same SSID using older standards.

**Important**
Transmission mode with Auto Protected Frame Management across all radios (including 6 GHz) requires IQ Engine 10.7.3. If you push the Auto setting to an AP with IQ Engine below 10.7.3, the AP defaults to the best 802.11w setting available, and Protected Management Frames is set to **Mandatory**.

There are three distinct types of transition modes, each functioning in its own unique way:

- **Open to Enhanced Open (OWE)**: Supports both OWE and open standards. Newer devices can connect using OWE, while older client devices can connect without encryption. This is provided through two distinct SSIDs: a visible open network and a similarly-named hidden OWE network. All clients attempt to join the visible open network, but clients that support OWE receive an an information element in the open network SSID probe response to join the hidden OWE network instead.
- **WPA2/WPA3 Personal** (PSK to SAE): Supports both WPA2 and WPA3 on a single passphrase protected SSID. Devices supporting WPA3 can connect using WPA3 with SAE, while older devices can still connect using WPA2 with PSK. 802.11w (Protected Frame Management, or PMF) is set to optional on these SSIDs, enabling newer clients to use Protected Frames, while older clients do not.
- **WPA2/WPA3 Enterprise**: Supports both WPA2-Enterprise and WPA3-Enterprise on the same SSID. While all clients use the same backwards-compatible encryption (AES 128), 802.11w is set to Optional on these SSIDs. Newer clients use PMF, while older clients do not.

Transition Mode is only supported on the legacy radio bands (2.4 and 5 GHz), while 6 GHz networks are required to use the newer security standards. To simplify the adoption and use of the same SSIDs across all radios, ExtremeCloud IQ intelligently applies PMF settings on an SSID within an Enterprise network, based on the selected security and radio settings.

**Table 127: Transition Mode Security and Radio Settings**

| | Transition Mode | 2.4/5 GHz Enabled | 6 GHz Enabled | 802.11w Setting |
|---|---|---|---|---|
| WPA2-Enterprise | N/A | Yes | N/A | Off |
| WPA3-Enterprise | No | Yes | No | Mandatory |
| WPA3-Enterprise | Yes | Yes | No | Optional |
| WPA3-Enterprise | No | Yes | Yes | Mandatory |
| WPA3-Enterprise | Yes | Yes | Yes | Auto* |

**Note**
*Auto 802.11w requires IQ Engine 10.7.3 or newer.

Related Links

Configure the SSID for a Standard Wireless Network on page 308
Configure Enterprise SSID Authentication on page 319
Configure Personal SSID Authentication on page 321

*Configure Private Pre-Shared Key SSID Authentication*

First, create a standard wireless network policy. For more information, see Configure the SSID for a Standard Wireless Network on page 308.

A PPSK is a unique pre-shared key assigned to a user rather than to an SSID. With this approach, you can assign different PPSKs and user profiles to different users on the same SSID. If a user is no longer permitted to use the WLAN or a wireless client becomes lost, stolen, or compromised, you can revoke just that user's PPSK without having to reconfigure the PPSKs on all the other clients.



**Note**
ExtremeCloud IQ Connect does not support Private Pre-Shared Keys.

This task is part of the network policy configuration workflow. Use this task to configure Private Pre-Shared Key SSID authentication options.

1. On the **2 Wireless** page for the policy, under **SSID Usage**, select **Private Pre-Shared Key**.

   Private Pre-Shared Key SSID authentication uses WPA2-(WPA2 Personal)-PSK for **Key Management**.

   The **Encryption Method** for WPA2-(WPA2 Personal)-PSK is **CCMP (AES)**. Counter Mode-Cipher Block Chaining Message Authentication Code Protocol (CCMP) uses AES (Advanced Encryption Standard) encryption. CCMP provides message integrity by combining counter mode with CBC (cipher block chaining) to produce a MAC (message authentication code).
2. Select **Set the maximum number of clients per private PSK**, and then type the maximum number of simultaneous clients allowed for each PPSK user. (Range: 1 through 15, or type 0 for an unlimited number.)

   **Note**
   Setting the maximum number of clients per PPSK in the user group to a custom (non-zero) value overrides this setting in the SSID.

3. Select **MAC binding**, and then select an Extreme Networks AP from the menu to define it as a PPSK server.

   When you enable this option, an Extreme Networks AP functions as a PPSK server and automatically binds MAC addresses to PPSKs. When the first client authenticates with a PPSK, the PPSK server creates an internal MAC address-to-PPSK binding list for it. If a second client authenticates with the same PPSK, the server automatically binds its MAC address to the PPSK and adds it to the list—if allowed by the configuration. You can configure a PPSK server to bind up to five MAC addresses to one PPSK so users can submit the same PPSK for all their smart phones, tablets, PCs, and other clients.

   **Note**
   Only APs that you previously configured with static network settings appear in the PPSK server list.

   A PPSK server stores PPSK users, binds multiple client MAC addresses to a PPSK, and automatically updates and tracks PPSK-to-MAC address bindings. The AP must be at the site location defined in the network policy. Extreme Networks APs (PPSK authenticators) at the same site contact this server when checking and requesting a user-submitted PPSK binding to the client MAC address.

4. To configure **Private Client Group Options**, see Configure Private Client Group Options on page 317.
5. Select **PPSK Classification Options** to use this network policy with associated local user groups.
6. To create a captive web portal, select **Enable Captive Web Portal**.
7. Select an existing user group from the list, or select + and configure the settings.

   See Cloud User Group Settings on page 311 and Local User Group Settings on page 312.
8. Use the existing **Default User Profile**, select a profile from the list, or select + and configure the settings..

   See Add a User Profile on page 315.
9. (Optional) Under **User Access Settings**, select the **Apply a different user profile to various clients and user groups** check box.

   See Apply Different User Profiles to Clients and User Groups on page 376.
10. To customize the **SSID Availability Schedule**, select the **Restrict the availability of this SSID to selected schedules** check box to enable SSID schedules.
11. Select **Customize**.

    To create a new schedule, select +, and see Schedule Settings on page 374.
12. To customize **Advanced Access Security Controls**, see Customize Advanced Access Security Controls on page 377.
13. To customize **Optional Settings** (not available for 6 GHz), see Customize Wireless Network Optional Settings on page 379.
14. Toggle **Client Monitor ON** (default) to enable devices to detect client issues and report client connection activities and problems to ExtremeCloud IQ (New).
15. Select **SAVE**.

Related Links

Cloud User Group Settings on page 311

Local User Group Settings on page 312
Apply Different User Profiles to Clients and User Groups on page 376
Schedule Settings on page 374
Customize Advanced Access Security Controls on page 377
Customize Wireless Network Optional Settings on page 379
Configure the SSID for a Standard Wireless Network on page 308

## Configure Client Mode AP Profile using Wired Connection and Device Template

There must be at least one client mode profile configured before you can define a LAN-side AP radio for client mode.

You can set a radio on some AP models to client mode, which enables the AP to connect to existing open and PSK wireless networks, including third-party networks as a generic BYOD client. The method described here is recommended because it is often the fastest way to perform this task.

This task is part of the network policy configuration workflow. Use this task to configure a Client Mode Profile as part of an SSID for a network policy.

1. Go to **Configuration** > **Network Policies**.
2. Select an existing network policy, and then select , or to add a new one, select ..
3. After you save the **Policy Details**, select **NEXT** or **2 Wireless**.
4. Configure a client mode AP device template.
   a. From the **Wireless** > **Configuration Settings** menu, select **AP Template**.
   b. Select , and then select an AP model to use as the client mode AP.
   c. Type a **Template Name**.
   d. Configure the WAN-side backhaul (WiFi0 or WiFi1) radio for **Backhaul Mesh Link**.
   e. Select **Client Mode** for the LAN-side client mode radio (WiFi0 or WiFi1).
   f. Select an existing client mode **Radio Profile** for the LAN-side client mode radio.
   g. Select **SAVE TEMPLATE**.
5. Add an Open, or PSK SSID, without a captive web portal.
   For more information, see SSID Usage in Standard Wireless Networks on page 316.

Related Links

SSID Usage in Standard Wireless Networks on page 316

## Captive Web Portals

Extreme Networks supports two types of captive web portal:

- AP hosted portals on built-in web servers (device-based)
- Extreme Networks hosted portals on cloud web servers (cloud-based)

AP hosted portals support several user registration types (user authentication, self-registration to provide user data, use policy acceptance, self-registration to obtain a PPSK) plus an extensive set of configuration options. Cloud server hosted portals support two registration options: users can register by authenticating with their social media credentials or

by requesting and submitting a PIN. A cloud-based captive web portal also has a simpler set of configuration options. See also, Registration Types and SSID Access Security Compatibility on page 329.

After defining a captive web portal, you must take one of two actions for your changes to take effect:

- For an AP hosted captive web portal, upload the configuration, web page files, and certificates (for secure communications using HTTPS) to your devices.
- For a cloud-based captive web portal, upload the configuration to your devices. ExtremeCloud IQ (New) automatically stores the web page files and certificates in the cloud.

**Note**
To remove an existing login button that has already been deployed, you must resave the captive web portal and the Network Policy, and then redeploy the respective network policy to the device.

ExtremeCloud IQ (New) can include multiple captive web portals. You can view the information submitted by captive web portal users in the event logs, and in the syslog records. To view the information for PPSK users, go to **Configuration** > **Network Policies** > **Menu** > **User Management** > **Users**.

Related Links

Registration Types and SSID Access Security Compatibility on page 329
Customize and Preview Cloud-based Captive Portal Settings on page 338
Customize and Preview Device-based Captive Web Portal Settings on page 331
Import Captive Web Portal HTML Files on page 339

*Registration Types and SSID Access Security Compatibility*

When you create a captive web portal object for an SSID, the available registration types depend on access security mode of the SSID. Selecting a captive web portal registration type that does not match the SSID security mode causes the following error: *profile type does not match*.

The `registrationType` specified for the captive web portal object must match the captive web portal type selected in the SSID configuration. Use the following table to verify compatibility before creating a captive web portal object for an SSID.

**Table 128: Registration Types by SSID Access Security**

| SSID Access Security | User Auth | External Auth | Self-Reg | Both (Auth + Self-Reg) | Private PSK | UPA |
|---|---|---|---|---|---|---|
| Open (Unsecured) | Y | Y | Y | Y | N | Y |
| PSK (WPA/WPA2 Personal) | Y | Y | Y | Y | N | Y |

**Table 128: Registration Types by SSID Access Security (continued)**

| SSID Access Security | User Auth | External Auth | Self-Reg | Both (Auth + Self-Reg) | Private PSK | UPA |
|---|---|---|---|---|---|---|
| PPSK (Private Pre-Shared Key) | N | N | N | N | Y | Y |
| WPA/WPA2 Enterprise (802.1X) | N | N | N | N | N | Y |
| WEP (Static) | Y | Y | Y | Y | N | Y |
| WEP 802.1X | N | N | N | N | N | Y |

#### Registration Type Descriptions

**User Authentication (AUTH)**

User logs in with credentials validated against a RADIUS server. Supports PAP, CHAP, and MS-CHAP V2 authentication methods. Intended for employee access.

**External Authentication (EXTERNAL)**

Redirects the client to an external web server for authentication. The external server handles the login UI; RADIUS authentication is still performed by the AP. Requires a walled garden configuration.

**Self-Registration (SELF_REG)**

User fills in basic information (name, email, phone, etc.) without credential validation. Authentication always passes. Intended for guest access.

**Both — User Auth + Self-Registration (AUTH_AND_SELF)**

Combines User Authentication and Self-Registration on a single captive web portal page. The user can choose either method to register.

**Private PSK Server (PPSK)**

Used with a companion open SSID to issue private pre-shared keys via self-registration. The user registers on the open SSID and receives a unique PSK to connect to the PPSK SSID. Only valid on PPSK SSIDs.

**Use Policy Acceptance (USER_ACCEPT / UPA)**

User simply accepts an acceptable-use policy by clicking a button. No credentials or personal information are required. Supported on all SSID access security modes.

#### Common Causes of the "Profile Type Does Not Match" Error

- Reusing a captive web portal object across different registration types
- Attaching a captive web portal type that is incompatible with the SSID security mode (for example, User Auth captive web portal on a PPSK SSID)
- Editing an existing SSID and changing the captive web portal registration type on the SSID without replacing the captive web portal object

To resolve a mismatch error, do the following:

1. Verify the SSID access security mode (Open, PSK, PPSK, 802.1X, WEP, or WEP 802.1X).
2. Confirm that the captive web portal registration type and the security mode selected for the SSID are compatible.
3. Ensure the attached captive web portal object `registrationType` matches the captive web portal type selected on the SSID. If it does not, either create a new captive web portal object of the correct type or change the SSID captive web portal type selection to match the existing object.

*Customize and Preview Device-based Captive Web Portal Settings*

To configure a device-based captive web portal (CWP), you must first create a wireless network SSID with **Enterprise 802.1X** access security.

To join the SSID, users enter a user name and password, which are checked against a RADIUS server. When they open a web browser, the captive web portal opens to the **Use Policy Acceptance** (UPA) page. After the user agrees to the UPA, the AP allows them to access the rest of the network as determined by settings in the user profile applied to them.

This task is part of the network policy configuration workflow. Use this task to configure a device-based captive web portal.

1. Go to **Configuration** > **Network Policies**.
2. On the **Wireless** tab, select an existing SSID, and then select , or to add a new one, select ..
3. In the **SSID Usage** section, toggle **Enable Captive Web Portal** to **ON**.
4. Select **Captive Web Portal**, and then select the features.

**Table 129: CWP features**

| Feature | Description |
|---|---|
| User Auth on Captive Web Portal | Authenticates users on the splash page. |
| Enable Self-Registration | Enables user registration on the splash page.<br><br>**Note:** The **First Name** and **Last Name** fields cannot contain the following characters: $,`,<,>,+, and #. |
| Return Aerohive Private PSK | Issues a Private PSK for the user. |
| Enable UPA | Enables the display of the **Use Policy Acceptance** page. |
| Choose Authentication Type: | (This setting is not available if Self-Registration is enabled.) Authenticate using either a Radius Server, or redirect to an external URL. |

5. **SELECT** an existing CWP, or select **ADD**.
6. Type a **Name** for the CWP.

7. If you selected **Return Aerohive Private PSK**, configure the **PPSK Settings**.

**Table 130: PPSK settings**

| Setting | Description |
|---|---|
| Choose Access SSID (Private PSK) | Select an access SSID from the menu. |
| Choose a PPSK Server | Select a PPSK server from the menu. |

8. Select **CUSTOMIZE AND PREVIEW** > **CUSTOMIZATION AND PREVIEW**.

   Alternatively, you can import HTML files. See Import Captive Web Portal HTML Files on page 339.
9. Preview and Customize the Landing Page on page 333.
10. Preview and Customize the Use Policy Acceptance Page on page 333.
11. Preview and Customize the Success Page on page 333.
12. Preview and Customize the Error Page on page 334.
13. Enable or disable the **Success Page**.
14. Enable or disable **Redirect clients after a successful login attempt**.

    When enabled, ExtremeCloud IQ (New) sends successful clients to either the login page or to a specified URL.
15. Enable or disable the **Failure Page**, and choose the page to display the failure message.

    When enabled, ExtremeCloud IQ (New) displays the failure message on either the login page or the standard failure page. See Preview and Customize the Error Page on page 334.
16. Enable or disable **Redirect clients after a failed login attempt**.

    When enabled, ExtremeCloud IQ (New) sends unsuccessful clients to either the login page or to a specified URL.
17. Configure the default language, and additional languages.

**Table 131: Supported languages**

| Setting | Description |
|---|---|
| Default Language | Select the **Default Language** from the menu. |
| Support Additional Languages | Select the additional languages you intend to support. |

    ExtremeCloud IQ (New) adds the files required for the selected languages to the default CWP directory when you save the CWP.
18. Expand the **Advanced Configuration** section, and configure the settings.
19. To create a walled garden, select , and configure the settings.
20. Select **SAVE CWP**.

Return to the **Wireless Network** page to complete the network policy configuration.

Related Links

Import Captive Web Portal HTML Files on page 339
Advanced Configuration Settings on page 334
Walled Garden Settings on page 337
Configure the SSID for a Standard Wireless Network on page 308

#### Preview and Customize the Landing Page

This task is part of Customize and Preview Device-based Captive Web Portal Settings on page 331. Use this task to preview and customize the landing page for a device-based captive web portal.

1. Select **LANDING PAGE** to preview the landing page.
2. Select **CUSTOMIZE** to modify the landing page colors, logo, language, and message text.
3. Select **SAVE CUSTOMIZATION**.
4. Select the corresponding check boxes to enable fields and to specify which fields are required.
5. Select **SAVE CONFIGURATION**, or select **USE POLICY ACCEPTANCE**.

Next, Preview and Customize the Use Policy Acceptance Page on page 333.

Related Links

Customize and Preview Device-based Captive Web Portal Settings on page 331
Preview and Customize the Use Policy Acceptance Page on page 333

#### Preview and Customize the Use Policy Acceptance Page

This task is part of Customize and Preview Device-based Captive Web Portal Settings on page 331. Use this task to preview and customize the use policy acceptance page for a device-based captive web portal.

1. Select **USE POLICY ACCEPTANCE** to preview the page that displays the use policy.
2. Select **CUSTOMIZE** to modify the page colors, logo, language, and message text.
3. Select **SAVE CUSTOMIZATION**.
4. Select **SAVE CONFIGURATION**, or select **SUCCESS PAGE**.

Next, Preview and Customize the Success Page on page 333

Related Links

Customize and Preview Device-based Captive Web Portal Settings on page 331
Preview and Customize the Success Page on page 333

#### Preview and Customize the Success Page

This task is part of Customize and Preview Device-based Captive Web Portal Settings on page 331. Use this task to preview and customize the success page for a device-based captive web portal.

1. Select **SUCCESS PAGE** to preview the page that appears after a successful login.
2. Select **CUSTOMIZE** to modify the page colors, logo, language, and message text.
3. Select **SAVE CUSTOMIZATION**.
4. Select **SAVE CONFIGURATION**, or select **ERROR PAGE**.

Next, Preview and Customize the Error Page on page 334.

Related Links

Customize and Preview Device-based Captive Web Portal Settings on page 331
Preview and Customize the Error Page on page 334

#### Preview and Customize the Error Page

This task is part of Customize and Preview Device-based Captive Web Portal Settings on page 331. Use this task to preview and customize the error page for a device-based captive web portal.

1. Select **ERROR PAGE** to preview the page that appears after an unsuccessful login.
2. Select **CUSTOMIZE** to modify the page colors, logo, language, and message text.
3. Select **SAVE CUSTOMIZATION**.
4. Select **SAVE CONFIGURATION**.

Related Links

Customize and Preview Device-based Captive Web Portal Settings on page 331

#### Advanced Configuration Settings

Refer to the following settings when you configure a captive web portal, either as part of a network policy, or as a common object.

**Table 132: Advanced configuration settings**

| Setting | Description |
|---|---|
| Session Timer | Select **Display session timer alert before session expires** to display the session timer in the client browser.<br>The timer shows the login status for the registered client, the time remaining in the session, and the elapsed time. You can choose to display the timer alert 5, 15, or 30 minutes before the session expires. |
| Network Settings | Select **Use default settings** to use the default IP address and netmask for the interface hosting the SSID with the captive web portal, or an admin-defined IP address and netmask.<br>Select **Customize** to enter an IP address and netmask for each of the interfaces. You can use IPv4 or IPv6 addresses. |
| **DHCP and DNS servers > Use external servers** | |
| Use external servers | Select **Use external servers** to forward DHCP and DNS traffic from unregistered clients to external servers on the network. When enabled, unregistered and registered clients must be assigned to the same VLAN. |
| Override the VLAN ID used during registration | Select **Override the VLAN ID used during registration** and choose a previously defined VLAN ID from the drop-down list to assign to clients before and during the registration process.<br>Select  to add a new VLAN ID. |
| **DHCP and DNS servers > Use Extreme Network Devices** | |

**Table 132: Advanced configuration settings (continued)**

| Setting | Description |
|---|---|
| Use Extreme Networks Devices | Select **Use Extreme Network Devices** to forward DHCP and DNS traffic from unregistered clients to internal servers on the AP hosting the captive web portal. When enabled, unregistered and registered clients can be assigned to the same VLAN or to different VLANs, because unregistered clients use DHCP and DNS servers on the AP, and registered clients use servers on the network.<br><br>**Note:** When the client of a previously unregistered guest first associates with the Guest Access SSID, the AP acts as a DHCP server, DNS server, and web server. Client network access is limited to the AP with which it is associated, and the client browser redirects to a registration page. After the guest registers, the AP stores the client MAC address as a registered client and allows the guest to access external servers. |
| Lease Time | Type the length of the DHCP lease assigned to the quarantined client of an unregistered guest, and choose the unit of time measure from the menu.<br>DHCP clients typically renew at the midpoint of the lease. After the client successfully registers, the AP allows the next DHCP lease request to pass to an external DHCP server. Keeping the lease short allows the client to obtain new network settings soon after registering. |
| Renewal Response | From the menu, choose how you want the AP to respond to a DHCP lease renewal request for a nonexistent lease.<br>• **Renew-NAK-Broadcast**: By default, the AP responds by broadcasting DHCPNAK messages. Choosing either this option or the unicast DHCPNAK option can accelerate the transition to an external DHCP server on the network, or back to a quarantined address after the client logs out or the session times out.<br>• **Renew-NAK-Unicast**: Choose to have the AP respond by sending unicast DHCPNAK messages. Sending unicast messages can reduce traffic on the network; however, broadcasting the DHCPNAK is safer in environments where there is a large and uncontrollable variety of clients.<br>• **Keep Silent**: Choose to have the AP ignore the renewal request completely and enable the external DHCP server to respond. With this approach, the transition between DHCP servers can be slightly longer. |
| **Web Servers** | |

**Table 132: Advanced configuration settings (continued)**

| Setting | Description |
|---|---|
| Registration Period | Set the length of time that a registered client with an active session remains registered. Type a value and choose the unit of time measure from the menu.<br>If the client closes one session and later starts a new one while the AP still has a roaming cache entry for that client (one hour by default), the client does not have to register with the captive web portal again. If the client closes a session and starts a new session after the roaming cache entry has been removed, the client must complete the registration process again, even if the new session begins within the registration period. |
| Domain Name | Type the same domain name as the CN (common name) value in the server certificate that the captive web portal uses for HTTPS.<br>The domain name must be a valid domain name that a DNS server can resolve to the IP address of the interface hosting the captive web portal. This option allows you to use a server certificate from a CA that supports domain names as CNs, but not IP addresses.<br><br>**Note:** If the CN has a wildcard domain name that can match multiple valid domain names, enter one of the valid domain names instead of selecting **Override Web server domain name with CN value in the certificate**. For example, if the CN is *.aerohive.com, then you can enter something like `cwp.aerohive.com` in the Web Server Domain Name field, and the clients' browsers will not show a security warning when they make an HTTPS connection to the captive web portal. |
| **Security** | |
| Enable HTTPs | Select **Enable HTTPs** to enable HTTPS on the captive web portal. |
| HTTPS certificate | Select **Default-CWPCert.pem** for preloaded captive web portals.<br>The AP hosting the captive web portal then uses HTTPS to secure traffic between the client and its captive web portal server. The certificate file must have the following properties:<br>• The file format must be PEM (Privacy Enhanced Mail).<br>• It must contain a server private key stored in an unencrypted format.<br>• It must contain a server certificate concatenated to the private key. |
| Override Web server domain name with CN value in the certificate | Select to replace the Web server domain name with the common name value in the certificate. |
| **Client Redirection** | |

**Table 132: Advanced configuration settings (continued)**

| Setting | Description |
|---|---|
| Use HTTP 302 | Select **Use HTTP 302** to redirect code as the redirection method instead of JavaScript.<br>This option is useful for clients accessing the network with mobile browsers. |
| Introduce a delay before redirecting after a successful login attempt | Specify how long the captive web portal displays the success page before initiating the redirection. Type a value in seconds. |
| Introduce a delay before redirecting after a failed login attempt | Specify how long the captive web portal displays the failure page before initiating the redirection. Type a value in seconds.<br>**Note:** This redirection differs from that in the **Captive Web Portal Failure Page Settings** section, which the AP applies after a failed log in attempt. |
| Prevent the Apple CNA (Captive Network Assistant) application from requesting credentials | Select **Prevent the Apple CNA (Captive Network Assistant) application from requesting credentials** to bypass the Apple CNA application for redirect actions. |

#### Walled Garden Settings

Refer to the following settings when you configure a Captive Web Portal, either as part of a network policy, or as a common object.

**Table 133: Walled garden settings**

| Setting | Description |
|---|---|
| Service Type | Select one of the following options:<br>• **Web**: Permit client access only to the World Wide Web.<br>• **All**: Permit client access to the World Wide Web and all other servers.<br>• **Advanced**: Permit client access only to the admin-defined IP object or host name.<br>If you selected **Web** or **All**, paste IP addresses or host names separated by commas into the **Service Type** text box. Then select **ADD**.<br>If you selected **Advanced**, configure the settings, and then select **ADD**. |
| IP Object/Host Name | Enter an IP object or host name of the external web server. Choose a previously-defined IP address or host name from the menu, enter a new IP address or domain name, or select  and define a new one. |
| Service | Select the service from the menu: Web, All, or Protocol. |

**Table 133: Walled garden settings (continued)**

| Setting | Description |
|---|---|
| Protocol Number | (Protocol service only)<br>Type a protocol number (from 0 to 255). |
| Port | (Protocol service only)<br>Type a port number to define the type of service you want to permit. |

*Customize and Preview Cloud-based Captive Portal Settings*

To configure a cloud-based captive web portal, you must first create a wireless network SSID with **Open** access security. For more information, see Captive Web Portals on page 328.

ExtremeCloud IQ (New) supports two types of cloud-hosted captive web portals. One controls network access by leveraging user credentials in social media services like Google and LinkedIn. The other type authenticates users by requiring them to enter a PIN, which is sent to them by email, to gain network access. The PIN is bound to MAC address of the device. It can be reused from the same device until the specified validity period expires.

This task is part of the network policy configuration workflow. Use this task to configure a cloud-based captive web portal (CWP).

1. Go to **Configuration** > **Network Policies**.
2. Select an existing policy with open access security, and then select , or to add a new one, select ..
3. On the **Wireless** tab, select an existing SSID, and then select , or to add a new one, select ..
4. In the **SSID Usage** section, toggle the **Enable Captive Web Portal** setting **ON**.
5. Select **Cloud Captive Web Portal**.
6. To use social media services, select **Social Login**, or to require a PIN for logging in, select **Request a PIN**.

   If you require a PIN, ExtremeCloud IQ (New) sends a randomly generated PIN to authenticate the user.
7. **Select** an existing captive web portal or select **ADD**.
   a. If you selected **ADD**, enter a new **Name** for the captive web portal.
   b. Enter the length of time that the PIN remains valid.

      The validity period begins when ExtremeCloud IQ (New) receives the PIN request and can last from 1 to 24 hours.
   c. Enter an email address where you want ExtremeCloud IQ (New) to send daily reports about successfully authenticated users on this captive web portal.

      Each report is in CSV format and shows the login time (in UTC, or universal coordinated time) when the user submitted a PIN, the user name, and the MAC address of the client device used for the connection. ExtremeCloud IQ (New) sends a separate email for when there are no entries to report.

d. Set the hour and minute when ExtremeCloud IQ (New) generates a daily report of successful user authentications.

   ExtremeCloud IQ (New) reports the time in UTC, and the report contains events for the previous 24 hours.

e. Use the default captive web portal without customization, or toggle **Customize** to **ON** and select **PIN-Login-Example** to export the necessary files.

f. Modify the files and import them in the **New Captive Web Portal** window.

g. Select **Upload/Remove**, navigate to the files on your system and upload them.

h. Select **Done**.

i. Select the files you want to use for the **Login** and **Success** pages, and then select **SAVE CWP**.

   The imported files are immediately saved to ExtremeCloud IQ (New).

**Note**
If you previously completed the configuration with default files and uploaded the network policy to your APs, you do not need to upload the configuration again.

If the customized files have the same name as the default files, the custom files overwrite the default files after import to ExtremeCloud IQ (New).

8. Select **Use a different captive web portal for various clients** to use other captive web portals for different clients based on device classification and classification rules.
9. Select **Select a Classification Rule** to choose an existing rule, and then select **Link**.

   To add a new classification rule, select **Add a Classification Rule** and complete the steps. For more information, see Configure Classification Rules for a Device Template on page 438.

Return to the Wireless Network page to complete the network policy configuration.

Related Links

Configure Classification Rules for a Device Template on page 438
Configure the SSID for a Standard Wireless Network on page 308

*Import Captive Web Portal HTML Files*

To import an HTML file for a captive web portal (CWP), you must first create a wireless network SSID and enable CWP.

This task is part of the network policy configuration workflow. Use this task to to import an HTML file for your captive web portal configuration.

**Note**
**Import HTML** overrides the settings that are configured in **Customize and Preview**.

1. Go to **Configuration** > **Network Policies**.
2. Select an existing policy, and then select , or to add a new one, select .
3. On the **Wireless** tab, select an existing SSID, and then select , or to add a new one, select ..

4. In the **SSID Usage** section, toggle the **Enable Captive Web Portal** setting **ON**.
5. Select **Captive Web Portal**.
6. On the **New Captive Web Portal** page, select **IMPORT HTML**.
7. Select **UPA-Example** to download a template that you can modify.
8. Select an existing **Web File Directory**, or select **Create** and type a new file directory name.
9. Select **Upload/Remove**, navigate to the files on your system and upload them.
10. Select **DONE**.
11. Select a file to use for the **Login Page**.
12. Select a file to use for the **Success Page**.
13. (Optional) Select **Redirect clients after a successful login attempt**.
14. Select the files you want to use for the **Login** and **Success** pages, and then select **SAVE CWP**.

    There is no need for a failure page because error messages appear on the **Login** page rather than requiring navigation to a separate page. ExtremeCloud IQ (New) immediately saves the imported files.



**Note**
If you previously completed the configuration with default files and uploaded the network policy to your APs, you do not need to upload the configuration again.
If the customized files have the same name as the default files, the custom files overwrite the default files after import to ExtremeCloud IQ (New).

Return to the **Wireless Network** page to complete the network policy configuration.

Related Links

Configure the SSID for a Standard Wireless Network on page 308

## Hotspot

ExtremeCloud IQ (New) supports the definition of Hotspot 2.0 service, and simplified configuration for WBA OpenRoaming on Hotspot 2.0 networks.

When configuring a hotspot, you have the following options:

- Use WBA OpenRoaming for a simplified NAI routing configuration that automatically creates a AAA policy.
- Configure a traditional hotspot and enable NAI routing in the AAA Policy.

  WBA OpenRoaming is a simplified configuration for a hotspot that uses a single realm.

All currently supported Extreme Networks AX (Wi-Fi 6), 6E (Wi-Fi 6E), and Wi-Fi 7 model APs support OpenRoaming.

Traditionally, using a hotspot presents end users with several challenges, including initial connection issues, security concerns, and connectivity while roaming. Hotspot 2.0 offers the following features to improve the hotspot end-user experience:

- Pre-association network discovery and selection using the dot11u ANQP protocol, resulting in a seamless initial connection.
- Simplified account registration. Provisioning is achieved without user input.
- Enhanced security, using over-the-air transmission secured by WPA2 or WPA3.
- Simplified **WBA OpenRoaming**.
- NAI Routing. When NAI Routing is enabled, you can associate RADIUS Servers with realms.

Each hotspot WLAN has its own Access Network Query Protocol (ANQP) configuration. The HESSID and ANQP Domain ID are specific to the hotspot WLAN.

With pre-association, a mobile device uses ANQP to perform network discovery. The mobile device connection manager uses the hotspot information, including the service provider policy and user preferences, to automatically select a hotspot network. A mobile device queries the hotspot for key service provider identification and authentication information and selects a network. The system generates the ANQP response using parameters configured by the hotspot operator.

Related Links

Configure a Hotspot on page 341
Hotspot WBA OpenRoaming on page 346

*Configure a Hotspot*

First configure an Enterprise SSID. For more information, see Configure the SSID for a Standard Wireless Network on page 308.

IQ Engine v10.7.5 or later is required.

**Note**
AP305C/X, AP410C, AP510C/X, AP460C/S6C/S12C, AP3000, AP4000, AP3000, AP5010, and AP5050 models support Hotspot 2.0.

Hotspot 2.0, also called Wi-Fi Certified Passport, is a standard for public access Wi-Fi that provides seamless and secure roaming among Wi-Fi networks and between Wi-Fi and cellular networks.

This task is part of the network policy configuration workflow. Use this task to configure a hotspot for an Enterprise SSID.

1. On the **2 Wireless** page for the policy, select an existing **Enterprise** SSID, or select to add a new one.
2. From the **Hotspot** list, select **Enabled**.
3. From the **Hotspot Profile** list, select an existing profile, or select to add a new one.
4. On the **Hotspot Identification** tab, configure the settings to identify the hotspot.

   For more information, see Hotspot Identification on page 342.

5. On the **SP Identification** tab, select an existing Service Provider Profile from the list, or select + and configure the settings.

   For more information, see Service Provider Identification on page 343.
6. On the **Network Characteristics** tab, configure the settings.

   For more information, see Network Characteristics on page 345.
7. On the **Online Signup** tab, configure the settings.

   For more information, see Online Signup on page 346.
8. Select **SAVE**.

Related Links

Hotspot Settings on page 342

*Hotspot Settings*


- Hotspot Identification on page 342
- Service Provider Identification on page 343
- Table 135 on page 343
- Network Characteristics on page 345
- Online Signup on page 346


#### Hotspot Identification

On the **Hotspot Identification** tab, configure the settings to uniquely identify the hotspot and specify the languages for the venue.

**Table 134: Hotspot Identification settings**

| Setting | Description |
|---|---|
| Name | (Required)<br>Type a name for the hotspot. |
| HESSID | (Required)<br>Type the Homogenous Extended Service Set Identifier (HESSID) for the Hotspot 2.0 network.<br>One SSID can be used across multiple WLANs (BSS). A Beacon with the same {HESSID, SSID} pair belongs to same WLAN. The {HESSID, SSID} pair must be unique for each WLAN. By default, the HESSID is the MAC address of the controller Ethernet port. Hotspots can have the same HESSID as long as the SSID is unique. If you configure the HESSID manually, we recommend using an AP BSSID as the HESSID. In a mobility domain, manually configure the HESSID to a unique value, to differentiate it from the value used in the WLAN of the controller. |
| Domain | (Required)<br>Type the Fully-Qualified Domain Name (FQDN) for the Hotspot 2.0 network. (Default: empty string)<br>Domain names in the domain name list might contain sub-domains. If the FQDN of the service provider is not in the domain name list but is in the realm list, mobile devices that use that service provider are considered to be roaming. |

**Table 134: Hotspot Identification settings (continued)**

| Setting | Description |
|---|---|
| Venue Info | Describe the venue. From the lists of predefined values, first select the category of the venue, and then select the subtype.<br>**Example:** Institutional, Hospital<br>Select ➕, configure the settings, and then select **ADD**. |
| Operator Name | (Required)<br>Type the name of the venue operator. |
| Venue Name | (Required)<br>Type the name of the venue. |
| Language | (Required)<br>Select a language from the list. You can configure up to four languages for each venue. |

#### Service Provider Identification

On the **SP Identification** tab, configure the settings to identify the service provider and configure authentication. Select existing **Service Provider Profiles**, or select ➕ to add a new Service Provider Profile.

**Note**
Keep your DNS server records up to date so that mobile devices can resolve the server domain names (FQDN).

Mobile devices with a SIM or USIM credential, can obtain a realm from the hotspot NAI Realm list. While hotspot access usually requires 3GPP credentials, a targeted NAI home query is an efficient alternative approach. The device connection manager compares the realm information from the list to the information stored on the device. The connection manager uses the preconfigured user preferences and policy from the mobile device to make a decision between a hotspot AP or a non-hotspot AP, if both are available.

**Table 135: Service Provider Profile Settings**

| Setting | Description |
|---|---|
| **NAI Realm**: The Network Access Identification (NAI) Realm list is a list of realms that can be successfully authenticated. Each realm may have up to four supported EAP methods.<br>• Add all realms that can authenticate the login credentials or certificate credentials of a mobile device, including the realms of all roaming partners that are accessible from the hotspot AP. Include the realm of the home service provider.<br>• Add a realm for the PLMN ID. This is the cellular network identity based on public land mobile network (PLMN) information.<br>Select ➕ and configure the settings. | |
| Realm | (Required)<br>Type the Fully-Qualified Domain Name (FQDN) of the service provider.<br>Wildcards are supported for realm. For example, you can enter *.extreme.area120.com, instead of entering specific realms. |

**Table 135: Service Provider Profile Settings (continued)**

| Setting | Description |
|---|---|
| EAP Method | From the list, select the Extensible Authentication Protocol (EAP) authentication type.<br>Mobile devices provisioned to authenticate against the home service provider do not require the EAP methods configured for the NAI Realm List. |
| Description | Type a description for the realm.<br>Although optional, descriptions can be helpful when you are configuring or troubleshooting your network. |
| **Roaming Consortium**: Use roaming consortium authentication when you do not know all the authenticated realms. Using identifiers unique to the organization in the beacon is a battery-efficient roaming method because ANQP queries are not required.<br>Select +, configure the settings for the Roaming Consortium, and then select **ADD**. | |
| Consortium | (Required)<br>Type the Roaming Consortium Organization Identifier (RCOI).<br>Specify up to eight identifiers unique to the organization that are part of the MAC address. |
| Description | Type a description for the consortium.<br>Although optional, descriptions can be helpful when you are configuring or troubleshooting your network. |
| **3GPP CellularNetwork**: Create a list of cellular network IDs in the form of mobile country code (MCC), mobile network code (MNC). This list establishes whether an AP has a roaming arrangement with the 3GPP service providers.<br>Select +, configure the settings for a 3rd Generation Partnership Project (3GPP) mobile network, and then select **ADD**. | |
| MCC | (Required)<br>Type the mobile country code (MCC). |
| MNC | (Required)<br>Type the mobile network code (MNC). |
| Description | Type a description for the 3GPP mobile network.<br>Although optional, descriptions can be helpful when you are configuring or troubleshooting your network. |
| **Advanced Settings** | Select the arrow to expand this section and configure the following settings:<br>• **NAI Realm**<br>• **Roaming Consortium**<br>• **3GPP CellularNetwork**<br><br>**Note:** Advanced Settings override the corresponding settings in the associated Service Provider profiles. |

#### Network Characteristics

On the **Network Characteristics** tab, configure network settings to specify the type of access network, IP address type availability, WLAN metrics, and connection capabilities.

**Table 136: Network Characteristics settings**

| Setting | Description |
|---|---|
| **Access Network**: From the list, select the type of access network:<br>• **Private network**—An enterprise network with user accounts.<br>• **Private network with guest access**—An enterprise network providing guest access.<br>• **Chargeable public network**—(Default) Open to anyone but access requires payment.<br>• **Free public network**—An open network, free of charge but may still require acceptance of terms of use (and may involve OSU servers with a captive portal). | |
| DGAF | Select **DGAF** to enable Downstream Group Addressed Forwarding for the access network. If enabled, the system forwards all downlink wireless broadcast ARP and multicast packets. (Default: disabled) |
| **IP Address Type Availability**: Mobile devices use information about IP address type availability to make network selection decisions. Select the level of restriction for each network type. | |
| IPV4 | From the list, select the type of IPV4 address:<br>• Not Available<br>• Public<br>• Port Restricted<br>• Single NAT<br>• Double NAT<br>• Port Restricted Single NAT<br>• Port Restricted Double NAT<br>• Unknown |
| IPV6 | From the list, select the type of IPV6 address:<br>• Not Available<br>• Available<br>• Unknown |
| **WLAN Metrics**: Mobile devices use the WAN Metrics settings to make network selection decisions. The mobile device can determine whether necessary throughput is available from the hotspot before connecting. If the mobile device receives indication that the basic service set (BSS) is at capacity, the device will not associate with that AP. | |
| Link Status | From the list, select a status. (Up, Down, or Test) |
| Downlink Speed | Specify the download speed in kbps. |
| Uplink Speed | Specify the upload speed in kbps. |
| **Connection Capability**: Select , configure the settings, and then select **ADD**.<br>Mobile devices use connection capability information to make network selection decisions by determining which services are blocked or supported at the hotspot. | |
| Protocol | From the list, select the network protocol. |

**Table 136: Network Characteristics settings (continued)**

| Setting | Description |
|---|---|
| Port Number | Type the port number. |
| Status | From the list, select a status. (Open, Closed, or Unknown) |

#### Online Signup

With Online Signup (OSU), users who are not part of the provider network can manually connect to the hotspot. This feature also provides added security for users who want to connect anonymously.

From the **Network Authentication Type** list, select an authentication method and configure the settings.

**Table 137: Online Signup settings**

| Setting | Description |
|---|---|
| **Acceptance of Terms and Conditions**—Redirection occurs after the user accepts the Terms and Conditions. | |
| **Online Sign up**—Authentication supports online enrollment. | |
| OSU SSID | Type the SSID for the online signup service. |
| **CWP (Captive Web Portal)**—Redirection occurs after the CWP authenticates the user. | |
| Redirection URL | Type the HTTP or HTTPS address for automatic redirection after authentication. |

Related Links

Configure a Hotspot on page 341

*Hotspot WBA OpenRoaming*

WBA OpenRoaming provides users with roaming access to Wi-Fi hotspots without having to register with different operators or enter login credentials each time. The Wi-Fi roaming standard combines a federation of network providers and identity providers, enabling users to join any compliant network through a federation member. Authentication is achieved through the user's identity provider when the provider is a federation member. All federation members support the WBA PKI.




**Figure 8: WBA OpenRoaming**

The WBA OpenRoaming is based on the following elements:

- Hotspot 2.0
- DNS Discovery
- WBA OpenRoaming PKI
- RADSEC

The OpenRoaming policy offers the following:

- Accepts users from any ID provider
- Free roaming. The service provider does not charge the roaming subscriber for Wi-Fi access
- QoS on a best effort basis.
- The user identity can remain anonymous. The ID provider does not share the user's identity with the service provider.

**Note**
RadSec proxy AP election relies on APs sharing compatible software support and SSID profile configuration. Mixing APs that do not all support OpenRoaming, or assigning different RadSec-enabled SSID sets to APs that share the same profile in the same management subnet, can result in a proxy AP that cannot serve all OpenRoaming SSIDs correctly. To avoid issues, keep APs with different RadSec/OpenRoaming requirements in separate network policies and profiles.

Related Links

Configure WBA Open Roaming on page 347
Hotspot on page 340

*Configure WBA Open Roaming*

First, obtain the CA, CERT, and KEY files from your Access Network Provider (ANP), and import them into ExtremeCloud IQ (New). Depending on the file format provided, you might have to convert the files during the import process.For more information, see Import a Certificate or Key on page 559. Then, use these three files to create a certificate bundle.
Use this task to configure WBA Open Roaming.

1. Configure an Enterprise SSID.

   For more information, see Configure Enterprise SSID Authentication on page 319.
2. For **Hotspot** (in the SSID configuration) select **WBA Open Roaming**.
3. In the **WBA OpenRoaming Configuration** dialog configure the settings:

**Table 138: WBA Open Roaming settings**

| Setting | Description |
|---|---|
| Trust Point | Select the Certificate Bundle that you created using the certificate and key files obtained from your Network Access Provider. |
| WBAID | Type your Wireless Broadband Alliance Identity (WBAID). The WBAID enables secure and automated connectivity between Wi-Fi networks and identity providers. |

4. Select **OK**.

Related Links

Hotspot WBA OpenRoaming on page 346
Hotspot on page 340

## RADIUS Authentication

RADIUS authentication is for use by Enterprise WPA/WPA2 802.1X and WEP 802.1X SSIDs, MAC authentication, and captive web portals that require user authentication. Extreme Networks devices use the wireless network (SSID) RADIUS server group for RADIUS lookups, unless there is a classification rule directing them to a different group based on location or other parameters. The servers in the group can be external RADIUS servers, Extreme Networks RADIUS servers, Extreme Networks proxy servers, or a combination of these three types.

**Note**
The WEP protocol is no longer effective for securing wireless networks. For security reasons, WEP configuration is no longer available in the UI. If you require WEP for business continuity purposes, you can enable it through Supplemental CLI.

When configuring RADIUS Authentication, you can associate a Tunnel Policy to encapsulate and route authenticated client traffic to a designated Tunnel Concentrator. Traffic for clients authenticated through the RADIUS server is automatically directed through the specified tunnel.

**Important**
Ensure the selected Tunnel Policy is active and associated with a valid Tunnel Concentrator before deploying the network policy. For more information, see Configure Tunnel Policies on page 542.

Related Links

Configure a RADIUS Server Group on page 348
Configure RADIUS Server Settings on page 350
Configure an External RADIUS Server on page 352
Configure an Extreme Networks RADIUS Server on page 354
Configure a RADIUS Proxy Server Realm on page 360
Add an Active Directory Server on page 357
Add an LDAP Server on page 358

*Configure a RADIUS Server Group*

You must first create a wireless network SSID with **Enterprise 802.1X (WPA/WPA2/WPA3)** access security. This option requires users to authenticate themselves by entering a user name and password, which are checked against a RADIUS authentication server.

RADIUS servers offer two different types of services:

- Authentication for user credentials (usually on port 1812)
- Accounting (logging) (usually on port 1813)

Extreme Networks devices use the default wireless network (SSID) RADIUS server group, which can include up to four RADIUS servers, for RADIUS lookups, unless there is a device classification rule directing them to a different RADIUS server group. The servers in the group can be external RADIUS servers, Extreme Networks A3 RADIUS servers, Extreme Networks RADIUS servers, Extreme Networks proxy servers, or a combination of these four types.

Security for RADIUS servers uses simple passwords. Configure one password on the server, and the other on each of the clients.

This task is part of the network policy configuration workflow. Use this task to to configure a RADIUS server group for an SSID, as part of a network policy.

1. Go to **Configuration** > **Network Policies**.
2. Select an existing policy, and then select , or to add a new one, select .
3. After you save the **Policy Details**, select **NEXT** or **2 Wireless**.
4. In the **Authentication Settings** section, toggle the **Authentication with ExtremeCloud IQ Authentication Service** setting **OFF**.

   The **Authenticate via RADIUS Server** section becomes available.
5. To add an existing RADIUS server group, select and choose an existing object, or to add a new one, select .
6. Type a **RADIUS Server Group Name**.
7. (Optional) Type a **RADIUS Server Group Description**.

   Although optional, descriptions can be helpful when you are configuring or troubleshooting your network.
8. Under **RADIUS Traffic Path**, specify how authentication and accounting traffic is routed between access points and external RADIUS servers:

   - **AP Local Bridge** (Default): Sends RADIUS authentication and accounting traffic directly from the AP over the local management network to the RADIUS server without passing through a tunnel.
   - **Tunnel**: Forwards RADIUS control traffic from the AP through a GRE or GRE-over-IPsec tunnel to a designated Tunnel Concentrator (TC), allowing centralized authentication for RADIUS servers located behind a TC termination point.

   When you select **Tunnel**:

   - A list of available **Tunnel Policies** (mobility policies) configured in the system appears.
   - Select the radio button corresponding to the **Tunnel Policy** you want to use for carrying RADIUS traffic to the Tunnel Concentrator.

- (Optional) Select next to a Tunnel Policy to review or modify its settings.

**Note**

- To select **Tunnel**, a Tunnel Concentrator Address Pool (TCAP) Profile must be configured and assigned to the Tunnel Concentrator service. APs require a client tunnel IP from this address pool to source RADIUS requests inside the tunnel. For more information, see Configure Tunnel Concentrator Address Pool (TCAP) Profiles on page 541.
- Selecting **Tunnel** routes RADIUS authentication traffic through the tunnel regardless of whether client data traffic is locally bridged at the AP or centrally tunneled to the TC.
- RADIUS servers using tunneled traffic must be defined by IP address (FQDN resolution is not supported over tunneled RADIUS paths).
- Dynamic VLAN overrides (`Tunnel-Private-Group-ID`) received in RADIUS `Access-Accept` responses are supported over tunneled paths.

9. Configure the RADIUS server settings for IQ Engine devices.

   See Configure RADIUS Server Settings on page 350.
10. Depending on the type of server that you want to add, select one of the following tabs:

| Tab | Configuration task |
|---|---|
| EXTERNAL RADIUS SERVER | Configure an External RADIUS Server on page 352 |
| EXTREME NETWORKS A3 | Configure an Extreme Networks A3 Server on page 354 |
| EXTREME NETWORKS RADIUS SERVER | Configure an Extreme Networks RADIUS Server on page 354 |
| EXTREME NETWORKS RADIUS PROXY | Configure an Extreme Networks RADIUS Proxy on page 360 |

   Select up to four existing servers to add to your wireless network (SSID) RADIUS server group.
11. Select **SAVE RADIUS**.

**Note**

In addition to those set by you, or by default, Extreme Networks APs report updated DHCP-snooped IP addresses of associated clients to the RADIUS server asynchronously, or as soon as the information is available.

Related Links

Configure RADIUS Server Settings on page 350

*Configure RADIUS Server Settings*

First begin configuring a RADIUS server group. See Configure a RADIUS Server Group on page 348.

This task is part of the network policy configuration workflow. Use this task to configure RADIUS server settings for IQ Engine devices for a RADIUS server group, as part of a network policy.

1. On the **Configure RADIUS Servers** page, select  and configure the following settings:

| Setting | Description |
|---|---|
| Retry Interval | Specify the time between retries for an unresponsive primary RADIUS server Access-Request. The device retries the primary server after the interval elapses, even if the current backup server is responding.<br>Range: 60–100000000 (seconds)<br>Default: 600<br><br>**Note:** Do not enter commas in this field. Enter 100,000,000 as 100000000. |
| Accounting Interim Update Interval | Specify the interval for sending RADIUS accounting updates to report the client session status and cumulative length.<br>Range: 10–100000000 (seconds)<br>Default: 600<br><br>**Note:** Do not enter commas in this field. Enter 100,000,000 as 100000000. |
| Permit Dynamic Change Of Authorization Messages (RFC 3576) | Enable the RADIUS server to dynamically change the authorization for a user, or to disconnect a user per RFC 3576. When you enable this parameter, devices acting as RADIUS authenticators can accept unsolicited disconnect and Change of Authorization (CoA) messages from a RADIUS authentication server, such as GuestManager, per RFC 3576. Disconnect messages terminate a user session immediately, and CoA messages modify session authorization attributes such as VLANs and user profile IDs. |
| Inject Operator-Name attribute | Select to include the Operator-Name attribute in the Access-Request and Accounting-Request messages that the Extreme Networks RADIUS authenticators send to the RADIUS authentication server. The attribute value is the domain name suffix of the Extreme Networks authenticator, usually assigned by DHCP, and helps to identify the authentication requests source. Providing source information like this can aid in troubleshooting authentication problems. |

| Setting | Description |
|---|---|
| Message Authenticator attribute | The Message Authenticator attribute is an HMAC-MD5 checksum of the entire Access-Request packet, containing the Type, ID, Length, and Authenticator field, using the shared secret as the key. This ensures the authenticity and integrity of the packet.<br>ExtremeCloud IQ uses this attribute to authenticate RADIUS server replies, and to encrypt passwords. |
| Override default failover settings | Select this option to override the default RADIUS server failover and retry interval. The retry interval is the number of seconds between RADIUS server requests.<br>Select **Aggressive** or **Custom (Range 1-5)**.<br>Set the **First retry interval**. (Default: 1)<br>Set the **Max-retries** value, which is the maximum number or retries, before failing over to a configured backup RADIUS server. (Default: 3) |

2. Select **SAVE RADIUS SETTINGS**.

Finish configuring the RADIUS server group.

Related Links

Configure a RADIUS Server Group on page 348

*Configure an External RADIUS Server*

First begin configuring a RADIUS server group. See Configure a RADIUS Server Group on page 348.

To add an external RADIUS server, you require the IP address, authentication port number, and the shared secret for the RADIUS server.

This task is part of the network policy configuration workflow. Use this task to configure a RADIUS server for a RADIUS server group, as part of a network policy.

1. On the **Configure RADIUS Servers** page, select **EXTERNAL RADIUS SERVER**.
2. Select an existing external RADIUS server object, and then select , or to add a new one, select .
3. Configure the settings.
4. Select **SAVE EXTERNAL RADIUS**.

Finish configuring the RADIUS server group.

Related Links

Configure a RADIUS Server Group on page 348
External RADIUS Server Settings on page 353

#### External RADIUS Server Settings

Use the following settings when you configure an external RADIUS server for a RADIUS server group, as part of a network policy. You can also use this settings if you are configuring an AP template object or a common object.

**Table 139: Settings for external RADIUS servers**

| Setting | Description |
|---|---|
| Name | Type a **Name** for the server. |
| Description (optional) | Type a **Description** for the server.<br>Although optional, descriptions can be helpful when you are configuring or troubleshooting your network. |
| Type | Select the transport and security mechanism for RADIUS server communication:<br>• **Standard**: Standard unencrypted RADIUS protocol over UDP (default UDP port 1812 for Authentication, 1813 for Accounting).<br>• **Secure**: Secure RADIUS traffic forwarding (for example, routing RADIUS control traffic through a GRE or GRE-over-IPsec tunnel to a Tunnel Concentrator using a mobility policy).<br>• **RADSEC**: RADIUS over TLS (RFC 6614), encrypting RADIUS transport over TCP (default TLS port 2083). |
| IP/Host Name | Select the **IP/Host Name** for the server.<br>If you do not see the IP address that you need, select  to define a new one (IPv4 or IPv6).<br>If the address object is a host name, ensure that the devices can resolve it to an IP address. If you configure a domain name for the devices, or if the devices dynamically receive a domain name through DHCP, and the RADIUS server belongs to the same domain, the RADIUS server name can be just the host name without the domain name. If the RADIUS server belongs to a different domain, the address object must be the fully qualified domain name (FQDN): the host name + the domain name. |
| Server Type | Choose the RADIUS server role:<br>• **Authentication**: As an authentication server, the RADIUS service requests that the client device demonstrate its identity.<br>• **Port**: Set the RADIUS authentication port.<br>• **Accounting**: As an accounting server, the RADIUS service tracks client-server session details.<br>• **Port**: Set the RADIUS accounting port number. |

**Table 139: Settings for external RADIUS servers (continued)**

| Setting | Description |
|---|---|
| Shared Secret | Type the **Shared Secret** for authenticating communications with the RADIUS server. |
| Show Password | (optional)<br>To display the password, select the check box. |

Related Links

Configure an External RADIUS Server on page 352
Configure AP Templates on page 466
Configure External RADIUS Servers on page 554

*Configure an Extreme Networks A3 Server*

You must have existing A3 RADIUS server services.

First, begin configuring a RADIUS server group. See Configure a RADIUS Server Group on page 348.

This task is part of the network policy configuration workflow. Use this task to configure an A3 server for a RADIUS server group, as part of a network policy.

1. On the **Configure RADIUS Servers** page, select **EXTREME NETWORKS A3**.
2. Select an existing server, or select .
3. Type a **Name** for the server.
4. (Optional) Type a **Description**.
5. Enter the **IP/Hostname** of the server.
6. Accept the defaults or enter specific **Server Type** ports.
7. Type the **Shared Secret** for authenticating communications with the A3 server.
8. (Optional) Select **Show Password**.
9. Select **SAVE EXTREME NETWORKS A3**.

Finish configuring the RADIUS server group.

Related Links

Configure a RADIUS Server Group on page 348

*Configure an Extreme Networks RADIUS Server*

First begin configuring a RADIUS server group. See Configure a RADIUS Server Group on page 348.

Extreme Networks devices can serve as RADIUS authentication servers and respond to 802.1X requests from other Extreme Networks devices acting as RADIUS authenticators. The Extreme Networks RADIUS server can store user accounts locally, or check user login credentials against user accounts stored externally on the following user database servers: Active Directory, or LDAP.

This task is part of the network policy configuration workflow. Use this task to configure an Extreme Networks RADIUS server for a RADIUS server group, as part of a network policy.

1. On the **Configure RADIUS Servers** page, select **EXTREME NETWORKS RADIUS SERVER**.
2. Select a **User Database Type** from the menu.
3. Select an existing server, or select .
4. Select the devices to configure.
5. Configure the AAA Server Profile.
   See Configure an AAA Server Profile on page 355.

Related Links

Configure an AAA Server Profile on page 355

#### Configure an AAA Server Profile

First, configure an Extreme Networks RADIUS Server. See Configure an Extreme Networks RADIUS Server on page 354.

Extreme Networks devices can serve as RADIUS authentication servers and respond to 802.1X requests from other Extreme Networks RADIUS authenticators. The Extreme Networks RADIUS server can store user accounts locally or check user login credentials against user accounts stored externally on Active Directory or LDAP (lightweight directory access protocol) user database servers.

This task is part of the network policy configuration workflow. Use this task to configure an AAA server profile.

1. On the **Wireless** tab, select **Add Radius Server Group**.
2. Select **EXTREME NETWORKS RADIUS SERVER**.
3. Type a **RADIUS Server Group Name**.
4. Type an optional **RADIUS Server Group Description**.
5. Select the **User Database** type.
   - **Active Directory**: Select to enable an Extreme Networks RADIUS server to interoperate with an Active Directory server.
   - **LDAP Server**: Select to direct user account look-ups to one or more LDAP servers.
   - **Local Database**: Select to enable an Extreme Networks device to support authentication for local user groups.
6. Select the corresponding check boxes for the devices that you want to configure.
7. Select **CREATE NEW** to add a new AAA server profile.
   Alternately, select **USE EXISTING**, and then select an AAA server profile from the list.
8. Type a **Profile Name**.
9. Type an optional **Profile Description**.
10. Select the **User Database** type: **Active Directory**, **LDAP Server**, or **Local Database**.
    Available configuration options depend on the type of database that you select.
11. Type a **User Group Attribute**, and then select , and choose an existing user group.
12. Expand the **Additional Settings** section, and then enter the number of seconds for each response scenario.
    The **Additional Settings** section is not available for local databases.

13. Select **Enable Caching of Credentials** to improve performance across WAN links.
14. Type the number of seconds to retain the credential cache.
15. Complete the database-specific configuration options as follows:

| User database type | Configuration |
|---|---|
| Active Directory | See Add an Active Directory Server on page 357. |
| LDAP Server | See Add an LDAP Server on page 358. |
| Local Database | The Extreme Networks device that authenticates users directly, maintains the user database locally. |

16. Select **Security Options**, and then Configure AAA Server Security Options on page 356.
17. Select **Approved RADIUS Clients**, and then Add Approved RADIUS Clients on page 361.
18. Select **SAVE RADIUS SERVER**.

Continue configuring the RADIUS server profile.

Related Links

Configure an Extreme Networks RADIUS Server on page 354
Add an Active Directory Server on page 357
Add an LDAP Server on page 358
Configure AAA Server Security Options on page 356
Add Approved RADIUS Clients on page 361

#### Configure AAA Server Security Options

Configure an Extreme Networks device as a RADIUS Server.

This task is part of the network policy configuration workflow. Use this task to add increased security to the AAA Server Profile. For more information, see Configure an AAA Server Profile on page 355.

**Note**
Default certificates are intended to be used for testing only.

1. Select an **Authentication Protocol** from the drop-down list.
   - **TLS** requires mutual authentication using client-side certificates. With a client-side certificate, a compromised password is not enough to break into TLS-enabled systems because the intruder still needs the client-side certificate. A password is only used to encrypt the client-side certificate for storage. Credentials are used for a one-time certificate enrollment. The certificate is sent to the RADIUS server for authentication.
   - **PEAP** encapsulates EAP within a potentially encrypted and authenticated TLS tunnel. The user must enter their credentials, which are sent to the RADIUS Server that verifies the credentials, and authenticates them for network access.
   - **TTLS** extends TLS. The client can, but does not have to, be authenticated via a CA-signed PKI certificate to the server. This greatly simplifies the setup procedure since a certificate is not needed for every client.
   - **LEAP** uses dynamic WEP keys and mutual authentication between the client and RADIUS server. Uses an authentication protocol in which user credentials are not strongly

protected and are easily compromised. Users who absolutely must use LEAP should do so with sufficiently complex passwords.

**Note**
The WEP protocol is no longer effective for securing wireless networks. For security reasons, WEP configuration is no longer available in the UI. If you require WEP for business continuity purposes, you can enable it via Supplemental CLI.

- **MD5** offers minimal security, is vulnerable to dictionary attacks, and does not support key generation. This method is commonly used in a trusted network.

2. Select a **Default Authentication Protocol** from the drop-down list.
3. Select the default certification authority digital certificate type.
4. Select the default server digital certificate type.
5. Select whether to verify the server certificate file.
6. Enter the client key file password.
7. Select whether to **Check common name in certificate against the user for TLS authentication**.
8. Select the authentication that has been assigned to a user.
9. If you **Enable Authentication**, the recommended value for the **Age Timeout for Active Session** is three times the value of the **Accounting Interim Update Interval** in the RADIUS Client.

   For example, if the Accounting Interim Update Interval is set to 600 seconds, set the Age Timeout for Active Session to 1800 seconds.

Continue configuring the server.

#### Add an Active Directory Server

First, configure an AAA server profile. See Configure an AAA Server Profile on page 355.

This task is part of the network policy configuration workflow. Use this task to add an Active Directory (AD) database to an Extreme Networks device acting as a RADIUS Server.

1. For Step 3, on the **Configure RADIUS Servers** page, to add an existing AD server, select  and choose an existing object, or to add a new one, select .
2. Type a **Name** for the AD server.
3. Type the name of the **Domain**, to which the RADIUS authentication server and the AD server both belong.

   (Range: 1–64 characters). Include parent domains, such as .com, .net, and .org.
4. Select **Auto** or **Manual**.

| Setting | Description |
|---|---|
| Auto | ExtremeCloud IQ (New) automatically populates the Active Directory Server and the base distinguished name (BaseDN) parameters.<br>Go to Step 9 on page 358. |
| Manual | Go to Step 5. |

5. From the drop-down list, choose a previously-defined IP object or host name for the **Active Directory Server** that contains the user accounts the RADIUS authentication server will authenticate.

   If you do not see the one that you need listed, select **New** and enter an IP object or host name.
6. Type the **BaseDN**—The starting point for directory server searches, and the point in the directory tree structure where the server stores user accounts.
7. Type a **Short Domain Name**.
8. Type the **Realm** name that corresponds to the user account location, which is often the same as the domain name.
9. Set the organizational unit (OU) where the Extreme Networks RADIUS server has privileges to add itself as a computer in the domain or leave it blank.

   **Note**
   By default, the RADIUS server attempts to add itself into **Computers** unless you specify a computer-ou here. If you do not want to give a device access to the Computers container, you can create your own OU and give the device user permissions to create computers (that is, to add itself) to the specified OU. For example, the computer OU might be `wireless/APs`.
10. Select **Enable TLS Encryption** to encrypt the user look-up requests that the Extreme Networks RADIUS server sends to the Active Directory server.
11. Select **NEXT**.
12. Select an existing **DNS Server**, or select to create a new one.
13. Select **NEXT**.

Continue configuring the RADIUS server.

Related Links

Configure an AAA Server Profile on page 355

#### Add an LDAP Server

First, configure an AAA server profile. See Configure an AAA Server Profile on page 355.

This task is part of the network policy configuration workflow. Use this task to add an Lightweight Directory Access Protocol (LDAP) database to an Extreme Networks device acting as a RADIUS Server.

1. On the **Configure RADIUS Servers** page, to use an existing LDAP server, select and choose an existing object, or to add a new one, select .
2. Configure the settings.

   See LDAP Server Settings on page 359

Continue configuring the RADIUS server.

Related Links

LDAP Server Settings on page 359
Configure an AAA Server Profile on page 355

**LDAP Server Settings**

**Table 140: Settings for LDAP servers**

| Setting | Description |
|---|---|
| Name | Type a **Name** for the new or cloned server. |
| LDAP Server | Specify an **IP Address** or **Host Name**. Select and choose an existing object, or to add a new one, select . |
| Description | (Optional)<br>Although optional, entering a description is helpful for troubleshooting and for identifying the server. |
| RADIUS User Base DN | Type the RADIUS user base distinguished name, or the starting point for directory server searches, such as cn=visitors, and the point in the directory tree structure under which the server stores user accounts in its database.<br><br>**Note:** ExtremeCloud IQ (New) supports up to 2000 users per user group. For more than 2000 users, you must separate the users into different user groups. |
| Bind DN Name | Type the LDAP client distinguished name used during the authentication part of an LDAP session, such as cn=users, cn=students, dc=southamerica, ou=student, and ou=school. |
| Bind DN Password | Type the password for the LDAP client distinguished name for use during the authentication part of an LDAP session. |
| Show Password | Select **Show Password** to see the password. |
| Communication | Select **LDAP** or **LDAPS** for the required communication protocol. |
| **Optional Settings** | |
| Filter Attribute | Enter required **Filter Attribute** for searching for elements below the baseObject. |
| Strip realm name from filter | Select the check box to disable the realm, which is commonly appended to a user name and delimited with an @ sign, from the filter. |
| Destination Port | (Required)<br>Enter the LDAP server **Destination Port**. |
| TLS Authentication/ Encryption | Select the check box to enable Transport Layer Security authentication and encryption, and configure the settings. |
| **TLS Authentication/Encryption** | |
| CA Certificate File | (Required)<br>Select the default certification authority digital certificate type from the list. |
| LDAP Client Certificate | (Required)<br>Select the default LDAP client digital certificate type from the list. |
| Client Key File | (Required)<br>Select the default client key digital certificate type from the list. |

**Table 140: Settings for LDAP servers (continued)**

| Setting | Description |
|---|---|
| Key File Password | Type the client key file password. |
| Show Password | Select the check box to see the password. |
| Verify Server | Choose how often the Extreme Networks device checks the relationship between a certificate and its server:<br>• **Try** (on first authorization or authentication)<br>• **Never**<br>• **Demand** (as required, on demand) |

*Configure an Extreme Networks RADIUS Proxy*

First begin configuring a RADIUS server group. See Configure a RADIUS Server Group on page 348.

This task is part of the network policy configuration workflow. Use this task to to configure an Extreme Networks device as a RADIUS proxy server.

1. On the **Configure RADIUS Servers** page, select **EXTREME NETWORKS RADIUS PROXY**.
2. Select the device to configure as a proxy.
3. Type a **Name** for the proxy.
4. Type a **Description**.

   Although optional, descriptions can be helpful when you are configuring or troubleshooting your network.
5. For the **Realms** section, see Configure a RADIUS Proxy Server Realm on page 360.
6. For the **Approved RADIUS Clients** section, see Add Approved RADIUS Clients on page 361.
7. For the **Realm Settings** section, see Configure Realm Settings on page 362.
8. Select **SAVE RADIUS PROXY**.

Related Links

Configure a RADIUS Server Group on page 348
Configure a RADIUS Proxy Server Realm on page 360
Add Approved RADIUS Clients on page 361
Configure Realm Settings on page 362

*Configure a RADIUS Proxy Server Realm*

First configure an Extreme Networks Device as a RADIUS proxy server. See Configure an Extreme Networks RADIUS Proxy on page 360.

You can add a postfix notation realm after a user name, separated by an "@" symbol, and the result resembles an email address domain name. Or you can add a prefix notation realm before a user name, with a backslash "\" separator. User names can also include multiple realms, for example `domain1.com\username@domain2.com` is a valid user name with two realms. Realms can be arbitrary text and do not need to contain real domain names, even though they can look like domains.

This task is part of the network policy configuration workflow. Use this task to configure realms for a RADIUS proxy.

1. On the **Configure RADIUS Servers** page, select **REALMS**.
2. Select **ADD A RADIUS SERVER GROUP** to display and configure the settings.

   See Configure a RADIUS Server Group on page 348.
3. Configure **Required Realms**.
   a. Select the **Default Realm** from the menu.
   b. Select **Strip the realm name from the proxied access requests** to remove the realm name from proxied access requests.
   c. Select the **RADIUS Server Group** from the menu.
4. To create a realm, select an existing realm and then select , or to add a new one, select ..
   a. Type the **Realm Name**.
   b. Select a RADIUS server group from the menu.
   c. Select **Strip the realm name from the proxied access requests** to remove the realm name from proxied access requests.
   d. Select **ADD**.
5. Select **SAVE RADIUS PROXY**.

Continue configuring the proxy server.

Related Links

Configure an Extreme Networks RADIUS Proxy on page 360
Configure a RADIUS Server Group on page 348

*Add Approved RADIUS Clients*

Configure an Extreme Networks device as a RADIUS proxy server. See Configure an Extreme Networks RADIUS Proxy on page 360.

This task is part of the network policy configuration workflow. Use this task to add one or more approved RADIUS clients to each configured realm associated with a RADIUS proxy server.

1. On the **Configure RADIUS Servers** page, select **APPROVED RADIUS CLIENTS**.
2. Select .
3. To use an existing **IP/Host Name/Network** for a client, select  and choose an existing object, or to add a new one, select .
4. Type the associated **Shared Secret** (password).
5. To see the password, select **Show Password**.
6. (Optional) Type a **Description**.

   Although optional, entering a description is helpful for troubleshooting and for identifying the approved RADIUS client list.
7. Select **ADD**.
8. Select **SAVE RADIUS PROXY**.

Next, see Configure Realm Settings on page 362.

Related Links

Configure an Extreme Networks RADIUS Proxy on page 360
Configure Realm Settings on page 362

*Configure Realm Settings*

Configure an Extreme Networks device as a RADIUS proxy server and create a realm.

- Configure an Extreme Networks RADIUS Proxy on page 360
- Configure a RADIUS Proxy Server Realm on page 360

This task is part of the network policy configuration workflow. Use this task to optimize the realm settings for a RADIUS proxy.

1. On the **Configure RADIUS Servers** page, select **REALM SETTINGS**.
2. Select a **User and Realm Name** format:
   - NAI (Network Access Identifier)—The standard syntax is `user@realm`.
   - Windows NT Domain—The standard syntax is `user1@example.com`.
   - SPN (service principal name)—The standard syntax is `serviceclass/host`.
   - AUTO—Extreme automatically applies a format.
3. Type the **Retry Delay**—The time interval between retries.
4. Type the **Retry Count**—The number of retries before declaring failure.
5. Type the **Dead Time**—The time elapse (in seconds) before declaring failure.
6. Select **Inject Operator-Name Attribute**.
   If you do not want to inject an operator-named attribute, clear the check box.
7. Select **SAVE RADIUS PROXY**.

Finish configuring the RADIUS proxy.

Related Links

Configure an Extreme Networks RADIUS Proxy on page 360
Configure a RADIUS Proxy Server Realm on page 360

## Configure VLAN Settings

This task is part of the SSID configuration workflow. Use this task to set the default user profile and configure the VLAN settings.

1. Go to **Configuration** > **Network Policies**
2. Select an existing network policy, and then select , or to add a new one, select .
3. After you save the **Policy Details**, select **NEXT** or **2 Wireless**.
4. Select an existing SSID, and then select , or to add a new one, select .
5. Scroll to **User Access Settings**, select the **Default User Profile**, and configure the settings.
6. Select **SAVE USER PROFILE**.

Continue the SSID configuration.

Related Links

User Profile Settings on page 315

*VLAN Object Settings*

Configure the following settings, and then select **SAVE VLAN**.

**Table 141: Settings for VLANs**

| Setting | Definition |
|---|---|
| Name | (Required)<br>Type a name for the new VLAN. |
| VLAN ID | (Required)<br>Type an ID for the new VLAN. |
| Apply VLANs to devices using classification | Select **Apply VLAN to devices for classification** to create VLANs that you can apply to specific devices based on their location.<br>To add a classification rule, select .<br>To specify an existing classification rule, select .<br>For more information, see Configure Classification Rules on page 291. |

Related Links

Configure VLAN Settings on page 362

*VLAN Group Object Settings*

VLAN groups combine multiple VLANs as a single common object. Configure the following settings, and then select **SAVE**.

**Table 142: Settings for VLAN group objects**

| Setting | Definition |
|---|---|
| Name | (Required)<br>Type a name for the new VLAN group object. |
| VLANs | (Required)<br>Specify individual VLANs or ranges. Indicate a range with a hyphen. Separate VLAN entries with commas, for example, 1-30, 100-200, 500.<br>Range: 1–4094 |
| Description | (Optional)<br>Type a description to identify the VLAN group. Although optional, descriptions can be helpful when you are troubleshooting your network. |

Related Links

Configure VLAN Settings on page 362

*Configure User Profile Security*

Use this task to apply IP or MAC firewall rules to a user policy when you configure VLAN settings, or when you configure a user profile object.

1. On **Create User Profile** page, select the **SECURITY** tab and turn on **Firewall Rules**.

2. To redirect a user device to an external web site, select **IP Firewall** and complete the following steps:
   a. Select .
   b. Type the **IP Firewall Name**.
   c. Select whether this firewall rule is for **Inbound Traffic** or **Outbound Traffic**.
   d. Select whether this firewall rule is used to **Permit** or **Deny** traffic.

      **Permit** enables traffic to traverse the firewall. **Deny** prevents the device from allowing traffic inside the firewall.
   e. Configure IP Firewall rules.
3. To determine how the device manages traffic based on source and destination IP addresses, select **MAC Firewall** and complete the following steps:
   a. Enter a name for the firewall rule.
   b. Select whether this firewall rule is for **Inbound Traffic** or **Outbound Traffic**
   c. Select whether this firewall rule is used to **Permit** or **Deny** traffic.
   d. Select an existing MAC Firewall Rule or select the plus sign to create a new rule.

      See Add MAC Firewall Policies on page 366.
4. Continue configuring the user profile, or select **SAVE USER PROFILE**.

Related Links

Add a User Profile on page 315
Configure User Profiles on page 495
Configure VLAN Settings on page 362

#### Add IP Firewall Rules

IP Firewall rules determine how devices manage traffic based on network or application services, and source and destination IP addresses.

Use this task to create IP firewall rules when you configure security for a user profile as part of network policy, or for a user profile object.

1. On the **SECURITY** > **IP Firewall** tab, select an existing IP firewall rule, and then select , or to add a new one, select .
2. Enter a **Name** for the new rule.
3. Enter an optional **Description**.
4. Select to add a new rule.
5. Select one or more network or application services.

   **Network Service** objects identify Layer 4 traffic by protocol and port number. Extreme Networks provides a number of predefined services. Select to create a new network service. For more information, see Configure Network Services on page 366.
   a. Select , and choose either **Network Services** or **Application Services**.

      You cannot select both.
   b. Select up to 100 items.
   c. Select **Add Service**.

6. For **Source IP**, select , and choose an **IP Address**, **IP Address Range**, **Host Name**, **Network**, or **Any**.

   Alternatively, select **New** to add a new IP address, IP range, host name, or network.

   **Note**
   If you select **Any**, you cannot select additional specific sources.

   a. To specify an IP address range:
      - For IPv4, use the format: starting_address–ending_address (e.g., 10.1.1.10–10.1.1.50)
      - For IPv6, use the format: starting_address–ending_address (e.g., 2001:db8::100–2001:db8::1ff)
7. For **Destination IP**, , one or more options: **IP Address**,**IP Address Range**, **Host Name**, **Network**, or **Any**.

   Alternatively, select **New** to add a new IP address, IP range, host name, or network.

   **Note**
   If you select **Any**, you cannot select additional specific destinations.

   a. To specify an IP address range:
      - For IPv4, use the format: starting_address–ending_address (e.g., 10.1.1.10–10.1.1.50)
      - For IPv6, use the format: starting_address–ending_address (e.g., 2001:db8::100–2001:db8::1ff)
8. Select the action the device performs when it receives traffic matching the source address-destination address-service.

   The firewall can perform the following actions:

   - **Permit**: Allows traffic to traverse the firewall.
   - **Deny**: Blocks traffic from traversing the firewall.
   - **Drop traffic between stations**: Drops traffic between stations if both stations are associated with one or more members of the same hive. This setting applies to unicast, broadcast, and multicast traffic that the device receives on an interface in access mode.
   - **NAT**: Translates the source IP address of a packet permitted to traverse the firewall to that of the mgt0 interface on the device.
9. Choose one of the following logging options from the drop-down list:
   - **Off**: Disables logging for packets and sessions that match the IP firewall policy rule.
   - **Session Initiation**: Log details about a session created after passing an IP firewall policy lookup.
   - **Session Termination**: Log details about a session matching an IP firewall policy termination.
   - **Both**: Log details after initiating and terminating a session.
10. Select **SAVE FIREWALL RULE**.

    As you continue to add firewall rules, each subsequent rule is positioned at the bottom of the list. Use the up and down arrows in the rules table to rearrange the position of rules to determine their application order.

Related Links

Configure Network Services on page 366

#### Configure Network Services

Network service objects identify Layer 4 traffic by protocol and port number. ExtremeCloud IQ (New) provides some predefined services and you can create custom network services to use when defining firewall policies, and QoS traffic classification and marking policies.

Use this task to configure a network service, as part of an IP Firewall policy for a user profile.

1. Select .
2. Type a **Name** for the service.
3. (Optional) Type a **Description** for the service.
4. Select a service idle timeout (for APs and routers only).

   This is the amount of time (in seconds) after which the device terminates an inactive session using this service.
5. Select an **IP Protocol Number**.

   The number of the protocol the service will use. Predefined services appear in the drop-down list, or you can configure a custom protocol.
6. Specify the destination **Port Number** or **Port Range** for the service.

   For services that use TCP or UDP, you can specify a single port number (e.g., 80) or a port range (e.g., 1024–65535) using a hyphen. The receiving device uses the port number or range to map the service to the appropriate processor. When you use a custom protocol, a port number is not required.
7. Select an **ALG Type**.

   ALG is supported for APs and routers only. If the service must use an ALG, select DNS, FTP, HTTP, SIP, or TFTP, from the list. Otherwise, leave this field empty.
8. Select **SAVE NETWORK SERVICE**.

Related Links

Add IP Firewall Rules on page 364

#### Add MAC Firewall Policies

MAC firewall policies determine how the device manages traffic based on source and destination IP addresses, and the actions (permit or deny) the device can take. When the policy contains multiple rules, the order of the rules affects how they are applied. Use this task to create a new rule.

Use this task to add MAC firewall policy objects and rules.

1. Select an existing IP firewall policy and then select , or to add a new one, select .
2. Enter a **Name** for the new policy.
3. Enter an optional **Description**.
4. Select  to add a new rule.

5. For **Source MAC**, select **Any**, an existing MAC OUI or the plus sign.

   If you choose to add a new **Source MAC**, select **MAC Address** or **MAC OUI** and perform the following:

   a. Enter a new name.
   b. Enter the **MAC Address** or **MAC OUI**.
6. For **Destination MAC**, select **ANY**, an existing MAC OUI or the plus sign.

   If you choose to add a new **Source MAC**, select **MAC Address** or **MA OUI** and do the following:

   a. Enter a new name.
   b. Enter the **MAC Address** or **MAC OUI**.
7. Select the action the device performs when it receives traffic matching the source address-destination address-service.

   The firewall can perform the following actions:

   - **Permit**: Allows traffic to traverse its firewall.
   - **Deny**: Blocks traffic from traversing its firewall.
8. Choose one of the following logging options from the drop-down list:
   - **Off**: Disable logging for packets and sessions that match the MAC firewall policy rule.
   - **Session Initiation**: Log session details about a session created after passing a MAC firewall policy lookup.
   - **Session Termination**: Log session details about a session matching a MAC firewall policy termination.
   - **Both**: Log session details after initiating and terminating a session.
9. Select **Save**.

As you continue to add rules to a policy, each new rule is positioned at the bottom of the list. Use the up and down arrows in the rules table to rearrange the position of rules to determine their application order.

Related Links

Configure User Profile Security on page 363

*Configure User Profile Traffic Tunneling*

You can enable the following types of GRE traffic tunneling for new and existing user profiles:

**Layer 3 Roaming**

Adjusts roaming thresholds so that a device disassociates with a wireless client that has roamed to it from another subnet and has either been idle for a period of time, or for which traffic is below a specified threshold.

**Identity-Based Traffic Tunneling**

Tunnels guest traffic directly to the network.

**Standard GRE Tunneling**

Tunnels traffic to non-Extreme Networks tunnel endpoints.

**Tunnel Concentrator**

Tunnels traffic to Extreme Networks Tunnel Concentrator.

Use this task to configure traffic tunneling when you configure security for a user profile as part of network policy, or for a user profile object.

1. On **Create User Profile** page, select the **TRAFFIC TUNNELING** tab, turn on **Traffic Tunneling (GRE)**.
2. Select an existing profile from the **Re-use Tunnel Policy** menu, and then select the type of tunneling.
3. **Layer 3 Roaming**:
   a. Specify a time period between 10 and 600 seconds.
   b. Specify a threshold number between 0 and 2147483647 packets per minute.
4. **Identity-Based Traffic Tunneling**:
   a. **Tunnel Source**: select a subnet from the drop-down list, or add a new subnet.
   b. **Tunnel Destination**: choose an IP address or host name from the drop-down list or add a new address or host name.
   c. **Tunnel Authentication**: type the password the AP uses to authenticate to the GRE termination point.
5. **Standard GRE Tunneling**:
   a. **Tunnel Destination**: choose an IP address or host name from the drop-down list or add a new address or host name.
   b. If you select **Tunnel Mode dot1q**, type, select, edit, or add the 802.1Q native VLAN ID.

      To add a VLAN ID, see Configure VLAN Settings on page 362.
   c. **Tunnel Mode Access Mode**: type, select, edit, or add the VLAN ID.

      To add a VLAN ID, see Configure VLAN Settings on page 362.
6. For **Tunnel Concentrator**, select the tunnel concentrator services to act as the Primary (required) tunnel destinations.

   You can add a new Tunnel Concentrator service, or edit an existing instance. For more information, see Single Tunnel Concentrator Services Settings on page 369 and Redundant Tunnel Concentrator Services Settings on page 370.
7. Continue configuring the user profile, or select **SAVE USER PROFILE**.

Related Links

Single Tunnel Concentrator Services Settings on page 369
Redundant Tunnel Concentrator Services Settings on page 370
Add a User Profile on page 315
Configure User Profiles on page 495
Configure VLAN Settings on page 362

**Single Tunnel Concentrator Services Settings**

**Table 143: Single Tunnel Concentrator**

| Field | Description |
|---|---|
| Name | **(Required)**<br>Type a name to identify the new Tunnel Concentrator service. |
| Description | **(Optional)**<br>Provide a description that might be helpful when troubleshooting. |
| Single Tunnel Concentrator | **(Required)**<br>Select this option to create a single Tunnel Concentrator without redundancy. |
| Tunnel IP Address/CIDR | **(Required)**<br>Type the IP Address for the tunnel (CIDR). |
| Gateway | **(Optional)**<br>Type the IP address of the gateway. |
| Native VLAN ID | **(Required)**<br>Type the Native VLAN ID.<br>The Native VLAN is untagged. |
| Device Tunnel Concentrator | **(Required)**<br>Select a Tunnel Concentrator from the menu. |
| Tunnel Port | **(Required)**<br>Select a port from the menu. |
| VLAN ID | **(Required)**<br>Type the VLAN ID.<br>**(Optional)** For an untagged VLAN, select the corresponding check box. |
| Bridge Port | **(Required)**<br>Select a bridge port for the tunnel from the menu. |
| AP Keepalive Interval (seconds) | Set the keepalive interval to send keepalives to tunnels that are not in use. |
| AP Keepalive Retries | Set the maximum number of times the AP resends a failed keepalive before it changes the tunnel status to inactive. |
| To add or edit broadcast or multicast control for the Tunnel Concentrator service, select **Broadcast/Multicast Control**. | |
| Add New Rule | Select **Add New Rule** and type an IP address to permit. |
| Add Pre-defined Rule | Select and choose a pre-defined rule from the menu. |
| Block Non- Essential Broadcast | Select or clear the check box.<br>Essential Broadcasts are ARP and DHCP |
| ARP Proxy | Select or clear the check box.<br>**Caution:** Disabling the **ARP Proxy** option can lead to undesired traffic. |

Related Links

Configure User Profile Traffic Tunneling on page 367

**Redundant Tunnel Concentrator Services Settings**

**Table 144: Redundant (Primary and Backup) Tunnel Concentrators**

| Field | Description |
|---|---|
| Name | **(Required)**<br>Type a name to identify the new Tunnel Concentrator service. |
| Description | **(Optional)**<br>Provide a description that might be helpful when troubleshooting. |
| Redundant Tunnel Concentrator | **(Required)**<br>Select this option to create a redundant Tunnel Concentrator. |
| Tunnel IP Address/CIDR | **(Required)**<br>Type the IP Address for the tunnel (CIDR). |
| Gateway | **(Optional)**<br>Type the IP address of the gateway. |
| VRRP Router ID | **(Required)**<br>Type the ID for the VRRP router.<br>ExtremeCloud IQ configures the same VRRP Router ID for both the primary and backup Tunnel Concentrators (range 1-255). The **VRRP Router ID** must be different for each cluster of VRRP devices. |
| Native VLAN ID | **(Required)**<br>Type the Native VLAN ID.<br>The Native VLAN is untagged. |
| Device Tunnel Concentrator | **(Required—Primary and Backup)**<br>Select a primary Tunnel Concentrator from the menu.<br>Select a backup Tunnel Concentrator from the menu. |
| Tunnel Port | **(Required—Primary and Backup)**<br>Select a port for the tunnel from the menu for the primary Tunnel Concentrator from the menu.<br>Select a port for the tunnel from the menu for the backup Tunnel Concentrator from the menu. |
| VLAN ID | **(Required—Primary and Backup)**<br>Type the VLAN ID for the primary and for the backup Tunnel Concentrators.<br>**(Optional)** For an untagged VLAN, select the corresponding check box. |
| IP Address | **(Required—Primary and Backup)**<br>Type the IP address for the primary and the backup Tunnel Concentrators. |

**Table 144: Redundant (Primary and Backup) Tunnel Concentrators (continued)**

| Field | Description |
|---|---|
| Bridge Port | **(Required—Primary and Backup)**<br>Select a bridge port for the tunnel from the menu for the primary Tunnel Concentrator.<br>Select a bridge port for the tunnel from the menu for the backup Tunnel Concentrator. |
| AP Keepalive Interval (seconds) | Specifies the interval at which the AP sends keepalive messages to the primary and backup tunnel concentrators. The AP sends keepalive only to tunnels that are not in use and listens for a response from each tunnel concentrator independently.<br>If the AP receives a response, it sets the tunnel status to **Active**. If no response is received within the interval, the AP retries the keepalive based on the configured **AP Keepalive Retries** value.<br>Possible values: 1 to 60 seconds<br>Default: 3 seconds |
| AP Keepalive Retries | Specifies the maximum number of retry attempts for a failed keepalive before the AP changes the tunnel status to **Inactive** for the primary or backup tunnel concentrator.<br>If the AP does not receive a keepalive response within the configured interval, it retries until the maximum retry count is reached. When the retry limit is exceeded, the AP marks the tunnel as **Inactive**. If a response is later received, the AP changes the tunnel status to **Active** and resets the retry count.<br>Possible values: 1 to 10 retries<br>Default: 5 retries |
| To add or edit broadcast or multicast control for the Tunnel Concentrator service, select **Broadcast/Multicast Control**. | |
| Add New Rule | Select **Add New Rule** and type an IP address to permit. |
| Add Pre-defined Rule | Select and choose a pre-defined rule from the menu. |
| Block Non- Essential Broadcast | Select or clear the check box.<br>Essential Broadcasts are ARP and DHCP |
| ARP Proxy | Select or clear the check box.<br>**Caution:** Disabling the **ARP Proxy** option can lead to undesired traffic. |

Related Links

Configure User Profile Traffic Tunneling on page 367

*Configure User Profile QoS*

Extreme Networks devices can apply QoS to traffic originating from members of user profiles to prioritize traffic by category, set rate limits and traffic forwarding rules for each traffic

class, and set the maximum traffic forwarding rate and scheduling weight at two levels: for individual users in a user profile and for all users to whom the user profile applies. Through the rate control and queuing profile, you define QoS policing rates and scheduling weights at the individual user level. In the **QoS** section in a user profile configuration, you define the rates and weights at the user profile level. Through the combined configuration of forwarding mechanisms and rate limits, you control how a device schedules traffic forwarding.

1. On the **QOS** tab, turn on **Quality of Service (QoS)**.
2. Configure the **Rate Limit per User Profile per AP** to set the aggregate rate limit for all the users in the user profile.
3. Select **Manage Rate Limit per Client**.
   a. Set the **Rate Limit Per Client** from 0 to 2000 Mbps (0-2000000 Kbps).
   b. Set a weight percentage for each of the seven traffic classes in **Traffic Queue Management Per User per AP**, and set other details as required.
   c. Select **Save**.
4. Type the **Scheduling Weight**.

   **Note**
   Devices forward traffic of a higher class and greater weight faster than traffic of a lower class and lesser weight.

5. Select a QoS classification system from the **Mark outgoing traffic using** list.

   Extreme Networks devices can apply priority and class mappings to outgoing traffic based on either of the standard QoS classification systems.
6. To add a marker map, see Configure Marker Maps on page 372.
7. Continue configuring the user profile, or select **SAVE USER PROFILE**.

Related Links

Configure Marker Maps on page 372
Add a User Profile on page 315
Configure User Profiles on page 495
Configure VLAN Settings on page 362

#### Configure Marker Maps

For outgoing traffic, you can define marker maps to map classes to priority numbers in standard classification systems (802.11e, 802.1p, and DSCP). After you define classifier and marker maps, you then define classifier and marker profiles that enable one or more of the methods defined in the maps. Finally, you associate those profiles with SSIDs or interfaces to apply the mappings to traffic arriving at or exiting those interfaces.

Use this task to configure marker maps for outgoing traffic. When you configure marker maps at the network policy level, you can reuse existing maps. Select the list, and in the dialog box,

select the check box of a map and choose **Select**. All fields are automatically populated with the information for the selected map.

**Note**
Deleting a marker map from the **Location Server** dialog box also deletes it from the **Common Objects** list. You can only delete a marker map if no other configuration object is using it. to see a list of configuration objects that reference a marker map, hover over the number in the **Used By** column for that map in the **Marker Maps** window in the **Common Objects** section.

1. Select an existing map, and then select , or to add a new one, select .

   If you are configuring an AP template object, skip to Step 2.
2. Enter a **Name** for the marker map.
3. Enter an optional **Description** for the map.
4. On the **802.1p Markers** tab, toggle **802.1p Markers** to **On**.

   The QoS marking table shows the mapping of classes to WMM® (Wi-Fi Multimedia™) queues and the 802.1p classification system (marked in the L2 frame header in Ethernet frames). You can modify these mappings if necessary.

   Extreme Network devices automatically include 802.11e priority marking in the L2 headers of wireless frames, so it is not included here as a configurable option.

   Depending on the classification systems used in the surrounding network, select the appropriate check boxes to map classes to one or both systems for outgoing traffic. A network policy can reference just one marker map.
5. On the **Diffserv** tab, toggle **Diffserv** to **On**.

   The QoS marking table shows the mapping of classes to WMM® (Wi-Fi Multimedia™) queues and the DiffServ codepoint marking system (marked in the L3 packet header) on outgoing packets. You can modify these mappings if necessary.

   **Note**
   If both 802.1p and DiffServ are enabled, only DiffServ takes effect.

Related Links

Configure User Profile QoS on page 371

*Configure an Availability Schedule*

Begin to Configure VLAN Settings on page 362.

You can make the user profile available for specific dates, days, and times by assigning defined availability schedules to the profile. Profile members can access the network through the device only during these scheduled times. When the user profile is inactive, the device blocks access to the network.

Use this task to enable the Availability Schedule feature and configure the settings when creating a user profile as part of a network policy.

1. On the **AVAILABILITY SCHEDULE** tab, turn on **Availability Schedule**.
2. Select  and configure the settings.

   See Schedule Settings on page 374.
3. Continue configuring the user profile, or select **SAVE USER PROFILE**.



**Note**
To apply your SSID availability schedule to a wireless network, you must activate it in the **Additional Settings** section of the Standard Wireless Networks configuration page. See Configure Enterprise SSID Authentication on page 319.

Related Links

Schedule Settings on page 374
Configure Enterprise SSID Authentication on page 319
Add a User Profile on page 315
Configure User Profiles on page 495
Configure VLAN Settings on page 362

#### Schedule Settings

**Table 145: Settings for a One Time Schedule**

| Setting | Description |
|---|---|
| Name | Type a name for the schedule. |
| Description | (Optional)<br>Type a description for the schedule. |
| One Time | Select to apply this schedule one time only. |
| Start Time | Use the **Start** and **Time** controls to specify the starting date and time for the schedule. |
| End Time | Use the **End** and **Time** controls to specify the end date and time for the schedule. |

**Table 146: Settings for a Recurring Schedule**

| Setting | Description |
|---|---|
| Name | Type a name for the schedule. |
| Description | (Optional)<br>Type a description for the schedule. |
| Recurring | Select to apply this schedule on an ongoing basis. |
| Recurrence | Select **Every Day**, or select **From** and use the menus to select the day of the week to start, and the day to end the recurrence. |
| Limit recurrence between | Select the check box to apply the schedule to a specific date range. Use the controls to specify the start and end dates. |

Related Links

Configure an Availability Schedule on page 373

*Configure User Profile Client SLA*

Service-level agreements (SLAs) are contracts that specify the performance parameters within which a network service is provided.

Extreme Networks devices monitor client throughput and take action if the actual throughput is below the defined target minimum level. Use this task to enable client SLA settings for the user profile.

1. On the **CLIENT SLA** tab, turn on **Client SLA**.
2. Use the **Targeted minimum throughput** slider bar to adjust the minimum throughput level.
3. Select **Log** to generate a log entry about the performance sentinel violation.
4. Select **Boost Airtime** to increase the airtime available to clients so they can reach their targeted minimum throughput level.
5. Select both **Log** and **Boost Airtime** to combine the previous two actions.

   **Note**
   Using just the Log option to see if wireless clients throughout the corporate network are SLA-compliant is useful even without the Boost Airtime option. When clients do not get the expected level of throughput, you can see the results in graphs in the ExtremeCloud IQ (New) SLA reports. For Extreme Networks devices with non-compliant clients, you can drill down in the graph to see an SLA report for each client and determine why it is not meeting the SLA. If you conclude that the devices are oversubscribed, you can add more devices in that area to improve client throughput.

6. Continue configuring the user profile, or select **SAVE USER PROFILE**.

Related Links

Add a User Profile on page 315
Configure User Profiles on page 495
Configure VLAN Settings on page 362

*Configure User Profile Access Restrictions*

Use this task to configure access restrictions (date and time limits) for users based on their assigned user profiles. This is particularly helpful when you manage non-employee guest users, such as visitors, VIPs, and contractors.

1. On the **DATA/TIME LIMIT** tab, turn on **Access Restrictions**.
2. Select **Time Limit**.
   a. Select the limit in minutes, hours, days, or weeks (the number of minutes in a number of hours, or hours in days, or days in weeks).
   b. Select how to define an hour (either a fixed or rolling time window).
3. Select **Data Usage Limit**.
   a. Configure a data usage limit (in MB or GB).
   b. Limit the duration to days, weeks, or months.

c. Select how a day is measured (either a fixed or rolling time window).

4. Continue configuring the user profile, or select **SAVE USER PROFILE**.

Related Links

Add a User Profile on page 315
Configure User Profiles on page 495
Configure VLAN Settings on page 362

## Apply Different User Profiles to Clients and User Groups

Before you can apply different user profiles, configure the SSID for the network. For more information, see Configure the SSID for a Standard Wireless Network on page 308.

With user-profile assignment rules, you can assign clients to user profiles that match all configured conditions. The available conditions are as follows:

- Advanced Guest Policy
- Client OS Type
- Client MAC Address
- Client Location
- Schedule
- Cloud Config Group

This task is part of the network policy configuration workflow. Use this task to apply different user profiles to clients and user groups as part of a network policy.

1. Go to **Configuration** > **Network Policies**.
2. Select an existing policy, and then select , or to add a new one, select .
3. After you save the **Policy Details**, select **NEXT** or **2 Wireless**.
4. Under **User Access Settings**, select **Apply a different user profile to various clients and user groups**.
5. To choose an existing user profile, select  and choose an existing object, or to add a new one, select .
6. To add an existing user profile assignment rule, select .
   a. Select one of the existing rules.
   b. Select **Link**.
7. (Optional) To add a new user profile assignment rule, select .
   a. Type a **Name** for the user profile assignment rule.
   b. Type a **Description**.
   c. Select , and choose a category.
   d. Complete the configuration for the selected category.
      See Configure Classification Rules on page 291.

   You can add multiple assignment rules to create more granular control.
8. Select **SAVE**.

Related Links

Configure the SSID for a Standard Wireless Network on page 308
Configure Classification Rules on page 291

## Customize Advanced Access Security Controls

This task is part of the network policy configuration workflow. Use this task to configure and manage the cryptographic keys used to encrypt Wi-Fi traffic during the four-way handshake authentication process between an AP and clients, and to manage and set up Pairwise Transient Keys.

1. Go to **Configuration** > **Network Policies**.
2. Select an existing policy, and then select , or to add a new one, select .
3. After you save the **Policy Details**, select **NEXT** or **2 Wireless**.
4. Select an existing SSID, and then select , or to add a new one, select .
5. Expand the **Additional Settings** section.
6. For **Advanced Access Security Controls** (802.11w, Authentication timeout options), select **CUSTOMIZE**.
7. Configure the settings:

**Table 147: Settings for Advanced Access Security Controls**

| Setting | Description |
|---|---|
| **Advanced Authentication Options** | |
| Generate new Group Master Key (GMK) after | Type the time interval, after which the system generates a new GMK. Select the unit of time (seconds, minutes, hours, or days) from the list.<br>The GMK is a large random number that an Extreme Networks device chooses. From the GMK, the device derives a GTK (Group Temporal Key), which it then sends to all associated clients within EPOL-key messages. The Extreme Networks device and clients use the GTK to encrypt and decrypt broadcast or multicast traffic transmitted between themselves. |
| Generate New Group Temporal Key (GTK) after | Type the time interval, after which the system generates a new GTK. Select the unit of time (seconds, minutes, hours, or days) from the list.<br>The wireless client and Extreme Networks device use a GTK to encrypt to and decrypt broadcast and multicast traffic transmitted between themselves. A GTK is a temporal key that an Extreme Networks device derives from a GMK (Group Master Key) by performing a cryptographic hash on the concatenation of the GMK, a nonce, and the MAC address of the Extreme Networks device. The Extreme Networks device then sends the GTK to all associated clients within EAPOL-Key messages. |

**Table 147: Settings for Advanced Access Security Controls (continued)**

| Setting | Description |
|---|---|
| GTK Timeout Period | Type the time interval (in Milliseconds) that the device waits for client replies during the handshake process.<br>To accommodate clients that have shorter or longer timeout values, you can change this to a value from 100 (the standard timeout value) to a maximum of 8000 milliseconds. |
| Number of GTK Retries | Type the maximum number of times the device will retry sending GTK messages. |
| Generate a new Pairwise Transient Key (PTK) after | Select to enable PTK rekeying, and enter a value between 10 and 50,000,000 seconds (~231 days).<br>If you enable PTK rekeying, an interval between 2 and 10 minutes (120 and 600 seconds) is the best practice, which is enough to thwart the known TKIP exploit. Enable this option only when you know that the clients using the SSID support it. In addition, you might need to configure PTK rekeying on the clients.<br><br>**Note:** There is a flaw in TKIP that allows an attacker to decrypt unicast packets sent from an access point to a wireless client, and then send the client-forged packets, possibly with the purpose of poisoning ARP or DNS caches. If you cannot transition to AES-CCMP—which is not susceptible to this attack—you can mitigate attacks against TKIP-encrypted data by setting the PTK (pairwise transient key) to rekey at short intervals. |
| PTK timeout period | Type the interval (in Milliseconds) that the device waits for client replies during the four-way handshake in which they derive a PTK for encrypting and decrypting unicast traffic.<br>To accommodate clients that have shorter or longer timeout values, you can change the value from 100 milliseconds (the standard timeout value) to a maximum of 8000 milliseconds. |
| Number of PTK retries | Type the maximum number of times the device will retry sending PTK messages. |
| Replay window | Type a window size, within which the device accepts replies to previously sent messages during four-way handshakes.<br>0 indicates that the device does not accept any messages other than a reply to the last message that it sent. You might want to accept replies to previously sent messages if there are clients that reply more slowly than the device retries sending it messages. |

**Table 147: Settings for Advanced Access Security Controls (continued)**

| Setting | Description |
|---|---|
| Local TKIP Countermeasure | (Available only when the encryption method is Auto-TKIP or CCMP (AES) or TKIP)<br>Select to enable the deauthentication of all clients when the local device detects message integrity check failures during TKIP operations.<br>If one key fails an integrity check, the discovery of such a failure suggests that other keys in current use might also be compromised. The cautious security stance is to deauthenticate all clients and stop using all existing keys immediately. When clients reauthenticate, they use newly generated pairwise and group primary and temporal keys. If this feature is disabled, the device continues to use existing keys and maintain currently connected clients after detecting MIC failures. |
| Remote TKIP Countermeasure | (Available only when the encryption method is Auto-TKIP or CCMP (AES) or TKIP)<br>Select to deauthenticate all previously authenticated clients when a client reports MIC failures during TKIP operations.<br>The distinction between the local and remote countermeasure options is where the discovery occurs:<br>• Local—A device discovered the failure.<br>• Remote—A client discovered and reported the failure. |
| Enable to refresh the GTK only when the rekey period elapses. | To disable GTK refresh when either the rekey period elapses or a client disassociates from the SSID, clear the check box. |

8. Select **SAVE**.

## Customize Wireless Network Optional Settings

Complete the Add a Network Policy on page 278 task.

When configuring an SSID, you can configure and apply radio rates, DoS prevention settings, traffic filters, and other options.

Use this task to configure the **Optional Settings** for a standard wireless network.

1. Go to **Configuration** > **Network Policies**.
2. Select an existing policy, and then select , or to add a new one, select .
3. After you save the **Policy Details**, select **NEXT** or **2 Wireless**.
4. Go to **Additional Settings** > **Optional Settings**, and then select **CUSTOMIZE**.
5. Customize Radios and Rates Settings on page 380.
6. Customize DoS Prevention Settings on page 380.
7. Customize Traffic Filters on page 381.
8. Customize the User Profile Application Sequence on page 382.
9. Customize Voice Enterprise Options on page 383.
10. Customize Wi-Fi Multimedia™ on page 384.

11. Customize Broadcast and Multicast Handling Settings on page 385.
12. Customize Client Related Network Settings on page 386.
13. Customize Other Options on page 387.
14. Select **SAVE OPTIONAL SETTINGS**.

*Customize Radios and Rates Settings*

Complete the Add a Network Policy on page 278 task.

By default, Extreme Networks devices advertise support for all rates. By setting specific rates, you can restrict access to just those clients that can support them. Use these controls to force clients to connect at higher data rates on an SSID, which can help increase average data transfer rates.

1. Go to **Configuration** > **Network Policies**.
2. Select an existing policy, and then select .
3. Select **NEXT** to open the **Wireless Network** page.
4. Go to **Additional Settings** > **Optional Settings**, and then select **CUSTOMIZE**.
5. Go to the **Radios and Rates** section.
6. Select a radio frequency and configure the basic (mandatory) and optional data rates per SSID.
7. Select **SAVE RATE SETTING**.
8. Repeat steps 6–7 for each radio frequency.

Continue customizing **Optional Settings** in the **Wireless Networks** configuration window. Select **SAVE OPTIONAL SETTINGS** to save your changes.

Related Links

Add a Network Policy on page 278
Customize Wireless Network Optional Settings on page 379

*Customize DoS Prevention Settings*

Complete the Add a Network Policy on page 278 task.

This task is part of a series for configuring the **Optional Settings** for a standard wireless network. Use this task to customize settings for broadcast and multicast handling. Use this task to configure defensive settings to protect against Denial of Service (DoS) attacks, and configure SSID access filters based on MAC addresses.

1. Go to **Configuration** > **Network Policies**.
2. Select an existing policy, and then select .
3. Select **NEXT** to open the **Wireless Network** page.
4. Go to **Additional Settings** > **Optional Settings**, and then select **CUSTOMIZE**.
5. Go to the **MAC-based Dos Prevention rules for** section.

6. Select an option and configure the settings.
   - **SSID**—Select to protect against DoS attacks at the MAC layer (Layer 2) on the radio channel that an AP uses for SSID access traffic. The settings for an SSID apply cumulatively to the total amount of Layer 2 traffic that an AP receives on the access channel for the SSID.
   - **Client**—Select to protect against DoS attacks at the MAC layer (Layer 2) on the radio channel that an AP uses for SSID access traffic. The settings in the MAC DoS configuration object apply to the total amount of Layer 2 traffic that an AP receives on the access channel for the SSID from a single MAC address.
7. Under **IP-based Dos Prevention rules for**, select **SSID** and configure the settings. This configuration protects against Denial of Service attacks at the IP layer (Layer 3) on the radio channel that an AP uses for SSID access traffic.

   The settings in the IP DoS configuration object apply cumulatively to the total amount of Layer 3 traffic that an AP receives on the access channel for the SSID.
8. **Enable MAC-Based filters** and select an option for the **Default Action**.
   - **Permit**—Enable traffic from clients that do not match one of the selected filters.
   - **Deny**—Block traffic from clients that do not match any of the selected MAC filters.

   This step makes the **Add MAC-Based Filters** section available.
9. Add Mac-based filters.
   a. Scroll to the **Add MAC-Based Filters** section, and and then select .
   b. Specify a MAC or a MAC Oui.
      - Select  and choose an existing MAC or MAC Oui.
      - Select  to add a new **MAC Address**, or **MAC Oui**.
   c. Select an **Action** from the menu.
   d. Select **ADD**.

Continue customizing **Optional Settings** in the **Wireless Networks** configuration window. Select **SAVE OPTIONAL SETTINGS** to save your changes.

Related Links

Add a Network Policy on page 278
Customize Wireless Network Optional Settings on page 379

*Customize Traffic Filters*

Complete the Add a Network Policy on page 278 task.

Select traffic filters to control which management and diagnostic services an AP may receive, and whether to allow traffic between clients connected to the AP.

This task is part of a series for configuring the **Optional Settings** for a standard wireless network. Use this task to customize optional traffic filter settings.

1. Go to **Configuration** > **Network Policies**.
2. Select an existing policy, and then select .
3. Select **NEXT** to open the **Wireless Network** page.

4. Go to **Additional Settings** > **Optional Settings**, and then select **CUSTOMIZE**.
5. Go to the **Traffic Filters** section.
6. Select or clear the following check boxes to permit or deny specific types of management and diagnostic access to the mgt0 interface, or to enable traffic between clients connected to the AP.
   - **Enable SSH**
   - **Enable Telnet**
   - **Enable Ping**
   - **Enable SNMP**
   - **Enable Inter-station Traffic**

   **Note**
   When an Ethernet interface is in access mode, stations can communicate directly with each other without sending traffic through the AP. In this case, the AP cannot control their traffic. However, the AP can block traffic between stations connected to an Ethernet interface and stations connected to a wireless interface through an SSID.

Continue customizing **Optional Settings** in the **Wireless Networks** configuration window. Select **SAVE OPTIONAL SETTINGS** to save your changes.

Related Links

Add a Network Policy on page 278
Customize Wireless Network Optional Settings on page 379

*Customize the User Profile Application Sequence*

Complete the Add a Network Policy on page 278 task.

You can specify which profile you want to apply to user traffic. By default, an AP applies user profiles in the following order (the last one is the profile that the AP ultimately applies to user traffic):

- First, the AP applies the user profile indicated by attributes returned by a RADIUS server performing MAC authentication.
- Second, the AP applies the user profile specified in an SSID for traffic management. This overrides the first user profile.
- Third, the AP applies the user profile indicated by attributes returned from a RADIUS server when a captive web portal requires user authentication. This user profile overrides both the first and second profiles.

To give priority to a user profile by applying it later in the sequence, reorder the profiles.

This task is part of a series for configuring the **Optional Settings** for a standard wireless network. Use this task for configurations with different SSID components referencing different user profiles.

1. Go to **Configuration** > **Network Policies**.
2. Select an existing policy, and then select .

3. Select **NEXT** to open the **Wireless Network** page.
4. Go to **Additional Settings** > **Optional Settings**, and then select **CUSTOMIZE**.
5. Go to the **Choose User Profile Application Sequence** section, and then use the arrows to change the application sequence.

Continue customizing **Optional Settings** in the **Wireless Networks** configuration window. Select **SAVE OPTIONAL SETTINGS** to save your changes.

Related Links

Add a Network Policy on page 278
Customize Wireless Network Optional Settings on page 379

*Customize Voice Enterprise Options*

Complete the Add a Network Policy on page 278 task.

Navigate to **Optional Settings CUSTOMIZE** under **Additional Settings** in the **Configure Standard Wireless Networks** window.

This task is part of a series for configuring the **Optional Settings** for a standard wireless network. Use this task to customize Voice Enterprise options.

**Note**
To enable Voice Enterprise or 802.11r, the SSID must be configured to use WPA2 key management.

1. Go to Go to **Configuration** > **Network Policies**.
2. Select an existing policy, and then select .
3. Select **NEXT** to open the **Wireless Network** page.
4. Go to **Additional Settings** > **Optional Settings**, and then select **CUSTOMIZE**.
5. Go to the **Voice Enterprise** section.
6. Select an option.
   - **Enable Voice Enterprise**—Select to enable all options that are required for full voice enterprise support.
   - **Custom**—Select and choose one of the following options:
     - **Enable 802.11k**: (Radio Resource Measurement of Wireless LANs): Select to enable the devices to monitor the RF environment and network performance to help manage network usage and client roaming.
       - **Enable dualband neighbor list**: Select to enable APs to monitor 2.4 GHz, 5 GHz, and 6 GHz bands at the same time to widen the search for a less-loaded AP channel.
       - **Max. neighbor APs**: Set the maximum neighbor APs to send to the client to reduce the computational resources required for 802.11k handover.
     - **Enable 802.11v**: (IEEE 802.11 Wireless Network Management): Select to enable network devices and clients to share information such as location and neighbor information.
     - **Enable forced disassociation**: Select to enable APs to send disassociate or deauthenticate frames for a variety of reasons per 802.11v.
     - **Disassociate after**: (If forced disassociation is enabled.) Range: 0 to 5 seconds.

- **SNR Checking**: (If forced disassociation is enabled.) Select to enable APs to consider signal-to-noise ratio to determine when to disassociate.
  - **Disassociate the Client**: : (If forced disassociation and SNR checking are enabled.) Select to enable APs to send disassociation frames to client devices.
  - **BSSID Transition Request**: (If forced disassociation and SNR checking are enabled.) Select to enable APs to send BSSID transmission management request frames to client devices.
- **SLA Checking**: (If forced disassociation is enabled.) Select to enable Extreme Networks APs to consider service level agreement performance thresholds to determine when to disassociate.
  - **Disassociate the Client**: : (If forced disassociation and SLA checking are enabled.) Select to enable APs to send disassociation frames to client devices.
  - **BSSID Transition Request**: (If forced disassociation and SLA checking are enabled.) Select to enable APs to send BSSID transmission management request frames to client devices.
- **Enable 802.11r**: (Fast BSS Transition): Select to optimize roaming by forcing stations to forward QoS state and encryption keys preemptively.

Continue customizing **Optional Settings** in the **Wireless Networks** configuration window. Select **SAVE OPTIONAL SETTINGS** to save your changes.

Related Links

Add a Network Policy on page 278
Customize Wireless Network Optional Settings on page 379

*Customize Wi-Fi Multimedia™*

Complete the Add a Network Policy on page 278 task.

Enable Wi-Fi Multimedia™ (WMM) to prioritize network traffic according to the settings.

This task is part of a series for configuring the **Optional Settings** for a standard wireless network. Use this task to enable WMM and customize the settings.

1. Go to **Configuration** > **Network Policies** .
2. Select an existing policy, and then select .
3. Select **NEXT** to open the **Wireless Network** page.
4. Go to **Additional Settings** > **Optional Settings**, and then select **CUSTOMIZE**.
5. Go to the **WMM** section, and then select **Enable WMM**.
6. Select and clear the following check boxes as required:
   - **Voice**—Select to enable admission control algorithms for voice traffic.
   - **Video**—Select to enable admission control algorithms for video traffic.
   - **Enable Unscheduled Automatic Power Save Delivery**—Select to enable stations to request queued traffic at any time, rather than receiving queued traffic scheduled with the beacon.

Continue customizing **Optional Settings** in the **Wireless Networks** configuration window. Select **SAVE OPTIONAL SETTINGS** to save your changes.

Related Links

Add a Network Policy on page 278
Customize Wireless Network Optional Settings on page 379

*Customize Broadcast and Multicast Handling Settings*

Complete the Add a Network Policy on page 278 task.

To reduce unnecessary airtime usage for multicast transmissions, a device can convert multicast frames to unicast frames under certain conditions or at all times, and can drop multicast frames when there are no group members present to receive them. Unicast traffic can increase the reliability of video delivery. If a wireless client does not receive a unicast frame and does not reply with an ACK, the AP will retransmit. Multicast traffic does not support wireless frame delivery confirmation.

This task is part of a series for configuring the **Optional Settings** for a standard wireless network. Use this task to customize settings for broadcast and multicast handling.

1. Go to **Configuration** > **Network Policies**.
2. Select an existing policy, and then select .
3. Select **NEXT** to open the **Wireless Network** page.
4. Go to **Additional Settings** > **Optional Settings**, and then select **CUSTOMIZE**.
5. Go to the **Broadcast and Multicast Handling** section, and then select one of the following **Convert IP Multicast to Unicast** options:
   - **Auto**: The device is enabled to convert multicast frames to unicast when the channel utilization or membership count conditions are met.
   - **Always**: The device makes the conversion unconditionally.
   - **Disable**: The device does not use the multicast-to-unicast conversion feature, but instead follows the standard 802.11 behavior for sending multicast frames.
6. Set the **Channel Utilization Threshold** from 1 to 100%.
7. Set the **Membership Count Threshold** from 1 to 30.
8. Select **Enable Non-Essential Broadcast Filtering** to reduce unnecessary broadcast and multicast traffic forwarding (such as AMRP, HSRP, LLC, and STP) from APs with no registered listeners.
9. Select **Enable Multicast Drop** to drop multicast and broadcast traffic, excluding frames for any of the selected protocols. With the exception of **MDNS**, by default, all protocols are selected and are therefore included in multicast and broadcast traffic. To exclude protocols in multicast and broadcast traffic, proceed as follows:
   - **DHCPv4**: Clear the check-box to drop Dynamic Host Configuration Protocol version 4.
   - **DHCPv6**: Clear the check box to drop Dynamic Host Configuration Protocol version 6.
   - **ARP**: Clear the check box to drop Address Resolution Protocol.
   - **IGMP-query**: Clear the check box to drop Internet Group Management Protocol queries.
   - **IPv6-Discovery**: Clear the check box to drop Internet Control Message Protocol router discovery messages.
   - **MDNS**: This check box is not selected by default and is therefore preset to drop multicast DNS frames. Select this check box to **include** multicast DNS frames in multicast and broadcast traffic.

Continue customizing **Optional Settings** in the **Wireless Networks** configuration window. Select **SAVE OPTIONAL SETTINGS** to save your changes.

Related Links

Add a Network Policy on page 278
Customize Wireless Network Optional Settings on page 379

*Customize Client Related Network Settings*

Complete the Add a Network Policy on page 278 task.

Use this task to define client usage parameters that control how devices in the SSID transmit data, how neighboring devices exchange information with each other, and the maximum number of clients that the SSID supports.

1. Go to **Configuration** > **Network Policies**.
2. Select an existing policy, and then select .
3. Select **NEXT** to open the **Wireless Network** page.
4. Go to **Additional Settings** > **Optional Settings**, and then select **CUSTOMIZE**.
5. Go to the **Client Related Network Settings** section, and then configure the settings:
   - **Maximum client limit**: Set the maximum number of clients that can associate with an SSID on a device.
   - **EAP Timeout** (Enterprise Security Mode Only): During the 802.1x authentication phase, in the event of an EAP retry due to packet loss or lack of response from the client, the AP can retry the EAP request. Some clients cannot properly handle fast retry timers, so this might need adjustment to facilitate fast recovery for bad RF environments.
   - **RTS threshold**: The RTS (request-to-send) threshold indicates the minimum packet size to trigger an RTS/CTS (request-to-send/clear-to-send) exchange. The purpose of this exchange is to reserve the medium and thereby reduce collision interference.
   - **Fragment threshold**: The fragment threshold indicates the minimum packet size to begin fragmenting packets before transmitting them. If there is a high level of interference, smaller packet sizes can reduce the need to retransmit packets and improve performance.
   - **DTIM settings**: Extreme Networks devices include delivery traffic indication messages (DTIM) in beacons at scheduled intervals. DTIMs are included in beacons according to the DTIM period that you set. Increase the DTIM setting to improve battery life or shorten it to deliver buffered broadcast and multicast traffic more frequently.
   - **Inactive client ageout**: Set the length of time to age out and automatically disassociate inactive clients.
   - **EAP Retries** (Enterprise Security Mode Only): After the EAP timeout, authentication fails and the client tries to reconnect per this value.
   - **Roaming cache update interval**: An Extreme Networks AP updates its neighbors about its currently associated clients. Neighboring APs use this information to update their roaming caches—if necessary—with the most up-to-date client information from their neighboring APs.
   - **Roaming cache ageout**: By default, an Extreme Networks device removes an entry from its roaming cache if it is absent from 60 consecutive updates from a neighbor. You can change the number of times an entry must be absent.

Continue customizing **Optional Settings** in the **Wireless Networks** configuration window. Select **SAVE OPTIONAL SETTINGS** to save your changes.

Related Links

Add a Network Policy on page 278
Customize Wireless Network Optional Settings on page 379

*Customize Other Options*

Complete the Add a Network Policy on page 278 task.

This task is part of a series for configuring the **Optional Settings** for a standard wireless network. Use this task to customize the **Other Options**.

1. Go to **Configuration** > **Network Policies**
2. Select an existing policy, and then select .
3. Select **NEXT** to open the **Wireless Network** page.
4. Go to **Additional Settings** > **Optional Settings**, and then select **CUSTOMIZE**.
5. Select **Ignore broadcast probe request** to enable Extreme Networks devices hosting this SSID to ignore probe requests from wireless clients.
6. Select **Hide SSID (Stealth mode)** to enable a simple but ineffective method to secure a wireless network; it hides the SSID (Service Set Identifier).

   **Note**
   This method provides very little protection against anything but the most casual intrusion efforts.

7. Select **FTM(11mc) Responder Support** to enable client devices to determine their distance from the AP.

   If the civic address, latitude, longitude, or altitude of the AP is configured, the AP advertises this information in the beacon.

   **Note**
   Enabling FTM (Fine Timing Measurement) 11mc causes a radio reset.

8. Select **Enable enhanced RNR** to enhance roaming for 6 GHz clients, or clear the check box to turn off this feature.

   If you select **Broadcast SSID Using** > **6 GHz radio**, ExtremeCloud IQ (New) enables this feature by default. To disable the feature, turn off the 6 GHz radio.
9. Select **SAVE OPTIONAL SETTINGS** to save your changes.

Finish configuring the network policy.

Related Links

Add a Network Policy on page 278
Customize Wireless Network Optional Settings on page 379

### Settings for Multi-Link Operation

Multi-Link Operation (MLO) is a core capability in Wi-Fi 7 that allows devices to simultaneously connect to and use multiple frequency bands (2.4 GHz, 5 GHz, and 6 GHz) at the same time. MLO supports various modes, including:

- **Simultaneous Transmit and Receive (STR):** The device transmits and receives data on multiple links at the same time.
- **Nonsimultaneous Transmit and Receive (NSTR):** The device can only transmit or receive on one link at a time, but it can switch between links quickly.

MLO is supported on the AP3020, AP3020X, AP3020W, AP4020, AP4020X, AP4020FX, AP4060, AP4060X, and AP5020 switches. To enable MLO, the following conditions must be met:

- Security for the SSID must be WPA3(SAE).
- The 802.11k protocol must be enabled.
- Transition Mode must be disabled.
- The 2.4 GHz, 5 GHz, and 6 GHz frequency bands must enabled simultaneously.

## Electronic Shelf Labels

Electronic Shelf Labels (ESL) are small battery-powered (e-paper) devices that use *electrophoretic display* technology to replace paper shelf labels. The technology creates an image by rearranging tiny microcapsules filled with black and white charged particles suspended in fluid, when voltage is applied. An ESL draws power only when the image changes (updated product or price information), so a battery can last from five to ten years.

An ESL system requires the following components:

- ESL tags, which are 2.4 GHz RF-based battery powered devices
- An ESL communicator, connected to a supported AP, used to communicate with the ESL tags
- A server that provides the configuration and updates to the ESL tags

Configure ESL in a device template or as an individual AP override.

### Supported APs

The following access points support ESL:

- AP305C
- AP410C
- AP4020
- AP5010
- AP5020

## Supported Vendors

Table 148 lists supported vendors and the supported communicators (**Hardware Type**).

**Table 148: Supported vendors and communicator models**

| Vendor | Communicator |
|---|---|
| Vusion Group (Formerly SES Imagotag) | APG2-USB-A<br>APUG-LR01-A |
| Hanshow | HS_C09979 |
| Solum | SLG-EN101U |

## Important Considerations for ESL Deployments

- An ESL server behind a NAT (Network Address Translation) or firewall is not supported.
- Do not make configuration changes during ESL programming and setup.

Related Links

Connect the ESL Communicator on page 389
Configure ESL in a Device Template on page 390
Configure ESL as a Device Override on page 390

## Connect the ESL Communicator

Use this task to connect an ESL communicator to a supported AP.

1. Prepare the AP device:
   a. Ensure that the access point is getting 3AT/3AT+ power.
   b. Connect the ESL communicator to the access point USB port.
   c. Ensure that the LED on the ESL communicator is red.
2. In ExtremeCloud IQ (New), Configure ESL in a Device Template on page 390 or Configure ESL as a Device Override on page 390.
3. Ensure that the LED on the ESL communicator is amber.

**Important**
**Troubleshooting Tips:**

**No LED light on ESL communicator**

Check the power supply. The AP requires 3AT/3AT+ power supply to work with a USB port.

**The LED continues to be red**

Check the AP logs to verify that ThinAP2 has started.

**The LED continues to be Amber**

Check the IP address of AP, the AP-ID, and the connectivity between the AP and the ESL server.

Related Links

Electronic Shelf Labels on page 388
Configure ESL in a Device Template on page 390
Configure ESL as a Device Override on page 390
ESL Settings on page 390

## Configure ESL in a Device Template

Use this task to configure ESL in a device template.

1. Select an AP template for one of the supported AP models.
2. Scroll down to the **USB Ports** section and select the **USB Port Mode** > **Electronic Shelf Label (ESL)**.
3. Configure the ESL Settings on page 390.

Related Links

Configure AP Templates on page 392
ESL Settings on page 390

## Configure ESL as a Device Override

Use this task to configure Electronic Shelf Labels as a device override.

1. From **Network Devices**, select a supported AP model.
2. From the left pane, expand **Action** and select **Configure Device**.
3. In the **CONFIGURATION** section, select **Interface Settings**.
4. Scroll down to the **USB Ports** section and select the **USB Port Mode** > **Electronic Shelf Label (ESL)**.
5. Configure the ESL Settings on page 390.

Related Links

ESL Settings on page 390

## ESL Settings

Settings for ESL are vendor and model-specific. First select the vendor and then select the ESL communicator model (**Hardware Type**).

**Table 149: ESL settings by vendor and communicator model**

| Setting | Description |
|---|---|
| **Vusion Group** and **APG2-USB-A** | |
| Server | The IP address of the ESL server. |
| Channel | The RF channel used for ESL communications. Set the channel to **Managed (Auto)** to have ExtremeCloud IQ (New) select the communications channel. |

**Table 149: ESL settings by vendor and communicator model (continued)**

| Setting | Description |
|---|---|
| Port | The port associated with the defined rule. To explicitly specify a port number, type the port number in this field. Traffic from this port is subject to the defined rule. |
| VLAN | The VLAN used to route ESL traffic. |
| **Vusion Group** and **APUG-LR01-A**<br>**Hanshow** and **HS_CO9979**<br>**Solum** and **SLG-EN101U** | |
| VLAN | The VLAN used to route ESL traffic. |

Related Links

Configure ESL in a Device Template on page 390
Configure ESL as a Device Override on page 390
Electronic Shelf Labels on page 388

## Configure Device Templates

Create or configure an existing network policy.

Use a device template to configure default port settings and other device functions for a specific Extreme Networks model using a visual diagram of the physical ports. After you configure a device template, you can:

- Assign various port types to the device ports, then apply the device template configuration settings to large numbers of devices of the same type.
- Apply different device templates to other devices in the same network policy.

**Note**
Each network policy has only one template corresponding to each device model. To update devices with different configurations for the same model, you must create a new network policy or modify an existing policy and then configure a new template.

1. To add an AP template to the network policy, select **2 Wireless** in the workflow and proceed to Configure AP Templates on page 392.
2. To add a switch template to the network policy, select **3 Switching** in the workflow and proceed to Configure a Switch Template on page 419.

   For legacy and Dell switch models, select **4 SR/Dell Switching** in the workflow.

Continue configuring the network policy.

Related Links

Configure AP Templates on page 392
Configure a Switch Template on page 419

## Configure AP Templates

Create a network policy for the APs. After you save the **Policy Details**, select **NEXT** or **2 Wireless**.

Create AP device templates with default settings for all APs, and settings that ExtremeCloud IQ (New) applies when APs are onboarded. You can then modify the default AP settings individually, as required. AP templates enable quick AP deployment, with most of the port settings already applied by the associated template. Some devices have extra possible configuration options, depending on the device model.

Use this task to configure an AP device template as part of a network policy.

1. On the **2 Wireless** page, select **Configuration Settings** > **AP Template**.
2. Select an existing AP Template, and then select , or to add a new one, select .

   To delete the selected template, select .
3. For a new template, type a **Name**, and for an existing template, edit as required.
4. Select the ports or interface icons on the template graphic.
   a. To select all of the ports and interfaces, choose **Select All Ports**.
   b. To deselect all of the ports and interfaces, select **Deselect All Ports**.
5. To **Assign** an Ethernet port profile, see Assign an Ethernet Port Profile on page 392.
6. To configure **Wireless Interfaces**, see Configure Wireless Interfaces for an AP Template on page 394.
7. To configure **Wired Interfaces**, see Configure Wired Interfaces for an AP Template on page 416.
8. To configure **SES-imagotag**, see Electronic Shelf Labels on page 388.
9. To configure **Advanced Settings**, see Configure AP Template Advanced Settings on page 418.
10. Select **SAVE TEMPLATE**.

Continue configuring the network policy.

Related Links

Configure Device Templates on page 391

*Assign an Ethernet Port Profile*

An Ethernet port profile lets you manage a variety of features such as port status (on or off), port usage (bridge access, bridge 802.1Q, or uplink), wired connectivity, and MAC authentication.

This task is part of the network policy configuration workflow. Use this task to assign a port profile to device ports.

1. Select an existing AP Template, and then select , or to add a new one, select . to create a new template.

   If you are configuring an AP Template object, go to Step 2.

2. To assign an existing port profile, select one or more Ethernet ports on the AP template graphic.
   a. Select **Assign**.
   b. Select **Choose Existing**.
   c. Choose any of the options from the **Port Type Assignment** list, and select **Save**.
3. To create a new port profile, select **Create New**.
   a. Type a **Port Name** for the port type.
   b. (Optional) Type a **Description** for the port profile.
   c. Select the **Port Usage** type:
      - **Uplink Port**: Use to connect the AP to the WAN.
      - **Access Port**: Use for an AP in client access mode, connected to a forwarding device like a switch that supports multiple VLANs.
      - **Trunk Port**: Use to connect the AP in bridge mode to a forwarding device, such as a switch that supports multiple VLANs.
4. For **Wired Connectivity**, enable **User Authentication**.
5. See Configure an External RADIUS Server on page 352 if you are not selecting an existing RADIUS Server Group.
6. Enable **MAC Authentication**, see Configure MAC Authentication on page 318.
7. For **QoS Settings**, see Configure Marker Maps on page 372.
8. For **User Access Settings**, to add a new User Profile, see Add a User Profile on page 315.
9. For **Traffic Filter Management**, see Configure Traffic Filters Policy Settings on page 305.
10. For **Port Settings**, see Configure LLDP/CDP Policy Settings on page 295.
11. For **Storm Control Settings**, see Configure Storm Control on page 433.

Continue configuring the AP template.

Related Links

Configure Port Types on page 436

#### Enable STP—Device Configuration

**Note**
Switch templates are supported only for Switch Engine and Extreme XOS devices.

Use this task to enable STP and configure the settings for a switch template.

1. Go to **Configure** > **Common Objects** > **Policy** > **Switch Template**.
2. Select an existing template, and then select , or select +
3. From the **Configuration** menu, select **Device Configuration**.
4. Toggle **STP (Spanning Tree Protocol)** to **ON**.

5. Select the STP Mode:
   - **STP**—The initial version of this protocol uses a single tree without regard to VLAN. After convergence (30-50 seconds), only the root bridge sends configuration Bridge Protocol Data Units (BPDUs).
   - **RSTP (Rapid STP)**—Like STP, RSTP uses single tree without regard to VLAN. After convergence (a few millisecond to 6 seconds), all switches send BPDUs every 2 seconds.
   - **MSTP (Multiple STP)**—Multiple Spanning Tree Protocol (MSTP) can map a group of VLANs into a single Multiple Spanning Tree instance (MSTI). Configure the MSTP settings.
6. Select a **Priority** for STP from the drop-down list.
7. Configure the **STP Timers**:
   - **Forward Delay**—This is the time the switch spends in the listening and learning state. The default is 15 seconds, and the range is 4 to 30 seconds.
   - **Max Age**—This is the maximum time period before a bridge port saves configuration BPDU information. The default is 20 seconds, the range is 6 and 40 seconds.
8. Select **SAVE**.

Continue configuring the Ethernet port.

*Configure Wireless Interfaces for an AP Template*

This task is part of the network policy configuration workflow. Use this task to configure the Wi-Fi 0, Wi-Fi 1, Wi-Fi 2, and IoT0 ports for an AP template, as part of a network policy.

You can also use this task if you are configuring an AP template object.

1. Select a **Device Model**, and then select an existing **Template**, or a default template.
2. Expand the **Wireless Interfaces** section.
3. Select an **Operating Mode**.
   - Mode 1: 2.4 GHz / 5 GHz (Full) / 6 GHz — Tri-Radio
   - Mode 2: Tri-Radio / 5GHz (Full) / 6 GHz — Full Band with Scan
   - Mode 3: 5 GHz (Low) / 5 GHz (High) / 6 GHz — Dual 5 GHz with 6 GHz
   - Mode 4: Tri-Radio / 5 GHz (Full) / 2.4 GHz — DBDC
   - Mode 5: 5 GHz (Low) / 5 GHz (High) / 2.4 GHz — Dual 5 GHz with 2.4 GHz
   - Mode 6: 6 GHz (Low) / 5 GHz (Full) / 6 GHz (High) — Dual 6 GHz with 5 GHz
4. Select either the **WiFi0**, **WiFi1**, **WiFi2**, **WiFi3**, or **IoT0** tab.

   **Note**
   - The **WiFi3** tab applies only to AP5020/AP5022/AP5060 models
   - The **IoT0** tab applies only to AP5010/AP5020 and AP3020/AP3020X/AP3020W models.

5. Set the **Radio Status** to **On**.
6. Select a **Radio Profile**—or an **IoT Profile** if applicable.

   You can also add a new Radio Profile or IoT Profile here, or clone and modify an existing profile.

7. Select the **Radio Usage** type.
   - Select **Client Mode** to configure a device for AP client mode radio usage, and to configure advanced features such as **Port Forwarding Rules** and **DHCP Server** settings. Choose a **Client Mode Profile** from the drop-down list. If required, you can configure a new Client Mode Profile or edit an existing profile.
   - Select **Client Access** for normal client operation. Optionally, select **Backhaul Mesh Link** for wireless portal and mesh backhaul operation.
   - Select **Sensor** for presence operation.
8. Continue configuring the AP template, or select **Save Interface Settings**.

Related Links

Configure AP Templates on page 392
Configure a Radio Profile on page 396
Configure IoT Profile Settings on page 410
Configure a Client Mode Profile on page 395

#### Radio Profiles

A radio profile contains settings for the radios in APs. The radios generally operate in two frequency bands: radio 1 (WiFi0) operates at 2.4 GHz, and radio 2 (WiFi1) operates at 5 GHz. WiFi2 supports only the 6 GHz band for client access. The number of radios and frequency bands supported vary by AP model.

In the **Radio Profiles** window, you can view, add, modify, and delete radio profile settings. You can also modify radio profile settings when you configure a device template. See Configure Device Templates on page 391.

The **Radio Profiles** table displays the following information:

- **Radio Profile Name**: The name assigned to a profile when it was created. It is a convenient reference when assigning radio profiles to the WiFi0 and WiFi1 interfaces for an AP.
- **Applied to Radio**: 2.4 GHz, 5 GHz, or 6 GHz.
- **Radio Mode**: 802.11a, a/n, ac, b/g, g/n, ax, or be.
- **Used By**: Shows the number of devices associated with this radio profile. Hover over any non-zero number in this column to see the associated device templates.

Related Links

Configure Device Templates on page 391
Configure a Radio Profile on page 396
Configure Wireless Interfaces for an AP Template on page 394

#### Configure a Client Mode Profile

This task is part of the network policy configuration workflow. Use this task to configure a Client Mode Profile as part of a network policy.

1. While configuring **Radio Usage**, select an existing Client Mode Profile, and then select , or to add a new one, select .
2. Type a **Client Mode Profile Name**.

3. (Optional) Type a **Description**.

   Although optional, descriptions can be helpful when you are troubleshooting your network.
4. The **Enable Local Web Page** option is enabled by default.

   The client mode AP activates a local SSID portal web page, which includes choices to select and connect the client mode AP WAN-side radio to a WAN Wi-Fi network. Clear this check box to configure other options for this profile.
5. Choose one of the following DHCP server options:
   - In the **DHCP Server Scope** field, enter the first IP address of the DHCP server range. The first IP address in this range is the IP address used to display the client mode SSID portal web page. Make a note of this first IP address for later reference.
   - In the **DHCP Server Scope** field, enter a single IP address to reserve a specific client (MAC address) to an IP. A DHCP reservation is a permanent IP address assignment. It is a specific IP address within a DHCP scope that is permanently reserved for a specific DHCP client. DHCP reservations on the AP support security on the local side of the Network Address Translation (NAT) and ensure that the client IP address does not change.
   - Set the **Advanced DHCP Server** slider button to **On**, then choose a pre-configured **DHCP Server and Relay** agent.
6. Toggle **Enable Port Forwarding** to **ON**, and then configure **Port Forwarding Rules** as follows:
   a. Select the plus sign to add a new port forwarding rule.
   b. Enter a description of how this rule is to be used (optional).
   c. Select a number for the outside port in the range of 1025-65535 (reserved ports cannot be used).
   d. Select a number for the local port in the range of 1-65535.
   e. Select **TCP**, **UDP**, or **Both** from the **Protocol** drop-down list.
   f. Select a **Host IP Address** for the internal device from the drop-down list, or select the plus sign to add a new address.
   g. Select **Add**.
7. Select **SAVE**.

Related Links

Configure Wireless Interfaces for an AP Template on page 394

#### Configure a Radio Profile

Use this task to create or edit a radio profile for 2.4 GHz, 5 GHz or 6 GHz device interfaces. For more information about radio profiles, see Radio Profiles on page 395.



**Note**
Extreme Networks provides defaults for each item in this section. The following steps are optional, except for the required radio profile **Name**.

1. In the device template, select **Device Configuration** and expand **Wireless Interfaces.**
2. Select the radio (2.4 GHz, 5 GHz, or 6 GHz).
3. Select an existing **Radio Profile**, and then select , or to add a new one, select .
4. Type the radio profile **Name**.

5. Type a **Description**.

   Although optional, descriptions can be helpful when you are configuring or troubleshooting your network.
6. Select the desired 802 specification from the **Support Radio Modes** menu.
7. Select a **Supported Power Mode**.

   **Note**
   Only applicable to AP5020/AP4020 and future WiFi 7 APs.
8. To set the optimal maximum power level, enter a value for **Maximum Transmit Power**.
9. To set the minimum power level, enter a value for **Transmission Power Floor**.
10. To set the maximum value to which the radio power can drop below the current power level, type a value for **Transmission Power Drop**.
11. To set the maximum number of wireless clients that can use the radio, type a value for **Maximum Number of Clients**.

    (Default: 100, Range: 1-255)

    A lower value permits fewer concurrent connections to the AP and provides a higher quality of service. A high number of concurrent connections to a radio might affect the quality of service. While 100 might be a bit high for a classroom setting, higher values are suitable for larger public spaces, such as cafeterias or gymnasiums. A higher setting is appropriate for APs that serve dense outdoor areas with frequent connections that quickly roam to other areas.
12. Select **SAVE RADIO PROFILE**.

Now that you have completed the basic configuration, you can modify the advanced radio profile settings. Remember to select **SAVE RADIO PROFILE** after changing the **Advanced Settings**.

Related Links

Radio Profiles on page 395
Configure Neighborhood Analysis on page 397
Channel Selection on page 398
Configure Dynamic Channel Switching on page 401
Optimize Radio Usage on page 402
Configure Radio Settings on page 404
Configure Backhaul Failover on page 406
Configure an Outdoor Deployment on page 407
Configure RF Interface Reports on page 407
Configure Client SLA Definitions on page 408
Configure WMM QoS Settings on page 409
Configure Sensor Mode Scan Settings on page 409
Configure IoT Profile Settings on page 410

#### Configure Neighborhood Analysis

First, Configure a Radio Profile on page 396.

Using background scanning, an AP divides a full background channel scan into several shorter partial scans so they do not interfere with the beacons sent by the AP. The scan takes less time than the beacon interval (100 TU by default), and is spread out over multiple beacon intervals until the AP scans all available channels. Full scans occur at admin-defined intervals, with a default of 10 minutes.

Background scanning is required for WIPS and Layer 3 roaming to function.

**Note**
ExtremeCloud IQ (New) automatically enables background scanning for all DFS enabled radios in the VIQ when you enable AI RRM. When you disable AI RRM, the system automatically disables background scanning.

This task is part of the Radio Profile configuration workflow. Use this task to configure neighborhood analysis (background scanning) settings.

**Note**
Extreme Networks provides defaults for each item in this section. The following steps are optional.

1. In the device template, select **Device Configuration** and expand **Wireless Interfaces.**.
2. Select the radio (2.4 GHz, 5 GHz, or 6 GHz).
3. Select an existing **Radio Profile**, and then select , or to add a new one, select ..
4. In the **Neighborhood Analysis** section, toggle **Background Scan** to **ON**.

   Background scanning is necessary for WIPS and Layer 3 roaming to function.
5. Set the interval between background scans of all radio channels.

   **Perform Background Scan Every**: The range is 1 to 1440 minutes (24 hours).
6. For **Skip Background Scan When**, specify when to skip background scans:
   - Select **Clients are connected** to enable an AP with connected clients to scan channels.
   - Select **Connected clients are in power save mode** to enable an AP to scan channels when connected clients are in power save mode.
   - Select **Network traffic with voice priority is detected** to prevent an AP from performing a background scan when voice traffic is detected.

   Voice traffic takes priority and is the least forgiving of slow or degraded connections.
7. Select **SAVE RADIO PROFILE**.

Related Links

Configure Channel Selection on page 400
Configure a Radio Profile on page 396

**Channel Selection**

2.4 GHz Radio Settings

The 2.4 GHz radio has between 11 and 14 channels, depending on the country code, but only three are completely non-overlapping (channels 1 - 6 - 11). Most wireless vendors recommend choosing one of the non-overlapping channels to avoid interference. However, in some cases,

especially in very dense deployments, it can be better to use four channels, particularly in European countries where there are more channels available.

You can set the channel model as three or four channels, depending on the selected region (USA or Europe). When you select Europe, you can modify the channel choices and set a different combination of channels. If you disable limiting channel selection, the AP uses Advanced Channel Selection Protocol (ACSP) to determine the best among all available channels in its region, using data about channel utilization, interference, CRC errors, noise floor, and the number of neighbors and their signal strength. The AP then selects the best channel available.

5 GHz Radio Settings

The 5 GHz radio mode is 802.11a, 802.11n, or 802.11ac. One of the key features in the 802.11n and 802.11ac standards is channel bonding, in which the radio bonds two or four adjacent 20-MHz channels into one 40-MHz or 80-MHz channel to increase the transmit data bandwidth. Unlike the 2.4 GHz radio band, the 5 GHz band has enough space for channel bonding. When you enable channel bonding on an AP whose region code is **FCC** and choose **40 MHz** or **80 MHz**, ACSP automatically chooses the primary channel based on the current RF environment and optimizes channel usage.

You can also use channel bonding in the European Community in conjunction with Dynamic Frequency Selection (DFS), which makes channels 52-64 and 100-140 available in addition to channels non-DFS channels 36-48. Without DFS enabled, channel bonding is not recommended for client access in the European Community because only the Unlicensed National Information Infrastructure (U-NII) lower band would be available (5.15-5.25 GHz; bandwidth: 100 MHz; channels 36 - 40 - 44 - 48) and there would not be enough space for three non-overlapping 40-MHz channels.

**Note**
The DFS option only takes effect when the AP is configured with the country code of a country complying with European Telecommunications Standards Institute (ETSI) or Federal Communications Commission (FCC) regulations. All Extreme Networks APs are certified to use DFS channels in the ETSI region and all are certified for the FCC region.

The 5-GHz radio frequency spectrum is partitioned U-NII bands. Extreme Networks devices support the following:

- U-NII Low: 5.15-5.25 GHz (bandwidth: 100 MHz; available in the U.S. and E.C.)

- U-NII Upper: 5.725-5.85 GHz (bandwidth: 125 MHz; available in the U.S.)

**Note**
When a hive contains some APs that do not support channel bonding and others that do, the dynamic channel selection process works as follows:

- Channel selection for backhaul mode: The APs that support only 20-MHz channels converge on the control channel that the other members use as part of their 40-MHz channel.
- Channel selection for access mode: The APs that support only 20-MHz channels avoid choosing either the control channel or extension channel that the other members are using as part of their 40-MHz channels.

6 GHz Radio Settings

Wi-Fi 6 is the next generation of Wi-Fi based on 802.11ax HE (high efficiency) technology. Currently, AP3000, AP4000, AP4020 and AP5000 devices support Wi-Fi 6 on 160 MHz channels.

Wi-Fi 7 is a tri-radio based on 802.11be technology on 320 MHz channels. Currently, only AP5020 devices support Wi-Fi 7 across three bands - 2.4 GHz (4x4:4), 5 GHz (4x4:4), and 6 GHz (4x4:4).

Related Links

Configure Channel Selection on page 400

#### Configure Channel Selection

First, Configure a Radio Profile on page 396.

This task is part of the Radio Profile configuration workflow. Use this task to make changes to the device channel width. The available settings depend on the **Supported Radio Mode** that you selected in the basic configuration section.

**Note**
Extreme Networks provides defaults for each item in this section. The following steps are optional.
Channel selection is dimmed and set to **Auto**. Perform channel selection at the device level.

1. In the device template, select **Device Configuration** and expand **Wireless Interfaces.**.
2. Select the radio (2.4 GHz, 5 GHz, or 6 GHz).
3. Select an existing radio profile, and then select , or to add a new one, select ..
4. Specify the **Channel Width and Exclusions**.
   a. To customize the display, select and clear the check boxes as desired:
      - **Show UNII Groups**
      - **Show Frequency Markers**
      - **Show Primary Channels**
      - **Show Preferred Scan Channels (PSC)**

5. To manually exclude channels, select a specific channel.
6. Enable **Dynamic Frequency Selection** to help maintain a balance between Wi-Fi performance and avoid interference with essential radio services.

   **Note**
   Dynamic Frequency Selection (DFS) settings do not apply to AP121, AP141, AP330, and AP350 access points that were shipped after 2 June 2016 and operate in the FCC domain.

   a. Select **Enable manual channel selection return** to return the affected radio to its original statically assigned DFS channel after a DFS event.
   b. Select **Enable ZeroWait DFS** to dedicate a single antenna chain to quickly identify a usable DFS channel. With ZeroWait DFS enabled, a 4x4 AP become a 3x3 AP.

      **Note**
      ZeroWait DFS is only available for 3- or 4-stream APs.

   c. Select **Enable Background Scan** to enable DFS to run background scans.
7. To manually set **Transmission Power**, select **Manual** and then use the slider to select a dBm setting.
8. Enable **Enable client transmission power control (802.11h)**.
9. To manually enable client transmission power control (802.11h), use the slider to select a dBm setting.
10. Enable **Limit Channel Selection** to limit channel selection to non-overlapping channels.
    a. Select the operating **Region** for the device from the drop-down list.
    b. For **Channel Model**, select 3 channels for USA and 4 channels for Europe.
    c. For **Limit Channel Selection**, USA defaults are 1, 6, and 11, and European defaults are 1, 5, 9.
11. Enable **Use the last known power and channel during the AP boot up process**.
12. Select **SAVE RADIO PROFILE**.

Related Links

Channel Selection on page 398
Configure Dynamic Channel Switching on page 401
Configure a Radio Profile on page 396

#### Configure Dynamic Channel Switching

This task is part of the Radio Profile configuration workflow. Use this task to enable Dynamic Channel Switching (DCS) to select and switch channels based on specified criteria.

1. In the device template, select **Device Configuration** and expand **Wireless Interfaces.**.
2. Select the radio (2.4 GHz, 5 GHz, or 6 GHz).
3. Select an existing radio profile, and then select , or to add a new one, select ..
4. Expand **Advanced Settings** and toggle **Dynamic Channel Switching** to **ON**.
5. Select **Automatically select and switch channels during specified time interval**.
   a. In the **From** field, enter the start time for the interval.
   b. In the **To** field, enter the end time for the interval.

c. In the **Do not switch channels if the number of connected clients exceeds** field, specify the number of connected clients.

   If the number of associated clients is equal to or less than the specified value, and if the AP finds a better channel, it can switch to a new channel. Associated clients lose their connections and must reconnect. If the number of clients exceeds the value, the AP does not switch to a new channel. When a client de-authenticates during the scheduled time range, the AP checks the number of clients against the value. If the number of clients does not exceed the value, the AP switches channels. If the number of clients still exceeds the value, the AP does not change channels.

6. Select **Switch channels anytime if RF interference exceeds the threshold**.
   a. In the **Interference Threshold** field, enter the value (%).
   b. In the **CRC Error Threshold** field, enter the value (%).
   c. Select **Do not switch channels if clients are connected**.
7. Select **SAVE RADIO PROFILE**.

Related Links

Optimize Radio Usage on page 402
Configure Dynamic Channel Switching on page 401

#### Optimize Radio Usage

First, Configure a Radio Profile on page 396.

Management frames such as beacons, and probe and association requests and responses, consume airtime that might otherwise be used to transmit user data.

This task is part of the Radio Profile configuration workflow. Use this task to minimize management traffic by using higher data rates, and suppressing and reducing probe and association responses under certain circumstances.



**Note**
Use caution when configuring radio optimization settings. When device configuration limits specific clients, there is a risk that end user clients will deny access to the WLAN. Extreme Networks provides default values for each setting. Modifying the radio configuration is optional and should be done with caution.

1. In the device template, select **Device Configuration** and expand **Wireless Interfaces.**.
2. Select the radio (2.4 GHz, 5 GHz, or 6 GHz).
3. Select an existing radio profile, and then select , or to add a new one, select ..
4. Choose **High data rates** to transmit management frames at the highest basic data rate specified in an SSID or **Low data rates** to use the lowest basic data rate.
5. Select **Suppress successive requests within the same beacon interval** to enable APs to suppress responses to repeated probe requests from the same client received within a single beacon interval.

6. Select **Suppress response to broadcast probes by** to reduce responses to broadcast probe requests by enabling only one of several SSIDs to respond, in rotation, or reduce responses from specific client device types.

   With this feature enabled, select a suppression method:

   a. Select **Allowing only one SSID to respond at a time** to enable a single SSID to respond at a time.
   b. For **Reducing responses to certain client device types** add a new MAC OUI.

      See Configure a MAC Object and MAC OUI on page 403.

   **Note**
   When high-density WLAN optimization is enabled, the suppression setting is disabled by default.

7. Enable **Band Steering** and select a mode from the menu.
8. Use the slider to set the **Allowed percentage distribution of 2.4 and 5.0 GHz clients**.
9. Enable **Client Load Balancing** and configure the threshold settings.

**Table 150: Load balance clients based on**

| Airtime | Number of clients |
|---|---|
| Ignore probe and association requests per device when threshold exceeds:<br>• CRC Error Rate<br>• RF Interference<br>• Average Airtime Per Client | Ignore probe and association requests from clients associated with other Extreme Networks devices until:<br>• Anchor Period Elapses<br>• Query neighbors about client load every |
| Ignore probe and association requests from clients associated with other Extreme Networks devices until:<br>• Anchor Period Elapses<br>• Query neighbors about client load every | |

10. Enable **Radio Load Balancing** and specify the **Number of Connection Attempts**.
11. Enable **Weak Signal Probe Request Suppression** and specify the **Signal-to-Noise Threshold** in dB.
12. Enable **Safety Net** and specify the time elapse, in seconds or minutes, before a device responds again to association requests after an overload incident.
13. Configure Configure Radio Settings on page 404.
14. Select **SAVE RADIO PROFILE**.

Related Links

Configure a MAC Object and MAC OUI on page 403
Configure Radio Settings on page 404
Configure a Radio Profile on page 396

#### Configure a MAC Object and MAC OUI

A MAC address is a 48-bit number typically written in hexadecimal notation that provides a unique address for each client device. An OUI is the first 24 bits of a MAC address.

After a MAC object is assigned to a device, it can be grouped to a specific hive. In a MAC firewall policy rule, you can determine which traffic to permit or deny based on the source or destination MAC address. In QoS traffic classification and marking policies, you can prioritize traffic based on the OUI.

Use this task to configure a MAC object and MAC OUI.

1. Select .
2. Select **MAC Address**.
3. Type a **Name**.
4. Type the **MAC Address**.
5. Select **SAVE**.
6. Select .
7. Select **MAC OUI**.
8. Type a **Name**.
9. Type the first six digits of the Mac address, for the **MAC OUI**.
10. Select **SAVE**.

Related Links

Optimize Radio Usage on page 402

#### Configure Radio Settings

First, Configure a Radio Profile on page 396.

You can configure whether you want to use long or short preambles, adjust the beacon period (or interval), and enable the detection of spoofed BSSIDs. For more information about radio settings, see Radio Settings on page 405.

This task is part of the Radio Profile configuration workflow. Use this task to configure the radio settings.

**Note**
Extreme Networks provides defaults for each item in this section. The following steps are optional.

1. Select the radio (2.4 GHz, 5 GHz, or 6 GHz).
2. Select an existing radio profile, and then select , or to add a new one, select .
3. Expand the **Advanced Settings** section.
4. Select **Auto (Short/Long)** to enable support for short preambles or **Long** to disable short preamble support.
5. Set the period during which APs send beacons.
6. Set the Guard Interval to 800 nanoseconds by deselecting **Enable Short Guard Interval**.
7. To no longer combine data frames into larger frames before transmission, clear the check box for **Enable MAC Aggregate Protocol Data Units**.
8. Select **Enable Frame Burst** so a wireless client will transmit a burst sequence of up to three packets without releasing control of the transmission medium.

9. Select **Enable Transmit Beamforming** to improve data transfer rates for directional signal transmission processing.
10. Select **Enable MU-MIMO** to enable multiple users to receive data using different simultaneous spatial streams from an AP transmit radio chain.
11. If you selected **Enable MU-MIMO**, set **Station Receive Chain** to **Auto** or **1**, which is the chain the AP uses to receive data from the wireless client.
12. If you are using 802.11ax radios, enable **ODFMA**.
13. If you selected **Enable ODFMA**, select **Uplink** or **Downlink**.
14. If you are using 802.11ax radios, enable **BSS Coloring**.
15. If you selected **Enable BSS Coloring**, enter the numerical value of the new BSS color the AP will transmit after surpassing the beacon threshold.
16. Select **Enable Target Wake Time** to enable an AP to minimize medium contention between stations, and to reduce the required amount of **time** that a station in the power-save mode needs to be **awake**.
17. Select **SAVE RADIO PROFILE**.

Related Links

Configure a Radio Profile on page 396

**Radio Settings**

Preambles

When you enable short preambles, the AP broadcasts support of short preambles and attempts to negotiate using them with clients. If a client also supports short preambles, the client and AP agree to use them. If a client only supports long preambles, then the AP automatically adjusts to accommodate it, and they agree to use long preambles instead. When you select long preambles, the AP and client both agree to use long preambles. Although a short preamble saves time and improves throughput, a long preamble allows more time for the receiver to tune into and synchronize with the transmitting radio, providing additional decoding accuracy in noisier environments.

Beacon Periods

APs broadcast beacons to all clients within range, and by default, send beacons every 100 TUs (approximately 10 times per second). If APs are in an area with lots of background noise, you might want to add more time between beacon broadcasts, or set an interval from 40 to 3500 TUs (about 24 times per second to about every 3.5 seconds).

Guard Intervals

A guard interval is the amount of time between transmissions to ensure that they do not collide. The default is 800 nanoseconds, which is still suitable for large areas, such as warehouses or outdoors, where the distances between points of reflection are great. For smaller areas, such as office spaces, you can use a shorter interval of 400 nanoseconds. Enabling this option in the right environment can improve data rates.

Aggregate MAC Protocol Data Unit (AMPDU)

AMPDU transmissions reduce overhead when the transmission channel is busy. When AMPDU is enabled, the AP combines data frames into fewer, larger frames before transmission, and

recognizes the format of larger frames when it receives them. Generally, enabling AMPDU increases performance.

Frame Bursts

Frame bursts enable a wireless client to transmit data at a higher throughput by using the inter-frame wait intervals to burst a sequence of up to three packets without releasing control of the transmission medium.

BSS Colors

A basic service set (BSS) is the cornerstone topology of any 802.11 network. The communicating devices that make up a BSS consist of one access point radio with one or more client stations. The BSS color is a numerical identifier of the BSS. 802.11ax radios are able to differentiate between BSSs using BSS color identifiers when other radios transmit on the same channel. If the color is the same, this is considered to be an intra-BSS frame transmission. In other words, the transmitting radio belongs to the same BSS as the receiver. If the detected frame has a different BSS color from its own, then the station considers that frame as an inter-BSS frame from an overlapping BSS.

Related Links

Configure Radio Settings on page 404

#### Configure Backhaul Failover

First, Configure a Radio Profile on page 396.

When **Backhaul Failovers** are enabled, the AP forms a mesh link with other hive members and can failover backhaul communications from Eth0 to a wireless interface if the Ethernet link goes down.

**Note**
Extreme Networks provides defaults for each item in this section. The following steps are optional.

This task is part of the Radio Profile configuration workflow. Use this task to configure backhaul failover.

1. In the device template, select **Device Configuration** and expand **Wireless Interfaces.**.
2. Select the radio (2.4 GHz, 5 GHz, or 6 GHz).
3. Select an existing radio profile, and then select , or to add a new one, select .
4. Enable **Backhaul Failover**.
5. Configure the following settings to define when to failover the backhaul link from Ethernet to wireless, and when to return the backhaul to Ethernet:
   a. In **Switch to Wireless Backhaul**, set how long the Ethernet link must be down to trigger a failover to the wireless link.
   b. In **Revert Back to Wired Backhaul**, set how long the Ethernet link must be up before the AP returns backhaul communications to Ethernet.

      Use the menu to specify the time in seconds or minutes.
6. Select **SAVE RADIO PROFILE**.

Related Links

Configure an Outdoor Deployment on page 407
Configure a Radio Profile on page 396

#### Configure an Outdoor Deployment

First, Configure a Radio Profile on page 396.

You can configure outdoor APs to communicate wirelessly with each other across a great distance by using a directional antenna for the backhaul link, while continuing to use omnidirectional antennas for access. However, you must make some adjustments to the radios to accommodate the longer transmission intervals. A Wi-Fi radio expects to receive an ACK for every transmitted Unicast frame. If it does not receive an ACK, it retransmits the frame. If the distance between the transmitter and receiver is too great, the ACK timeout period elapses before the ACK from the receiver reaches the transmitter, causing the transmitter to retransmit frames repeatedly until concluding that the frames are not reaching their target.

This task is part of the Radio Profile configuration workflow. Use this task to define the ACK timeout range between APs. By increasing the range, the radio increases the ACK timeout period accordingly.

1. In the device template, select **Device Configuration** and expand **Wireless Interfaces.**.
2. Select the radio (2.4 GHz, 5 GHz, or 6 GHz).
3. Select an existing radio profile, and then select , or to add a new one, select .
4. Set a distance (between 300 and 10,000 meters) over which to support the radio.
5. Select **SAVE RADIO PROFILE**.

Related Links

Configure RF Interface Reports on page 407
Configure a Radio Profile on page 396

#### Configure RF Interface Reports

First, Configure a Radio Profile on page 396.

ExtremeCloud IQ can periodically poll APs and collect RF interface-related data. ExtremeCloud IQ forces APs to adopt a shorter polling interval if CRC error, channel interference, or short-term polling thresholds are exceeded.

**Note**
Extreme Networks provides defaults for each item in this section. The following steps are optional.

This task is part of the Radio Profile configuration workflow. Use this task to configure RF interference reports.

1. In the device template, select **Device Configuration** and expand **Wireless Interfaces.**.
2. Select the radio (2.4 GHz, 5 GHz, or 6 GHz).
3. Select an existing radio profile, and then select , or to add a new one, select .

4. Set the level of CRC errors for polling.

   The default threshold is 20% for 802.11g/n, and 35% for 802.11a and 802.11ac. The range is from 15 to 60%.
5. Set the level of channel interference for polling.

   The default threshold is 20% for 802.11g/n, and 35% for 802.11a and 802.11ac. The range is from 15 to 60%.
6. Set the short-term average for polling.

   The range is 5 to 30 minutes.
7. Select **SAVE RADIO PROFILE**.

Related Links

Configure Client SLA Definitions on page 408
Configure a Radio Profile on page 396

#### Configure Client SLA Definitions

First, Configure a Radio Profile on page 396.

For each radio mode (or phymode)—11a, 11b, 11g, 11n, 11ac, 11ax—there are default settings for bit rate, success rate, and usage.

In most cases, the AP and client use several different rates to transmit and receive packets, changing rates as factors such as RSSI and packet loss change. To determine a common mid point to which various client scores can be compared, ExtremeCloud IQ provides three settings for each phymode:

**Rate**: This setting defines the transmission bit rated used by clients with healthy connectivity. For 80211a/b/g, rates are Mbps. For 802.11n, the rates are Mbps and modulation coding scheme (MCS).

**Success**: This setting defines the percentage of packets that you expect clients with healthy connectivity to transmit successfully (without retries) at the defined rate.

**Usage**: This setting defines the percentage of time that clients with healthy connectivity will transmit at the defined rate. The aggregated usage for the two bit rates must be equal to or less than 100%.

**Note**
To counter traffic congestion from clients with otherwise healthy Tx/Rx bit rates, APs can monitor client throughput and report SLA status to ExtremeCloud IQ. APs can also dynamically increase the amount of airtime for clients with a significant backlog of queued packets and improved throughput.

This task is part of the Radio Profile configuration workflow. Use this task to configure the client SLA definitions.

1. In the device template, select **Device Configuration** and expand **Wireless Interfaces.**.
2. Select the radio (2.4 GHz, 5 GHz, or 6 GHz).
3. Select an existing radio profile, and then select , or to add a new one, select .

4. To use the default settings, select one of the three options: **High Density (performance-oriented)**, **Normal Density**, or **Low Density (coverage-oriented)**.

   Alternately, to customize the settings for each option, select **CUSTOMIZE** and configure the settings on each tab.
5. Select **SAVE RADIO PROFILE**.

Related Links

Configure WMM QoS Settings on page 409
Configure a Radio Profile on page 396

#### Configure WMM QoS Settings

First, Configure a Radio Profile on page 396.

Wi-Fi Multimedia (WMM) classifies traffic into Voice, Video, Best-effort, and Background access categories, and provides mechanisms to prioritize each category at differing levels. **Contention Window Minimum**, **Contention Window Maximum**, and **AIFS** work together to determine the back-off time for each category. The first two define the minimum and maximum contention window parameters. When there is contention for access to the wireless medium, the AP calculates a random value between these two parameters. The higher the values, the longer the AP will back off during periods of access contention, resulting in longer delays for that traffic category. The lower the values, the shorter the back-off period, with shorter delays for traffic delivery. The AP adds the fixed arbitration interframe space (AIFS) back-off value to the first two values. The higher the setting, the longer the AP backs off, and the longer traffic is delayed during times of contention. The smaller the setting, the less time the AP backs off, resulting in shorter delays.

This task is part of the Radio Profile configuration workflow. Use this task to configure Wi-Fi Multimedia.

1. In the device template, select **Device Configuration** and expand **Wireless Interfaces.**.
2. Select the radio (2.4 GHz, 5 GHz, or 6 GHz).
3. Select an existing radio profile, and then select , or to add a new one, select .
4. If necessary, modify the default settings in the **Contention Window Minimum**, **Contention Window Maximum**, and **AIFS** columns.
5. If necessary, modify the default setting in the **TXOP Limit** column to determine how long bursts of traffic last before relinquishing the medium.
6. Set the **No ACK** flag to inform the recipient not to send ACKs of the frames it receives, which is useful for the video category where lost packets in streaming video go unnoticed, and retransmissions are unnecessary.
7. Select **SAVE RADIO PROFILE**.

Related Links

Configure Sensor Mode Scan Settings on page 409
Configure a Radio Profile on page 396

#### Configure Sensor Mode Scan Settings

First, Configure a Radio Profile on page 396.

These settings determine how your APs behave during the scanning process. You can specify how long a device scans each channel and which channels to scan.

**Note**
Dwell time defines how long the radio transmits on a specific channel frequency to scan client probe requests before moving to the next channel in the sequence. For presence data collection, setting the dwell time above the default value raises the throughput of data collected on each channel. Setting the minimum dwell time below the default value reduces latency but also reduces the throughput of data collected on each channel.

This task is part of the Radio Profile configuration workflow. Use this task to configure scan settings for sensor mode.

1. In the device template, select **Device Configuration** and expand **Wireless Interfaces.**
2. Select the radio (2.4 GHz, 5 GHz, or 6 GHz).
3. Select an existing radio profile, and then select , or to add a new one, select .
4. If necessary, modify the **Dwell Time**.
5. Deselect **Scan All Channels** and set individual channel numbers to collect client probe request data.
6. Select **SAVE RADIO PROFILE**.

Related Links

Configure a Radio Profile on page 396

#### IoT Profiles

The IoT (Internet of Things) is a network of interconnected smart devices. Smart devices are embedded with software, sensors, and network connectivity that enables them to collect and share data. The smart devices communicate with each other and with other internet-enabled devices, like smartphones and gateways, creating a vast network of interconnected devices that can exchange data and perform a variety of tasks autonomously.

ExtremeCloud IQ (New) uses IoT profiles to support IoT applications.

Related Links

Configure IoT Profile Settings on page 410
Configure the Thread Commissioner on page 414

#### Configure IoT Profile Settings

First, Configure a Radio Profile on page 396.

This task is part of the Radio Profile configuration workflow. Use this task to configure IoT applications for the following supported APs:

- AP5010/AP5020: Configure the AP as a backbone border router in a Thread network, as part of a network policy.

- AP3020/AP3020X/AP3020W: Enable Bluetooth (BLE) IoT configuration. The IoT radio is disabled by default on AP3020/X/W models. When enabled, only the **Multiple (Bluetooth)** IoT application is available.

1. In the device template, select **Device Configuration** and expand **Wireless Interfaces.**
2. Select the **IoTO** tab.
3. Toggle **Radio Status** to **ON**.
4. Select an existing profile, and then select , or to add a new one, select .
5. Configure the settings as described in Table 151 on page 411 or Table 152 on page 412.

**Note**
The AP3020/AP3020X/AP3020W does not support Single IoT Application. Configure settings as described in the Thread Profile Settings (Multiple IoT Applications) table.

6. Select **Save**.
7. (Optional) Select **Customize** to Configure the Thread Commissioner on page 414.

**Note**
Thread Commissioner configuration applies to AP5010/AP5020 only. This option is not available for AP3020/AP3020X/AP3020W models.

Related Links

IoT Profile Settings on page 411
Configure the Thread Commissioner on page 414

#### IoT Profile Settings

- Thread Profile Settings (Single IoT Application) (AP5010/AP5020 only)
- Thread Profile Settings (Multiple IoT Applications)

**Table 151: Thread Profile Settings (Single IoT Application)**

| Setting | Description |
|---|---|
| Name | Enter a **Name** for the profile. |
| IoT Application(s) Supported | Select **Single** from the menu. |
| Function | The default is **Thread**. |
| Application | The default is **Thread Gateway**. |
| Network Name | Enter a **Network Name** for the Thread network of an AP. Each AP participates in a Thread network identified with the PAN ID and EXT PAN ID configured for the Thread Profile. |
| Network Key | Enter the **Network Key** used to encrypt communication between devices in a Thread network. |
| PAN ID | The **PAN ID** (Personal Area Network Identifier) identifies the Thread network of the AP. Enter a 16-bit value for use in RF data transmissions between devices in a Thread network. |

**Table 151: Thread Profile Settings (Single IoT Application) (continued)**

| Setting | Description |
|---|---|
| EXT PAN ID | Enter a 64-bit value for use in RF data transmissions between devices in a Thread network. The **EXT PAN ID** must be unique. It is used for a more specific network identification. |
| Channel | Choose an IEEE 802.15.4 AP **Channel** number from the drop-down list (11-26). The default is channel 15.<br><br>**Note:**<br>Thread channel 25 is only supported if the country supports IEEE 802.11 channels 12, 13, or 14.<br>Thread channel 26 is only supported if the country supports IEEE 802.11 channels 13 or 14. |
| Default User Profile | Set the default VLAN user profile. Select an existing user profile to associate with this VLAN or create a new profile.<br>To create a new user profile, see Add a User Profile on page 315.<br><br>**Note:** Currently, only the VLAN of the associated User Profile is configured by the IoT profile. |
| Enable NAT64 | **Enable NAT64** allows an AP to perform IPv6 to IPv4 translations between the Thread and backbone networks. This option is selected by default. |
| Add domain to upstream DNS queries | To append the domain name to the host name before forwarding the DNS query, select **Add domain to upstream DNS queries**. |

**Table 152: Thread Profile Settings (Multiple IoT Applications)**

| Setting | Description |
|---|---|
| Name | Enter a **Name** for the profile. |
| IoT Application(s) Supported | Select **Multiple** from the menu. |
| **BLE Beacon** | |
| Application | Select the corresponding check boxes for the applications that you want to configure: **iBeacon**, and **Eddystone-url**. |
| iBeacon | Edit the settings as required and select **SAVE**. |
| Eddystone-url Beacon | Edit the settings as required and select **SAVE**. |
| **BLE Scan** | |
| Application | Select the corresponding check boxes for the applications that you want to configure: **iBeacon**, **Eddystone-url**, and **Generic**. |

**Table 152: Thread Profile Settings (Multiple IoT Applications) (continued)**

| Setting | Description |
|---|---|
| Destination | Select **Cloud Reporting**, **Batch Reporting**, or both.<br>Specify the interval in seconds.<br>For **Batch Reporting**, specify the destination URL.<br>To remove duplicate entries reported for the **Batch Reporting** interval, keeping only the latest entry for each BLE tag, toggle **Remove Duplicates** to **ON**.<br>**Note:** ExtremeCloud IQ always removes duplicate entries for **Cloud Reporting**. |
| iBeacon Filter | Edit the settings as required and select **SAVE**. |
| Eddystone-url Beacon Filter | Edit the settings as required and select **SAVE**. |
| Generic Filter | Edit the settings as required and select **SAVE**.<br>**Note:** If you select Custom for the **Vendor**, type the **Company Name** and the **Company ID**. |

Related Links

Configure IoT Profile Settings on page 410

**Thread Application**

Thread is an IP-based, low-power wireless protocol designed to facilitate connecting to and controlling IoT devices. Thread uses a mesh architecture, which supports more efficient and robust networking.

Elements of a Thread network include the following:

- **Thread Router**
  - Manages communication between devices within the Thread network.
  - Maintains a routing table to promote the efficient routing of messages.
  - Generally has no ability to communicate with networks outside the Thread network.
- **Border Router**
  - Extends the capabilities of a Thread Router to allow communication with networks outside the Thread network.
  - Acts as a gateway to external networks.
  - Performs NAT (Network Address Translation) to facilitate communication between external networks and the Thread network.
- **Backbone Border Router**
  - Extends the capabilities of a Border Router to allow communication between the Thread network and backbone networks.
  - Supports fail-over mechanisms to ensure network resilience.
  - Generally supports higher capacity and greater speeds compared to regular routers for faster and more reliable communication with external networks.

With ExtremeCloud IQ (New), assign an IoT Thread profile to an AP5010/AP5020 wireless interface to have the device function as a BBR (Backbone Border Router).

**Note**

ExtremeCloud IQ (New) IoT Thread application is supported on AP5010/AP5020 only. IoT Thread is not supported on simulated devices.

With ExtremeCloud IQ (New), the BBRs in the network negotiate and together elect one PBBR (Primary Backbone Border Router). The PBBR routes traffic between the Thread network and the Backbone network.

Although there can be multiple BBRs in a Thread network, only one can be PBBR at any time. The others act as secondary BBRs. If the PBBR is unreachable, failover occurs to a negotiated secondary BBR, which then becomes the new PBBR.

The IoT Thread profile allows for:

- Specifying key properties of the Thread network, such as its name, network key, PAN ID, Extended PAN ID, channel, and whether or not to enable NAT64.
- Optionally, you can specify the behavior of the Commissioner for the Thread network, including its credentials, timeout, and list of allowed devices.
- Optionally, you can configure the Default User Profile to be associated with the IoT Thread profile by applying only the VLAN.

Consider the following:

- IoT Thread profile configuration automatically takes precedence over BLE configuration. If BLE is configured and deployed, and later IoT Thread is configured and deployed, BLE becomes disabled and IoT Thread is enabled. If BLE configuration exists but has yet to be deployed, and then later IoT configuration is done and deployed, only the IoT configuration is pushed to the AP.
- Only one Commissioner can be active at any given time in a Thread network.

Related Links

IoT Profiles on page 410
Configure IoT Profile Settings on page 410
Configure the Thread Commissioner on page 414

#### Configure the Thread Commissioner

First, Configure IoT Profile Settings on page 410.

Use this task to define the behavior of the Thread Commissioner role, which can later be assigned to an AP5010/AP5020. The Thread Commissioner securely screens endpoint devices

attempting to join the Thread network. The Commissioner uses an Allow List to identify the IoT endpoint devices which have permission to join the Thread network.

**Note**
Only one Commissioner can be active at any given time in a Thread network.

1. Select an existing Thread Application profile, and then select , or to add a new one, select ..
2. Scroll down to **Commissioner**, and select **CUSTOMIZE**.
3. (Optional) Type the **Commissioner Credential** consisting of 6 to 250 alphanumeric characters.
4. (Optional) Set the **Commissioner Timeout** to a value in the range of 1-2000000 seconds.

   This value represents the ideal or known amount of time it takes for all the IoT endpoint devices defined in the Allow List to join the Thread network. The default is 120 seconds.

   **Note**
   If all of the IoT endpoint devices defined in the Allow List have joined the network but the Commissioner is still running because the Timeout value is set too high, you can force the Commissioner to stop running.

5. Under **Allow List of Thread-End Devices**, choose from the following actions:
   - Add devices to the Allow List either manually or in bulk, or using a combination of both methods.
     - To add devices manually, proceed to step 6 on page 415.
     - To add devices in bulk, proceed to step 7 on page 416.

       **Note**
       This method is available only after the Thread profile is saved.

   - Edit a device entry in the Allow List. Select the target entry, then select .

     Edit the entry according to steps 6.b on page 415 and 6.c on page 415, then select **Save**. When editing is complete, proceed to step 8 on page 416.
   - Delete entries in the Allow List. Select one or more entries, then select . Proceed to step 8 on page 416.
   - Download the entries in the Allow List to a csv file. Select .
   - Search for an entry in the Allow List. Enter a Joiner ID or PSK ID in the search field, then select .
6. Optionally, add devices to the **Allow List** manually, as follows:
   a. Select .
   b. In the **Joiner ID** field, enter a value consisting of 16 hex digits (excluding 16 "F"s) representing the device's EUI-64 (64-bit Extended Unique Identifier). Alternatively, enter * to admit any joiner.
   c. In the **Pre-Shared-Key for Device (PSKd)** field, enter a value for the shared password in the range of 6-32 alphanumeric characters (0-9, upper-case A-Y, excluding I, O, Q, and Z).

d. Select **Add**.
e. Repeat steps 6.a on page 415 through 6.d for each device added.
f. Proceed to step 8 on page 416.

7. Optionally, add devices in bulk. Select **Import** to upload a csv file containing the device details. From the **Import Allow List of Thread End-Devices** window, choose from the following actions:
   - Deselect the **Delete all Allow List entries prior to import** check box to append the IoT device entries in a csv file to the existing Allow List. By default, this option is selected, resulting in the removal of existing Allow List entries before device entries in a csv file are imported.
   - Select **Download an example CSV import file** to view the required format of device entries to successfully import the list.
   - Drag to the **Choose File** field a csv file containing device entries to be imported, or select **Choose** to upload a locally stored csv file.
   - Select **Submit** to upload and add the device entries from the csv file to the Allow List, or select **Close** to exit the window.
8. To save the settings, select **Save**, or select **Cancel** to close the window without saving settings.

To assign the Thread Commissioner role to an AP, go to **Manage** > **Devices** < *select an AP5010 or AP5020*> **Actions** > **Start Thread Commissioner**. If necessary, you can select **Stop Thread Commissioner** and reassign the Commissioner role to another AP.

Related Links

Configure IoT Profile Settings on page 410

*Configure Wired Interfaces for an AP Template*

Create or edit an AP template.

This task is part of the network policy configuration workflow. Use this task to configure wired interfaces on the AP. You can also use this task if you are configuring an AP template object.

1. Select a **Device Model**, and then select an existing **Template**, or a default template.
2. Scroll down to the **Wired Interfaces** section.
3. To activate an Ethernet port, toggle the **Interface State** to **ON**.
4. Select one of the following **Port Types**:
   - **Uplink Port**: Use when connecting the AP to the WAN. Use when dynamic trunk port configurations are desired. The Uplink Port automatically translates SSDI configurations as well as global native and Management ports to reduce the need for static trunk port configurations.
   - **Access Port**: Use when the AP is working in client access mode and is connected to a forwarding device, such as a switch that supports multiple VLANs.
   - **Trunk Port**: Use when connecting the AP in bridge mode to a forwarding device, such as a switch that supports multiple VLANs.

5. For **Native VLAN (read only)**: The native (untagged) VLAN assigned to frames that do not have any 802.1Q VLAN tags in their headers.

   By default, Extreme Networks devices use VLAN 1 as the native VLAN. To apply VLANs to devices using classification (uplink port only; not trunk ports), highlight the Ethernet port icons and see Configure Classification Rules for a Device Template on page 438.
6. For **Allowed VLANs (read only)**: Enter the VLANs—including the native VLAN—that you want the trunk port to permit.

   You can list the VLANs individually, separated by commas, or as a range of VLANs using a hyphen. Alternatively, you can enter the word `all` in this field to support all existing VLANs previously configured in the network policy (the default). To apply VLANs to devices using classification (uplink port only; not trunk ports), highlight the Ethernet port icons and see Configure Classification Rules for a Device Template on page 438.
7. For **Fabric Attach**: Select the add icon, enter the device's associated **VLAN ID** and select its **I-SID#** from the drop down.

   Use this field to configure a device connected to an existing Fabric Connect network. The device must already be physically connected to the Fabric Connect switch.
8. For **Transmission Type**, select one of the following:
   - **Auto**: The switch negotiates the best common duplex mode with the connected device.
   - **Full-Duplex**: Forces the switch to communicate with the connected device using full duplex communication.
   - **Half-Duplex**: Forces the switch to use half duplex communication.
9. Select the **Speed** the Ethernet port uses to communicate with the connected device.
10. Select **Green Ethernet** for the following supported AP models to enable Energy-Efficient Ethernet (EEE): AP4020, AP5020, AP5060U/D, AP_410C, AP_305C/CX, AP_510C/CX, AP_460C/S6C/S12C, AP_4000/4000U.

    The IEEE 802.3az standard, also known as EEE, introduces enhancements that enable physical layer transmitters to reduce power consumption during periods of idleness or low data activity. By enabling EEE, the network port can switch between active mode (during data transmission) and idle mode (when there is no Ethernet traffic), thereby consuming less power during idle or low activity states.
11. Select **LLDP** for devices to advertise their identities, status, and capabilities to each other.

    Devices can transmit data about themselves and receive transmitted data from other devices, but they cannot solicit and retrieve data from other devices.
12. Select **CDP** for devices to advertise an IP address that can send and receive SNMP traps.
13. Select **MCast Filter** to enable Multicast Rate Limiting on the interface for multicast/broadcast traffic, and configure **Multicast Rate Limit** to set the maximum rate (in Kbs) for incoming multicast traffic for the interface.
14. Optionally, set **USBNET** to **On** to activate the USB Port, and configure the **VLAN**.



**Note**
By default, the USB port will provide power when the AP is powered by 802.3 at the power source. If USBNET is enabled, it will be configured as an access port. The USBNET interface can be configured only for IQ Engine version 10.2r4 and later.

Continue configuring the AP template.

*Configure AP Template Advanced Settings*

ExtremeCloud IQ (New) can update device firmware and reboot the device during onboarding.

Use this task to configure **Advanced Settings** for an AP template.

1. In the AP template, select **Advanced Settings**.
2. To upgrade the device firmware when onboarding, toggle **Upload device firmware upon device authentication** to **ON** .

   If you have activated device firmware upgrading, select one of two options:

   - Update firmware to the latest version.
   - Upgrade to a specific device firmware version.

     If you choose this option, select the firmware version. To manage the list of firmware versions, select **ADD/REMOVE**.
3. To **Reboot after uploading**, toggle the setting **ON**.

   **Note**
   As a best practice, disable the reboot option when deploying devices in a meshed environment.

4. For **Antenna Location Type**, select a location.

   **Note**

   - You must have IQ Engine Version 10.2.2 or higher. The 6 GHz radio is supported Low Power Indoor (LPI) only.
   - Antenna Location Type does not apply to AP5020.
   - Because different radio tables are used, a full config push is required.

5. For **Supplemental CLI**, see Configure Supplemental CLI on page 437.
6. Select a **Country Code** from the menu.

   **Note**
   For Legacy World and EU SKU devices, the template country code assignment only takes place when a device is initially onboarded.

7. Enable **Override MGT0 MTU** to manually enter a maximum transmission unit (MTU) value, ranging from 100-1500 Bytes. Default value is 1500 Bytes.
8. Enable **POE Profile Override** (AP5010 only), and select the override option from the menu.

   Hover over the **i** to view the corresponding override table.
9. Select **SAVE TEMPLATE**.

Related Links

Configure Supplemental CLI on page 437
Configure AP Templates on page 392

## Configure a Switch Template

You can create a switch template during the network policy creation process, or at the device level after you have a network policy in place. Device-level changes to a switch template override settings in the network policy.

Create a network policy for the switch model. After you save the **Policy Details**, select **3 Switching/Routing**.

A switch template is a visual depiction of the physical ports on a switch. Configure how ports function by assigning port types and port usage settings to the template, and then applying the template to managed switches. The following steps describe how to create a switch template inside the network policy creation workflow.

Under **Device Configuration**, you can choose to override settings made under **Common Settings** in a network policy. The Switch Template Override feature allows you to create and manage switch templates based on common settings for SwitchEngine and ExtremeXOS. These common settings include STP, MAC Locking, IGMP, Extreme Loop Recovery Protocol Settings (ELRP), MTU, PSE, and Management Interfaces (Switch Engine only). The default values for these settings are defined within the common switch settings for each platform type. When you create a new switch template and enable the override option, you can customize device configuration settings that will override the network policy switch common settings. If the override option is disabled, the network policy common settings inherit the device configuration.

This task is part of the network policy configuration workflow. Use this task to configure a switch template as part of a network policy.

1. On the **3 Switching/Routing** page, select **Configuration Settings** > **Switch Templates**.
2. To edit an existing switch template, select the corresponding link in the table, or to add a new template, select  and select the switch model.
3. Type a **Name** for the template.
4. To make changes to the device configuration, enable **Override Policy Common Settings**.
5. For STP Configuration, see Configure Switch STP Settings on page 420.
6. For **MAC Locking Settings**, select to control the forwarding database for learned MAC address entries on a port.

   **Note**
   MAC Locking must also be enabled on a per-port basis.

7. Enable **IGMP Snooping** and configure the settings.
   - **Enable immediate leave**: Instructs the switch to remove a multicast host from the multicast forwarding table immediately upon receipt of a leave-group-membership message.
   - **Suppress redundant IGMP membership reports to optimize traffic**: Suppresses redundant IGMP membership reports from multiple hosts on a subnet. The switch sends a single report to the IGMP router, reducing traffic.

8. For **Extreme Loop Recovery Protocol Settings**, select to configure ELRP client periodic packet transmission for VLANs assigned to a port type to detect and prevent loops.

   This option enables an ELRP client and disables a port when a loop is detected on the applied access or trunk VLANs assigned to the port type.

   **Note**
   ELRP must also be enabled within the switch template.

9. Enable **DHCP Snooping**, and select **Enable drop rogue DHCP Packets action**

   Ports configured as trusted do not apply the drop action. By default, port types configured as Trunk Port are trusted.

10. For **MTU Settings**, enter a maximum transmission unit value for Ethernet interfaces.

    The MTU value determines the largest packet size that can be transmitted through your system.

11. For **PSE Settings**, toggle to **On** to configure maximum power thresholds to generate alerts to ExtremeCloud IQ about exceeding maximum power levels.
12. Select **Enable Flow Control** to manage the port data receive transmission rate.
13. For **Management Interface Settings**, select one of the following options:
    - **Infer from device** (Switch Engine/EXOS): Select when the switch supplies the management interface.
    - **VLAN Interface**: Select when the management interface is to be supplied by the management VLAN.
      - **Management VLAN**: Enter the VLAN to be used by the switch.
      - **Management IP Settings**: Select to enable DHCP on this interface.
14. For the **Port Configuration** section, see the following:
    - To configure **Instant Port Profile**, see Configure Instant Port Profiles on page 176.
    - To **Configure Ports in Bulk**, see Create a New Port Type on page 427
    - To **Configure Ports Individually**, see Configure Individual Ports on page 430
15. For **Advanced Settings**, see Configure Switch Template Advanced Settings on page 435.
16. Select **Save**.

*Configure Switch STP Settings*

First, create or modify a switch template as part of a network policy, or as a common object.

By default, STP is disabled. Use this task to toggle it on and configure the settings. Extreme Networks recommends that you enable STP.

1. In the switch template, select **Configuration** > **Device Configuration**.
2. Select one of the following modes:
   - **STP**: Uses a single spanning tree without regard to VLANs. After convergence, only the root bridge sends configuration BPDUs, and other switches only relay those BPDUs.
   - **RSTP**: Uses a single spanning tree without regard to VLANs. After convergence, all switches send BPDUs every two seconds in the event of a physical link failure.

- **MSTP**: Can map a group of VLANs into a single multiple spanning tree instance (MSTI). MSTP uses BPDUs to exchange information between spanning-tree compatible devices, to prevent loops in each MSTI by selecting active and blocked paths.
  - Under **MSTP Region**, enable the toggle to use the default the MAC address of the switch as the default region or the toggle to customize a defined MSTP region.
  - Enter a value from 0 to 65536 under **MSTP Revision**. The default is 3.

3. Select the **STP Bridge Priority**.

   Every switch taking part in spanning tree has a bridge priority. The switch with the lowest priority becomes the root bridge. If there's a tie, the switch with the lowest bridge ID number wins. The ID number is typically derived from a MAC address on the switch.
4. Set the following parameters for **STP Timers**:

   **Forward Delay**: The time the switch spends in the listening and learning state.

   **Max Age**: The maximum time before a bridge port saves its configuration BPDU information.

*Instant Port Profiles*

The Instant Port Profiles (IPP) feature in ExtremeCloud IQ (New) is an automated approach to configuring switch ports based on the connected devices. Instant Port Profiles streamline the management of network-connected devices, such as access points (AP), security cameras, and VoIP devices by dynamically provisioning the appropriate port configuration.

To configure IPP, perform the following tasks:

- Configure Instant Port Profiles
- Configure Instant Secure Port Profiles
- Configure an Instant Port Device Type

**Configure an Instant Port Device Type**

Configure a Network Policy with a switch template and an Instant Port Profile.

The Port Device type profile is part of the Instant Port Profile. When a device connects to a switch port, ExtremeCloud IQ (New) uses the criteria defined in the Instant Port device type to determine whether to apply the IPP to the port.

Universal Switches running Switch Engine and x435 models running ExtremeXOS version 32.x or later support the definition of up to 260 Instant Port device types for an IPP.

Use this task to configure device types for use with IPP.

1. In the **Create Instant Port Profile** dialog, under **Device Types**, select .
2. Configure settings.

   See IPP Device Type Settings on page 422.
3. Select **Save** to commit changes, or select **Cancel**.

#### IPP Device Type Settings

Configure the following Instant Port Profile (IPP) device type settings.

**Table 153: IPP Device Type Settings**

| Field | Description |
|---|---|
| Name | Type a **Name** for the device type profile. |
| Description | Optionally, type a **Description** of the device type profile. |

**Table 153: IPP Device Type Settings (continued)**

| Field | Description |
|---|---|
| Match Category | Select a **Match Category**. Options are:<br>• **MAC Learning** - Matches the device based on the MAC address learned on the port from untagged traffic. The match criteria can be an exact MAC, OUI-based MAC, or custom MAC mask format.<br>• **LLDP Src MAC** - Matches the device based on the source MAC of a LLDP PDU. The match criteria can be an exact MAC, OUI-based MAC, or custom MAC mask format.<br>• **LLDP Capability** - Matches the device based on the LLDP capability from the source LLDP PDU. Options are:<br>• **LLDP Src MAC + LLDP Capability** - Matches the device based on the source MAC of a LLDP PDU and the selected LLDP capability from the source LLDP PDU.<br><br>**Note:**<br>Instant Port will not function correctly if LLDP Transmit is disabled especially if LLDP-based matching is part of the Device Type profile.<br><br>If you choose **MAC Learning** or **LLDP Src MAC**, configure the following fields:<br>• **MAC Address/OUI**<br>◦ Select  and choose a MAC address.<br>◦ Select  to add a custom **MAC Address** or **MAC OUI**.<br>◦ Select  to edit a custom MAC Address or MAC OUI.<br>• **MAC Mask**<br>◦ Enter a custom MAC mask format.<br>◦ Select the **Edit MAC Mask** check box, then edit the entry in the MAC Mask field.<br><br>Instant Port uses Link Layer Discovery Protocol (LLDP) as one of its key device matching mechanisms, especially for:<br>• LLDP Source MAC<br>• LLDP Capability<br>• LLDP MAC + Capability<br><br>If LLDP is disabled on a port:<br>• The switch cannot receive LLDP PDUs from the connected device.<br>• The switch cannot transmit LLDP advertisements, which may be required for devices like VoIP phones to configure themselves (e.g., voice VLAN).<br>• LLDP-based match rules will fail, and the device may fall into the non-match action (e.g., default port type or non-forwarding VLAN).<br><br>However,LLDP Is Not Required If your Instant Port profile uses MAC-based matching only, then LLDP can be disabled and Instant Port will still work.<br>For example:<br><br>Match:<br><br>Category: MAC |

**Table 153: IPP Device Type Settings (continued)**

| Field | Description |
|---|---|
| | OUI: "00:1A:2B"<br><br>In this case, Instant Port relies on MAC Learning from untagged traffic and does not need LLDP.<br>If you choose **LLDP Capability**, use the drop-down menu to select one of the following options:<br>• Avaya Phone<br>• Gen Tel Phone<br>• Router<br>• Bridge<br>• Repeater<br>• WLAN Access Pt<br>• Docsis Cable Ser<br>• Station Only<br>• Other<br><br>If you select **LLDP Src MAC + LLDP Capability**, configure the parameters as described above. |
| **PORT USAGE** tab | |
| Port Usage | Select a **Port Usage** option, as follows:<br>• Access Port<br>• Trunk Port (802.1Q VLAN Tagging)<br>• Phone with a Data Port |
| **VLAN** tab | |
| VLAN | This field appears if **Port Usage** is configured as **Access Port**. Choose from the following actions:<br>• Select and choose a VLAN.<br>• Select to add a custom VLAN. Optionally, select the **Apply VLANs to devices using classification** check box.<br><br>To add a classification rule, select<br><br>To specify an existing classification rule, select .<br><br>For more information, see Configure Classification Rules on page 291.<br>• Select to edit a custom VLAN. |

**Table 153: IPP Device Type Settings (continued)**

| Field | Description |
|---|---|
| Native VLAN | This field appears if **Port Usage** is configured as **Trunk Port (802.1Q VLAN Tagging)**. Choose from the following actions:<br>• Select and choose a Native VLAN.<br>• Select to add a custom Native VLAN. Optionally, select the **Apply VLANs to devices using classification** check box.<br>To add a classification rule, select<br>To specify an existing classification rule, select<br>For more information, see Configure Classification Rules on page 291.<br>• Select to edit a custom Native VLAN. |
| Allowed VLANs | This field appears if **Port Usage** is configured as **Trunk Port (802.1Q VLAN Tagging)**. Enter the VLAN names using comma delimiters (vlan1,vlan2,vlan3...). |
| Voice VLAN (tagged) | This field appears if **Port Usage** is configured as **Phone with a Data Port**. Choose from the following actions:<br>• Select and choose a Voice VLAN.<br>• Select to add a custom Voice VLAN. Optionally, select the **Apply VLANs to devices using classification** check box.<br>To add a classification rule, select<br>To specify an existing classification rule, select<br>For more information, see Configure Classification Rules on page 291.<br>• Select to edit a custom Voice VLAN. |
| Data VLAN (untagged) | This field appears if **Port Usage** is configured as **Phone with a Data Port**. Choose from the following actions:<br>• Select and choose a Data VLAN.<br>• Select to add a custom Data VLAN. Optionally, select the **Apply VLANs to devices using classification** check box.<br>To add a classification rule, select<br>To specify an existing classification rule, select<br>For more information, see Configure Classification Rules on page 291.<br>• Select to edit a custom Data VLAN. |
| **STORM CONTROL** tab | |
| Broadcast | Select **Broadcast** to include traffic that is forwarded to all destinations simultaneously. |

**Table 153: IPP Device Type Settings (continued)**

| Field | Description |
|---|---|
| Unknown Unicast | Select **Unknown Unicast** to include traffic whose destination address does not appear in the forwarding database. |
| Multicast | Select **Multicast** to include traffic whose destination is a multicast address. |
| Thresholds | The default is **Packet Based**. |
| Rate Limit Type | The default is **PPS** (packets per second). |
| Rate Limit Value | Enter (in packets per second) when the switch should discard traffic of the selected types. |

Related Links

Configure an Instant Port Device Type on page 421

#### Instant Port Profile Switch Template Configuration

Choosing a Non-Forwarding VLAN

Choosing a Non-Forwarding VLAN is essential for detecting MAC addresses on switch ports. The non-forwarding VLAN will be used to detect attached devices and will not forward traffic. The non-forwarding VLAN cannot be utilized within a port type assigned to the switch. Only the VLAN attribute **Name** is supported by a non-forwarding VLAN.

**Choosing a Default Port Type**

Configure the Default Port Type settings, which serve as a baseline for other port configuration parameters. Ports assigned with an Instant Port Profile inherit the selected port type setting such as type, speed, STP, MAC locking, ELRP, and PSE port settings. Storm control settings are inherited when the non-match action is set to use the default port type, and a device does not match a defined device type. See Configure Individual Ports on page 430 for more information on these port types.

**Configuring Non-Match Actions**

There are two options to choose between for non-match actions when a device does not match any defined device type criteria, including storm control settings:

- Non-forwarding VLAN – Traffic is not forwarded for devices that do not match an assignment rule when non-forwarding VLAN is selected.
- Use Default Port Type VLAN – Selecting the non-match action of the default port type assigns the VLANs associated with the port type.

**Defining Match Criteria**

Matches are based on the following criteria:

- MAC Learning – Matches the device based on the MAC address learned on the port from untagged traffic. The match can be an exact MAC, OUI based MAC, or custom MAC mask format.
- LLDP Src MAC – Matches the device based on the source MAC of an LLDP PDU. The match can be an exact MAC, OUI based MAC, or custom MAC mask format.
- LLDP Capability – Matches the device based on the LLDP capability from the source LLDP PDU. The LLDP capability is selectable.
- LLDP MAC + Capability – Matches the device based on the source MAC of an LLDP PDU and the LLDP capability from the source LLDP PDU selected.

*Create a New Port Type*

First, create or modify a switch template as part of a network policy, or as a common object.

Use this task to create ports in bulk.

1. In the switch template, select **Configuration** > **Port/VLAN Configuration**.
2. Under **Create Ports in Bulk**, select one or more ports and select **Assign** > **Create New**, or select (next to **Port Type** under **Configure Ports Individually**).
3. If this template applies to a 5570 or 5520 switch, define the VIM Port Channelization ports.
   a. Under **Configure Ports in Bulk**, select **Select VIM**.
   b. For a 5570 switch, select **VIM-6YE** or **VIM-2CE**.
   c. For a 5520 switch, select **VIM-4X**, **VIM-4XE**, or **VIM-4YE**.
   d. For Universal 7830 switch, select **7830-VIM-24CE** , **7830-VIM-8DE** , **7830-VIM-16CE** , or **7830-VIM-24YE**.

   **Note**
   When different templates for the same switch SKU are required to be created with different VIMs, then a classification rule can be created to assign the same template SKU with different VIM options to different devices. See Configure Classification Rules for a Device Template on page 438 for more information about classification rules.

   **Note**
   The 7830-VIM-24CE and 7830-VIM-8DE modules support hot-swapping in Slot 1 and Slot 2 on the Universal 7830 chassis running Fabric Engine 9.4.1 or later. You can insert or remove these modules without powering off the switch. The 7830-VIM-16CE and 7830-VIM-24YE modules do not support hot-swap and require the switch to be powered off before installation or removal.

   e. Select one or more of these VIM ports and continue to Step 4.
4. Type a **Name**.
5. (Optional) Edit the associated **Description**.
6. Toggle the port **ON** or **OFF**.

7. In the **Port Usage Settings** section, select one of the following port types:
   - **Access Port**: Ports connected to individual hosts such as printers, servers, and end-user computers.
   - **Phone with a data port**: Ports connected to IP phones, and optionally, to computers cabled to the phones.
   - **Trunk port**: Ports connected to network forwarding devices, such as switches and APs that support multiple VLANs on trunk ports.
8. Select **Next**.
9. Select an existing VLAN or select the add icon to add a new one.

   To add a new VLAN, see Configure VLAN Settings on page 362.
10. Select **Next**.
11. Set authentication options for switches with Instant Secure Port enabled. By default User Authentication (802.1x) and MAC authentication will set the reauthentication period to 3600 seconds. Instant Secure Port Profile must be enabled within the network policy and switch template. For **Instant Secure Port Authentication Settings**:
    - **User Authentication**: Turn **On** for wired devices, such as printers, servers, and end-user computers.
    - **MAC Authentication**: Turn **On** for legacy devices that use MAC addresses as the user name and password to authenticate clients.
      - **Authentication Protocol**: Select the authentication protocol that determines how the port forwards requests to the RADIUS or Active Directory server. Valid values are PAP, CHAP, and MS Chap V2.

        With PAP, the port sends an unencrypted password to the RADIUS server. With CHAP or MS CHAP V2, instead of sending a password, the port and the authentication server perform the same operation on the password, the server compares the results to determine if the results match.
12. Select **Next**.
13. Add RADIUS Servers under **RADIUS Settings** to use this form of user authentication.

    Either select an existing **RADIUS Server Group** or select the add icon to add a new one. See Configure an External RADIUS Server on page 352.
14. For **Authentication Method Priority**, use the up or down arrows to determine the authentication method use order.
15. For **QoS Settings**, toggle **On** to create custom settings.

    Select the 802.1p classification system (marked in the L2 frame header in Ethernet frames) or the DiffServ codepoint marking system (marked in the L3 packet header) on outgoing packets from the drop-down list. See Configure Marker Maps on page 372.
16. Select **Next**.
17. For **Transmission Settings**, configure the following:
    - **Transmission Type**: Select **Auto**, **Half-Duplex**, or **Full-Duplex**. Auto causes the switch to negotiate the best possible duplex mode possible with the connected device. Full-Duplex forces the switch to communicate with the connected device using full-duplex communication. Half-Duplex forces the switch to use half-duplex communication.
    - **Transmission Speed**: Choose the speed the switch port uses to communicate with the connected device.

- **Debounce Timer**: Select the amount of time the switch does not register another input.
- **CDP Receive**: Enables the switch to receive and parse the information within Cisco CDP frames.
- **Auto MDIX**: Automatically detects the required cable connection type (straight through or crossover) and configures the connection appropriately.
- **LLDP Transmit**: Enables the switch to transmit LLDPDU frames.

  **Note**
  Instant Port will not function correctly if LLDP Transmit is disabled, especially if LLDP-based matching is part of the Device Type Profile.

- **LLDP Receive**: Enables the switch to receive LLDPDU frames.

18. Select **Next**.
19. For **STP**:
    - **STP Enabled**: Toggle **ON** to enable STP for the port.
    - **Edge Port**: Connects to a user terminal or server, instead of other switches or shared network segments. A port configured as an Edge port does not cause a loop upon network topology changes.
    - **BPDU Protection**: Use the drop-down list to change BPDU protection to guard or filter status.
      - **Guard** - Controls whether a port explicitly configured as Edge disables itself upon reception of a BPDU. The port enters the error-disabled state, and is removed from the active topology.
      - **Filter** - Controls whether a port explicitly configured as Edge transmits and receive BPDUs. You must select this option for Fabric Engine switches.
      - **Disabled** - Turns off BPDU Protection.
    - **Priority**: When this port is an STP edge port, select a port priority for STP from the drop-down list.
20. Select **Next**.
21. For **Storm Control**:
    - **Broadcast**: Select to include traffic that is forwarded to all destinations simultaneously.
    - **Unknown Unicast**: Select to include traffic whose destination address does not appear in the forwarding database.
    - **Multicast**: Select to include traffic whose destination is a multicast address.
    - **TCP-SYN**: Select to include TCP-SYN flood traffic.
    - **Thresholds**: Select **Byte Based** or **Packet Based**.
    - **Rate Limit Type**: Select **Kbps** (kilobytes per second) or **Percentage** if you selected **Byte Based** and **PPS** (packets per second) if you selected **Packet Based**.
    - **Rate Limit Value**: Enter when the switch should discard traffic of the selected types.
22. For **MAC Locking**, enable the per port type with the option to specify **Maximum First Arrival Limit** and specify the **Link Down Action**.

    By default, **Link Down Action** it is set to clear first arrival MACs, with the option to retain MAC's. We also have the option to take action when MACs are aged out.

23. Select general **ELRP Settings** and configure the settings:
    - Toggle **Enable ELRP**.
    - Select the **Enable ELRP for dynamically created VLAN(s)** check box.
    - Toggle **Configure ELRP Port Duration** and enter the duration in seconds.
24. Select **SAVE**.
25. For device-level ELRP interface options, select the specific interface check box and toggle **ELRP Enabled** to enable ELRP per port or toggle **ELRP Exclude** to exclude ELRP.
26. For **PSE**, select an existing profile or select the plus sign to add a new one.

    See Configure PSE on page 435.
27. Review all the port settings in the **Summary** section and select **Save** when complete.

*Configure Individual Ports*

First, create or modify a switch template as part of a network policy, or as a common object.

Create or modify a switch template, then select from the menu.

**Note**
To modify an existing port, select the **Port Type** from the list and then select the edit icon. You can edit all port parameters from the **Summary** page.

Use this task to configure or modify settings for individual ports.

**Note**
To support Stacking Mode for Switch Engine 5320-16P-2MXT-2X switch templates, select the edit button next to the ports and enable to **Stacking Support Mode** toggle.

1. In the switch template, select **Configuration** > **Port/VLAN Configuration**.
2. For **Port Name & Usage** and **VLAN**, see Configure Port Details on page 430.
3. For **Instant Secure Port Settings**, see Configure Authentication on page 432.
4. For **Port Settings**, see .
5. For **Transmission Settings**, see Configure Transmission Settings on page 432.
6. For **STP**, see Configure STP Settings on page 433.
7. For **Storm Control**, see Configure Storm Control on page 433.
8. For **MAC Locking**, see Configure MAC Locking on page 434
9. For **Voice**, see
10. For **ELRP**, see Configure ELRP on page 434
11. For **PSE**, see Configure PSE on page 435.
12. For **VLAN Attributes, see**
13. Review the settings on the **Summary** tab, and then select **SAVE**

**Configure Port Details**

Create or modify a switch template, and then open it for configuration. See Configure Individual Ports on page 430.

The **PORT DETAILS** tab of the **Configure Ports Individually** table displays the following information:

- **Interface**: The interfaces available for the switch, such as Eth1/0/1-Eth1/0/52.
- **Port Type**: Indicates the current port usage setting.
- **Enabled**: Indicates whether the port is currently activated.
- **LACP**: Indicates link aggregation control protocol for a member of a link aggregation port group. See Aggregate LAG and LACP Ports on page 437.
- **VLAN**: This column displays the VLAN assigned to the port. Change the VLAN number directly in the VLAN text box.
- **Description**: A brief description of the port.

**Tip**
These settings appear in the **Info & VLAN** section of the **Summary** tab.

Use this task to configure the settings for a new port, on the **Port Name & Usage** and **VLAN** tabs.

1. Under **Configure Ports Individually**, select the the **Port Details** tab.
2. For the interface that you want to configure:
   - To edit an existing port, select .
   - To configure a new port, select .
3. Configure the settings on the **Port Name & Usage** tab:
   a. Type a **Name** for the new port.
   b. Type a **Description** for the new port.

      Although optional, descriptions can be helpful when you are troubleshooting your network.
   c. Toggle the **Status** to **ON** or **OFF**.
4. Select the **Port Usage** setting:
   - **Access Port**: Ports connected to individual hosts such as printers, servers, and end-user computers.
   - **Phone with a data port**: Ports connected to IP phones, and optionally, to computers cabled to the phones.
   - **Trunk port**: Ports connected to network forwarding devices, such as switches and APs that support multiple VLANs on trunk ports.
5. Select **NEXT** to open the **VLAN** tab.
6. For **VLAN**, select and choose an existing object, or to add a new one, select to create a new VLAN object.
7. Select **NEXT**, or select the **User Authentication** or **QoS** tab, and continue configuring the port.
8. Select the **Instant Secure Port Settings** tab, and continue configuring the port.

#### Configure Authentication

First configure the **Port Name & Usage** and **VLAN** tabs. See Configure Port Details on page 430.

**Tip**
These settings appear in the **Authorization** section of the **Summary** tab.

Use this task to configure the authentication settings for a new port, on the **Instant Secure Port Settings** tab.

**Note**
The **User Authentication** tab is part of the taskflow for older Dell and SR-based devices.

1. Toggle **User Authentication** to **ON** or **OFF**.
2. Toggle **MAC Authentication** to **ON** or **OFF**.
3. Select **NEXT**, or select the **Transmission Settings** tab, and continue configuring the port.

   See Configure Transmission Settings on page 432.

#### Configure Transmission Settings

First, Configure Authentication on page 432.

**Tip**
These settings appear in the **Port Settings** section of the **Summary** tab.

Use this task to configure the settings for a new port, on the **Transmission Settings** tab.

1. For **Transmission Type**, select **Auto**, **Half-Duplex**, or **Full-Duplex**.

   **Auto** causes the switch to negotiate the best possible duplex mode possible with the connected device. **Full-Duplex** forces the switch to communicate with the connected device using full-duplex communication. **Half-Duplex** forces the switch to use half-duplex communication.
2. Select the **Transmission Speed** the switch port uses to communicate with the connected device.
3. To display learned switch port client MAC addresses on ExtremeCloud IQ monitoring screens, select **Client Reporting**.

   When client reporting is disabled, client MAC addresses are not displayed. It is disabled when **CDP Receive** is turned off.
4. To enable Cisco Discovery Protocol (CDP), select **Enable CDP Transmit/Receive**.
5. To enable the switch to transmit LLDPDU frames, select **LLDP Transmit**.
6. To enable the switch to receive LLDPDU frames, select **LLDP Receive**.
7. To enable Link Layer Discovery Protocol-Media Endpoint Discovery, select **Enable LLDP MED Capabilities**.
8. Select **NEXT**, or select the **STP** tab, and continue configuring the port.

   See Configure STP Settings on page 433.

### Configure STP Settings

First Configure Transmission Settings on page 432.

**Note**
Extreme Networks recommends that you enable STP.

Extreme Networks switches can use Spanning Tree Protocol (STP) to activate links with the lowest cost (highest bandwidth), establish backup links where possible, and prevent Layer 2 network loops, which can result in duplicate unicast frames and broadcast storms. Bridge Protocol Data Unit (BPDU) protection is a security feature designed to protect the active STP topology by preventing spoofed BPDU packets from entering the STP domain. BPDU protection is applied to edge ports connected to end-user devices that do not run STP. If an STP BPDU protected port receives packets, this feature disables that port and alerts the network admin.

The BPDU Restrict feature disables the port as soon as a BPDU is received on the BPDU restrict port, blocking the loop. Specify a BPDU recovery timeout, enabling the port after the configured amount of time.

**Note**
You can enable BPDU Restrict only when Edge port is also enabled.

By default, STP is disabled. Use this task to enable STP and configure the settings for an individual port, on the **STP** tab.

1. Toggle **STP ON**.
2. Toggle **Edge Port ON** so the port connects to a user terminal or server, instead of other switches or shared network segments.

   A port configured as an edge port will not cause a loop upon network topology changes.
3. For **BPDU Protection**, select **Guard** or **Disabled** status.
   - **Guard**: Controls whether a port explicitly configured as Edge disables itself upon reception of a BPDU. The port enters the error-disabled state, and is removed from the active topology.
   - **Disabled**: Turns off BPDU Protection.
4. Select the port **Priority**.

   If Spanning Tree Mode is set to STP, set the port priority to either 0 or 16.
5. Select **NEXT**, or select the **Storm Control** tab, and continue configuring the port.

   See Configure Storm Control on page 433.

### Configure Storm Control

First Configure STP Settings on page 433.

Extreme Networks switches can mitigate traffic storms by tracking the source and type of frames to determine whether they are legitimately required. Switches then discard frames that are determined to be the products of a traffic storm. You can apply storm control to

broadcast, unknown unicast, and multicast traffic, and configure packet-based or byte-based rate limit thresholds for each interface.



**Tip**
These settings appear in the **Storm Control** section of the **Summary** tab.

Use the following procedure to configure traffic storm mitigation for an individual port.

1. Select the traffic to include:
   - Select **Broadcast** to include traffic that is forwarded to all destinations simultaneously.
   - Select **Unknown Unicast** to include traffic with a destination address does not appear in the forwarding database.
   - Select **Multicast** to include traffic with a multicast address as a destination.
2. Type the **Rate Limit Value** for discarding traffic of the selected types.
3. Select **NEXT**, or select the **MAC Locking** tab, and continue configuring the port.
   See Configure MAC Locking on page 434.

#### Configure MAC Locking

First, configure Configure Storm Control on page 433.

Configure MAC locking security to control the forwarding database for learned MAC address entries on a port. You must also enable MAC locking in the switch template.

Use this task to configure the settings for MAC locking.

1. Toggle **MAC Locking Enable** to **ON**, and configure the settings.

**Table 154: MAC Locking settings**

| Setting | Description |
|---|---|
| Maximum First Arrival | Specify the number of first-arrival MAC addresses allowed to communicate on the port.<br>Range (0-600) |
| Disable Port | To disable the port when the maximum first arrival limit is exceeded, toggle **Disable Port** to **ON**. |
| Link Down Action | Select one of the following options:<br>• **Clear first arrival MACs when port link goes down**<br>• **Retain first arrival MACs when port link goes down** |
| Remove Aged MACs | To remove learned MAC Addresses after they age out from the switch forwarding database, toggle **Remove Aged MACs** to **ON**. |

2. Select **NEXT**, or select the **ELRP** tab, and continue configuring the port.
   See Configure ELRP on page 434.

#### Configure ELRP

First, Configure MAC Locking on page 434.

Extreme Loop Recovery Protocol (ELRP) is a loop protection mechanism designed to detect and prevent loops. In ExtremeCloud IQ (New) you can configure ELRP client periodic packet

transmission for VLAN(s) assigned to a port type. You must also enable ELRP in the switch template.

Use this task to enable and configure ELRP.

1. Toggle **Enable ELRP client and disable port when a loop is detected on applied access or trunk VLANs assigned to the port type** to **ON**.
2. To prevent the ELRP client port from being disabled, toggle **ELRP Exclude** to **ON**.
3. Select **NEXT**, or select the **PSE** tab, and continue configuring the port.

**Configure PSE**

Create or modify a switch template.



**Tip**
These settings appear in the **PSE Settings** section of the **Summary** tab.

Use this task to configure PSE settings, which define how ports manage the power that they supply to devices.

1. Select an existing PSE profile from the menu, or select +.
2. Type a **Name**.
3. For **Power Mode**, select **802.3af** or **802.3at**.
   **802.3af (PoE)** can deliver 15.4 watts over Cat5 cables. **802.3at (PoE+)** can deliver up to 30 watts over Cat 5 cables with 25.5 watts available to devices.
4. For **Power Limit**, limit the available PoE power to a level lower than the maximum allowed by the power mode.
5. Select a **Priority** from the drop-down list:
   **Low**: If the total powered device (PD) power consumption exceeds the PSE power budget, power output is modified to bring the total consumption back to within the PSE power budget.

   **High**: When the total PD power consumption exceeds the PSE power budget, power output is modified only after ports with low priority PSE profiles are regulated.

   **Critical**: When the total PD power consumption exceeds the PSE power budget, power output is shut down last.
6. (Optional) Type a description.
   Although optional, descriptions can be helpful when you are troubleshooting your network.
7. Select **SAVE**.
8. Toggle **POE Status** to **ON** or **OFF**.
9. Select **NEXT**, or select the **Summary** tab, and review the settings for the port.
10. Select **SAVE.**

*Configure Switch Template Advanced Settings*

First, create or modify a switch template as part of a network policy, or as a common object.

ExtremeCloud IQ (New) can update device firmware and reboot the device during onboarding. Currently, switch onboarding and firmware/configuration updates require manual steps. Use

this task to enable the firmware upgrade option, as well as auto config push, during switch onboarding within the defined template for the switch assigned to the associated network policy. Each can be enabled/disabled together or independently.

1. In the switch template, select **Configuration** > **Advanced Settings**.
2. For **Upgrade device firmware upon device authentication**, select **On** to upgrade the device firmware upon onboarding.

   If you have activated device firmware upgrading, select one of two options:

   - Update firmware to the latest version.
   - Upgrade to a specific device firmware version.
3. To reboot and roll back a device to a previous configuration if there are issues with the template configuration, select **On** for **Upload Configuration Automatically**, followed by the check box below.
4. To use **Supplemental CLI**, select **On**.

   For more information, see Configure Supplemental CLI on page 437.

Complete configuring the device template.

## Configure Port Types

After you select ports in a new device template, you must assign a port type. For AP ports, select **Choose Existing** or **Create New**. For switch ports, select from **Choose Existing**, **Create New**, or **Advanced Actions > Aggregate**.

**Note**
Only Switch Engine and Extreme XOS support port types.

For 1- and 2-port APs, there are three port types:

- **Bridge-Access ports** connect to individual hosts. You can configure captive web portal access, MAC authentication via a RADIUS server, change the user profile, and configure traffic management.
- **Bridge-802.1Q ports** provide network access through forwarding devices and support multiple VLANs. You can change the default user profile and manage incoming traffic.
- **Uplink Ports** act as WAN uplinks. You can change the default user profile and configure traffic control settings.

For 24- and 48-port switch templates there are three port types:

- **Access Ports** are connected to individual hosts such as printers, servers, and end user computers. A VLAN ID tag is added to the frame before it is forwarded using the 802.1Q tagging protocol. You can enable User Authentication or MAC Authentication, and configure QoS settings, Client Detection and VLAN ID.
- **Phone Data Ports** are used for voice transmission.
- **Trunk Port frames that are not VLAN-aware**. Frames are in a native VLAN (default) or Management VLAN.

You can also configure ports at the device level. Port settings that you configure there override any settings you make in the network policy device template.

Use this task to configure port types as part of a network policy.

1. Select an existing device template, and then select , or to add a new one, select .
2. To assign an existing port type, select the port and then select **Assign**.
3. To create a new port type and assign it to a port at the same time, select an interface port, then select **Assign** > **Create New**.
4. Type a **Name** for the port type.
5. (Optional) Type a brief **Description** for the port type.
6. Turn the port off or on.
7. Select **Save**.

Related Links

Assign an Ethernet Port Profile on page 392

## Aggregate LAG and LACP Ports

Create or modify a switch template.

You can group individual ports into aggregate ports on 24- and 48-port switches by selecting two or more ports of the same type on the switch template.

**Note**
You can change the LAG port type after a port has been assigned to a LAG, without having to delete and recreate the LAG.

1. Select the ports you want to aggregate, and then select **AGGREGATE PORTS** .
   Alternatively, select **Assign** > **Advanced Actions** > **Aggregate**.
2. Enter an optional description.
3. Toggle **LACP (Link Aggregation Control Protocol)** to **ON**.
   If LACP (Link Aggregation Control Protocol) is disabled, ExtremeCloud IQ (New) creates a static LAG.
4. Use the arrows to add or remove ports from the LAG.
5. Select the **Master Port**.
6. Select a **Port Load Balancing** option.

# Configure Supplemental CLI

First, enable Supplemental CLI in ExtremeCloud IQ (New). Go to **Administration & Settings** > **Global Settings** > **Backup & Restore** > **VIQ Management**, and toggle **Supplemental CLI** to **ON**.

Create or modify a switch template as part of a network policy, or as a common object.

After you save supplemental CLI objects containing CLI commands, you can update the commands for devices automatically.

To avoid an unnecessary system reboot, select **Delta Configuration Update**. ExtremeCloud IQ (New) attempts to update only the configuration deltas. If a full update is required, the system prompts you to select **Complete Configuration Update**. For information about how the configuration push behaves with each **Activation Time** option, see Configuration Push

Scheduling Behavior on page 154. Examples of CLI commands that require a full configuration update are: **`system antenna-type`** and **`system environment`**.

Use this task to configure supplemental CLI (sCLI) objects.

1. In the switch template, select **Configuration** > **Advanced Settings**.
2. Select an existing Supplemental CLI object, and then select , or to add a new one, select .
3. Type a **Name**.
4. (Optional) Type an optional **Description**.
   Although optional, descriptions can be helpful when you are configuring or troubleshooting your network.
5. Type or paste the **CLI commands** into the field.
   - Enter multiple CLI commands, one command per line, not exceeding a maximum total of 8192 characters.
   - Use CLI Commands that contain IP and VLAN objects: **`${ip:ip_object_name}`** and **`${vlan:vlan_object_name}`**.
   - Perform a complete configuration update each time commands are appended to device configurations.
   - For Dell EMC switches, enter the CLI commands, `enable`, and `config` in the beginning of a sequence of CLI commands.
6. Select **SAVE TEMPLATE**.

## Configure Classification Rules for a Device Template

Before you can add classification rules to a network policy, you must add a default AP device template and a location for the target AP. Also, create cloud config groups, IP addresses, and IP subnets.

You can create classification rules as part of a network policy or as a common object. Use this task to create classification rules associated with a network policy. ExtremeCloud IQ (New) supports multiple classification rules for DNS servers, VLANs, RADIUS servers, device templates, user groups, and private client groups (PCGs).

This task is part of the network policy configuration workflow. Use this task to configure classification rules for a device template, as part of a network policy.

1. Go to **Configuration** > **Network Policies**.
2. Select an existing policy, and then select , or to add a new one, select .
3. After you save the **Policy Details**, select **NEXT** or **2 Wireless**.
4. From the **Configuration Settings** menu, select **AP Template**.
5. Select and choose the desired default template.
   Default templates apply to all of the devices of the selected template type that do not have a matching classification rule.
6. Select , and then select the desired device template.
   Classification rules templates apply only to the devices of the selected template type that match the rules.

7. Type the new **Template Name**.
8. Select **SAVE TEMPLATE**.

   The new template appears in the table, on the AP template landing page. The **Classification Rules** column for the template contains the controls for configuring classification rules.
9. To configure classification rules, see Configure Classification Rules on page 291.

Related Links

Configure Classification Rules on page 291

## Add a Cloud Config Group

Before you begin, configure devices to associate with the cloud configuration groups.

Use cloud configuration groups to create network-level policies that can be replicated for multiple network roll-out scenarios. Use this task to create a new cloud config group as part of a network policy. You can also use this task to create a new cloud config group when you configure classification rules objects.

1. Type a **Name** for the new group.
2. (Optional) Type a **Description** for the new group.
3. Select real and simulated devices to have their host names shown in the **Selected Devices** field.

   **Note**
   You can also import a comma-separated-values (CSV) file including the host names, serial numbers, and optional MAC addresses of other devices.

   a. Selec t**Import**.
   b. Select the CSV file, or drag the CSV file to the **Import Cloud Config Group Members** window.
   c. Select **Submit**.
4. Select **SAVE CLOUD CONFIG GROUP**.

Related Links

Configure Classification Rules for a Device Template on page 438
Configure the SSID for a Standard Wireless Network on page 308

# Fabric Attach

Fabric Attach is a software-based feature that automates the connection to the Fabric Connect environment, enabling devices and their associated end-points to be quickly mapped to the appropriate virtualized Fabric Connect service.

Provisioning a non-fabric AP to the Fabric Connect network is as easy as taking the Fabric Attach-enabled AP out of the box and physically connecting it to a Fabric Connect-enabled switch. The Fabric Attach device then automatically configures itself with the appropriate management VLAN, preparing itself for the dynamic extension of virtualized fabric services on behalf of its connected end-point devices or users. This can speed the deployment of edge devices to the Fabric Connect environment since no manual configuration is required, and can

be especially valuable at locations where networking skills are at a premium, such as remote offices.

ExtremeCloud IQ (New) APs support the following functions:

- Discover the Fabric Attach Server upon startup.
- Receive management VLAN configuration from the Fabric Attach Server, if discovered.
- Configure received management VLAN on the Management interface and Ethernet interface of the AP.
- Establish the management plane communication path to ExtremeCloud IQ (New).
- Support Native VLAN Tagging on the Management interface.

ExtremeCloud IQ APs do not support the following functions:

- Get VLAN to I-SID Mapping from ExtremeCloud IQ (New) as a management command.
- Configure the Fabric Attach Server port with VLAN to I-SID mapping.
- Establish data plane communication path for every configured VLAN.

Related Links

Configure Fabric Attach on page 440

## Configure Fabric Attach

Before you begin, physically connect the device to a Fabric Connect-enabled switch. To perform the following task, you require the device VLAN ID and I-SID number.

For more information about Fabric Attach, see Fabric Attach on page 439.

This task is part of the network policy configuration workflow. Use this task to configure Fabric Attach for a device connected to an existing Fabric Connect network.

1. Go to **Configuration** > **Network Policies**.
2. Select an existing network policy, and then select , or to add a new one, select .
3. After you save the **Policy Details**, select **NEXT** or **2 Wireless**.
4. Select an existing **Device Template** to edit, or select .
5. Scroll down to the **Wired Interfaces** section.
6. To use an existing **Fabric Attach** profile, and choose an existing object, or to add a new one, select .
7. Type a **Name** for the new profile.
8. (Optional) Type a description for the new profile.

   Although optional, descriptions can be helpful when you are configuring or troubleshooting your network.
9. Select to add a VLAN.
10. Type the associated **VLAN ID** for the device.
11. Select the **I-SID#** for the device from the drop down.
12. Select **SAVE**.

Related Links

Fabric Attach on page 439
Configure the SSID for a Standard Wireless Network on page 308

## Configure Device Data Collection and Monitoring Options

First, create a network policy.

This task is part of the network policy configuration workflow. Use this task to set the following data collection and monitoring options:

- **Application Visibility and Control (AVC)**: AVC gives you information that can help you manage network traffic and applications. AVC detects the application-layer contents of the frame to determine the application or protocol that is transmitting the data. ExtremeCloud IQ (New) can then track the amount of data being transmitted by a particular application or protocol.
- **Device Wireless Activity Thresholds**: Set activity threshold limits above which event alarms are generated.
- **Client Wireless Activity Thresholds**: These alarms identify when violations occur that affect the wireless health of a client as reported in SLA reports for non-compliant clients. To trigger more alarms, lower thresholds. To reduce the number of alarms, increase thresholds.
- **Kernel Diagnostic Data Recorder (KDDR)**: KDDR logs capture run-time statistical data about unexpected events for Extreme Networks devices. Extreme Networks Support analyzes the content of these binary log files for troubleshooting.
- **Automatic Synthetic Traffic Generation**: Some of the Client 360°, Device 360°, and Network 360° monitoring capabilities require synthetic traffic generation.

1. Go to **Configuration** > **Network Policies**.
2. Select an existing policy, and then select , or to add a new one, select .
3. After you save the **Policy Details**, select **NEXT** or **2 Wireless**.
4. From the **Application Management** menu, select **Device Data Collection And Monitoring**.
5. Toggle the **Application Visibility and Control** setting **ON** to detect frame application-layer contents.
6. Toggle the **Statistics Collection** setting **ON** to record wireless activity statistics between the device and connected clients.
7. To change the data collection interval, select the number of minutes from the menu.
8. For **Device Wireless Activity Thresholds**, type values for the following fields:
   - **CRC error rate exceeds**: The point at which the percent of CRC errors in received wireless frames during the collection interval is considered to be excessive.
   - **Tx drop rate exceeds**: The point at which the percent of transmitted wireless unicast frames that a device drops during the collection interval is considered excessive. A transmitted wireless frame is dropped when the device tries to transmit the same unicast frame a maximum number of times without receiving an acknowledgment from the intended recipient.
   - **Rx drop rate exceeds**: The point at which the percent of dropped wireless frames during collection interval is considered excessive. A device might drop wireless frames

on its ingress Wi-Fi interface for several reasons, such as the arrival of duplicate frames or frames that cannot be decrypted.

- **Tx retry rate exceeds**: The point at which the percent of retransmitted wireless frames during the collection interval is considered excessive. A device tries to resend a unicast frame if the first effort does not elicit an acknowledgment from its intended recipient.
- **Airtime Consumption exceeds**: The point at which the percent of transmitted and received airtime usage for a wireless interface during the collection interval exceeds the maximum airtime consumption threshold.

9. For **Client Wireless Activity Thresholds**, type values for the following fields:
   **Tx drop rate exceeds**: Indicates the point at which the percent of wireless unicast frames that a device drops during transmission to the same client during the statistics collection interval is considered excessive.

   **Rx drop rate exceeds**: Indicates the point at which the percent of dropped wireless frames received from the same client during the statistics collection interval is considered excessive.

   **Tx retry rate exceeds**: Indicates the point at which the percent of retransmitted wireless frames to the same client during the collection interval is considered excessive.

   **Airtime Consumption exceeds**: Indicates the point at which the percent of airtime that a device consumes while transmitting traffic to and receiving traffic from the same client during the collection interval is considered excessive.
10. Toggle the **Kernel Diagnostic Data Recorder** setting **ON** to capture run-time statistical data about unexpected events.
11. For **Automatic Synthetic Traffic Generation**:
    a. Enable **RADIUS Authentication** to create synthetic traffic.
    b. Toggle the **Check Radius service connectivity via Status-Server** setting **ON** to check RADIUS service connectivity.
    Ensure that **Status-Server** is enabled on the RADIUS server.
    c. Adjust the check **Interval** if necessary.

Related Links

Configure the SSID for a Standard Wireless Network on page 308

## Configure the BLE Service

First, configure a network policy.

Consider the following:

- The BLE Service settings configured in this task apply to the Device template associated with the network policy. You can override the settings configured here, and also configure device-level settings, by going to **Manage** > **Devices** > **Configure** > **Interface Settings** > **Wireless Interfaces** > **BLE Service**.
- IoT Thread profile configuration automatically takes precedence over BLE configuration. If BLE is configured and deployed, and later IoT Thread is configured and deployed, BLE becomes disabled and IoT Thread is enabled. If BLE configuration exists but has yet to be deployed, and then later IoT configuration is done and deployed, only the IoT configuration is pushed to the AP.

You can configure the embedded BLE transmitter in APs. As transmitters, these beacons broadcast numerical advertisements that trigger an action on Bluetooth-enabled devices that come within range. For example, an app running on a mobile device might react to a BLE signal by displaying welcome messages, sale announcements, or coupons.

This task is part of the network policy configuration workflow. Use this task to configure the iBeacon service for a network policy.

1. Go to **Configuration** > **Network Policies**.
2. Select an existing policy, and then select , or to add a new one, select .
3. After you save the **Policy Details**, select **NEXT** or **2 Wireless**.
4. From the **Application Management** menu, select **BLE Service**.
5. Toggle the **BLE Services** setting **ON**.
6. Type a **Service Name**.
7. (Optional) Type a **Description**.

   Although optional, entering a description is helpful for troubleshooting and identification.
8. For **BLE Scan**, select **iBeacon** or **Generic** or both, and then configure the **Destination** settings.

**Table 155: Destination settings**

| Setting | | Description |
|---|---|---|
| Cloud Reporting (iBeacon scan only) | | Toggle **ON** to enable Cloud Reporting for the device. Deselect to disable Cloud Reporting for the device.<br>Cloud Reporting provides real-time analytics and insights into the performance and usage of your BLE network. Use this feature to monitor key metrics, track user interactions, and optimize BLE for maximum efficiency. |
| | Interval | Specify an interval value between 10-1200 seconds to determine how often iBeacon transmits to ExtremeCloud IQ (New). The default value is 60 seconds. |
| Batch Reporting (Required for Generic BLE scan) | | Toggle **ON** to submit iBeacon reports in batch files.<br>Batch Reporting compiles and analyzes large sets of iBeacon interaction data at scheduled intervals. This feature is ideal for generating periodic reports and gaining insights into long-term trends and patterns. |
| | Interval | Specify an interval value between 10-60 seconds to determine how often iBeacon transmits batch file reports. The default is 10 seconds. |
| | URL | Type the destination URL to submit batch file reports. |
| Ignore Duplicates | | Enable this feature to remove duplicate entries automatically, within the specified time interval. |
| Secure Connection | | Toggle **ON** and specify the credentials to secure the data flow to your server. |
| **Token renewal setting** | | |
| | Client ID | Specify the unique identifier assigned to the client application. (String, 10-255 characters) |
| | Client Secret | Specify the confidential key used to authenticate the client. (String, 10-255 characters) |

**Table 155: Destination settings (continued)**

| Setting | | Description |
|---|---|---|
| | Show Password | Select the check box to show the password (Client Secret). |
| | Token URL | Specify the API URL where the client sends requests to obtain or refresh access tokens.<br>(String, valid URL format, max 255 characters) |

9. Configure the **iBeacon Filter** settings (iBeacon Filter only).

**Table 156: iBeacon Filter settings**

| Setting | Description |
|---|---|
| Min RSS(dBm) | The minimum Received Signal Strenth (RSS) value used for filtering iBeacon signals. RSS is measured in dBm (decibels relative to 1 milliwatt). |
| UUID | The iBeacon unique identifier. If your organization already has a UUID number, type it in the **iBeacon UUID** field.<br>UUID format: 32 hexadecimal (base 16) digits, displayed in five groups separated by hyphens, in the form 8-4-4-4-12 for a total of 36 characters (32 alphanumeric and four hyphens). For example: 123e4567-e89b-12d3-a456-426655440000<br>You can also automatically create a UUID with an online UUID generator, such as the one at https://www.uuidgenerator.net/. |

10. Configure the **Generic Filter** settings (Generic Filter only).

**Table 157: Generic Filter settings**

| Setting | | Description |
|---|---|---|
| Min RSS(dBm) | | The minimum Received Signal Strength (RSS) value used for filtering generic signals. RSS is measured in dBm (decibels relative to 1 milliwatt). |
| Vendor | | Select **Any**, **CHORUS**, or **Custom**. |
| | Any | Select **Any** to accept all beacons. |
| | Chorus | Select **Chorus** to auto-populate the settings for this vendor, and then select **ADD**. |
| | Custom | Select **Custom**, type the **Name** and **Company Id** of the vendor, and then select **ADD**. You can specify an ID for up to five vendors. |

11. Select **Save**.

Related Links

Configure the SSID for a Standard Wireless Network on page 308

## Configure Presence Analytics

First, configure a network policy.

**Note**
It is not necessary to change the default values if devices are connected over faster links.
Adjust these settings to accommodate situations where devices are connected over slower links and where the data must be aggregated at different rates.

This task is part of the network policy configuration workflow. Use this task to specify how frequently APs send data to ExtremeCloud IQ (New).

1. Go to **Configuration** > **Network Policies**.
2. Select an existing policy, and then select , or to add a new one, select .
3. After you save the **Policy Details**, select **NEXT** or **2 Wireless**.
4. From the **Application Management** menu, select **Presence Analytics**.
5. Toggle the **Enable Presence Analytics** setting **ON**.

   Presence Analytics is required to access the location mini map on the Client details page.
6. Type a **Name**.
7. (Optional) Type a **Description**.

   Although optional, entering a description is helpful for troubleshooting and for identification.
8. For **Trap Interval**, specify (in seconds) how often the presence sensor reports data to ExtremeCloud IQ.

   Lowering this interval below 15 seconds pushes data faster but also increases network traffic. Raising this interval above 15 seconds pushes data at a slower rate and decreases network traffic.
9. Specify the **Aging Time** (in seconds) for a given presence profile.
10. Specify the **Aggregate Time** interval (in seconds) for the set period during which aggregation occurs for the presence profile.

Related Links

Configure the SSID for a Standard Wireless Network on page 308

## Configure WIPS

This task is part of the network policy configuration workflow. Use this task to enable and configure the Extreme Networks Wireless Intrusion Prevention System (WIPS), as part of a wireless network policy.

1. Go to **Configuration** > **Network Policies**.
2. Select an existing network policy, and then select , or to add a new one, select ..
3. After you save the **Policy Details**, select **NEXT** or **2 Wireless**.
4. From the **Application Management** menu, select **WIPS**.

5. Toggle **WIPS** to **ON**, and configure the settings.

   For more information, see WIPS Policy Settings on page 446.

   To reuse WIPS settings, select and choose a WIPS policy object.
6. Select **SAVE**.

Related Links

WIPS Policy Settings on page 446
Configure the SSID for a Standard Wireless Network on page 308

## WIPS Policy Settings

**Table 158: Settings for WIPS policy**

| Setting | Description |
|---|---|
| Name | Type a **Name** for the new policy. |
| Description | (Optional)<br>Type a **Description**.<br>Although optional, descriptions can be helpful when you are troubleshooting your network. |
| AirDefense Essentials | Toggle **AirDefense Essentials** to **OFF** to disable it, and then select **Save**.<br>By default, **AirDefense Essentials** is **ON** (enabled).<br>To **Allow change of operating channel for air-termination**, select the check box. |
| **Rogue Access Point Detection** | |
| Rogue Access Point Detection (Legacy) | Toggle **Rogue Access Point Detection (Legacy) ON** to enable the feature. |
| Determine if detected rogue APs are connected to your wired (backhaul) network | Use **Determine if detected rogue APs are connected to your wired (backhaul) network** in combination with other WIPS techniques to determine if a detected rogue AP is in the same network as compliant APs.<br>An Extreme Networks AP builds a MAC learning table from source MAC addresses in the broadcast traffic it receives from devices in its Layer 2 broadcast domain. When an AP running XOS 5.0r2 or later detects a rogue AP through any of the rogue detection mechanisms in the WIPS policy, it checks the MAC learning table for an entry within a 64-address range above or below the BSSID of the invalid SSID. If there is a match, it is assumes that both MAC addresses belong to the same device. Because one of its addresses is in the MAC learning table, the rogue is considered to be in the same backhaul network as the detecting AP, and **In Net** displays in the **In Network** column for that rogue in the list of rogue APs. |
| Detect rogue access points based on their MAC OUI | Select the check box to enable detection of rogue APs based on MAC OUI. |

**Table 158: Settings for WIPS policy (continued)**

| Setting | Description |
|---|---|
| Select MAC OUIs of wireless devices that are permitted in the WLAN | Create an allow list of wireless devices allowed on the WLAN, according to MAC OUI.<br>To use an existing MAC OUI, select and choose an existing object, or to add a new one, select .<br>Select **ADD**. |
| Detect rogue access points based on hosted SSIDs and encryption type | Select the check box to enable detection of rogue APs based on hosted SSIDs and the encryption type.<br>Select , and then choose one of the following:<br>For example, if you have a network security policy that requires all SSIDs to use Enterprise 802.1x, any valid SSID using Enterprise 802.1x makes the access point hosting it valid. An access point is categorized as a rogue if it hosts an SSID using WEP or no encryption at all.<br>• **Select an SSID**—Select the SSID from the menu.<br>• **Enter an SSID Name**—Type the SSID name.<br>Select **Check the type of encryption used by this SSID**, and then select the type of encryption from the list. Otherwise, clear the check box.<br>Select **ADD**. |
| Detect if wireless clients have formed an ad hoc network to identify rogue clients | Toggle **Detect if wireless clients have formed an ad hoc network to identify rogue clients ON** to enable the feature. Select **Enable rogue client reporting** and type the number of seconds, after which disconnected rogue APs drop from the reports. |
| **Rogue Mitigation** | |
| Mitigation Mode | Select one of the following:<br>• **Manual**: Manually mitigate rogue APs and their clients. In manual mode, you must periodically check for rogue APs and their clients on the heat map pages in your network hierarchy.<br>**Note:** Use caution when mitigating a suspected rogue AP. If your WLAN is within range of other neighboring wireless networks, the access point that might initially be considered a rogue AP, along with its clients, might be valid in another WLAN.<br>• **Automatic**: APs automatically mitigate rogue APs and their clients, starting and stopping the mitigation process without any administrator involvement.<br>**Note:** Use only the automatic mode for rogue APs that are in-network (in the backhaul network of your organization). Otherwise, automatic mitigation can impact the normal operation of valid APs belonging to a nearby business by blocking their wireless clients from connecting to their APs. Reference the appropriate FCC regulations that prohibit Wi-Fi blocking in these cases. |

**Table 158: Settings for WIPS policy (continued)**

| Setting | Description |
|---|---|
| Detect and Mitigate rogue clients every | After you enable rogue detection on an AP, it scans detected rogue APs for clients during the period that you specify. If you manually start mitigation against a rogue, the AP not only continues scanning for clients during this period, it also sends deauthentication frames to the rogue AP and to any detected clients during the same period.<br>For example, if you leave this at the default setting of 1 second, the AP checks for rogues and attacks them every second. Each time an AP checks if there are clients associated with a detected rogue, it must switch channels for about 80 milliseconds (unless it happens to be using the same channel as the rogue).<br>To minimize channel switching, choose an AP that is on the same channel as the rogue to perform the mitigation. The Rogue AP list shows which channel the rogue is using. If none of the APs are using the same channel, choose the one with the fewest clients. Finally, if all the APs are busy and on different channels from the rogue, consider reducing the amount of channel switching by increasing the period so that the associated client check occurs less frequently. You can change the duration from 1 to 600 seconds (10 minutes). |
| Repeat mitigation for detected rogue clients | Specify how many consecutive periods to spend attacking a rogue AP and its clients before allowing client inactivity to stop and commence a countdown to end the mitigation. If you use the default settings for both the length of the mitigation period and the consecutive number of periods, an attack lasts for 60 seconds before stopping because of client inactivity. The range is from 0 to 2,592,000 seconds (30 days). A value of 0 means that mitigatory APs send deauthentication frames for the entire amount of time that a mitigation effort is in effect. |
| Limit mitigation efforts per rogue AP to | The maximum length of time that an attack against a rogue AP can last. If the length of client inactivity does not cause the attack to be suspended or if you do not manually stop the attack, the AP stops it after this time limit elapses. The default duration is 14,400 seconds (4 hours), which means that an AP continues checking for clients of a detected rogue for up to four hours and mitigates them if it finds them. The mitigation might stop sooner if the period of client inactivity lasts long enough to stop it. You can change the maximum time limit between 0 and 2,592,000 seconds (30 days).<br>In cases where the response time to detect a rogue AP would be greater than the default duration of four hours, consider increasing the duration to enable more time to locate the AP before ending the mitigation process. A value of 0 means that the client detection and mitigation continues indefinitely, unless the client inactivity period elapses. |

**Table 158: Settings for WIPS policy (continued)**

| Setting | Description |
|---|---|
| Stop mitigation if no client activity is detected in | Set the period of time to stop the mitigation process if the AP no longer detects that clients are associated with the rogue AP. During this time, the AP stops sending DoS attacks but continues checking if any clients form new associations with the targeted AP. If the AP detects any associated clients before this period elapses, it sends a deauthentication flood attack and resets the counter. If there are no more clients associated with the AP after this period, the AP stops the mitigation process even if there is still time remaining in the maximum time limit. |
| Max number of mitigator APs per rogue AP | (Applies only to automatic mode.)<br>For automatic mitigation, hive members choose one AP to be the arbitrator, which is the one to which all the detector APs send reports. The arbitrator AP also determines which detector APs perform mitigation. When they start, they become mitigatory APs. Set the number of mitigatory APs that the arbitrator AP can automatically assign to attack a rogue AP and its clients. If you set the maximum as 0, all the detector APs can be assigned to perform rogue mitigation. |

Related Links

Configure WIPS on page 445

## Configure a Location Server

This task is part of the network policy configuration workflow. Use this task to enable and configure a location server as part of a network policy.

1. Go to **Configuration** > **Network Policies**.
2. Select an existing network policy, and then select , or to add a new one, select ..
3. After you save the **Policy Details**, select **NEXT** or **2 Wireless**.
4. From the **Application Management** menu, select **Location Server**.
5. Toggle **Location Server** to **ON**, and configure the settings, or select  and choose an existing location server.

**Table 159: Location server settings**

| Setting | Description |
|---|---|
| Name | (Required)<br>Type a **Name** for the location server. |
| Description | Type a **Description** for the location server. Although optional, descriptions can be helpful when you are troubleshooting your network. |

**Table 159: Location server settings (continued)**

| Setting | Description |
|---|---|
| Client Location Tracking | Toggle the setting **ON** to enable tracking. Enable this setting to track the location of currently associated client, rogue APs, and devices carrying RFID (radio frequency identification) tags. |
| Track Client Location Using | Choose one of the options:<br>• Extreme Networks Location Server<br>• AeroScout Location Server<br>• Tazmen Sniffer Protocol (Ekahau, etc...) |

Related Links

Configure the SSID for a Standard Wireless Network on page 308

## Install CA Certificates

This task is part of the network policy configuration workflow. Use this task to install CA certificates as part of a network policy.

1. Go to **Configuration** > **Network Policies**.
2. Select an existing network policy, and then select , or to add a new one, select .
3. After you save the **Policy Details**, select **NEXT** or **2 Wireless**.
4. From the **Application Management** menu, select **Certificates**.
5. Toggle **Install CA Certificates** to **ON**.
6. Select , and then choose a WIPS policy object from the menu.

   If the menu is empty, or does not contain the entry that you want, select . For more information, see Import a Certificate or Key on page 559.

Related Links

Configure the SSID for a Standard Wireless Network on page 308
Import a Certificate or Key on page 559

## Configure a Layer 2 IPsec VPN Service

Layer 2 IPsec VPN is a logical extension of the Layer 2 broadcast domain across an IPsec VPN tunnel. After configuration, it is available for use in multiple network policies.

**Note**
A Layer 2 VPN server on an AP can terminate a maximum of 128 tunnels. A Layer 2 VPN Gateway Virtual Appliance can terminate up to 1024 tunnels.

Because the NAT mechanism on the device involves both the source IP address and source port number, wireless clients can only send TCP or UDP traffic. Note that the clients will be unable to ping local servers because ICMP does not use port numbers.

When a wireless client associates with a device, the device applies a user profile to traffic from that client. If the device is a VPN client with a user profile tunnel policy, the device tunnels that traffic back to a VPN server at the primary site. The clients receive network settings from a DHCP server at the primary site, query DNS servers at the primary site for domain name resolution, and access other network servers through the tunnel to any site in the VPN network.

Layer 2 IPsec VPNs tunnel traffic between APs functioning as VPN clients at remote sites and a VPN Gateway Virtual Appliance or Extreme Networks APs functioning as VPN servers at the corporate site, providing Layer 2 extensions of the main network. You can define at least one VPN server or two for redundancy. Each VPN client must belong to the same management network as the VPN server and build a GRE (Generic Routing Encapsulation) tunnel between the client and server. DHCP traffic is also tunneled, so clients receive IP addresses from the DHCP server at the corporate site just as if they were on the primary network.

This task is part of the network policy configuration workflow. Use this task to configure a new Layer 2 IPsec VPN service as part of a network policy.

1. Go to **Configuration** > **Network Policies**.
2. Select an existing network policy, and then select , or to add a new one, select ..
3. After you save the **Policy Details**, select **NEXT** or **2 Wireless**.
4. From the **Network Services** menu, select **Layer2 IPsec VPN Services**.
5. Toggle **Layer 2 IPsec VPN Service** to **ON**.
6. To use an existing service, select and choose an existing object, or to add a new one, select .
7. Configure the Layer 2 VPN Services Settings on page 451.

Related Links

Layer 2 VPN Services Settings on page 451
Configure the SSID for a Standard Wireless Network on page 308

## Layer 2 VPN Services Settings

**Table 160: Settings for Layer 2 VPN services**

| Setting | Description |
|---|---|
| Name | Type a name for the service. |
| Description | (Optional)<br>Type a description. Although optional, descriptions can be helpful when you are troubleshooting your network. |
| **Device VPN Server and Device VPN Client Settings** | |
| Single Device VPN Server | Select **Single Device VPN Server** if you are not implementing redundant VPN servers. |
| Redundant Device VPN Servers | Select **Redundant Device VPN Servers** to configure a redundant VPN server.<br>Configure the settings for **Device VPN Server 1** and **Device VPN Server 2**. |

**Table 160: Settings for Layer 2 VPN services (continued)**

| Setting | Description |
|---|---|
| Device VPN Server | Select an AP with Layer 2 IPsec VPN services enabled. |
| Server Public IP Address | Auto-populated based on the selected VPN server settings. To change this setting, type the IP address of a VPN server that VPN clients can reach across the network.<br><br>**Note:**<br>If the VPN server is behind a NAT device, enter the address of the MIP address on the NAT device.<br>If there is no NAT device in front of the VPN server, enter the mgt0 IP address of the server. |
| Server MGT0 IP Address | Auto-populated and read-only. |
| Server MGT0 Default Gateway | Auto-populated and read-only. |
| Client Tunnel IP Address Pool Start | Type the first IP address of the range of addresses that the VPN server assigns to tunnel interfaces on VPN clients during the Xauth phase of tunnel setup.<br>As a best practice, put this address pool in the same subnet as the VPN server mgt0 interface, and the same subnet as the addresses that the DHCP server assigns to wireless clients through the tunnel. If the tunnel interfaces are in a different subnet, you must define a route the VPN server default gateway router uses to forward traffic destined for the tunnel interface, and traffic destined for the wireless clients to the VPN server mgt0 interface. |
| Client Tunnel IP Address Pool End | Type the IP address at the end of the range of IP addresses in the address pool. |
| Client Tunnel IP Address Pool Netmask | Type the netmask that defines the subnet to which the tunnel interfaces belong. |
| Device VPN Client DNS Server | Select the DNS server IP address or host name object that VPN clients use to resolve domain names, or select + to define a new one. |
| **User Profiles for Traffic Management**<br>ExtremeCloud IQ displays a list of available user profiles, for which traffic can be forwarded through the Layer 2 IPsec VPN tunnel or forwarded without tunneling. | |
| VPN Tunnel Mode | In the **VPN Tunnel Mode** column, select **Enable** to enable VPN clients to tunnel traffic for specific user profiles. |
| Tunnel All Traffic | To tunnel all client traffic, select **Tunnel All Traffic**. |
| Split Tunnel | To enable split mode tunneling, select **Split Tunnel**. |

Related Links

Configure a Layer 2 IPsec VPN Service on page 450

## Settings for Multi-Link Operation

Multi-Link Operation (MLO) is a core capability in Wi-Fi 7 that allows devices to simultaneously connect to and use multiple frequency bands (2.4 GHz, 5 GHz, and 6 GHz) at the same time. MLO supports various modes, including:

- **Simultaneous Transmit and Receive (STR):** The device transmits and receives data on multiple links at the same time.
- **Nonsimultaneous Transmit and Receive (NSTR):** The device can only transmit or receive on one link at a time, but it can switch between links quickly.

MLO is supported on the AP3020, AP3020X, AP3020W, AP4020, AP4020X, AP4020FX, AP4060, AP4060X, and AP5020 switches. To enable MLO, the following conditions must be met:

- Security for the SSID must be WPA3(SAE).
- The 802.11k protocol must be enabled.
- Transition Mode must be disabled.
- The 2.4 GHz, 5 GHz, and 6 GHz frequency bands must enabled simultaneously.

# Configuration | Guest Access

Guest Access | Splash Templates on page 454
Guest Access | Users on page 458
Guest Access | Settings on page 460
Guest Access | Notification Policies on page 461
Guest Access | Onboarding on page 462

Guest Access is a comprehensive guest management and engagement solution integrated into Extreme Cloud IQ (NEW). Use the **Guest Access** menu to manage guest onboarding, user accounts, access policies, notifications, and splash page templates.

Go to **Configuration** > **Guest Access**.

The **Guest Access** menu contains the following options:

- Splash Templates
- Users
- Settings
  - Authorization Policy
  - Access Groups
- Notification
  - Policy
- Onboarding
  - Policy
  - Rules

## Guest Access | Splash Templates

ExtremeCloud IQ (New) provides templates that you can customize for your guest access splash screen. The splash screen is the initial page that the system displays before users access a website, software application, or event page.

To manage captive portal splash pages for guest users, go to **Configuration** > **Guest Access** > **Menu** > **Splash Templates**.

The page contains the following tabs:

**System Templates**

The system templates are predefined captive portal templates for common guest onboarding scenarios, provided by Extreme Networks. You can clone or download a system template and customize it according to your deployment requirements.

**User Templates**

User templates are the customized splash page templates that you create for application to network locations as required by your organization.

Table 161 lists the actions that are available on the **User Templates** tab:

**Table 161: User Templates tab: Actions**

| Action | Description |
|---|---|
| Upload | Upload a customized splash template |
| Apply | Apply a template to a network and location |
| Edit | Open the splash template editor |
| Download | Download a template |
| Delete | Delete a template |
| Mapping Summary | View splash template mapping information |

## Create a Splash Template

Use this task to create a new splash template. The **Splash Template Editor** provides a drag-and-drop interface for designing captive web portal pages. The following default pages are available:

- **Landing**: Displays the initial page that guest users see when they access the captive portal.
- **Welcome**: Displays a confirmation or welcome message after successful authentication or registration.
- **Failure**: Displays an error message when authentication, registration, or onboarding fail.

You can optionally add a **Login** page that displays login options for guest users.

1. Go to **Configuration** > **Guest Access** > **Menu** > **Splash Templates**.
2. Select **Create**.

   The **Splash Template Editor** opens.
3. Select a page to configure: **Landing**, **Welcome**, or **Failure**, or select  and choose the page type.
4. Use the **Themes** tab to configure the page layout and visual appearance.

   The **Themes** tab provides column layouts, sidebar layouts, and predefined page templates.

5. Use the **Widgets** tab to add content and interactive elements to the page.
   Drag widgets onto the design canvas and configure them as required.

**Table 162: Available widgets**

| Widget | Description |
|---|---|
| Text | Adds formatted text content |
| Image | Adds image files |
| HTML | Adds custom HTML or JavaScript |
| Slide Show | Adds an image slideshow |
| Video Content | Adds video content |
| Button | Adds a hyperlink button |
| Registration Form | Adds a guest registration form |
| Login Options | Adds login or Accept & Connect actions |
| Social Options | Adds Google or LinkedIn sign-in options |
| Terms and Conditions | Adds Terms and Conditions and Privacy Policy links |
| Login Form | Adds a passcode login form |
| WiFi Logout | Adds a logout button |
| Redirect | Redirects users to a specified URL |

6. Use **Page Settings** to customize the appearance of the selected page.
   Page settings apply only to the currently selected page.

**Table 163: Available page settings**

| Setting | Description |
|---|---|
| Background Color | Specifies the background color for the selected page. Specify a hexadecimal color value or select a color using the color picker. |
| Upload Image | Upload a custom image to use as the page background. Select **Select File** and then select **Upload** to add the image. |
| Gallery Images | Select a predefined image from the gallery and use it as the page background. |
| Background Repeat | Specify how to display the background image when the image size is smaller than the page. Select a repeat mode such as **No Repeat**, **Repeat**, **Repeat Horizontal**, or **Repeat Vertical**. |

**Table 163: Available page settings (continued)**

| Setting | Description |
|---|---|
| Background Attachment | Specify how the background image behaves when users scroll the page. Select **Scrolling** to allow the image to move with the page content, or **Fixed** to keep the image stationary. |
| Reset Background | Remove the current background configuration and restores the default background settings. |

7. Select **Save**.

## Clone a System Template

Use this task to create a template by cloning and editing a system template.

1. Go to **Configuration** > **Guest Access** > **Menu** > **Splash Templates**.
2. Select the **System Templates** tab.
3. Select the corresponding **Clone** icon for the template you want to copy.

   The template opens in the splash template editor.
4. Customize the cloned template.

   For information about the settings and widgets, see Create a Splash Template on page 455.
5. Select **Save**.

## Download a System Template

Use this task to download a system template to save it locally for reference or offline customization.

1. Go to **Configuration** > **Guest Access** > **Menu** > **Splash Templates**.
2. Select the **System Templates** tab.
3. Select the corresponding **Download** icon for the template you want to save.
4. Browse to and select the save location, and select **Save**.

After editing a template offline,

## Upload a User Template

Use this task to upload a splash template that you customized offline.

1. Go to **Configuration** > **Guest Access** > **Menu** > **Splash Templates**.
2. Select the **User Templates** tab.
3. Select .
4. Specify a name for the template, and then use **Select File** browse to the template file (.tar format) and select it.
5. Select **Upload**.

## Apply a Splash Template

Use this task to apply a custom splash page template to a network and location.

1. Go to **Configuration** > **Guest Access** > **Menu** > **Splash Templates**.
2. Select the **User Templates** tab.
3. Select the **Apply** icon.
4. Select one or more locations.
5. Select a network.
6. Select **Apply**.

**Note**
The **Apply** button is available only after you select both a location and network.

# Guest Access | Users

The **User Management** page displays the list of users in table format. Use this page to create and manage guest user accounts and bulk vouchers for guest network access.

Go to **Configuration** > **Guest Access** > **Menu** > **Users**.

## Create a Guest User

Use this task to manually create a guest user account.

1. Go to **Configuration** > **Guest Access** > **Menu** > **Users**.
2. Select **Create User** > **Create User**.
3. In the **Create User** dialog, configure the settings.

**Table 164: Guest user settings**

| Setting | Description |
|---|---|
| First Name | Specify the first name of the guest user. |
| Last Name | Specify the last name of the guest user. |
| Email | Specify the email address of the guest user. |
| Mobile | Specify the mobile number of the guest user. |
| Use as username/password | Use the email address or mobile number as the username and password. |
| Username* | Specify the login username for the guest account. |
| Password* | Specify the password for the guest account. |
| Access Group | Specify the access group assigned to the user.<br>Access Groups determine the network access permissions assigned to the guest user after authentication. Select an existing Access Group from the drop-down list to associate the user with the required authorization policy. |
| Location | Specify the location associated with the guest user. |
| Organization | Specify the organization or company name. |

**Table 164: Guest user settings (continued)**

| Setting | Description |
|---|---|
| Reason | Specify the reason for creating the guest account. |
| Start Date/Time** | Specify the date and time when the account becomes active. |
| Expiry Date/Time** | Specify the date and time when the account expires. |

* Select **Generate** next to the **Username** or **Password** field to automatically generate credentials.

** The **Start Date/Time** and **Expiry Date/Time** fields determine the validity period for the guest account. The guest user can authenticate only during the configured validity period.

4. Select **Create**.

   Alternatively, select **Clear** to remove all configured values from the dialog.

## Download Guest User Details

Use this task to download the details for guest user accounts as a .CSV file.

1. Go to **Configuration** > **Guest Access** > **Menu** > **Users**.
2. Select .
3. Use the check boxes and corresponding menus to select the criteria to apply, and then select **Download**.

   You can download users according to **Network**, **Location**, and **Time**.

   **Note**
   If no user accounts match the selected criteria, the download fails.

4. Choose the save location, and then select **Save**.

## Delete Guest Users

Use this task to manually delete one or more guest user accounts.

1. Go to **Configuration** > **Guest Access** > **Menu** > **Users**.
2. To delete a single guest user, select  for the user account, and then select **Delete**.
3. To delete multiple guest users, select the corresponding check boxes and then select **Delete**.

   When you select multiple users, the **User Management** page displays the number of selected users and the **Delete** option above the table header row.

## Create Bulk Vouchers

Use this task to generate multiple guest access credentials in bulk. Bulk vouchers are commonly used for temporary guest access deployments such as conferences, visitor onboarding, classrooms, events, or shared guest access environments.

The **Start Date/Time** and **Expiry Date/Time** fields determine the active duration for all vouchers in the batch. Users can authenticate using the generated vouchers only during the configured validity period.

1. Go to **Configuration** > **Guest Access** > **Menu** > **Users**.
2. Select **Create User**.
3. Select **Create Bulk Vouchers**.
4. In the **Create Bulk Vouchers** dialog, configure the settings.

**Table 165: Bulk voucher settings**

| Setting | Description |
|---|---|
| Access Group | Specify the access group assigned to all generated vouchers. |
| Number of Vouchers | Specify the number of vouchers to generate. |
| Description | Specify a description for the voucher batch. |
| Location | Specify the location associated with the vouchers. |
| Start Date/Time | Specify when the vouchers become active. |
| Expiry Date/Time | Specify when the vouchers expire. |

5. Select **Create Vouchers**.

## Guest Access | Settings

Use authorization policies and access groups to specify the settings for guest users.

Authorization policies define session and inactivity timeout values applied after successful guest authentication.

Access groups associate guest users with authorization policies to control network access behavior.

### Add an Access Group

Use this task to associate guest users with authorization policies. Access groups simplify guest access management by applying common authorization settings to multiple guest users. When guest users are mapped to an access group during onboarding or user creation, the associated authorization policy automatically applies.

1. Go to **Configuration** > **Guest Access** > **Menu** > **Settings** > **Access Groups**.
2. Select **Add Group**, and configure the settings.

**Table 166: Access group settings**

| Settings | Description |
|---|---|
| Group Name | Specify the name of the access group. |
| Description | Specify the description of the access group. |
| Authorization Policy | Specify the authorization policy associated with the access group. |

3. Select **Add**.

## Add an Authorization Policy

Use this task to add an authorization policy. Authorization policies define how long guest users can remain connected and how ExtremeCloud IQ (New) handles inactive sessions. These policies can be associated with access groups and applied during guest onboarding workflows.

1. Go to **Configuration** > **Guest Access** > **Menu** > **Settings** > **Authorization Policy**.
2. Select **Add Authorization Policy** and configure the settings.

**Table 167: Authorization policy settings**

| Settings | Description |
|---|---|
| Policy Name | Specify the name of the authorization policy. |
| Policy Description | Specify the description of the authorization policy. |
| Session Timeout (seconds) | Specify the maximum session duration for authenticated users.<br>When the configured session timeout expires, the guest user session terminates and the user must authenticate again to regain network access. |
| Inactivity Timeout (seconds) | Specify how long a session remains active without user traffic.<br>If no user activity is detected during the configured interval, the session terminates automatically. |

3. Select **Add**.

# Guest Access | Notification Policies

Notification policies define how ExtremeCloud IQ (New) sends onboarding information to guest users and sponsors.

You can configure notification policies to deliver:

- One-time passcodes
- Guest credentials
- Sponsor approval requests
- Guest onboarding notifications

Guest Access supports both SMS and email-based notifications.

The **Notification Policy** page displays configured notification policies and lists the specified **Description** and **Policy Type** for each. Go to **Configuration** > **Guest Access** > **Menu** > **Notification** > **Policy**.

## Add a Notification Policy

Use this task to configure a notification policy.

1. Go to **Configuration** > **Guest Access** > **Menu** > **Notification** > **Policy**.
2. Select **Add Notification Policy**.
3. Type a **Policy** name.
4. (Optional) Type a **Description** for the policy.
5. Select a policy type.
   - **User**: Sends notifications directly to guest users.
   - **Sponsor**: Sends notifications to sponsors during approval workflows.
6. Enable one or both notification methods:
   - **SMS Notification**: Sends onboarding information using SMS messages.
   - **Email Notification**: Sends onboarding information using email messages.
7. Use the formatting controls on the toolbar and the supported variables to configure the notification content for each selected notification method.

**Table 168: Supported variables**

| Email Notification | SMS Notification |
|---|---|
| • GM_NAME<br>• GM_USERNAME<br>• GM_PASSCODE<br>• GM_EMAIL<br>• GM_MAC<br>• GM_SNAME<br>• GM_ACTION_URL | • GM_NAME<br>• GM_USERNAME<br>• GM_PASSCODE<br>• PERMIT_URL<br>• DENY_URL |

8. Select **Add**.

# Guest Access | Onboarding

Guest access uses onboarding policies and onboarding rules together to control guest onboarding behavior. Onboarding policies define the conditions and actions used during onboarding, while onboarding rules associate those policies with specific WLANs and locations.

Go to **Configuration** > **Guest Access** > **Menu** > **Onboarding**.

## Onboarding Policy

Onboarding policies define how guest access handles guest registration and authentication requests. An onboarding policy consists of one or more criteria. Each criterion contains:

- Conditions used to identify guest users
- Actions applied when the conditions are matched

You can create onboarding policies for different guest access scenarios. The **Onboarding Policies** page displays configured onboarding policies and the number of criteria associated with each policy.

## Onboarding Rules

Onboarding rules associate onboarding policies with specific WLANs and locations.

When a guest user attempts to access the network, Guest Access evaluates the configured onboarding rules and applies the matching onboarding policy based on the configured precedence value.

The **Rules** page displays configured onboarding rules and their associated onboarding policy, WLAN, location, and precedence value.

## Add an Onboarding Policy

Use this task to configure an onboarding policy that defines how guest access handles guest registration and authentication requests. A policy can contain multiple criteria to support different onboarding scenarios.

1. Go to **Configuration** > **Guest Access** > **Menu** > **Onboarding** > **Policy**.
2. Select **Add Onboarding Policy**.
3. Provide the following information:
   - **Policy Name**
   - **Description**
4. Configure one or more criteria.

   Conditions identify guest users based on onboarding attributes. Each criterion includes:
   - Criteria description
   - Conditions
   - Action

   To configure additional matching conditions within a criterion, select **Add Condition**. The following condition types are supported:

**Table 169: Supported condition types**

| Condition Type | Description |
|---|---|
| User Email Domain | Match users based on email domain |
| Sponsor Email Domain | Match sponsor email domains |
| Social Type | Match users based on social sign-in provider |
| User Type | Match users based on guest category |
| User Device Count | Match users based on the number of registered devices |

   When multiple conditions are configured within a criterion, all conditions must match before the system applies the policy.
5. To specify how the system responds when the configured conditions are matched, choose one of the following **Actions**.
   - **Deny Access**
   - **Register Client**

6. To send status notifications to guest users during onboarding workflows, enable **Update User**.
7. Select **Create**.

# Configuration | Common Objects

Policy Configuration on page 466
Basic Configuration on page 495
Security Configuration on page 507
QoS Configuration on page 512
Management Configuration on page 519
Network Configuration on page 522
Authentication Configuration on page 552
Certificate Configuration on page 554
Clone a Common Object on page 561
Delete a Common Object on page 561

Use the information and tasks in this chapter to define objects for use throughout the configuration process, in particular when you configure network policies.

The landing page for each configuration object type displays a list of existing objects in table format. Available actions vary depending on the configuration object type, but typically include the following actions:

- Add ()
- Edit ()
- Clone ()
- Delete ()

Most of the tasks in this chapter cover how to configure (add or edit) objects. See the following general tasks for managing objects:

- Clone a Common Object on page 561
- Delete a Common Object on page 561

**Note**

The assigned **Access Scope** determines an administrator's access to **Common Objects**. Only Administrators assigned global access can see and work with common objects created for sites to which they are not assigned. This restriction applies only to new objects created after enabling the Access Scope feature. For more information about site assignment, see Table 195 on page 581.

# Policy Configuration

The topics in this section provide details about configuration objects related to network policy.

Related Links

Configure AP Templates on page 466
Configure Auto-Provisioning on page 467
Configure Bonjour Gateway Settings on page 470
Configure Classification Rules on page 472
Configure Client Monitor Profiles on page 474
Configure Cloud Config Groups on page 474
Configure Fabric Attach Profiles on page 475
Configure Hives on page 476
Configure Hotspot Profiles on page 479
Configure Hotspot Service Provider Profiles on page 479
Configure IoT Profiles on page 479
Manage Port Types on page 480
Delete Instant Secure Port Profiles on page 480
Delete Instant Port Profiles on page 480
Configure Radio Profiles on page 481
Configure SDR Profiles on page 490
Configure SSIDs on page 492
Configure a Switch Template on page 492
Configure URL Filtering Detail on page 493
Configure URL Filtering on page 494
Configure User Profiles on page 495

## Configure AP Templates

Before you begin, create a network policy for the access points (APs).

Create AP templates with default settings for all APs, and settings that Extreme Cloud IQ (NEW) applies when APs are onboarded. Default AP settings can then be modified individually as required. AP templates enable quick AP deployment, with most of the port settings already applied by the associated template. Some devices have extra possible configuration options, depending on the device model.

**Note**
When AP templates and auto-provisioning rules are both in place for an AP, the auto-provisioning rules are applied during onboarding and the AP template is ignored.

Use this task to configure an AP template.

1. Go to **Configuration** > **Network Policies**, select **Menu**, and then go to **Common Objects** > **Policy** > **AP Template**.

2. Select an existing AP Template, and then select , or to add a new one, select .

   To delete the selected template, select .
3. Enter or edit the **Name**.
4. Select the ports or interface icons on the template graphic.
   a. To select all of the ports and interfaces, choose **Select All Ports**.
   b. To deselect all of the ports and interfaces, select **Deselect All Ports**.
5. To **Assign** an Ethernet port profile, see Assign an Ethernet Port Profile on page 392.
6. To configure **Wireless Interfaces**, see Configure Wireless Interfaces for an AP Template on page 394.
7. To configure **Wired Interfaces**, see Configure Wired Interfaces for an AP Template on page 416.
8. To configure **SES-imagotag**, see Electronic Shelf Labels on page 388.
9. To configure **Advanced Settings**, see Configure AP Template Advanced Settings on page 418.
10. Select **SAVE TEMPLATE**.

Continue configuring the network policy.

Related Links

Add a Network Policy on page 278
Configure Auto-Provisioning on page 467
Configure Device Templates on page 391

## Configure Auto-Provisioning

Although AP templates function similarly to auto-provisioning rules, the best-practice recommendation is to use AP templates rather than auto-provisioning rules to configure APs as they are onboarded.



**Note**
If AP templates and auto-provisioning rules are both in place when the AP is onboarded, ExtremeCloud IQ (New) ignores the AP template and applies the auto-provisioning rules.

Identify devices for auto provisioning by adding or importing serial numbers or IP subnetworks. Import serial numbers by selecting devices that have already been on-boarded, importing a CSV file populated with serial numbers, or entering serial numbers manually. You can use a combination of any of these methods. To add or import IP subnetworks to an auto-

provisioning profile, enter IP subnetworks manually or import a CSV file containing the subnetworks. You can also use IPv6 addresses to identify subnetworks.

**Note**
Auto-provisioning rules are based on device models. You can define multiple profiles for the same model and distinguish which devices get which profile by specifying a serial number or IP address.

1. Go to **Configuration** > **Network Policies**, select **Menu**, and then go to **Policy** > **Auto Provisioning**.
2. Select an existing rule, and then select , or to add a new one, select .
3. Type a **Name** for the rule.
4. (Optional) Type a **Description** for the rule.
5. Select a **Device Function**.
6. Select a **Device Model**.

   The model that you choose determines the available device functions, interface settings, and radio settings.
7. Select **Serial Number** to restrict automatic provisioning to particular serial numbers.
   a. Choose the **Select Serial Numbers** bar.
   b. Add serial numbers from the imported list, import them from a CVS file, or add them manually.
8. Choose **IP Subnetworks** to auto-provision devices by IP subnetworks.
9. Choose **Select IP Subnetworks**, then add IP Subnetworks from either a CVS file or manually.

   **Note**
   To create an auto provisioning profile that contains IP subnetworks, the devices in the profile cannot have been previously onboarded.

   When you create multiple auto provisioning profiles for the same device model and use serial numbers or IP subnetworks to identify them, be aware of the following situations:

   - If a conflict arises because two auto provisioning profiles applied to the same device, for example, one profile based on the serial number and the other based on the subnetwork, the profile based on the serial number takes precedence.
   - The same serial number must not appear in more than one auto provisioning profile.
10. Select a **Network Policy** from the drop-down list.
11. Select the **Country** for the device from the dropdown list.

    If you later select the **Upload configuration automatically** check box, ExtremeCloud IQ (New) applies the country code specified here when it automatically pushes a configuration to devices during the initial CAPWAP connection.

Auto-assign Location

12. Select **Assign** to assign a **Default Location** to all the devices in the auto provisioning profile.

    **Note**
    You can only assign devices to a floor within a building.

13. If you enabled **Select IP Subnetworks**, select + to **Select a Location and IP Subnetwork**.
    a. Select a **Subnet** and **Location**.
    b. Select **Save**.

Advanced Settings

14. Select **Upload device firmware upon device authentication** to upload an image automatically.
    a. Select the **Golden** version if you want to automatically upload the version with fewer features, but fully tested and super stable for those environments where stability is more important than feature richness.
    b. Select the **Latest** version if you want to automatically upload new features, some of which might contain bugs.
15. Select **Upload configuration automatically** to automatically upload a pre-defined configuration, which consists of a network policy, two radio profiles, a topology map, a pair of root and read-only administrators, and CAPWAP settings.
16. Select **Reboot after uploading** to activate the uploaded image and configuration by rebooting the devices.

    If your deployment includes mesh points, do not select this option. Reboot the devices manually so that you can control the order in which the devices reboot.

Device Credentials

17. Select **Enable Device Credential** to set device credentials.
    - **Root Admin Configuration**: Enter a name and password for the root admin for the device. ExtremeCloud IQ (New) uses root admin log in credentials to make SSH connections to configured devices and upload full configurations to them. This admin can also access the device through Telnet, SSH, or console connections.
    - **Read-Only Admin Configuration**: Enter a name and password for an admin that has read-only privileges.
18. Select **Enable CAPWAP configurations** to configure primary and secondary CAPWAP servers.
    - **Primary CAPWAP Server**: From the Primary CAPWAP Server drop-down list, choose the ExtremeCloud IQ (New) address with which you want devices to form a CAPWAP connection first. If you do not see the address you need, select the plus sign and add an IP address or host name.
    - **Backup CAPWAP Server**: If you are deploying ExtremeCloud IQ (New) as a standalone device, leave this field empty. If it is in an HA pair behind a NAT device from its configured devices, use the drop-down menu to select the domain name or MIP linking to its MGT interface. If you do not see the address you need, select the plus sign and add an IP address or host name.
    - **Shared Key for Authentication**: To change the passphrase, enter a new alphanumeric string in the **Passphrase** and **Confirm Passphrase** fields.

Interface Settings

19. To **Enable Interface Settings**, set the slider to **On**.
20. Configure a Wireless interface. See Configure Wireless Interfaces for an AP Template on page 394 for general instructions.
21. Configure Wired interface. See Configure Wired Interfaces for an AP Template on page 416 for general instructions.

22. When the auto-provisioning rule configuration is complete, select **Save** to commit the changes, or select **Cancel**.

## Configure Bonjour Gateway Settings

Extreme Networks devices can function as Bonjour Gateways and forward service advertisements across VLAN or subnet boundaries.

**Note**
You must add at least one filter rule to the Bonjour Gateway profile before you can save it.

Use this task to define a Bonjour Gateway profile that specifies which VLANs the Bonjour Gateway scans, and which services it shares with other Bonjour Gateways.

1. Go to **Configuration** > **Network Policies**, select **Menu**, and then go to **Policy** > **Bonjour Gateway Settings**.
2. Select an existing Bonjour Gateway, and then select , or to add a new one, select ..
3. Configure the following settings.

**Table 170: Bonjour Gateway Settings**

| Field | Description |
|---|---|
| Name | The Bonjour Gateway name for referencing in a network policy. |
| Description | An optional description for the Bonjour Gateway. |
| Scan the following VLANs for services | The VLANs that you want the Bonjour Gateway to scan for service advertisements.<br><br>**Note:** Use commas to separate multiple VLAN IDs (do not include a space after a comma) and dashes to indicate ranges. |

4. Select to add a Bonjour filter rule.
5. Configure the settings for the Bonjour filter rule.

   See Bonjour Filter Rule Settings on page 471.
6. Select **Save**.

Related Links

Bonjour Filter Rule Settings on page 471

*Bonjour Filter Rule Settings*

**Table 171: Bonjour Filter Rule Settings**

| Field | Description |
|---|---|
| Service | Choose the name of a previously defined **Service**, or enter the name of the service in the field.<br>To add a new Service:<br>1. Select .<br>2. Enter the service **Name**.<br>3. Enter the **Type**.<br>4. Select **Save**. |
| From VLAN Group | Choose the VLAN group from which to share services.<br>**Note:** If you do not want to restrict sharing services based on source VLANs, choose **Any**. To create a new VLAN group, select the plus sign. Enter a name for the group, the VLANs to include, a description, and then save your new group.<br>To add a new From VLAN Group:<br>1. Select .<br>2. Enter the service **Name**.<br>3. Enter the **VLANs**. VLANs can be configured as ranges or individually. Indicate a range with a hyphen. Separate VLAN entries with commas, for example, 1-30, 100-200, 500.<br>4. Enter an optional **Description**.<br>5. Select **Save**. |
| To VLAN Group | Choose the VLAN group to which services are advertised.<br>**Note:** If you do not want to restrict sharing services based on destination VLANs, choose **Any**. To create a new VLAN group, see the previous step.<br>To add a new To VLAN Group:<br>1. Select .<br>2. Enter the service **Name**.<br>3. Enter the **VLANs**. VLANs can be configured as ranges or individually. Indicate a range with a hyphen. Separate VLAN entries with commas, for example, 1-30, 100-200, 500.<br>4. Enter an optional **Description**.<br>5. Select **Save**. |
| Max Wireless Hop | Enter the maximum number of management subnet hops between one Bonjour device and another for the recipient to accept service advertisements. |

**Table 171: Bonjour Filter Rule Settings (continued)**

| Field | Description |
|---|---|
| Realm | Choose the name of an existing **Realm** to apply this rule only to members of that realm.<br><br>**Note:** If the members are not within radio range, you can put them in the same realm by doing either of the following: Place all of the devices on the same map, or manually set the same Bonjour **Realm** name in the **Bonjour Gateway Settings** section in individual device configuration. |
| Apply Realm Filter Advertisement | Enable **Apply Realm Filter Advertisement** to direct the Bonjour Gateway to detect and retransmit only from the specified realm.<br><br>**Note:** By default, the Bonjour Gateway detects and retransmits from the selected VLAN group. |

Related Links

Configure Bonjour Gateway Settings on page 470

## Configure Classification Rules

Before you can use classification rules, you must create a network location, along with cloud config groups, IP addresses, and IP subnets.

You can create classification rules as part of a network policy or as a common object.

- Configure **Device Location** rules to assign different DNS and RADIUS servers and different time zones to different physical locations.
- Configure **Cloud Config Groups** (CCGs) to create user passwords which restrict access to private and personal network devices.
- Configure **IP Address** classification rules to associate user groups so they can communicate using their own private networks.
- Configure **IP Subnet** classification rules to support multiple user-group private networks.
- Configure **IP Range** classification rules for multiple user-group private networks.

Use this task to create a classification rules object. ExtremeCloud IQ (New) supports multiple classification rules for DNS servers, VLANs, RADIUS servers, device templates, user groups, and private client groups (PCGs).

1. Go to **Configuration** > **Network Policies**, select **Menu**, and then go to **Common Objects** > **Policy** > **Classification Rules**.

   To use this task to configure classification rules objects as part of another workflow, skip to Step 3.
2. Select an existing rule, and then select , or to add a new one, select .
3. Enter a **Name** for the rule.
4. (Optional) Enter a **Description** for the rule.

5. Select , and then choose the rule type to configure.

   Choose from the following rule types:

**Table 172: Rule types**

| Selected rule type | Do this |
|---|---|
| Device Location | a. Drill down until you reach the location level at which the device resides.<br>b. Select **Select**.<br>The location appears in the **Classification Rules** table. |
| Cloud Config Group | a. Select the **Match Type**.<br>b. Select and choose an existing group, or select .<br>c. Select **CLOUD CONFIG GROUP**.<br>d. Select **CONTINUE**. |
| IP Address | a. From the **Match Type** menu, select **Contains** or **Does Not Contain**.<br>b. Select and choose an existing IP address, or select .<br>If you do not see the IP address that you want, select **New** to create a new IP address.<br>c. Select **SAVE IP**.<br>d. Select **CONTINUE**. |
| IP Subnet | a. From the **Match Type** menu, select **Contains** or **Does Not Contain**.<br>b. Select and choose an existing IP subnet, or select menu.<br>If you do not see the IP subnet that you want, select **New** to create a new IP subnet.<br>c. Select **SAVE SUBNET**.<br>d. Select **CONTINUE**. |
| IP Range | a. From the **Match Type** menu, select **Contains** or **Does Not Contain**.<br>b. Select and choose an existing IP range, or select .<br>If you do not see the IP range that you want, select **New** to create a new IP range.<br>c. Select **SAVE IP**.<br>d. Select **CONTINUE**. |

6. Select **SAVE RULE**.

Related Links

Add a Cloud Config Group on page 439

## Configure Client Monitor Profiles

First enable Client Monitor.

Use this task to configure client monitor profile policies.

1. Go to **Configuration** > **Network Policies**, select **Menu**, and then go to **Common Objects** > **Policy** > **Client Monitor Profiles**.
2. Select an existing client monitor profile, and then select , or to add a new one, select ..
3. Configure the settings for the Client Monitor Profile policy.

   See Client Monitor Profile Settings on page 201.
4. Select **Save**.

Related Links

Troubleshooting on page 201
Client Monitor Profile Settings on page 201

*Client Monitor Profile Settings*

**Table 173: Client Monitor Profile Settings**

| Field | Description |
|---|---|
| Name | Type a name to identify the Client Monitor Profile policy. |
| **Association Problem** | |
| Trigger Times | Set the number of times an association problem can be triggered, between 1 and 10. |
| Report Interval | Set the interval between reporting an association problem, between 30 and 3600 seconds. |
| **Authentication Problem** | |
| Trigger Times | Set the number of times an authentication problem can be triggered, between 1 and 10. |
| Report Interval | Set the interval between reporting an authentication problem, between 30 and 3600 seconds. |
| **Networking Problem** | |
| Trigger Times | Set the number of times a network problem can be triggered, between 1 and 10. |
| Report Interval | Set the interval between reporting a network problem, between 30 and 3600 seconds. |

Related Links

Configure Client Mode Profiles on page 496

## Configure Cloud Config Groups

Before you begin, configure devices to associate with the cloud configuration groups.

Cloud configuration groups enable administrators to create network-level policies that can be replicated for multiple network roll-out scenarios. Use this task to configure a cloud configuration group.

1. Go to **Configuration** > **Network Policies**, select **Menu**, and then go to **Common Objects** > **Policy** > **Cloud Config Groups**.
2. Select an existing group, and then select , or to add a new one, select ..
3. Type a **Name** for the new group.
4. (Optional) Type a **Description** for the new group.
5. Select real and simulated devices to show the host names in the **Selected Devices** field.

   **Note**
   You can also import a comma-separated-values (CSV) file including the host names, serial numbers, and optional MAC addresses of other devices.

   a. Select **Import**.
   b. Select the CSV file, or drag the CSV file to the **Import Cloud Config Group Members** window.
   c. Select **Submit**.
6. Select **SAVE CLOUD CONFIG GROUP**.

## Configure Fabric Attach Profiles

Before you begin, physically connect the device to a Fabric Connect-enabled switch. To perform the following task, you require the device VLAN ID and I-SID number.

For more information about Fabric Attach, see Fabric Attach on page 439.

Use this task to configure Fabric Attach profiles that you can assign to network policies.

1. Go to **Configuration** > **Network Policies**, select **Menu**, and then go to **Common Objects** > **Policy** > **Fabric Attach Profiles**.
2. Select an existing profile, and then select , or to add a new one, select ..
3. (Optional) Type a **Description** for the new profile.
4. Type a **Name** for the new profile.
5. Select to add a VLAN.
6. Type the associated **VLAN ID** for the device.
7. Select the **I-SID#** for the device from the drop down.
8. Select **SAVE**.

Related Links

Fabric Attach on page 439
Configure Fabric Attach on page 440

## Configure Hives

Use this task to configure a Hive profile object.

1. Go to **Configuration** > **Network Policies**, select **Menu**, and then go to **Common Objects** > **Policy** > **Hives**.
2. Select an existing hive profile, and then select , or to add a new one, select .
3. (Optional) To use existing Hive settings, choose a Hive object from the menu.
4. Configure the Hive Profile Settings on page 288.
5. Apply MAC filters to restrict devices that can join the hive.

   You can select existing filters from the table, or add new filters.
6. From the menu, choose the default action (**Permit** or **Deny**) for devices that have a MAC address or an OUI that does not match the selected MAC filter.
7. Select **SAVE**.

Related Links

Hive Profile Settings on page 288

*Hive Profile Settings*

**Table 174: Hive profile settings**

| Setting | Description |
|---|---|
| Name | Type a **Name** for the new profile. |
| Hive Control Traffic Port | Type the port number for Hive traffic control.<br>Hive communications operate at Layers 2 and 3. The default port number for Layer 3 hive communications and for roaming-related traffic is UDP 3000. If a different service on your network is already using port 3000, you can change this to a number from 1024 to 65535, as long as the new setting is at least 50 greater or less than the current setting. For example, if the current port number is 3000, you can set a new port number higher than 3050. |
| Description | (Optional)<br>Type a description for the new profile. Although optional, entering a description is helpful for troubleshooting and for identifying the profile. |
| **Alarms** | |
| CAPWAP Delay Alarms | Toggle the setting **ON** or **OFF**. |
| **Security** | |
| Encryption Protection | Toggle the setting **ON** or **OFF**.<br>Disable **Encryption Protection** to have ExtremeCloud IQ derive a default password from the hive name. |
| Encryption Password | Choose between **Auto Generate** and **Manual**.<br>Hive members use this password to authenticate to each other over the wireless backhaul link using WPA-PSK CCMP (AES). To see the password that you entered, clear the **Shared Secret** > **Show Password** check box. |

**Table 174: Hive profile settings (continued)**

| Setting | Description |
|---|---|
| MAC-based DoS Prevention Rules | Select **Hive** or **Client**, and modify the settings in the dialog box.<br>Extreme Networks devices ship with default hive- and SSID-level DoS detection settings for some frame types commonly used in DoS attacks. You can raise the thresholds to reduce false alarms or lower them to receive more alarms indicative of spikes in certain types of traffic.<br>• **DoS prevention rules for hives** apply to wireless traffic from all radios that might reach the backhaul or access channel from wireless clients or nearby access points broadcasting on the same channel. You can define settings to detect DoS attacks on the radio channels that a device uses for hive communications and for SSID access traffic.<br>• **DoS prevention rules for clients** apply to traffic originating from a single neighboring radio. The source might be a neighbor member or a nearby device outside the network that is broadcasting on the same channel the Extreme Networks device is using for its wireless backhaul communications, or for SSID access traffic.<br>For both types of rules, you can change the alarm thresholds and enable or disable settings for each DoS Detection type: Probe Requests and Responses, (Re) Associations, Association and Disassociation Requests and Responses, Authentication and Deauthentication, and EAP over LAN (EAPoL). Wireless clients periodically send probe requests to determine whether access points are within range. The threshold determines the number of messages per minute required to trigger an alarm about a possible DoS attack. The alarm interval determines the length between repeated alarms when the number of messages continues to exceed the threshold. |
| **Wireless Mesh Settings** | |
| Request to Send Threshold | Type the maximum frame size that triggers the device to send a request to send (RTS) message, before sending a large frame. The default setting is 2346 bytes. |
| Fragment Threshold | Type the maximum IEEE 802.11 frame size for control traffic sent over the wireless backhaul. The device sends larger frames in fragments. The default setting is 2346 bytes. |
| Require minimum wireless signal strength for creating wireless mesh | Select the check box to require a minimum wireless signal strength for creating wireless mesh, and configure the related settings. |
| Signal Strength Threshold | Use the slider to specify a signal strength between 90 dBm and - 55 dBm.<br>This value is the minimum signal strength required to enable members to form a wireless backhaul link. The default is -80 dBm. |

**Table 174: Hive profile settings (continued)**

| Setting | Description |
|---|---|
| Polling Interval | Type the number of minutes (1 to 60) between polling for the signal strength of neighboring members.<br>A lower interval increases traffic on the network slightly, especially in dense environments. However, a lower interval also increases the responsiveness to changes in signal strength. A higher interval reduces responsiveness to signal strength changes, which can be preferable in environments where severe and frequent signal strength fluctuations cause members to drop and re-establish connections. The default is every 60 seconds. |
| **Client Roaming > Detect neighbor devices** | |
| Devices send keepalive heartbeats every | Set the interval between keepalive heartbeats.<br>The default is 10 seconds, and the range is 5 to 360,000 seconds (100 hours). To calculate the length of time, multiply the keepalive interval by the number of missed keepalives. For example, 10 seconds (interval) x 5 (missed keepalives) results in a neighbor aging out after 50 seconds. |
| Remove neighbor if the number of missed keepalive heartbeats exceeds | Specify the number of missed heartbeats before ExtremeCloud IQ (New) removes a neighbor. |
| **Client Roaming > Share connected client information (Roaming cache)** | |
| Devices send client information every | Specify how often devices send client information. The default is 60 seconds. |
| Remove cached client information when absent from updates after | Specify the number of missed updates, after which ExtremeCloud IQ (New) deletes cached client information for the affected client. |
| Update all hive members within radio range, including Layer 3 neighbors | Select the check box to update all hive members within radio range, including Layer 3 neighbors. |
| Update hive members in the same subnet and VLAN. | Select the check box to update hive members in the same subnet and VLAN. |
| **IP Address Preference** | |
| Use IP address type first with | (Required)<br>Choose the IP address version **IPv4** or **IPv6**. |

Related Links

Configure Hive Policy Settings on page 288

## Configure Hotspot Profiles

Use this task to configure a Hotspot Profile object for reuse in network policies.

**Note**
As a best practice, configure Hotspot Profiles as part of the Network Policy workflow. For more information, see Configure a Hotspot on page 341.

1. Go to **Configuration** > **Network Policies**, select **Menu**, and then go to **Common Objects** > **Policy** > **Hotspot Profiles**.
2. Select an existing Hotspot Profile, and then select , or to add a new one, select ..
3. Configure the Hotspot Settings on page 342.

Related Links

Hotspot Settings on page 342
Configure a Hotspot on page 341

## Configure Hotspot Service Provider Profiles

Use this task to configure a Hotspot Service Provider Profile object for reuse in network policies.

**Note**
As a best practice, configure Hotspot Service Provider Profiles as part of the Network Policy workflow. For more information, see Configure a Hotspot on page 341.

You can also configure a Hotspot Service Provider when you configure a Hotspot Profile object.

1. Go to **Configuration** > **Network Policies**, select **Menu**, and then go to **Common Objects** > **Policy** > **Hotspot Service Provider Profiles**.
2. Select an existing Hotspot Service Provider, and then select , or to add a new one, select ..
3. Configure the Service Provider Profile Settings.

Related Links

Configure a Hotspot on page 341
Configure Hotspot Profiles on page 479
Hotspot Settings on page 342

## Configure IoT Profiles

Use this task to add a new IoT profile to the list, or to edit, clone, or delete existing IoT profiles.

1. Go to **Configuration** > **Network Policies**, select **Menu**, and then go to **Common Objects** > **Policy** > **IoT Profiles**.
2. Select an existing profile, and then select , or to add a new one, select ..
3. Configure the settings as described in Table 151 on page 411 or Table 152 on page 412.

4. Select **Save**.

Related Links

IoT Profiles on page 410
IoT Profile Settings on page 411

## Manage Port Types

The **Port Types** table displays a list of the configured port types. Use this procedure to clone or delete configured port types.

1. Go to **Configuration** > **Network Policies**, select **Menu**, and then go to **Common Objects** > **Policy** > **Port Types**.
2. To clone a port type, select the corresponding check box and then select .
3. To delete a port type, select the corresponding check box and then select .

Related Links

Configure Port Types on page 436

## Delete Instant Secure Port Profiles

You can delete Instant Secure Port Profiles (ISPPs) that you no longer use.

**Note**
To add a new ISPP, see Configure Instant Secure Port Profiles on page 177.

1. Go to **Configuration** > **Network Policies**, select **Menu**, and then go to **Common Objects** > **Policy** > **Instant Secure Port Profiles**.
2. Select the corresponding check boxes for the ISPPs that you want to delete, and then select .

## Delete Instant Port Profiles

You can delete Instant Port Profiles (IPPs) that you no longer use.

**Note**
To add a new IPP, see Configure Instant Port Profiles on page 176.

1. Go to **Configuration** > **Network Policies**, select **Menu**, and then go to **Common Objects** > **Policy** > **Instant Port Profiles**.
2. Select the corresponding check boxes for the IPPs that you want to delete, and then select .

## Configure Radio Profiles

Use this task to create or edit a radio profile object for 2.4-GHz, 5-GHz or 6-GHz device interfaces. For more information about radio profiles, see Radio Profiles on page 395.

**Note**
Extreme Networks provides defaults for each item in this section. The following steps are optional, except for the required radio profile **Name**.

1. Go to **Configuration** > **Network Policies**, select **Menu**, and then go to **Common Objects** > **Policy** > **Radio Profiles**.
2. Select an existing profile, and then select , or to add a new one, select .
3. Type the radio profile **Name**.
4. Type a **Description**.

   Although optional, descriptions can be helpful when you are configuring or troubleshooting your network.
5. Select the desired 802 specification from the **Support Radio Modes** menu.
6. Select a power mode from the **Supported Power Mode** menu.

   **Note**
   Only applicable to AP4020/AP4060/AP5020 and future WiFi 7 APs.
7. To set the optimal maximum power level, enter a value for **Maximum Transmit Power**.
8. To set the minimum power level, enter a value for **Transmission Power Floor**.
9. To set the maximum value the radio power can drop below the current power level, enter a value for **Transmission Power Drop**.
10. To set the maximum number of wireless clients that can use the radio, type a value for **Maximum Number of Clients**.

    (Default: 100, Range: 1-255)

    A lower value permits fewer concurrent connections to the AP and provides a higher quality of service. A high number of concurrent connections to a radio might affect the quality of service. While 100 might be a bit high for a classroom setting, higher values are suitable for larger public spaces, such as cafeterias or gymnasiums. A higher setting is appropriate for APs that serve dense outdoor areas with frequent connections that quickly roam to other areas.
11. Select **SAVE RADIO PROFILE**.

Now that you have completed the basic configuration, you can modify advanced radio profile settings. Remember to select **SAVE RADIO PROFILE** after changing advanced settings.

Related Links

Configure Neighborhood Analysis on page 482
Configure Dynamic Frequency Selection on page 482
Configure Dynamic Channel Switching on page 484
Optimize Radio Usage on page 484
Configure Radio Settings on page 486
Configure Backhaul Failover on page 486

Configure Outdoor Deployment on page 487
Configure RF Interface Reports on page 487
Configure Client SLA Definitions on page 488
Configure WMM QoS Settings on page 489
Configure Sensor Mode Scan Settings on page 490
Radio Profiles on page 395

*Configure Neighborhood Analysis*

Begin configuring a radio profile.

Using background scanning, an AP divides a full background channel scan into several shorter partial scans so they do not interfere with the beacons sent by the AP. The scan takes less time than the beacon interval (100 TU by default), and is spread out over a number of beacon intervals until the AP scans all available channels. Full scans occur at admin-defined intervals, with a default of 10 minutes.

Background scanning is required for WIPS and Layer 3 roaming to function.

**Note**
ExtremeCloud IQ (New) automatically enables background scanning for all DFS enabled radios in the VIQ when you enable AI RRM. When you disable AI RRM, the system automatically disables background scanning.

Use this task to configure neighborhood analysis (background scanning).

**Note**
Extreme Networks provides defaults for each item in this section. The following steps are optional.

1. In the radio profile, go to the **Neighborhood Analysis** section, and enable **Background Scan**.
2. Set the interval between background scans of all radio channels.
   **Perform Background Scan Every**: The range is 1 to 1440 minutes (24 hours).
3. For **Skip Background Scan When**, specify when to skip background scans:
   - Select **Clients are connected** to enable an AP with connected clients to scan channels.
   - Select **Connected clients are in power save mode** to enable an AP to scan channels when connected clients are in power save mode.
   - Select **Network traffic with voice priority is detected** to prevent an AP from performing a background scan when voice traffic is detected.

   Voice traffic takes priority and is the least forgiving of slow or degraded connections.
4. Select **SAVE RADIO PROFILE**.

Related Links

Configure Radio Profiles on page 481

*Configure Dynamic Frequency Selection*

Begin configuring a radio profile.

Use this section to make changes to the device channel width. The available settings depend on the **Supported Radio Mode** that you selected in the basic configuration section.

**Note**
Extreme Networks provides defaults for each item in this section. The following steps are optional.

The following **Channel Selection** sections are dimmed and not available:

- **Channel**
- **Channel Width and Exclusions**

Perform channel selection at the device level.

1. In the radio profile, scroll to **Channel Selection** and enable **Dynamic Frequency Selection**.

   Dynamic Frequency Selection (DFS) helps to maintain a balance between Wi-Fi performance and avoid interference with essential radio services

   **Note**
   **Dynamic Frequency Selection** settings do not apply to AP121, AP141, AP330, and AP350 access points that were shipped after 2 June 2016 and operate in the FCC domain.

   a. Select **Enable manual channel selection return** to return the affected radio to its original statically assigned DFS channel after a DFS event.
   b. Select **Enable ZeroWait DFS** to dedicate a single antenna chain to quickly identify a usable DFS channel.

      With ZeroWait DFS enabled, a 4x4 AP become a 3x3 AP.

      **Note**
      ZeroWait DFS is only available for 3- or 4-stream APs.

   c. Select **Enable Background Scan** to enable DFS to run background scans.
2. To manually set **Transmission Power**, select **Manual** and then use the slider to select a dBm setting.
3. Enable **Enable client transmission power control (802.11h)**.
4. To manually enable client transmission power control (802.11h), select Manual and use the slider to select a dBm setting.
5. Enable **Limit Channel Selection** to limit channel selection to non-overlapping channels.
   a. Select the operating **Region** for the device from the drop-down list.
   b. For **Channel Model**, select 3 channels for USA and 4 channels for Europe.
   c. For **Limit Channel Selection**, USA defaults are 1, 6, and 11, and European defaults are 1, 5, 9.
6. Enable **Use the last known power and channel during the AP boot up process**.
7. Select **SAVE RADIO PROFILE**.

Related Links

Configure Radio Profiles on page 481

*Configure Dynamic Channel Switching*

Begin configuring a radio profile.

Use this task to enable Dynamic Channel Switching (DCS) and configure the settings to dynamically select and switch channels based on specified criteria.

1. In the radio profile, go to the **Neighborhood Analysis** section, and enable **Background Scan**.
2. Expand **Advanced Settings** and enable **Dynamic Channel Switching**.
3. Select **Automatically select and switch channels during specified time interval**.
   a. In the **From** field, enter the start time for the interval.
   b. In the **To** field, enter the end time for the interval.
   c. In the **Do not switch channels if the number of connected clients exceeds** field, specify the number of connected clients.

      If the number of associated clients is equal to or less than the specified value, and if the AP finds a better channel, it can switch to a new channel. Associated clients lose their connections and must reconnect. If the number of clients exceeds the value, the AP does not switch to a new channel. When a client de-authenticates during the scheduled time range, the AP checks the number of clients against the value. If the number of clients does not exceed the value, the AP switches channels. If the number of clients still exceeds the value, the AP does not change channels.
4. Select **Switch channels anytime if RF interference exceeds the threshold**.
   a. In the **Interference Threshold** field, enter the value (%).
   b. In the **CRC Error Threshold** field, enter the value (%).
   c. Select **Do not switch channels if clients are connected**
5. Select **SAVE RADIO PROFILE**.

Related Links

Configure Radio Profiles on page 481

*Optimize Radio Usage*

Begin configuring a radio profile.

Management frames such as beacons, and probe and association requests and responses, consume airtime that might otherwise be used to transmit user data.

Use this task to configure radio profile objects to minimize management traffic by using higher data rates, and suppressing and reducing probe and association responses under certain circumstances.



**Note**
Use caution when configuring radio optimization settings. When device configuration limits specific clients, there is a risk that end user clients will deny access to the WLAN. Extreme Networks provides default values for each setting. Modifying the radio configuration is optional and should be done with caution.

1. In the radio profile, expand **Advanced Settings** and go to the **Optimizing Radio Usage** section.

2. Enable **High Density Configuration** and choose **High data rates** to transmit management frames at the highest basic data rate specified in an SSID or **Low data rates** to use the lowest basic data rate.
3. Select **Suppress successive requests within the same beacon interval** to enable APs to suppress responses to repeated probe requests from the same client received within a single beacon interval.
4. Select **Suppress response to broadcast probes by** to reduce responses to broadcast probe requests by enabling only one of several SSIDs to respond, in rotation, or reduce responses from specific client device types.

   With this feature enabled, select a suppression method:

   a. Select **Allowing only one SSID to respond at a time** to enable a single SSID to respond at a time.
   b. For **Reducing responses to certain client device types** add a new MAC OUI.

   **Note**
   When high-density WLAN optimization is enabled, the suppression setting is disabled by default.

5. Enable **Band Steering** and select a mode from the menu.
6. Use the slider to set the **Allowed percentage distribution of 2.4 and 5.0 GHz clients**.
7. Enable **Client Load Balancing** and configure the threshold settings.

**Table 175: Load balance clients based on**

| Airtime | Number of clients |
|---|---|
| Ignore probe and association requests per device when threshold exceeds:<br>• CRC Error Rate<br>• RF Interference<br>• Average Airtime Per Client | Ignore probe and association requests from clients associated with other Extreme Networks devices until:<br>• Anchor Period Elapses<br>• Query neighbors about client load every |
| Ignore probe and association requests from clients associated with other Extreme Networks devices until:<br>• Anchor Period Elapses<br>• Query neighbors about client load every | |

8. Enable **Radio Load Balancing** and specify the **Number of Connection Attempts**.
9. Enable **Weak Signal Probe Request Suppression** and specify the **Signal-to-Noise Threshold** in dB.
10. Enable **Safety Net** and specify the time elapse, in seconds or minutes, before a device responds again to association requests after an overload incident.
11. Configure Configure Radio Settings on page 404.
12. Select **SAVE RADIO PROFILE**.

Related Links

Configure Radio Settings on page 404
Configure Radio Profiles on page 481

*Configure Radio Settings*

Begin configuring a radio profile.

You can configure whether you want to use long or short preambles, adjust the beacon period (or interval), and enable the detection of spoofed BSSIDs. For more information, see Radio Settings on page 405.

**Note**
Extreme Networks provides defaults for each item in this section. The following steps are optional.

1. In the radio profile, expand **Advanced Settings** and scroll to the **Radio Settings** section.
2. For **Preamble**, select **Auto (Short/Long)** to enable support for short preambles or **Long** to disable short preamble support.
3. Set the period during which APs send beacons.
4. Set the Guard Interval to 800 nanoseconds by deselecting **Enable Short Guard Interval**.
5. To stop combining data frames into larger frames before transmission, clear the check box for **Enable MAC Aggregate Protocol Data Units**.
6. Select **Enable Frame Burst** so a wireless client will transmit a burst sequence of up to three packets without releasing control of the transmission medium.
7. Select **Enable Transmit Beamforming** to improve data transfer rates for directional signal transmission processing.
8. Select **Enable MU-MIMO** to enable multiple users to receive data using different simultaneous spatial streams from an AP transmit radio chain.
9. If you selected **Enable MU-MIMO**, set **Station Receive Chain** to **Auto** or **1**, which is the chain the AP uses to receive data from the wireless client.
10. If you are using 802.11ax radios, enable **ODFMA**.
11. If you selected **Enable ODFMA**, select **Uplink** or **Downlink**.
12. If you are using 802.11ax radios, enable **BSS Coloring**.
13. If you selected **Enable BSS Coloring**, enter the numerical value of the new BSS color the AP will transmit after surpassing the beacon threshold.
14. Select **Enable Target Wake Time** to enable an AP to minimize medium contention between stations, and to reduce the required amount of **time** that a station in the power-save mode needs to be **awake**.
15. Select **SAVE RADIO PROFILE**.

Related Links

Radio Settings on page 405
Configure Radio Profiles on page 481

*Configure Backhaul Failover*

Begin configuring a radio profile.

When **Backhaul Failovers** are enabled, the AP forms a mesh link with other hive members and can failover backhaul communications from Eth0 to a wireless interface if the Ethernet link goes down.

**Note**
Extreme Networks provides defaults for each item in this section. The following steps are optional.

1. In the radio profile, go to the **Backhaul Failover** section, and enable **Backhaul Failover**.
2. Configure the following settings to define when to failover the backhaul link from Ethernet to wireless, and when to return the backhaul to Ethernet:
   a. In **Switch to Wireless Backhaul**, set how long the Ethernet link must be down to trigger a failover to the wireless link.
   b. In **Revert Back to Wired Backhaul**, set how long the Ethernet link must be up before the AP returns backhaul communications to Ethernet.

   Use the menu to specify the time in seconds or minutes.
3. Select **SAVE RADIO PROFILE**.

Related Links

Configure Radio Profiles on page 481

*Configure Outdoor Deployment*

Begin configuring a radio profile.

You can configure outdoor APs to communicate wirelessly with each other across a great distance by using a directional antenna for the backhaul link, while continuing to use omnidirectional antennas for access. However, you must make some adjustments to the radios to accommodate the longer transmission intervals. A Wi-Fi radio expects to receive an ACK for every transmitted Unicast frame. If it does not receive an ACK, it retransmits the frame. If the distance between the transmitter and receiver is too great, the ACK timeout period elapses before the ACK from the receiver reaches the transmitter, causing the transmitter to retransmit frames repeatedly until concluding that the frames are not reaching their target. To counter this, use this task to define the ACK timeout range between APs. By increasing the range, the radio increases the ACK timeout period accordingly.

1. In the radio profile, go to the **Miscellaneous Settings** section.
2. For **Outdoor Deployment**, set a distance (between 300 and 10,000 meters) over which to support the radio.
3. Select **SAVE RADIO PROFILE**.

Related Links

Configure Radio Profiles on page 481

*Configure RF Interface Reports*

Begin configuring a radio profile.

ExtremeCloud IQ can periodically poll APs and collect RF interface-related data. ExtremeCloud IQ forces APs to adopt a shorter polling interval if CRC error, channel interference, or short-term polling thresholds are exceeded.

**Note**
Extreme Networks provides defaults for each item in this section. The following steps are optional.

1. In the radio profile, go to the **Miscellaneous Settings** section.
2. For **RF interference Reports**, select the check box to collect RF interference-related data from the APs.
3. Set the level of CRC errors for polling.

   The default threshold is 20% for 802.11g/n, and 35% for 802.11a and 802.11ac. The range is from 15 to 60%.
4. Set the level of channel interference for polling.

   The default threshold is 20% for 802.11g/n, and 35% for 802.11a and 802.11ac. The range is from 15 to 60%.
5. Set the short-term average for polling.

   The range is 5 to 30 minutes.
6. Select **SAVE RADIO PROFILE**.

Related Links

Configure Radio Profiles on page 481

*Configure Client SLA Definitions*

Begin configuring a radio profile.

For each radio mode (or phymode)—11a, 11b, 11g, 11n, 11ac, 11ax—there are default settings for bit rate, success rate, and usage.

In most cases, the AP and client use several different rates to transmit and receive packets, changing rates as factors such as RSSI and packet loss change. To determine a common mid point to which various client scores can be compared, ExtremeCloud IQ (New) provides three settings for each phymode:

**Rate**: This setting defines the transmission bit rated used by clients with healthy connectivity. For 80211a/b/g, rates are Mbps. For 802.11n, the rates are Mbps and modulation coding scheme (MCS).

**Success**: This setting defines the percentage of packets that you expect clients with healthy connectivity to transmit successfully (without retries) at the defined rate.

**Usage**: This setting defines the percentage of time that clients with healthy connectivity will transmit at the defined rate. The aggregated usage for the two bit rates must be equal to or less than 100%.



**Note**
To counter traffic congestion from clients with otherwise healthy Tx/Rx bit rates, APs can monitor client throughput and report SLA status to ExtremeCloud IQ. APs can also dynamically increase the amount of airtime for clients with a significant backlog of queued packets and improved throughput.

Use this task to configure **Client SLA Settings**.

1. In the radio profile, go to the **Client SLA Settings** section.
2. To use the default settings, select one of the three options: **High Density (performance-oriented)**, **Normal Density**, or **Low Density (coverage-oriented)**.

   Alternatively, to customize the settings for each option, select **CUSTOMIZE** and configure the settings for each radio mode, on each tab.
3. Select **SAVE RADIO PROFILE**.

Related Links

Configure Radio Profiles on page 481

*Configure WMM QoS Settings*

Begin configuring a radio profile.

Wi-Fi Multimedia (WMM) classifies traffic into Voice, Video, Best-effort, and Background access categories, and provides mechanisms to prioritize each category at differing levels. **Contention Window Minimum**, **Contention Window Maximum**, and **AIFS** work together to determine the back-off time for each category. The first two define the minimum and maximum contention window parameters. When there is contention for access to the wireless medium, the AP calculates a random value between these two parameters. The higher the values, the longer the AP will back off during periods of access contention, resulting in longer delays for that traffic category. The lower the values, the shorter the back-off period, with shorter delays for traffic delivery. The AP adds the fixed arbitration interframe space (AIFS) back-off value to the first two values. The higher the setting, the longer the AP backs off, and the longer traffic is delayed during times of contention. The smaller the setting, the less time the AP backs off, resulting in shorter delays.

Use this task to configure QoS settings for Wi-Fi Multimedia.

1. In the radio profile, expand the **Advanced Settings** section, and go to **WMM QoS Settings**.
2. If necessary, modify the default settings in the **Contention Window Minimum**, **Contention Window Maximum**, and **AIFS** columns.
3. If necessary, modify the default setting in the **TXOP Limit** column to determine how long bursts of traffic last before relinquishing the medium.
4. Set the **No ACK** flag to inform the recipient not to send ACKs of the frames it receives, which is useful for the video category where lost packets in streaming video go unnoticed, and retransmissions are unnecessary.
5. Select **SAVE RADIO PROFILE**.

Related Links

Configure Radio Profiles on page 481

*Configure Sensor Mode Scan Settings*

Begin configuring a radio profile.

These settings determine how your APs behave during the scanning process. You can specify how long a device scans each channel and which channels are to be scanned.

**Note**
Dwell time defines how long the radio transmits on a specific channel frequency to scan client probe requests before moving to the next channel in the sequence. For presence data collection, setting the dwell time above the default value raises the throughput of data collected on each channel. Setting the minimum dwell time below the default value reduces latency but also reduces the throughput of data collected on each channel.

Use this task to configure scan settings for sensor mode.

1. In the radio profile, go to the **Sensor Mode Scan Settings** section.
2. If necessary, modify the **Dwell Time**.
3. To set individual channel numbers to collect client probe request data, deselect **Scan All Channels** and then select individual channel numbers.
4. Select **SAVE RADIO PROFILE**.

Related Links

Configure Radio Profiles on page 481

## Configure SDR Profiles

First, create radio profiles.

Software Defined Radio (SDR) scans the surrounding environment and chooses a channel based on those scans. It can also go to a different radio if it finds no suitable channels on the first radio. For example, if it finds no usable channels on the 2.4 GHz radio, then it will switch to the 5 GHz radio instead (so long as the device is capable of dual 5 GHz radios).

Use this task to create SDR profiles.

1. Go to **Configuration** > **Network Policies**, select **Menu**, and then go to **Common Objects** > **Policy** > **SDR Profiles**.
2. Select an existing profile, and then select , or to add a new one, select ..
3. Type a **Name** for the profile.
4. (Optional) Type a **Description** for the profile.

   Although optional, descriptions can be helpful when you are configuring or troubleshooting your network. the profile.

5. Select the radio profiles to be applied.

   This allows the device to switch radios automatically and still know which radio profile to use.

   **Note**
   If an AP with a 2.4GHz radio for wifi0 is in use (as opposed to a dual 5GHz radio AP), set the static radio profile (radio profile settings on the device specific settings, separate from the SDR profile) to radio_ng_0. If this default radio profile is not in use within device specific settings, the update will fail and the SDR profile will not work.

6. Select **Enable SDR during initial ACSP** (the initial boot up of the device) to enable the AP to choose the best channel it can see for the environment upon start up.
7. Select **Enable SDR to periodically run in the background** to set the interval for how often the SDR runs in the background.

   If there is a concern that the AP might switch channels and interrupt too many client connections, set a limit of client devices that can be connected and still enable an SDR scan and change.

   a. Type the **Interval** to specify the time period between SDR scans.
   b. In the **Do not switch when station number exceeds** field, enter the number of client devices that can be connected.
8. Select **Enable SDR during a schedule time range** to specify the time range.

   SDR profiles can limit the number of client connections to interrupt, and enable the profile to run in the background. If both settings are enabled, make sure both station number counts are the same.

   a. Enter values for the time range.
   b. In the **Do not switch when station number exceeds** field, enter the number of client devices that can be connected.

      If the station number count is 0, the rule does not apply.
9. Select **SAVE**.

Related Links

Configure Radio Profiles on page 481

## Configure a Schedule

Use this procedure to configure a schedule as a common object for reuse.

1. Go to **Configuration** > **Network Policies**, select **Menu**, and then go to **Common Objects** > **Policy** > **Schedules**.
2. Select an existing schedule, and then select , or to add a new one, select .
3. Configure the settings.

   See Schedule Settings on page 374.
4. Select **SAVE SCHEDULE**.

Related Links

Schedule Settings on page 374

## Configure SSIDs

As a best practice, configure an SSID as part of the network policy configuration workflow. For more information, see SSID Usage in Standard Wireless Networks on page 316.

Use this task to configure a new SSID object for reuse in network policies.

1. Go to **Configuration** > **Network Policies**, select **Menu**, and then go to **Common Objects** > **Policy** > **SSIDs**.
2. Select an existing SSID, and then select , or to add a new one, select .
3. Configure the settings.

   For more information, see SSID Usage in Standard Wireless Networks on page 316.
4. Select **SAVE**.

Related Links

SSID Usage in Standard Wireless Networks on page 316

## Configure a Switch Template

A switch template is a visual depiction of the physical ports on a switch. Configure how ports function by assigning port types and port usage settings to the template.

You can create a switch template during the network policy creation process, or at the device level after you have a network policy in place. Device-level changes to a switch template override settings in the network policy. For more detailed information about switch use in ExtremeCloud IQ (New), see the *Extreme Platform ONE Universal Switch Deployment Guide*.

Use this task to configure a switch template object.

1. Go to **Configuration** > **Network Policies**, select **Menu**, and then go to **Common Objects** > **Policy** > **Switch Template**.
2. Select an existing switch template, and then select , or to add a new one, select . and select the switch model from the list.
3. Type a **Name** for the template.
4. To make changes to device configuration (Switch Engine only), enable **Override Policy Common Settings**.
5. For STP Configuration, enable **STP (Spanning Tree Protocol)** and configure the settings.

   See Configure Switch STP Settings on page 420.
6. For **MAC Locking Settings**, select to control the forwarding database for learned MAC address entries on a port.

   **Note**
   MAC Locking must also be enabled on a per-port basis.

7. Enable **IGMP Snooping** and configure the settings.
   - **Enable immediate leave**: Instructs the switch to remove a multicast host from the multicast forwarding table immediately upon receipt of a leave-group-membership message.
   - **Suppress redundant IGMP membership reports to optimize traffic**: Suppresses redundant IGMP membership reports from multiple hosts on a subnet. The switch sends a single report to the IGMP router, reducing traffic.
8. For **Extreme Loop Recovery Protocol Settings**, select to configure ELRP client periodic packet transmission for VLANs assigned to a port type to detect and prevent loops.

   This option enables an ELRP client and disables a port when a loop is detected on the applied access or trunk VLANs assigned to the port type.

   **Note**
   ELRP must also be enabled within the switch template.

9. Enable **DHCP Snooping**, and select **Enable drop rogue DHCP Packets action**

   Ports configured as trusted do not apply the drop action. By default, port types configured as Trunk Port are trusted.
10. For **MTU Settings**, enter a maximum transmission unit value for Ethernet interfaces.

    The MTU value determines the largest packet size that can be transmitted through your system.
11. For **PSE Settings**, toggle to **On** to configure maximum power thresholds to generate alerts to ExtremeCloud IQ about exceeding maximum power levels.
12. Select **Enable Flow Control** to manage the port data receive transmission rate.
13. For **Management Interface Settings**, select one of the following options:
    - **Infer from device** (Dell EMC switches only): Select when the switch supplies the management interface.
    - **VLAN Interface**: Select when the management interface is to be supplied by the management VLAN.
      - **Management VLAN**: Enter the VLAN to be used by the switch.
      - **Management IP Settings**: Select to enable DHCP on this interface.
14. For the **Port Configuration** section, see the following:
    - To configure **Instant Port Profile**, see Configure Instant Port Profiles on page 176.
    - To **Configure Ports in Bulk**, see Create a New Port Type on page 427
    - To **Configure Ports Individually**, see Configure Individual Ports on page 430
15. For **Advanced Settings**, see Configure Switch Template Advanced Settings on page 435.
16. Select **Save**.

## Configure URL Filtering Detail

Extreme Networks routers support HTTP URL filtering rules, which define URL filtering by allowed list, blocked list, and category. Use this task to create or edit URL detail rules for use in URL filtering rules.

1. Go to **Configuration** > **Network Policies**, select **Menu**, and then go to **URL Filtering Detail**.

2. Select an existing detail, and then select , or to add a new one, select .
3. Type a **Name** for the detail.
4. Type a **Description** for the detail.

   Although optional, descriptions can be helpful when you are configuring or troubleshooting your network.
5. Configure allowed URLs on the **WHITELIST** tab, and blocked URLs on the **BLACKLIST** tab.
   a. To add URLs manually, type a **URL** and then select **ADD**.

      You can add up to 32 URLs.

      Alternatively, you can upload a .CSV file by dragging and dropping, or by selecting **Choose** and selecting the file. The file format must be as follows:

      ```
      cloud-whitelist1.aerohive.com
      cloud-w2.aerohive.com
      cloud-w3.aerohive.com
      cloud-w4.aerohive.com
      cloud-w5.aerohive.com
      cloud-w6.aerohive.com

      cloud-blacklist1.aerohive.com
      cloud-b2.aerohive.com
      cloud-b4.aerohive.com
      cloud-b6.aerohive.com
      ```
   b. To edit an existing URL detail rule, select it and then select .
   c. To delete an existing URL detail rule, select it and then select .
   d. To add a new schedule, select **Add**, or select **Choose** to select an existing schedule.
6. To block by category, select the **CATEGORIES** tab and select the categories to block.
7. Select **SAVE DETAIL**.

Related Links

Configure URL Filtering on page 494

## Configure URL Filtering

Extreme Networks routers support HTTP URL filtering rules, which define URL filtering by allowed list, blocked list, and category. Use this task to create a new URL rule, add filtering details to the rule, and then associate the rule with a user profile.

1. Go to **Configure** > **Common Objects** > **URL Filtering**.
2. Select an existing rule, and then select , or to add a new one, select .
3. Type a **Name** for the rule.
4. Type a **Description** for the rule.

   Although optional, descriptions can be helpful when you are configuring or troubleshooting your network.
5. Add URL detail rules.
   a. Select an existing URL detail rule, and then select , or to add a new one, select .

      For more information, Configure URL Filtering Detail on page 493.

b. To add existing URL filtering details to the URL filtering rule, select .

6. To add a new schedule, select **Add**, or select **Choose** to select an existing schedule.
7. Select **SAVE URL RULE**.

Related Links

Configure URL Filtering Detail on page 493

### Configure User Profiles

After a user associates with a device, the device assigns the user to a user profile. The device can make this assignment dynamically from attributes returned by a RADIUS authentication server or statically by using the default user profile set.

Use this task to create user profiles that define user traffic settings on APs.

1. Go to **Configuration** > **Network Policies**, select **Menu**, and then go to **Common Objects** > **Policy** > **User Profiles**.
2. Select and configure the settings.
3. Select **Save User Profile**.

Related Links

User Profile Settings on page 315

## Basic Configuration

The topics in this section provide details about basic configuration objects, such as Application Sets, Client Mode Profiles, DHCP and DNS, IP, MAC, and OS Objects, Notification Templates, and VLANs.

Related Links

Configure Application Sets on page 495
Configure Client Mode Profiles on page 496
Configure DHCP Servers and DHCP Relay Agents on page 497
Configure DNS Services on page 499
Configure IP Objects/Host Names on page 501
Configure MAC Objects/MAC OUIs on page 502
Configure Notification Templates on page 503
Configure OS Objects on page 504
Configure VLANs on page 505
Configure a VLAN Group on page 505
Configure Supplemental CLI Objects on page 506

### Configure Application Sets

Along with six predefined application sets, ExtremeCloud IQ (New) allows administrators to define custom application sets. Application sets are available as common objects for use in SD-WAN routing policies.

Use this task to create custom application sets.

1. Go to **Configuration** > **Network Policies**, select **Menu**, and then go to **Common Objects** > **Basic** > **Application Sets**.
2. Select an existing application set, and then select , or to add a new one, select ..
3. Type a **Name** for the new application.
4. Select **Application** or **Category**.
5. Type a character string to search for the application that you want to add.
6. Select applications to include in your application set.

   ExtremeCloud IQ (New) automatically adds your selections to **Selected Applications**.
7. Select **SAVE**.

## Configure Client Mode Profiles

You can set a radio on some APs to client mode, which enables the AP to connect to existing Open and PSK wireless networks—including third-party networks—as a generic BYOD client.

The best-practice recommendation is to use a wired interface to configure client mode APs, because the configuration process is much faster than it is with a wireless backhaul.

Use this task to configure a Client Mode profile object.

1. Go to **Configuration** > **Network Policies**, select **Menu**, and then go to **Common Objects** > **Basic** > **Client Mode Profiles**.
2. Select an existing Client Mode profile, and then select , or to add a new one, select ..
3. Type a **Client Mode Profile Name**.
4. (Optional) Type a **Description**.

   Although optional, descriptions can be helpful when you are configuring or troubleshooting your network.
5. The **Enable Local Web Page** option is enabled by default.

   The client mode AP activates a local SSID portal web page, which includes choices to select and connect the client mode AP WAN-side radio to a WAN Wi-Fi network. Clear this check box to configure other options for this profile.
6. The **Enable NAT/DHCP** option is enabled by default.

   Client Mode APs can function as wireless bridges, connecting wired devices to wireless networks. The NAT/DHCP toggle controls whether the AP performs Network Address Translation and DHCP services for connected clients.

7. Choose one of the following DHCP server options:
   - In the **DHCP Server Scope** field, enter the first IP address of the DHCP server range. The first IP address in this range is the IP address used to display the client mode SSID portal web page. Make a note of this first IP address for later reference.
   - In the **DHCP Server Scope** field, enter a single IP address to reserve a specific client (MAC address) to an IP. A DHCP reservation is a permanent IP address assignment. It is a specific IP address within a DHCP scope that is permanently reserved for a specific DHCP client. DHCP reservations on the AP support security on the local side of the Network Address Translation (NAT) and ensure that the client IP address does not change.
   - Enable **Advanced DHCP Server**, and then choose a preconfigured **DHCP Server and Relay** agent from the menu.
8. Configure the **Port Forwarding Rules** as follows:
   a. Select to add a new port forwarding rule.
   b. (Optional) Type a description of how this rule is to be used.
   c. Select a number for the outside port in the range of 1025-65535 (reserved ports cannot be used).
   d. Select a number for the local port in the range of 1-65535.
   e. Select **TCP**, **UDP**, or **Both** from the **Protocol** drop-down list.
   f. Select a **Host IP Address** for the internal device from the drop-down list, or select the plus sign to add a new address.
   g. Select **Add**.
9. Select **SAVE**.

## Configure DHCP Servers and DHCP Relay Agents

For small networks, you can configure and enable a DHCP server on a device to provide network settings dynamically to clients. After you configure one hive member as a DHCP server, the other hive members process the **DHCPDISCOVERY** and **DHCPREQUEST** messages that they receive from clients as usual, forwarding them to their neighbors through which they connect to the network. The only requirement about which device to use as the DHCP server is that it must be a portal.

When all hive members are in the same subnet and all devices in that subnet are on a single VLAN, you only need to configure the device that you want to be the DHCP server with a pool of IP addresses from which it can draw when responding to DHCP client requests.

When some hive members are in a different subnet from that of the DHCP server, you must also configure those devices to forward DHCP traffic to the IP address of the DHCP server. In this case, the other devices act as DHCP relay agents. You can configure both DHCP servers and relay agents here.

Use this task to add a new DHCP Server and Relay object.

1. Go to **Configuration** > **Network Policies**, select **Menu**, and then go to **Common Objects** > **Basic** > **DHCP Server and Relay**.
2. Select an existing object, and then select , or to add a new one, select ..

3. Type a **Name** for this object.
4. (Optional) Type a **Description** for this object.

   Although optional, descriptions can be helpful when you are configuring or troubleshooting your network.
5. Select the management interface on which the DHCP Server or Relay agent is set.
6. Select the type of service.
7. If you select **DHCP Server**, configure the following steps:
   a. **Set the DHCP server as authoritative** (enabled by default): Select the check box to set the DHCP server as authoritative.

      If this DHCP server is the only one on your network, it knows what the valid IP numbers on the network are. If a client tries to register with an invalid IP address (for example, if a client device sill has an active lease with another network), an authoritative DHCP server denies access to that client.
   b. **Use ARP to check for IP address conflicts** (enabled by default): By default, this DHCP server uses ARP to check for IP address conflicts on the network before assigning an IP address to a DHCP client.

      Clear the check box to disable this feature.
   c. **Enable NAT support**: Select this check box to automatically generate ARP responses for the default gateway specified in the DHCP server options.
   d. **Configure the IP Pool**: Define the IP address pool from which the DHCP server draws IPv4 or IPv6 addresses when making assignments.

      To add a new IP pool, select , enter the start and end IP addresses, and then select **Add**.
   e. **Configure DHCP Server Options**: Define custom DHCP options to provide additional network settings to connected clients.

      You can use IPv4 or IPv6 addresses. Configure the following settings:
      - **Default Gateway**: Type the IP address of the default gateway or the subnet to which the addresses in the IP pool belong.
      - **DNS Server1 IP**: Type the IP address of the primary DNS server for clients to contact when resolving domain names to IP addresses (DHCP option 6).
      - **DNS Server2 IP**: Type the IP address of a secondary DNS server for clients to contact if the primary DNS server is unresponsive (DHCP option 6).
      - **DNS Server3 IP**: Type the IP address of a third DNS server for clients to contact if neither the primary nor secondary DNS servers respond (DHCP option 6).
      - **POP3 Server IP**: Type the IP address of the POP3 server for clients to use (DHCP option 70).
      - **SMTP Server IP**: Type the IP address of the SMTP server for clients to use (DHCP option 69).
      - **WINS Server1 IP**: Type the IP address of the primary WINS server for NetBIOS name-to-address resolution (DHCP option 44).
      - **WINS Server2 IP**: Type the IP address of the secondary WINS server for NetBIOS name-to-address resolution (DHCP option 44).
      - **Lease Time**: Type the length of time (60-86400000 seconds) for the DHCP lease; by default, DHCP leases last for 86,400 seconds, or 24 hours (DHCP option 51).

- **Netmask**: Type the netmask defining the subnet to which the addresses in the IP pool belong.
- **Domain Name**: Type the domain name to assign to DHCP clients. This is the default domain name for DNS name resolution (DHCP option 15).
- **MTU**: Set the path MTU aging timeout in seconds for clients to use; the minimum value is 68 seconds, and the maximum is 8192 seconds (DHCP option 24).
- **NTP Server1 IP**: Type the IP address of the primary NTP (Network Time Protocol) server with which DHCP clients can synchronize their clocks (DHCP option 42).
- **NTP Server2 IP**: Type the IP address of the secondary NTP server with which DHCP clients can synchronize their clocks (DHCP option 42).
- **Log Server IP**: Type the IP address of the logging server for DHCP clients (DHCP option 7).

f. **Configure Custom Options**: Define custom DHCP options to provide additional network settings to connected clients.

You can use IPv4 or IPv6 addresses. To add a new custom DHCP option select the plus sign and complete the fields:

- **Number**: Type a custom option number from 2 to 5, 8 to 14, 16 to 25, 27 to 41, 43, 45 to 50, 52 to 57, 60 to 68, 71 to 224, 227, 228, or from 232 to 254.



**Note**
The following numbers are reserved: 226, ExtremeCloud IQ domain name; 225, ExtremeCloud IQ IP address; 229, PPSK server IP address; 230, RADIUS server authentication IP address; 231, RADIUS server accounting IP address. The following DHCP option numbers are reserved for other information: 3, 6, 7, 15, 26, 42, 44, 51, 58, 59, 69, and 70.

- **Type**: Select the type of data that the option will provide:
  - **Integer**: 0-2, 247, 483, 547
  - **IP Address**: Four octets of an IP address or eight groups of two octets each for an IPv6 address.
  - **String**: 1-255 characters
  - **Hex**: 1-254 hexadecimal digits

8. If you select **DHCP relay agent**, designate a **Primary DHP Server** and optional **Secondary DHCP Server**.
9. Select **SAVE**.

## Configure DNS Services

First, configure or modify a subnetwork space. It is also helpful to have configured your DNS servers.

Extreme Networks routers use DNS services in their subnetwork configurations. When the network type is for internal or guest use, an Extreme Networks router applies this service to the DNS requests from clients connecting to the router either directly or through an intermediary AP or switch. When the network type is management, the router applies this to DNS requests from APs and switches on the same management network behind the router, and to the mgt0 interface of the router itself.

Use this task to add or edit a DNS service for use at the network policy level, or at the device level for routers and VPN Gateway Virtual Appliances.

1. Go to **Configuration** > **Network Policies**, select **Menu**, and then go to **Common Objects** > **Basic** > **DNS Services**.
2. Select an existing DNS Service object, and then select , or to add a new one, select .
3. Type a **Name**.
4. (Optional) Type a **Description**.

   Although optional, descriptions can be helpful when you are configuring or troubleshooting your network.
5. Select **Enable DNS Snooping for static DNS clients** to enable access data collection.
6. With DHCP enabled, if you select **Supply external DNS server IP addresses in DHCP offers**, enter the static IP address of at least one external DNS server.
7. If you select **Set the router as the DNS server in DHCP offers**, configure the following settings:
   - **Set the router to use the same DNS servers for all domain name lookups**: This is non-split mode. With this option, the router sends DNS requests for names that match domains to the DNS servers you specify. Specify external domain name lookups:
     - **Resolve client name requests using the same DNS servers as configured for the router**: With this option, the router sends all requests to the DNS servers it learns through DHCP.
     - **Specify name servers**: Enter the static IP address of at least one DNS name server to resolve all domain name lookups.
   - **Set the router to use separate DNS servers for internal and external domain name lookups**: This is split mode. You must specify at least one DNS server, which can be accessed through either a VPN tunnel or on the Internet. The router sends DNS requests for names that match internal domains to the specified internal DNS servers, and sends other requests through DHCP to specified external DNS servers. For internal and external domain name lookups:
     - Enter the internal domain names that the internal DNS servers will use for comparison and name resolution. Enter each domain name on a separate line. Enter the static IP address of at least one internal DNS server.
     - Under **Domain Name Specific Settings**, to restrict a domain name to a single DNS server for security purposes, select the plus sign, enter the domain name and DNS server IP address, and select **ADD**.
     - **Resolve client name requests using the same DNS servers as configured for the router**: With this option, the router sends all requests to the DNS servers it learns through DHCP.
     - **Specify name servers**: Enter the static IP address of at least one DNS name server to resolve all domain name lookups.
8. Select **SAVE**.

Related Links

Configure a Subnetwork Space on page 546
Configure DNS Servers on page 519

## Configure IP Objects/Host Names

An IP object or host name is a network object that you can reference in IP firewall policy rules as a Layer 3 source or destination, and as a DNS server in a DNS assignment. An IP object or host name can be used by configuration objects throughout the ExtremeCloud IQ (New) GUI. IP objects and host names can be used to identify RADIUS clients that belong to the same user profile. For more information about RADIUS clients, see Configure an External RADIUS Server on page 352.

Use this task to configure an IP object and Host name.

1. Go to **Configuration** > **Network Policies**, select **Menu**, and then go to **Common Objects** > **Basic** > **IP Objects / HostNames**.
2. Select an existing IP object or host name, and then select , or to add a new one, select ..

   **Note**
   You cannot change the object type of an existing IP object or host name.

3. Type a **Name** for the new object.
4. Select an object type from the menu, and then configure the settings.

**Table 176: Object type settings**

| Object Type | Description |
|---|---|
| IP Address | Define an **IP Address** for a host.<br><br>**Note:** When you select IP Address, ExtremeCloud IQ (New) automatically sets a 32-bit netmask (255.255.255.255) for all IP addresses that you apply to this object. |
| Host Name | Type a resolvable **Host Name**, up to 64 characters long. |
| Network | Define a **Subnet IP** address and **Subnet Mask**.<br>Like an IPv4 address, a netmask is a 32-bit binary number commonly represented in dot-decimal notation. A netmask shows which part of an IP address is the subnet address and which part is the host address. For example, entering a netmask of 255.255.255.0 for IP address 10.1.1.5, indicates that the first 24 bits are the subnet ID (10.1.1) and the last 8 bits are the host ID (from 0 to 255), which in this case would be 5. When defining an IP address for a subnet, the host section of the address is irrelevant. Therefore, you can enter the previous example IP address/netmask as follows:<br>• Subnet IP: 10.1.1.0<br>• Subnet Mask: 255.255.255.0 |
| IP Range | Define a **Range Start** and **Range End** of IP addresses. This option is useful if the range of IP addresses does not easily conform to a standard range of IP addresses with its own subnet mask. |

**Table 176: Object type settings (continued)**

| Object Type | Description |
|---|---|
| Wildcard | Specify a **Wildcard** that uses 0 to mask one or more octets in an IP address, thereby applying the IP object/host name to all addresses that match the unmasked parts of the address.<br>For example, if there is a consistent addressing scheme at multiple sites (10.1.1.0/24, 10.1.2.0/24, 10.1.3.0/24, and so on), and each site uses the same host ID in the address for their HTTP proxy servers (2, for example), then you can create a **Wildcard IP** and **Wildcard Mask** of 10.1.0.2 255.255.0.255. This IP object/host name applies to the HTTP proxy server at all sites, making it a useful network object to use in a single network policy that is applied to ExtremeCloud IQ (New) devices at those sites.<br>**Tip:** You might find it useful to view a wildcard mask as a superset of a netmask; that is, it can accomplish the same goals as a netmask—in which case it makes more sense to use a netmask for such a task—plus it can mask parts of an address in ways that a netmask cannot. |
| Wildcard Host Name | Create a DNS record that uses an asterisk (*) as the leftmost label in a domain name, such as *.example.com, to match requests for non-existent subdomains. This type of record allows any subdomain that does not have a specific DNS record defined to resolve to the same IP address or resource specified in the wildcard record. For example, if a wildcard A record is set for *.example.com pointing to 192.0.2.1, then requests for subdomains like www.example.com, test.example.com, or other undefined subdomain resolve to that IP address.<br>Wildcard DNS records are useful for virtual hosting, where multiple domain names or subdomains (e.g., company1.api.example.com and company2.api.example.com) point to the same server or IP address. The wildcard applies only when no exact DNS record exists for the queried name; if a specific record or delegation exists, the wildcard does not apply.<br>The wildcard applies to the leftmost label only. |

5. To add a classification rules, see Configure Classification Rules on page 291.
6. Select **SAVE IP OBJECT**.

## Configure MAC Objects/MAC OUIs

A MAC address is a 48-bit number typically written in hexadecimal notation that provides a unique address for each client device. An OUI is the first 24 bits of a MAC address. After a MAC object is assigned to a device, it can be grouped to a specific hive. In a MAC firewall policy rule, you can determine which traffic to permit or deny based on the source or destination MAC address. For more information about firewall policies, see Add MAC Firewall Policies on page 366. In QoS traffic classification and marking policies, you can prioritize traffic based on its OUI.

Use this task to configure MAC objects and MAC OUIs.

1. Go to **Configuration** > **Network Policies**, select **Menu**, and then go to **Common Objects** > **Basic** > **MAC Objects/MAC OUIs**.
2. Select an exiting object, and then select , or to add a new one, select .
3. To configure a new Mac address, select **MAC Address** and configure the settings.
   a. Type a **Name**.
   b. Type the **MAC Address**.
   c. Select **SAVE**.
4. To configure a new Mac OUI, select **MAC OUI** and configure the settings.
   a. Type a **Name**.
   b. Type the first six digits of the Mac address, for the **MAC OUI**.
   c. Select **SAVE**.

Related Links

Add MAC Firewall Policies on page 366

## Configure Notification Templates

There are two default notification templates available in ExtremeCloud IQ (New); an SMS template and an email template. You can also configure customized notification templates for non-employees who need to obtain network access (for example, guests, contractors, and VIPs).

Use this task to configure notification templates.

1. Go to **Configuration** > **Network Policies**, select **Menu**, and then go to **Common Objects** > **Basic** > **Notification Templates**.
2. Select an existing template, and then select , or to add a new one, select .
3. Type a **Name** for the template.
4. Select the **Template Type** from the list.
5. If you selected **SMS**, configure the following settings:

**Table 177: Settings for the SMS template type**

| Setting | Description |
|---|---|
| Security Type | Select **PPSK** (private pre-shared key) or **RADIUS**. |
| Template Content | Type or paste the text that you want the SMS message to contain. To insert a variable (**Login Name**, **Password**, **SSID**, or **Expiration**) select the corresponding button below the text box. |

6. If you selected **Email**, configure the following settings:

**Table 178: Settings for the Email template type**

| Setting | Description |
|---|---|
| Security Type | Select **PPSK** or **RADIUS**. |
| Icon URL | Type the path to the URL. |
| Logo URL | Type the path to the logo image to upload. |
| Template Content | To insert a variable (**Login Name**, **Password**, **SSID**, or **Expiration**) select the corresponding button below the text box. |

7. Select **SAVE**.

## Configure OS Objects

Extreme Networks devices can reassign users to different user profiles based on several client characteristics:

- Operating system (OS)
- MAC address
- OUI and device domain name

To modify an existing OS object, select the edit icon and make your changes. To delete OS objects, select the check box and then select the delete icon.

Use this task to configure a DHCP or HTTP OS object:

1. Go to **Configuration** > **Network Policies**, select **Menu**, and then go to **Common Objects** > **Basic** > **OS Objects**.
2. Select an existing object, and then select , or to add a new one, select ..
3. Type a **Name** for the object.
4. Enter a **Description** for the object.

   Although optional, descriptions can be helpful when you are configuring or troubleshooting your network.
5. Select either **DHCP Option** or **HTTP Agent**.
6. Select .

7. Select , and then choose the **OS Type**.

   If you do not see the OS you need, you can type a new one in the field. For **DHCP Option**, if you select a default OS types, the **Parameter Request List** automatically populates with the default DHCP option 55 string. If you add a new OS type, you can create your own parameter request list, which is a number string, separated by commas, that determines the order by which the DHCP client requests specific parameter information from the DHCP server. An example string to detect Windows 7 is: 1,15, 3, 6, 44, 46, 47, 31, 33, 121, 249, 43.

   **Note**
   Because devices use HTTP snooping to learn client operating systems, the OS version string that you provide must match the version that appears in the user-agent field in HTTP request headers. Lists of user-agent strings for most OS versions are available online.

   If you selected **HTTP Agent**, type a description.
8. Select **ADD**.

## Configure VLANs

Although you can manage VLANs from **Common Objects**, it is a best practice to configure them inside a network policy workflow.

Use this task to configure a VLAN object.

1. Go to **Configuration** > **Network Policies**, select **Menu**, and then go to **Common Objects** > **Basic** > **VLANs**.
2. Select an existing VLAN, and then select , or to add a new one, select ..
3. Type a **Name** for the new VLAN.
4. Type a **VLAN ID**.
5. (Optional) Select **Apply VLANs to devices using classification** and configure the settings.
6. Select **SAVE**.

Related Links

Configure VLAN Settings on page 362

## Configure a VLAN Group

Although you can manage VLANs from **Common Objects**, it is a best practice that you configure them inside a network policy workflow. See Configure VLAN Settings on page 362, and VLAN Group Object Settings on page 363.

Use this task to configure a VLAN Group object.

1. Go to **Configuration** > **Network Policies**, select **Menu**, and then go to **Common Objects** > **Basic** > **VLAN Group**.
2. Select an existing VLAN Group, and then select , or to add a new one, select ..
3. Type a **Name** for the new VLAN Group.

4. Type the IDs for the **VLANs**.

   Configure VLANs as ranges, or individually. Indicate a range with a hyphen. Separate VLAN entries with commas, for example, 1-30, 100-200, 500.
5. (Optional) Type a **Description** for the VLAN Group.

   Although optional, descriptions can be helpful when you are configuring or troubleshooting your network.
6. Select **SAVE**.

Related Links

Configure VLAN Settings on page 362
VLAN Group Object Settings on page 363

## Configure Supplemental CLI Objects

To use supplemental CLI (sCLI), first go to **Administration & Settings** > **Global Settings** > **Backup & Restore** > **VIQ Management**, and enable **Supplemental CLI**. See VIQ Management on page 721.

After you save sCLI objects containing CLI commands, you can update the commands for devices automatically, each time you update the network policy.

To avoid an unnecessary system reboot, select **Delta Configuration Update**. ExtremeCloud IQ (New) attempts to update only the configuration deltas. If a full update is required, the system prompts you to select **Complete Configuration Update**. For information about how the configuration push behaves with each **Activation Time** option, see Configuration Push Scheduling Behavior on page 154. Examples of CLI commands that require a full configuration update are: **`system antenna-type`** and **`system environment`**.

Use this task to configure sCLI objects.

1. Go to **Configuration** > **Network Policies**, select **Menu**, and then go to **Common Objects** > **Basic** > **Supplemental CLI Objects**.
2. Select an existing Supplemental CLI object, and then select , or to add a new one, select ..
3. Type a **Name**.
4. (Optional) Type an optional **Description**.

   Although optional, descriptions can be helpful when you are configuring or troubleshooting your network.
5. Type or paste the **CLI commands** into the field.
   - Enter multiple CLI commands, one command per line, not exceeding a maximum total of 8192 characters.
   - Use CLI Commands that contain IP and VLAN objects: **`${ip:ip_object_name}`** and **`${vlan:vlan_object_name}`**.
   - Perform a complete configuration update each time commands are appended to device configurations.
   - For Dell EMC switches, enter the CLI commands, `enable`, and `config` in the beginning of a sequence of CLI commands.

6. Select **SAVE**.

Related Links

VIQ Management on page 721

## Security Configuration

The topics in this section provide details about network security configuration objects, including AirDefense Policies, IP and MAC Firewall Policies, MGT IP and Traffic Filters, and WIPS Policies.

Related Links

Configure AirDefense Policies on page 507
Configure Firewalls on page 508
Configure MAC Firewall Policies on page 509
Configure MGT IP Filters on page 510
Configure Traffic Filters on page 510
Configure WIPS Policies on page 511

### Configure AirDefense Policies

Extreme AirDefense simplifies the management, monitoring, and protection of your WLAN networks. Use the following procedure to add policy objects for AirDefense.

1. Go to **Configuration** > **Network Policies**, select **Menu**, and then go to **Common Objects** > **Security** > **AirDefense Policies**.
2. Select an existing AirDefense policy object and then select and then select , or to add a new one, select .
3. Type a **Name** for the new policy.
4. (Optional) Type a **Description**.

   Although optional, descriptions can be helpful when you are configuring or troubleshooting your network.
5. (Optional) Select **Enable 3rd radio to act as a sensor**.
6. For the **Primary Server**, type the IP address of the server and the **Port** number.
7. (Optional) For the **Secondary Server**, type the IP address of the server and the **Port** number.
8. Select **SAVE**.

Related Links

Security Configuration on page 507

## Configure Firewalls

Use the following procedure to create firewall objects and rules that determine how devices manage traffic based on network or application services, and source and destination IP addresses.

1. Go to **Configuration** > **Network Policies**, select **Menu**, and then go to **Common Objects** > **Network** > **Firewalls**.
2. Select an existing firewall object, and then select , or to add a new one, select .
3. Type a **Name** for the new policy.
4. Type an optional **Description**.
5. Select an existing rule, and then select , or to add a new one, select .
6. Select one or more network or application services.

   **Network Service** objects identify Layer 4 traffic by protocol and port number. Extreme Networks provides a number of predefined services. Select to create a new network service. For more information, see Configure Network Services on page 366.

   a. Choose either **Network Services** or **Application Services**.

      You cannot select both.

   b. Select up to 100 items.

   c. Select **Add Service**.
7. Select a source IP address, host name, network, or **Any** from the drop-down list, or select **New** to add a new IP address, host name, or network.
8. Select a destination IP address, host name, network, or **Any** from the drop-down list, or select **New** to add a new IP address, host name, or network.
9. Select the action the device performs when it receives traffic matching the source address-destination address-service.

   The firewall can perform the following actions:

   - **Permit**: Allows traffic to traverse the firewall.
   - **Deny**: Blocks traffic from traversing the firewall.
   - **Drop traffic between stations**: Drops traffic between stations if both stations are associated with one or more members of the same hive. This setting applies to unicast, broadcast, and multicast traffic that the device receives on an interface in access mode.
   - **NAT**: Translates the source IP address of a packet permitted to traverse the firewall to that of the mgt0 interface on the device.
10. Choose one of the following logging options from the drop-down list:
    - **Off**: Disables logging for packets and sessions that match the IP firewall policy rule.
    - **Session Initiation**: Log details about a session created after passing an IP firewall policy lookup.
    - **Session Termination**: Log details about a session matching an IP firewall policy termination.
    - **Both**: Log details after initiating and terminating a session.
11. Select **SAVE**.

    As you add rules to a policy, each subsequent rule is positioned at the bottom of the list.

12. Use the up and down arrows in the rules table to rearrange the position of rules to determine the order of application.
13. Select **SAVE**.

Related Links

Configure Network Services on page 366
Network Configuration on page 522

## Configure MAC Firewall Policies

MAC firewall policies determine how the device manages traffic based on source and destination IP addresses, and the actions (permit or deny) the device can take. When the policy contains multiple rules, the order of the rules affects how they are applied. Use this task to create a new rule.

Use the following procedure to add MAC firewall policy objects and rules.

1. Go to **Configuration** > **Network Policies**, select **Menu**, and then go to **Common Objects** > **Security** > **MAC Firewall Policies**.
2. Select an existing IP firewall policy and then select , or to add a new one, select .
3. Enter a **Name** for the new policy.
4. Enter an optional **Description**.
5. Select an existing rule, and then select , or to add a new one, select .
6. For **Source MAC**, select **Any**, an existing MAC OUI or the plus sign.

   If you choose to add a new **Source MAC**, select **MAC Address** or **MAC OUI** and perform the following:

   a. Enter a new name.
   b. Enter the **MAC Address** or **MAC OUI**.
7. For **Destination MAC**, select **ANY**, an existing MAC OUI or the plus sign.

   If you choose to add a new **Source MAC**, select **MAC Address** or **MA OUI** and do the following:

   a. Enter a new name.
   b. Enter the **MAC Address** or **MAC OUI**.
8. Select the action the device performs when it receives traffic matching the source address-destination address-service.

   The firewall can perform the following actions:

   - **Permit**: Allows traffic to traverse its firewall.
   - **Deny**: Blocks traffic from traversing its firewall.

9. Choose one of the following logging options from the drop-down list:
   - **Off**: Disable logging for packets and sessions that match the MAC firewall policy rule.
   - **Session Initiation**: Log session details about a session created after passing a MAC firewall policy lookup.
   - **Session Termination**: Log session details about a session matching a MAC firewall policy termination.
   - **Both**: Log session details after initiating and terminating a session.
10. Select **SAVE**.

    As you add rules to a policy, each new rule is positioned at the bottom of the list.
11. Use the up and down arrows in the rules table to rearrange the position of rules to determine the application order.
12. Select **SAVE**.

Related Links

Security Configuration on page 507

## Configure MGT IP Filters

Before you begin, enable **MGT IP Filter** in the network policy settings.

By default, ExtremeCloud IQ (New) devices enable administrative access from all IP addresses. To provide tighter security, you can restrict administrative access. As soon as you apply a filter to a device—which you do by applying the filter to a network policy and then applying that policy to a device—the device denies access from all other IP addresses except those specified in the filter.

Use the following procedure to configure MGT IP Filter objects for use in network policies.

1. Go to **Configuration** > **Network Policies**, select **Menu**, and then go to **Common Objects** > **Security** > **MGT IP Filters**.
2. Select an existing MGT IP Filter and then select and then select , or to add a new one, select .
3. Configure the settings.
4. To add a new IP Object, select **Add Another IP Object**, configure the settings, and then select **SAVE SUBNET**.
5. Select **SAVE MGT IP FILTER**.

Related Links

Configure MGT IP Filters on page 306
Table 119 on page 307
Table 120 on page 307
Security Configuration on page 507

## Configure Traffic Filters

Before you begin, enable **Traffic Filters** in the network policy settings. See Configure Traffic Filters Policy Settings on page 305.

By default, Extreme Networks devices permit SSH and pings to access the mgt0 interface through the Ethernet and wireless interfaces to which you bind SSIDs.

You can control which management and diagnostic services a device can receive, and whether the device permits traffic between connected clients. You can apply traffic filters to Ethernet interfaces (in backhaul or access mode), to the wireless backhaul interface, and to the wireless access interface of individual SSIDs. These options permit certain types of traffic to reach the mgt0 interface through Ethernet interfaces eth0, eth1, red0, or agg0 (through the wireless backhaul interface), and through select SSIDs.

Use this task to configure new **Traffic Filters** objects.

1. Go to **Configuration** > **Network Policies**, select **Menu**, and then go to **Common Objects** > **Security** > **Traffic Filters**
2. Select an existing object, and then select , or to add a new one, select ..
3. Configure the settings.
4. Select **SAVE**.

Related Links

Traffic Filter Settings on page 305
Security Configuration on page 507

## Configure WIPS Policies

The Extreme Networks Wireless Intrusion Prevention System (WIPS) uses a variety of techniques for detecting unauthorized Access Points (APs) by checking for those that do not conform to specified criteria and ad hoc networks.

**Note**
You can configure both AP-based WIPS services (Rogue Access Point Detection) and advanced Extreme AirDefense Essentials WIPS services. The second option requires that you first install a Guest Manager on-premise service. Models that support AirDefense Essentials will default to that platform. All others will be on legacy WIPS.

Rogue Access Point Detection is supported on 802.11ac or older model APs **ONLY**.

Extreme AirDefense Essentials is supported on Wi-Fi6/6E (802.11ax) and newer model APs **ONLY**.

Use the following procedure to add a WIPS policy object for reuse in network policies. To configure WIPS as part of a network policy, see Configure WIPS on page 445.

1. Go to **Configuration** > **Network Policies**, select **Menu**, and then go to **Common Objects** > **Security** > **WIPS Policies**.
2. Select an existing WIPS policy object, and then select , or to add a new one, select .
3. Configure the settings.
4. Select **SAVE**.

Related Links

WIPS Policy Settings on page 446
Security Configuration on page 507

# QoS Configuration

The topics in this section provide details about QoS configuration objects, including classifier and marker maps, and rate control rules.

Related Links

Quality of Service on page 512
Classifier Maps on page 513
Configure Marker Maps on page 517
Configure Rate Control & Queuing on page 518

## Quality of Service

Traditional Quality of Service (QoS) separates client traffic into queues based on traffic type, and schedule the transmission of the traffic based on data rates from the queues. In a WLAN, a slower client (802.11b) uses significantly more airtime to transmit the same amount of data as a faster client (802.11ax). To make airtime access more equitable, Extreme Networks provides airtime-based QoS scheduling. Instead of using just bandwidth in the QoS calculations, APs allocate airtime per client, traffic class, and user profile by dynamically calculating airtime consumption per packet. When multiple client types (802.11a, ac, b, g, n or ax) are active in the same WLAN, all clients receive the same amount of airtime (10 ms for example), regardless of the client type. For example, an 11ax client could send 128 Kbps of traffic in the allocated slot, while an 11b client could only send 50 Kbps, but both clients receive the same amount of airtime.

A visual representation of the difference between bandwidth-based scheduling and airtime-based scheduling when two clients are transmitting at different data rates looks like this:

Dashes ( — ) indicate airtime for frames transmitted at a low data rate.

Bullets ( • ) indicate airtime for frames transmitted at a high data rate.

Bandwidth-based scheduling:

— • — • • — • — — • — • — • — •

Airtime-based scheduling:

— • • • • — • • • • — — — — — —

The faster client might be using 802.11ax and the slower client 802.11 a, b, g, or n, or they might both be using the same protocol, but one is farther away and must use a slower speed than the other.

With bandwidth-based scheduling, both slow and fast clients finish at the same time regardless of their data rates, and they compete the entire time for the air. Because both

clients have an equal opportunity to transmit frames, the faster client's throughput slows down to the rate of the slower client.

With airtime-based scheduling, both clients get their proportion of airtime. The faster client finishes four times faster, and the slower client finishes at the same time as it did with bandwidth-based scheduling. The fast client is rewarded, and the slow client is not penalized.

**Note**
QoS rate control and queuing on routers applies to traffic from the LAN to the WAN, but not the reverse, primarily because there is typically much less bandwidth on the WAN interface than on LAN interfaces. APs apply QoS rate control and queuing to both outbound and inbound traffic. They perform data rate limiting on incoming Ethernet and Wi-Fi interfaces, and they queue packets on outgoing Wi-Fi interfaces. APs do not queue any packets that they send out through their Ethernet interfaces because the Ethernet link is not a point of congestion; however, they do set the 802.1p or DSCP priority in the packet headers as defined in the marker map so that the next-hop router can perform QoS queuing.

The benefits of airtime-based scheduling include:

- **Multiple-service WLAN infrastructure**: When integrated with service-based QoS scheduling in user policies, Dynamic Airtime Scheduling lets you manage the air optimally to support different application types.
- **Dense deployments**: When there are many clients and the air is congested with wireless traffic, airtime-based scheduling ensures that faster clients get off the air faster, reducing the likelihood of collisions and contention among all client traffic.
- **Sparse or Partial Deployments**: When a few clients are spread out at various distances from the AP, airtime-based scheduling prevents fringe or distant clients from slowing down closer, faster clients and allows for phased roll-outs.
- **Environments with a mixture of 802.11 a/ac/ax/b/g/n clients**: When there is a mixed environment with clients using different protocols when connecting to the AP, airtime-based scheduling enables the faster clients to get the benefit of their speed without penalizing the legacy clients.

Related Links

QoS Configuration on page 512

## Classifier Maps

Quality of Service (QoS) prioritizes and optimizes the forwarding of different types of traffic through a network. You can use classifier maps to map traffic to Extreme Networks QoS classes by service type, specific MAC OUIs, individual SSIDs, and priority numbers in various standard QoS classification system (802.1p/DiffServ/802.11e). The device prioritizes, processes, and forwards the incoming traffic as determined by the QoS level to which it is mapped. For outgoing traffic, devices use marker maps.

For more information about QoS in general, see Quality of Service on page 512.

When a device applies a classifier map, it checks to see if an incoming packet matches a setting in the map by checking for matches in the following order. It then uses the first match it finds.

1. Services

2. MAC OUIs

3. SSIDs

4. 802.1p/DiffServ/802.11e

To map a traffic category to a QoS class, select the specified map and then define the traffic settings as described in Configure Classifier Maps on page 514.

## Configure Classifier Maps

To map a traffic category to a QoS class, select the specified tab, and then define the traffic settings described in the following procedures.

**Note**
Be sure to enable all the categorization methods you want devices to use when assigning incoming traffic to various QoS classes. A network policy can reference just one classifier map.

Classifier Maps are supported only by IQ Engine devices and do not effect other devices.

1. Go to **Configuration** > **Network Policies**, select **Menu**, and then go to **Common Objects** > **QOS** > **Classifier Maps** > **Services** tab.
2. Select an existing map, and then select , or to add a new one, select .
3. Type a **Name** for the Classifier Map.
4. (Optional) Type a **Description**.

   Although optional, descriptions can be helpful when you are configuring or troubleshooting your network.
5. Select an existing service, and then select , or to add a new one, select .
6. For a new service, select either **Network Services** or **Application Services**.

   Extreme Network devices can map incoming traffic to classes based on the network or application service type defined in the classifier map.
7. Select one or more services (up to a maximum of 100) to map to a class.
   a. Choose **Select from the following** and filter services by typing part or all of a service name in the **Filter** field.
   b. Select a QoS class to which you want to map the selected services or applications.

c. For the action, choose **Permit** or **Deny**.

The permit and deny actions in a QoS policy enable devices to enforce a simple stateless firewall policy that inspects packets individually, instead of within the context of an ongoing session. Because a stateless firewall configured to permit outgoing requests does not associate the corresponding incoming responses, you must configure a separate policy to permit the return traffic. A stateful firewall uses an internal table to associate corresponding outgoing and incoming traffic.

d. Enable **Logging** to permit devices to log traffic that matches the service-to-Extreme Networks class mapping.

Devices log traffic whether the action is permit or deny. The main reason to log traffic is to see if the devices are receiving expected or unexpected types of traffic when you debug connectivity issues. You can see these log entries in the even log using the following command:

```
show logging buffered
```

Or, you can configure the device to send event logs to a syslog server and view them there.

e. Select **SAVE**.

Alternatively, you can select services individually.

8. Select **SAVE**.

Related Links

QoS Configuration on page 512

*Configure Classifier Maps Based on MAC OUIs*

Devices can map traffic to classes based on either the source or destination MAC organizationally unique identifiers (OUIs) in a packet. To configure this mapping, follow these steps:

1. Go to **Configuration** > **Network Policies**, select **Menu**, and then go to **Common Objects** > **QOS** > **Classifier Maps** > **MAC OUIs** tab.
2. Select an existing map, and then select , or to add a new one, select .
3. Type a **Name** for the Classifier Map
4. Type an optional **Description**.
5. Select an existing MAC OUI, and then select , or to add a new one, select .
   a. Select the name of a **MAC OUI** (also known as a MAC vendor ID) from the drop-down list.

   If you do not see the MAC OUI that you want, select **New** and define one.

   b. Choose a **QoS Class** to which you want to map traffic using this SSID.
   c. For **Action**, select either **Permit** or **Deny**.

   Permit allows traffic that matches the source MAC OUI to pass through the device. Deny blocks it. These actions in a QoS policy enable devices to enforce simple stateless firewall policies.

d. Enable **Logging** to log traffic that matches the MAC-OUI-to-Extreme Networks class mapping.

   Logging is enabled by default, and helps you determine if the devices are receiving expected or unexpected types of traffic when you debug connectivity issues. You can see log entries in the event log on devices using the **`show logging buffer`** command. You can also configure the device to send logs to a syslog server where you can view log entries.

e. Select **SAVE**.

6. To add more MAC-OUI-to-Extreme Networks QoS class definitions, select + and repeat steps 3–5.
7. Select **SAVE**.

*Configure Classifier Maps Based on SSIDs*

Devices can map traffic to classes based on either the SSID on which a packet arrives or the SSID on which it leaves. Use the following steps:

1. Go to **Configuration** > **Network Policies**, select **Menu**, and then go to **Common Objects** > **QOS** > **Classifier Maps** > **SSIDs** tab.
2. Select an existing map, and then select , or to add a new one, select .
3. Type a **Name** for the Classifier Map
4. Type an optional **Description**.
5. To add a new SSID, select .
   a. Select the name of an **SSID**.
   b. Choose a **QoS Class** to which you want to map traffic using this SSID.
   c. Select **SAVE**.
6. Select **SAVE**.

*Configure Classifier Maps Based on 802.1p/DiffServ/802.11e*

Extreme Networks devices can apply priority and class mappings to incoming traffic based on the priority markers of standard QoS classification systems in use in the surrounding network, such as IEEE 802.1p, DSCP (DiffServ codepoint), or IEEE 802.11e. A device can map the values to the classes in the QoS classification system, process the traffic accordingly, and then use a marker map to map the classes back to appropriate values in an external classification system before forwarding. By doing this, the device can apply its own QoS system to optimize the flow of traffic it processes while supporting a different QoS system used in the surrounding network.

The QoS classification tables show the mapping of priority values on incoming packets to classes. To enable the mapping of one of these classification systems, select 802.1p/DiffServ/802.11e, and then select a system. You can use the default mappings or modify them if necessary.

1. Go to **Configuration** > **Network Policies**, select **Menu**, and then go to **Common Objects** > **QOS** > **Classifier Maps** > **802.1p/DiffServ/802.11e** tab.
2. Select an existing map, Select an existing map, and then select , or to add a new one, select .

3. Type a **Name** for the Classifier Map
4. Type an optional **Description**.
5. Select a classification system **802.1p**, **DiffServ**, **802.11e**.

   You can use the default mappings or modify them if necessary.
6. Select **SAVE**.

## Configure Marker Maps

For outgoing traffic, you can define marker maps to map classes to priority numbers in standard classification systems (802.11e, 802.1p, and DSCP). After you define classifier and marker maps, you can add them to user profiles. Finally, you associate the user profiles with SSIDs or interfaces to apply the mappings to traffic arriving at or exiting those interfaces.

**Note**
Marker Maps are supported only by IQ Engine devices. They do not apply to other devices.

Use this task to configure marker maps for outgoing traffic.

1. Go to **Configuration** > **Network Policies**, select **Menu**, and then go to
2. Select an existing map, and then select , or to add a new one, select .
3. Enter a **Name** for the marker map.
4. Enter an optional **Description** for the map.
5. On the **802.1p Markers** tab, toggle **802.1p Markers** to **On**.

   The QoS marking table shows the mapping of classes to WMM® (Wi-Fi Multimedia™) queues and the 802.1p classification system (marked in the L2 frame header in Ethernet frames). You can modify these mappings if necessary.

   Extreme Network devices automatically include 802.11e priority marking in the L2 headers of wireless frames, so it is not included here as a configurable option.

   Depending on the classification systems used in the surrounding network, select the appropriate check boxes to map classes to one or both systems for outgoing traffic. A network policy can reference just one marker map.
6. On the **Diffserv** tab, toggle **Diffserv** to **On**.

   The QoS marking table shows the mapping of classes to WMM® (Wi-Fi Multimedia™) queues and the DiffServ codepoint marking system (marked in the L3 packet header) on outgoing packets. You can modify these mappings if necessary.

**Note**
If both 802.1p and DiffServ are enabled, only DiffServ takes effect.

Related Links

Configure User Profiles on page 495
Configure User Profile QoS on page 371

## Configure Rate Control & Queuing

Through the combined configuration of rate limits and forwarding mechanisms, you can control how a device schedules traffic forwarding for users belonging to a user profile. You can apply QoS to traffic originating from members of user profiles to determine the prioritization of various categories of traffic. Through these settings, you can set rate limits and traffic forwarding for each traffic class.

Use the following task to configure rate control and queuing profiles for network traffic.

1. Go to **Configuration** > **Network Policies**, select **Menu**, and then go to **Common Objects** > **QOS** > **Marker Maps**.
2. Select an existing **Rate Limit**, and then select , or to add a new one, select .
3. Enter a **Name** for the rate control profile.
4. Type the **Rate Limit per Client** and use the menu to specify **Mbps** or **Kbps**
5. Configure **Traffic Queue Management Per User per AP**.

   The **Class Number/Name** is a read-only list of the eight classes.

   **Note**
   Extreme Networks devices control the maximum amount of concurrent, cumulative bandwidth that members of a user profile can use by enforcing a maximum rate limit.

6. Select from one of two types of scheduling methods, **Strict** or **Weighted Round Robin**.

   **Strict** forces devices to immediately forward traffic with strict scheduling. This type of traffic is not queued.

   Devices forward **Weighted Round Robin** traffic based on class and weight of the traffic. Traffic with a higher class and greater weight is forwarded more quickly.
7. Set the scheduling method that you want the device to use for each traffic class.

   The default scheduling methods for each class are:

   - 7—Network Control: Strict
   - 6—Voice: Strict
   - 5—Video: WRR
   - 4—Controlled: WRR
   - 3—Excellent Effort: WRR
   - 2—Best Effort 1: WRR
   - 0—Background: WRR
8. Type a number for the scheduling weight preference.

   This is a defined preference for forwarding traffic using WRR scheduling. The weight that you enter affects the automatically calculated percentage of weight of each class of traffic in relation to the weights of the other classes.

9. Set a rate limit for each of the eight classes.

   Devices allocate bandwidth by rate limiting traffic based on its class. For each class, you can set a different rate limit for devices supporting IEEE 802.11a/b/g, 802.11n, and 802.11ac/x. The default rate limits for each class are as follows:

   - 7—Network Control: 512 Kbps for 802.11a/b/g, 20,000 for 802.11n, 40,000 for 802.11ac and 802.11ax.
   - 6—Voice: 512 Kbps for 802.11a/b/g, 20,000 for 802.11n, 40,000 for 802.11ac/x.
   - 5—Video: 10,000 Kbps for 802.11a/b/g, 1,000,000 for 802.11n, 2,000,000 for 802.1ac/ax.
   - 4—Controlled: 54,000 Kbps for 802.11a/b/g, 1,000,000 for 802.11n, 2,000,000 for 802.11ac/ax.
   - 3—Excellent Effort: 54000 Kbps for 802.11a/b/g, 1,000,000 for 802.11n, 2,000,000 for 802.11ac/ax.
   - 2—Best Effort 1: 54000 Kbps for 802.11a/b/g, 1,000,000 for 802.11n, 2,000,000 for 802.11ac/ax.
   - 1—Best Effort 2: 54,000 Kbps for 802.11a/b/g, 1,000,000 for 802.11n, 2,000,000 for 802.11ac/ax.
   - 0—Background: 54,000 Kbps for 802.11a/b/g, 1,0000,00 for 802.11n, 2,000,000 for 802.11ac/ax.

10. Select **SAVE**.

Related Links

QoS Configuration on page 512

## Management Configuration

The topics in this section provide details about management server configuration objects, such as DNS, NTP, SNMP, and Syslog server objects.

Related Links

Configure DNS Servers on page 519
Configure NTP Servers on page 520
Configure SNMP Servers on page 521
Configure Syslog Servers on page 522

### Configure DNS Servers

The DNS (Domain Name System) translates human-friendly domain names into IP addresses. You can supply external DNS server IP addresses or use routers to provide proxy DNS services for every local network under their control. The DNS service transparently proxies DNS requests and responses to and from internal or external DNS servers.

Use this task to configure a DNS server profile object.

1. Go to **Configuration** > **Network Policies**, select **Menu**, and then go to **Common Objects** > **Management** > **DNS Servers**.

2. Select an existing DNS server profile object, and then select , or to add a new one, select ..
3. Configure the DNS Server Settings on page 281.
4. To add a new DNS server, select .
   a. Type the IP address of the new DNS server.
   b. Select **ADD**.

   You can add up to three servers. The first entry is the primary server. The secondary entry is the secondary server, and the third entry is the tertiary server. Use the arrows in the **Order** column to change the order.
5. Select **SAVE**.

Related Links

DNS Server Settings on page 281
Management Configuration on page 519

## Configure NTP Servers

Extreme Networks devices typically obtain the time and date for their internal clocks from an NTP server.

Use this task to create NTP server profiles objects.

**Note**
If enabled, these NTP server settings override the default NTP behaviors of your managed devices. The NTP servers defined here must be reachable from your managed devices on outbound UDP port 123.

1. Go to **Configuration** > **Network Policies**, select **Menu**, and then go to **Common Objects** > **Management** > **NTP Servers**.
2. Select an existing NTP Server, and then select , or to add a new one, select ..
3. Configure the NTP Server Settings on page 282.
4. To add a new NTP server to the list, select .
   a. To use an existing NTP server, select , and choose a server.
   b. To add a new NTP server, select , and then select **IP Address** or **Host Name**.
   c. Type a **Name** for the new object.

      You can use the menu to change your previous selection (**IP Address** or **Host Name**).
   d. Select **SAVE IP OBJECT**.
   e. Select **ADD**.

      ExtremeCloud IQ (New) accesses NTP servers in order, from the top down. Use the arrows to rearrange them.
5. Select **SAVE**.

Related Links

NTP Server Settings on page 282

Management Configuration on page 519

## Configure SNMP Servers

You can create an SNMP server profile at the device level for a specific VGVA to override the SNMP server profile inherited from the network policy to which the VGVA belongs.

**Note**
You can only add an SNMP server profile at the device level if SNMP is first enabled and configured at the network policy level.

Use this task to configure an SNMP server profile object.

1. Go to **Configuration** > **Network Policies**, select **Menu**, and then go to **Common Objects** > **Management** > **SNMP Servers**.
2. Select an existing SNMP server, and then select , or to add a new one, select ..
3. Configure the SNMP Server Settings on page 284.
4. To add a new SNMP server, select , and then select **IP Address** or **Host Name**.
   You can add up to three SNMP servers to the profile.
5. To use an existing SNMP server, select .
   Choose the IP address or host name object for the SNMP server or servers that will access the devices. To permit management access from a single SNMP server, choose an IP address or host name that defines just that server. To permit management access from an entire subnet, choose an IP address or host name that defines that subnet. If you do not see the IP address or host name that you need, select **New** and define one.
6. Type a **Name** for the new IP object.
7. (Optional) If you want to change your previous selection, select **IP Address** or **Host Name** from the menu.
8. Select **SAVE IP OBJECT**.
9. Select the version of SNMP server that is running on the management station you intend to use from the **Version** menu.
10. From the **Operation** menu, select the type of activity to permit between the specified SNMP management station and the devices in the network policy that are assigned to this profile.
    Options include:
    - **None**: Disable all SNMP activity for the specified management station.
    - **Get**: Permit GET commands sent from the management station to a device to retrieve MIBs.
    - **Get and Trap**: Permit the reception of GET commands from the management station and the transmission of traps to the management station.
    - **Trap**: Permit devices to send messages notifying the management system of events of interest.
11. In the **Community** field (for SNMP V2C and V1), enter a text string that must accompany queries from the management station.
    The community string acts similarly to a password, such that devices only accept queries from management stations that send the correct community string.

12. Select **ADD SNMP SERVER**.
13. Select **SAVE**.

Related Links

SNMP Server Settings on page 284
Management Configuration on page 519

## Configure Syslog Servers

Use this task to configure a syslog server object.

1. Go to **Configuration** > **Network Policies**, select **Menu**, and then go to **Common Objects** > **Management** > **Syslog Servers**.
2. Select an existing Syslog Server, and then select , or to add a new one, select ..
3. Configure the Syslog Server Settings on page 286.
4. To add a syslog server to the table, select .
   Use the up or down arrows to reorder the list of syslog servers in the table.
5. Select , and choose an existing syslog IP Address or host name.
6. For **Severity**, select the log level.
7. Type the **Port** number.
8. Select **ADD**.
9. Select **SAVE SYSLOG SERVER**.

Related Links

Syslog Server Settings on page 286
Management Configuration on page 519

# Network Configuration

The topics in this section provide details about network configuration objects, including: Access consoles, ALG, LLDP/CDP profiles, IP tracking groups, Layer 2 IPSec/VPN services, location servers, management options, tunnel policies, network services, subnetwork space, firewalls, and VPN services.

Related Links

Configure Access Consoles on page 523
Configure ALG Services on page 524
Configure LLDP/CDP Profiles on page 525
Configure IP Tracking Groups on page 526
Configure Layer 2 IPsec VPN Services on page 526
Configure Location Servers on page 532
Configure Management Options on page 535
Configure Tunnel Concentrator Services on page 535
Configure Tunnel Concentrator Address Pool (TCAP) Profiles on page 541
Configure Tunnel Policies on page 542
Configure Network Services on page 545

Configure a Subnetwork Space on page 546
Configure Firewalls on page 508

## Configure Access Consoles

An access console is a special SSID that provides wireless console access to a device when it is not accessible through the wired network.

**Note**
Access Console is supported by IQ Engine APs only, and cannot be used with other devices.

1. Go to **Configuration** > **Network Policies**, select **Menu**, and then go to **Common Objects** > **Network** > **Access Consoles**.
2. Select an existing Access Console, and then select , or to add a new one, select .
3. Enter a **Name** for the Access Console.
4. (Optional) Enter a **Description**.

   Although optional, descriptions can be helpful when you are configuring or troubleshooting your network.
5. Set the **Mode** for the console.
   - **Auto**—Automatically enabled
   - **Enable**—Manually enabled
   - **Disable**—Manually disabled
6. Select one of the following **Access Security** options:

   **WPA-(WPA or Auto)-PSK**: Use WPA for key management on devices introduced before ExtremeCloud IQ (New) 6.1r5; and for Extreme Networks devices introduced in ExtremeCloud IQ (New) 6.1r5 or later, to negotiate the use of WPA2 or WPA with their associated clients.

   **WPA2 -(WPA2 Personal)-PSK**: Force clients to use the WPA2 key management scheme. WPA supports PMK caching and preauthentication where WPA does not.

   **Auto-(WPA or WPA2)-PSK**: Negotiate the use of WPA2 or WPA with clients based on their supported version.

   **Note**
   This option automatically chooses the **Encryption Method**.

   **Open**: Unsecured network access.

   **Note**
   This option does not require an **Encryption Method** or **ASCII Key**.
7. Select an **Encryption Method** based on your chosen Access Security option.
8. When using one of the preshared key options, enter the **ASCII Key**.
9. Set the maximum number of wireless clients that can concurrently connect to the access console.

10. Select **Hide the SSID in beacons and probe responses** so that the device does not announce the SSID for the access console in its beacons or in its responses to clients' probes.
11. Select **Enable Telnet Access** to enable Telnet connectivity to the device through the access console.
12. To add a MAC Filter, select the plus sign.
13. For **MAC Filters/Default Action**, select **Permit** to enable traffic from clients that do not match one of the selected filters, or **Deny** to block traffic from clients that do not match any of the selected MAC filters.
14. Select the plus sign.
15. Either select an existing MAC Filter or select the plus sign to create a new **MAC Address** or **OUI**.
16. If you create a new address or OUI, enter the information and select **Save**.
17. For **Action**, select **Permit** to enable traffic from clients that do not match one of the selected filters, or **Deny** to block traffic from clients that do not match any of the selected MAC filters.
18. Select **ADD**.
19. Select **SAVE**.

Related Links

Network Configuration on page 522

## Configure ALG Services

Use this task to configure an Application Layer Gateway (ALG) service object.

1. Go to **Configuration** > **Network Policies**, select **Menu**, and then go to **Common Objects** > **Network** > **ALG Services**.
2. Select an existing ALG service object, and then select , or to add a new one, select ..
3. Type a **Name** for the ALG service.
4. (Optional) Type a **Description** for the service.
5. Select the corresponding check boxes to enable the protocols you want to associate with this ALG service.
6. Select the **QoS Class** to apply to each protocol for which QoS is available.
7. Specify the **Inactive Data Timeout** for FTP, SIP, and TFTP to keep devices from timing out during long file transfers.

   The range is 1 to 1800 seconds, and defaults vary by protocol.
8. Specify the **Max Session Duration** for FTP, SIP, and TFTP.

   The range is 1 to 7200 minutes, and defaults very by protocol.
9. Select **SAVE**.

Related Links

Network Configuration on page 522

## Configure LLDP/CDP Profiles

To enable LLDP/CDP for a port, ensure that LLDP/CDP is enabled in both the policy level and the port level configuration.

Extreme Networks devices can advertise LLDP data and receive, cache, and display both LLDP and CDP data. However, they do not advertise CDP data. You can use LLDP and CDP data to help debug network issues. For example, the CDP data can be used when debugging VLAN issues on Cisco switches.

Use this task to configure a new LLDP/CDP object.

1. Go to **Configuration** > **Network Policies**, select **Menu**, and then go to **Common Objects** > **Network** > **LLDP/CDP**.
2. Select an existing LLDP/CDP object, and then select , or to add a new one, select .
3. Enable **LLDP/CDP**, and then configure the settings.
4. Select **SAVE**.

Related Links

LLDP/CDP Profile Settings on page 525
Network Configuration on page 522

*LLDP/CDP Profile Settings*

| Setting | Description |
|---|---|
| Name | Type a **Name** for the new LLDP/CDP object. |
| Description | (Optional)<br>Type a **Description** for the new LLDP/CDP object. Although optional, descriptions can be helpful when you are configuring or troubleshooting your network. the LLDP/CDP object. |
| Enable LLDP on access ports | Select the check box to permit LLDP on access ports.<br><br>**Note:** LLDP is enabled on other port types by default. |
| Enable receive only mode. | Select the check box to permit devices to receive, cache, and display LLDP advertisements from other devices, but to not advertise their own data. |
| LLDP entries to cache | (IQ Engine Only)<br>Type the maximum number of LLDP entries from neighboring network devices that a device can store in its cache. |
| Neighbors keep Extreme Networks advertisements for | Type the number of seconds for which neighboring devices retain LLDP advertisements.<br>Increase the time while troubleshooting a network issue and decrease it if you need to reduce overall network traffic. |
| Advertisements Interval | Type the number of seconds between LLDP advertisements sent to neighboring network devices. |
| Timer Hold | Type a multiple of the advertisements interval. (EXOS/Switch Engine, VOSS/Fabric Engine, SR22XX/23XX, Dell) |

| Setting | Description |
|---|---|
| Max power for LLDP advertisements | Select **Use the default max power in IQ Engine** to use the maximum power level that devices can request in LLDP advertisements. |
| LLDP Initialization Delay Time | Type the length of time that you want the interface to wait before initializing LLDP. |
| Fast start repeat count | Type the number of advertisement LLDP frames to send when the connected device (such as an IP phone) starts up or is discovered. |
| CDP (Cisco Discovery Protocol) | Toggle CDP **ON** to enable devices to receive and cache CDP advertisements.<br><br>**Note:** You can enable LLDP and CDP concurrently.<br><br>CDP is a proprietary Data Link Layer protocol developed by Cisco Systems. |
| Enable CDP on access ports. | Select the check box to permit CDP on access ports. By default, CDP is enabled on other port types. |
| CDP entries to cache | Type the maximum number of CDP entries that a device can store in its cache. |

## Configure IP Tracking Groups

You can specify groups of IP addresses to track and take action if one or more IP addresses become unreachable. IP group tracking logs and sends alerts when group IPs are unresponsive, and when actions are taken. A customized tracking group can be used to disable specific SSIDs when an IP is unavailable.

This task is part of the network policy configuration workflow. Use this task to configure IP tracking group objects.

1. Go to **Configuration** > **Network Policies**, select **Menu**, and then go to **Common Objects** > **Network** > **IP Tracking Groups**.
2. Select an existing IP tracking group, and then select , or to add a new one, select . to create a new group.
3. Configure the settings.
4. Select **SAVE**.

Related Links

IP Tracking Group Settings on page 294
Network Configuration on page 522

## Configure Layer 2 IPsec VPN Services

First configure a new VPN service. See Configure VPN Services on page 550.

Layer 2 IPsec VPN is a logical extension of the Layer 2 broadcast domain across an IPsec VPN tunnel. After configuration, it is available for use in multiple network policies.

Use this task to configure a new Layer 2 IPsec VPN service object.

1. Go to **Configuration** > **Network Policies**, select **Menu**, and then go to **Common Objects** > **Network** > **Layer 2 IPsec VPN Services**.
2. Select an existing Layer 2 IPsec VPN service, and then select , or to add a new one, select .
3. Configure the Layer 2 VPN Services Settings on page 527.
4. Select **SAVE**, or configure **Optional Settings**.

Configure **Optional Settings** > **IPsec VPN Authority Settings**, see Configure IPsec VPN Authority Settings on page 528.

Related Links

Configure VPN Services on page 550
Layer 2 VPN Services Settings on page 527
Configure IPsec VPN Authority Settings on page 528

*Layer 2 VPN Services Settings*

| Setting | Description |
|---|---|
| Name | Type a **Name** for the service. |
| Description | (Optional)<br>Type a **Description**. Although optional, descriptions can be helpful when you are configuring or troubleshooting your network. |
| **Device VPN Server and Device VPN Client Settings** | |
| Single Device VPN Server | Select **Single Device VPN Server** if you are not implementing redundant VPN servers. |
| Redundant Device VPN Servers | Select **Redundant Device VPN Servers** to configure a redundant VPN server.<br>Configure the settings for **Device VPN Server 1** and **Device VPN Server 2**. |
| Device VPN Server | Select an AP with Layer 2 IPsec VPN services enabled. |
| Server Public IP Address | Auto-populated based on the selected VPN server settings. To change this setting, type the IP address of a VPN server that VPN clients can reach across the network.<br><br>**Note:**<br>If the VPN server is behind a NAT device, enter the address of the MIP address on the NAT device.<br>If there is no NAT device in front of the VPN server, enter the mgt0 IP address of the server. |
| Server MGT0 IP Address | Auto-populated and read-only. |
| Server MGT0 Default Gateway | Auto-populated and read-only. |

| Setting | Description |
|---|---|
| Client Tunnel IP Address Pool Start | Type the first IP address of the range of addresses that the VPN server assigns to tunnel interfaces on VPN clients during the Xauth phase of tunnel setup.<br>As a best practice, put this address pool in the same subnet as the VPN server mgt0 interface, and the same subnet as the addresses that the DHCP server assigns to wireless clients through the tunnel. If the tunnel interfaces are in a different subnet, you must define a route the VPN server default gateway router uses to forward traffic destined for the tunnel interface, and traffic destined for the wireless clients to the VPN server mgt0 interface. |
| Client Tunnel IP Address Pool End | Type the IP address at the end of the range of IP addresses in the address pool. |
| Client Tunnel IP Address Pool Netmask | Type the netmask that defines the subnet to which the tunnel interfaces belong. |
| Device VPN Client DNS Server | Select the DNS server IP address or host name object that VPN clients use to resolve domain names, or select + to define a new one. |
| **User Profiles for Traffic Management**<br>ExtremeCloud IQ displays a list of available user profiles, for which traffic can be forwarded through the Layer 2 IPsec VPN tunnel or forwarded without tunneling. | |
| VPN Tunnel Mode | In the **VPN Tunnel Mode** column, select **Enable** to enable VPN clients to tunnel traffic for specific user profiles. |
| Tunnel All Traffic | To tunnel all client traffic, select **Tunnel All Traffic**. |
| Split Tunnel | To enable split mode tunneling, select **Split Tunnel**. |

Related Links

Configure a Layer 2 IPsec VPN Service on page 450
Configure Layer 2 IPsec VPN Services on page 526

*Configure IPsec VPN Authority Settings*

First, create or edit a Layer 2 IPsec VPN service. For more information, see Configure Layer 2 IPsec VPN Services on page 526.

The authentication mechanism between a VPN gateway and a VPN client operates in hybrid mode, which employs a combination of certificates and passwords for VPN peer authentication. Use this task to import certificates in PFX or DER formats, to import a pair of DER-formatted files, one containing a certificate and the other its accompanying private key, and convert the format from DER to PEM.

**Note**

Default certificates are intended to be used for testing only.

Extreme Networks VPN gateways do not support password-encrypted certificates.

For hybrid mode authentication, ExtremeCloud IQ (New) distributes the certificates as follows:

- **VPN Certificate Authority**: The CA certificate is loaded on VPN clients so that they can validate the server certificate that the VPN gateway presents.
- **VPN Server Certificate**: The server certificate on the VPN gateway is used during IKE Phase 1 negotiations to authenticate itself to the VPN client.
- **VPN Server Cert Private Key**: The private key accompanies the public key in the server certificate. This is also loaded on the VPN gateway.

Use this task to configure **IPsec VPN Authority Settings** as part of a Layer 2 VPN service object.

1. Go to **Configuration** > **Network Policies**, select **Menu**, and then go to **Common Objects** > **Network** > .
2. Select an existing Layer 2 IPsec VPN service, and then select , or to add a new one, select .
3. In the **Optional Settings** section, expand **IPsec VPN Authority Settings**.
4. If you do not have a certificate or key that you want to use, select **Import**.
5. To import a PFX-formatted file, which contains a certificate and private key combined, and convert its format from PFX to PEM:
   a. Choose **Select**, navigate to and select the .PFX file.
   b. Select **Convert the certificate format from PFX to PEM**.
   c. Enter the password that was used to encrypt the PFX file.
   d. Select **Import**.

      Later, when you use the PEM-formatted file that contains both the certificate and private key, you must choose the same file as both the VPN Certificate and the VPN Cert Private Key.
6. To import a pair of DER-formatted files, one containing a certificate and the other its accompanying private key, and convert their format from DER to PEM:
   a. Choose **Select**, navigate to and select the .DER file.
   b. Select **Convert the certificate format from DER to PEM**.
   c. Select the type of file you are importing; in this case, **Certificate**.
   d. Select **Import**.
   e. To import the private key file matching the public key in the certificate you just imported, repeat Steps a-c, but select **Key** for the file type.
   f. When importing a DER-formatted private key, enter the password used to encrypt the file.
   g. Select **Import**.

      When you choose the VPN Server Certificate and VPN Server Cert Private Key, make sure they correspond with each other.

For information about **Optional Settings** > **Server-Client Credentials**, see Server-Client Credentials on page 530.

Related Links

Configure Layer 2 IPsec VPN Services on page 526
Server-Client Credentials on page 530

*Server-Client Credentials*

After you save the Layer 2 IPsec VPN service configuration, ExtremeCloud IQ (New) populates the table with randomly generates text strings that VPN clients use to identify themselves to VPN gateways. Extreme Networks VPN clients use these strings like passwords when identifying themselves to the VPN gateway during the Xauth stage between IKE Phase 1 and 2 negotiations.

After you configure a device as a VPN client, ExtremeCloud IQ (New) allocates one of the credentials to it. The name of the VPN client appears in the **VPN Client Name** column and the entry in the **Allocated** column changes from false to true. The primary and secondary VPN servers assigned to that client appear in their respective columns.

Next, configure **Optional Settings** > **Advanced Server Options** for the VPN service. See Configure Advanced Server Options on page 530.

Related Links

Configure Advanced Server Options on page 530

*Configure Advanced Server Options*

First, create a Layer 2 IPsec VPN service. For more information, see Configure Layer 2 IPsec VPN Services on page 526.

Use this task to configure the **Advanced Server Options** for a new Layer 2 IPsec VPN object.

1. **Common Objects** > **Policy** > **IoT ProfilesCommon Objects** > **Network** > **Layer 2 IPsec VPN Services**.
2. Select an existing VPN service, and then select , or to add a new one, select ..
3. In the **Optional Settings** section, expand **Advanced Server Options**.
4. Configure the **IKE Phase 1 Options**.
   a. Set the **Encryption Algorithm** as 3DES (Triple DES, Data Encryption Standard), or AES (Advanced Encryption Standard) with a 128-bit key, a 192-bit key, or a 256-bit key.
   b. Set the **Hash Algorithm** as MD-5 (Message Digest, version 5) or SHA-1 (Secure Hash Algorithm).
   c. Set the **Diffie-Hellman Group** for generating a shared key during Phase 1 negotiations to 1, 2, or 5.
   d. Set the phase 1 SA (security association) **Lifetime**.

      Before the SA expires, the authentication and encryption keys automatically refresh with new ones. You can set it to a different value, from 180 seconds (3 minutes) to 10,000,000 seconds (a very long time).
5. Configure the **IKE Phase 2 Options**.

   The options are the same as for Phase 1, except you can choose to not perform a Diffie-Hellman key exchange by selecting **No PFS (Perfect Forward Secrecy)**.
6. Select **SAVE**, or continue configuring the VPN service.

*Configure Advanced Client Options*

First, create a Layer 2 IPsec VPN service. For more information, see Configure Layer 2 IPsec VPN Services on page 526.

For Layer 2 IPsec VPN tunnels, all management servers (CAPWAP, Syslog, SNMP, NTP, RADIUS, Active Directory, and LDAP) should be reachable from the VPN client without tunneling by default. However, you might want to tunnel some or all management traffic from the VPN client to servers on the main network.

1. Go to **Configuration** > **Network Policies**, select **Menu**, and then go to **Common Objects** > **Network** > **Layer 2 IPsec VPN Services**.
2. Select an existing VPN service, and then select , or to add a new one, select ..
3. In the **Optional Settings** section, expand **Advanced Client Options**.
4. For **Management Tunnel Traffic Options**:

   **Note**
   Set the following options only when the servers are in a different subnet from that of the tunnel interface. When they are in the same subnet, tunneling is automatic. In addition, the IP address/host name objects for the following servers must have IP address definitions as opposed to host name definitions.

   a. Select **ExtremeCloud IQ (CAPWAP)** to tunnel all CAPWAP (Control and Provisioning of Wireless Access Points) traffic from VPN clients to ExtremeCloud IQ, which is a CAPWAP server.
   b. Select **Syslog** to send log entries to a syslog server through the VPN tunnel.
   c. Select **SNMP Traps** to send all SNMP traps through the VPN tunnel to an SNMP management system.
   d. Select **NTP** to tunnel all NTP traffic from VPN clients to an NTP server.
   e. Select **RADIUS** to tunnel all RADIUS traffic from VPN clients to a RADIUS authentication server.
   f. Select **Active Directory** to tunnel all traffic from an Extreme Networks RADIUS authentication server to an Active Directory server.
   g. Select **LDAP** to tunnel all traffic from a RADIUS authentication server to an LDAP server.
5. Select **Enable NAT Traversal** to enable VPN traffic to traverse NAT devices.
6. For **DPD Settings**:

   The Dead Peer Detection (DPD) settings control when to fail over from the primary to the secondary VPN server. The DPD messages verify the presence of an IKE peer.

   a. Set the **Heartbeat Interval** for sending DPD R-U-There heartbeat messages from the VPN client to the VPN gateway.
   b. Set the **Number of Retries** after a DPD R-U-There message does not elicit a response.
   c. Set the **Retry Interval** (length of time between retries).
7. For **Tunnel Heartbeat Settings**:

   The tunnel heartbeat settings control when to fail over from the primary to the secondary VPN server. The AMRP (Advanced Mobility Routing Protocol) tunnel heartbeats verify communications through the GRE and VPN tunnel.

   a. Set the **Interval** for sending AMRP heartbeats through the GRE and VPN tunnel from the VPN client to the VPN server.
   b. Set the number of times to **Retry** sending a heartbeat if the VPN server fails to respond.

      After a heartbeat fails to elicit a response from the VPN server, the VPN client retries every second.

8. Select **SAVE**.

Related Links

Configure Layer 2 IPsec VPN Services on page 526

## Configure Location Servers

Create a network policy for these settings.

Extreme Networks devices perform background monitoring for Wi-Fi devices, RFID tags, rogue APs, and others. When found, the devices send information to ExtremeCloud IQ (New), AeroScout location servers, or location services such as Ekahau that use Tazmen Sniffer Protocol (TZSP) to be monitored and tracked.

1. Go to **Configuration** > **Network Policies**, select **Menu**, and then go to **Common Objects** > **Location Servers**
2. Type a **Name**.
3. (Optional) Type a **Description**.

   Although optional, descriptions can be helpful when you are configuring or troubleshooting your network.
4. To turn on location tracking and reporting to the location processing engine, enable **Client Location Tracking**.
5. For **Track Client Location Using**:

   **Extreme Networks Location Server**: See Configure Track Client Location Using an Extreme Location Server on page 533.

   **AeroScout Location Server**: See Configure Track Client Location Using an AeroScout Location Server on page 533.

   **Tazmen Sniffer Protocol (Ekahau, etc...)**: See Configure Track Client Location Using the Tazmen Protocol on page 534.
6. In the **Extreme Networks Location Service Configuration** section, specify values for the following settings:
   - **RSSI Change Threshold**—Type a value in dB.
   - **RSSI Valid Period**—Type a value in seconds.

Related Links

Network Configuration on page 522

*Configure Track Client Location Using an AeroScout Location Server*

First, configure a Location server.

**Note**
When tracking AeroScout RFID tags, you must use the **AeroScout Tag Manager** to configure the tags to broadcast beacons using the IBSS data frame format. Navigate to the **Transmission** tab in the **Configuration** window. Choose **IBSS** from the Data Frame Format drop-down list, make sure that the MAC address in the **IBSS/WDS** field is `01-0C-CC-00-00-00`, which it is by default with **IBSS** chosen, and then select **Save**.

To integrate devices with AeroScout real-time locating services (RTLS), define the IP address or domain name of the AeroScout Engine, designate the types of wireless devices locations to track, set a threshold for the maximum number of packets per second, and enable the feature.

Use this task to configure the Track Client Location feature using an AeroScout Location Server.

1. Select **AeroScout Location Server**.
2. For **IP Address or Domain Name**, from the drop-down list, choose the IP address or host name of the AeroScout location processing engine that will receive tracking reports.

   Extreme Networks devices receive messages from the server on UDP port 1144. To add a new IP Address or Host Name, see Configure IP Objects/Host Names on page 501.
3. Select **Enable location detection for tags** to enable Extreme Networks devices to track Wi-Fi enabled tags and then forward them together with their RSSI values to the AeroScout location processing engine.

   Set a rate limit threshold to protect devices from CPU overload and attack by floods of malformed tag frames.
4. Select **Enable location detection for stations** to enable tracking currently active wireless stations.

   Set a rate limit threshold to determine the maximum number of station-transmitted packets to process each second. This threshold limits the amount of device CPU resources allocated to station tracking and protects the device from packet flood attacks.
5. Select **Enable location detection for rogue APs** to enable Extreme Networks devices to track the location of rogue APs, and report captured packets and rogue AP RSSI values to the AeroScout location processing engine.

   Set a rate limit threshold to protect Extreme Networks devices from CPU overload and packet flood attacks.

Related Links

Configure Location Servers on page 532

*Configure Track Client Location Using an Extreme Location Server*

Configure a Location Server.

Devices configured as location servers take readings on the RSSI. The RSSI indicates the RF signal strength of the link between the AP and the wireless client. Each Extreme Networks device within the client range sends its most recent RSSI measurement for that client to the

owner device. The owner device is the one to which a client is associated. Then the owner device sends an aggregated RSSI report to ExtremeCloud IQ.

1. Select **Extreme Networks Location Server**.
2. For **RSSI Change Threshold**, set the number of decibels (dB) a client RSSI must increase or decrease to trigger an Extreme Networks device to update its report to the owner device, and for the owner device to update its report to ExtremeCloud IQ.
3. For **RSSI Valid Period**, set the time that a client RSSI measurement remains valid.

   After this period elapses, an updated report for that client is transmitted even if the RSSI value has not crossed the RSSI change threshold.
4. For **RSSI Hold Count**, set the number of times the owner device can include the same client RSSI measurement from another device in its aggregate report to ExtremeCloud IQ before omitting it from future reports.
5. For **Location Report Interval**, set the interval between RSSI measurements from an Extreme Networks device to an owner device, and the owner device to ExtremeCloud IQ.
6. For **Report Suppression Count**, select the number of consecutive reports to suppress when a client RSSI measurement does not change significantly.

Continue configuring a network policy.

*Configure Track Client Location Using the Tazmen Protocol*

Create a Location Server.

**Note**
To integrate Extreme Networks devices with location services such as Ekahau that use the Tazmen Sniffer Protocol (TZSP), you must first configure the RFID tags with the SSID settings that they will use to associate with a device. With the IP address of the location processing engine or domain name, they will connect through the device. Refer to Ekahau product documentation for details on configuring tags through the Ekahau Activator and Ekahau Positioning Engine.

Use this task to configure Extreme Networks devices to work with a TZSP-based location service.

1. Select **Tazmen Sniffer Protocol**.
2. For **IP Address or Domain Name**, from the drop-down list, choose the IP address or host name for the location server that will receive TZSP-encapsulated multicast data frames, RSSI measurement, and channel information for each multicast frame.

   To add a new IP Address or Host Name, see Configure IP Objects/Host Names on page 501.
3. For **Port**, the Extreme Networks device listens for the connection request on the UDP port that you enter here.

   It must be the same port configured on the server.
4. Enter the **Multicast MAC Address** that RFID tags periodically transmit data frames to, so that devices can listen for them on their wireless interfaces, and forward them to the location engine specified in the **IP Address or Domain Name** field.

5. Enter the **Rate Limit Threshold for Tags** to protect Extreme Networks devices from CPU overload and attack by floods of malformed tag frames.

   The threshold applies to tags transmitting frames within the same second to the same set of Extreme Networks devices. The larger the number of tags, the less probable they will all happen to be sending multicast frames within the same second, and the less likely they will all associate within radio range of the same set of Extreme Networks devices. The threshold can be considerably lower than the number of deployed tags.

Continue configuring the network policy. If you have not already done so, configure an SSID with which the RFID tags will associate, and add it to the network policy.

## Configure Management Options

For more information about the settings, see Management Options on page 297.

Use this task to configure **Management Options** objects for administers.

1. Go to **Configuration** > **Network Policies**, select **Menu**, and then go to **Common Objects** > **Network** > **Management Options**.
2. Select an existing management object, and then select , or to add a new one, select .
3. Type a **Name**.
4. (Optional) Type a **Description**.

   Although optional, descriptions can be helpful when you are configuring or troubleshooting your network.
5. Configure Forwarding Engine Control Management Options on page 297.
6. Configure System Settings Management Options on page 300.
7. Configure Authentication Settings Management Options on page 304.
8. Select **SAVE**.

Related Links

Management Options on page 297
Network Configuration on page 522

## Configure Tunnel Concentrator Services

Add the Tunnel Concentrator (TC) as a device type. For more information, see Network Devices | Add Devices on page 129.

Configure TC services to establish secure tunnels for client data traffic and AP-originated RADIUS control traffic between access points and a Tunnel Concentrator.

Tunnel Concentrator services allow you to terminate GRE and GRE-over-IPsec tunnels from managed access points (APs). In addition to centralizing wireless client data traffic, TC

services support forwarding AP-originated RADIUS authentication and accounting traffic to corporate RADIUS servers located behind the TC termination point.

**Note**
To route RADIUS control traffic through a Tunnel Concentrator service, an active **Tunnel Concentrator Address Pool (TCAP) Profile** must be assigned to the service to provide inner IP addresses to APs.

Use this task to configure a new Tunnel Concentrator service.

1. Go to **Configuration** > **Network Policies**, select **Menu**, and then go to **Common Objects** > **Network** > **Tunnel Concentrator Services**.
2. Select an existing service, and then select , or to add a new one, select .
3. Configure Tunnel Concentrator Service Settings on page 537.
   - General Settings: Defines the foundational parameters for a Tunnel Concentrator Service, including the service name, description, IPsec data-plane encryption settings, tunnel IP address and CIDR, and gateway configuration.
   - Single Tunnel Concentrator: Configures a single Tunnel Concentrator Service when setting up centralized traffic tunneling for smaller branch deployments, lab environments, or non-critical guest networks. A single concentrator setup aggregates AP traffic to a single appliance endpoint, providing a straightforward configuration process without the management overhead or hardware costs associated with high-availability pairs.
   - Redundant Tunnel Concentrator: Configures a primary and secondary Tunnel Concentrator pair for high-availability deployments. Cloud APs establish active and standby tunnel endpoints, enabling instant, automated failover without requiring client re-authentication if the primary appliance becomes unreachable.
   - Tunnel Concentrator Address Pool (TCAP) Profile: These settings define the IP network parameters used by the Tunnel Concentrator to assign addresses and route traffic. Attaching a TCAP profile streamlines IP allocation, prevents subnet collisions across distributed sites, and ensures proper VLAN tagging for tunneled client traffic and RADIUS authentication requests.
   - Broadcast/Multicast Control: These settings allow administrators to define handling rules for non-unicast network traffic passing through the Tunnel Concentrator. Because broadcast and multicast frames are transmitted to all endpoints, uncontrolled multicast traffic can quickly saturate low-bandwidth WAN tunnel links and degrade wireless airtime performance.
4. Select **SAVE**.

Related Links

Network Configuration on page 522

*Tunnel Concentrator Service Settings*

**Table 179: Tunnel Concentrator Service General Settings**

| Field | Description |
|---|---|
| Name (required) | A unique, descriptive name to identify the Tunnel Concentrator service. |
| Description | Describe the purpose, deployment site, or administrative context of this service configuration. |
| Secure connection (IPSec) | Enable IPsec data-plane encryption for GRE tunnels established between Cloud APs and the Tunnel Concentrator. When enabled, traffic is encrypted using IKEv2/IPsec using a Pre-Shared Key (PSK).<br><br>**Important:** Enabling **Secure connection (IPSec)** requires supported Access Point models capable of IPsec offload (AP3000, AP3000X, AP4000, AP4020, AP4020X, AP4020FX, AP4060, AP4060X, AP5010, AP5050, AP5020). Ensure that matching pre-shared key credentials are configured on both endpoints. |
| Tunnel IP Address/CIDR (required) | The virtual tunnel IPv4 address and CIDR prefix length (for example, `10.100.1.1/24`) used by managed APs as the destination endpoint for tunneled traffic. |
| Gateway | The default gateway IPv4 address for the tunnel network segment (for example, `10.100.1.254`). This gateway routes outbound traffic exiting the Tunnel Concentrator to internal destination networks or authentication servers. |

**Table 180: Single Tunnel Concentrator**

| Field | Description |
|---|---|
| Native VLAN ID (required) | The Native VLAN ID (1–4094) assigned to untagged management traffic traversing the physical connection between the network and the Tunnel Concentrator appliance. |
| Device Tunnel Concentrator (required) | The onboarded Tunnel Concentrator appliance used to terminate incoming tunnel connections from Cloud APs. |
| Tunnel Port (required) | The physical or logical interface port on the appliance designated to receive inbound tunnel traffic from managed access points. |
| VLAN ID (required) | The VLAN ID (1–4094) assigned to egress tunnel data traffic.<br>Select**Untagged** if tunnel data traffic should exit the Tunnel Concentrator without a VLAN tag. When selected, the **VLAN ID** field is disabled. |
| Bridge Port (required) | The bridge port on the Tunnel Concentrator through which tunneled traffic is bridged onto the internal network segment. |

**Table 180: Single Tunnel Concentrator (continued)**

| Field | Description |
|---|---|
| AP Keepalive Interval (seconds) (required) | The time interval in seconds (default is 3) between heartbeat keepalive messages sent from the access point to the Tunnel Concentrator to monitor tunnel health. |
| AP Keepalive Retries (required) | The maximum number of consecutive unacknowledged keepalive probes (default is 5) permitted before the access point declares the tunnel down and attempts connection recovery. |

**Table 181: Redundant Tunnel Concentrator**

| Field | Description |
|---|---|
| VRRP Router ID (required) | The Virtual Router Redundancy Protocol (VRRP) Router ID (1–255) assigned to the Tunnel Concentrator high-availability pair.<br>ExtremeCloud IQ (New) configures the same VRRP Router ID for both the primary and backup Tunnel Concentrators. The **VRRP Router ID** must be different for each cluster of VRRP devices. |
| Native VLAN ID (required) | The Native VLAN ID (1–4094) assigned to untagged management traffic traversing the physical connection between the network and the Tunnel Concentrator appliances. |
| **Primary & Backup Concentrator Pair Fields**: Configure the primary active appliance and secondary standby appliance options for the redundant pair. | |
| Device Tunnel Concentrator (required) | The onboarded Tunnel Concentrator appliance. |
| Tunnel Port (required) | The interface port receiving inbound tunnel connections. |
| VLAN ID (required) | The VLAN ID (1–4094) applied to egress tunnel data traffic for this appliance.<br>Select **Untagged** if tunnel data traffic should exit the appliance without a VLAN tag. |
| IP Address (required) | The physical interface IPv4 address of the Tunnel Concentrator appliance. |
| Bridge Port (required) | The bridge port forwarding tunneled traffic onto the internal network segment. |
| **AP Keepalive Parameters** | |

**Table 181: Redundant Tunnel Concentrator (continued)**

| Field | Description |
|---|---|
| AP Keepalive Interval (seconds) | Specifies the interval at which the AP sends keepalive messages to the primary and backup tunnel concentrators. The AP sends keepalive only to tunnels that are not in use and listens for a response from each tunnel concentrator independently.<br>If the AP receives a response, it sets the tunnel status to **Active**. If no response is received within the interval, the AP retries the keepalive based on the configured **AP Keepalive Retries** value.<br>Possible values: 1 to 60 seconds<br>Default: 3 seconds |
| AP Keepalive Retries | Specifies the maximum number of retry attempts for a failed keepalive before the AP changes the tunnel status to **Inactive** for the primary or backup tunnel concentrator.<br>If the AP does not receive a keepalive response within the configured interval, it retries until the maximum retry count is reached. When the retry limit is exceeded, the AP marks the tunnel as **Inactive**. If a response is later received, the AP changes the tunnel status to **Active** and resets the retry count.<br>Possible values: 1 to 10 retries<br>Default: 5 retries |

**Table 182: Tunnel Concentrator Address Pool (TCAP) Profile**

| Field | Description |
|---|---|
| Address Pool Profile | Select or create an Address Pool Profile to bind to the Tunnel Concentrator Service.<br>• Select the plus icon (**+**) to open the **Add Address Pool Profile** dialog and create a new pool profile. See Table 183 on page 540.<br>• Select  to open the **Select Address Pool Profile** dialog and choose from previously configured profiles. |
| VLAN ID (required) | Enter the VLAN ID (1–4094) assigned to traffic passing through the address pool. Required unless **Untagged** is selected. |

**Table 182: Tunnel Concentrator Address Pool (TCAP) Profile (continued)**

| Field | Description |
|---|---|
| Untagged | Select this check box if tunneled traffic using this address pool should be transmitted without a VLAN tag. When enabled, the **VLAN ID** field is disabled. |
| Bridge Port (required) | Select the bridge port (for example, **Port 1**) on the Tunnel Concentrator appliance through which traffic for this address pool is routed. |

**Table 183: Address Pool Profile Settings**

| Field | Description |
|---|---|
| Address Pool Profile Name (required) | Enter a unique, descriptive name for the Address Pool Profile (for example, `TCAP-Branch-Pool-1`). |
| Tunnel Concentrator Address Pool Start (required) | Enter the starting IPv4 address of the pool range allocated for tunneled traffic and RADIUS source requests (for example, `192.168.10.100`). |
| Tunnel Concentrator Address Pool End (required) | Enter the ending IPv4 address of the pool range (for example, `192.168.10.200`). |
| Tunnel Concentrator Address Netmask (required) | Enter the subnet mask defining the network boundary for the address pool (for example, `255.255.255.0`). |
| Tunnel Concentrator Address Next Hop (required) | Enter the IPv4 address of the default gateway or next-hop router used to forward traffic originating from the address pool (for example, `192.168.10.1`). |

**Table 184: Broadcast/Multicast Control**

| Field | Description |
|---|---|
| Add New Rule | Select to define a custom broadcast or multicast filtering exception. Enter a target IP address or network range to explicitly permit specific non-unicast traffic through the tunnel for designated network services or applications. |
| Add Pre-defined Rule | Select to apply a pre-configured protocol filter from the menu. Pre-defined rules automatically permit standard network service traffic through the tunnel without requiring manual IP address entries. |

**Table 184: Broadcast/Multicast Control (continued)**

| Field | Description |
|---|---|
| Block Non- Essential Broadcast | Select this check box to drop non-essential broadcast frames before they enter the tunnel. When enabled, the access point suppresses high-volume broadcast traffic while continuing to forward essential protocol packets required for network connectivity, specifically Address Resolution Protocol (ARP) and Dynamic Host Configuration Protocol (DHCP). |
| ARP Proxy | Select this check box to enable local ARP proxying on the access point. When enabled, the AP responds directly to client ARP queries using its local MAC-to-IP binding cache instead of forwarding broadcast ARP requests across the tunnel, significantly reducing tunnel bandwidth consumption and saving wireless airtime.<br><br>**Caution:** Disabling **ARP Proxy** forces all client ARP requests to broadcast across the tunnel link and RF medium, which can lead to broadcast storms, tunnel congestion, and degraded wireless performance. |

## Configure Tunnel Concentrator Address Pool (TCAP) Profiles

An active TCAP pool must be assigned to the Tunnel Concentrator service; otherwise, RADIUS Tunnel Policy configuration will be rejected or fail CLI binding.

When GRE or GRE-over-IPsec tunneling is enabled, the Tunnel Concentrator dynamically assigns an IP address from the TCAP pool to each connected AP. This inner IP address acts as the AP's source address inside the tunnel for carrying tunneled wireless client data and AP-originated control traffic (such as RADIUS authentication requests).

Configuring TCAP profiles ensures reliable IP address management and endpoint identification across both single and redundant Tunnel Concentrator deployments.

Use this task to configure Tunnel Concentrator Address Pool (TCAP) Profiles.

1. Go to **Configuration** > **Network Policies**, select **Menu**, and then go to **Common Objects** > **Network** > **Tunnel Concentrator Address Pool (TCAP) Profile**.
2. Select an existing profile, and then select , or to add a new one, select .

3. Configure the following settings, and then select **Save**.

**Table 185: Address Pool Profile Settings**

| Field | Description |
|---|---|
| Address Pool Profile Name (required) | Enter a unique, descriptive name for the Address Pool Profile (for example, `TCAP-Branch-Pool-1`). |
| Tunnel Concentrator Address Pool Start (required) | Enter the starting IPv4 address of the pool range allocated for tunneled traffic and RADIUS source requests (for example, `192.168.10.100`). |
| Tunnel Concentrator Address Pool End (required) | Enter the ending IPv4 address of the pool range (for example, `192.168.10.200`). |
| Tunnel Concentrator Address Netmask (required) | Enter the subnet mask defining the network boundary for the address pool (for example, `255.255.255.0`). |
| Tunnel Concentrator Address Next Hop (required) | Enter the IPv4 address of the default gateway or next-hop router used to forward traffic originating from the address pool (for example, `192.168.10.1`). |

Related Links

Network Configuration on page 522

## Configure Tunnel Policies

A tunnel policy sets parameters for Layer 3 roaming, identity-based tunnels, standard GRE tunnels, or Layer 2 roaming using Tunnel Concentrator (TC). Extreme Networks devices use dynamic tunnels to support client roaming between subnets and identity-based tunnels to transport user traffic from one part of the network to another. You can add new tunnel policies and view, modify, and remove previously defined policies.

In addition to routing wireless client data traffic, tunnel policies (mobility policies) support forwarding AP-originated RADIUS authentication and accounting control traffic through a standard GRE or GRE-over-IPsec tunnel to a designated TC.

RADIUS control traffic can be decoupled from client data traffic depending on your network design requirements:

- **Local Data with Tunneled RADIUS:** Wireless client data traffic is bridged locally at the AP, while RADIUS authentication traffic is tunneled to the TC for centralized processing against enterprise RADIUS servers behind the TC termination point.

- **Tunneled Data with Tunneled RADIUS:** Both wireless client data traffic and RADIUS authentication traffic are forwarded through the tunnel to the TC.

**Note**

- RADIUS servers assigned to a tunnel policy must be configured using a static IP address. FQDN (hostname) resolution is not supported for RADIUS traffic routed through a tunnel policy.
- An active **Tunnel Concentrator Address Pool (TCAP) Profile** must be assigned to the Tunnel Concentrator service. APs use an IP address allocated from the TCAP range as their source IP address when forwarding RADIUS control traffic inside the tunnel. For more information, see Configure Tunnel Concentrator Address Pool (TCAP) Profiles on page 541.

**Important**

HiveOS access points support either IKEv1 (VGVA / L2 IPsec VPN) or IKEv2 (Tunnel Concentrator IPsec) tunneling, but cannot run both simultaneously. Switching an access point's tunnel destination between VGVA and Tunnel Concentrator automatically triggers a full configuration push and reboots the access point to initialize the new tunnel mode.

You can enable the following types of GRE traffic tunneling:

**Layer 3 Roaming**

Adjusts roaming thresholds so that a device disassociates with a wireless client that has roamed to it from another subnet and has either been idle for a period of time, or for which traffic is below a specified threshold.

**Identity-Based Traffic Tunneling**

Tunnels guest traffic directly to the network.

**Standard GRE Tunneling**

Tunnels traffic to non-Extreme Networks tunnel endpoints.

**Tunnel Concentrator**

Tunnels traffic to Extreme Networks Tunnel Concentrator.

#### Automatic MTU Detection for Tunnel Concentrator Tunnels

ExtremeCloud IQ (New) automatically measures and verifies Maximum Transmission Unit (MTU) sizes for Cloud AP tunnels to a Tunnel Concentrator (TC). When Cloud APs tunnel client traffic to a TC, intermediate network devices along the WAN or LAN path may enforce lower MTU thresholds. If Path MTU Discovery (PMTUD) fails or intermediate devices silently drop fragmented frames, MTU mismatches can lead to packet dropouts or performance degradation.

Extreme Cloud APs continuously evaluate path MTU sizes to the Tunnel Concentrator using the following mechanism:

- Supported Tunnel Modes: MTU detection operates across both unsecure **GRE** tunnels and secure **GRE over IPsec** tunnels.
- Data Plane Probing: MTU discovery uses ICMP-based keep-alive packets exchanged directly between the AP and the TC in the data plane prior to IP packet assembly for accurate real-time measurement.
- Dynamic MTU Verification: Validates both configured MTU limits and dynamically learned path MTU variations.
- Mismatch Reporting: If an MTU mismatch or bottleneck is detected along the path, Extreme Platform ONE Networking flags the mismatch on the device monitoring dashboard and alerts the network administrator.

**Note**
Because MTU detection occurs before IP packet assembly, it provides a reliable validation mechanism without relying on client-initiated ping traffic.

Use the following steps to configure new tunnel policies.

1. Go to **Configuration** > **Network Policies**, select **Menu**, and then go to **Common Objects** > **Network** > **Tunnel Policies**.
2. Select an existing policy, and then select , or to add a new one, select .
3. Type a **Name** for the policy.
4. (Optional) Type a **Description** for the policy.

   Although optional, descriptions can be helpful when you are configuring or troubleshooting your network.
5. Select **Layer 3 Roaming** to adjust Layer 3 roaming thresholds.
   a. Specify a time period between 10 and 600 seconds.
   b. Specify a threshold number between 0 and 2147483647 packets per minute.
6. Select **Identity-based Traffic Tunneling** to configure the tunnel source and destination, and to create a password or tunnel authentication.
   a. For the **Tunnel Source**, select a subnet from the drop-down list, or add a new subnet.

      To add a new IP address or host name, see Configure IP Objects/Host Names on page 501.
   b. For **Tunnel Destination**, choose an IP address or host name from the drop-down list or add a new address or host name.

      To add a new IP Address or Host Name, see Configure IP Objects/Host Names on page 501.
   c. For **Tunnel Authentication**, type the password the AP uses to authenticate to the GRE termination point.
7. Select **Standard GRE Tunneling** to configure non-Extreme Networks tunnel endpoints.
   a. For **Tunnel Destination**, choose an IP address or host name from the drop-down list or add a new address or host name.

      To add a new IP address or host name, see Configure IP Objects/Host Names on page 501.

b. If you select **Tunnel Mode dot1q**, type, select, edit, or add the 802.1Q native VLAN ID.

   To add a VLAN ID, see Configure VLAN Settings on page 362.

c. If you select **Tunnel Mode Access Mode**, type, select, edit, or add the VLAN ID.

   To add a VLAN ID, see Configure VLAN Settings on page 362.

8. Select **Tunnel Concentrator** and then select the **Tunnel Destination** from the drop-down list.

   You can select an existing Tunnel Concentrator service, and then select , or to add a new one, select . For more information, see Configure Tunnel Concentrator Services on page 535.

9. Select **SAVE**.

Related Links

Configure IP Objects/Host Names on page 501
Configure VLAN Settings on page 362
Configure Tunnel Concentrator Services on page 535
Network Configuration on page 522

## Configure Network Services

Network service objects identify Layer 4 traffic by protocol and port number. ExtremeCloud IQ (New) provides some predefined services, and you can create custom network services to use when defining firewall policies, and QoS traffic classification and marking policies.

Use the following task to configure **Network Services** objects:

1. Go to **Configuration** > **Network Policies**, select **Menu**, and then go to **Common Objects** > **Network** > **Network Services**.
2. Select an existing object, and then select , or to add a new one, select .
3. Type a **Name** for the service.
4. Type a **Description** for the service.

   Although optional, descriptions can be helpful when you are configuring or troubleshooting your network.

5. Select a **Service Idle Timeout** (for APs and routers only).

   This is the length of time (in seconds) after which the device terminates inactive sessions using this service.

6. Select an **IP Protocol** number.

   The number of the protocol the service will use. Predefined services appear in the drop-down list, or you can configure a custom protocol. Predefined services use the following protocols:

   - 1 : ICMP (Internet Control Message Protocol)
   - 6: TCP (Transmission Control Protocol)
   - 17: UDP (User Datagram Protocol)
   - 89: OSPF (Open Shortest Path First)
   - 119: SVP (SpectraLink Voice Priority)

7. Specify the destination **Port Number** for the service.

   For services that use TCP or UDP, you must set a destination port number, which the receiving device uses to map the service to a specific processor. When you use a custom protocol, a destination port number is not required because the receiving device can use the protocol to map the service to the appropriate processor.
8. Select an **ALG Type**.

   ALG is supported for APs and routers only. If the service must use an ALG, select DNS, FTP, HTTP, SIP, or TFTP. Otherwise, leave this field empty.
9. Select **SAVE NETWORK SERVICE**.

Related Links

Network Configuration on page 522

## Configure a Subnetwork Space

When you create a subnetwork for branch sites, you can create one large parent subnetwork that ExtremeCloud IQ sections into individual segments for each site, or a smaller subnetwork that each site reuses. You define the subnetwork type—whether it is for internal, guest, or management traffic—and configure options for DHCP, DNS, NTP, and NAT.

1. Go to **Configuration** > **Network Policies**, select **Menu**, and then go to **Common Objects** > **Network** > **Subnetwork Space**.
2. Select an existing object, and then select , or to add a new one, select .
3. Type a **Name** for the object.
4. (Optional) Type a **Description** for the object.

   Although optional, descriptions can be helpful when you are configuring or troubleshooting your network.
5. Choose a **Network Type**:
   - **Internal Use:** Routers can apply internal subnetworks to regular users, such as employees or students. DNS and DHCP services are optional. The addressing for internal subnetworks can be unique among all branch sites so that routers can tunnel traffic through a VPN gateway to a central site and to other branch sites without needing NAT. If you decide to replicate the same subnetwork at each site, then routers will require NAT to send traffic between themselves and a VPN gateway.
   - **Guest Use:** Routers use a subnetwork for guest use for temporary users, such as visitors. DHCP or DHCP relay is required and DNS service is optional. Because guests are not expected to access resources through VPN tunnels at the corporate or other branch sites, the addressing for a guest subnetwork is the same for all routers at all branch sites. Routers do not enable guest traffic to pass through a VPN tunnel to the main site. Guests are only allowed to access the Internet.
   - **Management:** An Extreme Networks router, and Extreme Networks APs and switches at the same branch site communicate with each other. DNS and DHCP services are required.

6. If you choose **Create a unique subnetwork at each site**, configure the following settings:
   - **Local IP Address Space**: Enter the parent IP address scope. The parent scope contains the IP address scopes of all remote sites.
   - **Partition the local IP address space into subnetworks**: Use the slider to select the best match for how many branch offices you need to configure and how many clients there are at each branch. Select the maximum number of foreseeable branches and be sure the number of clients per branch exceeds the maximum foreseeable number of clients at any one branch. If you cannot fit the maximum number of clients and branches within your chosen parent scope, you must increase the parent scope.
   - **Use the first IP address of the partitioned subnetwork for the default gateway**: Select to use the first IP address as your default gateway.
   - **Use the last IP address of the partitioned subnetwork for the default gateway**: Select to use the last IP address as your default gateway.
7. If you choose **Replicate the same subnetwork at each site**, configure the following settings:
   - **Local IP Address Space**: Enter the IP address and netmask of the local subnetwork at each branch site, and select either the first or last IP address as the default gateway, depending upon its configuration.
   - **Use the first IP address of the partitioned subnetwork for the default gateway**: Select this option to use the first IP address as your default gateway.
   - **Use the last IP address of the partitioned subnetwork for the default gateway**: Select this option to use the last IP address as your default gateway.

   **Note**

   If you have any branch sites in your enterprise topology that have overlapping or conflicting IP address schemes, and making changes to those address structures will pose difficulties, you can use NAT on the tunnel interfaces on the routers at each site. The branch routers can then map local subnetworks to different addresses that can be routed through VPN tunnels across your network. With this approach, you can configure the Extreme Networks branch routers, which function as NAT gateways, to map their local subnetwork addresses, one-for-one, to NAT subnetwork addresses. ExtremeCloud IQ maps each host address on the local subnetwork side of the router uniquely to a corresponding network host address on the NAT subnetwork side of the router.

8. Select **SAVE**, or proceed to Configure Subnetwork Space Advanced Settings on page 547.

Related Links

Configure Subnetwork Space Advanced Settings on page 547
Network Configuration on page 522

*Configure Subnetwork Space Advanced Settings*

First, create or modify a subnetwork space. For more information, see Configure a Subnetwork Space on page 546.

Use this task to configure the optional Advanced Settings for a subnetwork space.

1. Select **Advanced Settings**.
2. To enable branch routers to dynamically provide client devices with network settings, select **Enable DHCP**.

   When you select this option, additional configuration items become available.
3. Select one of the following options:
   - To avoid the need for additional hardware at remote sites, select **Enable branch router as DHCP server**, and then go to Step 4 on page 548.
   - To support a centralized DHCP server on a branch router, select **Enable DHCP Relay**, specify the IP address for the **Primary DHCP Server** (and optionally the **Secondary DHCP Server**), and then go to Step 10 on page 549.

     **Note**
     If you have deployed a centralized DHCP server on your network, you must first enable the DHCP relay on an Extreme Networks branch router to disable the DHCP server function for the router. This configuration enables the device to redirect client DHCP requests to a centralized DHCP server. The branch router now behaves as a proxy for client DHCP requests and no longer performs DHCP services. This is part of the DHCP Reservations and DHCP Relay feature.
4. Use the slider controls to select where you want your DHCP address pool to begin and end.

   The left slide control reserves addresses at the start of the pool. The right slide control reserves addresses at the end of the pool. Below the slide control is the total number of remaining unreserved addresses in the pool.

   **Note**
   IP Address 172.28.0.1 is reserved for Extreme Networks routers and is not available to client devices.
5. Specify the DHCP address **Lease Time** in seconds.
6. Specify the **NTP Server IP** that clients use to synchronize their system clocks.
7. Type your network **Domain Name**.
8. To enable Extreme Networks routers to function as DHCP servers and check IP address availability before offering the lease to a DHCP client, select **Use ARP to check IP address conflicts**.

   Clear this option to disable ARP broadcasts during the DHCP message exchange. You might do this if there are a large number of clients requesting DHCP leases and the extra effort to check address availability is unnecessarily consuming resources.
9. For **Custom Options**, select  and specify standard (1 – 224) and custom (225 – 254) DHCP options.

   **Note**
   Options 1, 3, 6, 7, 15, 26, 42, 44, 51, 58, 59, 69, and 70 are not supported here because the information is automatically retrieved elsewhere.

10. Choose the **DNS Service** profile.

    If you do not see a service profile that you want to use, select to create a new one. For more information, see Configure DNS Services on page 499.

    **Note**
    When the network type is for internal or guest use, an Extreme Networks router applies this service to the DNS requests from clients connecting to the router either directly or through an intermediary AP or switch. When the network type is management, the router applies this to DNS requests from Extreme Networks APs and switches on the same management network behind the router, and to the mgt0 interface of the router itself.

11. Select **Enable NAT through the VPN tunnels** to enable routers to perform NAT on traffic traversing their tunnel interfaces.

    **Note**
    If you selected **Replicate the same subnetwork at each site**, NAT is always enabled and this check box cannot be cleared.

    a. Specify the number of branch sites you want to replicate.
    b. Specify the NAT IP address space, which must be large enough to be mapped to the local subnetwork at every branch site of the local subnetwork IP address space.

12. Select **SAVE**.

Related Links

Configure a Subnetwork Space on page 546
Configure DNS Services on page 499

## Configure Firewalls

Use the following procedure to create firewall objects and rules that determine how devices manage traffic based on network or application services, and source and destination IP addresses.

1. Go to **Configuration** > **Network Policies**, select **Menu**, and then go to **Common Objects** > **Network** > **Firewalls**.
2. Select an existing firewall object, and then select , or to add a new one, select .
3. Type a **Name** for the new policy.
4. Type an optional **Description**.
5. Select an existing rule, and then select , or to add a new one, select .
6. Select one or more network or application services.

   **Network Service** objects identify Layer 4 traffic by protocol and port number. Extreme Networks provides a number of predefined services. Select to create a new network service. For more information, see Configure Network Services on page 366.

   a. Choose either **Network Services** or **Application Services**.

      You cannot select both.

b. Select up to 100 items.
c. Select **Add Service**.

7. Select a source IP address, host name, network, or **Any** from the drop-down list, or select **New** to add a new IP address, host name, or network.
8. Select a destination IP address, host name, network, or **Any** from the drop-down list, or select **New** to add a new IP address, host name, or network.
9. Select the action the device performs when it receives traffic matching the source address-destination address-service.
   The firewall can perform the following actions:
   - **Permit**: Allows traffic to traverse the firewall.
   - **Deny**: Blocks traffic from traversing the firewall.
   - **Drop traffic between stations**: Drops traffic between stations if both stations are associated with one or more members of the same hive. This setting applies to unicast, broadcast, and multicast traffic that the device receives on an interface in access mode.
   - **NAT**: Translates the source IP address of a packet permitted to traverse the firewall to that of the mgt0 interface on the device.
10. Choose one of the following logging options from the drop-down list:
    - **Off**: Disables logging for packets and sessions that match the IP firewall policy rule.
    - **Session Initiation**: Log details about a session created after passing an IP firewall policy lookup.
    - **Session Termination**: Log details about a session matching an IP firewall policy termination.
    - **Both**: Log details after initiating and terminating a session.
11. Select **SAVE**.
    As you add rules to a policy, each subsequent rule is positioned at the bottom of the list.
12. Use the up and down arrows in the rules table to rearrange the position of rules to determine the order of application.
13. Select **SAVE**.

Related Links

Configure Network Services on page 366
Network Configuration on page 522

## Configure VPN Services

Use this task to configure a new VPN service object for Layer 3 VPN tunneling. Layer 3 VPN tunnels are for use connecting XR routers to a VGVA or another IQ Engine device acting as a tunnel head-end.

1. Go to **Configuration** > **Network Policies**, select **Menu**, and then go to **Common Objects** > **Network** > **VPN Services**.
2. Configure the settings.
3. To create client credentials for servers and clients, expand **Server-Client Credentials** and select **GENERATE**.
   For more information, see Server-Client Credentials on page 530.

4. For the remaining optional settings see:
   - Configure IPsec VPN Authority Settings on page 528 (Extreme Networks VPN Gateway only)
   - Configure Advanced Server Options on page 530
   - Configure Advanced Client Options on page 530
5. Select **SAVE**.

Related Links

VPN Services Settings on page 551
Configure IPsec VPN Authority Settings on page 528
Server-Client Credentials on page 530
Configure Advanced Server Options on page 530
Configure Advanced Client Options on page 530
Network Configuration on page 522

*VPN Services Settings*

| Setting | Description |
|---|---|
| Name | Type a **Name** for the new VPN service. |
| Description | (Optional)<br>Type a **Description** for the new VPN service. Although optional, descriptions can be helpful when you are configuring or troubleshooting your network. |
| Extreme Networks VPN Gateway | Select this option to configure settings for a VPN using an Extreme Networks device. |
| Third Party Gateway | Select this option to configure settings for a VPN a using third-party (such as, Cisco) device. |
| **Extreme Networks VPN Gateway** | |
| Number of branches to be created | Type the number of branch sites that you expect to build tunnels to the VPN gateway. |
| Max tunnels per gateway | Type the maximum number of tunnels per gateway. |
| VPN Tunnel Addressing | Select **Auto (assigned from management subnetwork)** or **Use WAN interface IP addresses** to use specific IP addresses. |
| VPN Gateway Settings | Select , and then **Select** a VPN Gateway from the list.<br>The VPN Gateway Virtual Appliances (VGVA) that appear in this list are added to the network as Layer 3 VPN gateways. To change the settings for a VGVA, go to **Manage** > **Devices**. |
| **Third Party Gateway** | |
| VPN Tunnel Addressing | Select **Auto (assigned from management subnetwork)** or **Use WAN interface IP addresses** to use specific IP addresses. |
| Select Vendor | Select the vendor name from the list. |

| Setting | Description |
|---|---|
| External IP Address | Type the IP address of the third-party VPN gateway. |
| VPN Access List | Select and type the required **Source Network** and **Destination Network** in the respective fields. |

# Authentication Configuration

The topics in this section provide details about configuration objects for authentication methods, such as AAA servers, captive web portals, and external RADIUS servers, Extreme Networks A3, and LDAP servers.

Related Links

Clone AAA Server Settings on page 552
Configure Captive Web Portals on page 552
Configure External RADIUS Servers on page 554

## Clone AAA Server Settings

First, create an AAA Server Profile as part of a network policy. For more information, see Configure an AAA Server Profile on page 355.

ExtremeCloud IQ (New) stores settings for AAA Servers as an **AAA Server Profile** object.

Use this task to create a copy of an existing **AAA Server Profile** object.

1. Go to **Configuration** > **Network Policies**, select **Menu**, and then go to **Common Objects** > **Authentication** > **AAA Server Settings**.
2. Select a server profile from the table.
3. To create a copy, select an existing object and then select .
4. Type a name for the new object in the **Save As** field, and then select **CLONE**.

Related Links

Configure an AAA Server Profile on page 355
Authentication Configuration on page 552

## Configure Captive Web Portals

In the network policy, enable the Captive Web Portal feature for the SSID.

Use this task to configure a CWP object. For more information, see Captive Web Portals on page 328.

1. Go to **Configuration** > **Network Policies**, select **Menu**, and then go to **Common Objects** > **Authentication** > **Captive Web Portals**.
2. Select an existing CWP object, and then select , or to add a new one, select .
3. Type a **Name** for the CWP object.

4. On the **CUSTOMIZE AND PREVIEW** tab, configure the following settings:
   - Captive Web Portal Settings on page 553
   - **Supported Languages**

     Select the **Default Language** and specify additional languages to support.

     When you save the CWP, ExtremeCloud IQ (New) adds the files required for the selected languages to the default CWP directory.
   - Advanced Configuration Settings on page 334
   - Walled Garden Settings on page 337

   Alternatively, select the **IMPORT HTML** tab, and see .
5. Select **SAVE CWP**.

Related Links

Captive Web Portals on page 328
Captive Web Portal Settings on page 553

*Captive Web Portal Settings*

Configure the following settings for Captive Web Portals.

**Table 186: Settings for Captive Web Portals**

| Setting | Description |
|---|---|
| CUSTOMIZATION AND PREVIEW | Select to preview the Landing, Success, and Failure (Error) pages. Select the corresponding tab for each page, and then select **CUSTOMIZE** to make changes. |
| Authentication Method | Select PAP, CHAP, or MS-CHAP V2. |
| Success Page | To show the **Success** page after a successful login attempt. To preview the **Success** page, select **CUSTOMIZATION AND PREVIEW**. To make changes, select **CUSTOMIZE**.<br>To redirect clients after a successful login attempt, select the check box. |
| Failure Page | To show the **Failure** page after an unsuccessful login attempt, enable this option.<br>Choose **Use login page to display the failure message** or **Standard failure page**.<br>To preview the standard **Failure** page, select **CUSTOMIZATION AND PREVIEW**. To make changes, select **CUSTOMIZE**.<br>To redirect clients after a successful login attempt, select the check box. |

Related Links

Configure Captive Web Portals on page 552

## Configure External RADIUS Servers

Use this task to configure External RADIUS Server objects.

1. Go to **Configuration** > **Network Policies**, select **Menu**, and then go to **Common Objects** > **Authentication** > **External RADIUS Servers**.
2. Select an External RADIUS Server object, and then select , or to add a new one, select .
3. Configure the settings.

Related Links

External RADIUS Server Settings on page 353

# Certificate Configuration

The topics in this section provide details about certificate objects, including how to create certificates and keys, and how to import them.

Related Links

Certificate Management on page 554
Create a Certificate Bundle on page 560

## Certificate Management

To support secure wireless client traffic and captive web portal configurations using HTTPS, ExtremeCloud IQ (New) supports the following **Certificate Management** options:

**ExtremeCloud IQ CA**

Select to generate your own Certificate Authority (CA) certificate. See Create a ExtremeCloud IQ (New) Certificate of Authority on page 555.

**Server CSR**

Select to generate a certificate that consists of three parts used during the verification process. The first part describes the content of the certificate. The second part contains the server public key. The third part consists of the same fields hashed with the server message digest, or public key, and then encrypted with the issuing CA digital signature (for example, the **ExtremeCloud IQ CA**) private key. See Create a CSR for a Server on page 556.

**Concatenate an existing certificate and private key**

Select this option when working with captive web portals. One option in a captive web portal configuration is to secure wireless client traffic using HTTPS. The type of web server that an Extreme Networks device supports requires the server certificate be concatenated with an unencrypted private key that corresponds with the certificate's public key. You can concatenate an existing server certificate and private key or generate a new self-signed server certificate that already has the private key and certificate concatenated. See Concatenate an Existing Certificate and Private Key on page 558.

**Self-signed certificate**

Select to generate a new self-signed server certificate that already has the private key and certificate concatenated. See Create a Self-Signed Certificate on page 558.

You can import files, and also edit, export, or delete existing **Certificate Management** objects.

Related Links

Create a ExtremeCloud IQ (New) Certificate of Authority on page 555
Create a CSR for a Server on page 556
Concatenate an Existing Certificate and Private Key on page 558
Create a Self-Signed Certificate on page 558
Import a Certificate or Key on page 559
Export a Certificate or Key on page 560

*Create a ExtremeCloud IQ (New) Certificate of Authority*

Before generating a certificate, make sure the time and date on the ExtremeCloud IQ (New) clock are accurate. Otherwise, the certificate might be rejected during validation because the starting date has not occurred or the expiration date has passed.

Use this task to generate your own Certificate Authority (CA).

1. Go to **Configuration** > **Network Policies**, select **Menu**, and then go to **Certificate** > **Certificate Management**.
2. Select an existing certificate or key file, and then select , or to add a new one, select .

   **Note**
   You can only change the **Certificate Name** and **Description** for certificate or key files. For example, if you give a certificate or key file a name and description based on the location of the device, and then you have to move it, you can easily modify these attributes for your own reference.
   You cannot edit a default certificate or key file.

3. On the **Create Certificate/Key** page, select **ExtremeCloud IQ CA**.
4. Type **Common Name** for the ExtremeCloud IQ (New) instance that you will use to sign server certificates.

   The name you assign is used to verify the server certificates when they are used to authenticate participants in AAA exchanges.

   Example: Extreme NetworksCA
5. Type the **Organization Name**.

   Example: Extreme Networks
6. Type the **Organization Unit**.

   Examples: Marketing, Engineering, Sales
7. Type the **Locality Name**.

   The locality is the town, county, or city.
8. Type the **State/Province Name**.
9. Type the two-character **Country Code**.
10. (Optional) Provide a contact email address.
11. Specify the number of days the CA will be valid.

    A CA is typically valid for a much longer period than the server certificates it signs.

12. (Optional) Choose a key size for the key pair: 512, 1024, or 2048 bytes.

    The encryption produced by the smallest key size (512 bytes) can be cracked with relatively common tools and is not generally recommended. However, it might be needed if the devices on which the CA must be loaded do not support larger key sizes. Keys of 1024 or 2048 bytes provide far stronger encryption, but require greater processing power.
13. Type the corresponding **Password** for encrypting and decrypting the private key linked to the public key in the CA.

    To see the password as you type, select **Show Password**.
14. Select **SAVE**.

    ExtremeCloud IQ (New) saves the CA with the file name `Default_CA.pem` and the accompanying private key as `Default_key.pem`.

Related Links

Certificate Management on page 554

*Create a CSR for a Server*

Before generating a certificate, ensure that the time and date on the ExtremeCloud IQ (New) clock are accurate. Otherwise, the certificate might be rejected during validation because the starting date has not occurred or the expiration date has passed.

Use this task to create a Certificate Signing Request (CSR).

1. Go to **Configuration** > **Network Policies**, select **Menu**, and then go to **Common Objects** > **Certificate** > **Certificate Management**.
2. Select an existing certificate or key file, and then select , or to add a new one, select .

   **Note**
   Although you cannot change the certificate and private key in a concatenated file, you can modify the **Certificate Name** and **Description**. For example, if you give a certificate file a name and description based on the location of the device, and then you have to move it, you can easily modify these attributes for your own reference.
3. On the **Create Certificate/Key** page, select **Server CSR**.
4. Type **Common Name** for the ExtremeCloud IQ (New) instance that you will use to sign server certificates.

   The name you assign is used to verify the server certificates when they are used to authenticate participants in AAA exchanges.

   Example: Extreme NetworksCA
5. Type the **Organization Name**.

   Example:Extreme Networks
6. Type the Type the **Organization Unit**.

   Examples: Marketing, Engineering, Sales
7. Type the **Locality Name**.

   The locality is the town, county, or city.

8. Type the **State/Province Name**.
9. Type the two-character **Country Code**.
10. (Optional) Provide a contact email address.
11. (Optional) Provide a **Subject Alternative Name**.
    When using the server certificate to verify a VPN server, the VPN client that receives the certificate during IKE (Internet Key Exchange) negotiations uses the SAN ( subject alternative names) in that certificate to perform two validity checks for the server: The VPN client checks that the SAN which the VPN server presents as its IKE ID matches the SAN in the certificate that the server supplies, and the VPN client verifies that the IKE ID it receives from the VPN server matches the peer IKE ID in its configuration. Fill in the associated fields as follows:
    - **User FQDN**: Type a text string in the form of a fully-qualified domain name for an individual. It resembles an email address: **<string>@<domain>**. For example, `jhan@extremenetworks.com`.
    - **FQDN**: Type a text string in the form of a fully-qualified domain name, such as `portal.extremenetworks.com`.
    - **IP Address**: Type an IP address in dotted decimal notation, for example, `10.1.1.1`.
12. (Optional) Choose a key size for the key pair: 512, 1024, or 2048 bytes.
    The encryption produced by the smallest key size (512 bytes) can be cracked with relatively common tools and is not generally recommended. However, it might be needed if the devices on which the CA certificate must be loaded do not support larger key sizes. Keys of 1024 or 2048 bytes provide far stronger encryption, but require greater processing power.
13. (Optional) Type the corresponding password for encrypting and decrypting the private key linked to the public key in the CA.
    To see the password as you type, select **Show Password**.
14. Type a **CSR File Name** to identify the CSR file.
15. Select a **Generate Method** as follows:
    - To send the CSR to a third-party CA to generate a server certificate, select **Export** and **OK**, save the CSR file to your management system, and then send it to the CA.
    - To generate a server certificate using ExtremeCloud IQ (New) as a CA, select **Sign by ExtremeCloud IQ CA**, enter a valid time period, clear or select **Combine key and certificate into one file** as explained below, and then select **OK**:
      - Clear **Combine key and certificate into one file** to create two separate files—one with the certificate and another with the private key. Extreme Networks RADIUS servers use these two files to authenticate themselves to RADIUS supplicants using PEAP (Protected Extensible Authentication Protocol), TTLS (Tunneled Transport Layer Security), or TLS (Transport Layer Security).
      - Select **Combine key and certificate into one file** to create a single file that combines the certificate and private key. This simplifies the organization of server certificates and their related private keys so that they cannot accidentally become mismatched. You can use the concatenated server certificate/private key file to provide authentication between RADIUS authentication servers and their supplicants.
16. Select **SAVE**.
    ExtremeCloud IQ (New) saves the CA certificate with the file name `Default_CA.pem` and the accompanying private key as `Default_key.pem`.

Related Links

Certificate Management on page 554

*Concatenate an Existing Certificate and Private Key*

Before generating a certificate, make sure the time and date on the ExtremeCloud IQ (New) clock are accurate. Otherwise, the certificate might be rejected during validation because the starting date has not occurred or the expiration date has passed.

Use this task to create a new file containing a concatenation of a server certificate and an unencrypted private key.

1. Go to **Configuration** > **Network Policies**, select **Menu**, and then go to **Certificate** > **Certificate Management**.
2. Select an existing certificate or key file, and then select , or to add a new one, select .

   **Note**
   Although you cannot change the certificate and private key in a concatenated file, you can modify the **Certificate Name** and **Description**. For example, if you give a certificate file a name and description based on the location of the device, and then you have to move it, you can easily modify these attributes for your own reference.
   You cannot edit a default certificate or key file.

3. On the **Create Certificate/Key** page, select **Concatenate an existing certificate and private key**.
4. Type a **HTTPS Certificate/Key Name**.
5. (Optional) Type a **Description** to help identify the file.
6. Select the **Certificate** you want to use.
   You can also select **IMPORT** to import a certificate. See Import a Certificate or Key on page 559.
7. Select the **Private Key**.
   You can also select **IMPORT** to import a key. See Import a Certificate or Key on page 559.
8. Type the corresponding password for encrypting and decrypting the private key linked to the public key in the CA.
9. Select **SAVE**.

Related Links

Import a Certificate or Key on page 559
Certificate Management on page 554

*Create a Self-Signed Certificate*

Before generating a certificate, ensure that the time and date on the ExtremeCloud IQ clock are accurate. Otherwise, the certificate might be rejected during validation because the starting date has not occurred or the expiration date has passed.

Use this task to create a self-signed certificate.

1. Go to **Configuration** > **Network Policies**, select **Menu**, and then go to **Certificate** > **Certificate Management**.

2. Select an existing certificate or key file, and then select , or to add a new one, select .

   **Note**
   You can only change the **Certificate Name** and **Description** for certificate or key files. For example, if you give a certificate or key file a name and description based on the location of the device, and then you have to move it, you can easily modify these attributes for your own reference.
   You cannot edit a default certificate or key file.

3. On the **Create Certificate/Key** page, select **Self-signed certificate**.
4. Type a **HTTPS Certificate/Key Name**.
5. For **Common Name**, type a descriptive name to identify the organization and the purpose of the CA.

   Example: Extreme Networks Client CA
6. Type the **Organization Name**.

   Example: Extreme Networks
7. Type the **Organization Unit**.

   Examples: Marketing, Engineering, Sales
8. Type the **Locality Name**.

   The locality is the town, county, or city.
9. Type the **State/Province Name**.
10. Type the two-character **Country Code**.
11. (Optional) Provide a contact email address.
12. Specify the number of days the CA will be valid.

    A CA is typically valid for a much longer period than the server certificates it signs.
13. (Optional) Choose the key size for the key pair: 512, 1024, or 2048 bytes.

    The encryption produced by the smallest key size (512 bytes) can be cracked with relatively common tools and is not generally recommended. However, it might be needed if the devices on which the CA certificate must be loaded do not support larger key sizes. Keys of 1024 or 2048 bytes provide far stronger encryption, but require greater processing power.
14. Select **SAVE**.

Related Links

Certificate Management on page 554

*Import a Certificate or Key*

If you use a third-party CA to sign certificates, generate and export a CSR, send it to the CA, and when the CA returns the signed certificate and private key file, import the certificate into ExtremeCloud IQ (New). Extreme Networks devices support PEM-formatted certificates.

Use this task to import a certificate or key file.

1. **Common Objects** > **Certificate** > **Certificate Management**.
2. Select .
3. Use **Select** to navigate to the location of the certificate file.

4. Select **Open**.
5. Select **Import**.
6. Select whether this file is a certificate or key.

   To import certificates in PFX or DER formats, you must first use the conversion tool to reformat them as PEM files.
7. To import a PFX-formatted file, which contains a certificate and private key combined, first convert its format from PFX to PEM:
   a. Select **Convert the certificate format from PFX to PEM**.
   b. Type the password that was used to encrypt the PFX file.

   **Note**
   When you use the PEM-formatted file that contains both the certificate and private key, you must choose the same file for both the Certificate and Private Key fields.
8. To import a pair of DER-formatted files, one containing a certificate and the other its accompanying private key, first convert their format from DER to PEM:
   a. Select **Convert the certificate format from DER to PEM**.
   b. If converting a key, enter the password that was used to encrypt the file.
9. Select **SAVE**.

Related Links

Certificate Management on page 554

*Export a Certificate or Key*

Use this task to export a certificate or key file.

1. **Common Objects** > **Certificate** > **Certificate Management**.
2. Select the certificate or key.
3. Select .

   Check the download folder for your browser.

Related Links

Certificate Management on page 554

## Create a Certificate Bundle

Import the CA, CERT, and KEY files. See Import a Certificate or Key on page 559.
Use this task to create a new certificate bundle.

1. Go to **Configuration** > **Network Policies**, select **Menu**, and then go to **Certificate** > **Certificate Bundle**.
2. Select an existing certificate bundle, and then select , or to add a new one, select .

3. Configure the settings.

**Table 187: Certificate bundle settings**

| Setting | Description |
|---|---|
| Name | Type a name to identify the certificate bundle. |
| CA Certificate File | Select the CA certificate file. |
| Server Certificate File | Select the CERT file for the server. |
| Verify Server Certificate File | Select to verify the authenticity and validity of the digital certificate of the server. |
| Server Key File | Select the KEY file for the server. |

4. Select **SAVE**.

Related Links

Import a Certificate or Key on page 559

## Clone a Common Object

To save time, you can clone a common object and then edit it without affecting the original object. This feature is not available for all objects. If the icon is not present on the landing page for the selected object, cloning is not supported.

Use this task to clone supported common objects.

1. Go to **Configuration** > **Network Policies**, select **Menu**, and then go to **Common Objects**.
2. Expand a category, and then select the common object type.

   **Example: Authentication** > **Captive Web Portals**
3. On the landing page for the object type, select .
4. Type a new name in the **Save As** field, and then select **CLONE**.

Related Links

Configuration | Common Objects on page 465

## Delete a Common Object

1. Go to **Configuration** > **Network Policies**, select **Menu**, and then go to **Common Objects**.
2. Expand a category, and then select the common object type.

   **Example: Authentication** > **Captive Web Portals**
3. On the landing page for the object type, select the object and then select .

Related Links

Configuration | Common Objects on page 465

# Configuration | User Management

Add a User on page 563
Bulk Create Users on page 564
Add a User Group on page 565
Add a User to a User Group on page 566
Bulk Add Users to a User Group on page 566
Configure a Private Client Group on page 566
Unlock Users on page 567
Perform a RADIUS Test on page 568
Unbind a Device on page 568
Guest User Accounts on page 569

**Note**
The topics in this chapter apply to wireless network user management. For information about Extreme Cloud IQ (NEW) user management, see Administration & Settings | Access Management on page 576.

Create user groups for a selected network policy or all network policies. Add users and assign them to existing user groups, or add users when you create a user group. User groups define password settings such as, type, complexity, database location, and expiration settings.

**Note**
For existing user groups, settings related to passwords are unavailable for editing. To modify these settings, you must create a new user group.

Assign a user group to a specific SSID to control access and network policy for users. Associate a user group with a user profile to define network access parameters, including VLAN assignment, firewall policies, QoS, and traffic tunneling.

Related Links

Add a User Profile on page 315

# Add a User

**Note**
You must first create the user group to which you want to assign the user. You cannot edit the user group for an existing user.

Use this task to add a new user and assign an existing user group.

1. Go to **Configuration** > **Network Policies**.
2. On the **Network Configuration / Network Policies** page, select , and then go to **User Management** > **Users**.
3. Select and then configure the user settings.
4. Select **SAVE**.

Related Links

User Settings on page 563

## User Settings

**Table 188: Settings for new user accounts**

| Setting | Description |
|---|---|
| Create account in user group | (Required)<br>Select a user group from the menu. |
| Name | Type the name of the user.<br>This name appears in messages sent to the email address in the **Deliver Password** section. The email message, which contains login credentials and wireless connection instructions, begins with **`Welcome <this_name>`**.<br><br>**Note:** Required only if you select **Name** from the **User Name** menu. |
| Organization | Type the name of the organization for the user.<br>For permanent users, leave this field empty. |
| Purpose of Visit | Type the purpose of the user's visit.<br>For permanent users, leave this field empty. |
| Email Address | Type the user's email address.<br><br>**Note:**<br>Required only if you select **Name** from the **User Name** menu. |
| Phone Number | Type the user's phone number, and use the menu to set the international dialing code.<br><br>**Note:**<br>Required only if you select **Phone Number** from the **User Name** menu. |

**Table 188: Settings for new user accounts (continued)**

| Setting | Description |
|---|---|
| User Name | From the menu, select a field to use as the **User Name**. Choose from the following options:<br>• **Name**<br>• **Email Address**<br>• **Phone Number**<br>• **Other**<br>If you select **Other**, type a user name for the account. Example: jsmith |
| Password | (Required)<br>Type a password, or select **Generate** to automatically generate a password for the user. To see the password, select **Show Password**.<br>**Note:**<br>For either method, the password must conform to the password rules configured for the associated user group. |
| Description | (Optional)<br>Type a description for the user account. |
| Deliver Password | Select a password delivery method:<br>• **Email Address**<br>Type the email address for the user in the corresponding field. The auto-populates if you already entered an email address. This option is available only if you previously selected **Email** in the **Delivery Settings** section of the user group configuration.<br>• **Text Message**<br>Type the cell phone number for the user in the corresponding field. This option is available only if you previously selected **Text Messages (SMS)** in the **Delivery Settings** section of the user group configuration. |

Related Links

Add a User on page 563

## Bulk Create Users

You must first create the user group to which you want to assign the users.

Use this task to bulk-create and add users to an existing user group.

1. Go to **Configuration** > **Network Policies**.
2. On the **Network Configuration / Network Policies** page, select , and then go to **User Management** > **Users**.
3. Select **Bulk Create** and configure the settings.
   See Bulk Create Settings on page 565.

4. Select **SAVE**.

Related Links

Bulk Create Settings on page 565
Add a User Group on page 565

## Bulk Create Settings

**Table 189: Settings for the bulk creation of users**

| Setting | Description |
|---|---|
| Create account in user group | Select a user group from the menu. |
| Username Prefix | Type a prefix for the user names. Bulk-created user names include this prefix for each user name, starting with 1.<br>For instance, if the user name prefix is 1250, the first bulk-created user is 12501, the second user is 12502, and so on. |
| Number of Accounts | Type the number of users to add. Range: 1–1000 |
| Email User Account info to | Type the email address to which you want ExtremeCloud IQ (New) to send the user credentials. |

Related Links

Bulk Create Users on page 564
Bulk Add Users to a User Group on page 566

## Add a User Group

ExtremeCloud IQ (New) supports user groups for Private Pre-Shared Key (PPSK) users and RADIUS users. Administrators and NetSecOps can configure ExtremeCloud IQ (New) user groups with limited access privileges for VIPs and non-employees such as guests, visitors, and contractors who request network access.

Create user groups before you add users. You can add new users to existing user groups, or add new users when you create user groups.

Use this task to create a user group.

1. Go to **Configuration** > **Network Policies**.
2. On the **Network Configuration / Network Policies** page, select , and then go to **User Management** > **User Groups**.
3. Select , and then configure the settings.

   For a cloud-based user group, see Cloud User Group Settings on page 311.

   For a local user group, see Local User Group Settings on page 312.
4. Select **SAVE**.

Related Links

Cloud User Group Settings on page 311

Local User Group Settings on page 312

## Add a User to a User Group

You must first create the user group to which you want to assign the users.

Use this task to add a single user by editing an existing user group.

1. Go to **Configuration** > **Network Policies**.
2. On the **Network Configuration / Network Policies** page, select , and then go to **User Management** > **User Groups**.
3. Select an existing user group, and then select , or to add a new one, select ..
4. Expand the **Add Users** section.
5. Select and then configure the settings.

   See User Settings on page 563.
6. Select **DONE**.

Related Links

User Settings on page 563

## Bulk Add Users to a User Group

You must first create the user group to which you want to assign the users.

Use this task to bulk-add users to an existing user group, or while creating a new user group.

1. Go to **Configuration** > **Network Policies**.
2. On the **Network Configuration / Network Policies** page, select , and then go to **User Management** > **User Groups**.
3. Expand the **Add Users** section.
4. Select **Bulk Create** and configure the settings.

   See Bulk Create Settings on page 565.

   ExtremeCloud IQ (New) saves your changes, creates the requested user accounts, and emails the bulk-created login credentials to the email addresses in the CSV file. The CSV file contains the SSID, user ID, user name, user group, access key, and expiration date for each bulk-created user.
5. Select **DONE**.

Related Links

Bulk Create Settings on page 565

## Configure a Private Client Group

Create a Private Pre-shared Key (PPSK) standard wireless network. Enable **Private Client Group Options** and configure the settings. See Configure Private Pre-Shared Key SSID Authentication on page 326.

After you enable Private Client Groups (PCGs), you can designate them as using one of two main operating modes:

- **AP-based** PCG uses unique user and shared keys. This mode supports common shared devices within personal network spaces. It also requires room assignments for AP anchoring and traffic tunneling.
- **Key-based** PCG requires one password used by the entire device group. Key-based PCG does not need room assignments, and no traffic tunneling is used on anchor-based APs.

**Note**
Each network policy can have only one AP-based PCG wireless network (SSID), one key-based PCG SSID, and any number of non-PCG SSIDs.

Use this task to configure a private client group for a PPSK standard wireless network.

1. Go to **Configuration** > **Network Policies**.
2. On the **Network Configuration / Network Policies** page, select , and then go to **User Management** > **Private Client Groups**.
3. Select a **Network Policy** from the menu.
4. Select **AP-Based Groups** or **Key-Based Groups** and configure the settings.
   a. Toggle the corresponding setting **ON** to enable the feature.
      - **Enable AP-Based Groups**
      - **Enable Key-Based Groups**
   b. (Optional) For AP-based groups, select **Distribute Shared Keys**.
5. Select to add rooms for AP-based groups, or users for key-based groups.
6. Type a name for an AP-based group and then select users from the menus, or for key-based groups select a user from the menu.
   Alternatively, for key-based groups, you can bulk add users by selecting **IMPORT** and uploading a CSV file.
7. Repeat steps 5–6 until you finish adding groups or users.
8. Select **SAVE CHANGES**.

Related Links

Configure Private Pre-Shared Key SSID Authentication on page 326

## Unlock Users

ExtremeCloud IQ (New) authenticates PPSK clients against a large list of passwords. Users that repeatedly submit incorrect, deleted, or expired passwords can trigger a DoS attack. To prevent this, ExtremeCloud IQ temporarily puts the MAC address of a client device that repeatedly fails authentication 10 times in 7 minutes (default settings) into a sandbox and blocks future attempts for 30 minutes. For all authentication attempts, ExtremeCloud IQ first checks the client MAC address against the list of locked users in the sandbox.

Use this procedure to unlock users.

1. Go to **Configuration** > **Network Policies**.
2. On the **Network Configuration / Network Policies** page, select , and then go to **User Management** > **Locked Users**.

3. Select entries in the locked users list.
4. Select **Unlock**.

## Perform a RADIUS Test

The RADIUS Test tool tests network connectivity between a device acting as a RADIUS authenticator (RADIUS client) and RADIUS authentication server, which can be an Extreme Networks RADIUS server, or an external RADIUS authentication or accounting server.

Use this task to test the connectivity between a RADIUS authenticator and a RADIUS server.

1. Go to **Configuration** > **Network Policies**.
2. On the **Network Configuration / Network Policies** page, select , and then go to **User Management** > **RADIUS Test**.
3. Select the type of RADIUS server that you want to test.
   - To test connectivity to an Extreme Networks RADIUS server, choose **Select a Server (local RADIUS)**, and then select a RADIUS server from the drop-down list.
   - To test connectivity to an external RADIUS authentication or accounting server, select **Enter a Server (external RADIUS)**, and enter the IP address of the server in the field.
4. Select a managed device that is acting as a RADIUS authenticator (client) from the drop-down list.

   This is the device from which the **RADIUS Access-Request** or **Accounting-Request** message is sent.
5. Select either **RADIUS Authentication Server** or **RADIUS Accounting Server**.

   If you select an authentication server, you must also enter supplicant credentials (a user name or barcode, and a password or PIN) for a valid user account on the RADIUS authentication server. You can also enter a user name and password that do not match an account on the RADIUS server.
6. Select **Test**.

ExtremeCloud IQ (New) displays the results on the page, under **Test Result**. The following example shows a successful test result.

```
RADIUS server is reachable. Get attributes from RADIUS server: User-
Group-ID:0=13; VLAN-ID:1=1; Session-Timeout=1800
```

## Unbind a Device

Use this task to unbind a locally-based PPSK from a client device to free up that key or device. You can unbind the client MAC address, the PPSK, or both.

1. Go to **Configuration** > **Network Policies**.
2. On the **Network Configuration / Network Policies** page, select , and then go to **Configure** > **User Management** > **Unbind Device**.
3. Select the method for unbinding from the drop-down list.

   Choose **MAC address**, **PPSK**, or **MAC address and PPSK**.
4. Enter the MAC address, the PPSK, or both.
5. Select **Unbind**.

# Guest User Accounts

Guest user accounts are temporary, low-privilege accounts that permit individuals to access a system or network without a personalized login. Commonly used in public environments such as libraries and hotels, or in enterprise guest Wi-Fi networks, guest user accounts protect the integrity of the host network and data by limiting access to resources.

Extreme Platform ONE Networking supports Private Pre-Shared Key (PPSK), and captive web portal.

## PPSK

With PPSK, each guest device receives a unique passphrase for connecting to a shared SSID. Administrators can assign different access policies, set expiration dates, and revoke access for individual users or devices without affecting others. PPSK is ideal for environments like hotels, airports, or enterprises where guests need secure, temporary access.

For more information, see Configure PPSK Guest User Accounts on page 570.

## Captive Web Portal

A captive web portal can function independently of PPSK, and is a good choice when security requirements are moderate and the priority is ease of use and broad accessibility. Guests connect to an open SSID and are redirected to a web-based login page (splash page), where they authenticate using methods such as:

- Email registration
- Social media login

A captive web portal provides the following benefits:

- No need to manage individual keys (PPSK) or passwords, ideal for high-traffic, short-term guest access, such as cafes, or stores. Guests accept an Acceptable Use Policy (AUP) or register by email or SMS without a unique password.
- Support for more devices, including legacy or IoT devices that might not support complex authentication.
- The network is open but isolated, with the captive web portal enforcing terms and enabling basic tracking or analytics.

For more information, see Customize and Preview Cloud-based Captive Portal Settings on page 338.

## Captive Web Portal and PPSK

Extreme Platform ONE Networking supports captive web portal and PPSK together, with the captive web portal providing user-friendly onboarding, and PPSK providing per-user authentication, tracking, and security for the network. To implement a captive web portal and PPSK, you require two SSIDs:

- An SSID with Enterprise 802.1X access security for secure Wi-Fi access
- An open SSID with a device-based captive web portal for guest registration

After registering on the captive web portal, guests receive a PPSK that they use to connect to the secure Enterprise 802.1X SSID.

For more information, see Customize and Preview Device-based Captive Web Portal Settings on page 331.

## Configure PPSK Guest User Accounts

This topic provides an overview of the tasks required to set up PPSK guest user accounts.

The initial configuration for the creation of PPSK guest user accounts is part of the SSID configuration workflow. You can add guest user accounts when you create the SSID, but from an ongoing perspective, adding guest user accounts is not part of the SSID configuration workflow.

**Table 190: Workflow: Configure PPSK guest use accounts**

| | Task | Purpose |
|---|---|---|
| **Initial configuration** | | |
| 1 | Configure Private Pre-Shared Key SSID Authentication on page 326 | Create the PPSK SSID. |
| 2 | Configure cloud user groups for the SSID. See Cloud User Group Settings on page 311 and Local User Group Settings on page 312 | Create user groups for the SSID. You can add users to the groups at this time, or later. |
| 3 | Add a User Profile on page 315 | Create user profiles (default user profile or secondary user profile) to support the user groups for guest accounts. |
| 4 | Deploy a Network Policy on page 307 | Push the new SSID to the devices. |
| **Ongoing account creation** | | |
| 5 | Administrator or Operator Role: Add a User to a User Group on page 566<br>Alternatively, you can set up a script to add users to an existing user group by using the API. | Add new guest users to an existing user group, for a PPSK SSID. |

# Task Center

Manage Tasks in the Task Center on page 571
View Task Details and Run History on page 574

The **Task Center** is a centralized dashboard in Extreme Cloud IQ (NEW) where you can view historical, active, and scheduled tasks across your network infrastructure. The **Task Center** provides unified visibility into firmware upgrades, and backup and restore operations. The **Task Center** consolidates task management and monitoring in one location, allowing you to:

- Monitor in-progress tasks with real-time status and progress
- View completed tasks and their outcomes across all devices
- Review scheduled tasks and their recurrence patterns
- Search and filter tasks by multiple criteria
- Use task details to view device-level results and run history
- Access downloadable logs and error details for troubleshooting

## Manage Tasks in the Task Center

The **Task Center** page contains the following tabs:

- **All Tasks:** Displays all tasks.
- **Upgrade Firmware:** Displays only firmware upgrade tasks.
- **Backup & Restore:** Displays only backup and restore tasks.

The tasks on each tab can be filtered further by selecting one of the following tabs:

- **All:** All tasks within ExtremeCloud IQ (New).
- **Running:** Tasks that are currently running.
- **Scheduled:** Tasks that are scheduled to run.
- **Paused:** Tasks that have been paused.
- **History:** Tasks that have been run in the past.
- **Recurring:** Tasks that run on a regular basis.
- **Ad Hoc:** Tasks that have been run on-demand.

## Task Details

By default, the **Task Center** tabs display information about all tasks that fit the criteria. You can view and filter task details using the following methods:

- Use the **Time Range** controls to specify a time range for which you want to view tasks. Select a predefined range (Last 7 days, Last 30 days, Last 90 days) or specify a custom start and end date within the last 90 days.
- Use the **Search** field to find tasks. Tasks can be searched by device hostname, IP address, serial number, or partial task name.
- Use the **Refresh** button to view the most recent tasks.

The task details list can also be filtered using the following columns. You can make multiple selections.

- Use **Task Name** to filter tasks by the name of the task. The column can be sorted alphabetically from A to Z or Z to A.
- Use **Type** to filter tasks by the type of task:
  - **(Select All)**
  - **Backup**
  - **Firmware Upgrade**
  - **Restore**

  **(Select All)** is the default choice. The column can be sorted alphabetically from A to Z or Z to A.
- Use **Status** to filter the task by the status of the task:
  - **(Select All)**: The default choice.
  - **Archived**: The task or associated device/TPME has been deleted from the inventory. Historical data is retained for 90 days in read-only format for compliance and troubleshooting purposes.
  - **Canceled**: The task has been canceled.
  - **Completed**: The task has completed.
  - **Failed**: The task failed on all affected devices in the last execution. Check device logs for error details.
  - **Partial**: The task succeeded on some devices but failed on others in the last execution. Review the **Run Details** to identify which devices succeeded and which failed.
  - **Paused**: The scheduled task is temporarily paused, typically due to TPME disconnection or insufficient network connectivity. **Paused** tasks do not execute until the condition is resolved and the task is resumed. Date filters do not affect the display of **Paused** tasks.
  - **Running**: The task is currently executing on one or more devices. A progress bar indicates overall completion percentage. This status applies only to currently active tasks and does not change based on date filters.
  - **Scheduled**: The task is scheduled for future execution but has not yet run. No previous execution history exists for this task.
  - **Successful**: The task completed successfully on all affected devices in the last execution.

  The column can be sorted alphabetically from A to Z or Z to A.

- Use **Recurrence** to filter the tasks by when the task occurs:
  - **Ad Hoc**: One-time tasks.
  - **Recurring**: Scheduled tasks.

  The column can be sorted alphabetically from A to Z or Z to A.
- Use **Next/Last Run** to filter the tasks by tasks scheduled for the future AND have a previous execution; secondary status shows last run outcome.

  The column can be sorted from most recent to oldest or oldest to most recent.
- Use **Scope** to filter the tasks by the scope of the tasks:
  - Single device
  - Multiple devices
  - Device groups
  - Site
  - Multiple sites
  - TPME
  - Single UCP
  - UCP cluster

## Task Names

Tasks are automatically named based on task type and scope. Table 191 displays the task name formats per task type.

**Table 191: Task Naming Conventions**

| Task Type / Scope | Name Format Example |
|---|---|
| Recurring Backup (TPME) | "Daily Config Backup for *TPME-Hostname*" |
| Ad Hoc Backup (Device) | "Config Backup for *Device-Hostname*" |
| Firmware Upgrade (Single Device) | "Firmware Upgrade *version* for *Hostname*" |
| Firmware Upgrade (Multi-Device, Same Site) | "Firmware Upgrade *version* for *Site-Name*" |
| Backup Restore | "Backup Restore for *Device-Hostname*" |



**Note**
If a device or TPME hostname is changed outside of the ExtremeCloud IQ (New) user interface (for example, through the CLI on the device itself), the task name will reflect the hostname at the time of task creation. Subsequently updated hostnames will not be reflected in existing task records.

## View Task Details and Run History

Each task in the **Task Center** can be expanded to view detailed information, including affected devices, their individual status, and a complete run history with logs and error details.

1. Go to **Task Center**, locate the task you want to view and select the corresponding ⋮ button for the task and select **Details**.

   You can search for tasks by entering search terms in the **Search** field.
2. Review the following information in **Task Details**:
   - *Task Name:* Human-readable name automatically generated based on task type and scope
   - *Task ID:* Unique identifier for this task
   - *Type:* Task type (Firmware Upgrade, Backup, or Restore)
   - *Status:* Current status (Running, Scheduled, Successful, Failed, etc.)
   - *Scope:* Number of devices or sites affected
   - *Created By:* User or system that initiated the task
   - *Scheduled Time:* Expected execution time for scheduled tasks
   - *Last Update:* Timestamp of the most recent status update
   - *Affected Devices List:* Table showing each device, its role (source/target), and individual status
3. Select the **Run History** tab within **Task Details** to view the complete run history for this task.

   **Run History** appears, showing all past executions of this task (for recurring tasks) or the single run (for ad-hoc tasks).
4. Select a specific run entry in **Run History** to expand it and view device-level results:
   - Device hostname, IP, and serial number
   - Individual device status for this run (Success, Failed, Pending)
   - Duration (how long the operation took on that device)
   - Logs and error messages (if available for download)
   - Any applicable troubleshooting information
5. Select **Download Logs** or **Export** to download logs or error details.
6. Select **Close** to exit from **Task Details**.

# Subscriptions & Services

Use the **Subscriptions & Licensing** page to view and manage subscriptions, licenses, and trials. In the navigation pane, expand **Subscriptions & Services** and select **Subscriptions & Licensing**.

For more information, see *Extreme Platform ONE & ExtremeCloud IQ Licensing Guide*.

# Administration & Settings | Access Management

Role-Based Access on page 576
Users & Roles on page 579
Identity Providers | Network & Applications on page 584
Identity Providers | Management on page 688
Credential Distribution Groups on page 712
Configure the Idle Session Timeout on page 713

Access Management enables administrators to add users, configure single sign-on for users, or integrate role-based access (RBAC) groups that you configure in an identity provider (IdP). You can:

- Create new users. Add new internal or external user accounts and assign roles to manage their access.
- Implement and assign role-based groups and assign them to sites.
- Allow users to log in with Single Sign-On (SSO) using credentials from an existing SAML-enabled identity provider (IdP).

## Role-Based Access

Access to Extreme Cloud IQ (NEW) features is governed by user roles. Your assigned role determines feature access and visibility of features in the navigation menu. For example, access to certain features and parts of the user interface depends on your assigned role.



**Note**
ExtremeCloud IQ (New) user roles cannot be configured in ExtremeCloud IQ (Classic).

## Role-Mapping Between Extreme Platform ONE Networking and Other Applications

Table 192 and Table 193 on page 577 show the mapping between Extreme Platform ONE Networking roles to those in other applications.

**Table 192: Role-Mapping Between Extreme Platform ONE Networking and Other Applications**

| Extreme Platform ONE Networking | ExtremeCloud IQ (Classic) | ExtremeCloud IQ (New) | Extreme Intuitive Insights |
|---|---|---|---|
| **Administrator** | Administrator | Administrator | Administrator |
| **NetSecOps** | Operator | NetSecOps | NA |
| **BizOps** | Installer | BizOps | NA |
| **Observer** | Monitor<br>Help Desk<br>Application Operator | Observer | NA |
| **Guest Manager** | Guest Management | Guest Manager | NA |

**Note**
The following roles work better in ExtremeCloud IQ (Classic), and do not provide the same experience in ExtremeCloud IQ (New):

- Monitor
- Help Desk
- Application Operator

**Table 193: Role-Mapping Between Extreme Platform ONE Networking and Other Applications**

| Extreme Platform ONE Networking | ExtremeCloud SD-WAN | Extreme Platform ONE Security |
|---|---|---|
| **Administrator** | Administrator | Administrator |
| **NetSecOps** | Operator | NetSecOps |
| **BizOps** | NA | NA |
| **Observer** | Observer | Observer |
| **Guest Manager** | NA | NA |

**Note**
Extreme Platform ONE Security, was formerly known as Universal ZTNA.

## Security-Specific Roles and Features | ExtremeCloud IQ (New)

ExtremeCloud IQ (New) security includes the following additional capabilities not available in networking-only deployments.

- Onboarding: Administrator and NetSecOps roles have full access. Observer and BizOps roles have no access.
- Troubleshooting: Administrator and NetSecOps roles have full access. Observer and BizOps roles have no access.
- Policy Management: Includes Security Policies, Users & Devices, Conditions, Network Services, and Applications
- Security Services: Administrator role has full access. NetSecOps role has read access only.

## Role-Based Feature Access | ExtremeCloud IQ (New)

The following table lists work benches accessible from the navigation pane, according to role.

**Table 194: Role-based feature access**

| Feature | Administrator | NetSecOps | Observer | BizOps | Guest Manager |
|---|---|---|---|---|---|
| **Monitoring** | | | | | |
| Dashboard | R/W | R/W | Read-only | Read-only | No access |
| Visualize | R/W | R/W | Read-only | No access | No access |
| Alerts | R/W | R/W | Read-only | No access | No access |
| Network Devices | R/W | R/W | Read-only | No access | No access |
| Clients | R/W | R/W | Read-only | No access | No access |
| **Configuration** | | | | | |
| Sites | R/W (All sites) | R/W (Only assigned sites) | No access | No access | No access |
| Network Policies | R/W | R/W | Read-only | No access | No access |
| Guest Access | R/W | No access | No access | No access | R/W |
| **Subscriptions & Services** | | | | | |
| Subscriptions & Licensing | R/W | Read-only | No access | R/W | No access |
| **Administration & Settings** | | | | | |
| Access Management | R/W | No access | No access | No access | No access |
| Alert Policies | R/W | R/W | No access | No access | No access |
| External Notifications | R/W | R/W | No access | No access | No access |

**Table 194: Role-based feature access (continued)**

| Feature | Administrator | NetSecOps | Observer | BizOps | Guest Manager |
|---|---|---|---|---|---|
| Service Management | R/W | R/W | No access | No access | No access |
| Backup & Restore | R/W | R/W | No access | No access | No access |
| Integrations | R/W | No access | No access | No access | No access |
| Logs | R/W | R/W | No access | No access | No access |

*Read-Only Access*

Read-only access provides a "view-only" experience without the full functionality reserved for roles with read-write (R/W) access. With read-only access you can customize your view:

- Select the data range and pagination.
- Select which table columns to show.
- Filter and refresh tables.

For most table views, you can export the data to a .CSV file, but you cannot perform actions that require R/W access, such as:

- Download an inventory or configuration template.
- Link or unlink an Extreme Portal account.
- Renew subscriptions.

## Role-Based Site Awareness

When you create a new user, you can specify the sites to which that user will have access. The following ExtremeCloud IQ (New) pages display data only for the sites assigned to the user:

- **Monitor** > **Dashboard**
- **Monitor** > **Network Devices**
- **Monitor** > **Clients**
- **Monitor** > **Inventory**

You can assign sites to the NetSecOps, Observer, and BizOps roles. The Administrator role has global access.

Related Links

Create a New User on page 580

# Users & Roles

You can add multiple users and roles of the following types to ExtremeCloud IQ (New).

- Internal users
- External users

You can also implement single-sign-on via SAML-based identity providers.

**Note**
Roles for all applications can be assigned only in Extreme Platform ONE Networking. You cannot create or assign roles or custom roles that were previously assigned in individual applications.

## Role-Based Access

Access to Extreme Cloud IQ (NEW) features is governed by user roles. Your assigned role determines feature access and visibility of features in the navigation menu. For example, access to certain features and parts of the user interface depends on your assigned role.

**Note**
ExtremeCloud IQ (New) user roles cannot be configured in ExtremeCloud IQ (Classic).

## Create a New User

User access is controlled by the roles you assign. Use this task to add a new internal or external user account and assign roles to manage their site access.

**Note**
After you create a user account, the new user receives an email prompt to create a password and log in to Extreme Platform ONE Networking. Until the user logs in, their user status remains **Inactive**. When you edit a user account, you can resend the email.

1. Go to **Administration & Settings** > **Access Management**.
2. In the **Users & Roles** area, select one of the following account-types:
   - **Internal Users**: Select this tab to grant access to users within your organization.
   - **External Users**: Select this tab to grant access to users outside of your organization; for example, resellers, distributors, technical support, and sales.

     **Caution**
     Depending on the role assigned to an External User, that user may have full access or restricted access to all features and assets in Extreme Platform ONE Networking or ExtremeCloud IQ (New). Be cautious and evaluate role-based access options before assigning access to an External User. Provide access to only the minimum necessary resources. Use the Principle of Least Privilege, and add additional capabilities as needed.

3. Select **Create New User**.

4. For an Internal user account, perform the following steps:

   For an External user account, go to step 5 on page 582.

   a. Type the email address for the user and select **Next**.
   b. Configure the user configuration settings.

**Table 195: User configuration settings**

| Field | Description |
|---|---|
| Email | Email address, not more than 128 characters. |
| First Name | First name, not more than 63 characters. |
| Last Name | Last name, not more than 63 characters. |
| Primary Role | Specify access to Extreme Platform ONE Networking, ExtremeCloud IQ (New), and if applicable Security, SD-WAN, and other Platform ONE applications. The primary role is the platform role that is common across all accessible applications.<br>Default: Observer<br><br>**Note:** When you select a **Primary Role**, ExtremeCloud IQ (New) automatically selects a **Classic Role**. For more information, see Table 196 on page 582. |
| Classic Role | Specify access to ExtremeCloud IQ (Classic).<br>Default: Observer<br><br>**Note:** Options are limited by the **Primary Role** selection for application access. For more information, see Table 196 on page 582. |
| Sites | Specify access to sites. Administrators have access to all sites and locations if a site hierarchy is created. Users with other roles have access only to the sites they have been assigned, and do not see alerts or notifications for other sites.<br><br>**Important:** It is imperative that you assign users to a site or sites, with one exception: the **Guest Management** role does not support site assignment. |
| Idle Session Timeout | Specify whether to enforce idle session timeout. If you do not specify a time, the user session will not timeout.<br><br>**Note:** A non-expired timeout configuration overrides any admin-configured timeout. Otherwise, all admin-configured user timeout settings follow those that the admin configured. |

   c. Select **Save**.
   d. You can review the access and roles assigned to the new user by selecting **Internal Users** in the **Users & Roles** area.

5. For an External user account, perform the following steps:
   a. Type the external email address and select **Next**.

      **Note**
      ExtremeCloud IQ (New) validates the email address for availability. An error message provides notification if the address was already added or is ineligible to be added for an external user.

   b. Configure **Application Access** for the user. Select the user role value for the **Primary Role** and the **Classic Role**.

      For information about the **Primary Role** and the **Classic Role**, see Table 195 on page 581.
   c. **Configure site access** from the role-specific menu choices.

      See Role-Based Site Awareness on page 579.
   d. (Optional) Select the access duration:
      - **Time Dependent:** Select start and end dates (optional). Select the respective drop-down menus to assign workspace and application access, and roles to the external user.
      - **Indefinite:** Do not define start and end dates, meaning that site access is not time-limited until the value changes.
   e. Select **Save**.

      You can review the access and roles assigned to the new user in the **Users & Roles** area by selecting **External Users** in the **Users & Roles** area.

Related Links

Role-Based Site Awareness on page 579

*Primary and Classic Role Selection*

The following table describes the available options for the **Classic Role**, depending on the selected **Primary Role**.

**Table 196: Role selection**

| Primary Role | Classic Role options |
|---|---|
| Administrator | Administrator |
| NetSecOps | Operator |
| BizOps | Installer |
| Observer | Monitor<br>Help Desk<br>Observer |
| Guest Management | Guest Management |

## View the List of Users

Use this topic to view the list of users.

1. Go to **Administration & Settings** > **Access Management**.

2. In the **Users & Roles** area, select one of the following account-types:
   - **Internal Users**: Displays users within your organization.
   - **External Users**: Displays users outside of your organization, for example, resellers, distributors, technical support, and sales.

Select  to choose which columns to show. You can also change the order of some columns.



**Note**
The first three columns are frozen:
- Username
- Primary Role
- Classic Role

Use the search, group, and filter features to refine your result set.

Related Links

Create a New User on page 580
Edit, Disable, or Delete a User Account on page 583

## Edit, Disable, or Delete a User Account

The **Edit** option provides the ability to modify roles, site access, and idle session timeout.

Use this task to edit, disable (suspend), or delete a user account.

1. Go to **Administration & Settings** > **Access Management**.
2. In the **Users & Roles** area, select the **Internal Users** or **External Users** tab.
3. Locate and select the account to change.
4. Select  for the account, and then select one of the following options:
   - **Edit**. Make changes to the account configuration.
   - **Disable**. Inactivate the account, with the ability to reactivate if desired.
   - **Delete**. Remove the account permanently from the system.
5. Follow the prompts to make your changes, and select **Save**.
6. Select **Save**.

## Configure the Idle Session Timeout

Use this task to specify the idle period, after which an inactive session automatically times out, for all user accounts with **Enforce Idle Session Timeout** enabled. See Create a New User on page 580.

**Note**
If a user account has **Enforce Idle Session Timeout** disabled, sessions for that account do not time out. To change this setting, edit the user account.

1. Go to **Administration & Settings** > **Access Management**, and then select the **Access Settings** tab.
2. Select **Timeout Duration**, and select the hour and minutes for duration from the **HH** and **MM** menus, respectively.
3. Select **Save**.

Related Links

Create a New User on page 580
Edit, Disable, or Delete a User Account on page 583

# Identity Providers | Network & Applications

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

- Microsoft Entra ID
- Google Workspace
- Okta

The ability to support multiple identity providers (IdPs) within a single tenant is supported for complex identity management needs, such as during cloud service migrations, acquisitions, or ensuring redundancy. It also addresses the growing requirement to manage contractors with separate IdPs securely. This enhancement increases flexibility especially for customers.

There are three primary purposes for integrating with an Identity Provider for ExtremeCloud IQ (New). The applications created in the Identity Provider are to be different even if the type is the same, however they can be reused if desired.

The purposes are:

- User and User Group Synchronization – Used to make users and user groups available within ExtremeCloud IQ (New) for policy assignment.

  **Note**
  Synced User and User Groups cannot be removed from Extreme Platform ONE Security. First remove the user or group from the Identity Provider and then re-initiate synchronization.

- Application Access authentication – Used for logging into the ExtremeCloud IQ (New) Agent or the End User web portal.

- Network Access authentication – Used for 802.1X EAP-TTLS authentication of clients on access points and switches.

Within the IdP table the following columns displayed:

- Priority
- IdP Type
- Domain
- Status
- Purpose

For more information, see IdP Network & Applications | Support Multiple IdPs on page 688.

## Microsoft Entra ID

There are three primary purposes for integrating with an Identity Provider for ExtremeCloud IQ (New). The applications created in the Identity Provider are to be different even if the type is the same, however they can be reused if desired

The purposes are:

- User and User Group Synchronization – Used to make users and user groups available within ExtremeCloud IQ (New) for policy assignment.

  **Note**
  Synced User and User Groups cannot be removed from Extreme Platform ONE Security. It must be removed from the Identity Provider and then a syncing cycle should be initiated again.

- Application Access authentication – Used for logging into the ExtremeCloud IQ (New) Agent or the End User web portal.
- Network Access authentication – Used for 802.1X EAP-TTLS authentication of clients on access points and switches.

*Microsoft Entra ID | Synchronize Users and User Groups with Entra ID*

Synchronizing Users and User Groups from Entra ID is required to ensure policies can be applied to users connecting with Entra ID credentials in ExtremeCloud IQ (New). There are two methods available for synchronization:

1. Just in Time (JIT) Synchronization – this method has ExtremeCloud IQ (New) reach into Microsoft Entra ID and pull users and user groups on a polled basis. This method leverages an OIDC application to integrate with the Entra APIs.
2. System for Cross-Domain Identity Management (SCIM) Synchronization – this method has Microsoft Entra ID push users and user groups from Entra into ExtremeCloud IQ (New). This method requires an enterprise application to be set up in Entra ID so that automatic provisioning can be enabled.

**Microsoft Entra ID | Synchronizing Users and User Groups with JIT**

For JIT integration, the setup in Entra ID will be completed first, followed by the configuration of ExtremeCloud IQ (New).

### Microsoft Entra ID | JIT User and User Groups Synchronization

This method has Extreme Platform ONE Security reach into Microsoft Entra ID and pull users and user groups on a polled basis. The synchronization uses an OIDC application to integrate with the Entra ID APIs.

JIT integration is configured in these steps:

1. Configure Microsoft Entra ID.
2. Configure Extreme Platform ONE Security.

#### Microsoft Entra ID

1. Go to **Applications** > **App registration** and select **New registration**.

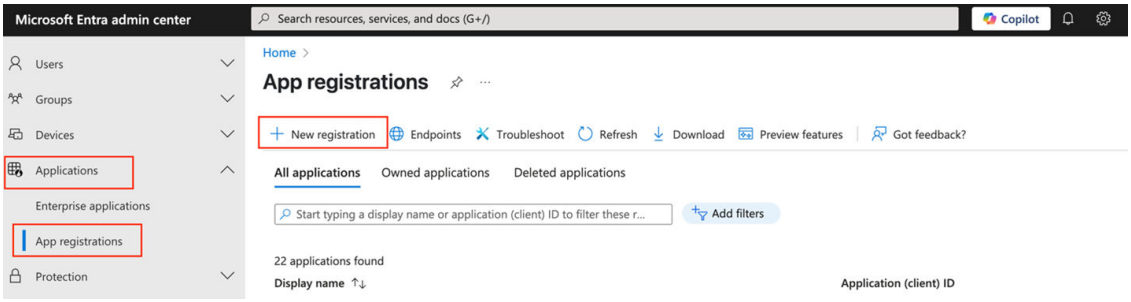



**Figure 9: App registrations page**

2. Under **Register an application**.
   a. Name the application appropriately for JIT Integration.
   b. Leave the default fields selected and select **Register**.
3. Copy the **Application (client) ID** and **Directory (tenant) ID** for use later. Under **Client Credentials**, select **Add a certificate or secret**.

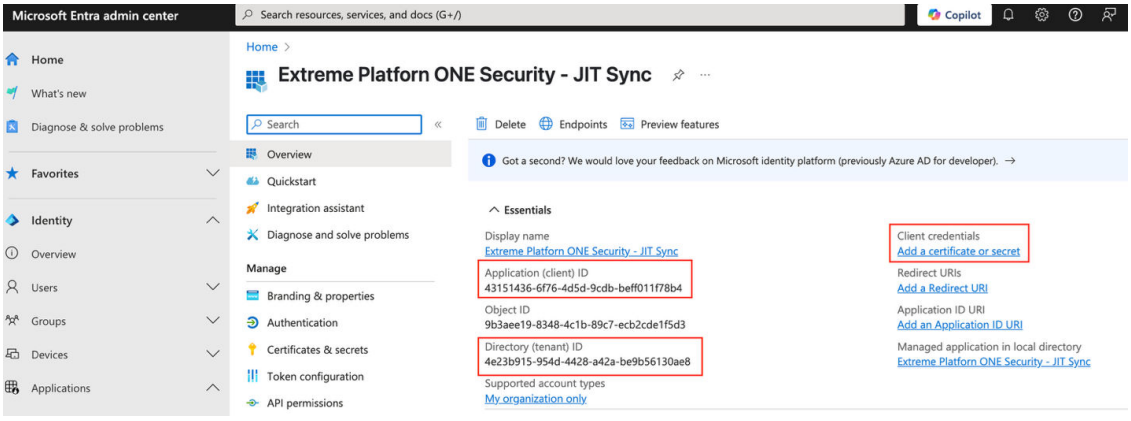



**Figure 10: Client credentials**

4. Select **New client secret**.

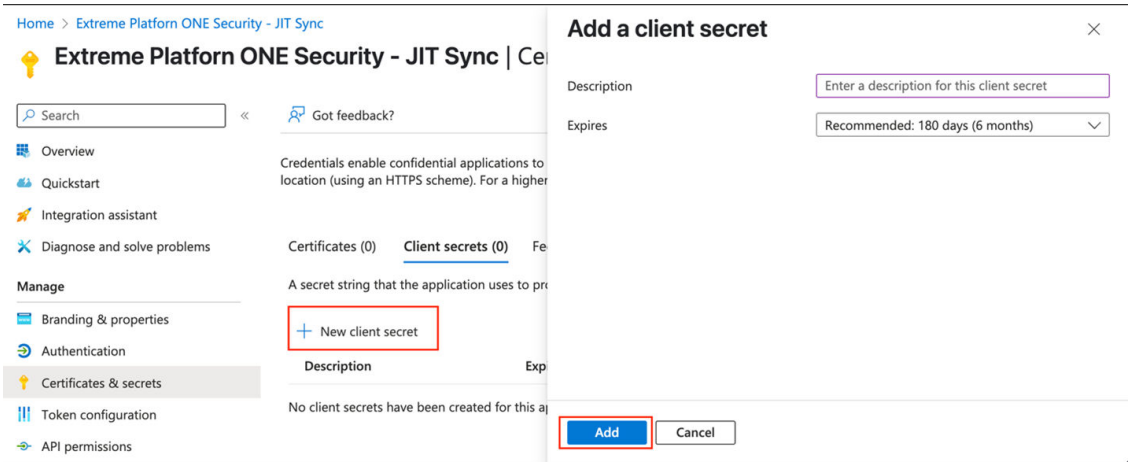



**Figure 11: Add a client secret window**

a. Enter a description if desired and a preferred expiration date of the secret.
b. Once complete, select **Add**.

5. Copy the value of the new secret for use later.

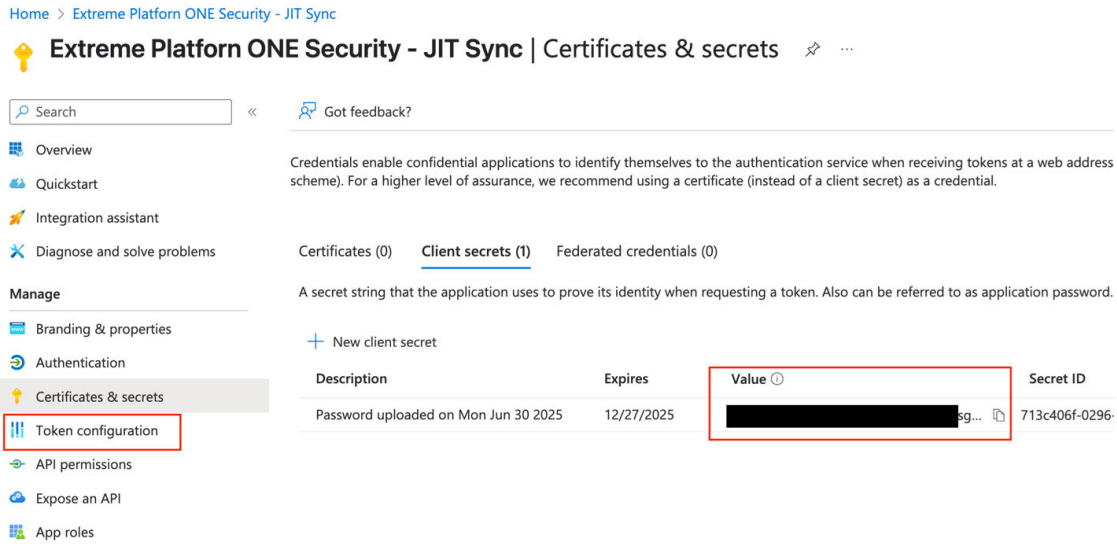



**Figure 12: Client secrets**

6. Go to **Manage** > **Token Configuration**, select **Add optional claim** and configure the settings in Table 197.

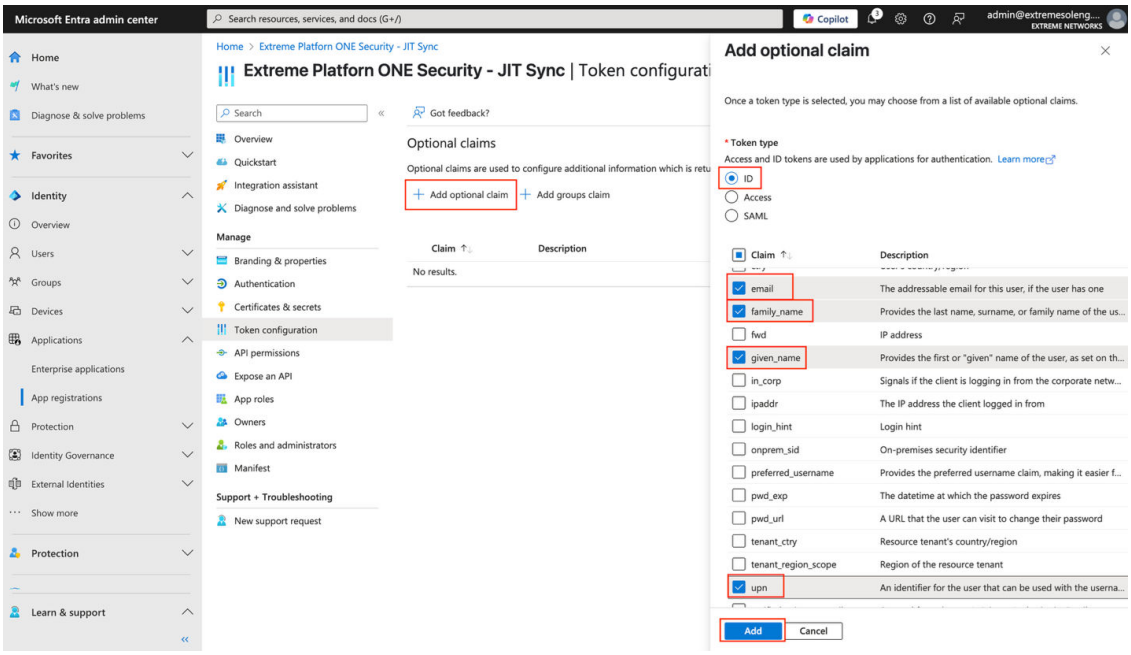



**Figure 13: Add optional claim window**

**Table 197: Optional Claim Configuration Settings**

| Field | Description |
|---|---|
| Token Type | Select the **ID** radio button. |
| Claim | Select the following from the available list:<br>• email<br>• family_name<br>• given_name<br>• upn |
| Turn on the Microsoft Graph email, profile permission (required for claims to appear in token). | Enable the toggle if prompted to turn on Microsoft Graph. |
| Select **Add**. | |

7. Select **Add groups claim** and configure settings in Table 198.

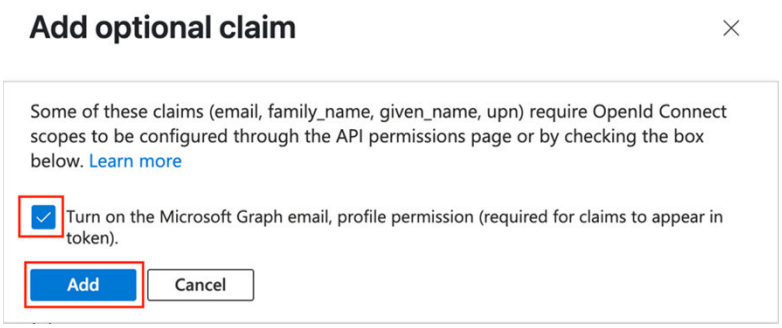



**Figure 14: Add optional claim**

**Table 198: Group Claim Configuration Settings**

| Field | Description |
|---|---|
| Select group types to include in Access, ID, and SAML tokens. | Select **Groups assigned to the application**. |
| Customize token properties by type | Select **Group ID**. |
| Select **Add**. | |

8. Go to **Manage** > **API permissions** and select **Add a permission**.

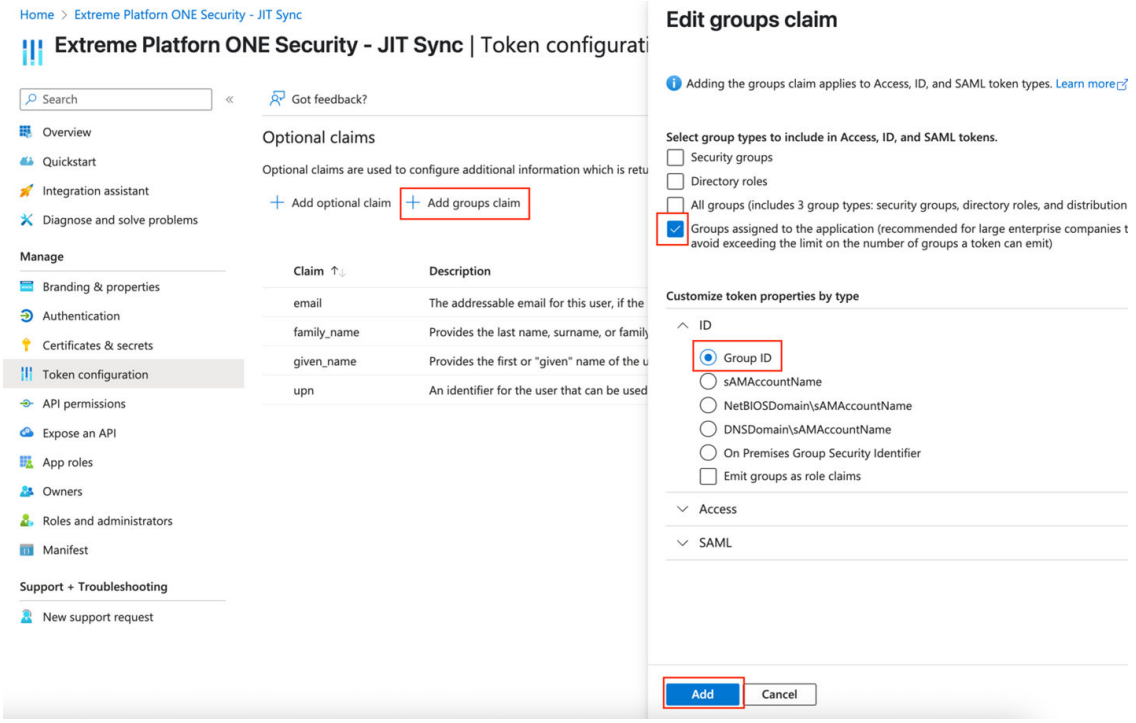



**Figure 15: Edit groups claim**

9. Select **Microsoft Graph** and configure the settings in Table 199.

**Table 199: Microsoft Graph Configuration Settings**

| Field | Description |
|---|---|
| What type of permissions does your application require? | Select the **Application permissions**. |
| Select permissions | Filter on text of the permission needed and select it from the drop-down list. The following permissions are required:<br>• User.Read.All<br>• Group.Read.All<br>• GroupMember.Read.All |
| Select **Add permissions** and the **Configured permissions** window is displayed. | |
| Configured permissions | Select **Grant admin consent for <Company Name>**. |

10. Go to **Overview**, scroll to the bottom, and select **Go to Enterprise applications**.

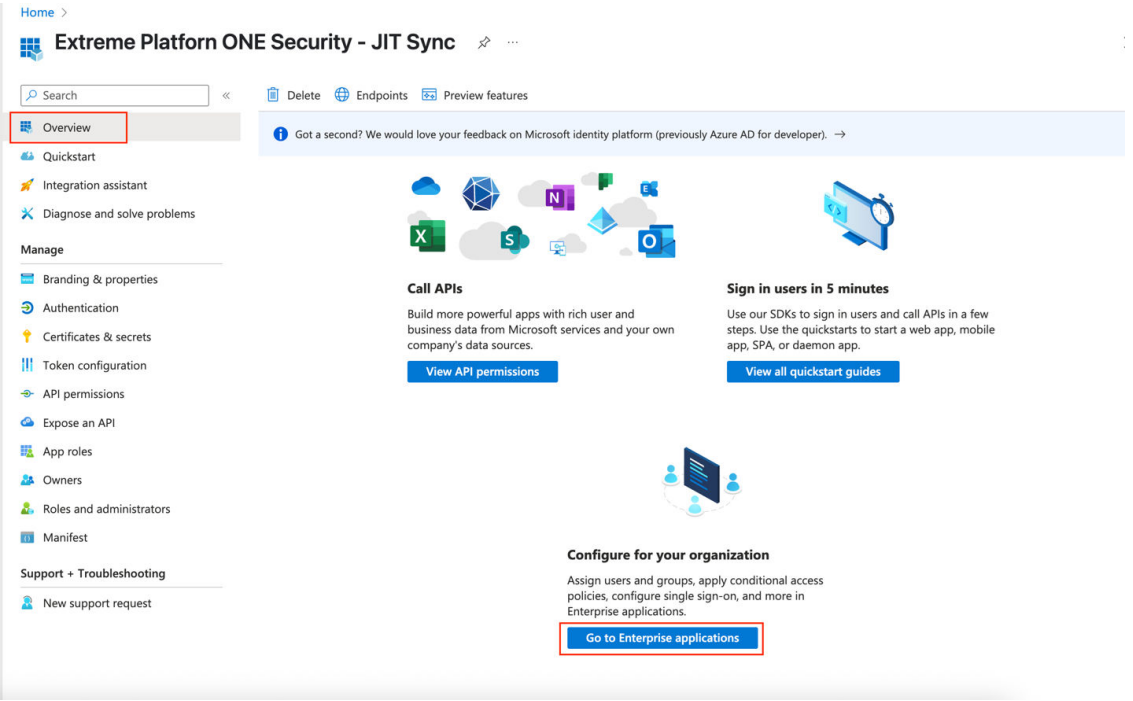



**Figure 16: Enterprise applications**

11. Go to **Manage** > **Properties**.
    a. Set **Assignment required?** to **Yes**
    b. Select **Save**.

12. Go to **Manage** > **Users and groups**.

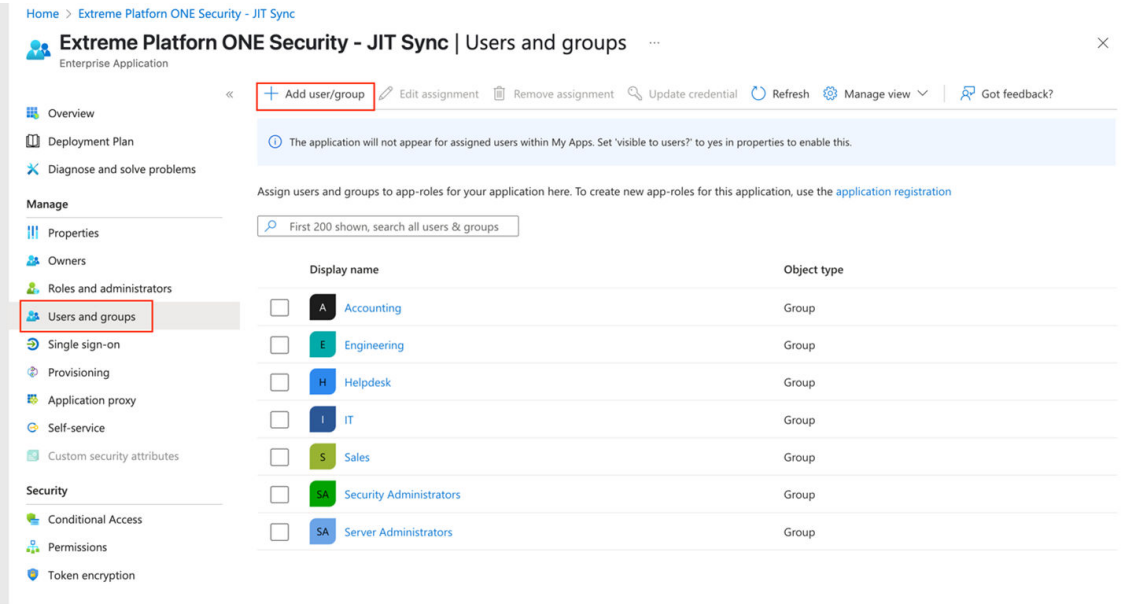



**Figure 17: Users and groups**

a. Select **Add user/group**.
b. Assign all groups to use in ExtremeCloud IQ (New).

**Extreme Platform ONE Security**

13. Go to **Administration and Settings** > **Access Management** > **Identity Providers** > **Network & Applications**.

14. Select **Add IDP Profile** and configure the settings in Table 200.

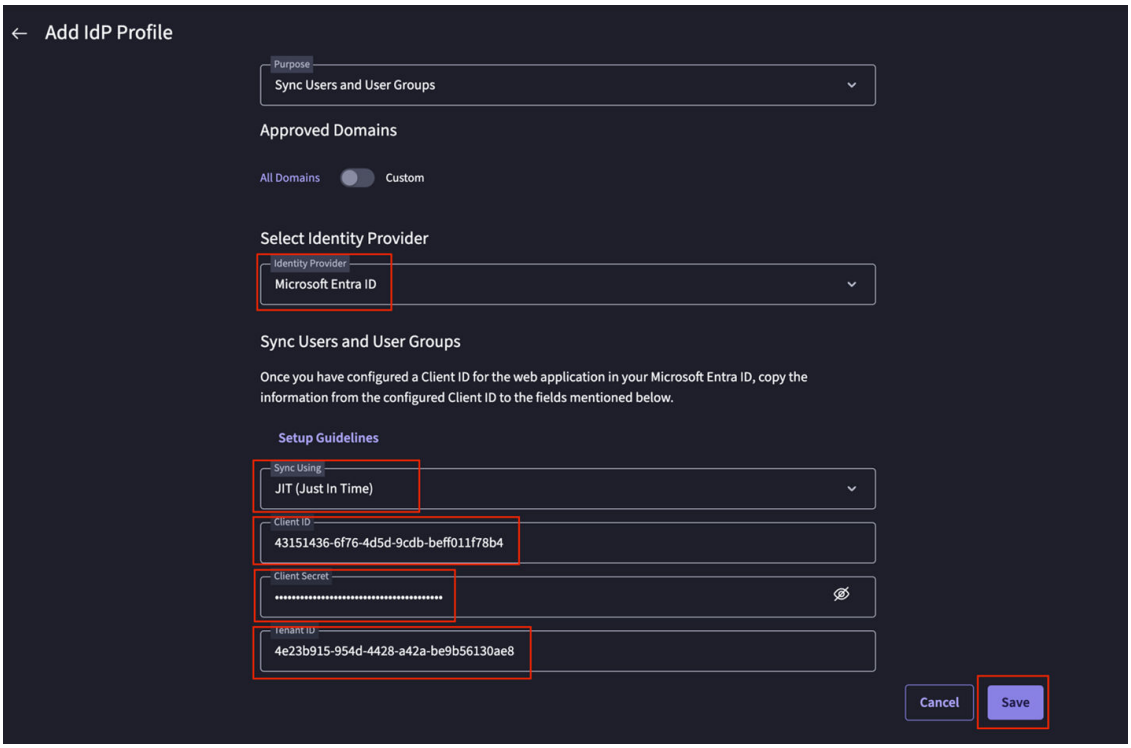



**Figure 18: IdP Profile Settings**

**Table 200: JIT for Microsoft Entra ID Configuration Settings**

| Field | Description |
|---|---|
| Set Up IdP | Select **Sync Users and User Groups** from the Purpose drop-down list. |
| Approved Domains | If the domain needs to be limited, it can be selected here with the **Custom** toggle, otherwise leave it to **All Domains** |
| Select Identity Provider | Select **Microsoft Entra ID** from the **Identity Provider** drop-down list. |
| Setup Guidelines | Select **JIT (Just in Time)** for the **Sync Using** drop-down list. |
| | Paste the copied credentials from Microsoft Entra ID:<br>• Client ID<br>• Client Secret<br>• Tenant ID |

15. To complete the setup, select **Save**.

A dynamic sync workflow will be schedule automatically. To force a sync, go to **Access Management** > **Identity Providers**, select ⋮ and select **Sync Now**.

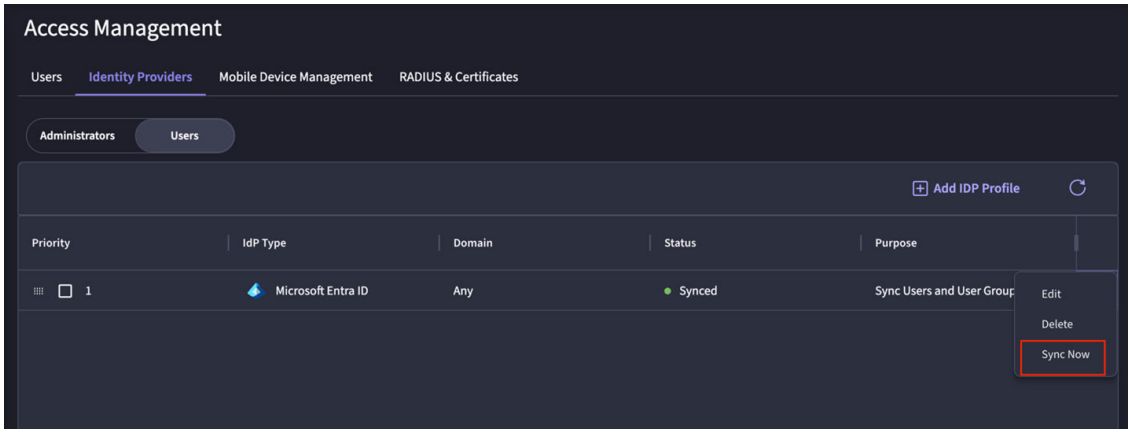



**Figure 19: Sync Now**

### Configure ExtremeCloud IQ (New) JIT

Use this task to configure the Sync IDP profile in ExtremeCloud IQ (New).

1. Log into your ExtremeCloud IQ (New) tenant.
2. Go to **Administration and Settings** > **Access Management** > **Identity Providers** > **Network & Applications**.
3. Select **Add IDP Profile** and configure the settings in Table 201.

**Table 201: JIT for Microsoft Entra ID Configuration Settings**

| Field | Description |
|---|---|
| Set Up IdP | Select **Sync Users and User Groups** from the Purpose drop-down list. |
| Approved Domains | If the domain needs to be limited, it can be selected here with the **Custom** toggle, otherwise leave it to **All Domains** |
| Select Identity Provider | Select **Microsoft Entra ID** from the **Identity Provider** drop-down list. |
| Setup Guidelines | Select **JIT (Just in Time)** for the **Sync Using** drop-down list. |
| | Paste the copied credentials from Microsoft Entra ID:<br>• Client ID<br>• Client Secret<br>• Tenant ID |

4. To complete the setup, select **Save**.

A dynamic sync workflow will be schedule automatically. To force a sync, go to **Access ManagementIdentity providers**, select ⋮ and select **Sync Now** .

### Synchronizing Users and User Groups with SCIM

This method has Microsoft Entra ID push users and user gorups from Entra into Extreme Platform ONE Security. This method requires an enterprise application to be set up in Entra ID

so tht automatic provisioning can be enabled. For SCIM integration, the setup in ExtremeCloud IQ (New) will be completed first, followed by the configuration of Microsoft Entra ID.

#### Microsoft Entra ID | SCIM User and Groups Synchronization

This method has Microsoft Entra ID push users and user groups from Entra into Extreme Platform ONE Security. Synchronization requires an enterprise application to be set up in Microsoft Entra ID to enable automatic provisioning.

SCIM integration is configured in these steps:

1. Configure Extreme Platform ONE Security.
2. Configure Microsoft Entra ID.

##### Extreme Platform ONE Security

1. Go to **Access Management** > **Administration & Settings** > **Identity Providers** and select **Network & Applications**.
2. To create a new profile, select the **Add IdP Profile** and configure the settings in Table 202.

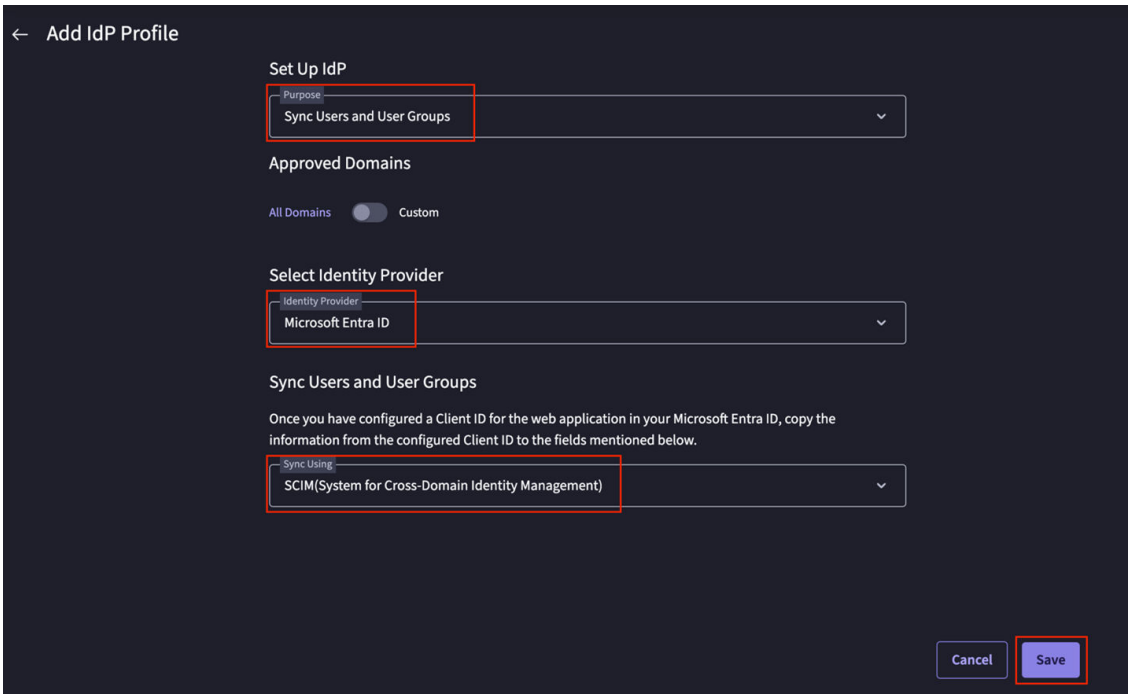



**Figure 20: Configuration Settings**

**Table 202: SCIM for Microsoft Entra ID Configuration Settings**

| Field | Description |
|---|---|
| Set Up IdP | Select **Sync Users and User Groups** as the **Purpose** from the drop-down list. |
| Approved Domains | If the domain needs to be limited, it can be selected here with the **Custom** toggle, otherwise leave it to **All Domains**. |

**Table 202: SCIM for Microsoft Entra ID Configuration Settings (continued)**

| Field | Description |
|---|---|
| Select Identity Provider | Select **Microsoft Entra ID** from the **Identity Provider** drop-down list. |
| Setup Guidelines | Select **SCIM (System for Cross-domain Identity Management)** for the **Sync Using** drop-down list. |

3. Select **Save**.
4. Once saved, from the 3-dot menu, select **Edit**.
   a. In the **Edit** window, select **Entra Syncing Credentials**.
   b. In the **Entra ID Syncing Credentials** window, save the **Tenant URL** and **Secret Token** for use within Entra ID.

### Microsoft Entra ID

5. Go to **Enterprise application** > **New application**.
6. Select **Create your own application**.

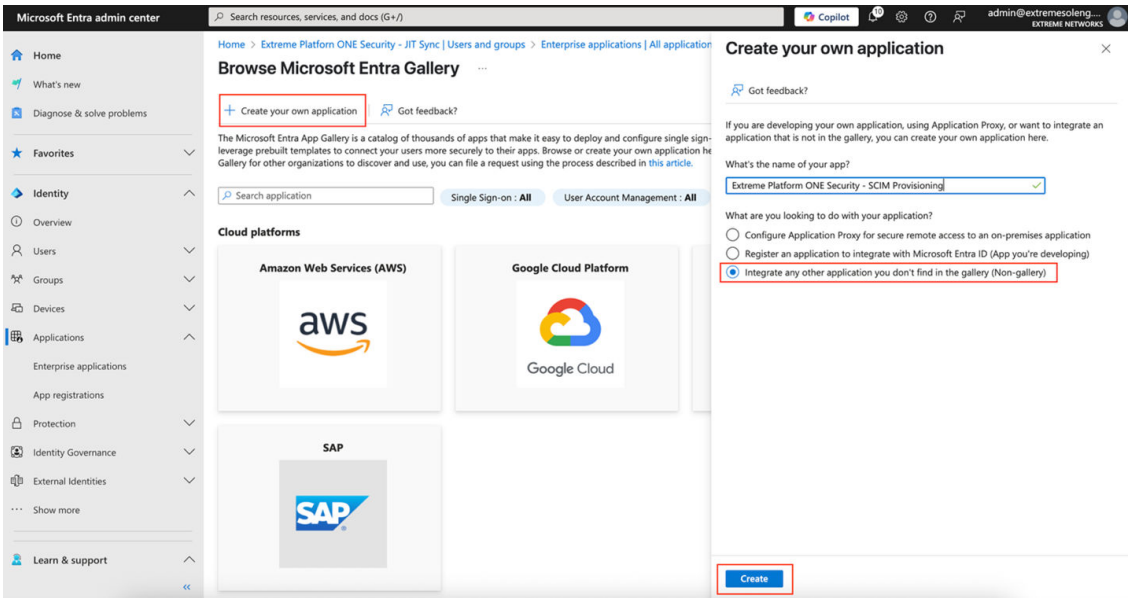



**Figure 21: Browse Microsoft Entra Gallery**

   a. Name the application with Provisioning in the title so that it can be easily located.
   b. Select the **Non-gallery** option.

7. Select **Properties** for the application.

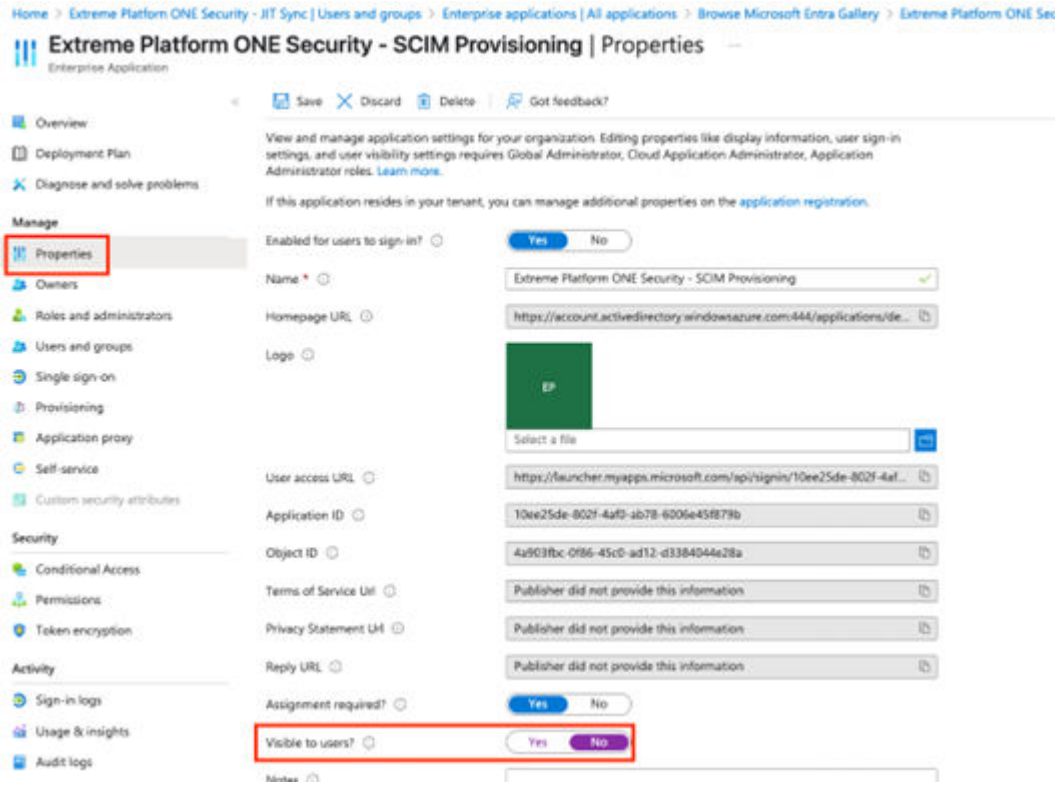



**Figure 22: Properties**

   a. Toggle **Assignment Required** to **Yes**.
   b. Toggle **Visible to Users** to **No**.
   c. Select **Save**.
8. Select **Users and groups** and assign the User groups to included in ExtremeCloud IQ (New).

9. Go to **Manage** > **Provisioning** and select **New configuration**.

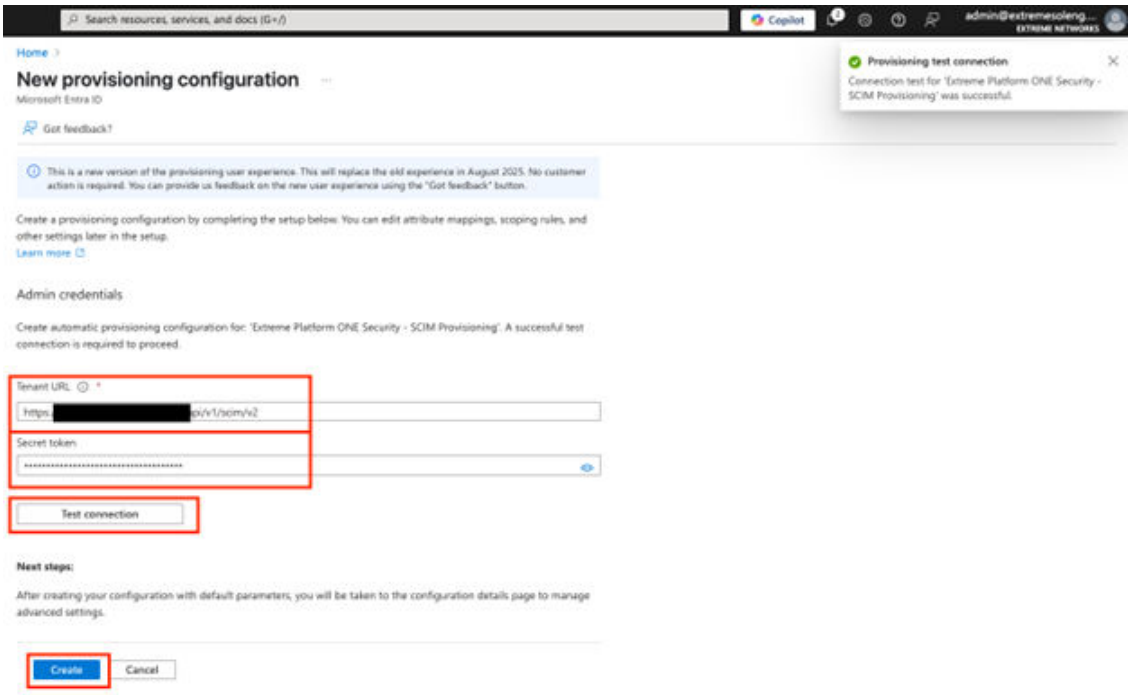



**Figure 23: Configuration Settings**

   a. Under **Admin Credentials**, paste the **Tenant URL** and **Secret Token** that were previously copied from ExtremeCloud IQ (New).
   b. Select **Test Connection** and on resulting success.
   c. Select **Create**.

10. On the **Attributes Mapping** page and complete the following:
   a. Select **Provision Microsoft Entra ID Users**.
   b. Under **Source Object Scope**, select **All records**.
   c. Select **Add new filter group**.

d. In **Add Scoping Filter**, select **mail** as the source attribute.

**Note**

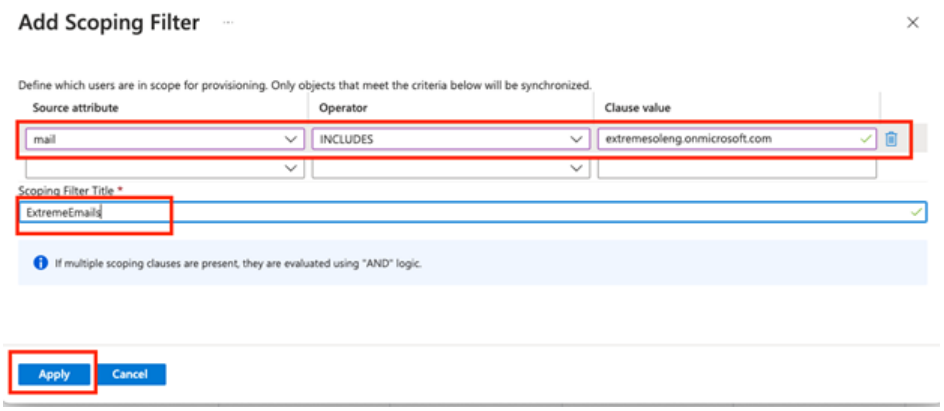



**Figure 24: Scoping Filter**

The mail attribute needs to exist for the user to be imported into ExtremeCloud IQ (New). If the desire is to only have corporate email accounts imported into ExtremeCloud IQ (New), matching on the email extension for the organization will work. For this example, select **INCLUDES** as the operator and the email domain as the clause value.

e. Name the scoping filter and select **Apply**.

f. In the resulting screens, select **Apply** and **Save** to save the filter to the provisioning profile.

11. Go to **Overview**, select **Start Provisioning** to begin the provisioning process.

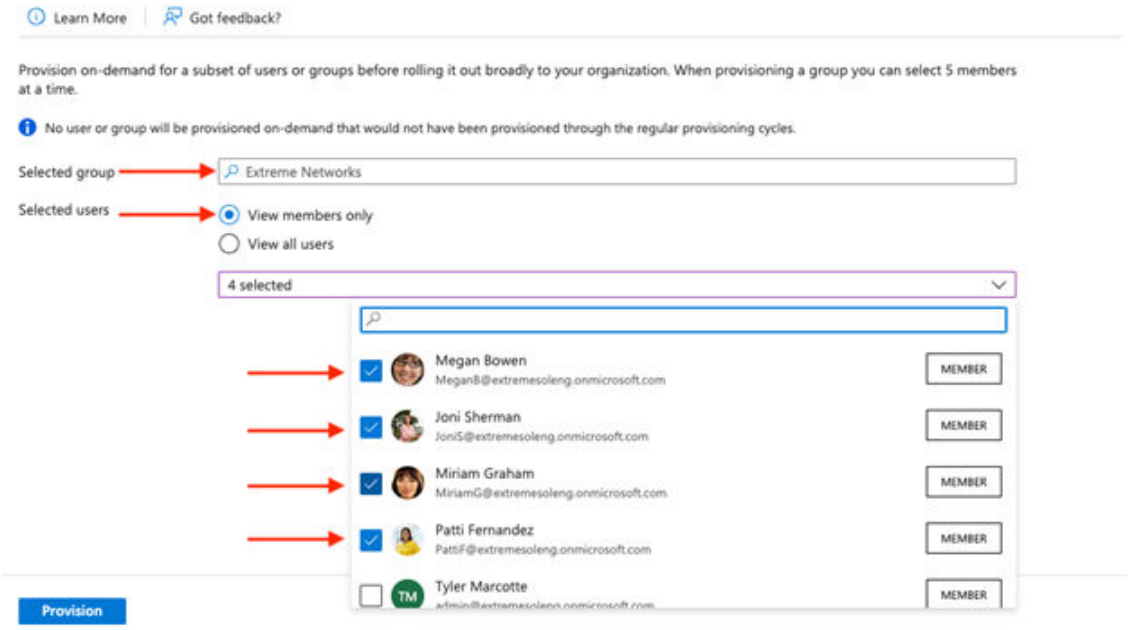



**Figure 25: Group selection**

**Note**
Provisioning can take up to an hour to start. If desired **Provision on Demand** can be selected from the **Provisioning Overview** to immediately start a provisioning cycle. Select the group or users to provision at that moment.

In ExtremeCloud IQ (New) the users and user groups should now be available in the **Policy** > **Users & Devices** > **Users** section. If the users or user groups do not show up, review errors or messages in Entra ID for why the provisioning failed.

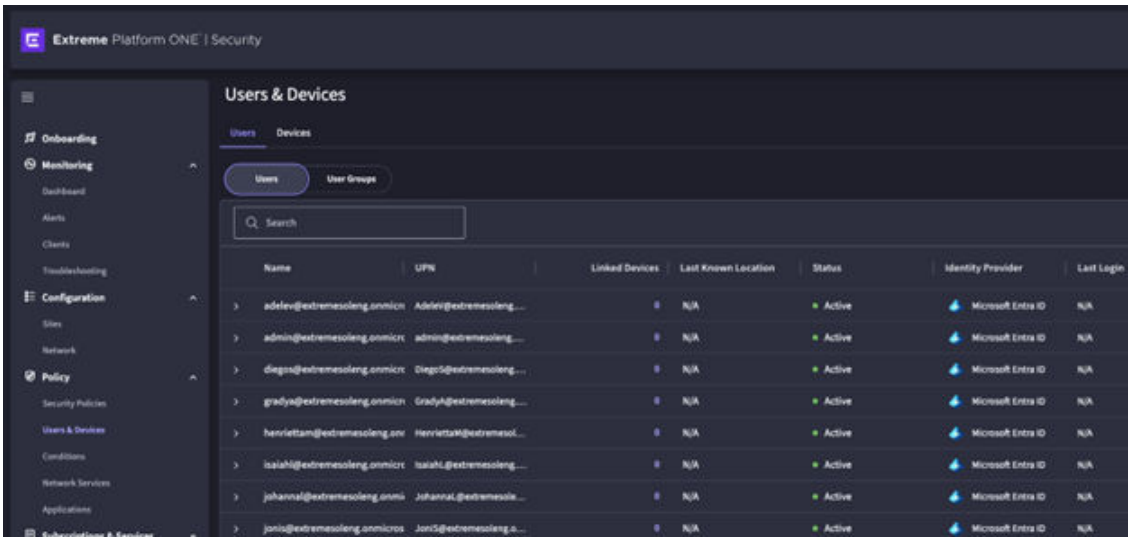



**Figure 26: User Confirmation**

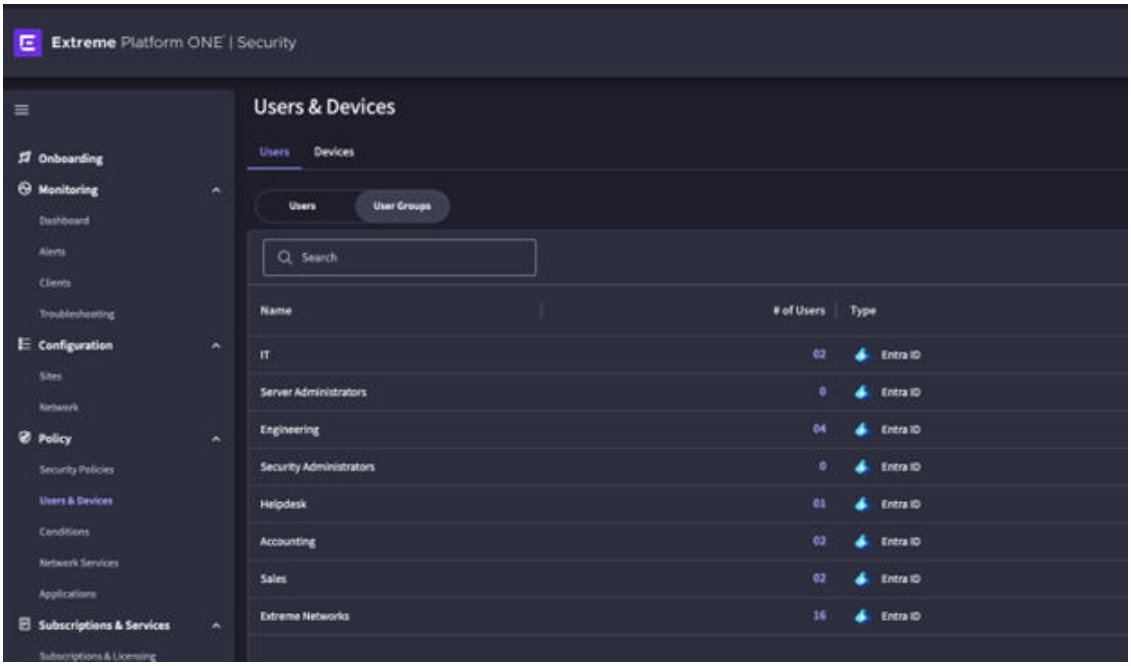



**Figure 27: Group Confirmation**

#### Synchronize Users and User Groups using SCIM Provisioning

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

1. Log in to Microsoft Entra ID and go to **Enterprise application** > **New application**.
2. Select **Create your own application**. Name the application with Provisioning in the title so that it can be easily located. Select the **Non-gallery** option.
3. Select **Properties** for the application and toggle **Assignment Required** to **Yes** and **Visible to Users** to **No**, then select **Save**.
4. Select **Users and groups** and assign the User groups that should be included in ExtremeCloud IQ (New).
5. Go to **Manage** > **Provisioning** and select **New configuration**.
6. Under **Admin Credentials**, paste the **Tenant URL** and **Secret Token** that were previously copied from ExtremeCloud IQ (New). Select **Test Connection** and on resulting success, select **Create**.
7. Select **Provision Microsoft Entra ID Users**.
8. On the **Attributes Mapping** page and complete the following:
   a. Under **Source Object Scope**, select **All records**.
   b. Select **Add new filter group**.
   c. In **Add Scoping Filter**, select **mail** as the source attribute. The mail attribute needs to exist for the user to be imported into ExtremeCloud IQ (New). If the desire is to only have corporate email accounts imported into ExtremeCloud IQ (New), matching on the email extension for the organization will work. For this example, select **INCLUDES** as the operator and the email domain as the clause value.

d. Name the scoping filter and select **Apply**.
e. In the resulting screens, select **Apply** and **Save** to save the filter to the provisioning profile.

9. Go to **Overview**, select **Start Provisioning** to begin the provisioning process.
10. Provisioning can take up to an hour to start. If desired **Provision on Demand** can be selected from the **Provisioning Overview** to immediately start a provisioning cycle.
11. Select the group or users to provision at that moment.
12. In ExtremeCloud IQ (New) the users and user groups should now be available in the **Policy** > **Users & Devices** > **Users** section. If the users or user groups do not show up, review errors or messages in Entra ID for why the provisioning failed.

*Microsoft Entra ID | Network Access*

If user-based 802.1X EAP-TTLS network authentication is going to be used with Microsoft Entra ID, a separate application is required to be created that bypasses MFA as 802.1X does not have a native method to provide real-time multi-factor authentication prompt. This can only be done with an OpenID Connect (OIDC) Application.

If EAP-TLS (Certificate-based authentication) is going to be the only source of 802.1X user and device authentication, this setup is not required.

**Microsoft Entra ID | Network Access**

If user-based 802.1X EAP-TTLS network authentication is going to be used with Microsoft Entra ID, a separate application is required to be created that bypasses MFA as 802.1X does not have a native method to provide real-time multi-factor authentication prompt. This can only be done with an OpenID Connect (OIDC) Application.

If EAP-TLS (Certificate-based authentication) is going to be the only source of 802.1X user and device authentication, this setup is not required.

Network Authentication requires that multi-factor authentication be disabled for an Entra ID application when using EAP-TTLS. If Entra ID premium is used, a rule can be created to exclude this only for the Network Access OIDC application. If Entra ID premium is not in use, this must be disabled for all users.

For more information on Conditional Access Policies, refer to Microsoft documentation here: https://learn.microsoft.com/en-us/entra/identity/conditional-access/overview Disable MFA using a conditional access policy for Entra ID.

For Network Access is configured in these steps:

1. Configure Microsoft Entra ID.
2. Configure Extreme Platform ONE Security.
3. Disable MFA using a conditional access policy for Entra ID.

**Microsoft Entra ID**

1. Go to **Applications** > **App registration** and select **New registration**.
2. Under **Register an application**, name the application appropriately for the Network Access Integration. Leave the default fields selected and select **Register**.

3. Copy the **Application (client) ID** and **Directory (tenant) ID** for use later. Under **Client Credentials**, select **Add a certificate or secret**.

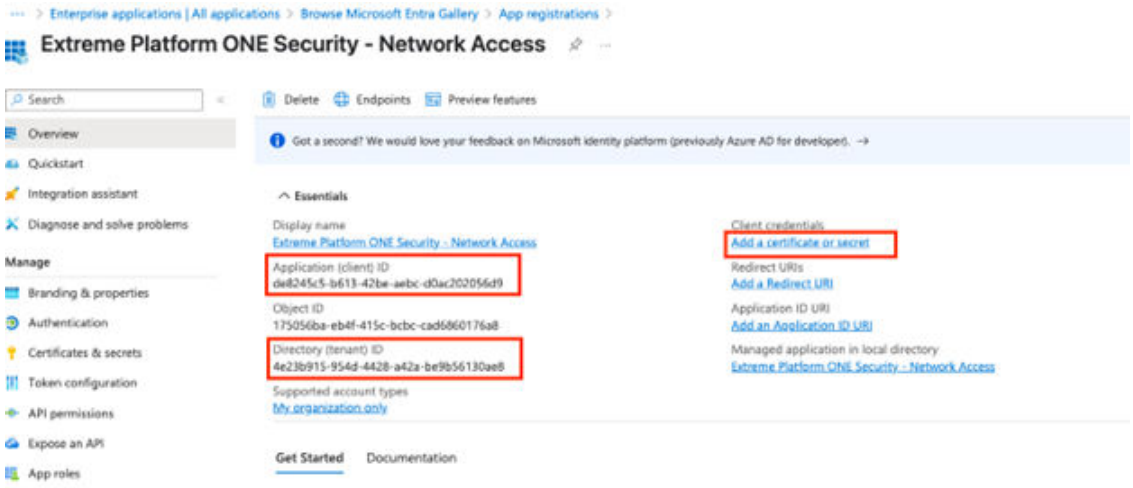



**Figure 28: Client Credentials**

4. Select **New client secret**.
   a. Enter a description if desired and a preferred expiration date of the secret.
   b. Once complete, select **Add**.
5. Copy the value of the new secret for use later.
6. Go to **Manage** > **API permissions** and select **Grant admin consent for <Company Name>**.

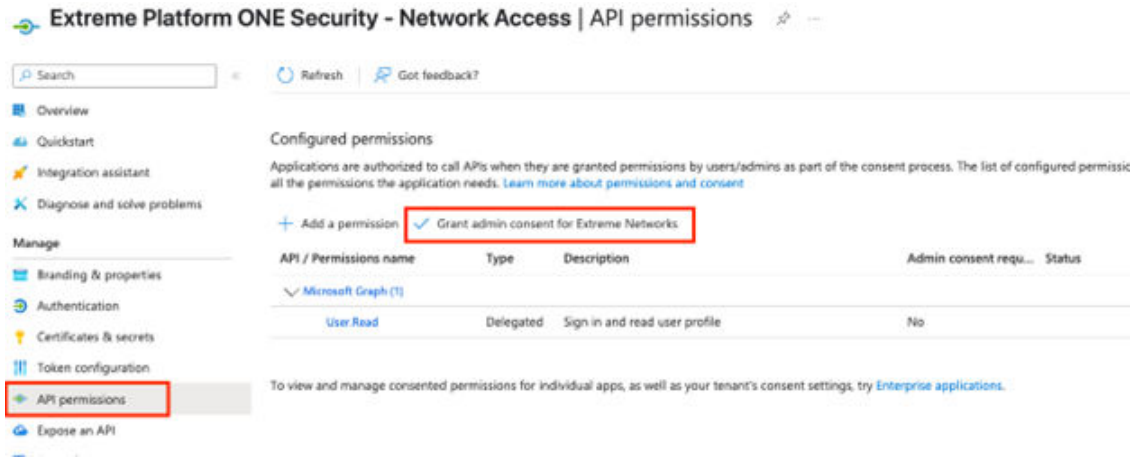



**Figure 29: API permissions**

**Extreme Platform ONE Security**

7. Go to **Administration and Settings** > **Access Management** > **Identity Providers** > **Network & Applications**.

8. Select **Add IdP Profile** and configure the settings in Table 203.

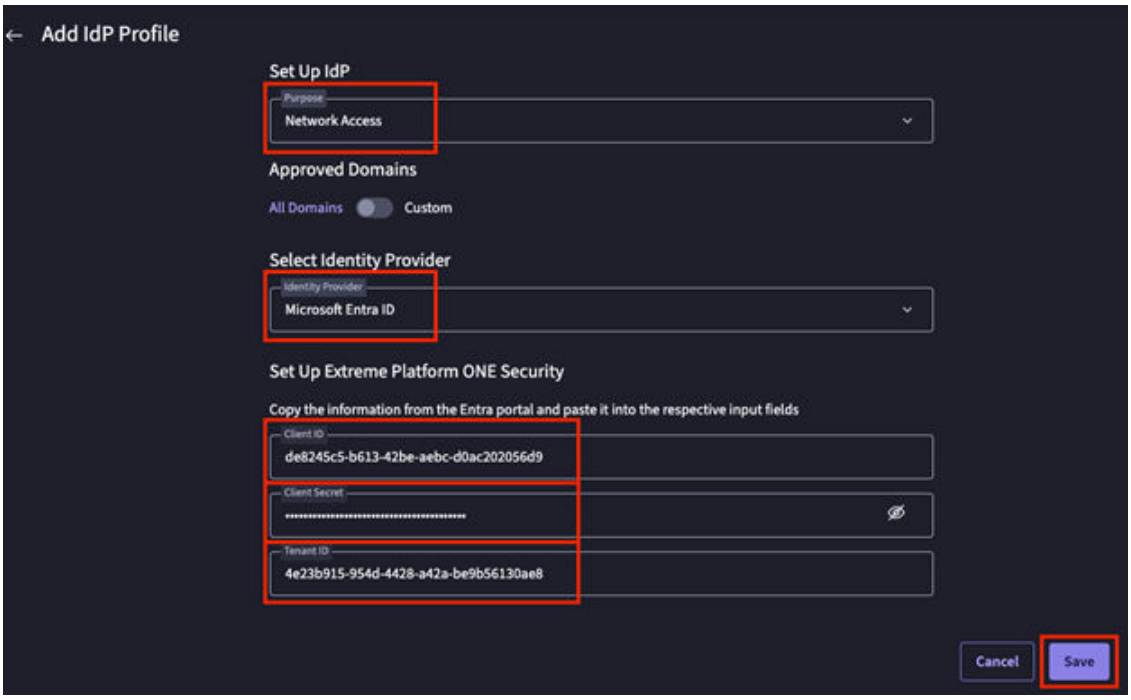



**Figure 30: Configuration Settings**

**Table 203: Entra ID IdP Profile Configuration Settings**

| Field | Description |
|---|---|
| Set Up IdP | Select **Network Access** from the Purpose drop-down list. |
| Approved Domains | If the domain needs to be limited, it can be selected here with the **Custom** toggle, otherwise leave it to **All Domains**. |
| Select Identity Provider | Select **Microsoft Entra ID** from the **Identity Provider** drop-down list. |
| Setup Guidelines | Paste the copied credentials from Microsoft Entra ID:<br>• Client ID<br>• Client Secret<br>• Tenant ID |

9. To complete the setup, select **Save**.

**Disable MFA in Microsoft Entra ID**

10. Go to **Manage** > **Properties** and configure the settings.
    a. Select **Manage Security defaults**.

b. Disable the toggle **Disabled** and select **Save**.

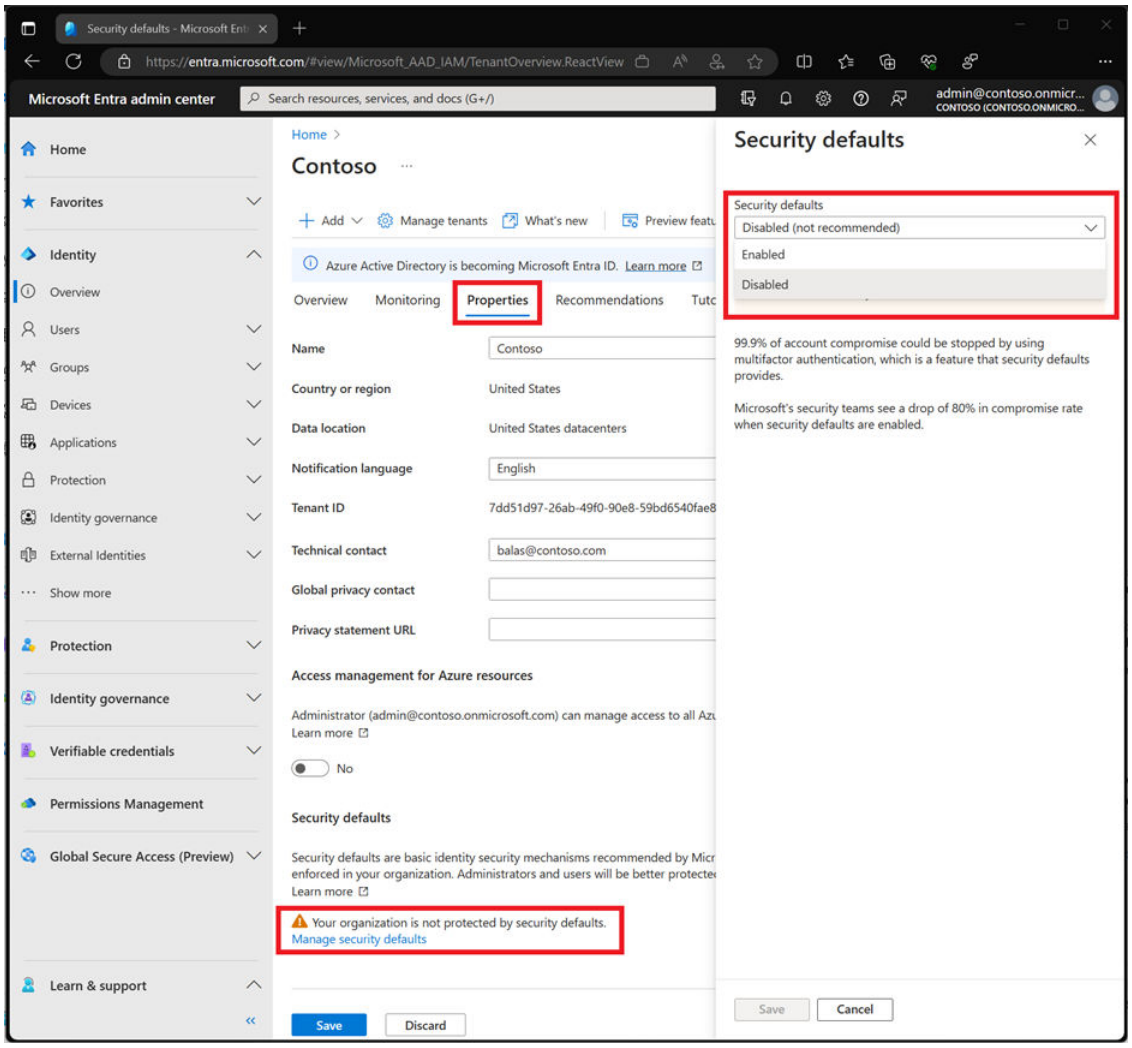



**Figure 31: Security defaults**

11. Go to **Identity** > **Protection** > **Conditional Access** and configure the settings in Table 204.

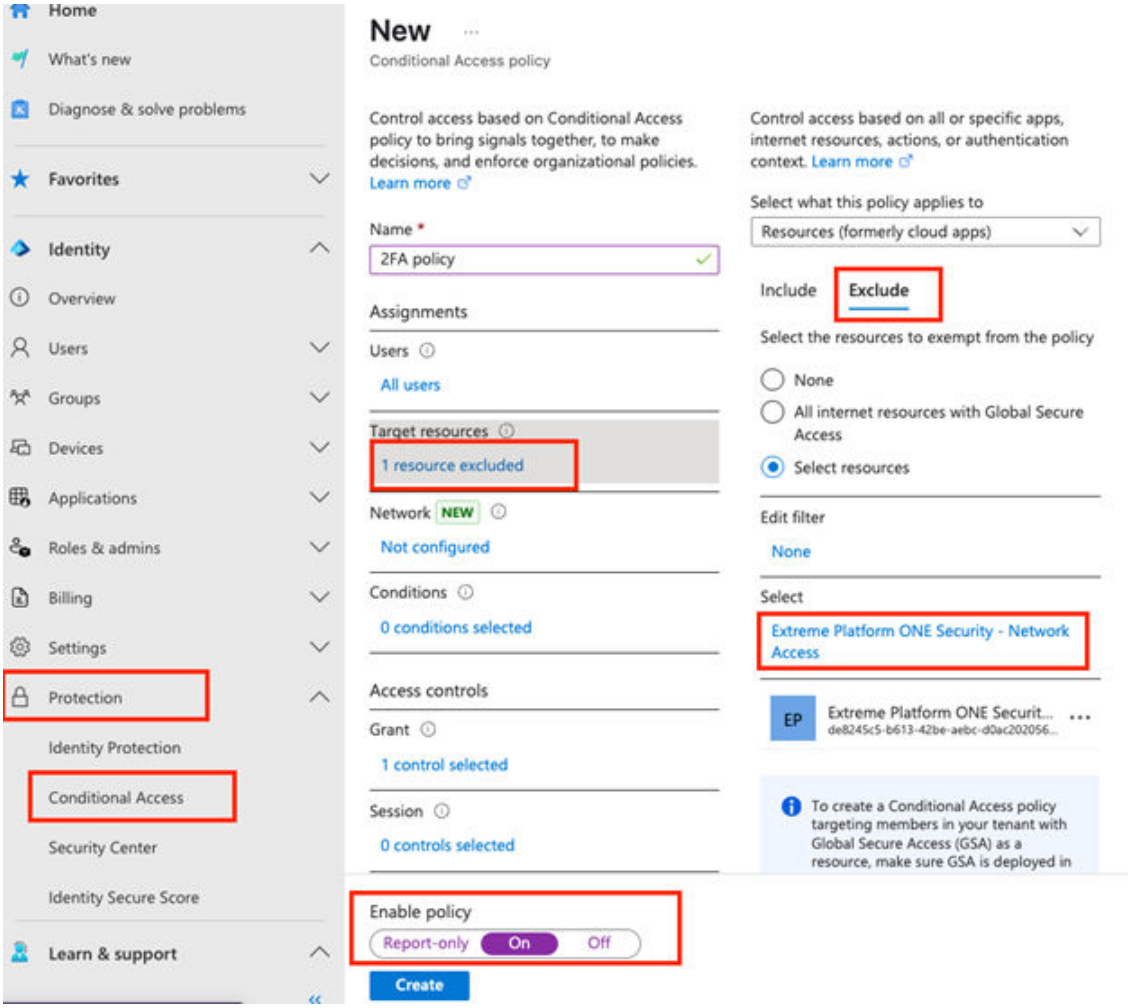



**Figure 32: Conditional Access policy**

**Table 204: Conditional Access Configuration Settings**

| Field | Description |
|---|---|
| User ad groups | Select **All users**. |
| Cloud apps or actions | Under **Exclude** select the OIDC app created earlier in the **Select excluded cloud apps**. |
| Grant | Select **Grant access** and check **Require multi-factor authentication** and any other settings your organization requires. |
| Enable policy | Set to **On**. |
| Select **Create**. | |

### Configure ExtremeCloud IQ (New) for Entra ID

Use this task to configure ExtremeCloud IQ (New) for Entra ID.

1. Log into your ExtremeCloud IQ (New) tenant.

2. Go to **Administration and Settings** > **Access Management** > **Identity Providers** > **Network & Applications**.
3. Select **Add IdP Profile** and configure the settings in Table 205.

**Table 205: Entra ID IdP Profile Configuration Settings**

| Field | Description |
|---|---|
| Set Up IdP | Select **Network Access** from the Purpose drop-down list. |
| Approved Domains | If the domain needs to be limited, it can be selected here with the **Custom** toggle, otherwise leave it to **All Domains** |
| Select Identity Provider | Select **Microsoft Entra ID** from the **Identity Provider** drop-down list. |
| Setup Guidelines | Paste the copied credentials from Microsoft Entra ID:<br>• Client ID<br>• Client Secret<br>• Tenant ID |

4. To complete the setup, select **Save**.

#### Disable MFA using a conditional Access Policy for Entra ID

Network Authentication requires that multi-factor authentication be disabled for an Entra ID application when using EAP-TTLS. If Entra ID premium is used, a rule can be created to exclude this only for the Network Access OIDC application. If Entra ID premium is not in use, this must be disabled for all users. For more information on Conditional Access Policies, refer to Microsoft documentation here: https://learn.microsoft.com/en-us/entra/identity/conditional-access/overview

1. Log in to Microsoft Entra ID.
2. Go to **Manage** > **Properties** and configure the settings.
   a. Select **Manage Security defaults**.
   b. Disable the toggle **Disabled** and select **Save**.
3. Go to **Identity** > **Protection** > **Conditional Access** and configure the settings in Table 206.

**Table 206: Conditional Access Configuration Settings**

| Field | Description |
|---|---|
| User ad groups | Select **All users**. |
| Cloud apps or actions | Under **Exclude** select the OIDC app created earlier in the **Select excluded cloud apps**. |
| Grant | Select **Grant access** and check **Require multi-factor authentication** and any other settings your organization requires. |
| Enable policy | Set to **On**. |
| Select **Create**. | |

*Microsoft ID | Application Access*

Application access for users can be authenticated via Microsoft Entra ID in two ways: OpenID Connect (OIDC) or SAML. The setup process is different in Entra ID depending on the type of integration being leveraged.

**Microsoft Entra ID | Application Access**

Application access for users can be authenticated via Microsoft Entra ID in two ways:

- OpenID Connect (OIDC)

  1. Retrieve Redirect URI in Extreme Platform ONE Security.
  2. Set up Microsoft Entra ID.
  3. Configure Extreme Platform ONE Security.

- SAML

  1. Retrieve identifier and Reply URL in Extreme Platform ONE Security.
  2. Configure Microsoft Entra ID.
  3. Finalize in Extreme Platform ONE Security.

The setup process is different in Microsoft Entra ID depending on the type of integration being used.

Optionally, you can enable Primary Refrest Token Authentication authentication for either SSO method. When enabled, in-app SSO login will use the Primary Refresh Token from the device's existing Microsoft Entra ID session, allowing users on Entra ID-joined devices to sign in seamlessly without being prompted for additional credentials.

1. Register the application in Microsoft Entra ID.
2. Enable Primary Refresh Token in Extreme Platform ONE Security.

**Application Access using Open ID Connect (OIDC)**

1. Retrieve Redirect URI In Extreme Platform ONE Security.
   a. Go to **Administration & Settings** > **Access Management** > **Identity Providers** > **Users**.
   b. To create a new profile, select **Add IdP Profile** and configure the settings in Table 207.

**Table 207: Entra ID Application Access OIDC IdP Profile Configuration Settings**

| Field | Description |
|---|---|
| Set Up IdP | Select **Application Access** from the Purpose drop-down list. |
| Approved Domain | If the domain needs to be limited, it can be selected here, otherwise leave it to **All Domains**. |
| Select Identity Provider | Select **Microsoft Entra ID** from the Identity Provider drop-down list. |
| Application Access | Select **OpenID Connect** from the Single Sign-On drop-down list. |

**Table 207: Entra ID Application Access OIDC IdP Profile Configuration Settings (continued)**

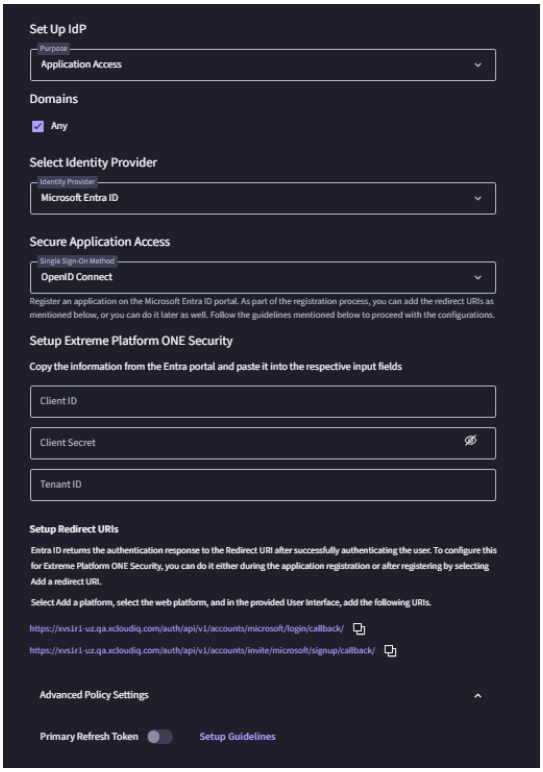
| Field | Description |
|---|---|
| Setup Redirect URIs | Copy the Redirect URI.<br><br><br>**Figure 33: Redirect URIs** |
| Advanced Policy Settings | Select **Advanced Policy Settings** to expand the section.<br>Enable the **Primary Refresh Token** toggle to allow Entra ID-joined devices to authenticate to applications using a Primary Refresh Token (PRT) acquired silently by the Windows Authentication Manager (WAM). When enabled, users are not prompted for separate credentials during application access.<br>Select **Setup Guidelines** for Microsoft Entra ID configuration steps required to support PRT authentication.<br><br>**Note:** The same app registration used for OIDC application access is also used for Primary Refresh Token authentication. A separate registration is not required.<br><br>Use the **Revocation Grace Period** setting to control how long the Extreme Platform ONE Security Agent waits for a user to complete interactive re-authentication after a Continuous Access Evaluation (CAE) revocation event is detected. If the user does not re-authenticate within the configured window, the agent logs the user out and sends the appropriate revocation event to NAC (ExtremeControl). |

**Table 207: Entra ID Application Access OIDC IdP Profile Configuration Settings (continued)**

| Field | Description |
|---|---|
| | Configure a value between 1 and 30 minutes. The default is 5 minutes. This setting is stored per tenant and does not affect other tenants.<br>To view setting changes, go to **Administration & Settings** > **Logs** within the Identity Provider Audit log. |

c. Select **Cancel**.

2. Set up Microsoft Entra ID.
   a. Go to **Applications** > **App registration** and select **New registration**.
   b. Under **Register an application**.
      i. Name the application appropriately for the Application Access Integration.
      ii. Leave the default fields selected and select **Register**.
   c. Select **Add a Redirect URI**.

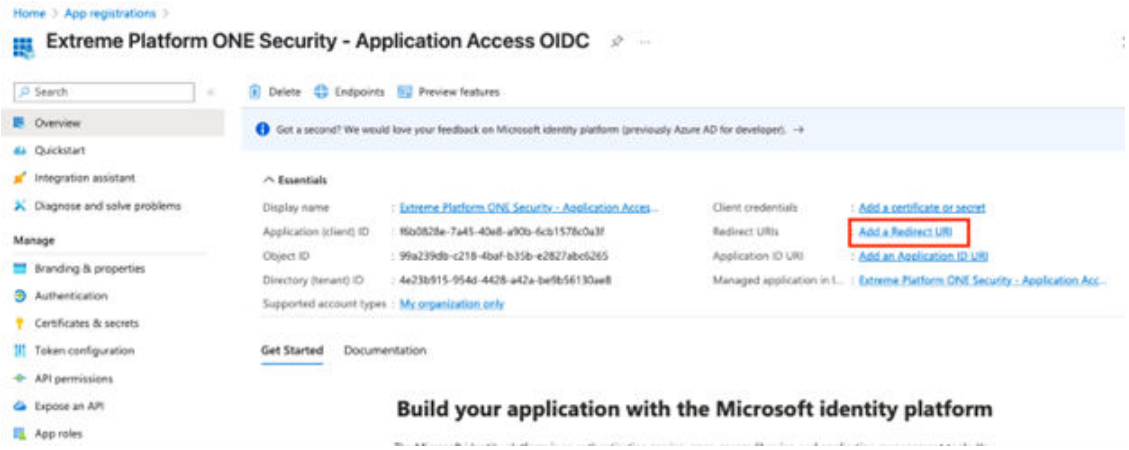



**Figure 34: Redirect URI**

d. Select **Add a platform** followed by **Web**.

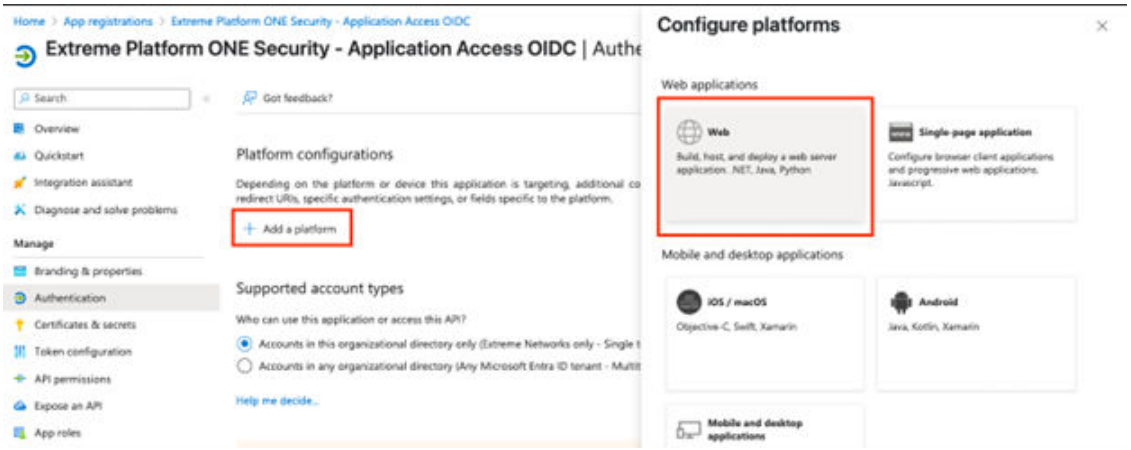



**Figure 35: Configure platforms**

e. Enter one of the Redirect URIs that was previously copied from ExtremeCloud IQ (New) and select **Configure**.

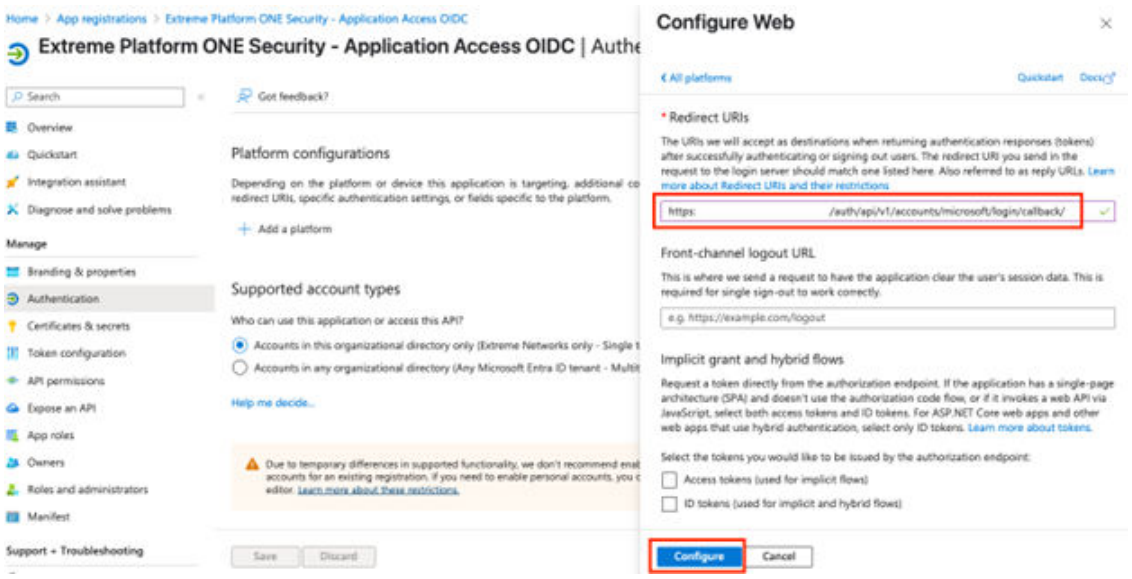



**Figure 36: Configure Web**

f. Select **Add URI**.
   i. Paste in the second Redirect URI that was copied from ExtremeCloud IQ (New).
   ii. Select **Save**.

g. Copy the **Application (client) ID** and **Directory (tenant) ID** for use later. Under **Client Credentials**, select **Add a certificate or secret**.

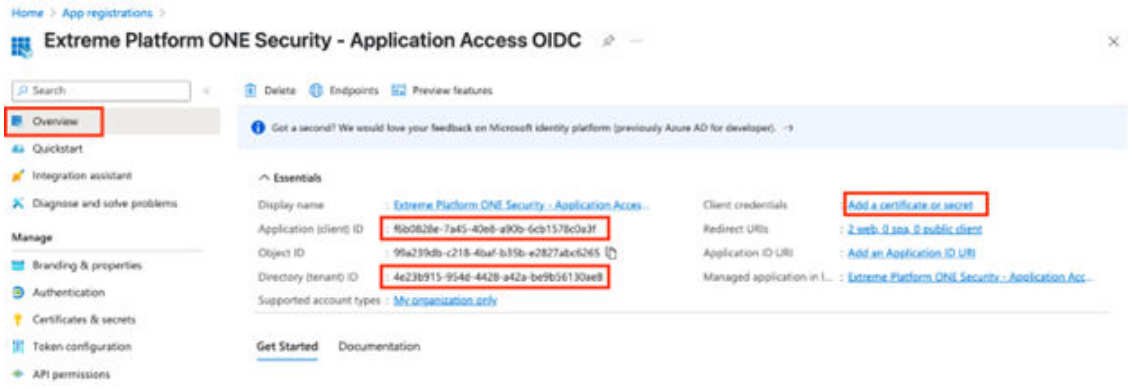



**Figure 37: Client credentials**

h. Select **New client secret**.
   i. Enter a description if desired and a preferred expiration date of the secret.
   ii. Once complete, select **Add**.
   iii. Copy the value of the new secret for use later.

i. Go to **Manage** > **API permissions** and select **Grant admin consent for <Company Name>**.

3. Configure Extreme Platform ONE Security.
   a. Go to **Administration and Settings** > **Access Management** > **Identity Providers** > **Network & Application**.
   b. Select **Add IdP Profile** and configure the settings in Microsoft Entra ID | Application Access on page 607.

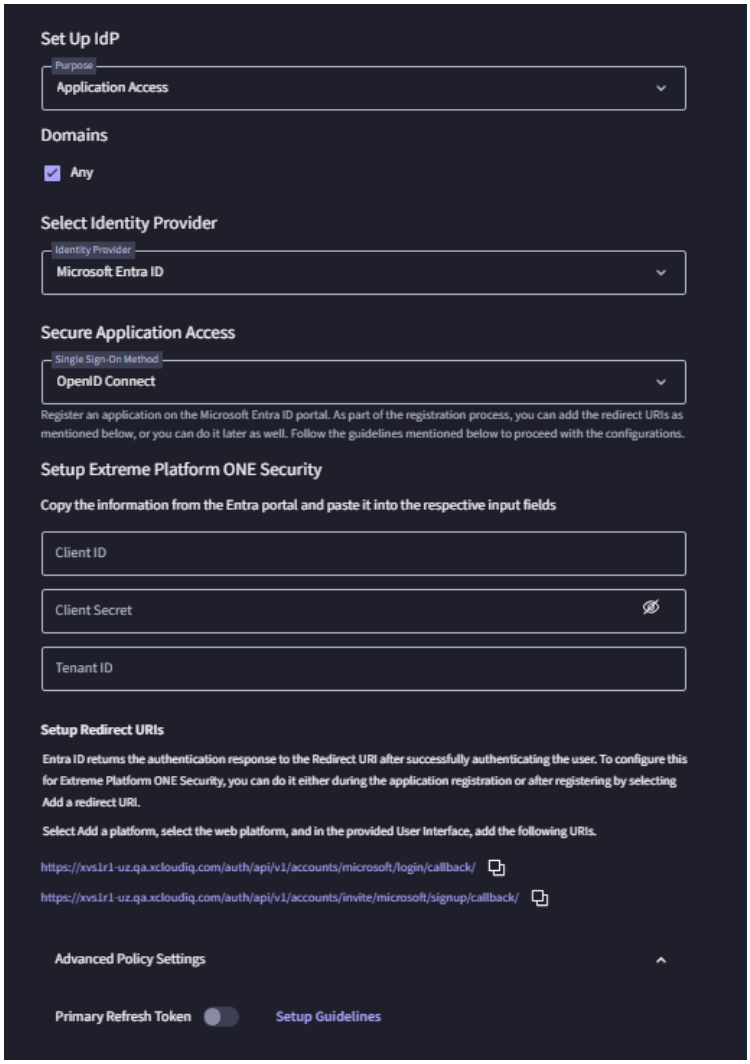



**Figure 38: IdP Profile settings**

**Table 208: Entra ID Application Access IdP Profile Configuration Settings**

| Field | Description |
|---|---|
| Set Up IdP | Select **Application Access** from the Purpose drop-down list. |
| Approved Domains | If the domain needs to be limited, it can be selected here with the **Custom** toggle, otherwise leave it to **All Domains** |
| Select Identity Provider | Select **Microsoft Entra ID** from the **Identity Provider** drop-down list. |

**Table 208: Entra ID Application Access IdP Profile Configuration Settings (continued)**

| Field | Description |
|---|---|
| Secure Application Access | Under **Single Sign-On Method**, select **OpenID Connect**. |
| Setup Extreme Platform ONE Security | Paste the copied credentials from Microsoft Entra ID:<br>• Client ID<br>• Client Secret<br>• Tenant ID |

c. To complete the setup, select **Save**.

**Application Access using SAML**

4. Retrieve identifier and Reply URL in Extreme Platform ONE Security.
   a. In ExtremeCloud IQ (New), go to **Administration & Settings** > **Access Management** > **Identity Providers** > **Users**.
   b. To create a new profile, select **Add IdP Profile** and configure settings in Table 208 on page 611.

**Table 209: Microsoft Entra ID SAML Preparation Configuration Settings**

| Field | Description |
|---|---|
| Set Up IdP | Select **Application Access** from the Purpose drop-down list. |
| Approved Domain | If the domain needs to be limited, it can be selected here, otherwise leave it to **All Domains**. |
| Select Identity Provider | Select **Microsoft Entra ID** from the Identity Provider drop-down list. |
| Single Sign-On Method | Select **SAML**. |

**Table 209: Microsoft Entra ID SAML Preparation Configuration Settings (continued)**

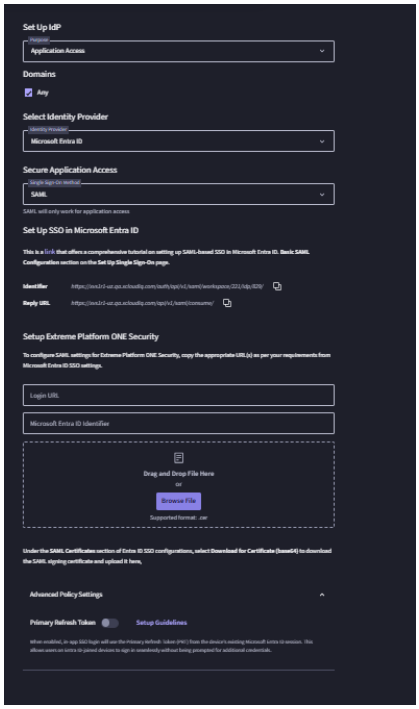
| Field | Description |
|---|---|
| Setup Up SSO in Microsoft Entra ID | Copy the Identifier and the Reply URL.<br><br>**Figure 39: Identifier and Reply URL** |
| Advanced Policy Settings | Select **Advanced Policy Settings** to expand the section.<br>Enable the **Primary Refresh Token** to allow in-app SSO login to use the Primary Refresh Token (PRT) from the device's existing Microsoft Entra ID session. This allows users on Entra ID-joined devices to sign in seamlessly without being prompted for additional credentials.<br>Select **Setup Guidelines** for Microsoft Entra ID configuration steps required to support PRT authentication.<br><br>**Note:** The same app registration used for OIDC application access is also used for Primary Refresh Token authentication. A separate registration is not required.<br><br>Use the **Revocation Grace Period** setting to control how long the Extreme Platform ONE Security Agent waits for a user to complete interactive re-authentication after a Continuous Access Evaluation (CAE) revocation event is detected. If the user does not re-authenticate within the configured window, the agent logs the user out and sends the appropriate revocation event to NAC (ExtremeControl).<br>Configure a value between 1 and 30 minutes. The default is 5 minutes. This setting is stored per tenant and does not affect other tenants. |

**Table 209: Microsoft Entra ID SAML Preparation Configuration Settings (continued)**

| Field | Description |
|---|---|
| | To view setting changes, go to **Administration & Settings** > **Logs** within the Identity Provider Audit log. |

**Note**
Leave this page open. If it is canceled, the Identifier will change, and this will need to be updated in the Microsoft Entra ID application.

c. Select **Save**.

5. Configure Microsoft Entra ID.
   a. Go to **Enterprise application** > **New application**.
   b. Select **Create your own application**.

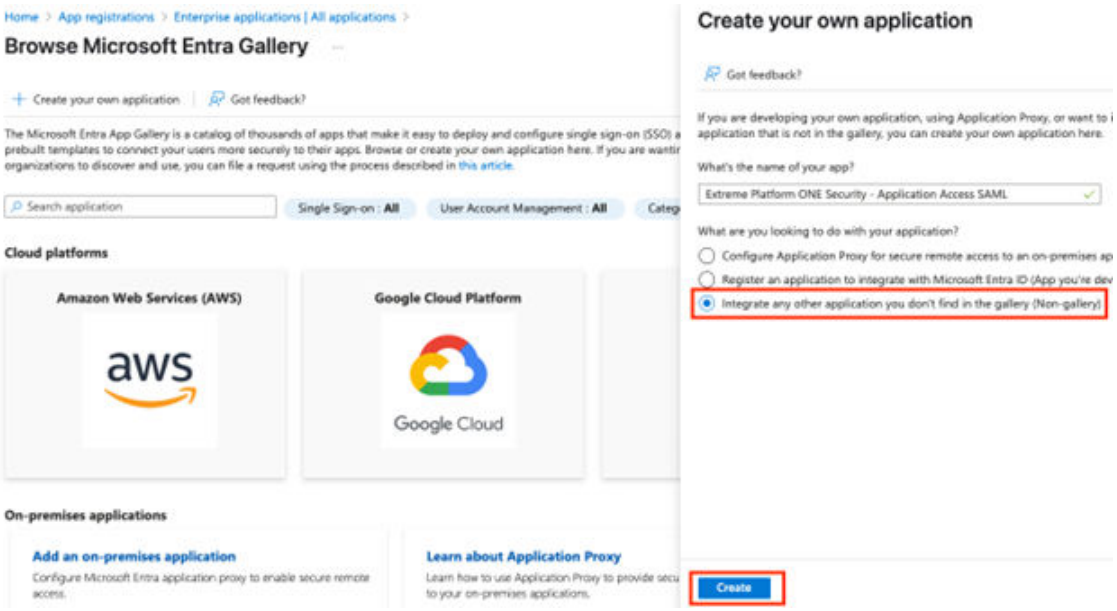



**Figure 40: Microsoft Entra Gallery**

i. Name the application so that it can be easily located.
ii. Select the **Non-gallery** option.

c. In the newly created application, select **Properties** and toggle **Assignment required** and **Visible Users** to **No**.

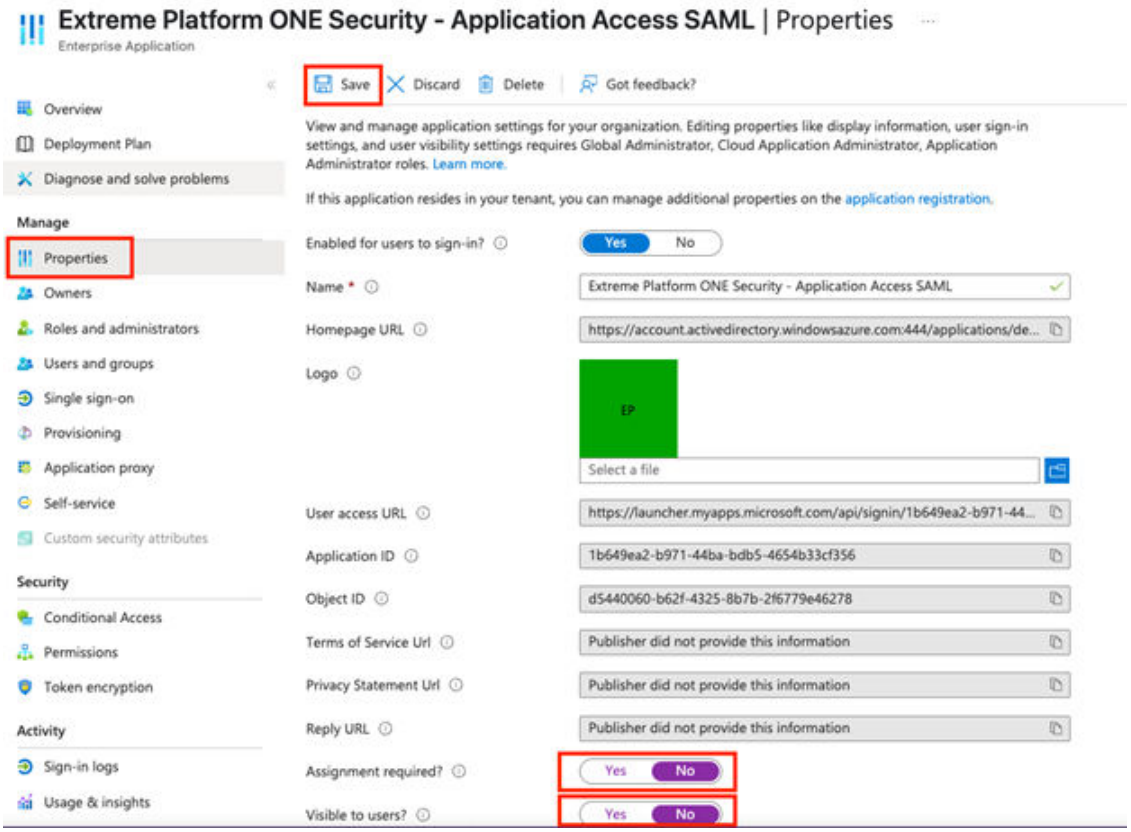



**Figure 41: Properties**

d. Go to **Manage** > **Single Sign-On** and select SAML.

e. Under **Basic SAML Configuration** select **Edit**.

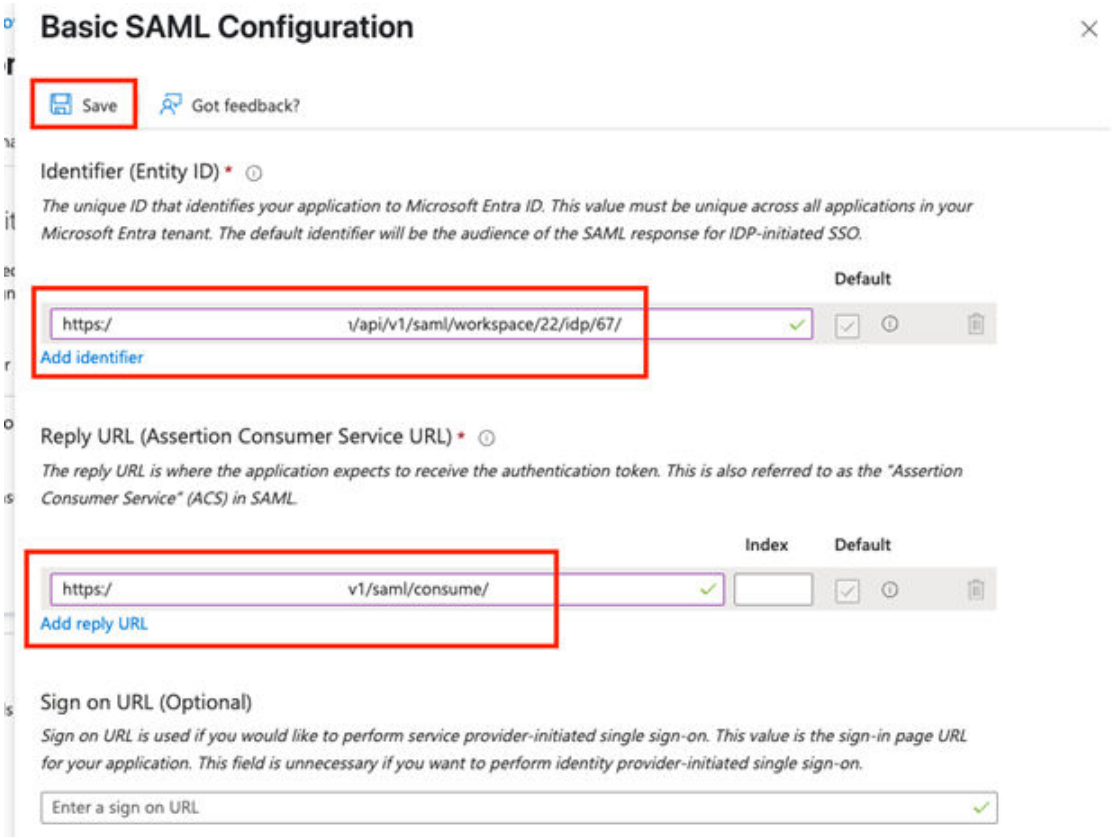



**Figure 42: Basic SAML Configuration**

i. Select **Add identifier** and paste in the Identifier from ExtremeCloud IQ (New) then select **Add reply URL** and paste in the **Reply URL** that was previously copied.
ii. Select **Save**.

iii. When prompted to test the integration, select **No, I'll test later**.

f. Further down the SAML application, download the SAML Certificate in Base64 format. Copy the Login URL and the Microsoft Entra Identifier.

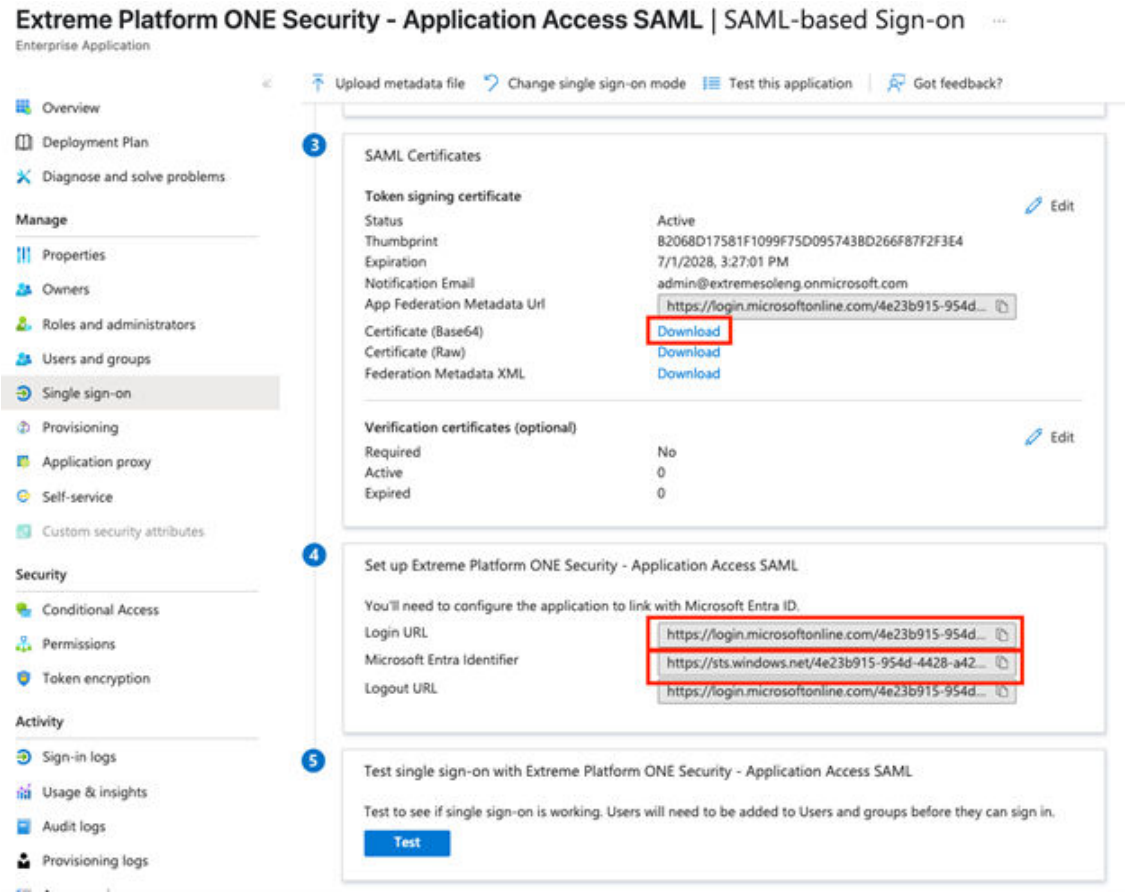



**Figure 43: SAML-based Sign-on**

6. Finalize in Extreme Platform ONE Security.
   a. In the **Application Access IdP** screen that was left open, paste in the Login URL, the Microsoft Entity ID Identifier, and upload the certificate that was downloaded. Select **Save**.

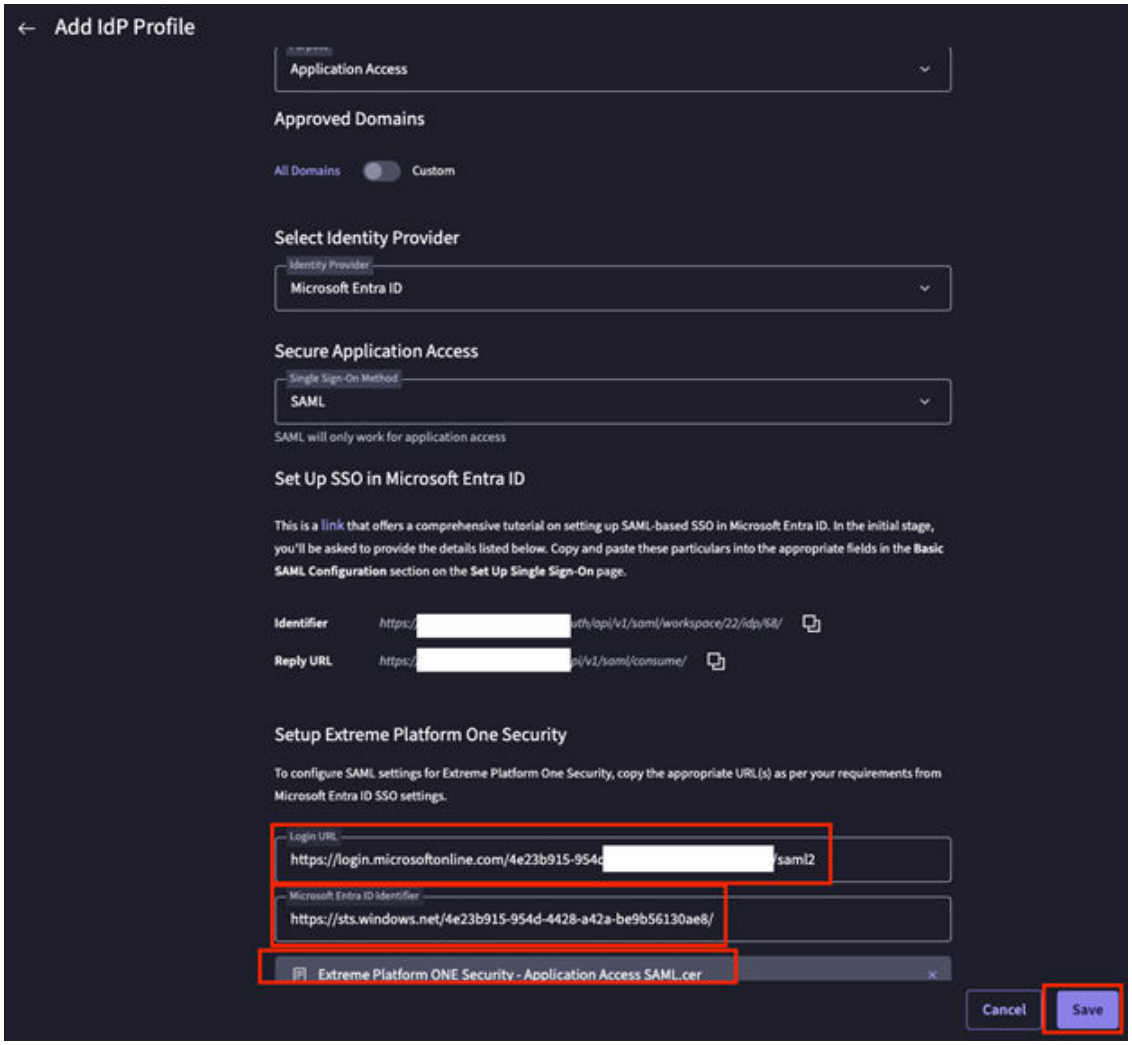



**Figure 44: Finalization**

**Note**
If this page was canceled, the Identifier will need to be updated in the Microsoft Entra ID application.

### Primary Refresh Token Authentication

7. Register the application in Microsoft Entra ID.

**Note**
The same app registration used for OIDC application access is also used for Primary Refresh Token authentication. Do not create a separate registration.

a. In Microsoft Entra ID, open the existing app registration created for OIDC application access and record the **Application (client) ID** from the Overview page.
b. Enable public client flows.
   i. Go to **Authentication** > **Settings**.
   ii. Set **Allow public client flows** to **Yes**.
c. Add redirect URIs.
   i. Go to **Authentication** > **Add a platform** > **Mobile and desktop applications**.
   ii. Enter the following redirect URI, replacing `[client_id]` with your Application (client) ID:
   ```
   ms-appx-web://microsoft.aad.brokerplugin/[client_id]
   ```
   iii. Enter the following Bundle ID:
   ```
   com.extremenetworks.ztna
   ```
d. Configure API permissions.
   i. Go to **App Registration** > **API permissions** > **Add a permission**.
   ii. Add the following Microsoft Graph delegated permission: **User.Read**.

   **Note**
   To send PRT events to NAC, enable the feature flag `prt_nac: true` and grant the additional Microsoft Graph delegated permission **Mail.Read**. This permission appears in the **Setup Guidelines** when the feature flag is enabled.

   iii. Select **Grant admin consent for {tenant}**.

8. Enable Primary Refresh Token in ExtremeCloud IQ (New).
   a. Go to **Administration and Settings** > **Access Management** > **Identity Providers** > **Network & Applications** and open the existing Microsoft Entra ID OIDC IdP profile.
   b. Select **Advanced Policy Settings** to expand the section.
   c. Enable the **Primary Refresh Token** toggle.
   d. Enter a **Revocation Grace Period** value between 1 and 30 minutes. The default is 5 minutes.

      This setting controls how long the Extreme Platform ONE Security Agent waits for a user to complete interactive re-authentication after a Continuous Access Evaluation (CAE) revocation event is detected. If the user does not re-authenticate within the configured window, the agent logs the user out and sends the appropriate revocation event to NAC (ExtremeControl).

      **Note**
      This setting is stored per tenant and does not affect other tenants.

      To view setting changes, go to **Administration & Settings** > **Logs** within the Identity Provider Audit log.
   e. Select **Save**.

#### Configure Microsoft Entra ID Application Access

Use this task to configure Microsoft Entra ID Application Access.

1. In Microsoft Entra ID go to **Applications** > **App registration** and select **New registration**.
2. Under **Register an application**, name the application appropriately for the Application Access Integration. Leave the default fields selected and select **Register**.
3. Select **Add a Redirect URI**.
4. Select **Add a platform** followed by **Web**.
5. Enter one of the Redirect URIs that was previously copied from ExtremeCloud IQ (New) and select **Configure**.
6. Select Add URI and paste in the second Redirect URI that was copied from ExtremeCloud IQ (New). Select **Save**.
7. Copy the **Application (client) ID** and **Directory (tenant) ID** for use later. Under **Client Credentials**, select **Add a certificate or secret**.
8. Select **New client secret**. Enter a description if desired and a preferred expiration date of the secret. Once complete, select **Add**.
9. Copy the value of the new secret for use later.
10. Go to **Manage** > **API permissions** and select **Grant admin consent for <Company Name>**.

#### Configure ExtremeCloud IQ (New) for Microsoft Entra ID Application Access

Use this task to configure ExtremeCloud IQ (New) for Microsoft Entra ID Application Access.

1. Log into your ExtremeCloud IQ (New) tenant.
2. Go to **Administration and Settings** > **Access Management** > **Identity Providers** > **Network & Application**.
3. Select **Add IdP Profile** and configure the settings in Table 210.

**Table 210: Entra ID Application Access IdP Profile Configuration Settings**

| Field | Description |
|---|---|
| Set Up IdP | Select **Application Access** from the Purpose drop-down list. |
| Approved Domains | If the domain needs to be limited, it can be selected here with the **Custom** toggle, otherwise leave it to **All Domains** |
| Select Identity Provider | Select **Microsoft Entra ID** from the **Identity Provider** drop-down list. |
| Secure Application Access | Under **Single Sign-On Method**, select **OpenID Connect**. |
| Setup Extreme Platform One Security | Paste the copied credentials from Microsoft Entra ID:<br>• Client ID<br>• Client Secret<br>• Tenant ID |

4. To complete the setup, select **Save**.

#### Microsoft Entra ID Application Access using SAML

For SAML integration, the preparation in ExtremeCloud IQ (New), followed by the configuration in Entra ID, and a finalization in ExtremeCloud IQ (New).

#### Configure ExtremeCloud IQ (New) Microsoft Entra ID SAML Preparation

Prior to configuring the SAML application in Microsoft Entra ID, an Identifier and Reply URL will be needed from ExtremeCloud IQ (New).

1. In ExtremeCloud IQ (New), go to **Administration & Settings** > **Access Management** > **Identity Providers** > **Users**.
2. To create a new profile, select **Add IdP Profile** and configure settings in Table 211.

**Table 211: Microsoft Entra ID SAML Preparation Configuration Settings**

| Field | Description |
|---|---|
| Set Up IdP | Select **Application Access** from the Purpose drop-down list. |
| Approved Domain | If the domain needs to be limited, it can be selected here, otherwise leave it to **All Domains**. |
| Select Identity Provider | Select **Microsoft Entra ID** from the Identity Provider drop-down list. |
| Single Sign-On Method | Select **SAML**. |
| Setup Up SSO in Microsoft Entra ID | Copy the Identifier and the Reply URL. |

**Note**
Leave this page open. If it is canceled, the Identifier will change, and this will need to be updated in the Microsoft Entra ID application.

3. Select **Save**.

#### Configure Microsoft Entra ID SAML

Use his task to configure Microsoft Entra ID SAML.

1. Log in to Microsoft Entra ID and go to **Enterprise application** > **New application**.
2. Select **Create your own application**. Name the application so that it can be easily located. Select the **Non-gallery** option.
3. Go to **Manage** > **Single Sign-On** and select SAML.
4. Under **Basic SAML Configuration** select **Edit**.
5. Select **Add identifier** and paste in the Identifier from ExtremeCloud IQ (New) then select **Add reply URL** and paste in the **Reply URL** that was previously copied. Select **Save**.
6. When prompted to test the integration, select **No, I'll test later**.
7. Further down the SAML application, download the SAML Certificate in Base64 format. Copy the Login URL and the Microsoft Entra Identifier.

#### Configure ExtremeCloud IQ (New) Microsoft Entra ID SAML Finalization

Use this task to complete the final Microsoft Entra ID SAML configuration in ExtremeCloud IQ (New).

In the **Application Access IdP** screen that was left open, paste in the Login URL, the Microsoft Entity ID Identifier, and upload the certificate that was downloaded. Select **Save**.

**Note**
If this page was canceled, the Identifier will need to be updated in the Microsoft Entra ID application.

## Google Workspace

There are three primary purposes for integrating with an Identity Provider for ExtremeCloud IQ (New). The applications created in the Identity Provider are to be different even if the type is the same, however they can be reused if desired.

The purposes are:

- User and User Group Synchronization – Used to make users and user groups available within ExtremeCloud IQ (New) for policy assignment.

  **Note**
  Synced User cannot be removed from Extreme Platform ONE Security. It must be removed from the Identity Provider and then a syncing cycle should be initiated again. For Google this can be initiated on the IdP page.

- Application Access authentication – Used for logging into the ExtremeCloud IQ (New) Agent or the End User web portal.
- Network Access authentication – Used for 802.1X EAP-TTLS authentication of clients on access points and switches.

*Google Workspace | Synchronize Users and Groups*

User and User Group synchronization is performed using the Directory APIs in Google Workspace. They are retrieved on a polled basis from ExtremeCloud IQ (New).

#### Google Workspace | Synchronize Users and User Groups

User and User Group synchronization is performed using the Directory APIs in Google Workspace. They are retrieved on a polled basis from ExtremeCloud IQ (New).

To synchronize user and user groups using Google Workspace:

1. Configure Google Cloud.
2. Configure in Google Admin Console.
3. Configure Extreme Platform ONE Security.
4. Adjust Security Defaults for Google Workspace.

**Note**
In cases where a newer Google Workspace or Google Cloud Platform instance was created, security defaults may be enabled so that the administrator cannot download keys for service accounts. If this is the case, use this task to adjust security defaults for Google Workspace.

**Configure Google Workspace.**

1. Log into Google Cloud via https://console.cloud.google.com.
2. To create a new project, from the drop-down menu at the top of the screen and select **New Project**.

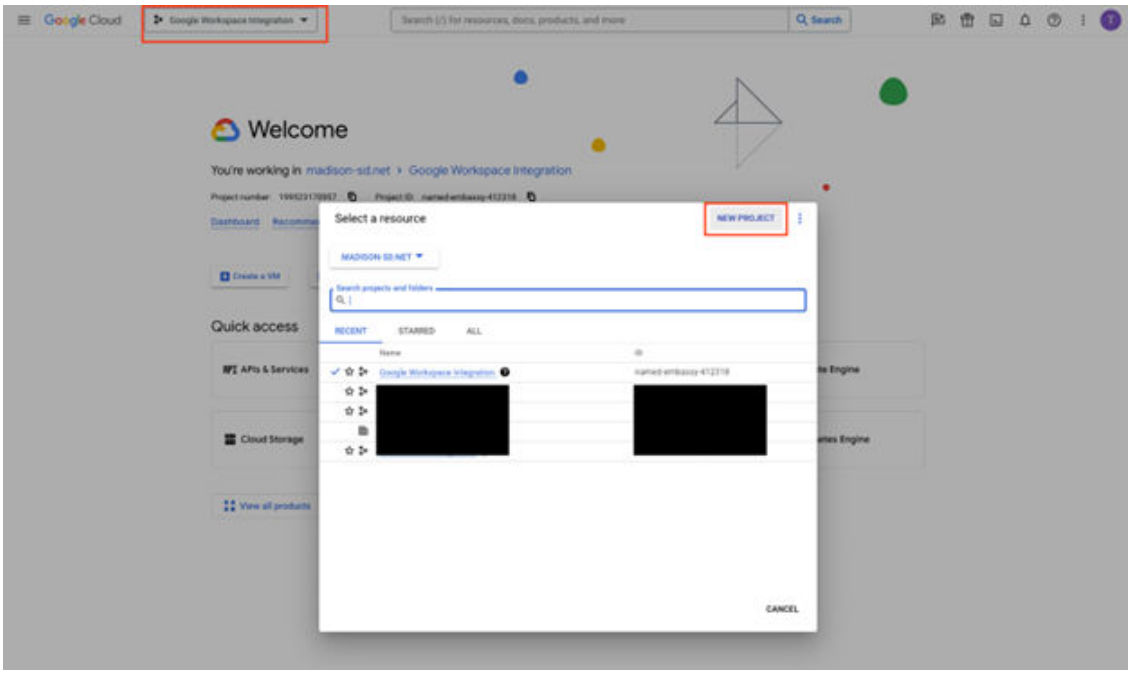



**Figure 45: New Project**

a. Name the project appropriately and select **Create**.
b. Under **Quick Access**, select **APIs & Services**.
c. Select **ENABLE APIS AND SERVICES**.

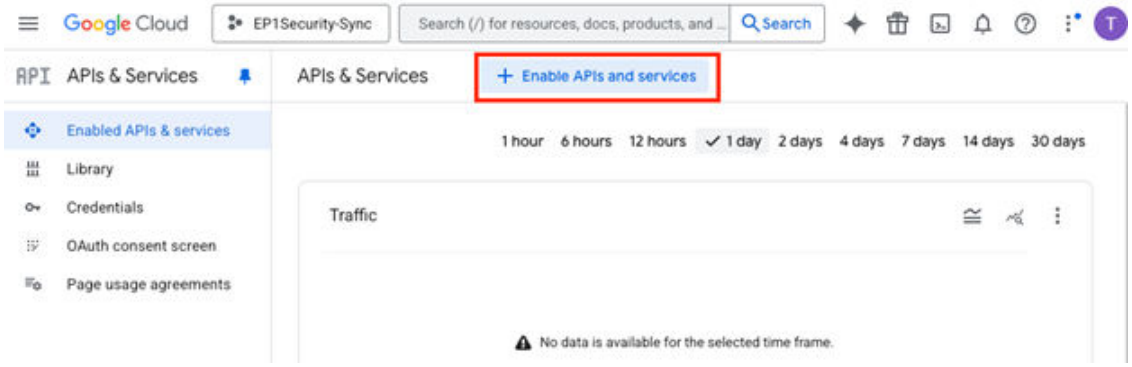



**Figure 46: API & Services**

d. In the search field, enter and select **Admin SDK API**.

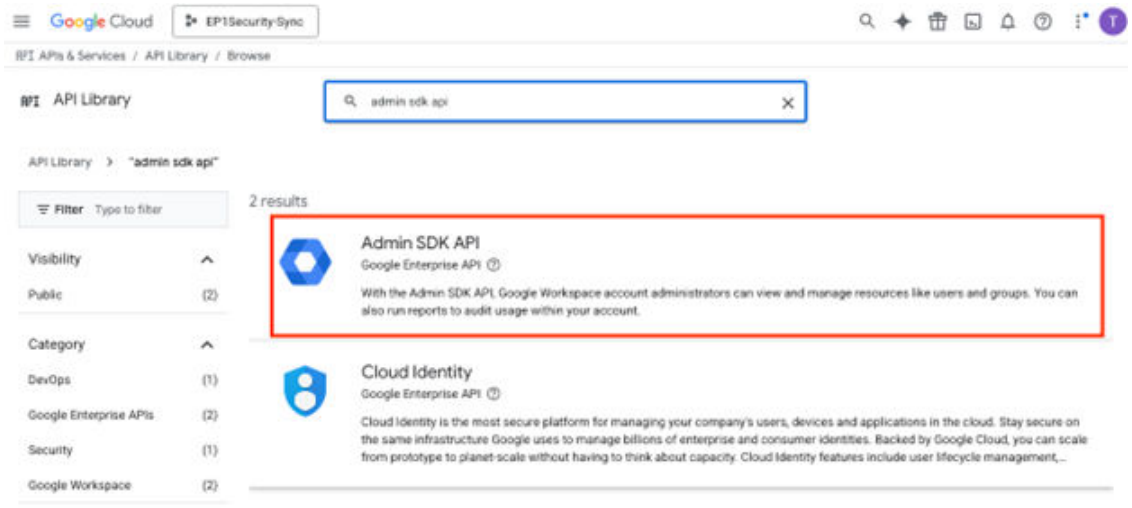



**Figure 47: Admin SDK API**

e. Select **ENABLE**.

3. Go to **APIS and SERVICES** > **Credentials**.
4. Select **CREATE CREDENTIALS** and from the drop-down select **Service account**.

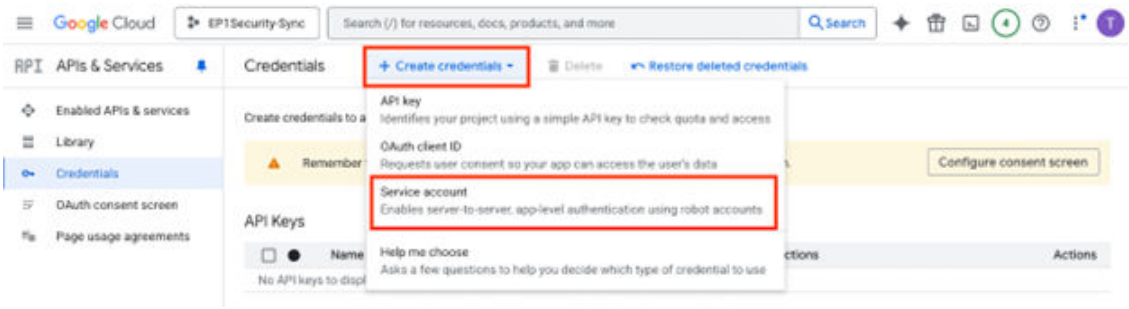



**Figure 48: Create credentials**

a. Enter a service account name to use for the syncing. Select **CREATE AND CONTINUE**, then leave the optional fields blank.
b. Select **DONE**.

c. Select the newly created service account. Copy the Email and Unique ID to be used in later steps and select **KEYS**.

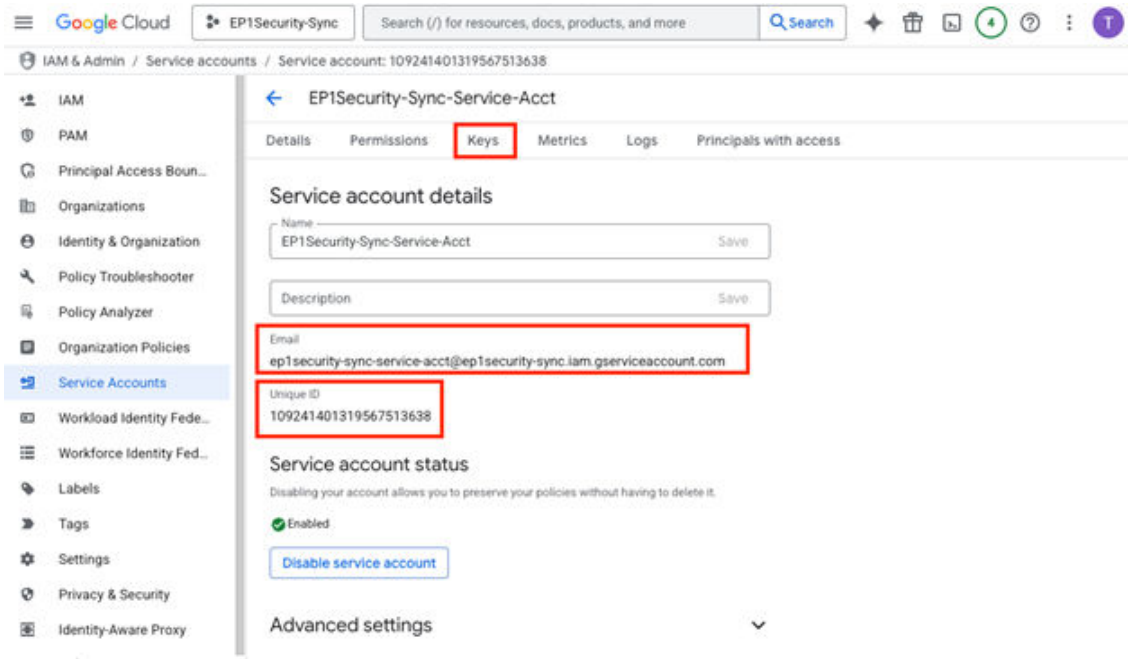



**Figure 49: Keys**

5. From the **ADD KEY** drop-down menu, select **Create new key**.

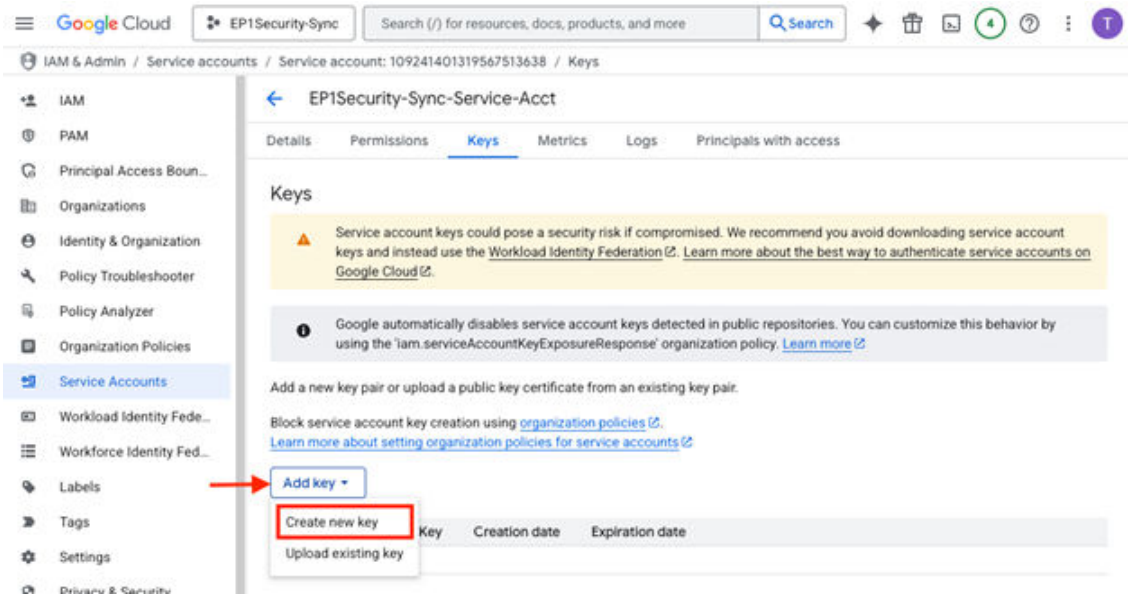



**Figure 50: New Key**

a. In the **Create Private Key** screen, select JSON as the key type and **CREATE**. This will download the private key to be used.

**Note**
If an error is received here due to a permissions issue, see <enter a link to the new security topic>. This restriction appears for newly created Google Cloud Accounts.

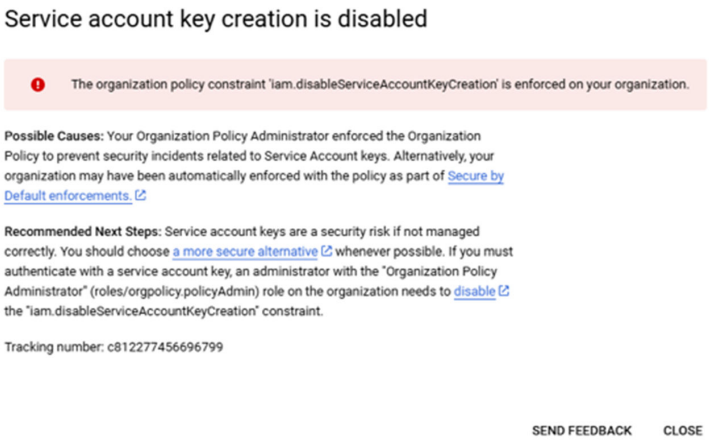



**Figure 51: Permissions Error**

## Google Admin Console Configuration

6. Log into Google Admin Console via https://admin.google.com.
7. Go to **Security** > **Access and data control** > **API controls** and select **MANAGE DOMAIN WIDE DELEGATION**.

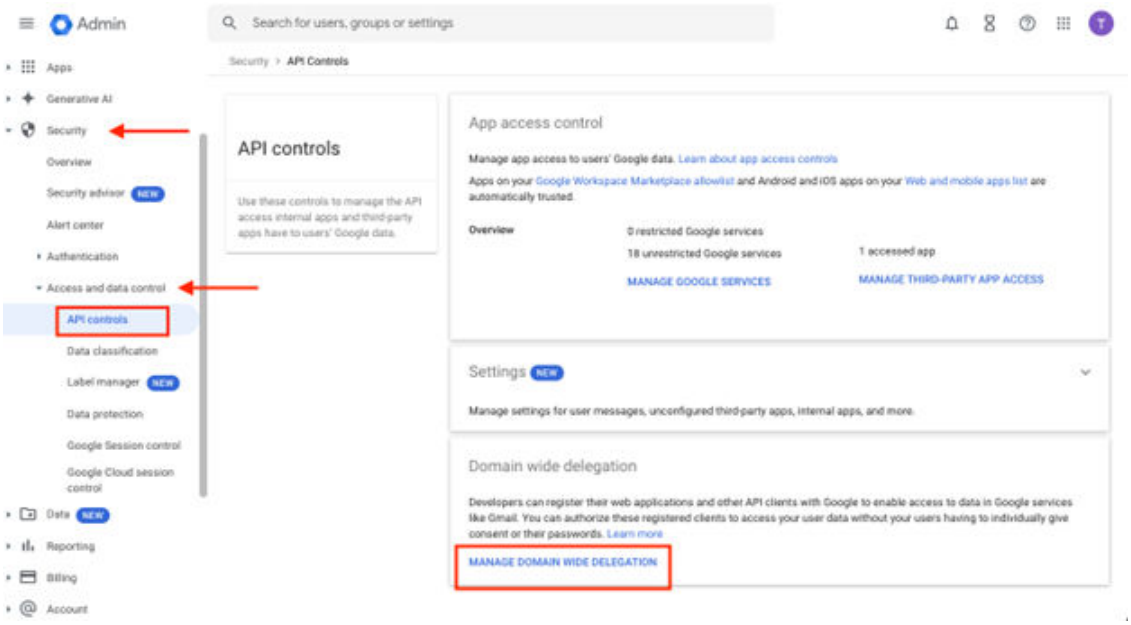



**Figure 52: API Controls**

8. Under **API clients**, select **Add new** and configure the settings in Table 212.

**Table 212: API Client Configuration Settings**

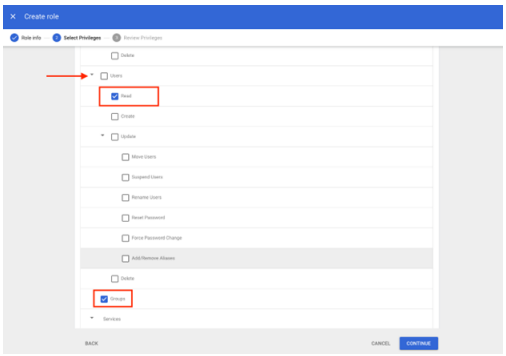
| Field | Description |
|---|---|
| Client ID | Enter the Unique ID that was previously copied from the Service Account entry. |
| OAuth Scopes | https://www.googleapis.com/auth/admin.directory.user<br><br>https://www.googleapis.com/auth/admin.directory.group.member<br><br>https://www.googleapis.com/auth/admin.directory.group<br><br>https://www.googleapis.com/auth/admin.directory.user.alias |

9. Select **AUTHORIZE**.
10. Go to **Account** > **Admin roles**.
    a. If no User and User Group with read privileges appears, select **Create role** and configure the settings in Table 213.

**Table 213: Role Configuration Settings**

| Field | | Description |
|---|---|---|
| Role Info | Name | Enter a group name. |
| | Description (Optional) | Enter a role description. |

**Table 213: Role Configuration Settings (continued)**

| Field | | Description |
|---|---|---|
| Select **CONTINUE**. | | |
| Select Privileges | Users | Within this group select **Read**.  **Figure 53: Privileges** |
| | Groups | |
| Select **CONTINUE**. | | |
| Review Admin API Privileges | | The review screen confirms that Read privileges are allowed for API calls for Users and Groups. |
| Select **CREATE ROLE**. | | |

b. If the role was just created, select Assign service accounts. If not, select **Assign role** > **Assign service accounts**.

c. Enter the email of the service account, select **ADD** then **ASSIGN ROLE**.

11. Go to **Account** > **Account Settings** and copy the Customer ID of Google Workspace.

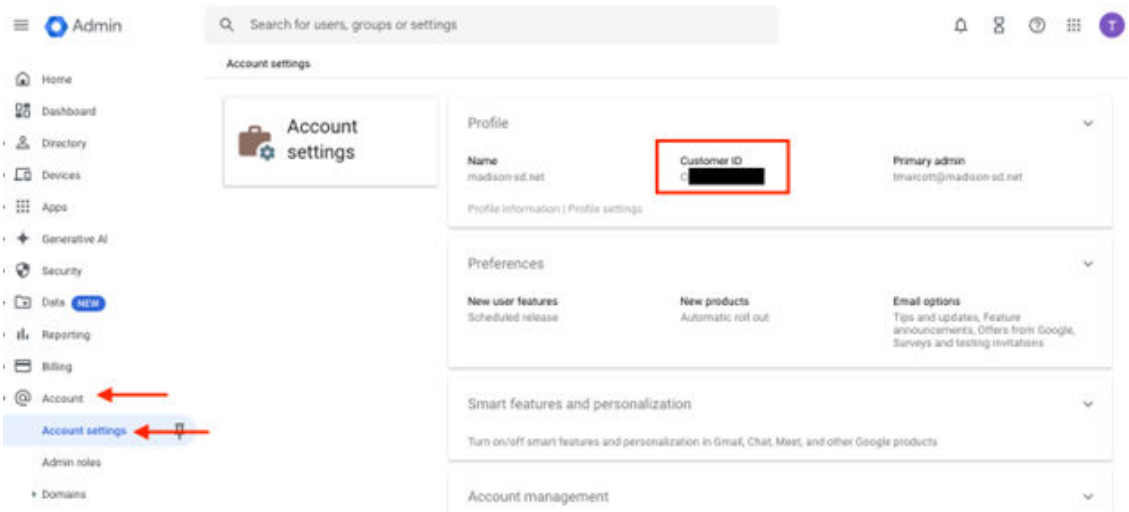



**Figure 54: Customer ID**

**Extreme Platform ONE Security Configuration**

12. Go to **Administration and Settings** > **Access Management** > **Identity Providers** > **Network & Applications**.
13. Select **Add IDP Profile** and configure the settings in Table 214.

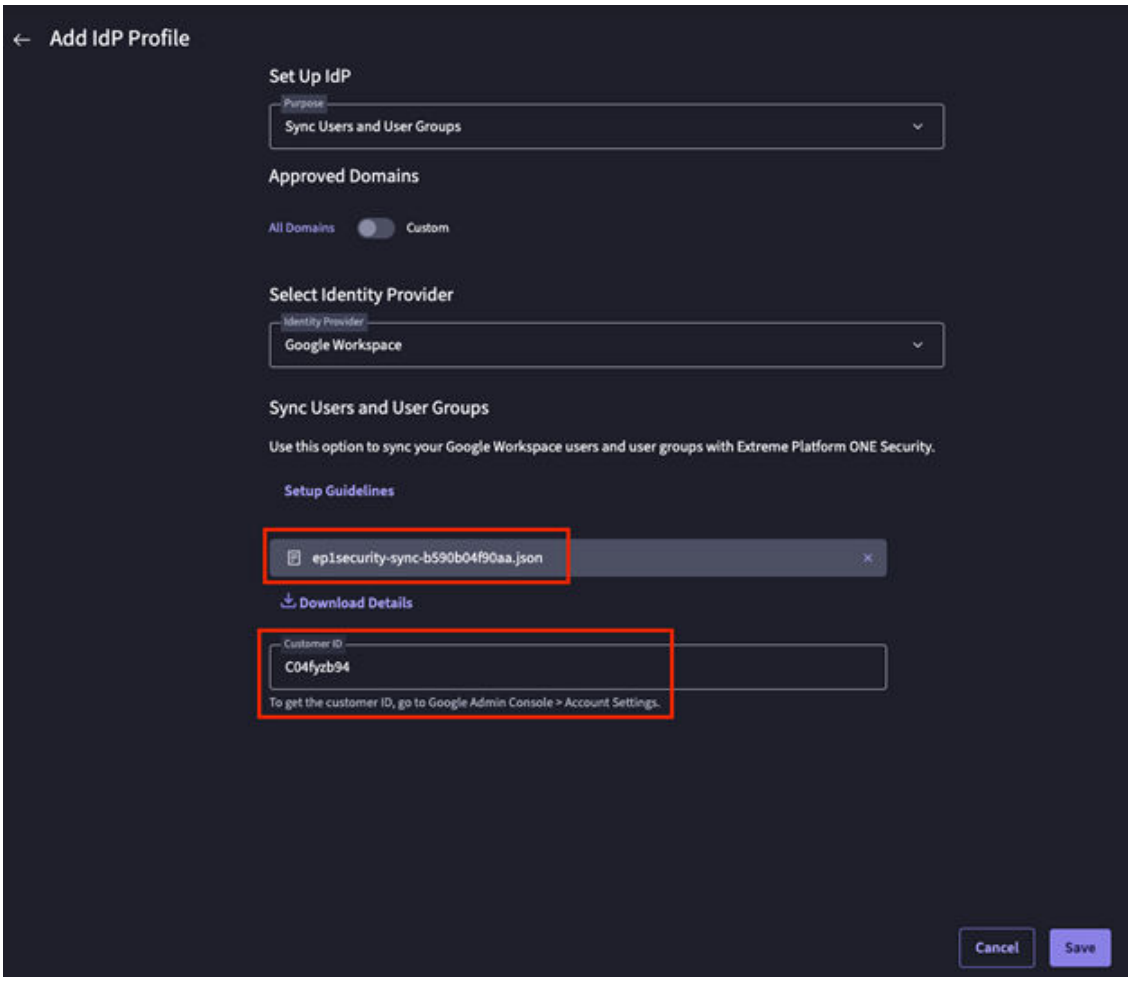



**Figure 55: IdP Profile**

**Table 214: Google Workspace IdP Profile Configuration Settings**

| Field | Description |
|---|---|
| Set Up IdP | Select **Sync Users and User Groups** from the Purpose drop-down list. |
| Domains | If the domain needs to be limited, it can be selected here with the **Custom** toggle, otherwise leave it to **All Domains** |

**Table 214: Google Workspace IdP Profile Configuration Settings (continued)**

| Field | Description |
|---|---|
| Select Identity Provider | Select **Google Workspace** from the **Identity Provider** drop-down list. |
| Sync Users and User Groups | Use this option to sync your Google Workspace users and user groups with ExtremeCloud IQ (New).<br>• Setup Guidelines - Upload the private key JSON file that was downloaded from Google Cloud Console and paste in the Customer ID that was saved from the Google Admin Console.<br>• Customer ID - To get the Customer ID, go to the Google Admin Console, under **Account Settings**.<br>• Select User Groups (Google Workspace Only) - Select group-specific APs and sync only those groups.The table retrieves all available groups.<br>a. Select available groups and select the side arrow to them to the **Added** box.<br>**Note:** There is no maximum for added groups.<br>b. Select **Save**.<br>c. To view synced users, go to **Policy** > **Users & Devices**, under **Users** and Google Workspace appears in the **Type** column.<br>d. Under **User Groups**, from the 3-dot menu, select **Sync Now** to view new groups.<br>e. To view the sync event details, go to **Administration & Settings** > **Logs**, select **Security Logs** from the drop-down menu. |

**Adjust Security Defaults for Google Workspace**

14. Log into Google Cloud via https://console.cloud.google.com.

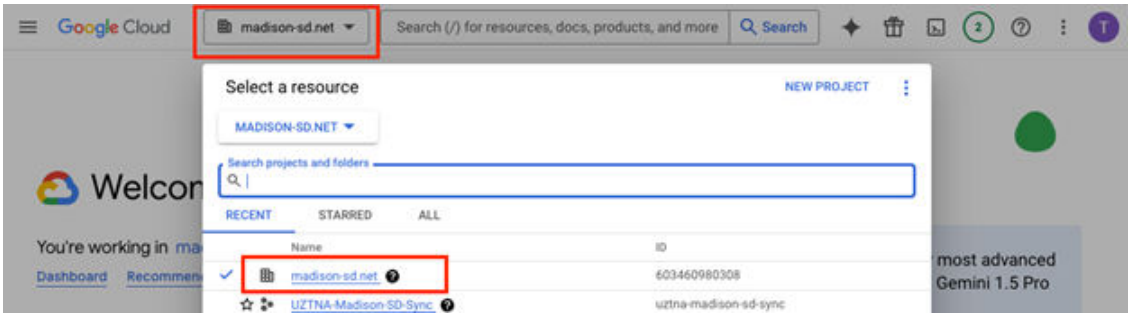



**Figure 56: Google Cloud**

15. From the top left, if you are already in a project, select the parent project from the drop-down list.
16. Go to **IAM & Admin** > **IAM**.

17. Under **IAM**, ensure that your account has an Organization Policy Administrator. If it does not, select Edit (pencil icon) next to your account to edit the roles. If your account isn't listed here, to add it select **GRANT ACCESS** and configure settings:

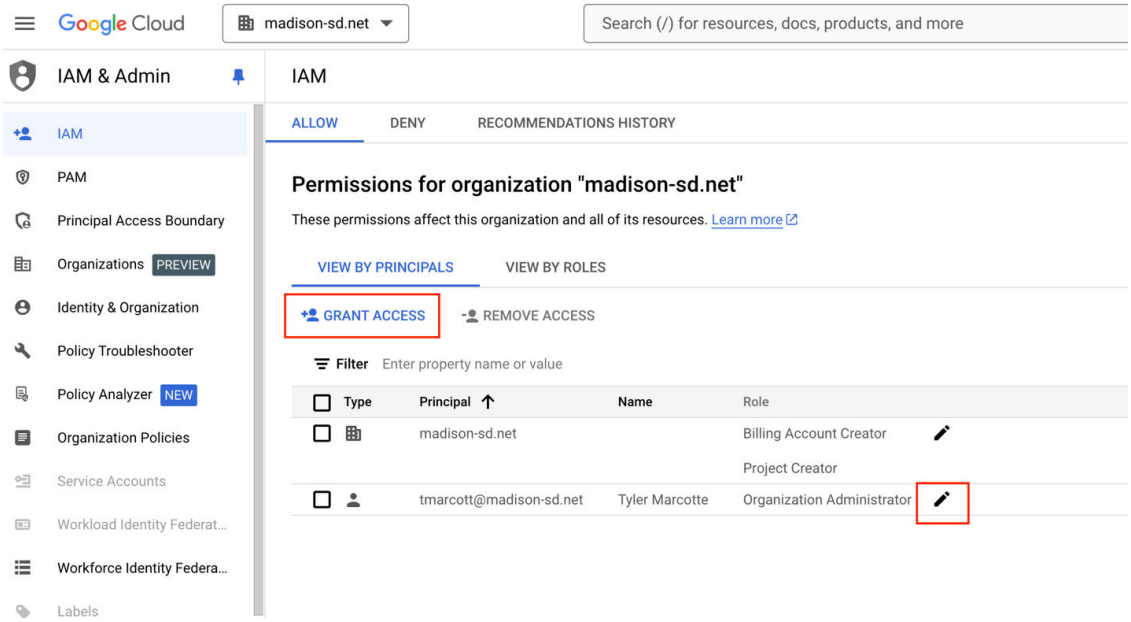



**Figure 57: Grant Access**

   a. Within the **Edit** window, select **Add Another Role**.
   b. Select the **Organization Policy Administrator** condition from the drop-down list.
   c. Select **SAVE**.
18. Once the roles are set, go to **Organization Policies** > **IAM & Admin**.
19. In the Organization Policies, search for iam.disableServiceAccountKeyCreation. Select edit to make updates.

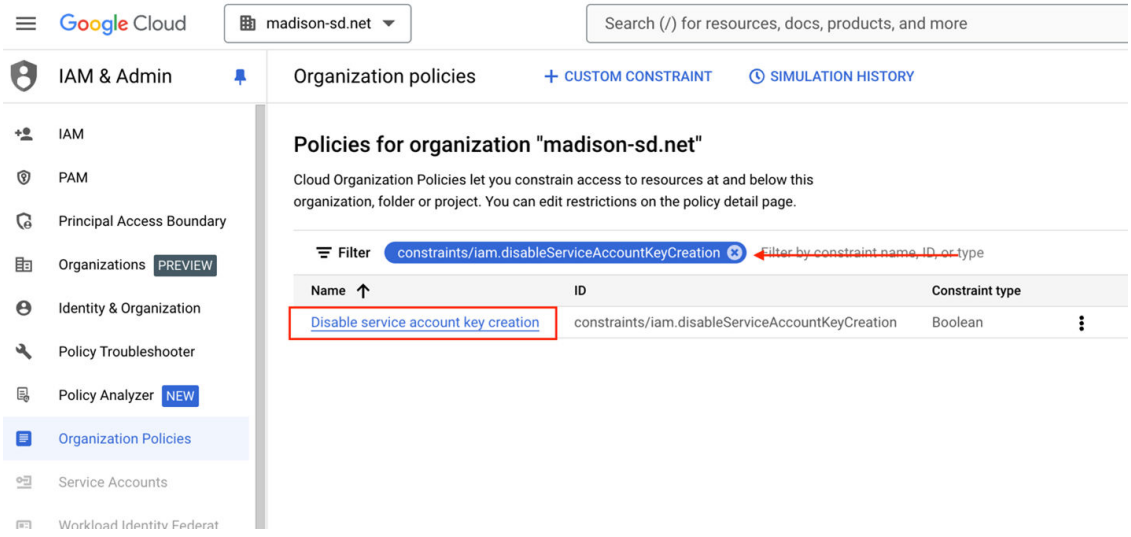



**Figure 58: Organization policies**

20. Select **MANAGE POLICY**.
21. Select **Override the parent's policy**. Then edit or create a rule to set the enforcement to **Off**. Finish by selecting the **SET POLICY**.

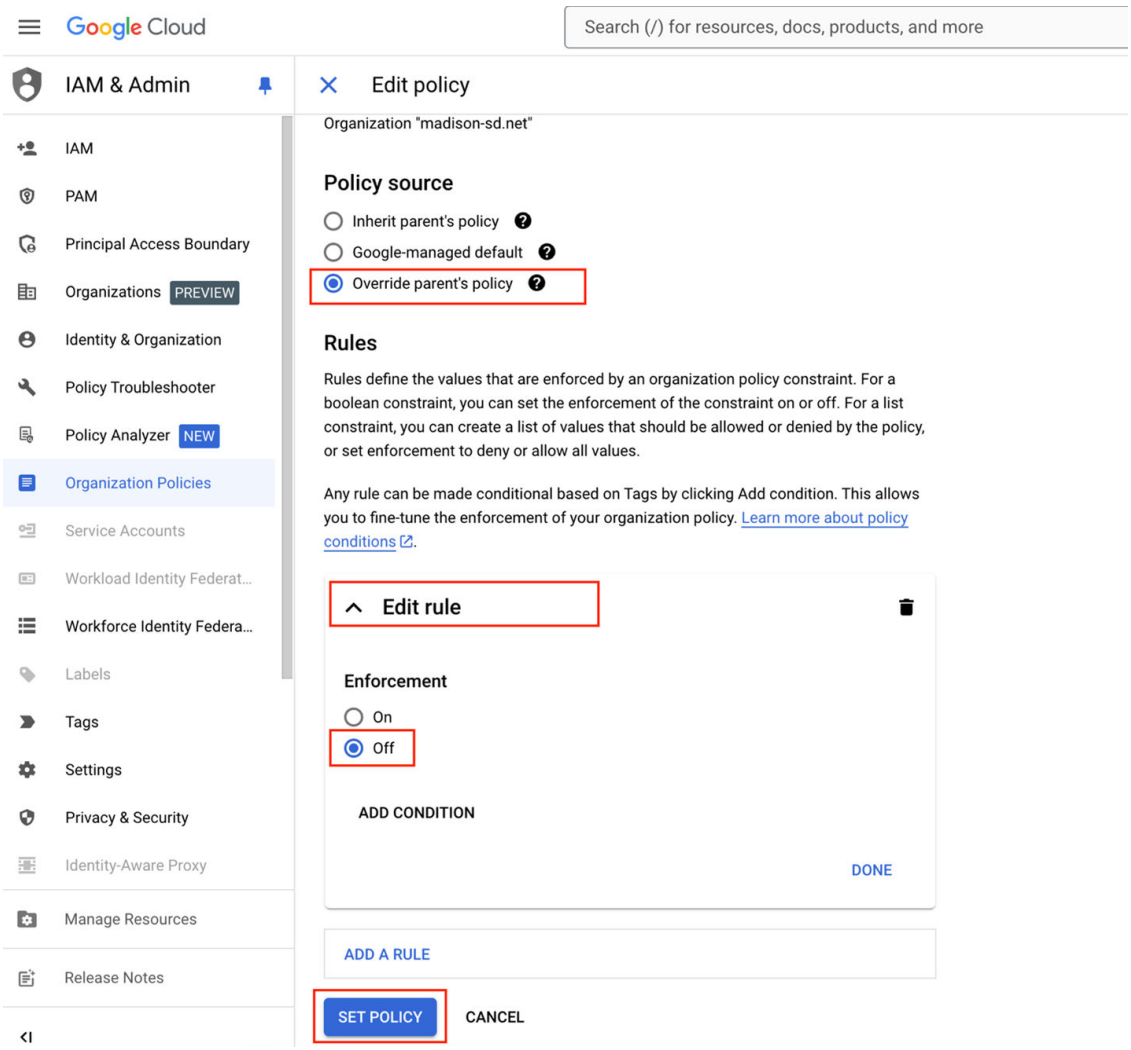



**Figure 59: Edit policy**

A successful configuration should look similar to the below screenshot. The creation and download of a private key for a service account should now be successful.

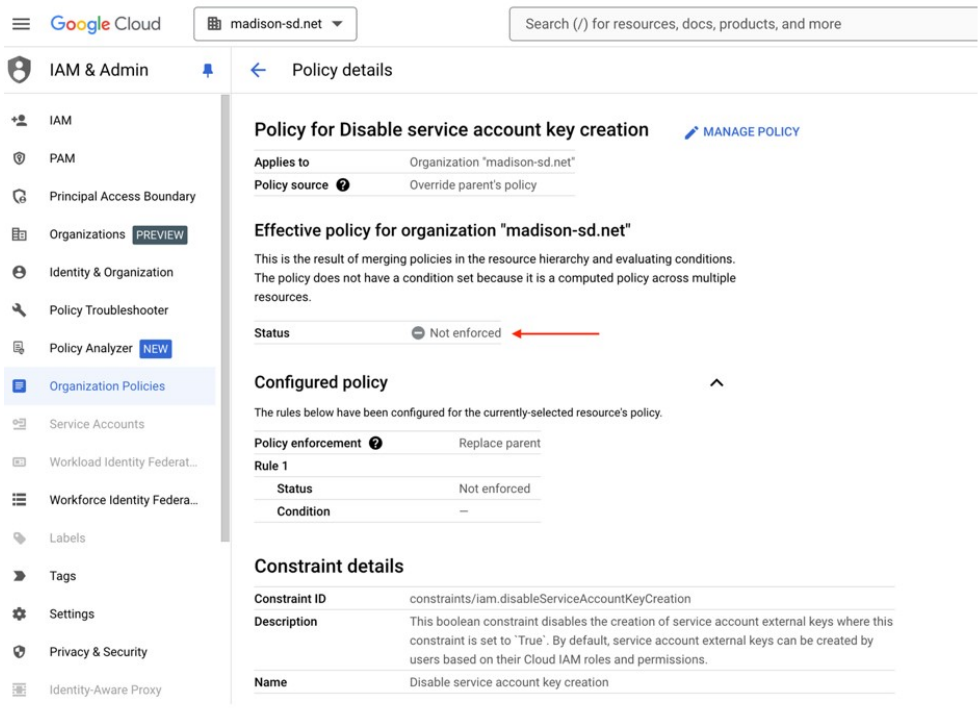



**Figure 60: Successful Configuration**

### Configure ExtremeCloud IQ (New) for Google Workspace

Use this task configure ExtremeCloud IQ (New) for Google Workspace.

1. Log into your ExtremeCloud IQ (New) tenant.
2. Go to **Administration and Settings** > **Access Management** > **Identity Providers** > **Network & Applications**.
3. Select **Add IDP Profile** and configure the settings in Table 215.

**Table 215: Google Workspace IdP Profile Configuration Settings**

| Field | Description |
|---|---|
| Set Up IdP | Select **Sync Users and User Groups** from the Purpose drop-down list. |
| Domains | If the domain needs to be limited, it can be selected here with the **Custom** toggle, otherwise leave it to **All Domains** |

**Table 215: Google Workspace IdP Profile Configuration Settings (continued)**

| Field | Description |
|---|---|
| Select Identity Provider | Select **Google Workspace** from the **Identity Provider** drop-down list. |
| Sync Users and User Groups | Use this option to sync your Google Workspace users and user groups with ExtremeCloud IQ (New).<br>• Setup Guidelines - Upload the private key JSON file that was downloaded from Google Cloud Console and paste in the Customer ID that was saved from the Google Admin Console.<br>• Customer ID - To get the Customer ID, go to the Google Admin Console, under **Account Settings**.<br>• Select User Groups (Google Workspace Only) - Select group-specific APs and sync only those groups.The table retrieves all available groups.<br>a. Select available groups and select the side arrow to them to the **Added** box.<br>**Note:** There is no maximum for added groups.<br>b. Select **Save**.<br>c. To view synced users, go to **Policy** > **Users & Devices**, under **Users** and Google Workspace appears in the **Type** column.<br>d. Under **User Groups**, from the 3-dot menu, select **Sync Now** to view new groups.<br>e. To view the sync event details, go to **Administration & Settings** > **Logs**, select **Security Logs** from the drop-down menu. |

#### Adjust Security Defaults for Google Workspace

In cases where a newer Google Workspace or Google Cloud Platform instance was created, security defaults may be enabled so that the administrator cannot download keys for service accounts. If this is the case, use this task to adjust security defaults for Google Workspace.

1. Log into Google Cloud via https://console.cloud.google.com.
2. From the top left, if you are already in a project, select the parent project from the drop-down list.
3. Go to **IAM & Admin** > **IAM**.
4. Under **IAM**, ensure that your account has an Organization Policy Administrator. If it does not, select Edit (pencil icon) next to your account to edit the roles. If your account isn't listed here, to add it select **GRANT ACCESS** and configure settings:
   a. Within the **Edit** window, select **Add Another Role**.
   b. Select the **Organization Policy Administrator** condition from the drop-down list.
   c. Select **SAVE**.
5. Once the roles are set, go to **Organization Policies** > **IAM & Admin**.
6. In the Organization Policies, search for iam.disableServiceAccountKeyCreation. Select edit to make updates.

7. Select **MANAGE POLICY**.
8. Select **Override the parent's policy**. Then edit or create a rule to set the enforcement to **Off**. Finish by selecting the **SET POLICY**.

A successful configuration should look similar to the below screenshot. The creation and download of a private key for a service account should now be successful.

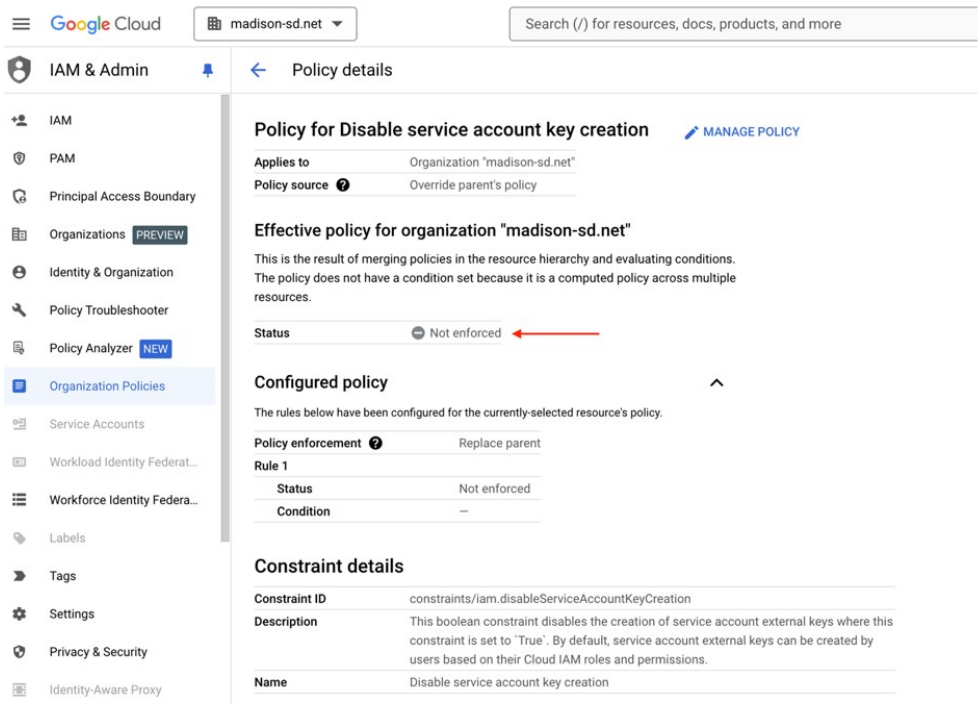



**Figure 61: Successful Configuration**

*Google Workspace | Network Access*

If user-based 802.1X EAP-TTLS network authentication is going to be used with Google Workspace, an Secure LDAP integration is required to be created.

If EAP-TLS (Certificate-based authentication) is going to be the only source of 802.1X user and device authentication, this setup is not required.

**Google Workspace | Network Access**

If user-based 802.1X EAP-TTLS network authentication is going to be used with Google Workspace, a secure LDAP integration must be created.

If EAP-TLS (Certificate-based authentication) is going to be the only source of 802.1X user and device authentication, this setup is not required.

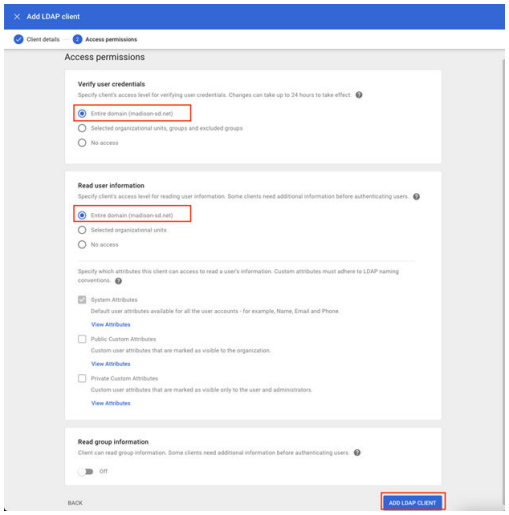
To configure Google Workspace for Network Access:

1. Configure the Google Admin Console.
2. Configure Extreme Platform ONE Security.

**Google Admin Console**

1. Go to **Apps** select **LDAP**.
2. Select **Add Client** and configure the settings in Table 216.

**Table 216: Client Configuration Settings**

| Section | Field | Description |
|---|---|---|
| Client Details | LDAP client name | Enter a client name. |
| Select **Continue**. | | |
| Access permissions | Verify user credentials | Select **Entire domain**. |
| | Read user information | Select **Entire domain**.<br><br>**Figure 62: Access permissions** |
| Select **ADD LDAP CLIENT**. | | |

Once the certificate is done generating, download and save it for use in ExtremeCloud IQ (New).

3. Select **Continue to Client Details**.
   a. By default, the LDAP client is not enabled. To enable it, select the drop-down list under **Service Status**.

b. Select **ON for everyone**.

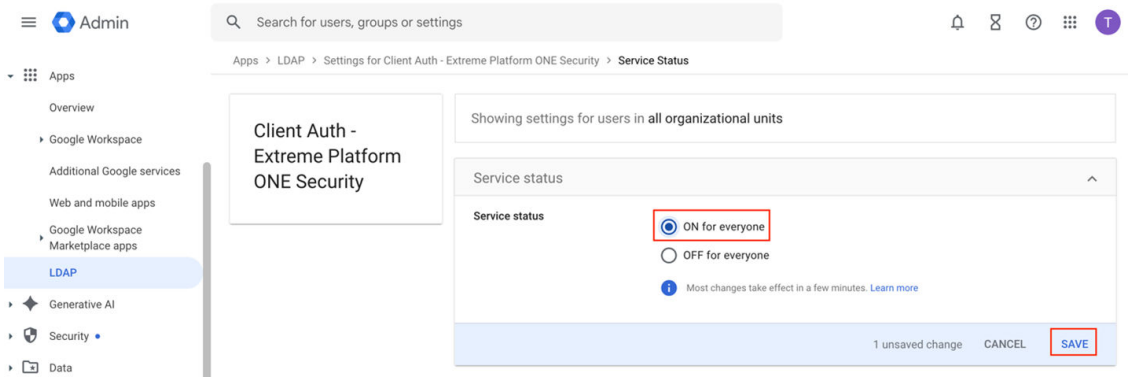



**Figure 63: Service Status**

**Extreme Platform ONE Security**

4. Go to **Administration and Settings** > **Access Management** > **Identity Providers** > **Network & Applications**.

5. Select **Add IDP Profile** and configure the settings in Table 217.

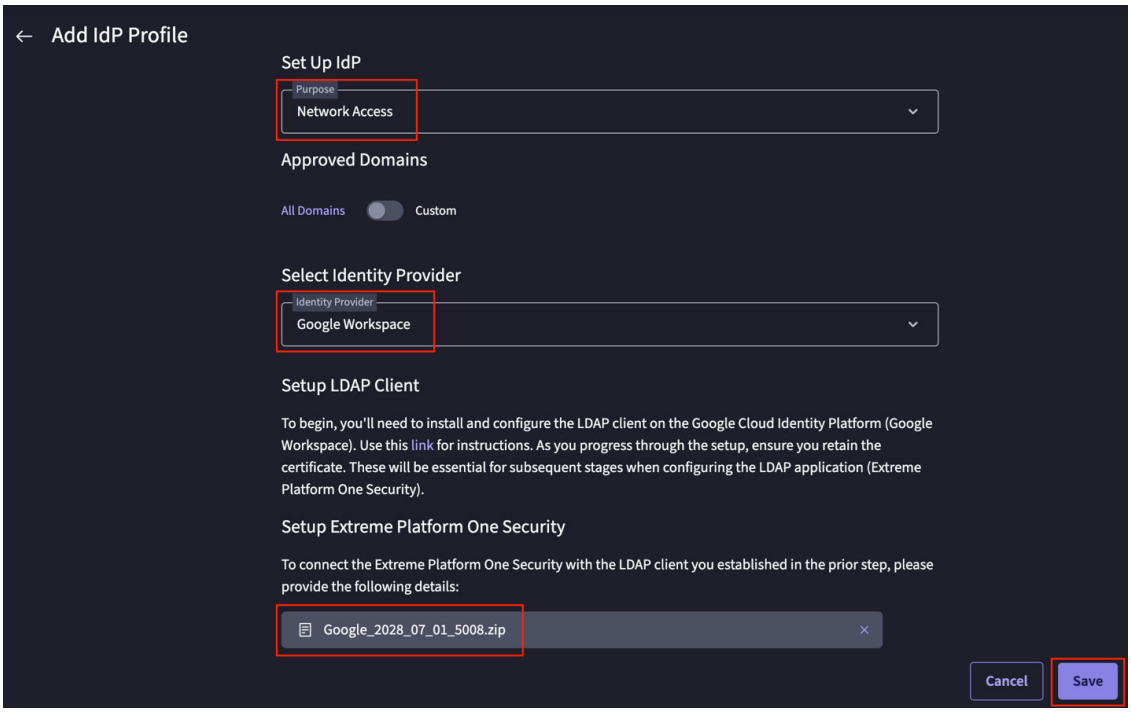



**Figure 64: IdP Profile**

**Table 217: Google Workspace Network Access IdP Profile Configuration Settings**

| Field | Description |
|---|---|
| Set Up IdP | Select **Network Access** from the Purpose drop-down list. |
| Approved Domains | If the domain needs to be limited, it can be selected here with the **Custom** toggle, otherwise leave it to **All Domains**. |
| Select Identity Provider | Select **Google Workspace** from the **Identity Provider** drop-down list. |
| Setup ExtremeCloud IQ (New) | Upload the saved Secure LDAP configuration from Google Admin Console. |

6. To complete the setup, select **Save**.

### Configure ExtremeCloud IQ (New) for Google Workspace Network Access

Use this task to configure ExtremeCloud IQ (New) for Google Workspace Network Access.

1. Log into your ExtremeCloud IQ (New) tenant.
2. Go to **Administration and Settings** > **Access Management** > **Identity Providers** > **Network & Applications**.

3. Select **Add IDP Profile** and configure the settings in Table 218.

**Table 218: Google Workspace Network Access IdP Profile Configuration Settings**

| Field | Description |
|---|---|
| Set Up IdP | Select **Network Access** from the Purpose drop-down list. |
| Approved Domains | If the domain needs to be limited, it can be selected here with the **Custom** toggle, otherwise leave it to **All Domains**. |
| Select Identity Provider | Select **Google Workspace** from the **Identity Provider** drop-down list. |
| Setup ExtremeCloud IQ (New) | Upload the saved Secure LDAP configuration from Google Admin Console. |

4. To complete the setup, select **Save**.

*Google Workspace | Application Access*

Application access for users can be authenticated via Google Workspace in two ways: OpenID Connect (OIDC) or SAML. The setup process is different in Okta depending on the type of integration being leveraged.

**Google Workspace | Application Access**

For OIDC integration, the setup in Google Workspace will be completed first, followed by the configuration of ExtremeCloud IQ (New). A Redirect URI will be needed from ExtremeCloud IQ (New).

Application access for users can be authenticated via Google Workspace in two ways:

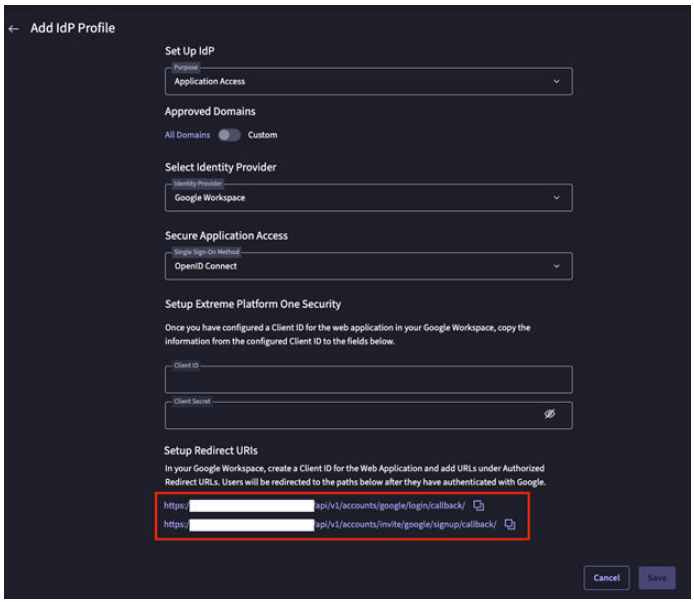
- Open ID Connect (OIDC)
  1. Retrieve Redirect URI in Extreme Platform ONE Security.
  2. Set up Google Workspace with Open ID Connect (OIDC) in Google Cloud (GCP).
  3. Configure Extreme Platform ONE Security.
- SAML
  1. Retrieve identifier and Reply URL in Extreme Platform ONE Security.
  2. Configure Google Admin Console.
  3. Finalize in Extreme Platform ONE Security.

**Application Access using Open ID Connect (OIDC)**

1. Retrieve Redirect URI In Extreme Platform ONE Security.
   a. Go to **Administration & Settings** > **Access Management** > **Identity Providers** > **Users**.

b. To create a new profile, select **Add IdP Profile** and configure the settings in Table 207 on page 607.

**Table 219: OIDC Application Access IdP Profile Settings**

| Field | Description |
|---|---|
| Set Up IdP | Select **Application Access** from the Purpose drop-down list. |
| Approved Domain | If the domain needs to be limited, it can be selected here, otherwise leave it to **All Domains**. |
| Select Identity Provider | Select **Google Workspace** from the Identity Provider drop-down list. |
| Application Access | Select **OpenID Connect** from the Single Sign-On drop-down list. |
| Setup Redirect URIs | Copy the Redirect URI.<br><br><br>**Figure 65: Redirect URI** |

c. Select **Cancel**.

2. Set up Google Workspace.
   a. Log in to Google Cloud using https://console.cloud.google.com.
   b. To create a new project:

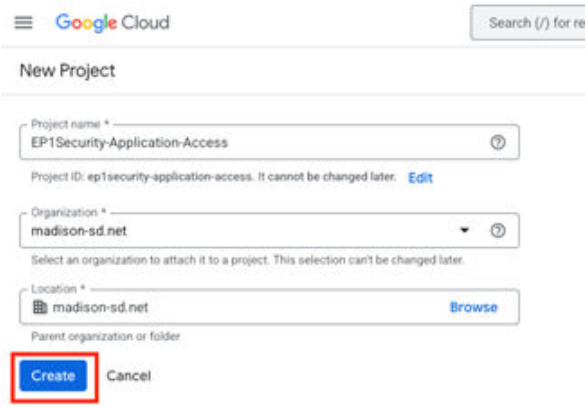



**Figure 66: New project**

   i. From the drop-down menu at the top of the screen, select **NEW PROJECT**.
   ii. Enter a name in the **Project Name** field and select **CREATE**.
   iii. Select the newly created Project, then from the left navigation screen select **VIEW ALL PRODUCTS**.
   iv. Under the **All products**, select **Google Auth Platform**.

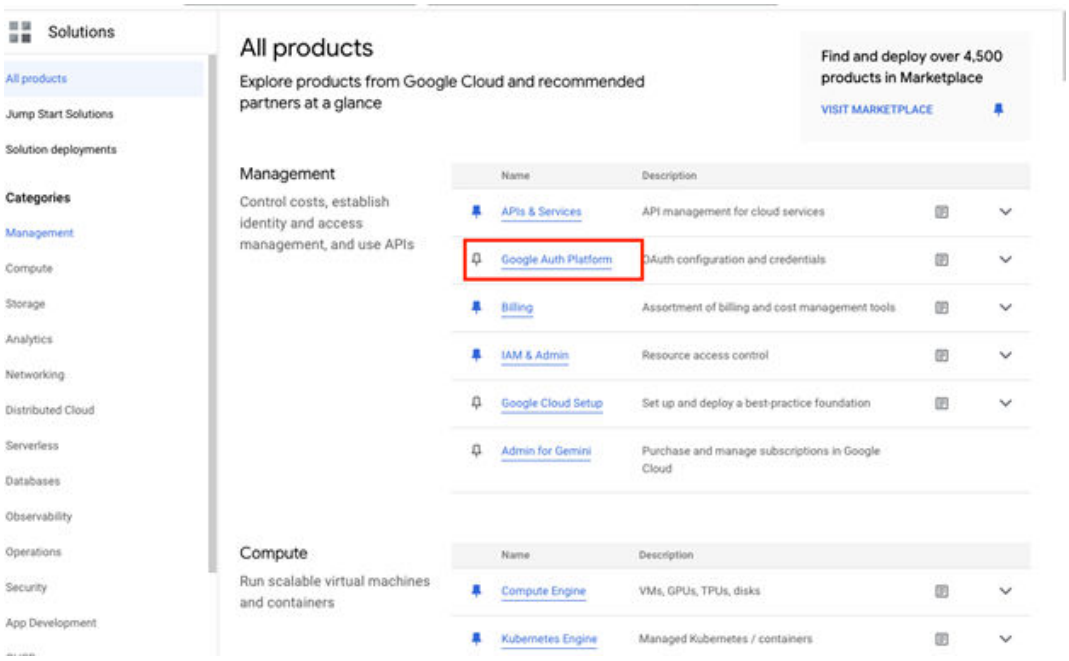



**Figure 67: Google Auth Platform**

   v. Select **GET STARTED**.
   vi. In the **App Information** section, enter the App Name, select a User support email from the drop-down list then select **Next**.

vii. In the **Audience** section, select **Internal** and then select **Next**.
viii. Under **Contact Information**, enter an email address and select **NEXT**.
ix. Finally, agree to the User Data Policy and select **CREATE**.

c. Go to **Overview**, select **CREATE OAUTH CLIENT** and configure the settings in Table 220.

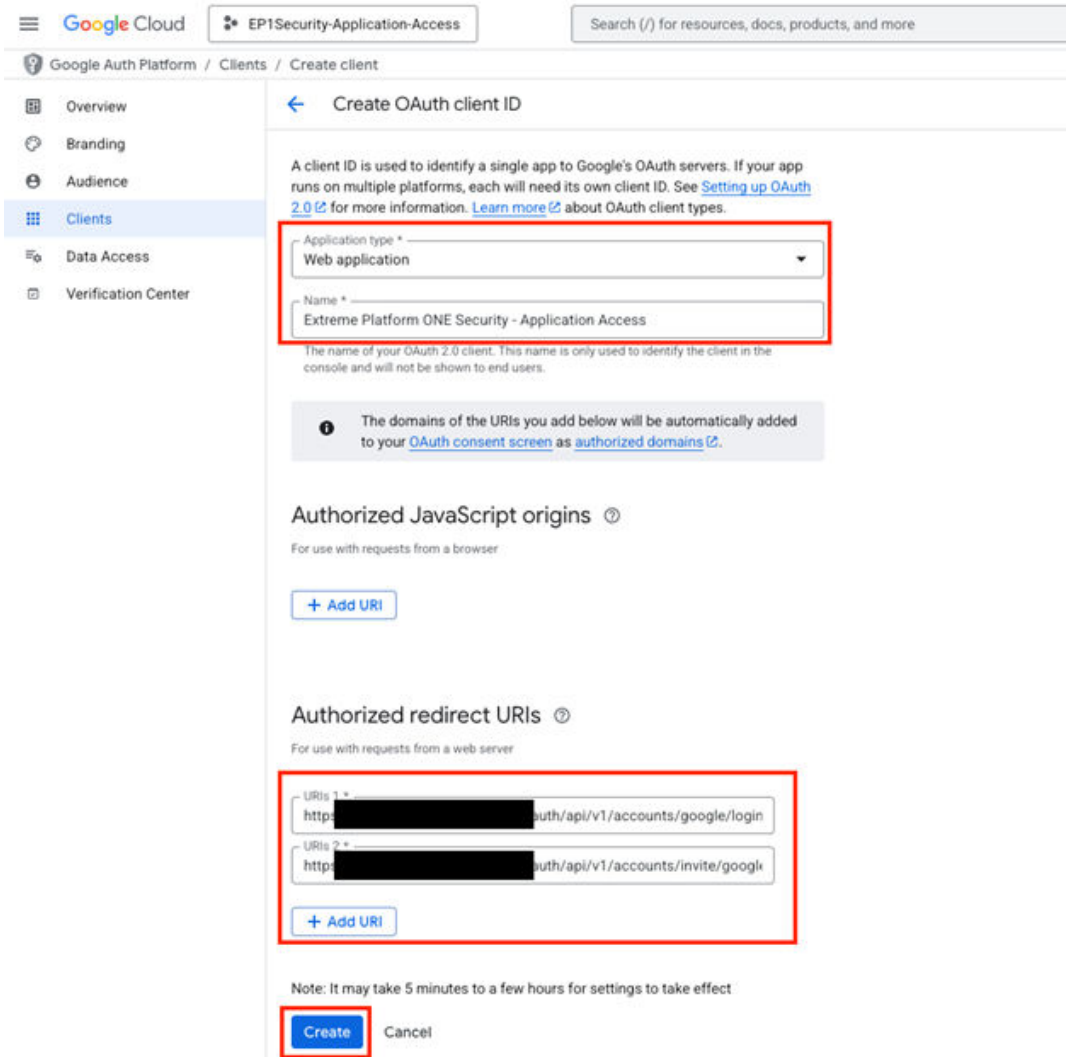



**Figure 68: OAuth client ID**

**Table 220: OAuth Client Configuration Settings**

| Section | Field | Description |
|---|---|---|
| CREATE OAuth client ID | Application Type | Select **Web application** from the drop-down list. |
| | Name | Name the OAuth client. |
| Authorized redirect URIs | URIs 1 | Create two entries and paste the two Redirect URIs that were previously copied from ExtremeCloud IQ (New). |
| | URIs 2 | |
| Select **Create**. | | |

d. Under **OAuth 2.0 Client IDs**, select the newly created client.
e. Under **Additional information**, copy the **Client ID** and **Client secret**.

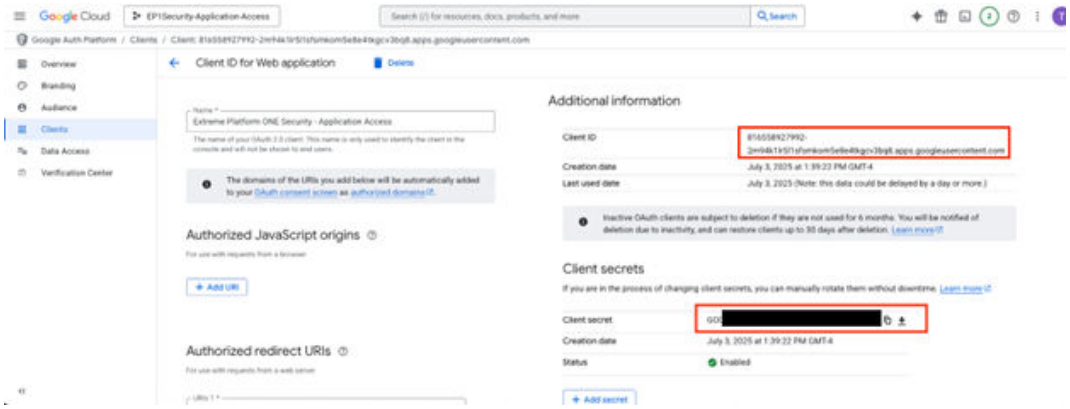



**Figure 69: Client ID and Client Secret**

3. Configure Extreme Platform ONE Security.
   a. Go to **Administration and Settings** > **Access Management** > **Identity Providers** > **Network & Application**.

b. Select **Add IdP Profile** and configure the settings in Table 221.

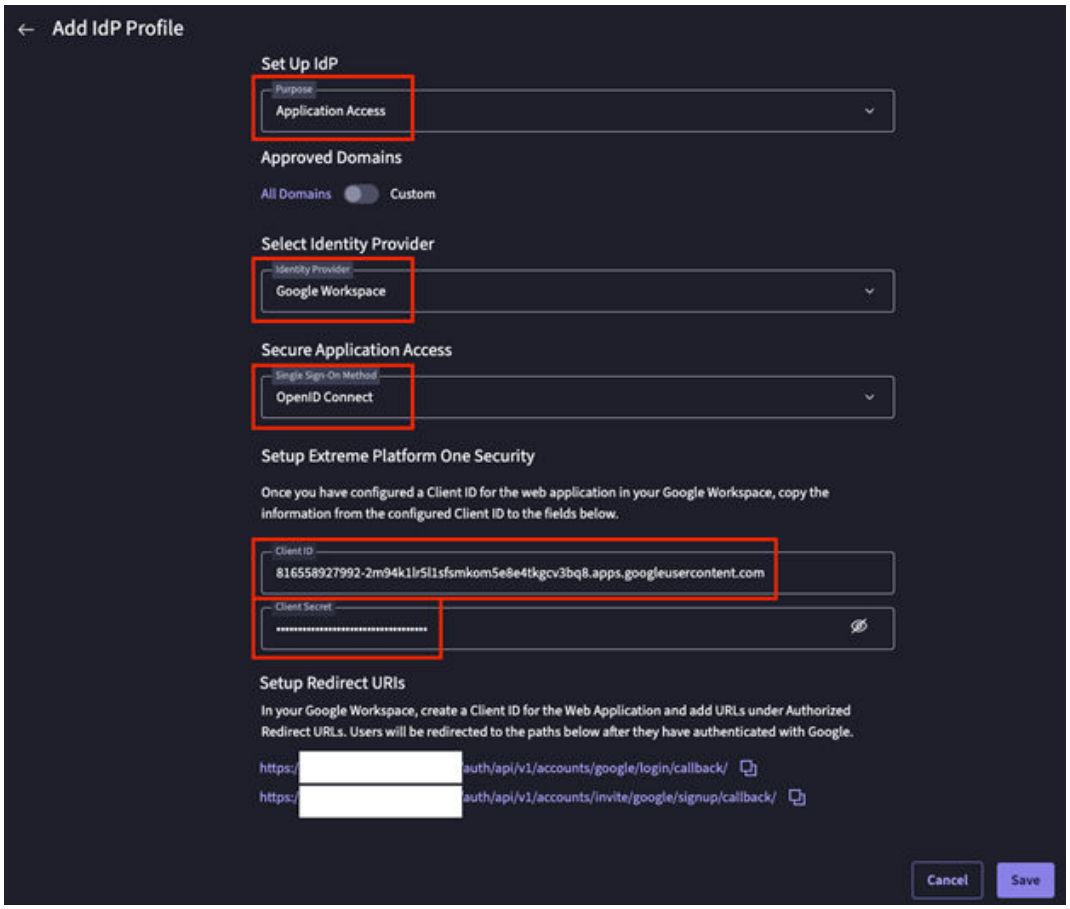



**Figure 70: IdP Profile**

**Table 221: Google Workspace Application Access IdP Profile Configuration Settings**

| Field | Description |
|---|---|
| Set Up IdP | Select **Application Access** from the Purpose drop-down list. |
| Approved Domains | If the domain needs to be limited, it can be selected here with the **Custom** toggle, otherwise leave it to **All Domains** |
| Select Identity Provider | Select **Google Workspace** from the **Identity Provider** drop-down list. |
| Secure Application Access | Under **Single Sign-On Method**, select **OpenID Connect**. |
| Setup Extreme Platform ONE Security | Paste the copied credentials from Microsoft Entra ID:<br>• Client ID<br>• Client Secret |

c. To complete the setup, select **Save**.

### Application Access using SAML

4. Retrieve identifier and Reply URL in Extreme Platform ONE Security.
   a. In ExtremeCloud IQ (New), go to **Administration & Settings** > **Access Management** > **Identity Providers** > **Network & Applications**.
   b. To create a new profile, select **Add IdP Profile** and configure the settings in Table 222.

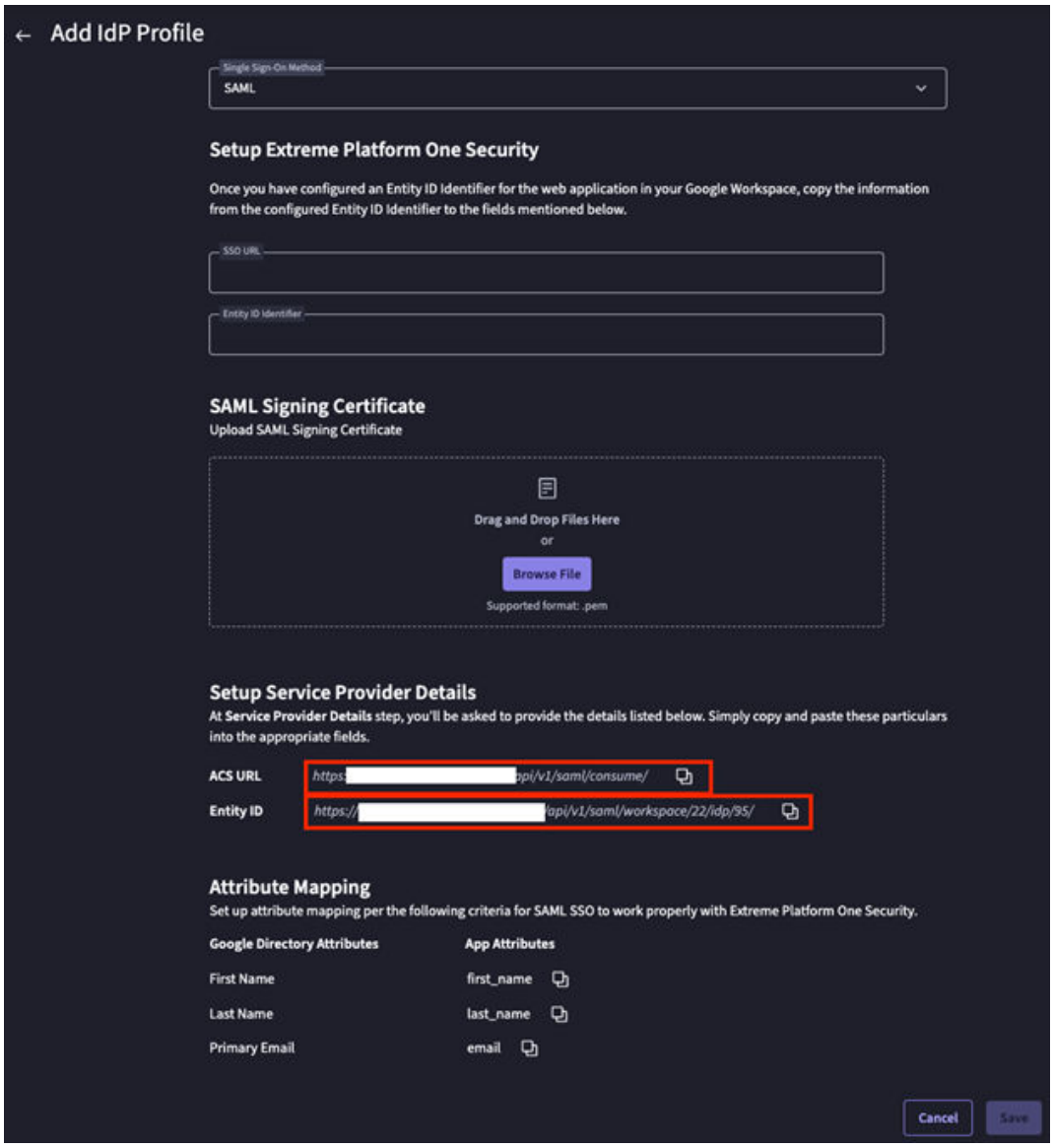



**Figure 71: SAML IdP**

**Table 222: SAML IdP Profile Configuration Settings**

| Field | Description |
|---|---|
| Set Up IdP | Select **Application Access** from the Purpose drop-down list. |
| Approved Domain | If the domain needs to be limited, it can be selected here, otherwise leave it to **All Domains**. |

**Table 222: SAML IdP Profile Configuration Settings (continued)**

| Field | Description |
|---|---|
| Select Identity Provider | Select **Google Workspace** from the Identity Provider drop-down list. |
| Single Sign-On Method | Select **SAML**. |
| Setup Up SSO in Microsoft Entra ID | Copy the Identifier and the Reply URL. |

**Note**
Leave this page open. If it is canceled, the Identifier will change, and this will need to be updated in the Google Workspace application.

c. Select **Save**.

5. Configure Google Admin Console.
   a. Log into the Google Admin Console and go to **Apps** > **Web and mobile apps**.
   b. From the **Add app** drop-down list, select **Add custom SAML app** and configure the settings in Table 223.

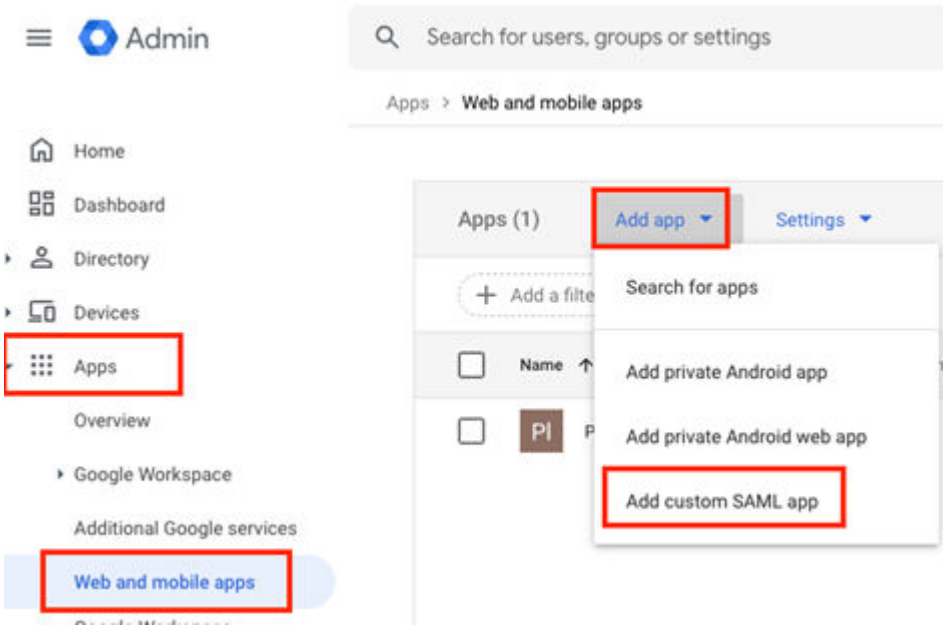



**Figure 72: SAML Application Access**

**Table 223: SAML Application Access Configuration Settings**

| Section | Field | Description |
|---|---|---|
| App details | App name | Name the App. |
| Select **Continue**. | | |

**Table 223: SAML Application Access Configuration Settings (continued)**

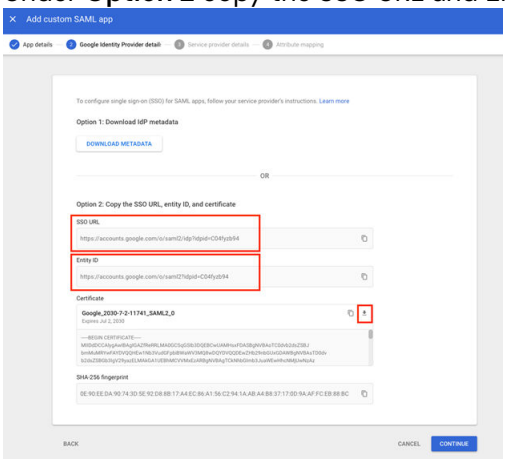
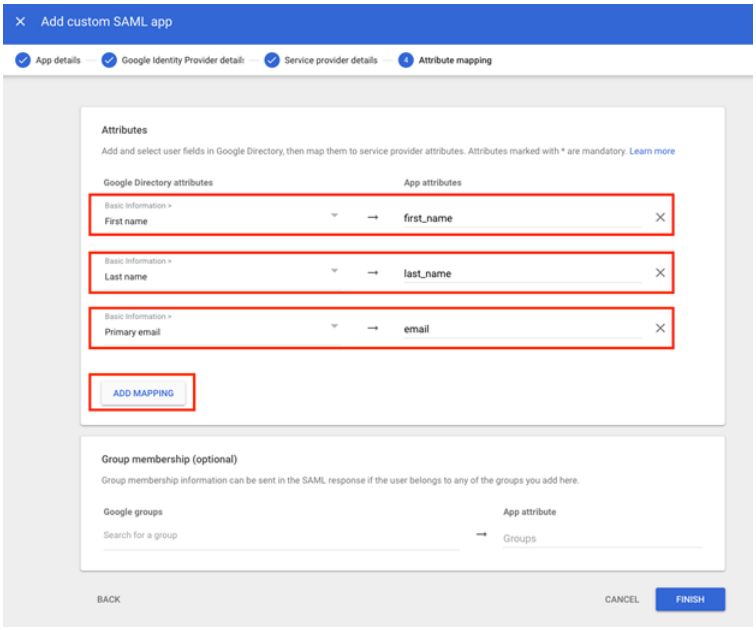
| Section | Field | Description |
|---|---|---|
| Google Identity Provider Details | SSO URL | Under **Option 2** copy the SSO URL and Entity ID.<br><br>**Figure 73: SSO URL** |
| | Entity ID | |
| | Certificate | Download certificate. |
| Select **Continue**. | | |
| Service provider details | ACS URL | Paste in the **ACS URL** and **Entity ID** that was previously copied from ExtremeCloud IQ (New). |
| | Entity ID | |
| Name ID | Name ID format | Set the **Name ID format** to **EMAIL**. |
| | Name ID | Set the **Name ID** to **Basic Information** > **Primary email**. |
| Select **Continue**. | | |

**Table 223: SAML Application Access Configuration Settings (continued)**

| Section | Field | Description |
|---|---|---|
| Attribute Mapping | Select **ADD MAPPING**.<br><br><br>**Figure 74: Attributes** | |
| | First name | Enter **first_name**. |
| | Last name | Enter **last_name**. |
| | Primary email | Enter **email**. |
| Select **FINISH**. | | |

6. Finalize in Extreme Platform ONE Security.
   a. In the **Application Access IdP** screen that was left open, paste in the SSO URL, the Entity ID Identifier, and upload the certificate that was downloaded. Select **Save**.

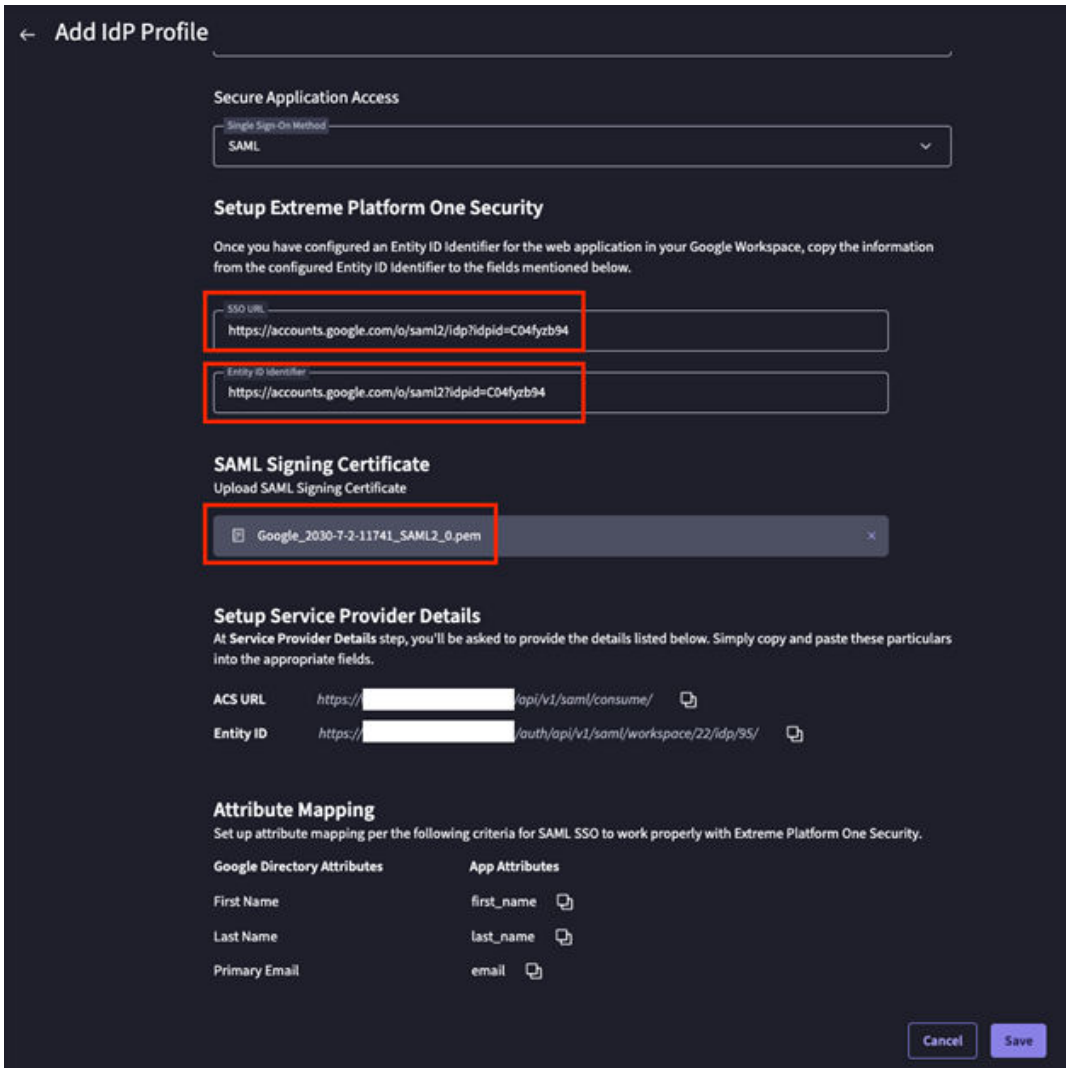



**Figure 75: Finalization**

**Note**
If this page was canceled, the Identifier will need to be updated in the Google Workspace application.

#### Set up Google Workspace with Open ID Connect

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

1. Log in to Google Cloud using https://console.cloud.google.com.
2. To create a new project:
   a. From the drop-down menu at the top of the screen, select **NEW PROJECT**.
   b. Enter a name in the **Project Name** field and select **CREATE**.

c. Select the newly created Project, then from the left navigation screen select **VIEW ALL PRODUCTS**.
d. Under the **All products**, select **Google Auth Platform**.
e. Select **GET STARTED**.
f. In the **App Information** section, enter the App Name, select a User support email from the drop-down list then select **Next**.
g. In the **Audience** section, select **Internal** and then select **Next**.
h. Under **Contact Information**, enter an email address and select **NEXT**.
i. Finally, agree to the User Data Policy and select **CREATE**.

3. Go to **Overview**, select **CREATE OAUTH CLIENT** and configure the settings in Table 224.

**Table 224: OAuth Client Configuration Settings**

| Section | Field | Description |
|---|---|---|
| CREATE OAuth client ID | Application Type | Select **Web application** from the drop-down list. |
| | Name | Name the OAuth client. |
| Authorized redirect URIs | URIs 1 | Create two entries and paste the two Redirect URIs that were previously copied from ExtremeCloud IQ (New). |
| | URIs 2 | |
| Select **Create**. | | |

4. Under **OAuth 2.0 Client IDs**, select the newly created client.
5. Under **Additional information**, copy the **Client ID** and **Client secret**.

*Configure Application Access with Google Workspace for SAML*

For SAML integration, the preparation in ExtremeCloud IQ (New), followed by the configuration in Google Workspace, and a finalization in ExtremeCloud IQ (New).

#### Prepare ExtremeCloud IQ (New) SAML

Prior to configuring the SAML application in Google Workspace, an Identifier and Reply URL will be needed from ExtremeCloud IQ (New).

Use this task to prepare ExtremeCloud IQ (New) for SAML application access.

1. In ExtremeCloud IQ (New), go to **Administration & Settings** > **Access Management** > **Identity Providers** > **Network & Applications**.
2. To create a new profile, select **Add IdP Profile** and configure the settings in Table 225.

**Table 225: SAML IdP Profile Configuration Settings**

| Field | Description |
|---|---|
| Set Up IdP | Select **Application Access** from the Purpose drop-down list. |
| Approved Domain | If the domain needs to be limited, it can be selected here, otherwise leave it to **All Domains**. |
| Select Identity Provider | Select **Google Workspace** from the Identity Provider drop-down list. |

**Table 225: SAML IdP Profile Configuration Settings (continued)**

| Field | Description |
|---|---|
| Single Sign-On Method | Select **SAML**. |
| Setup Up SSO in Microsoft Entra ID | Copy the Identifier and the Reply URL. |

**Note**
Leave this page open. If it is canceled, the Identifier will change, and this will need to be updated in the Google Workspace application.

3. Select **Save**.

#### Configure Google Workspace SAML Application Access

Use this task to configure Google Workspace for SAML Application Access.

1. Log into the Google Admin Console and go to **Apps** > **Web and mobile apps**.
2. From the **Add app** drop-down list, select **Add custom SAML app** and configure the settings in Table 226.

**Table 226: SAML Application Access Configuration Settings**

| Section | Field | Description |
|---|---|---|
| App details | App name | Name the App. |
| Select **Continue**. | | |
| Google Identity Provider Details | SSO URL | Under **Option 2** copy the SSO URL and Entity ID. |
| | Entity ID | |
| | Certificate | Download certificate. |
| Select **Continue**. | | |
| Service provider details | ACS URL | Paste in the **ACS URL** and **Entity ID** that was previously copied from ExtremeCloud IQ (New). |
| | Entity ID | |
| Name ID | Name ID format | Set the **Name ID format** to **EMAIL**. |
| | Name ID | Set the **Name ID** to **Basic Information** > **Primary email**. |
| Select **Continue**. | | |
| Attribute Mapping | Select **ADD MAPPING**. | |
| | First name | Enter **first_name**. |
| | Last name | Enter **last_name**. |
| | Primary email | Enter **email**. |
| Select **FINISH**. | | |

#### Configure ExtremeCloud IQ (New) Google Workspace SAML Finalization

Use this task to complete the final Google Workspace SAML configuration in ExtremeCloud IQ (New).

In the **Application Access IdP** screen that was left open, paste in the SSO URL, the Entity ID Identifier, and upload the certificate that was downloaded. Select **Save**.

**Note**
If this page was canceled, the Identifier will need to be updated in the Google Workspace application.

## Okta

The ExtremeCloud IQ (New) API Service Integration provides a secure, scalable interface to access your Okta directory without requiring individual user credentials. This integration is primarily designed for automated synchronization of users and groups, ensuring consistent and centralized identity management across the ExtremeCloud IQ (New) environment.

*Okta | Synchronize Users and User Groups*

Synchronizing Users and User Groups from Okta is required to ensure policies can be applied to users connecting with Okta credentials in ExtremeCloud IQ (New). There are two methods available for synchronization:

1. Just in Time (JIT) Synchronization – this method has ExtremeCloud IQ (New) reach into Okta and pull users and user groups on a polled basis. This method leverages an OIDC application to integrate with the Okta APIs.
2. System for Cross-Domain Identity Management (SCIM) Synchronization – this method has Okta push users and user groups from Okta into ExtremeCloud IQ (New). This method requires an enterprise application to be set up in Entra ID so that automatic provisioning can be enabled.

**Note**
Synced User cannot be removed from Extreme Platform ONE Security. It must be removed from the Identity Provider and then a syncing cycle should be initiated again.

#### Synchronizing Users and User Groups with JIT

For JIT integration, the setup in Okta will be completed first, followed by the configuration of ExtremeCloud IQ (New).

#### Okta | JIT Synchronize Users and User Groups

This method has ExtremeCloud IQ (New) reach into Okta and pull users and user groups on a polled basis. Synchronization uses an OIDC application to integrate with the Okta APIs.

JIT integration is configured in these steps:

1. Configure Okta Administrator Portal.

2. Configure Extreme Platform ONE Security.

**Note**
Synced User cannot be removed from Extreme Platform ONE Security. It must be removed from the Identity Provider and then a syncing cycle should be initiated again.

### Okta Administrator Portal

1. Go to the **Applications** > **API Service Integrations**.
2. Select **Add Integration**.

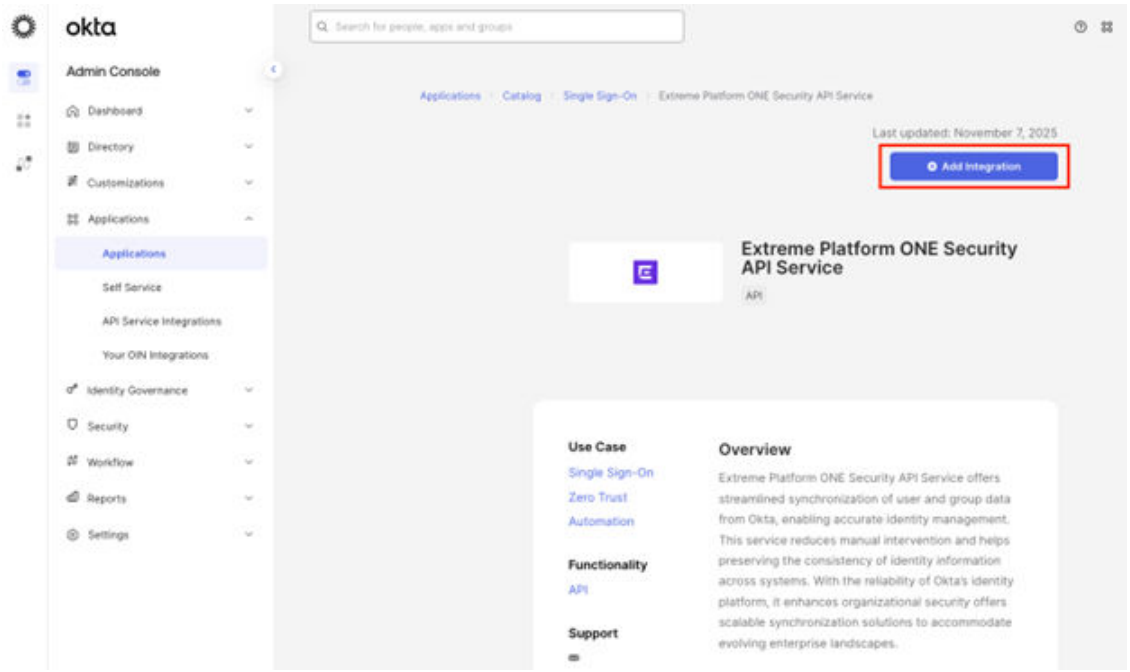



**Figure 76: Add Integration**

3. From the list, select **Extreme Platform ONE Security API Service**, then select **Install and Authorize**.

   The following API scopes are automatically applied:

   - `okta.users.manage`
   - `okta.apps.manage`
   - `okta.groups.manage`

4. To copy the Client Secret, when prompted, select **Copy to clipboard**.

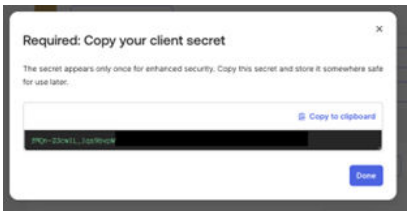



**Figure 77: Client Secret**

**Note**
The Client Secret is only shown once. Ensure it is copied and stored securely.

5. Select **Done**.
6. Copy and securely store the following:
   - Okta Org Domain (without the https prefix. e.g. trial-4343365.okta.com)
   - API Service Client ID

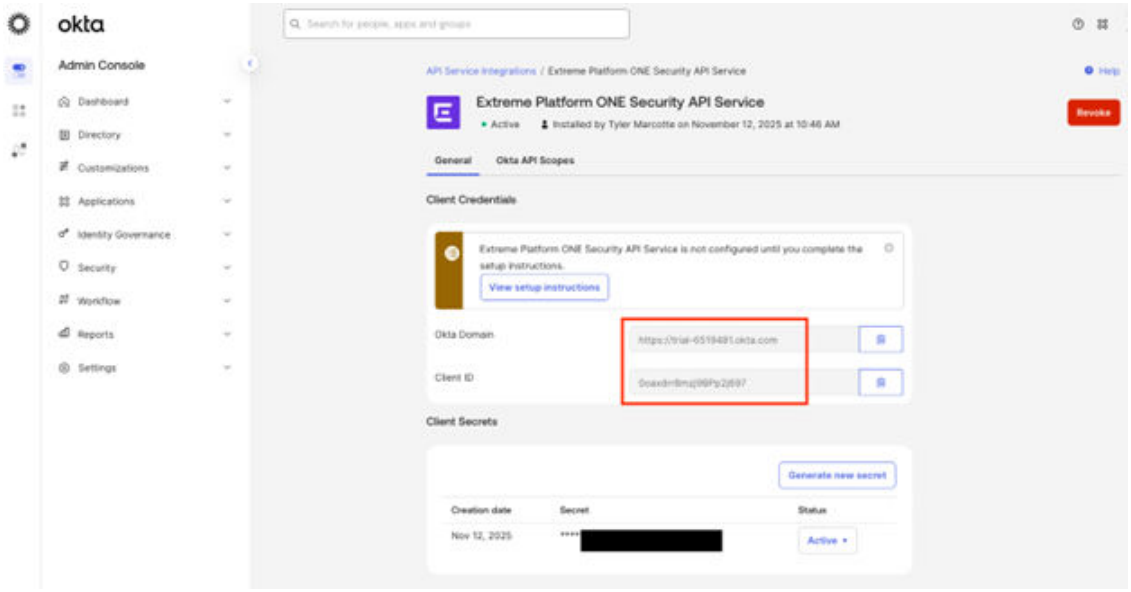



**Figure 78: Okta Domain and Client ID**

7. Under **Assignments**, locate and copy the Client ID of the OIDC application you wish to sync users and groups.

**Note**
Reference the image below oktauser@tempmail.com is assigned to OIDC App which will be synced after successful setup.

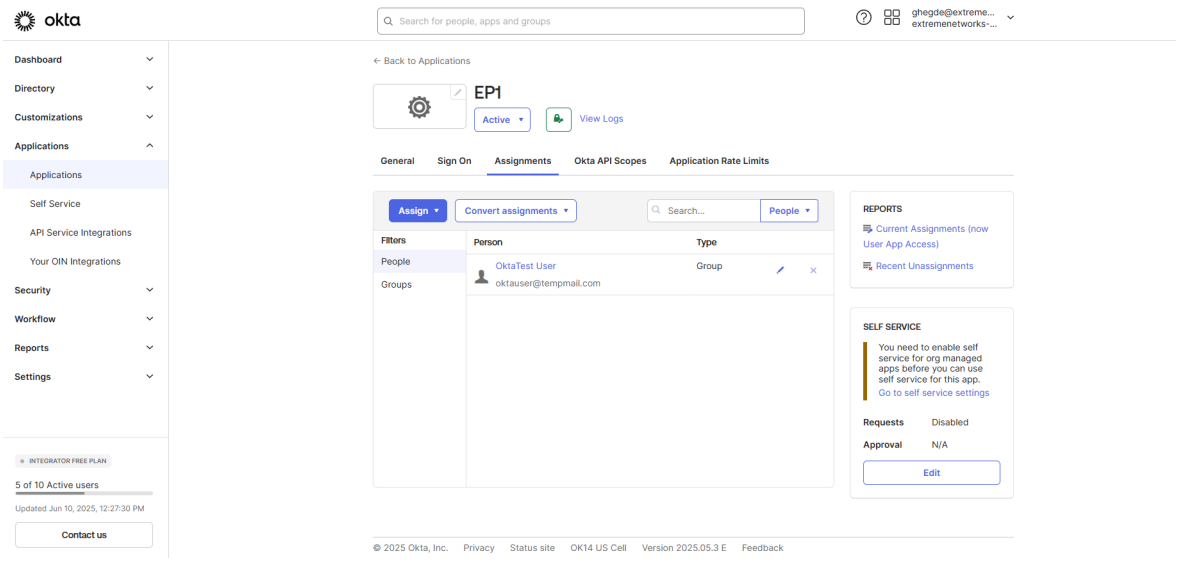



**Figure 79: Assign Users and Groups**

### Extreme Platform ONE Security

8. Go to **Administration and Settings** > **Access Management** > **Identity Providers** > **Network & Applications**.

9. Select **Add IdP Profile** and configure the settings in Table 227.

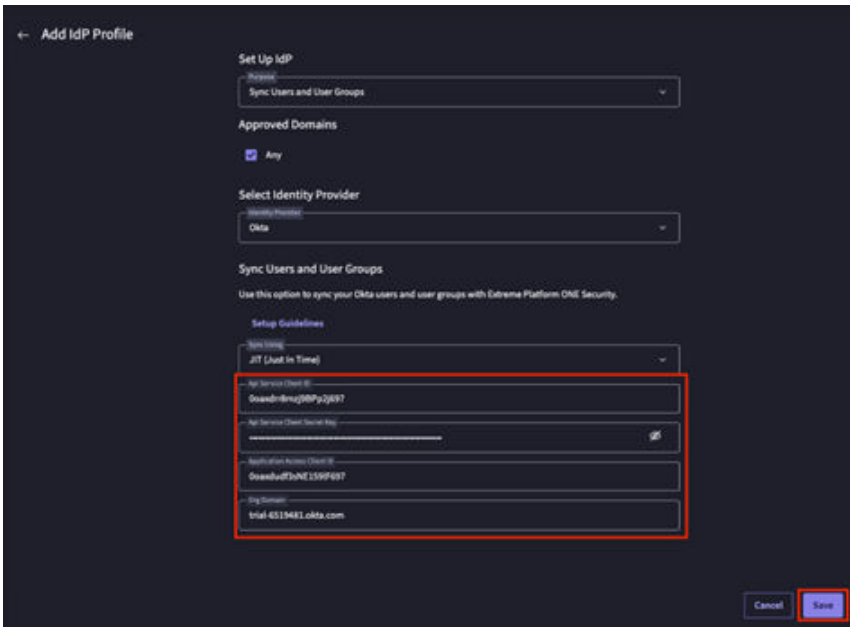



**Figure 80: IdP Profile**

**Table 227: JIT IdP Profile Configuration Settings**

| Field | Description |
|---|---|
| Set Up IdP | Select **Sync Users and User Groups** from the Purpose drop-down list. |
| Approved Domains | If the domain needs to be limited, it can be selected here with the **Custom** toggle, otherwise leave it to **All Domains** |
| Select Identity Provider | Select **Okta** from the **Identity Provider** drop-down list. |
| Setup Guidelines | Select **JIT (Just in Time)** for the **Sync Using** drop-down list. |
| | Paste the copied credentials from Okta:<br>• API Service Client ID<br>• API Service Client Secret Key<br>• Application Access Client ID<br>• Org Domain |

10. To complete the setup, select **Save**.

A dynamic sync workflow will be schedule automatically. To view synced users and groups, go to **Policy** > **Users & Devices**.

#### Configure Extreme Platform ONE Security JIT

Use this task to configure the Sync IdP profile in ExtremeCloud IQ (New).

1. Log into your ExtremeCloud IQ (New) tenant.
2. Go to **Administration and Settings** > **Access Management** > **Identity Providers** > **Network & Applications**.

3. Select **Add IdP Profile** and configure the settings in Table 228.

**Table 228: JIT IdP Profile Configuration Settings**

| Field | Description |
|---|---|
| Set Up IdP | Select **Sync Users and User Groups** from the Purpose drop-down list. |
| Approved Domains | If the domain needs to be limited, it can be selected here with the **Custom** toggle, otherwise leave it to **All Domains** |
| Select Identity Provider | Select **Okta** from the **Identity Provider** drop-down list. |
| Setup Guidelines | Select **JIT (Just in Time)** for the **Sync Using** drop-down list. |
| | Paste the copied credentials from Okta:<br>• API Service Client ID<br>• API Service Client Secret Key<br>• Application Access Client ID<br>• Org Domain |

4. To complete the setup, select **Save**.

A dynamic sync workflow will be schedule automatically. To view synced users and groups, go to **Policy** > **Users & Devices**.

*Okta | Synchronizing Users and User Groups with SCIM*

For SCIM integration, the setup in ExtremeCloud IQ (New) will be completed first, followed by the configuration of Okta.

#### Okta | SCIM Synchronize Users and User Groups

This method has Okta push users and user groups from Okta into ExtremeCloud IQ (New). Synchronization requires that you set up an enterprise application in Okta so that automatic provisioning can be enabled.

SCIM integration is configured in these steps:

1. Configure Extreme Platform ONE Security.
2. Configure System for Cross-Domain Identity Management (SCIM) in Okta.

**Note**
Synced User cannot be removed from Extreme Platform ONE Security. It must be removed from the Identity Provider and then a syncing cycle should be initiated again.

##### Extreme Platform ONE Security

1. Go to **Access Management** > **Administration & Settings** > **Identity Providers** and select **Network & Applications**.

2. To create a new profile, select the **Add IdP Profile** and configure the settings in Table 229.

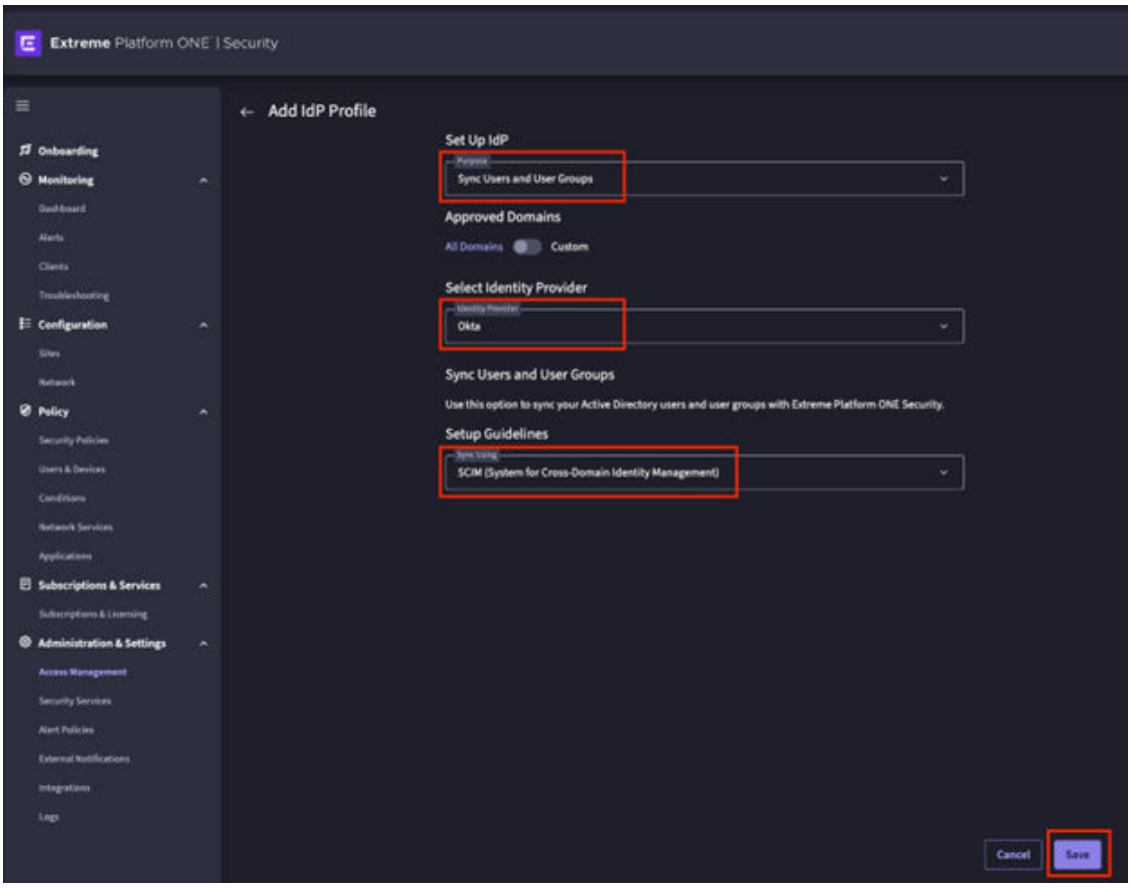



**Figure 81: IdP Profile**

**Table 229: Okta SCIM IdP Profile Configuration Settings**

| Field | Description |
|---|---|
| Set Up IdP | Select **Sync Users and User Groups** as the **Purpose** from the drop-down list. |
| Approved Domains | If the domain needs to be limited, it can be selected here with the **Custom** toggle, otherwise leave it to **All Domains**. |
| Select Identity Provider | Select **Okta** from the **Identity Provider** drop-down list. |
| Setup Guidelines | Select **SCIM (System for Cross-domain Identity Management)** for the **Sync Using** drop-down list. |

3. Select **Save**.
4. Once saved, from the 3-dot menu, select **Edit**.

5. In the **Edit** window, select **Okta Syncing Credentials**.

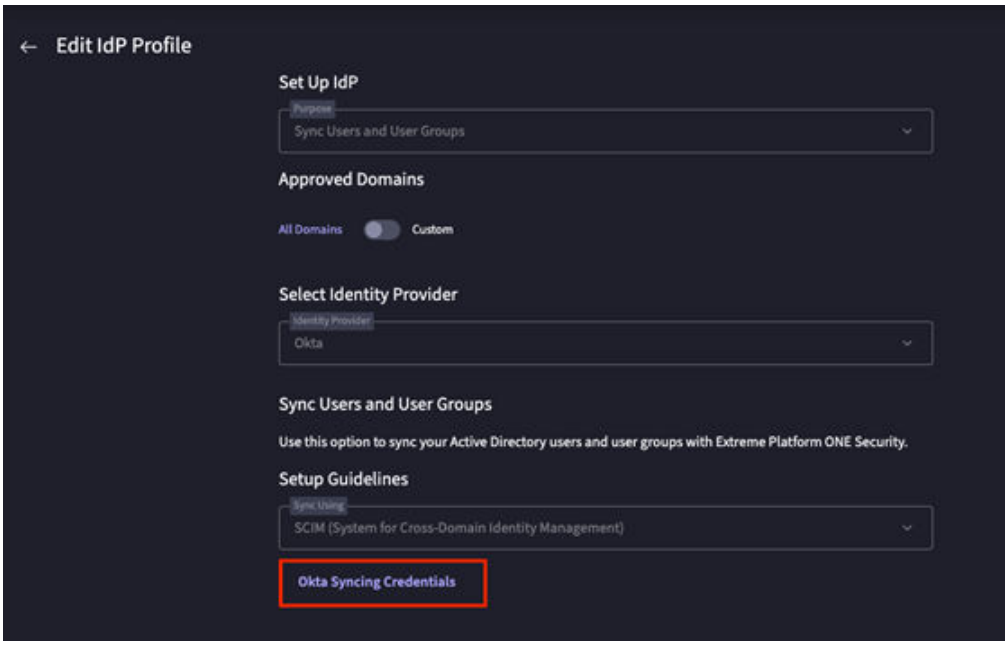



**Figure 82: Okta Syncing Credentials**

6. In the **Okta Syncing Credentials** window, save the **Tenant URL** and **Secret Token** for use within Okta.

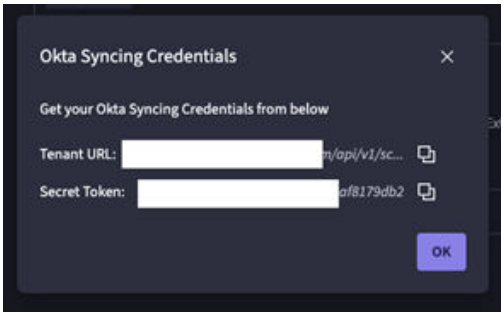



**Figure 83: Okta Syncing Credentials**

### Okta Administrator Portal

7. Go to the **Applications** > **Browse App Catalog**.

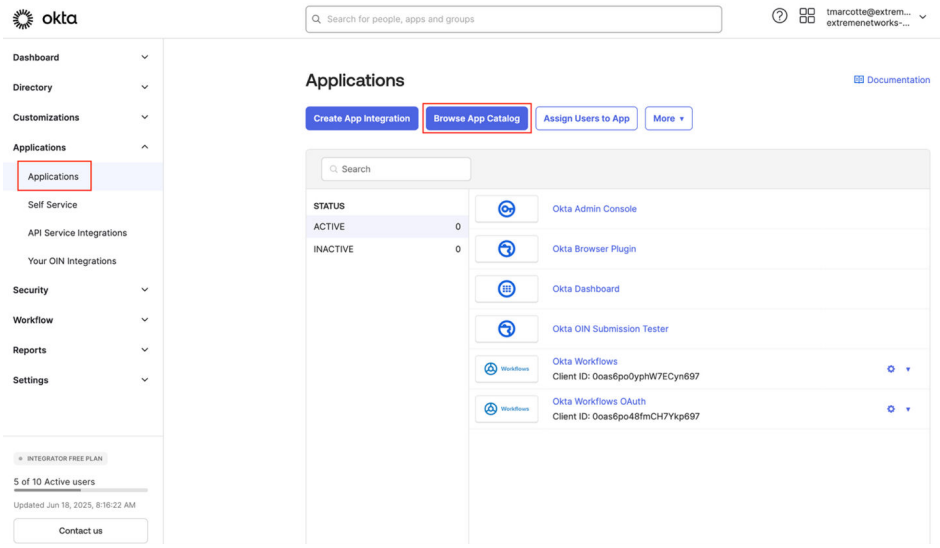



**Figure 84: Applications Menu**

8. In the search field, enter and select **(OAuth Bearer Token) Governance with SCIM 2.0**.
9. Select **Add Integration**.
10. On the **General Settings** tab, in the **Application label** field, enter **Extreme Platform ONE Security - SCIM** and select **Next**.

11. On the **Sign-On Options** tab, scroll to the bottom and select **Done**. No additional information needs to be added for the SCIM integration.

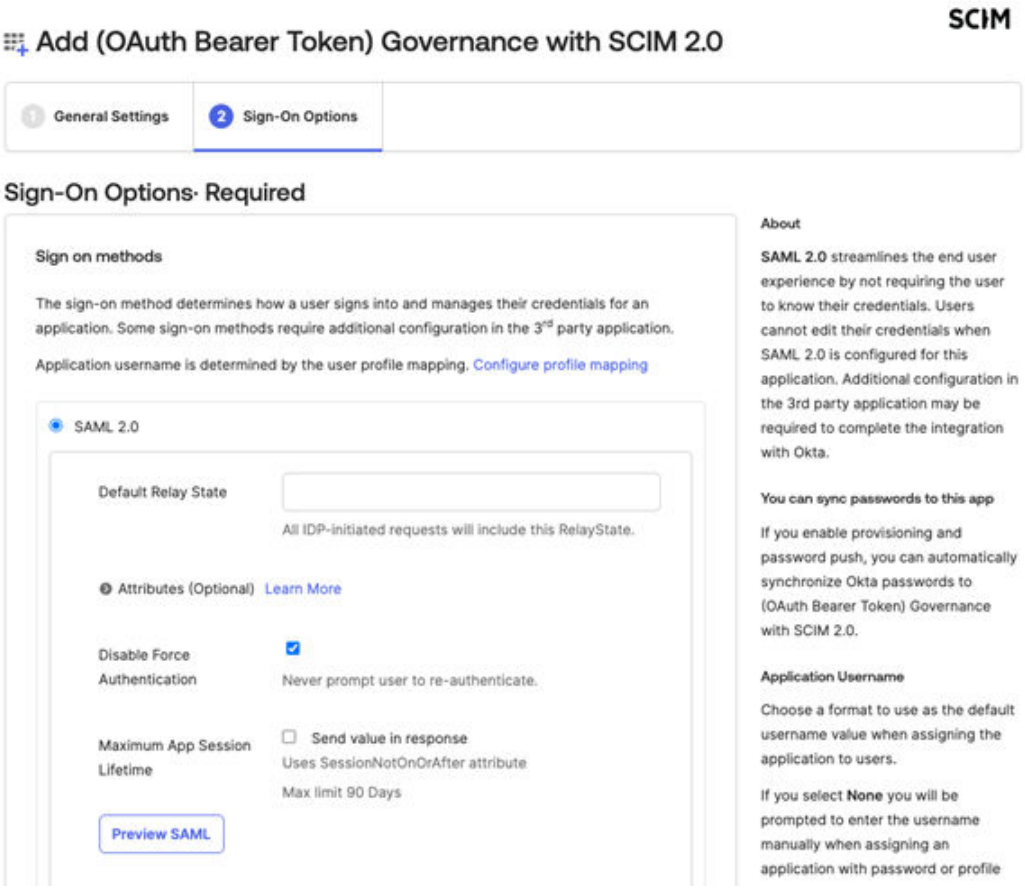



**Figure 85: Sign-On Options Required**

12. In the new application, select the **Provisioning** > **Configure API Integration** and configure the settings in Table 230.

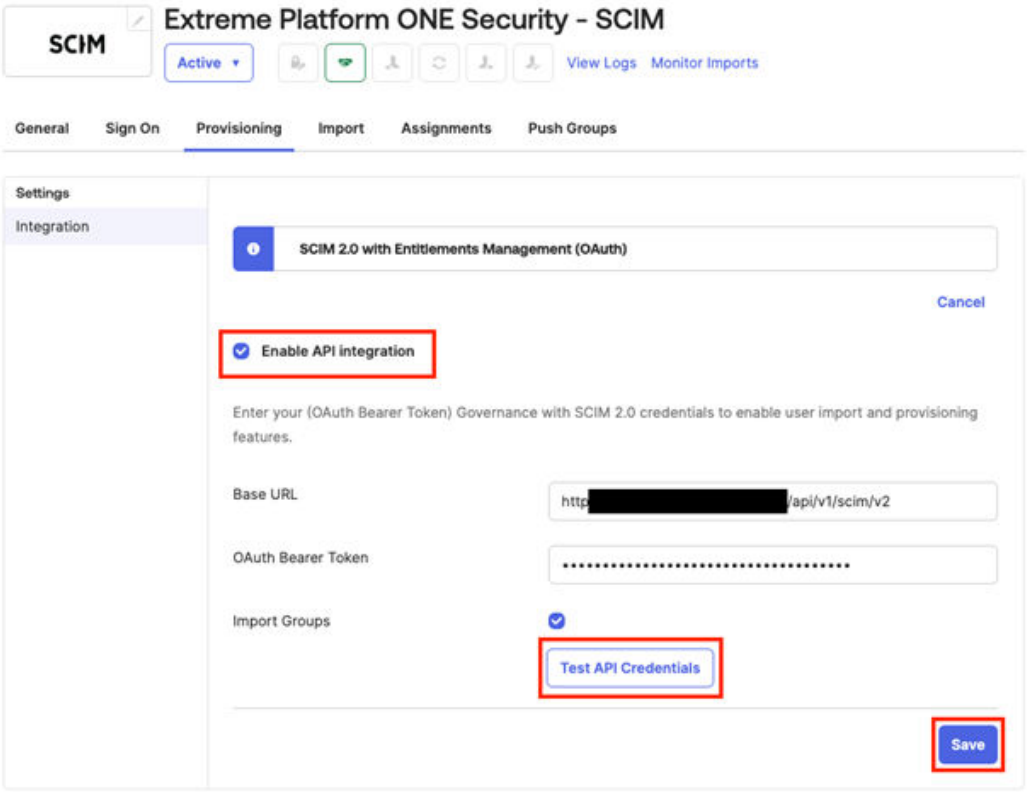



**Table 230: API Integration Configuration Settings**

| Field | Description |
|---|---|
| Enable API Integration | Select this option. |
| Base URL | Paste in the Tenant URL that was saved from ExtremeCloud IQ (New). |
| OAuth Bearer Token | Paste the Secret Token that was saved from ExtremeCloud IQ (New). |

13. Select **Test API Credentials**.

**Note**
If the credentials do not verify successfully, ensure there are not typos in the Tenant URL or Secret Token from the **IdP Profile** entry in ExtremeCloud IQ (New).

14. Upon successful verification, select **Save** and configure the settings in Table 231.

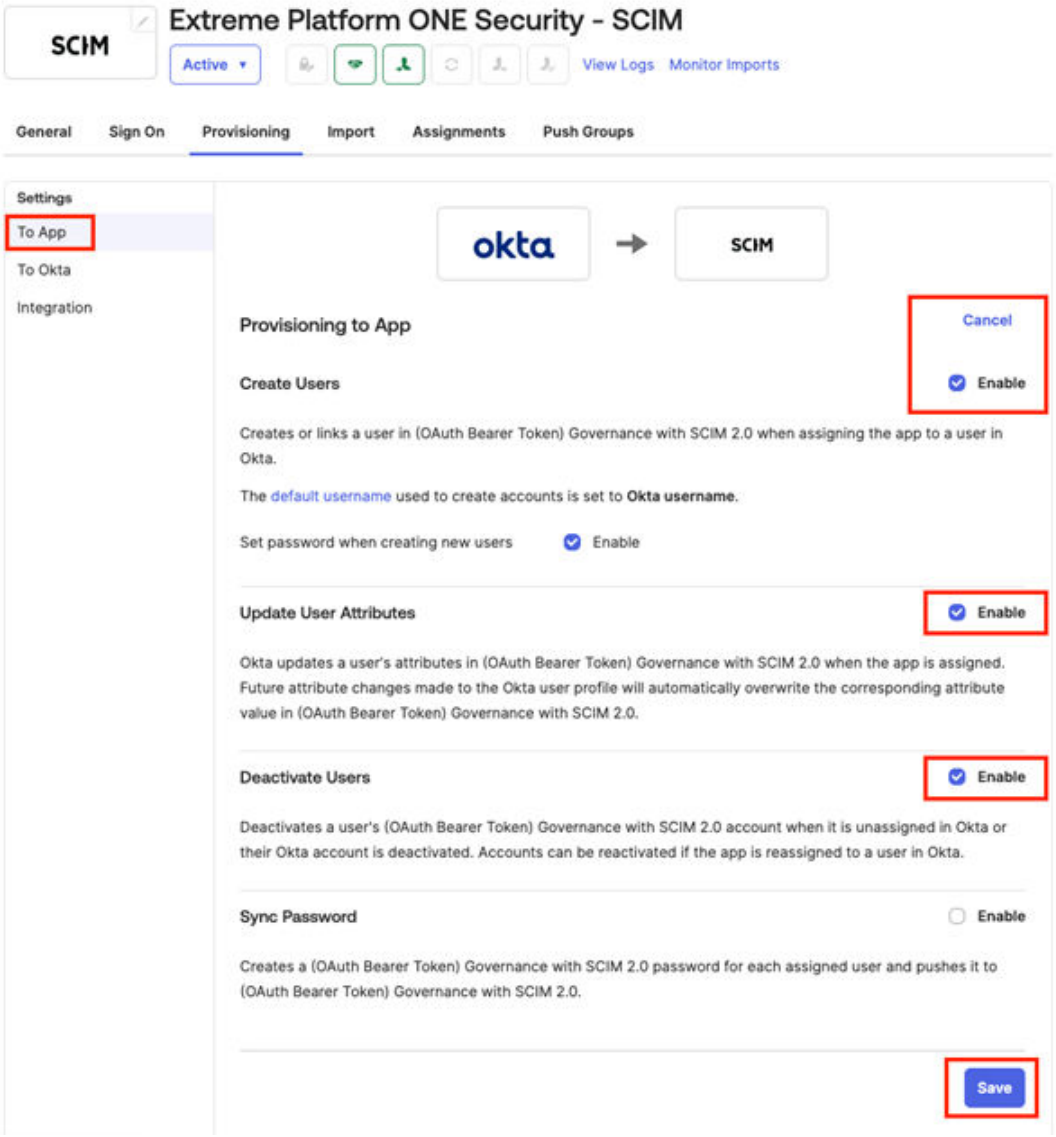



**Figure 86: Provisioning to App**

**Table 231: API Configuration Settings**

| Field | Description |
|---|---|
| Create Users | Enable this option. |
| Update User Attributes | Enable this option. |
| Deactivate Users | Enable this option. |

15. Select **Save**.
16. Go to **Assignments** > **Assign** and select **Assign to Groups** from the drop-down list.

17. Select **Assign** next to the groups that should be included with the synchronization into ExtremeCloud IQ (New).

> **Note**
> When assigning groups, do not change any defaults. Once you have selected the assign option, when prompted select **Save and Go Back**.

18. On the **Push Groups** tab, from the **Push Groups** drop-down list, select **Find groups by name**.
19. In the **Search** field enter the name of the group and select **Save** or **Save & Add Another** to add multiple. Repeat this action for each group that should be synchronized with ExtremeCloud IQ (New).
20. To view or change the status of the groups, go to the **Push Groups** tab. To force a push, select **Active** and select **Push now** from the drop-down list.

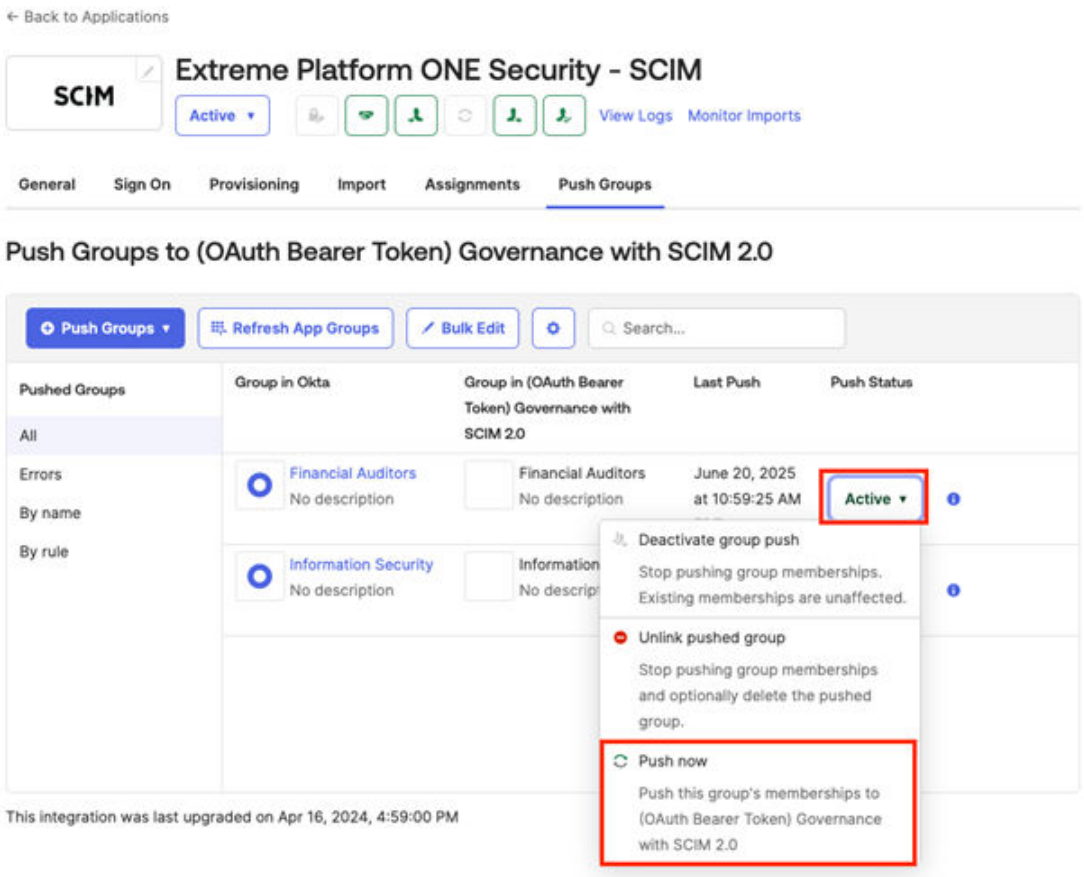



**Figure 87: Push Groups**

The users and user groups are now available in ExtremeCloud IQ (New) under **Policy** > **Users & Devices** > **Users**. If the user or group is not displayed, review errors or messages in Okta for the push failed description.

### Configure Okta SCIM

Use this task to configure Okta SCIM.

1. In the Okta administrator portal, go to the **Applications** > **Browse App Catalog**.

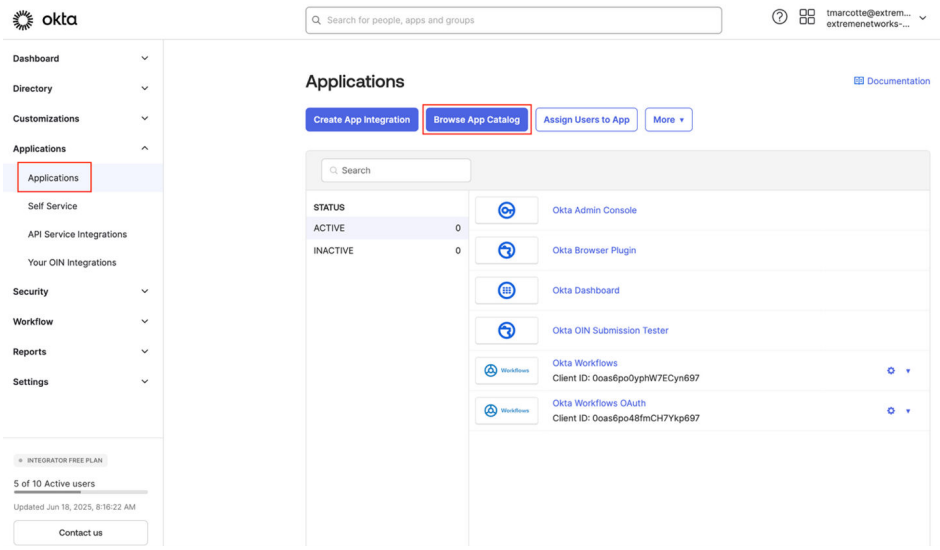



**Figure 88: Applications Menu**

2. In the search field, enter and select **(OAuth Bearer Token) Governance with SCIM 2.0**.
3. Select **Add Integration**.
4. On the **General Settings** tab, in the **Application label** field, enter **Extreme Platform ONE Security - SCIM** and select **Next**.
5. On the **Sign-On Options** tab, scroll to the bottom and select **Done**. No additional information needs to be added for the SCIM integration.
6. In the new application, select the **Provisioning** > **Configure API Integration** and configure the settings in Table 232.

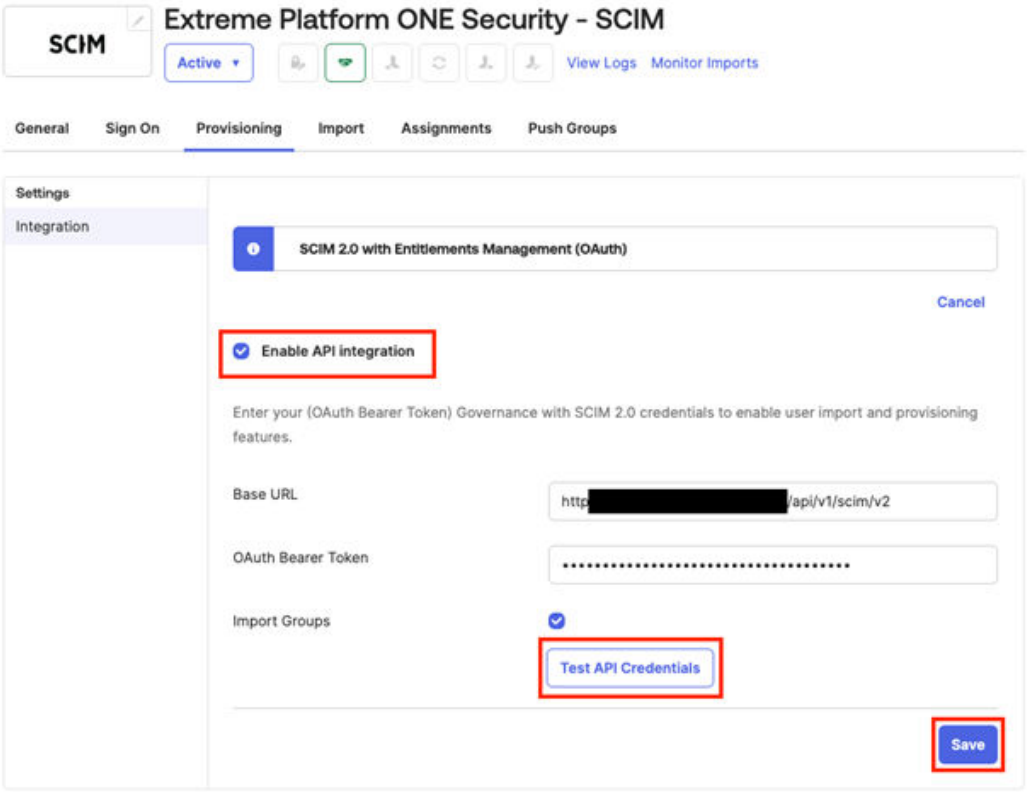



**Table 232: API Integration Configuration Settings**

| Field | Description |
|---|---|
| Enable API Integration | Select this option. |
| Base URL | Paste in the Tenant URL that was saved from ExtremeCloud IQ (New). |
| OAuth Bearer Token | Paste the Secret Token that was saved from ExtremeCloud IQ (New). |

7. Select **Test API Credentials**.

**Note**
If the credentials do not verify successfully, ensure there are not typos in the Tenant URL or Secret Token from the **IdP Profile** entry in ExtremeCloud IQ (New).

8. Upon successful verification, select **Save** and configure the settings in Table 233.

**Table 233: API Configuration Settings**

| Field | Description |
|---|---|
| Create Users | Enable this option. |
| Update User Attributes | Enable this option. |
| Deactivate Users | Enable this option. |

9. Select **Save**.

10. Go to **Assignments** > **Assign** and select **Assign to Groups** from the drop-down list.
11. Select **Assign** next to the groups that should be included with the synchronization into ExtremeCloud IQ (New).

    **Note**
    When assigning groups, do not change any defaults. Once you have selected the assign option, when prompted select **Save and Go Back**.

12. On the **Push Groups** tab, from the **Push Groups** drop-down list, select **Find groups by name**.
13. In the **Search** field enter the name of the group and select **Save** or **Save & Add Another** to add multiple. Repeat this action for each group that should be synchronized with ExtremeCloud IQ (New).
14. To view or change the status of the groups, go to the **Push Groups** tab. To force a push, select **Active** and select **Push now** from the drop-down list.

The users and user groups are now available in ExtremeCloud IQ (New) under **Policy** > **Users & Devices** > **Users**. If the user or group is not displayed, review errors or messages in Okta for the push failed description.

*Okta | Network Access*

If user-based 802.1X EAP-TTLS network authentication is going to be used with Okta, a separate application is required to be created that bypasses MFA as 802.1X does not have a native method to provide real-time multi-factor authentication prompt. This can only be done with an OpenID Connect (OIDC) Application.

**Okta | Network Access**

Use this task to configure ExtremeCloud IQ (New).

If user-based 802.1X EAP-TTLS network authentication is going to be used with Okta, a separate application is required to be created that bypasses MFA as 802.1X does not have a native method to provide real-time multi-factor authentication prompt. This can only be done with an OpenID Connect (OIDC) Application.

To configure Okta for Network Access:

1. Configure Okta Open ID Connect (OIDC).
2. Configure Extreme Platform ONE Security.

**Okta OIDC**

1. In the **Create a new app integration** window select **OIDC – OpenID Connect** as the sign-in method. For Application type select **Native Application** and then **Next**.

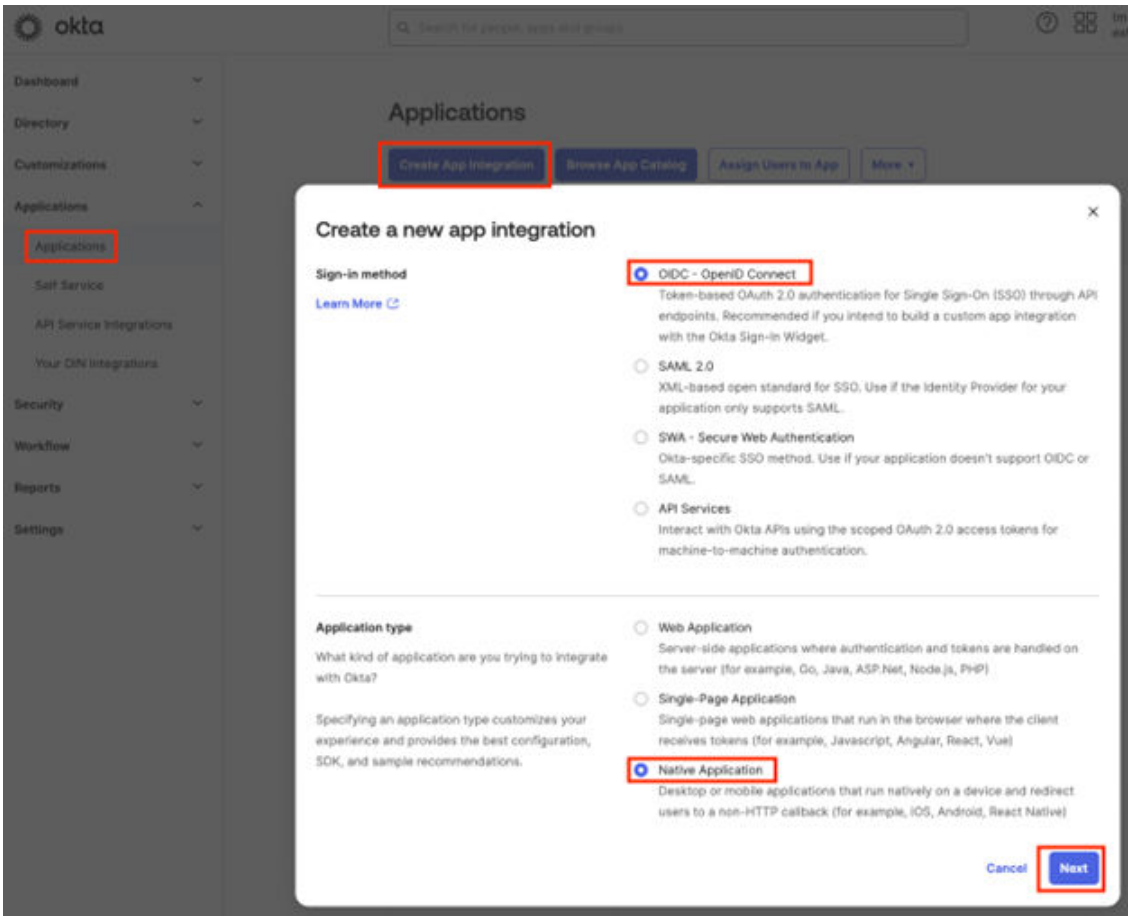



**Figure 89: New app integration**

a. In **New Native App Integration** window, name the application appropriately.
b. Under **Grant Type** select **Advanced**.

c. Under **Other Grants** select **Resource Owner Password**.

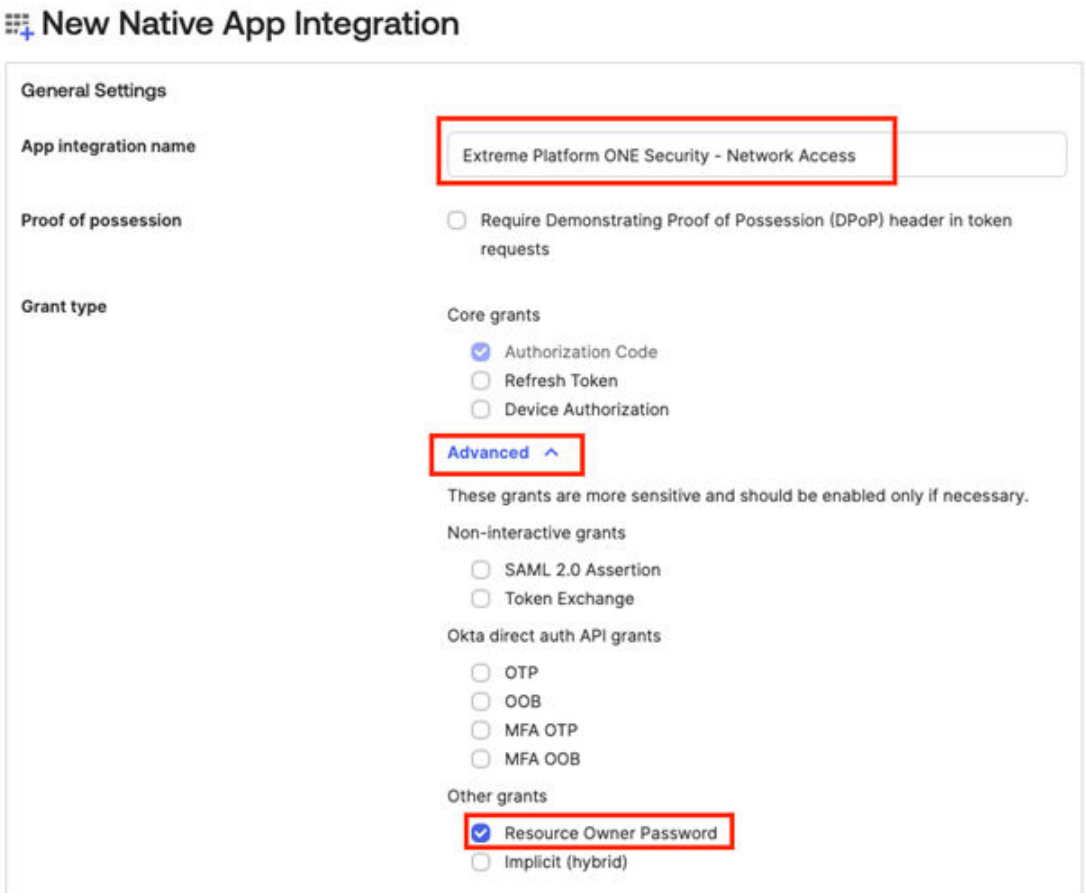



**Figure 90: Native App Integration**

d. Within the redirect URI sections maintain default settings.

e. Under **Assignments**, if there is a preference it can be used, however access is granted based on the policies in ExtremeCloud IQ (New).

f. If there is no preference, under **Controlled access** select **Allow everyone in your organization to access**.

g. Leave the check box for **Enable immediate access with Federation Broker Mode** enabled.

h. Select **Save**.

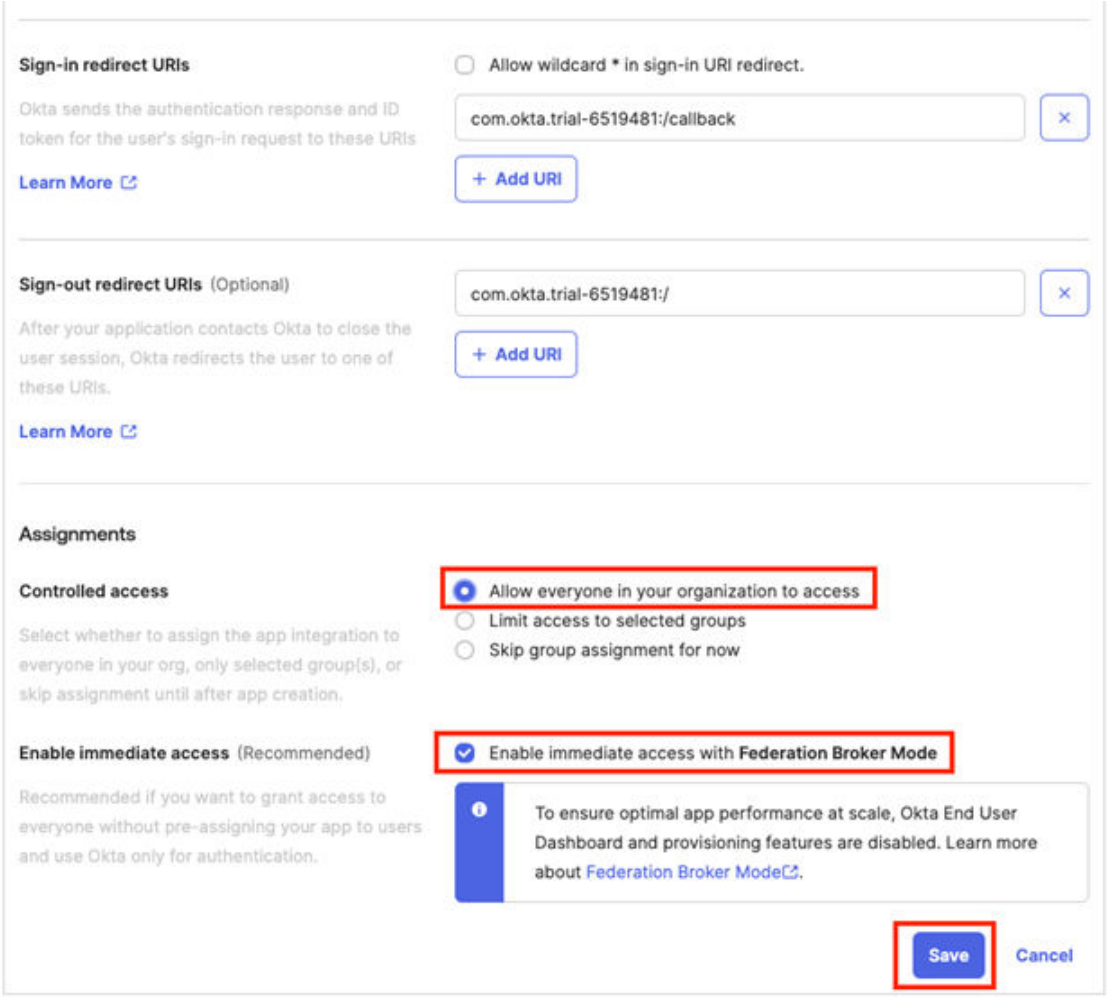



**Figure 91: Assignments**

2. Under **General**, under **Client Authentication** select **Client secret**.
   a. Select **Require PKCE as additional verification**.

b. Select **Save**.

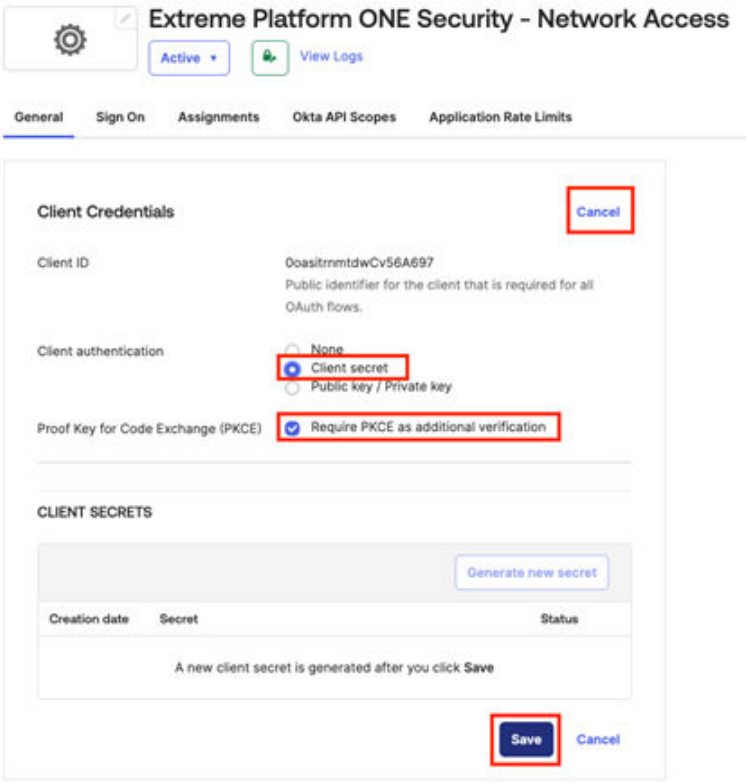



**Figure 92: Client Credentials**

3. To create a password-only authentication policy in Okta that is attached to this new application, go to **Security** > **Authentication Policies** and select **Add a policy**.
   a. In the **Add Authentication Policy** window, enter a policy name and description.
   b. Select **Save**.
4. Within the Password-Only authentication policy, under **Catch-all Rule** select **Edit** from the **Actions** drop-down list.

5. Within the **IF** section maintain default settings. Under **THEN** update the **User must authenticate with** to **1 factor type - Password** from the drop-down list and select **Save**.

   Once saved, the Authentication Policy should look similar to below:

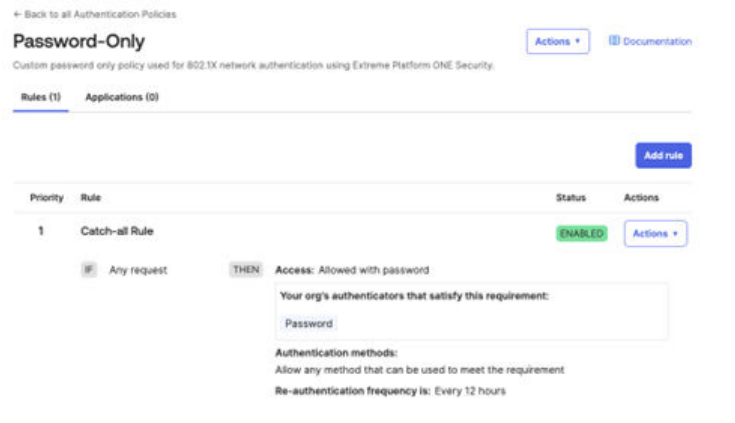



**Figure 93: Authentication Policy**

6. Go to **Applications**, select the Network Access Application previously created and do the following:
   a. Under **Sign One** > **User authentication** select **Password-Only** from the **Authentication policy** drop-down list.
   b. Select **Save**.
   c. Under **General** copy the generated Client ID and Client Secret.
7. If the Org Domain of the Okta tenant is required, select **Profile** and copy the tenant name.

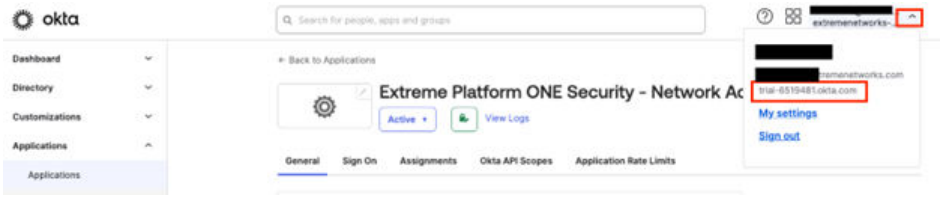



**Figure 94: Tenant Name**

**Extreme Platform ONE Security**

8. Go to **Administration & Settings** > **Access Management** > **Identity Providers** > **Network & Applications**.

9. To create a new profile, select **Add IdP Profile** and configure the settings in Table 229 on page 658.

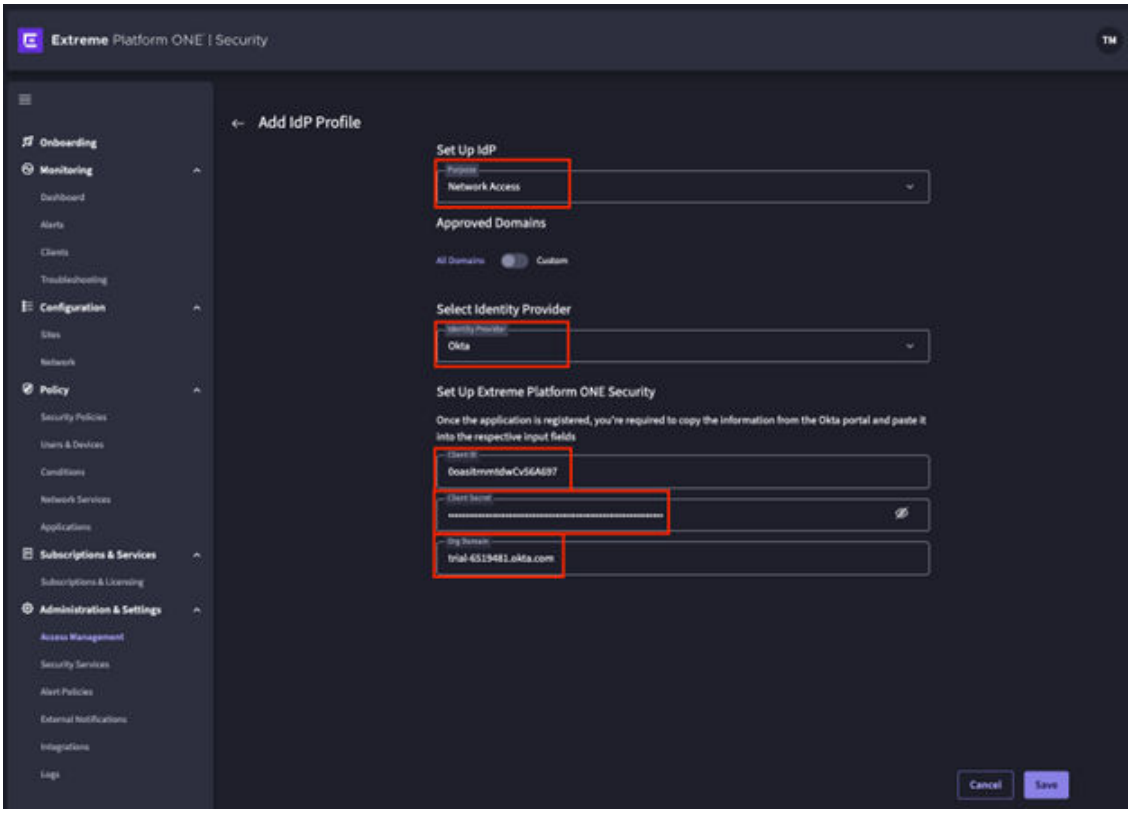



**Figure 95: IdP Profile**

**Table 234: Okta OIDC IdP Profile Configuration Settings**

| Field | Description | |
|---|---|---|
| Set Up IdP | Select **Network Access** from the Purpose drop-down list. | |
| Approved Domain | If the domain needs to be limited, it can be selected here, otherwise leave it to **All Domains**. | |
| Select Identity Provider | Select **Okta** from the Identity Provider drop-down list. | |
| Set Up Extreme Platform ONE Security | Client ID | Paste in the Client ID, Client Secret, and Tenant ID previously copied in Okta. |
| | Client Secret | |
| | Org Domain | |

10. Select **Save**.

### Configure Okta OIDC

Use this task to configure OIDC for Okta.

1. In the **Create a new app integration** window select **OIDC – OpenID Connect** as the sign-in method. For Application type select **Native Application** and then **Next**.

2. In **New Native App Integration** window, name the application appropriately. Under **Grant Type** select **Advanced** and under **Other Grants** select **Resource Owner Password**.
3. Within the redirect URI sections maintain default settings. Under **Assignments**, if there is a preference it can be used, however access is granted based on the policies in ExtremeCloud IQ (New). If there is no preference, under **Controlled access** select **Allow everyone in your organization to access**. Leave the checkbox for **Enable immediate access with Federation Broker Mode** enabled. Select **Save**.
4. Under **General**, under **Client Authentication** select **Client secret**. Select **Require PKCE as additional verification** and select **Save**.
5. To create a password-only authentication policy in Okta that is attached to this new application, go to **Security** > **Authentication Policies** and select **Add a policy**.
6. In the **Add Authentication Policy** window, enter a policy name and description. Select **Save**.
7. Within the Password-Only authentication policy, under **Catch-all Rule** select **Edit** from the **Actions** drop-down list.
8. Within the **IF** section maintain default settings. Under **THEN** update the **User must authenticate with** to **1 factor type - Password** from the drop-down list and select **Save**.

   Once saved, the Authentication Policy should look similar to below:

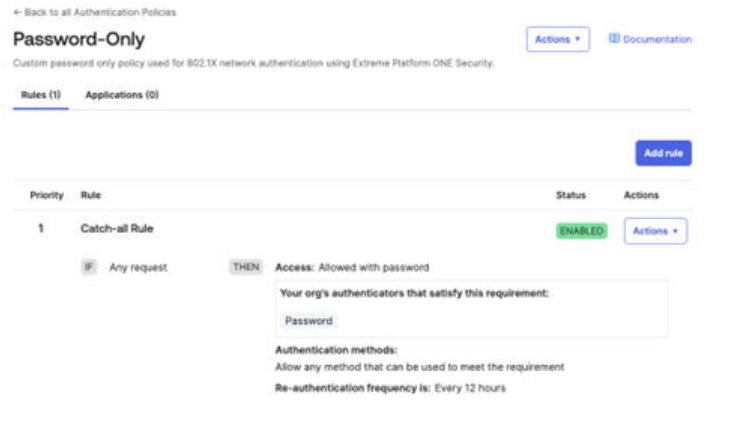



**Figure 96: Authentication Policy**

9. Go to **Applications**, select the Network Access Application previously created and do the following:
   a. Under **Sign One** > **User authentication** select **Password-Only** from the **Authentication policy** drop-down list.
   b. Select **Save**.
   c. Under **General** copy the generated Client ID and Client Secret.
10. If the Org Domain of the Okta tenant is required, select **Profile** and copy the tenant name.

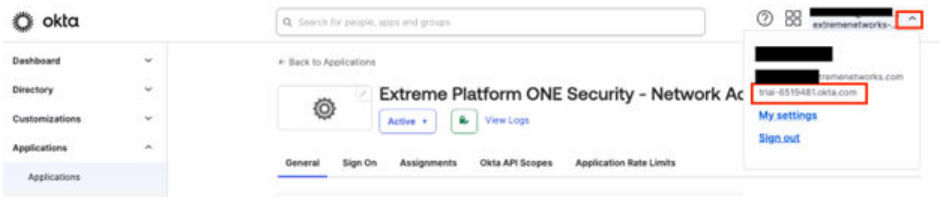



**Figure 97: Tenant Name**

*Okta | Application Access*

Application access for users can be authenticated via Okta in two ways: OpenID Connect (OIDC) or SAML. The setup process is different in Okta depending on the type of integration being leveraged.

**Okta | Application Access**

Application access for users can be authenticated via Microsoft Entra ID in two ways:

- Open ID Connect (OIDC)
  1. Retrieve Redirect URI in Extreme Platform ONE Security.
  2. Set up Okta Administrator Portal.
  3. Configure Extreme Platform ONE Security.
- SAML
  1. Configure Okta.
  2. Configure in Extreme Platform ONE Security.

The setup process is different in Okta depending on the type of integration being used.

**Application Access using Open ID Connect (OIDC)**

1. Retrieve Redirect URI In Extreme Platform ONE Security.
   a. Go to **Administration & Settings** > **Access Management** > **Identity Providers** > **Network & Applications**.

b. To create a new profile, select **Add IdP Profile** and configure the settings in Table 235.

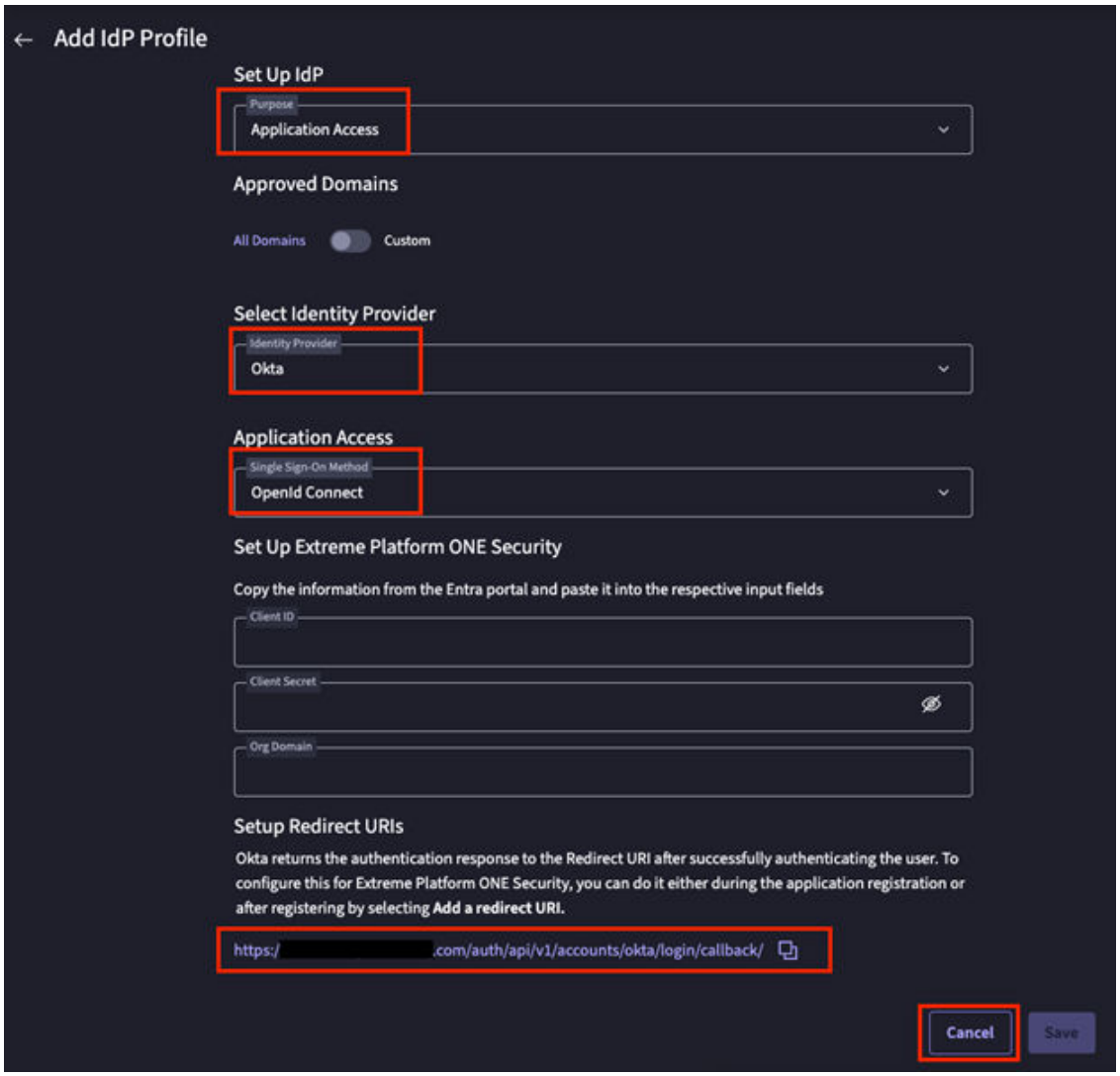



**Figure 98: IdP Profile**

**Table 235: Okta OIDC Application Access IdP Profile Configuration Settings**

| Field | Description |
|---|---|
| Set Up IdP | Select **Application Access** from the Purpose drop-down list. |
| Approved Domain | If the domain needs to be limited, it can be selected here, otherwise leave it to **All Domains**. |
| Select Identity Provider | Select **Okta** from the Identity Provider drop-down list. |
| Application Access | Select **OpenID Connect** from the Single Sign-On drop-down list. |
| Setup Redirect URIs | Copy the Redirect URI. |

c. Select **Cancel**.

2. Set up Okta Administrator Portal.
   a. Go to **Applications** then select **Create App Integration** and configure the settings. In the resulting window, select OIDC – OpenID Connect as the sign-in method. For **Application type** select **Web Application** and then **Next** and configure the settings in Table 236.

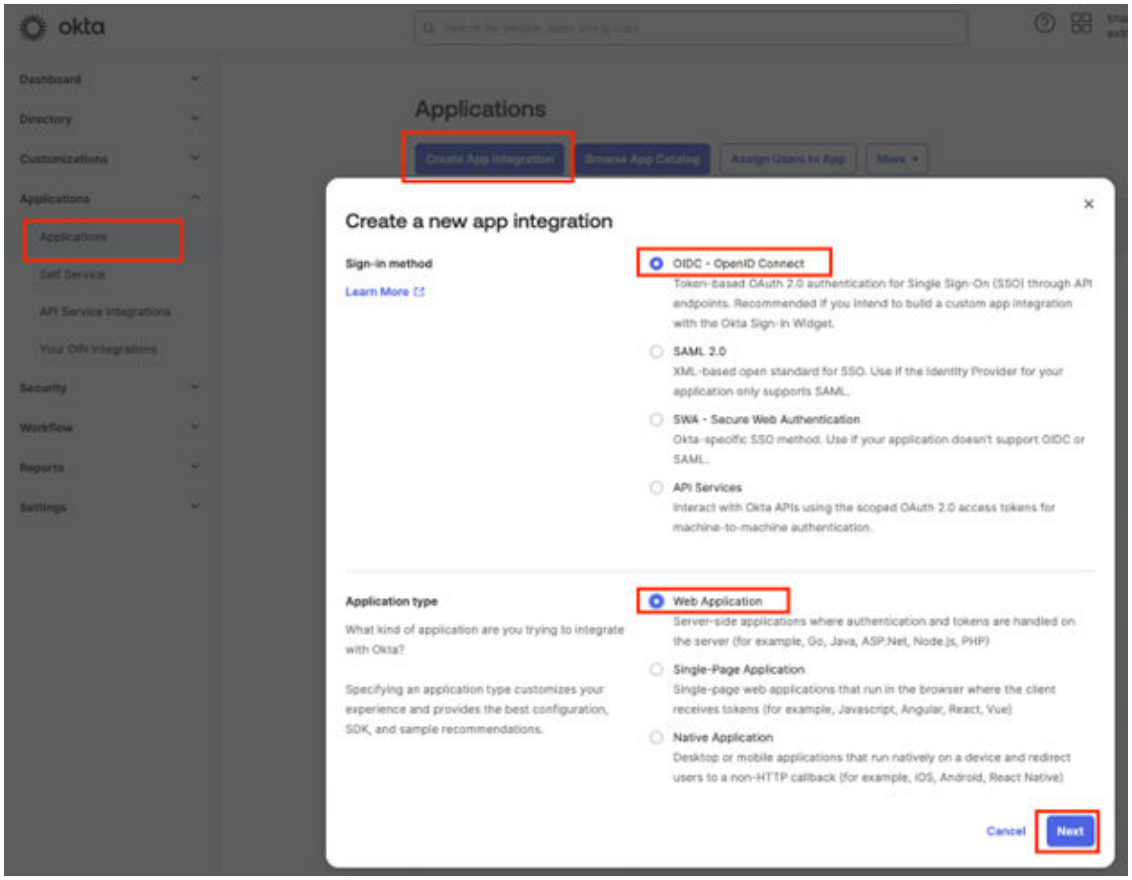



**Figure 99: New app integration**

**Table 236: Web Application Configuration Settings**

| Field | Description |
|---|---|
| Sign-in method | Select **OIDC – OpenID Connect**. |
| Application Type | Select **Web Application**. |

   b. Select **Next**.
   c. In the **New Web App Integration** window, enter a new integration name in the the **App Integration name** field and select **Client Credentials** under **Grant Type**.

d. Under **Sign-in redirect URIs**, paste the redirect URI saved when starting to create the application in ExtremeCloud IQ (New).

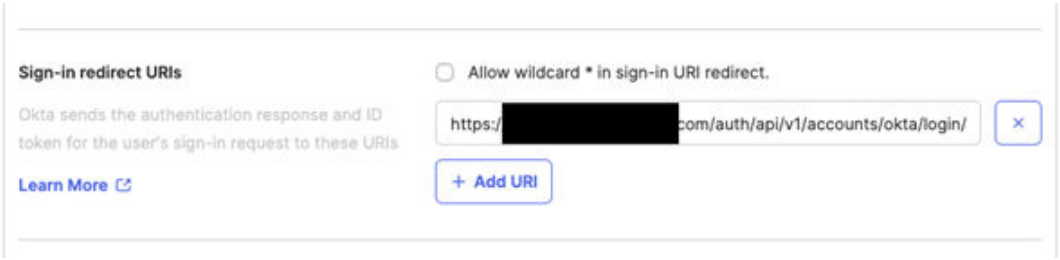



**Figure 100: Sign-in redirect URIs**

e. Leave the **Sign-out redirect URIs** and **Trusted Origins** to their defaults or clear them as they are not needed.

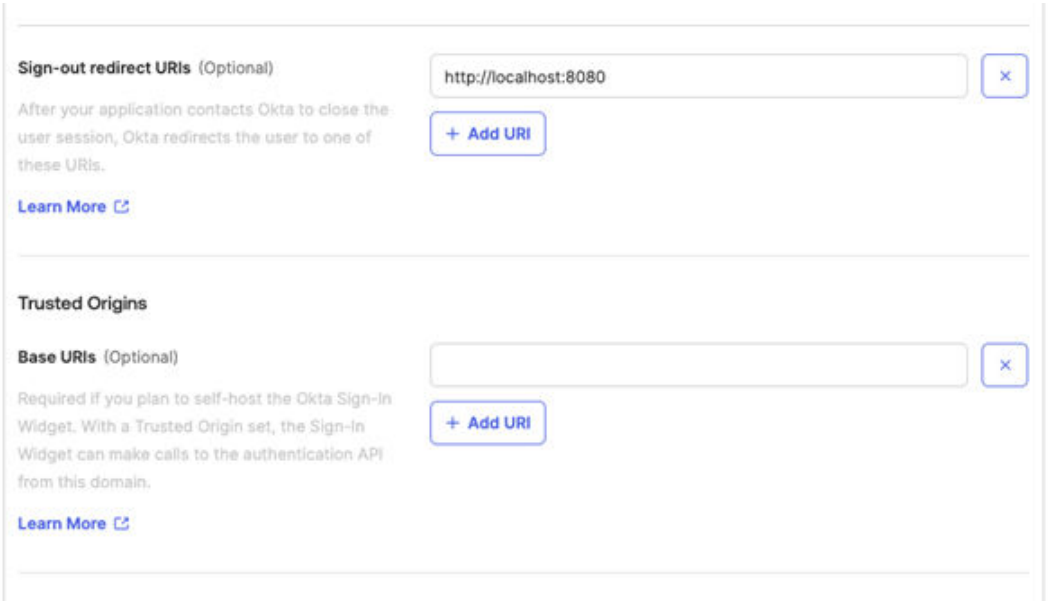



**Figure 101: Sign-out redirect URIs and Trusted Origins**

f. Under **Assignments** if there is a preference it can be used, however access is granted based on the policies in ExtremeCloud IQ (New). If there is no preference, select the **Allow everyone in your organization to access** option under **Controlled access**. Disable the check box for Enable immediate access. Select Save.

g. Disable the check box for **Enable immediate access with Federation Broker Mode** and select **Save**.

h. Under the **General** tab, copy the generated Client ID and Client Secret.
i. If the Org Domain of the Okta tenant is required, select **Profile** and copy the tenant name.

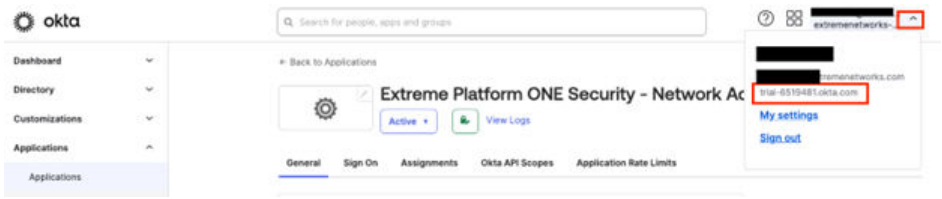



**Figure 102: Tenant Name**

3. Configure Extreme Platform ONE Security for OIDC.
   a. Go to **Administration and Settings** > **Access Management** > **Identity Providers** > **Network & Application**.
   b. Select **Add IdP Profile** and configure the settings in Table 237.

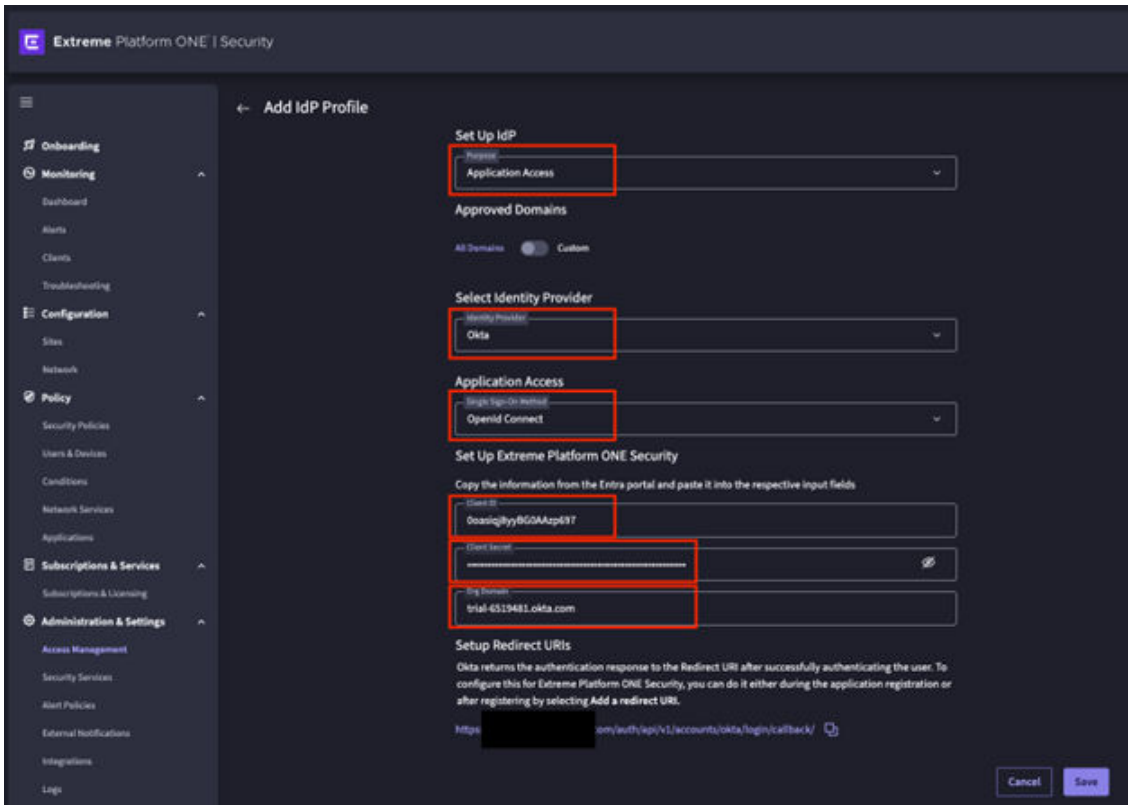



**Figure 103: IdP Profile**

**Table 237: Entra ID Application Access IdP Profile Configuration Settings**

| Field | Description |
|---|---|
| Set Up IdP | Select **Application Access** from the Purpose drop-down list. |
| Approved Domains | If the domain needs to be limited, it can be selected here with the **Custom** toggle, otherwise leave it to **All Domains** |

**Table 237: Entra ID Application Access IdP Profile Configuration Settings (continued)**

| Field | Description |
|---|---|
| Select Identity Provider | Select **Okta** from the **Identity Provider** drop-down list. |
| Secure Application Access | Under **Single Sign-On Method**, select **OpenID Connect**. |
| Setup Extreme Platform ONE Security | Paste the copied credentials from Okta:<br>• Client ID<br>• Client Secret<br>• Tenant ID |

c. To complete the setup, select **Save**.

**SAML**

4. Configure the Okta Administrator Portal for SAML.
   a. Go to the **Applications** then select **Browse App Catalog**.

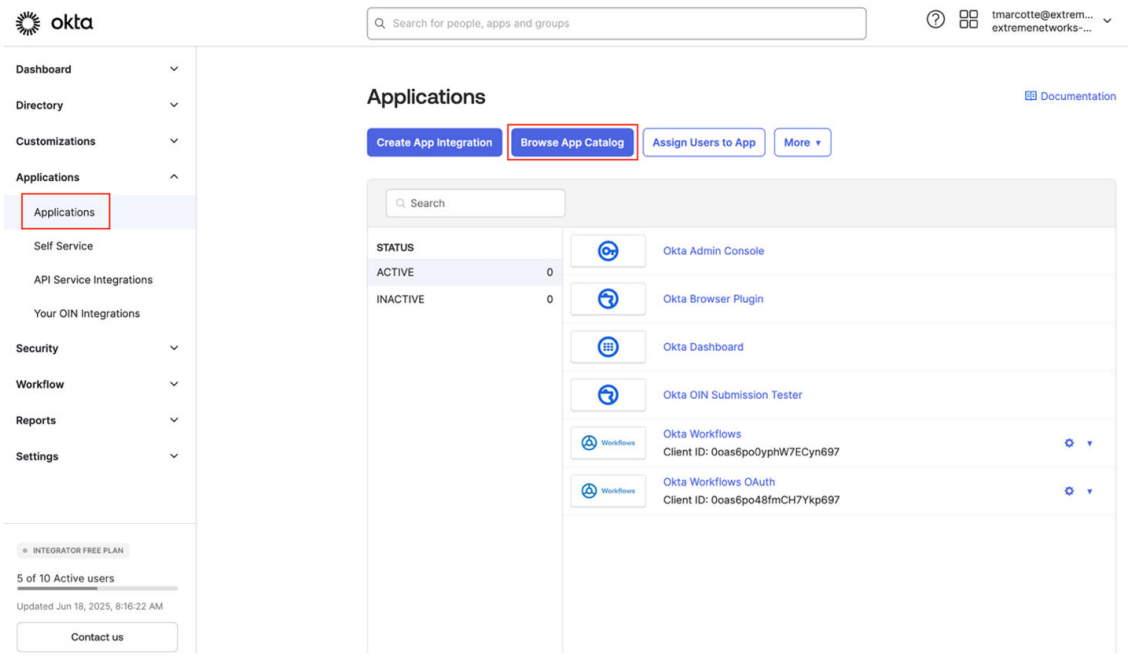



**Figure 104: App catalog**

   b. Search for **(OAuth Bearer Token) Governance with SCIM 2.0**. Select the app, then **Add Integration**.

c. Under **Application label** enter **Extreme Platform ONE Security – SAML** and select **Next**.

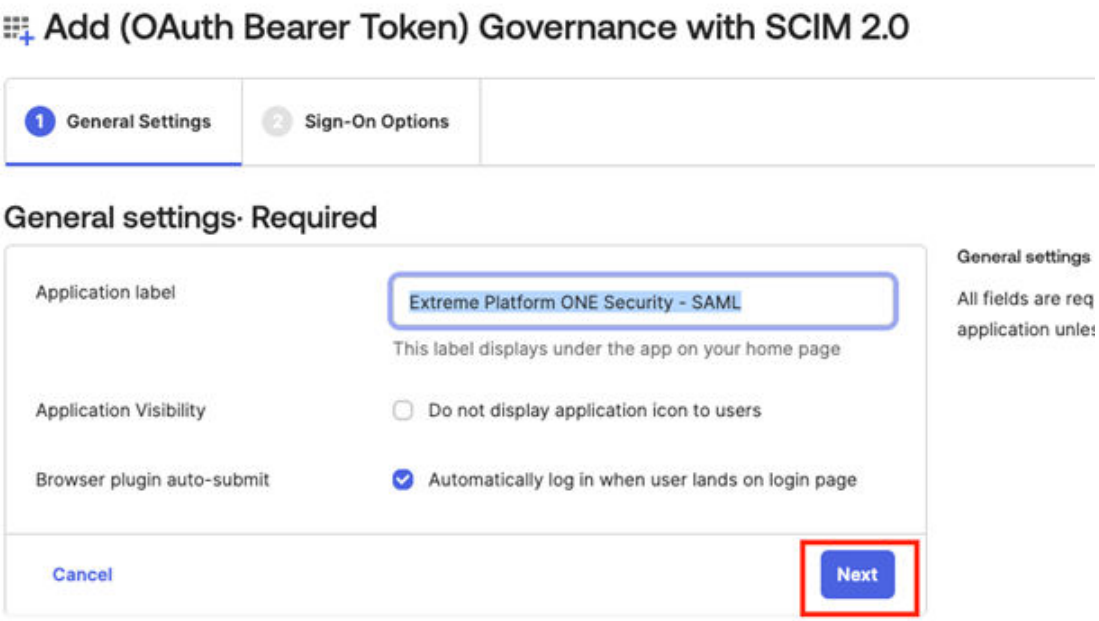



**Figure 105: General settings**

d. Under **Sign On Options**, expand the Attributes under SAML 2.0 and configure the settings in Table 238.

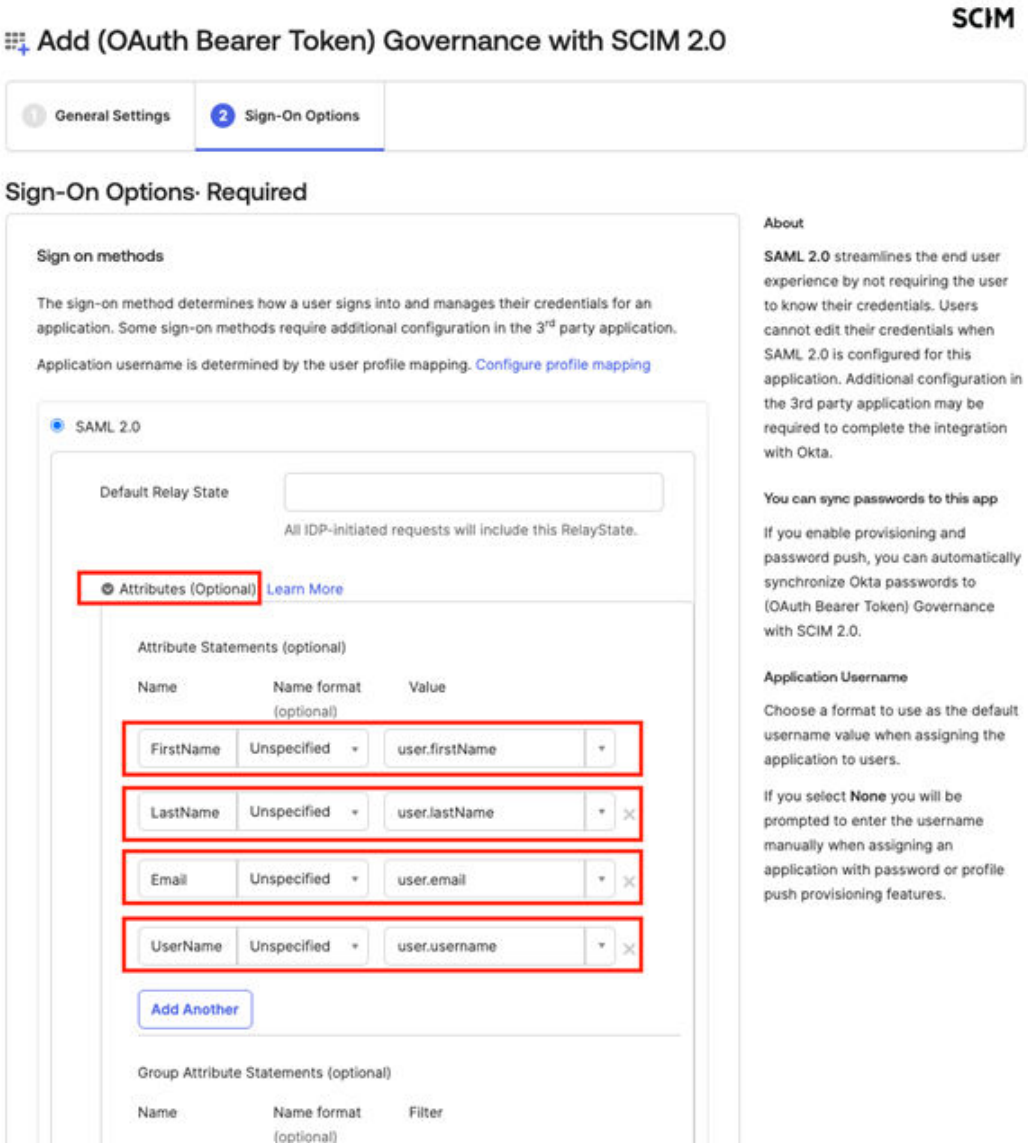



**Figure 106: Sign-On Options**

**Table 238: SAML 2.0 Configuration Settings**

| Field | Description |
|---|---|
| First Name | user.firstName |
| Last Name | user.lastName |
| Email | user.email |
| UserName | user.username |

e. Under **SAML 2.0**:

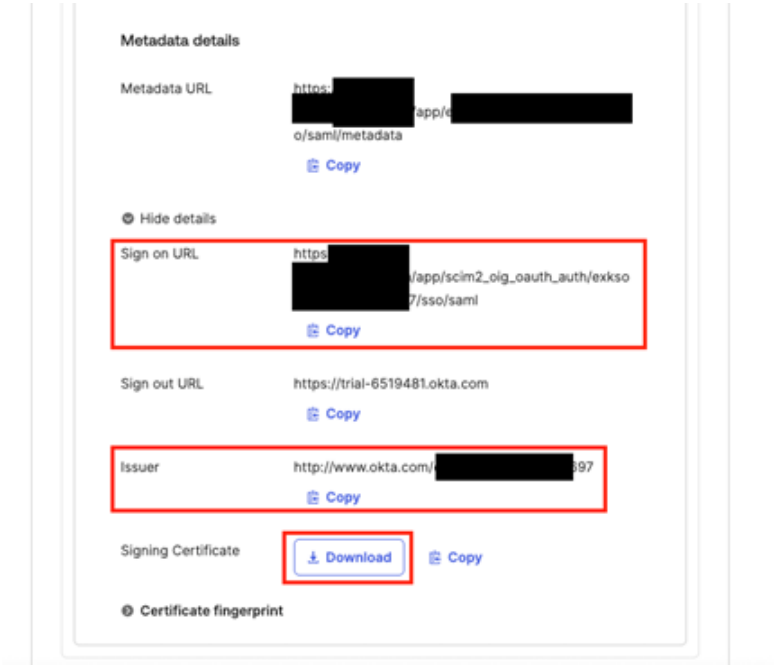



**Figure 107: Metadata details**

i. Expand **Metadata details**.
ii. Copy the Sign on URL and the Issuer for use in ExtremeCloud IQ (New).
iii. Download the Signing Certificate.
iv. Under **Advanced Sign-on**, paste the copied Reply URL Advanced Sign-on Settings section, paste the Reply URL previously copied from ExtremeCloud IQ (New) into the ACS URL field and the Identifier previous copied into Audience URI field.

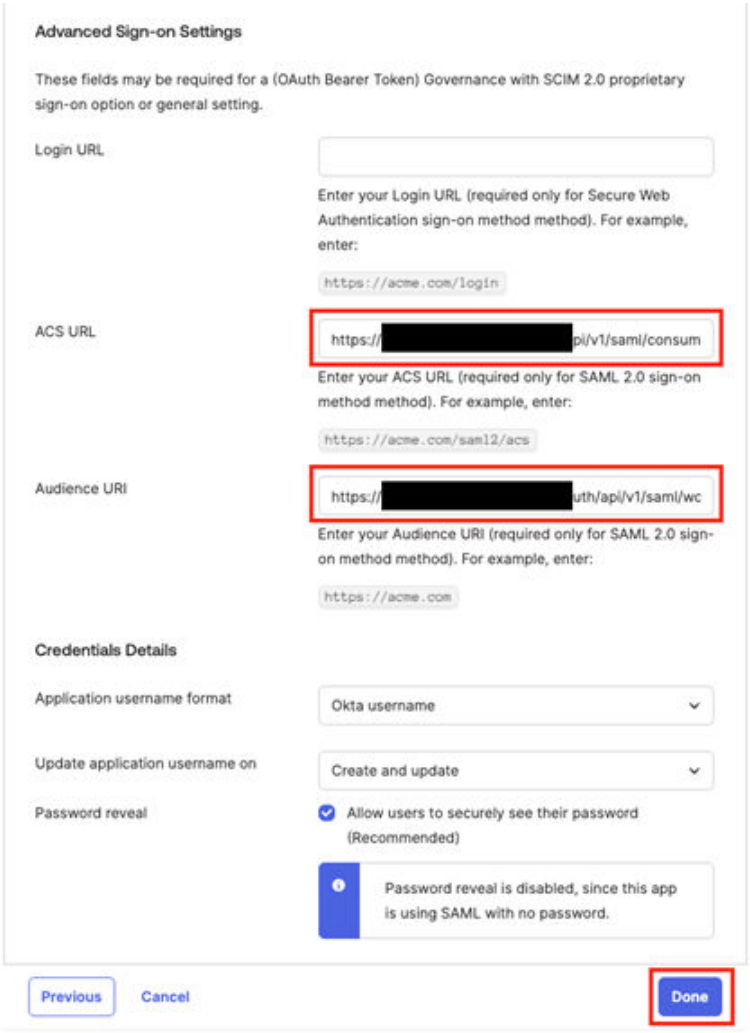



**Figure 108: Advanced Sign-on settings**

v. Select **Done**.

f. Under **Assignments**, select **Assign to Groups** from the Assign drop-down list.

g. Select specific users or groups and select **Done**.

All users are now displayed as assigned to the application.

5. Configure in Extreme Platform ONE Security for SAML.

a. In ExtremeCloud IQ (New), go to **Administration & Settings** > **Access Management** > **Identity Providers** > **Network & Applications**.

b. To create a new profile, select **Add IdP Profile** and configure the settings in Table 239.

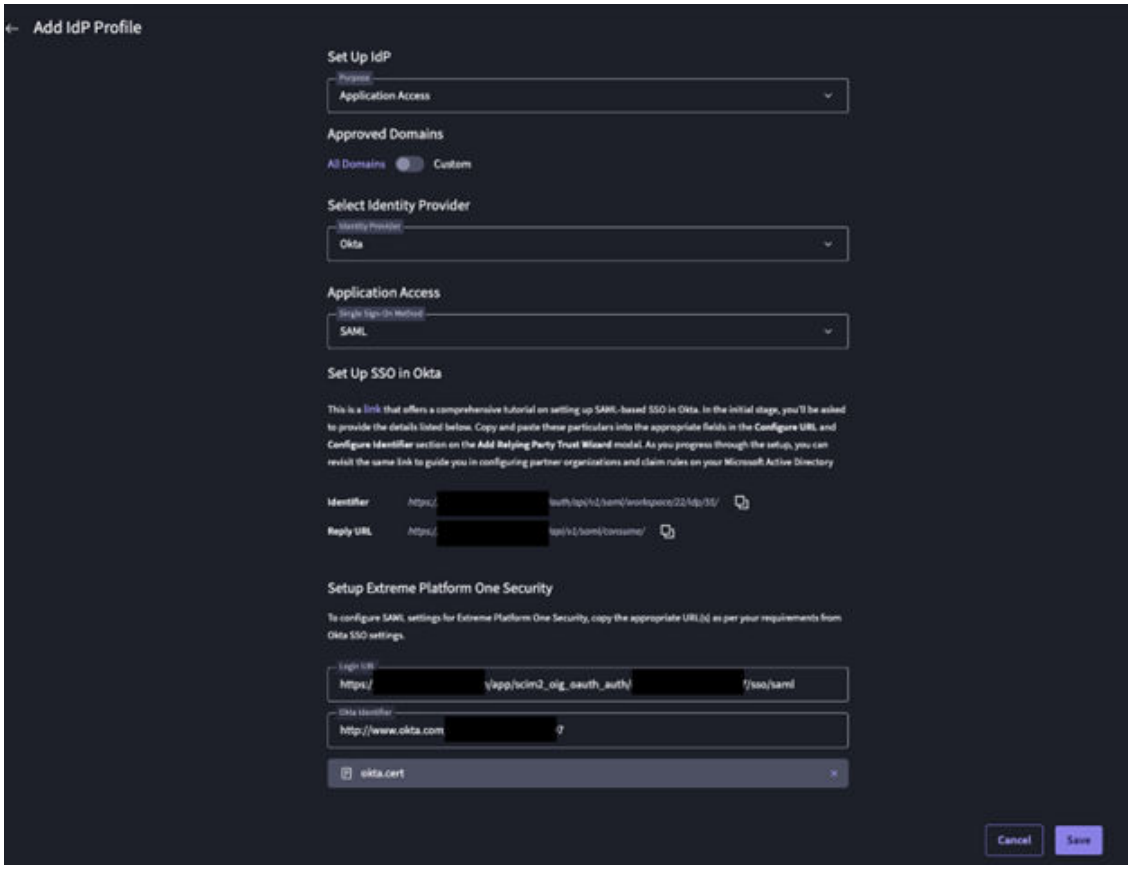



**Figure 109: IdP Profile**

**Table 239: SAML for Okta Configuration Settings**

| Field | Description | |
|---|---|---|
| Set Up IdP | Select **Application Access** from the Purpose drop-down list. | |
| Approved Domain | If the domain needs to be limited, it can be selected here, otherwise leave it to **All Domains**. | |
| Select Identity Provider | Select **Okta** from the Identity Provider drop-down list. | |
| Single Sign-On Method | Select **SAML**. | |
| Setup Extreme Platform ONE Security | Login URL | Paste in the Sign On URL in Okta. |
| | Okta Identifier | Paste in the Issuer from Okta. |

c. Select **Save**.

#### Configure Okta OIDC for Application Access

Use this task to configure Okta OIDC for Application Access.

1. In the Okta administrator portal, go to **Applications** then select **Create App Integration** and configure the settings. In the resulting window, select OIDC – OpenID Connect as the

sign-in method. For **Application type** select **Web Application** and then **Next** and configure the settings in Table 240.

**Table 240: Web Application Configuration Settings**

| Field | Description |
|---|---|
| Sign-in method | Select **OIDC – OpenID Connect**. |
| Application Type | Select **Web Application**. |

2. Select **Next**.
3. In the **New Web App Integration** window, enter a new integration name in the the **App Integration name** field and select **Client Credentials** under **Grant Type**.
4. Under **Sign-in redirect URIs**, paste the redirect URI saved when starting to create the application in ExtremeCloud IQ (New).
5. Leave the **Sign-out redirect URIs** and **Trusted Origins** to their defaults or clear them as they are not needed.
6. Under **Assignments** if there is a preference it can be used, however access is granted based on the policies in ExtremeCloud IQ (New). If there is no preference, select the **Allow everyone in your organization to access** option under **Controlled access**. Disable the checkbox for Enable immediate access. Select Save.
7. Disable the checkbox for **Enable immediate access with Federation Broker Mode** and select **Save**.
8. Under the **General** tab, copy the generated Client ID and Client Secret.
9. If the Org Domain of the Okta tenant is required, select **Profile** and copy the tenant name.

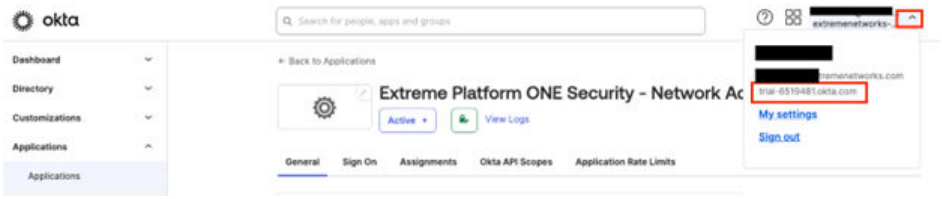



**Figure 110: Tenant Name**

### Configure ExtremeCloud IQ (New) for Okta OIDC Application Access

Use this task to configure ExtremeCloud IQ (New).

1. In ExtremeCloud IQ (New), go to **Administration & Settings** > **Access Management** > **Identity Providers** > **Network and Applications**.
2. To create a new profile, select **Add IdP Profile** and configure the settings in Table 241.

**Table 241: Idp Profile Settings**

| Field | Description |
|---|---|
| Set Up IdP | Select **Application Access** from the Purpose drop-down list. |
| Approved Domain | If the domain needs to be limited, it can be selected here, otherwise leave it to **All Domains**. |
| Select Identity Provider | Select **Okta** from the Identity Provider drop-down list. |

**Table 241: Idp Profile Settings (continued)**

| Field | Description | |
|---|---|---|
| Single Sign-On Method | Select **OpenID Connect**. | |
| Set Up Extreme Platform ONE Security | Client ID | Paste in the Client ID, Client Secret, and Tenant ID previously copied in Okta. |

3. Select **Save**.

#### Configure Okta SAML

Use this task to configure Okta SAML.

1. In the Okta administrator portal, go to the **Applications** then select **Browse App Catalog**.
2. Search for **(OAuth Bearer Token) Governance with SCIM 2.0**. Select the app, then **Add Integration**.
3. Under **Application label** enter **Extreme Platform ONE Security – SAML** and select **Next**.
4. Under **Sign On Options**, expand the Attributes under SAML 2.0 and configure the settings in Table 242.

**Table 242: SAML 2.0 Configuration Settings**

| Field | Description |
|---|---|
| First Name | user.firstName |
| Last Name | user.lastName |
| Email | user.email |
| UserName | user.username |

5. Under **SAML 2.0**:
   a. Expand **Metadata details**.
   b. Copy the Sign on URL and the Issuer for use in ExtremeCloud IQ (New).
   c. Download the Signing Certificate.
   d. Under **Advanced Sign-on**, paste the copied Reply URL Advanced Sign-on Settings section, paste the Reply URL previously copied from ExtremeCloud IQ (New) into the ACS URL field and the Identifier previous copied into Audience URI field.
   e. Select **Done**.
6. Under **Assignments**, select **Assign to Groups** from the Assign drop-down list.
7. Select specific users or groups and select **Done**.

   All users are now displayed as assigned to the application.

#### Configure ExtremeCloud IQ (New) SAML for Okta

Use this task configure ExtremeCloud IQ (New) SAML for Okta.

1. In ExtremeCloud IQ (New), go to **Administration & Settings** > **Access Management** > **Identity Providers** > **Network & Applications**.

2. To create a new profile, select **Add IdP Profile** and configure the settings in Table 243.

**Table 243: SAML for Okta Configuration Settings**

| Field | Description | |
|---|---|---|
| Set Up IdP | Select **Application Access** from the Purpose drop-down list. | |
| Approved Domain | If the domain needs to be limited, it can be selected here, otherwise leave it to **All Domains**. | |
| Select Identity Provider | Select **Okta** from the Identity Provider drop-down list. | |
| Single Sign-On Method | Select **SAML**. | |
| Setup Extreme Platform ONE Security | Login URL | Paste in the Sign On URL in Okta. |
| | Okta Identifier | Paste in the Issuer from Okta. |

3. Select **Save**.

## IdP Network & Applications | Support Multiple IdPs

Use this task to support and prioritize multiple IdP with a single tenant.

1. Log into your ExtremeCloud IQ (New) tenant.
2. Go to **Administration and Settings** > **Access Management** > **Identity Providers** > **Network & Applications**.
3. To prioritize IdPs, select and drag the IdPs in the correct order or the check box next to an Idp and from the select and select **Move to the top** or **Move to the bottom** from the drop-down list.
4. In the IdP Priority popup message, select **Save**.

# Identity Providers | Management

You can configure one or more identity providers (IdPs) to implement role-based access and single sign-on (SSO) functionality.

An IdP profile defines how ExtremeCloud IQ (New) interacts with an external IdP for user authentication. By creating an IdP profile, you allow your system to authenticate users for the defined domain, governed by the role and site-assignment rules in the IdP profile. ExtremeCloud IQ (New) SSO supports both IdP and Service Provider (SP) login methods. IdP Multi-factor Authentication (MFA) rules are supported on login.

The following IdPs are supported by ExtremeCloud IQ (New):

- Generic SAML Server
- Active Directory Federation Service (ADFS)
- Ping
- Okta
- Microsoft Entra ID

- OneLogin
- Auth0

**Note**
As a prerequisite to adding an IdP to ExtremeCloud IQ (New), you must configure your IdP before you begin.

From **Administration & Settings** > **Access Management** > **Identity Providers** > **Management**, you can integrate an external IdP with ExtremeCloud IQ (New). The configuration overview in Table 244 outlines the actions required to integrate an external IdP with ExtremeCloud IQ (New).

**Table 244: IdP Integration Configuration Overview**

| Action Navigation | Action Description |
|---|---|
| **Prepare the IdP**<br>Configure the IdP with the required users, groups, and application settings needed to support integration with ExtremeCloud IQ (New). This section summarizes the key IdP configuration actions performed prior to establishing trust. | |
| Create users | Create user accounts in your IdP. User identities must exist in the IdP before they can authenticate into ExtremeCloud IQ (New). User attributes (such as username or email) must align with ExtremeCloud IQ (New) for identification and authentication. For detailed instructions, refer to your IdP documentation. |
| Create groups | Create groups in your IdP that represent role or access boundaries. For detailed instructions, refer to your IdP documentation.<br><br>**Note:** ExtremeCloud IQ (New) uses group membership information provided by the IdP to assign roles through its RBAC implementation. The IdP must be configured to send group membership claims to ExtremeCloud IQ (New) during authentication. |
| Create IdP application | Create an application in your IdP to represent ExtremeCloud IQ (New). This application defines the trust relationship between the IdP and ExtremeCloud IQ (New) and controls authentication behavior, claims, and attribute mappings.<br>• To create a new application in Entra ID, see Microsoft Entra ID \| Create IdP Application on page 700.<br>• To create a new application in Okta, see Okta \| Create IdP Application on page 705. |
| Export metadata | Export the IdP metadata from the IdP application. The metadata contains the information ExtremeCloud IQ (New) requires to establish trust with the IdP, such as entity identifiers, endpoints, and signing certificates. This metadata is later imported into ExtremeCloud IQ (New) to complete the IdP configuration. To export the metadata from your IdP, refer to your IdP documentation. |
| **Prepare ExtremeCloud IQ (New)**<br>The following section summarizes the configuration actions performed when adding an IdP profile. To prepare for integration with an external IdP, complete the steps in Add an IdP Profile on page 692. To modify an existing external IdP, see Manage IdP Profiles on page 697. | |

**Table 244: IdP Integration Configuration Overview (continued)**

| Action Navigation | Action Description |
|---|---|
| Select an IdP provider | Select the IdP type to be used for authentication. The selected provider determines the available configuration options, supported authentication protocols, and metadata format used during integration. |
| Define the domain | Define the fully qualified domain name (FQDN) based on the selected IdP. This domain is used by ExtremeCloud IQ (New) to route authentication requests to the correct VIQ. |
| Import IdP Metadata | Import the metadata file exported from the IdP.<br>The IdP metadata establishes the trust relationship between ExtremeCloud IQ (New) and the IdP. It contains the IdP's entity information, endpoints, and signing certificates required to validate authentication assertions.<br>For information on how to import the IdP metadata into ExtremeCloud IQ (New), see Configure IdP Connection Metadata on page 692. |
| Define attributes for info sharing | Define and map the attributes that are exchanged between the IdP and ExtremeCloud IQ (New) during authentication.<br>These attributes identify users and can include values such as username, email address, or display name. Attribute mappings must align with the attributes configured in the IdP so that ExtremeCloud IQ (New) can correctly identify and authenticate users.<br>For more information, see Map User Profile Attributes on page 695. |
| Define IdP group membership to RBAC role assignment | Map IdP group membership to ExtremeCloud IQ (New) RBAC roles.<br>ExtremeCloud IQ (New) relies on group membership claims provided by the IdP to assign roles during user authentication. Each IdP group must be explicitly mapped to one role to ensure users receive the appropriate permissions upon login.<br>For more information, see Map User Profile Attributes on page 695. |
| Export metadata | Export metadata from ExtremeCloud IQ (New).<br>The exported metadata contains the service provider information required by the IdP, such as entity identifiers and endpoints. This metadata is imported into the IdP application to complete the trust configuration between the IdP and ExtremeCloud IQ (New).<br>For more information, see Export SP Metadata on page 696. |
| **Finalize the IdP**<br>Complete the final integration steps to establish trust between ExtremeCloud IQ (New) and the IdP. This section outlines the key actions required to finalize configuration and align the IdP with the ExtremeCloud IQ (New) profile. | |
| Import metadata | Import the metadata exported from ExtremeCloud IQ (New) into the IdP application.<br>This step completes the trust relationship by providing the IdP with Extreme Platform ONE service provider information, such as entity identifiers, endpoints, and certificates.<br>For more information on importing metadata into Microsoft Entra ID, see step 8 on page 704 in **Integrating with Microsoft Entra ID**. |

**Table 244: IdP Integration Configuration Overview (continued)**

| Action Navigation | Action Description |
|---|---|
| Adjust attributes | Review and update user and group attributes in the IdP. Ensure that attributes and claims used for user identification and group membership align with the mappings defined in ExtremeCloud IQ (New). |
| Clean up temp values | Some IdPs require manual cleanup of temporary values created in an earlier step, while others remove those values automatically during the metadata exchange. To replace temporary URLs within Okta, see Step 7.b on page 709. |
| **Test Logins**<br>Validate the IdP integration by performing authentication tests using both SP- and IdP-initiated login flows. These tests confirm that trust is established, attributes are mapped correctly, and users can successfully authenticate into ExtremeCloud IQ (New). | |
| Entra ID Test — IdP initiated | Initiate a login from the Microsoft Entra ID application and authenticate into ExtremeCloud IQ (New).<br>This test validates the IdP-initiated SSO flow, confirming that Entra ID can launch authentication to ExtremeCloud IQ (New) and that assertions are accepted and processed correctly. For more information, see step 9 on page 704 in **Integrating with Microsoft Entra ID**. |
| Entra ID Test — SP initiated | Initiate a login to ExtremeCloud IQ (New) directly and authenticate through Microsoft Entra ID.<br>This test validates the SP–initiated SSO flow, ensuring that authentication requests are correctly redirected to Entra ID and that users can successfully access ExtremeCloud IQ (New). For more information, see step 10 on page 704 in **Integrating with Microsoft Entra ID**. |
| Okta Test — IdP initiated | Initiate a login from the Okta application and authenticate into ExtremeCloud IQ (New).<br>This test validates the IdP-initiated SSO flow for Okta, confirming that Okta can successfully authenticate users and pass assertions to ExtremeCloud IQ (New). For more information, see step 8 on page 711 in **Integrating with Okta**. |
| Okta Test — SP initiated | Initiate a login to ExtremeCloud IQ (New) directly and authenticate through Okta.<br>This test verifies the SP–initiated SSO flow for Okta, ensuring successful redirection, authentication, and access to ExtremeCloud IQ (New). For more information, see step 9 on page 711 in **Integrating with Okta**. |

## Add an IdP Profile

You add an identity provider profile to begin the workflow that integrates an IdP with your application to enable single sign-on (SSO) authentication for your ExtremeCloud IQ (New) administrators. SSO authentication can be used with both IdP- and SP-initiated SSO.

**Important**
This task is part of a larger workflow. It is important to complete all steps in order. Skipping steps can result in incomplete configurations and require you to repeat parts of the process.

The following IdPs are supported by ExtremeCloud IQ (New):

- Generic SAML Server
- Active Directory Federation Service (ADFS)
- Ping
- Okta
- Microsoft Entra ID
- OneLogin
- Auth0

Use this task to add an IdP profile to your network.

1. Go to **Administration & Settings** > **Access Management** > **Identity Providers**, and then select **Management**.
2. Select **+ Add IdP Profile**.
3. Select an IdP **Provider**, and then select **Next**.
4. Configure the following **IdP Profile Information**, and then select **Next**:
   - **Domain**: Enter a fully qualified domain name (FQDN) based on the identity provider you selected in the preceding step.

     **Note**

   - **Description** (optional): Enter a description of up to 64 characters.
5. Configure IdP Connection Metadata, and then select **Next**.
6. Map User Profile Attributes, and then select **Save**.
7. Export SP Metadata on page 696, and then select **Done** to save the IdP profile.

Related Links

Microsoft Entra ID | Create IdP Application on page 700

Okta | Create IdP Application on page 705

*Configure IdP Connection Metadata*

Identity Provider (IdP) Metadata provides structured information that is used to configure and establish a connection between an IdP and a Service Provider (SP) in a SAML (Security

Assertion Markup Language) environment. This metadata includes details such as the following:

- **IdP Entity ID**: A unique identifier for an IdP used to identify the IdP to an SP.
- **SSO URLs**: Endpoints where the SP sends authentication requests.
- **Binding Methods**: Methods for communication between the IdP and SP.
- **Certificates**: Used for signing and encrypting SAML assertions.

**Important**
This task is part of a larger workflow. It is important to complete all steps in order. Skipping steps can result in incomplete configurations and require you to repeat parts of the process.

Metadata can be provided as a file (Import Metadata), as URL (Import from URL), or you can Enter Metadata Manually.

#### Import Metadata

1. Select **Import From Metadata**.
2. Select **Browse Files**, then select the metadata file from your local folder.
3. Configure any missing settings that are specific to the selected IdP. For more information, see IDP Metadata Settings Descriptions.
4. Click **Next** to map user profile attributes.

**Note**
If there is a problem uploading your file, check the file format and then try again. For further assistance, reach out to the Support Center.

#### Import from URL

1. Select **Import From URL**.
2. Type or paste an **IdP Metadata URL**, and then select **Import**.

**Note**
If the import was not successful, clear the URL and try again.

3. Configure any missing settings that are specific to the selected IdP. For more information, see IDP Metadata Settings Descriptions.
4. Click **Next** to map user profile attributes.

#### Enter Metadata Manually

1. Select **Manually Enter**.
2. Configure the IdP metadata settings that are described in IDP Metadata Settings Descriptions.

3. Click **Next** to map user profile attributes.

**Table 245: IDP Metadata Settings Descriptions**

| Setting | Description |
|---|---|
| IdP Entity ID | The IdP unique identifier URL. URLs must begin with `https`. |
| SSO Binding | Select **HTTP POST** to send messages within the body of an HTTP POST request.<br>Select **HTTP Redirect** to send encoded messages as query parameters in the URL of an HTTP GET request. |
| SSO URL | The endpoint where SSO authentication requests are sent. URLs must begin with `https`. |
| SSO Request | Select **SSO Request** to enhance SSO security. By signing the SSO request, you ensure its authenticity and integrity, confirming that it has not been tampered with. |
| SLO Binding | Single Logout (SLO) allows users to sign out from multiple applications or services with a single action.<br>Select **HTTP POST** to send messages within the body of an HTTP POST request.<br>Select **HTTP Redirect** to send encoded messages as query parameters in the URL of an HTTP GET request. |
| SLO URL | The endpoint where logout requests are sent to start the SLO process. This URL ensures that when a user logs out from one service, they are also logged out from all connected services. URLs must begin with `https`. |
| SLO Response URL | The endpoint where the Service Provider (SP) sends logout response messages after receiving a logout request from the IdP. This URL is used to confirm the completion of the SLO process. URLs must begin with `https`. |
| Verification Certificate | The digital certificate used to verify the authenticity and integrity of messages exchanged between the IdP and SPs.<br>Select an existing certificate from the drop-down list, or Import a new certificate. |

#### Import Verification Certificates

1. Select **Import Certificates**.
2. Drag and drop the certificate or browse to upload it to the **Verification Certificates** area.
3. Click **Next**.

Related Links

Add an IdP Profile on page 692

*Map User Profile Attributes*

You must map the appropriate User Profile Attributes to the SAML Attributes sent from the IdP. These strings must be created and be in sync with both IdP and SP.

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

Use this task to map user profile attributes to SAML profile attributes when you add a new IdP profile.

**Important**
This task is part of a larger workflow. It is important to complete all steps in order. Skipping steps can result in incomplete configurations and require you to repeat parts of the process.

1. Configure the following SAML attributes:
   - **First Name**: The URL or endpoint where the IdP provides the user's given name. For example, `https://schemas.xmlsoap.org/ws/2005/05/identity/ claims/givenname`
   - **Last Name**: The URL or endpoint where the IdP provides the user's family name or surname. For example, `https://schemas.xmlsoap.org/ws/2005/05/identity/claims/surname`
   - **Email**: The URL or endpoint where the IdP provides the user's email address. For example, `https://schemas.xmlsoap.org/ws/2005/05/identity/ claims/surname`
   - **IdP Group**: The URL or endpoint where the IdP provides the user's group memberships. For example, `https://schemas.microsoft.com/ws/2008/06/identity/ claims/groups`

   **Note**
   Default SAML attributes are automatically populated based on the selected IdP type.

2. (Optional) To add a new group mapping, select **+ Add a Group Mapping** and configure the settings in Table 246. You can add as many group mappings as needed.

**Table 246: Group Mapping Settings**

| Field | Description |
|---|---|
| IdP Groups | The IdP group name. |
| Primary Role | Select the **Primary Role** for this group from the list. The corresponding **Classic Role** populates based on the selected primary role. |

**Table 246: Group Mapping Settings (continued)**

| Field | Description |
|---|---|
| Classic Role | **Note:** Hover over ⓘ for information about access and access limitations for each role type. The **Primary Role** determines the scope of access for the group. |
| Sites | Assign site access for the group:<br>• To give the group access to all sites, toggle the setting to **All**.<br>**Note:** When a new group mapping is enabled, **Sites** is set to **All** by default. If you want to isolate the group mapping to specific sites, deactivate Sites All and then select the sites you want associated with that group mapping<br>• To give the group access to specific sites, uncheck **All**from **sites** , select one or more sites from the tree menu, and then select **Save**.<br>**Note:** This feature is only available if the VIQ has created sites. If no sites have been created within the VIQ, the default VIQ site is assigned to the IdP group. |
| • Select 🗑 to delete a group map.<br>• To reorder the group mappings, select ⠿ and drag the row to a new location. Rules are enforced top down. After a user matches a group, the process stops, and all remaining groups within the rule are ignored for that user. | |

3. When there is no available group map, select one of the following options to define ExtremeCloud IQ (New) behavior:
   a. **Deny user login**: Restrict user login access.
   b. **Allow user login and assign a default role and sites**: Assign user roles and site access permissions. See Group Map Settings.
4. Select **Save** to Export SP Metadata on page 696.

Related Links

Add an IdP Profile on page 692

*Export SP Metadata*

After mapping user profile attributes, you must export the SP metadata and import it to the IdP to complete the configuration.

**Important**
This task is part of a larger workflow. Attribute mapping is required before exporting SP metadata. For more information, see Map User Profile Attributes on page 695.

Use this task to export SP metadata for IdPs that support metadata files.

1. Select **Download SP Metadata**.

   This metadata includes:

   - SP Entity ID
   - ASC Binding
   - ASC URL
   - SLO Binding
   - SLO URL
   - SLO Response URL
   - Signing Certificate
2. Select **Done**.

Related Links

Add an IdP Profile on page 692

## Manage IdP Profiles

Use this task to manage Identity Provider (IdP) profiles in ExtremeCloud IQ (New). IdP profiles define the configuration required to integrate an external IdP for user authentication and role assignment.

1. Go to **Administration & Settings** > **Access Management** > **Identity Providers**, and then select **Management**.
2. Locate the IdP profile from the list, select ⋮ from the corresponding row, and then select one of the following actions:

   - To update an IdP profile, select **Edit**. Configure IdP Profile Settings, and then select **Save Changes**.
   - To prevent an existing IdP profile from being used for authentication, select **Disable** . Select **Disable** a second time to confirm.

     **Note**
     Disabling an IdP profile will make it temporarily inactive.

   - To allow an IdP profile to be used for authentication, select **Enable**.
   - To remove an existing IdP profile, select **Delete**. Select Delete a second time to confirm.

     **Note**
     Deleting an IdP profile permanently removes it from the system.

*Manage IdP Profile Settings*

| Field | Description |
|---|---|
| Purpose | Defines the purpose of the IdP within your network. |
| Last Updated | Indicates the last time the IdP profile was updated. |

| Field | Description |
|---|---|
| Configuration Status | The configuration status of the IdP profile. |
| Disable | Select to disable the IdP profile. Select **Disable** a second time to confirm.<br><br>**Note:** Disabling an IdP profile will make it temporarily inactive. |
| Enable | Select to enable the IdP profile. |
| Delete | Select to delete the IdP profile. Select **Delete** a second time to confirm.<br><br>**Note:** Deleting an IdP profile permanently removes it from the system. |

**IdP Profile Information**

| Field | Description |
|---|---|
| Domain | The domain used by the IdP to manage and authenticate user identities. |
| Description | A brief summary of the IdP profile. |

**IdP Connection**

| Field | Description |
|---|---|
| IdP Entity ID | The IdP unique identifier URL. URLs must begin with `https`. |
| SSO Request | Select **SSO Request** to enhance SSO security. By signing the SSO request, you ensure its authenticity and integrity, confirming that it has not been tampered with. |
| SSO Binding | Select **HTTP POST** to send messages within the body of an HTTP POST request.<br>Select **HTTP Redirect** to send encoded messages as query parameters in the URL of an HTTP GET request. Data is visible in the URL and is limited by the maximum URL length supported by browsers and servers. |
| SSO URL | The endpoint where SSO authentication requests are sent. URLs must begin with `https`. |
| SLO Binding | Single Logout (SLO) allows users to sign out from multiple applications or services with a single action.<br>Select **HTTP POST** to send messages within the body of an HTTP POST request.<br>Select **HTTP Redirect** to send encoded messages as query parameters in the URL of an HTTP GET request. |
| SLO URL | The endpoint where logout requests are sent to start the SLO process. This URL ensures that when a user logs out from one service, they are also logged out from all connected services. URLs must begin with `https`. |

| Field | Description |
|---|---|
| SLO Response URL | The endpoint where the Service Provider (SP) sends logout response messages after receiving a logout request from the IdP. This URL is used to confirm the completion of the SLO process. URLs must begin with `https`. |
| Verification Certificates | The digital certificates used to verify the authenticity and integrity of messages exchanged between the IdP and SPs. To view valid certificates, select **Show Certificates**.<br>To update the verification certificates for this IdP profile, select **Manage Certificates**. For more information, see Manage IdP Profile Certificates. |

**Attribute Mapping**

| Field | Description |
|---|---|
| First Name | The URL or endpoint where the IdP provides the user's given name. |
| Last Name | The URL or endpoint where the IdP provides the user's family name or surname. |
| Email | The URL or endpoint where the IdP provides the user's email address. |
| Group | The URL or endpoint where the IdP provides the user's group memberships. |
| Group Mapping | Specifies how group names from the IdP are translated, or mapped, to the corresponding group names in ExtremeCloud IQ (New):<br>• Select **Add a Group Mapping** to add a new group map row.<br>• Select the **IdP Group**, **Primary Role**, **Classic Role**, and **Site(s)** for each group name map. For more information, see Group Map Settings.<br>• Select to delete a group map.<br>• To reorder the group mappings, select and drag the row to a new location. Rules are enforced top down. After a user matches a group, the process stops, and all remaining groups within the rule are ignored for that user.<br>Determine what action ExtremeCloud IQ (New) should take when there is no available group map:<br>• **Deny User Login**: Restrict user login access.<br>• **Allow user login and assign a default user group**: Assign user roles and site access permissions. For more information, see Group Map Settings. |

**Extreme Cloud(SP) Connection**

To obtain SP connection information:

- Select **Download SP Metadata** for IdPs that support Metadata files.
- To manually add SP metadata into the IdP, copy the URL to your clipboard, and then paste it into your IdP. Repeat this process for each URL.

- Select **Download Signing Certificate** to acquire the signing certificate.

*Manage IdP Profile Certificates*

Identity Provider (IdP) profile certificates are essential for securing communication between the IdP and Service Providers (SPs). Properly managing these certificates is key to maintaining the integrity and trustworthiness of your Single Sign-On (SSO) environment.

From the **Certificates** window for an IdP profile, you can:

- View a list of certificates associated with the IdP profile to view details, including certificate provider, days remaining, valid from date, valid to date, and fingerprint.
- Make active certificates inactive.
- Import a new certificate to the IdP profile.

Use this task to ensure your IdP profile certificates are correctly configured and up-to-date.

1. Go to **Administration & Settings** > **Access Management** > **Identity Providers** > **Management**.
2. Locate the IdP profile from the list, select ⋮ from the corresponding row, and then select **Edit**.
3. Expand **IdP Connection**, and then select **Manage Certificates**.
   a. To add a new certificate, select **Import New Certificate**, and then select **Browse Files** to browse to your local folder and select the certificate.
   b. To deactivate a certificate, select ⋮, and then select **Make Inactive**.
   c. To delete a certificate, select ⋮, and then select **Delete**.

   **Note**
   If only one certificate is listed, you cannot delete the last valid certificate.

4. Select **Certificates for** the IdP you selected to return to the **Management** IdP profile list.

## Microsoft Entra ID | Create IdP Application

1. Create a New Enterprise Application in Entra ID:
   a. From the Azure Portal, under **Azure services**, select **Enterprise applications**.
   b. From **Enterprise Applications**, select **New application** > **Create your own application**.

      The **Create your own application** dialog displays.
   c. Provide the application name, select **Integrate any other application you don't find in the gallery (Non-Gallery)**, and then select **Create**.

      The application **Overview** page opens.
2. Assign Users and Groups in Entra ID:

   **Note**
   ExtremeCloud IQ (New) uses group membership information provided by the IdP to assign roles through its RBAC implementation. The IdP must be configured to send group membership claims to ExtremeCloud IQ (New) during authentication.

a. From the application **Overview** page, select **Assign Users and Groups**, and then select **Add user/group**.

   The **Add Assignment** page opens.

b. From the left pane, select the link under **Users and groups**.

   Azure displays the ExtremeCloud IQ (New) required user group.

c. Select the check box for each ExtremeCloud IQ (New) required user group, and then click **Select**.

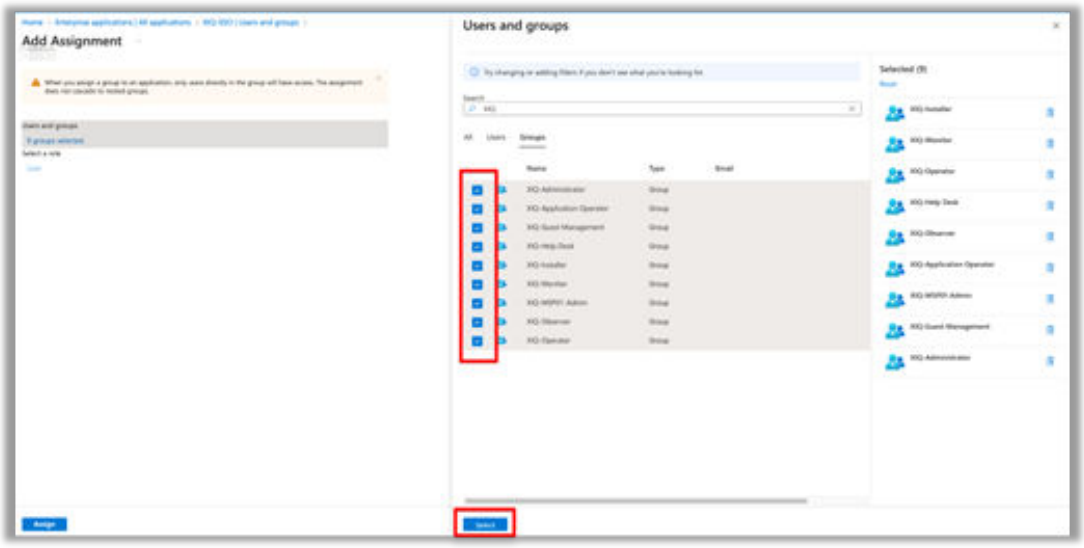



**Figure 111: Azure - Assigning ExtremeCloud IQ (New) User Groups to an Azure User Role**

d. Select **Assign**.

   The selected groups are mapped to the selected role. Azure displays the selected groups on the **Users and Groups** page.

**Note**
Only users assigned to the defined groups have access to the defined roles in ExtremeCloud IQ (New).

3. Select SAML as the Single Sign-On Method in Entra ID:

   a. From the application **Overview** page, navigate to **Manage** > **Single sign-on**, and then select **Get Started**.

   b. Select the **SAML** single sign-on method.

   c. On the **Set Up Single Sign-On with SAML** page, from the **Basic SAML Configuration** section, select **Edit**.

   d. For **Identifier (Entity ID)**, select **Add identifier** and provide a temporary URL.

      For example: `https://temp_ID`

e. For **Reply URL (Assertion Consumer Service URL)**, select **Add reply URL** and add a temporary reply URL.

   For example: `https://temp_reply`

f. Select **Save**.

4. Import Entra ID Metadata to Extreme Platform ONE Networking:

   To see Identity Provider (IdP) profile settings, log in to ExtremeCloud IQ (New) using the Global Data Center (GDC) SSO URL. For example, `https://extremeplatformone.com`.

   **Note**
   Single Sign-on integration can only be configured by ExtremeCloud IQ (New) users with Administrator permissions in their home account (VIQ). External Administrators cannot access the IdP profile configuration page when administering other customer accounts. An External Administrator is an administrative user whose identity and authentication are managed by an external identity provider rather than being created directly in ExtremeCloud IQ (New).

   a. From *ExtremeCloud IQ (New)*, go to **Administration & Settings** > **Access Management** > **Identity Providers** > **Management**.
   b. Select **Add IdP Profile**.
   c. Select the **Microsoft Entra ID** provider, and then select **Next**.
   d. Enter the Fully Qualified **Domain** name of the Azure Tenant and optional **Description**.

      **Note**
      You can only define a single domain name per IdP Profile. If your IdP supports multiple domains, you must create a separate IdP Profile for each domain. For example, user `gradya@testdomain.onmicrosoft.com` cannot log in when the IdP profile specifies `onmicrosoft.com`.

   e. Select **Next**.
   f. Select **Import From URL** to import the data from the App Federation Metadata URL.
   g. From the *Azure Enterprise Application*, scroll down to Section 3: SAML Certificates, and select the **App Federation Metadata Url** copy to clipboard icon.

   h. In *ExtremeCloud IQ (New)*, paste the URL string into the **Enter URL** field, and then select **Import**.

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

   i. Select **Next**.

5. Map Extreme Platform ONE Networking User Profile Attributes to SAML Attributes for Entra ID:

   In *ExtremeCloud IQ (New)*, you must map the appropriate **User Profile Attributes** to the **SAML Attributes** sent from the IdP. For more information, see Map User Profile Attributes on page 695.

Table 247 includes the required strings for integration with Microsoft Entra ID.

**Table 247: ExtremeCloud IQ (New) - Required Strings for Microsoft Entra**

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

6. Map Extreme Platform ONE Networking Group to Roles for Entra ID:

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

   In ExtremeCloud IQ (New), enter the exact **IdP Group** name (case sensitive) from Entra ID (for example, EP1-Operator), and then select the corresponding role. For more information, see Add a Group Mapping.

   **Important**
   For ExtremeCloud IQ (Classic), the Operator, Monitor, Help Desk, Installer, or Observer RBAC roles require the definition of one or more sites to gain visibility over managed devices. In the rule definition for those roles, specify one or more sites in the rules. Failure to do so will lead to the administrator being unable to view any devices after login. Administrator and Guest Management roles do not use sites, and ignores any site definition in the rule.

7. Map Entra ID Security Groups to Extreme Platform ONE Networking Roles:

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

   In the *Microsoft Azure* application, in Section 2: **Attributes & Claims**, select **Edit**.

   a. Perform the following steps to adjust the default claims:

      i. Under **Required claim**, select the **Unique User Identifier (Name ID)** row, change the **Source attribute** field to `user.mail`, and then select **Save**.

      ii. Under **Additional claims**, from the **http://schemas.xmlsoap.org/ws/2005/05/identity/claims/emailaddress** row, select the 3-dot menu, select **Delete**, and then select **OK**.

      iii. Select **Add a group claim**, and then select **Groups assigned to the application**. Under **Source attribute**, select one of the following options, and then select **Save**:

      - If your Entra ID instance is cloud-only, select **Cloud-only group display names**.
      - If your Entra ID instance is hybrid-cloud and on premises, select **sAMAccountName**.

      iv. Under **Additional claims**, select the **http://schemas.xmlsoap.org/ws/2005/05/identity/claims/name** row, change the **Name** field to `email`, and then select **Save**.

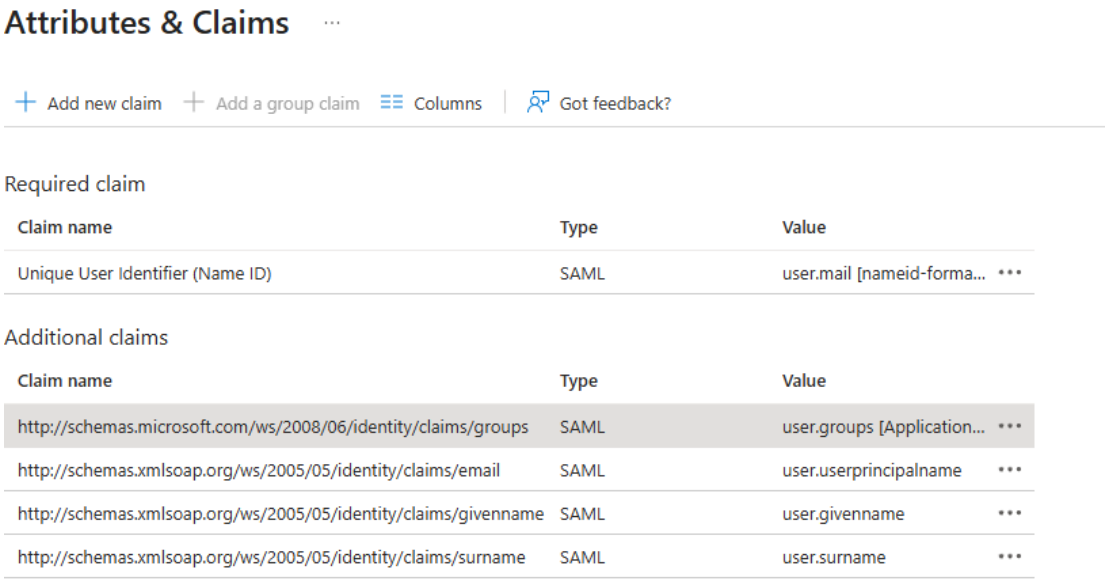



**Figure 112: Attribute & Claims Configuration with Updated Default Claims**

b. Perform the following steps to add a group claim:
   i. Select **Add a group claim**.
   ii. Select **Groups assigned to the application**.
   iii. From the **Source attribute** list, select **Cloud-only group display names**.

8. Export SP Metadata and Import into Entra ID:
   a. After saving the completed **Add IdP Workflow** in *ExtremeCloud IQ (New)*, download the SP metadata. For more information, see Export SP Metadata on page 696.
   b. In the *Microsoft Azure* application, on the **SAML-based Sign-on** page, select **Upload metadata file**, navigate to the saved exported file from ExtremeCloud IQ (New), and then select **Add**.
   c. Confirm that the imported data is correct, and then select **Save**.

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

9. Entra ID Test - IdP Initiated:

   After the integration is complete, test the application.

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

      After a successful login, you are redirected to the ExtremeCloud IQ (New) default view. The ExtremeCloud IQ (New) Audit Logs include the login action.

10. Entra ID Test - SP Initiated:
    a. Browse to the **GDC Login** page `https://extremeplatformone.com`, and then select **Log In with SSO**.

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

The browser is redirected to the Microsoft Login Portal. After a successful sign in, the browser redirects to the ExtremeCloud IQ (New) default view. The ExtremeCloud IQ (New) Audit Logs include the login action.

## Okta | Create IdP Application

1. Navigate to the Okta Admin Portal:
   a. Browse to `https://login.okta.com`, and then log in to your Okta Organization with an account with the necessary Administrator permissions to create user, groups, SAML applications, and Authentication Policies.
   b. From the Okta Dashboard page, select **Admin**.
2. Create a New SAML Application and Define User Group Mappings in Okta:



**Note**
You must create the user groups in the IdP before you can map the user roles in ExtremeCloud IQ (New).

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

3. Assign Users and Groups in Okta:

   **Note**
   ExtremeCloud IQ (New) uses group membership information provided by the IdP to assign roles through its RBAC implementation. The IdP must be configured to send group membership claims to ExtremeCloud IQ (New) during authentication.

   a. Select the **Assignments** tab.
   b. Select **Assign**, and then select **Assign to Groups**.
   c. For each group you want to permit authentication to ExtremeCloud IQ (New) with SSO login, select **Assign** next to the Group Name.

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

   d. Select **Done**.
4. Create New Password Authentication Policy in Okta:

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

   a. From the **Navigation Pane**, go to **Security** > **Authentication Policies**, and then select **Add a policy**.
   b. Enter a **Name**, and then select **Save**.

      You will be directed to the Rules tab of your new Authentication Policy, where we will modify the rules associated with the existing Catch-all Rule policy.
   c. For the **Catch-all Rule**, select **Actions**, and then select **Edit**.
   d. Scroll down to the **Then** section, for **AND User must authenticate with**, select **Password** from the list.
   e. For **Prompt for authentication**, select **Every time user signs in to resource**.
   f. Select **Save**.
   g. Select the **Applications** tab, and then select **Add app**.
   h. Find the SAML Application you created in Step 2, and then select **Add** for the associated row.
   i. Select **Done** to close the app assignment dialog box.
5. Export Metadata for your Okta SAML Application:
   a. From the **Navigation Bar**, go to **Applications** > **Applications**.
   b. Select the SAML Application you created in Step 2, and then select the **Sign On** tab.
   c. In the **Metadata Details** section, you will see the **Metadata URL**. Select **Copy** and retain the URL for use in the next step.

6. Create IdP Profile, Import Metadata, and Edit Settings in Extreme Platform ONE :

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

   a. In ExtremeCloud IQ (New), go to **Administration & Settings** > **Access Management** > **Identity Providers**, and then select **Management**.
   b. Select **+ Add IdP Profile**.
   c. From the **Provider** drop-down list, select **Okta**.
   d. Configure the following **IdP Profile Information**, and then select **Next**:
      - **Domain**: Enter a fully qualified domain name (FQDN) for which you want to provide single-sign on.
      - **Description** (optional): Enter a description of up to 64 characters.

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

   e. Select **Import from URL**.
   f. In the **ISP Metadata URL** field, paste the URL captured in Step 5, and then select **Import**.
      After successful import, metadata from Okta displays.

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

   g. To supply the placeholder values, copy the **SSO URL** and paste the value into the **SLO URL** and **SLO Response URL** fields.

h. From the **Choose Certificates** list, ensure the certificate that was included in the Metadata import is selected, and then select **Continue**.

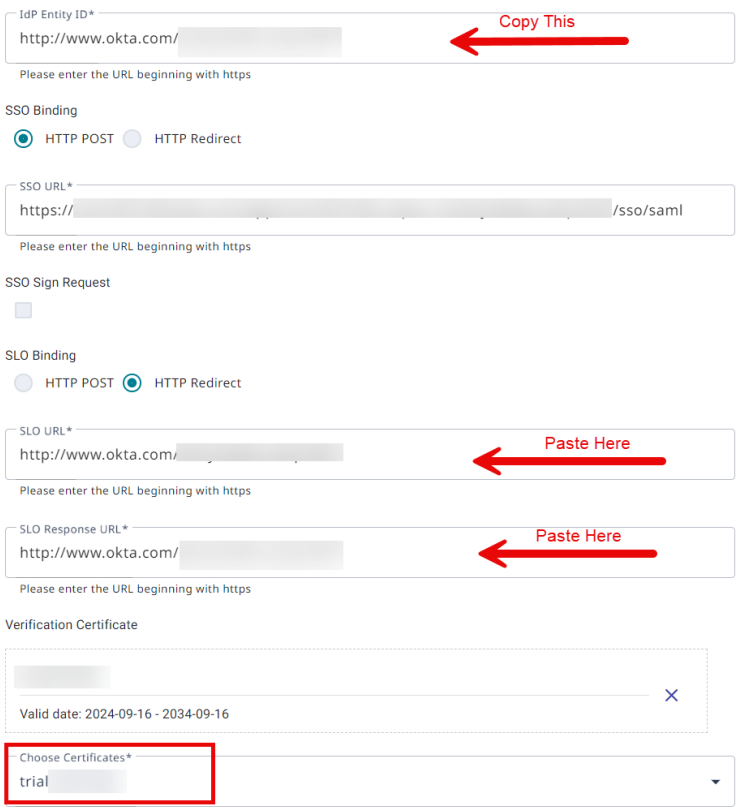



**Figure 113: Extreme Platform ONE – Placeholder Values for Single Logout**

i. On the **Attribute Mapping** page, enter the following values:
   - **First Name**: `user.firstName`
   - **Last Name**: `user.lastName`

j. Select **Add a group name mapping** for each Okta group to map to an ExtremeCloud IQ (New) role.

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

   Add additional mappings as needed.

**Note**
Each of the values for First Name, Last Name, and Group Name are case sensitive. Ensure that the values entered here are an exact match for the information entered in Okta. The list is applied from top to bottom, with the first match taking precedence. If a user belongs to multiple groups listed here, they will be assigned the ExtremeCloud IQ (New) role based on the order that you specify.

l. When there is no available group map, select one of the following options to define ExtremeCloud IQ (New) behavior:

i. **Deny user login**: A user that successfully logs into ExtremeCloud IQ (New) with their Okta credentials, but is not in an Okta group that is mapped to an ExtremeCloud IQ (New) access role, is denied access to the application.

ii. **Allow user login and assign a default role and sites**: A user that successfully logs into ExtremeCloud IQ (New) with their Okta credentials, but is not in an Okta group mapped to an ExtremeCloud IQ (New) access role, is mapped to the role defined here. See Group Map Settings.

m. Select **Save**.

**Important**
The Operator, Monitor, Help Desk, Installer, or Observer access roles require the definition of one or more sites to gain visibility over managed devices.The rule definition for these roles must include at least one site. Without the site definition in these roles, the user is unable to view devices after login. The Administrator and Guest Management access roles do not use sites, and ignores any site definition in the rule.

7. Modify Okta SAML Application Metadata with ExtremeCloud IQ (New) Settings:

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

a. In **Okta**:

i. Browse to your Admin Portal, navigate to **Applications** > **Applications**, and then select your SAML application.

ii. From the **General** tab, scroll down to **SAML Settings**, and then select **Edit**.

iii. Select **Next**, and then select the **Configure SAML** tab.

b. In **Extreme Platform ONE Networking**:

i. From **Administration & Settings** > **Access Management** > **Identity Providers** > **Management**, in the row for your IdP profile completed in Step 6, select , and then select **Edit**.

ii. Navigate to **Extreme Cloud (SP) Connection**, and then select **Download Certificate** to save the file to your computer.

iii. Copy the **SP Entity ID** value from ExtremeCloud IQ (New) and copy it to the **Audience URI (SP Entity ID)** field in Okta.

iv. Copy the **ACS URL** value from ExtremeCloud IQ (New) and copy it to the **Single Sign-On URL** field in Okta.

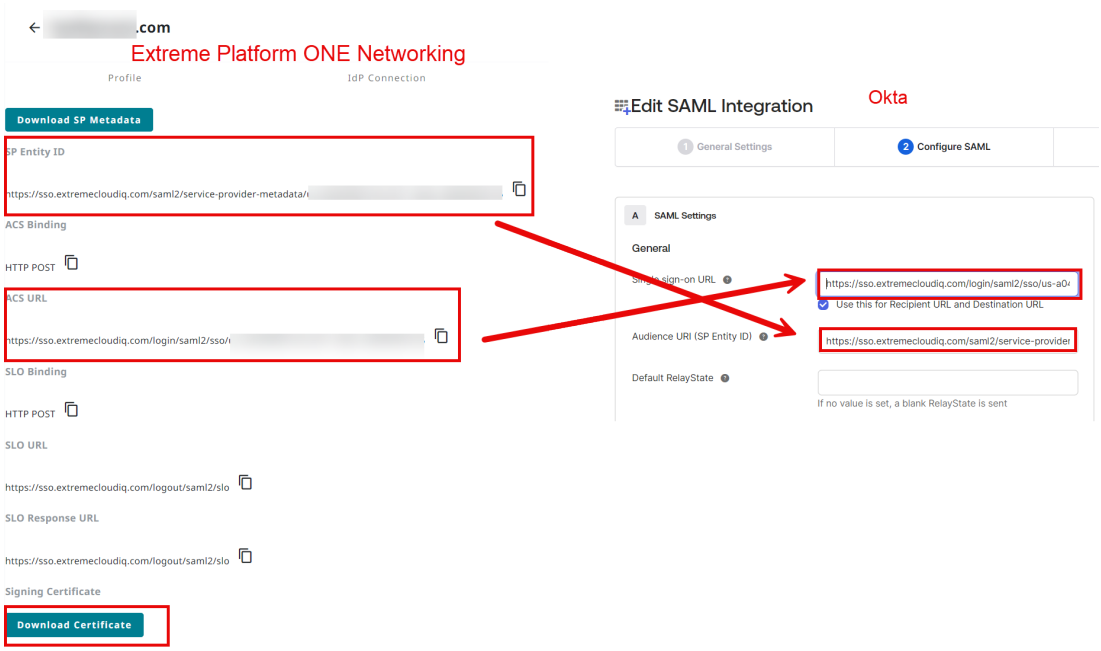



**Figure 114: Okta - Replace Temporary Data for Single Sign-On URL and Audience URI**

c. In **Okta**:

   i. Under **SAML Settings** > **General**, select **Show Advanced Settings**.

   ii. For **Signature Certificate**, select **Browse files**.

   iii. Select **All Files**, navigate to find the certificate file you downloaded in the previous step, select the certificate, and then select **Open** to upload the ExtremeCloud IQ (New) certificate.

   iv. Select **Enable Single Logout**.

   v. Copy the **SLO URL** value from ExtremeCloud IQ (New) and copy it to the **Single Logout URL** field in Okta.

   vi. Copy the **SP Entity ID** value from ExtremeCloud IQ (New) and copy it to the **SP Issuer** field in Okta.

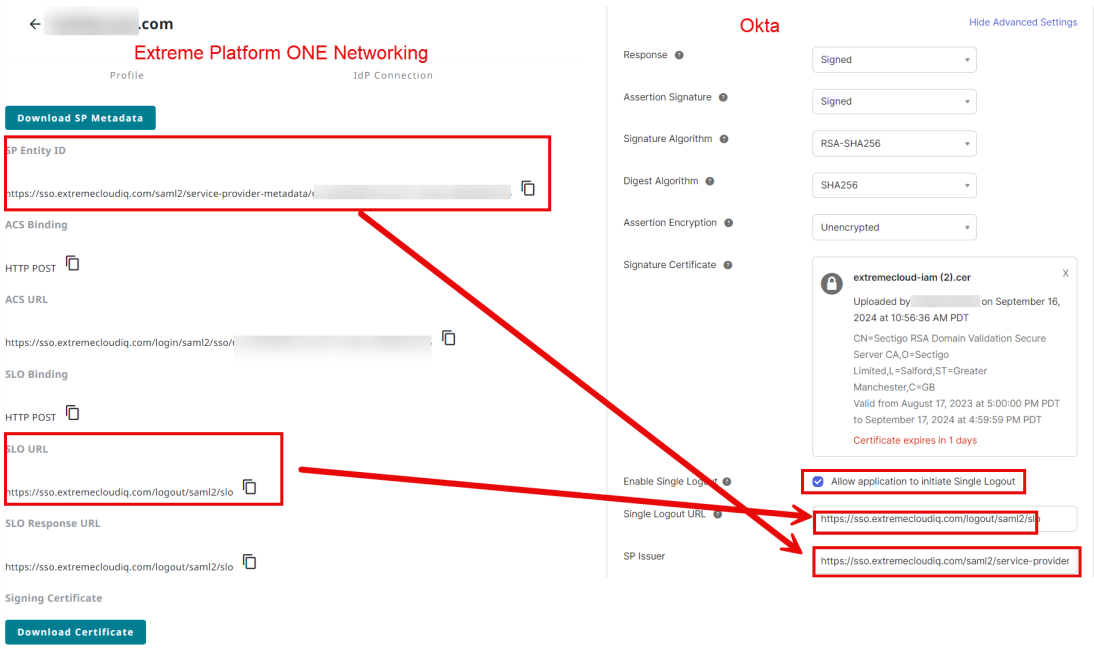



**Figure 115: Okta - Single Logout Setting Definition**

vii. Select **Next**, and then select **Finish**. Click to view your SAML application again.

viii. Select the **Sign On** tab, and in the **SAML 2.0** section, select **More Details**.

ix. Next to the **Single Logout URL** field, select **Copy**.

Use this URL to replace the placeholder text we submitted earlier.

d. In ExtremeCloud IQ (New):

i. Return to the **IdP Connection** section of your IdP profile and paste that value into the **SLO URL** and **SLO Response URL** fields, replacing your placeholder values.

ii. Select **Save Changes**.

The integration is now complete.

8. Okta Test - IdP Initiated:

After the integration is complete, test the application.

a. Log in to your Okta Organization at `https://login.okta.com` with a user account that has been granted access to the SAML application.

b. From the Okta Dashboard page, select your SAML application, and then from the right pane select **Launch App**.

The browser redirects to the Okta Login Portal.

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

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

9. Okta Test - SP Initiated:

a. Browse to the GDC Login page, and then select **SSO**.

`https://extremeplatformone.com`

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

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

# Credential Distribution Groups

You can create credential groups in Extreme Platform ONE Networking to define access to multiple users who share similar access privileges.

## Create a New Credential Distribution Group

Use this task to create a new credential distribution group.

1. Go to **Administration & Settings** > **Access Management** > **Credential Groups**.
2. Select **Create New Group** and configure the settings:

**Table 248: Credential Distribution Group settings**

| Setting | Description |
|---|---|
| Group Name | (Required)<br>Type a name for the group. |
| Admin Account | Required)<br>From the menu, choose **Active Directory User** or **Guest Management Role User**. |
| Member of | For **Active Directory User** only:<br>Type the name of the Active Directory user group for the account. |
| Guest Management User | For **Guest Management Role User** only: the system automatically specifies **Guest Management User**. |
| Add New Member Field (Optional) | If the account is a member of multiple groups, type the name of the first group, select **Add New Member Field**, and type the name of the next group. |
| Enable User Groups | To add existing user groups to this credential distribution group, select **Enable User Groups**. Then choose **Select All**, or select the check boxes for individual user groups. |
| Registration Operation | Select **Email Approval**. |
| Credential Restriction | Select **Restrict The Number of Credentials Per Employee**, and then enter the number of credentials that group members can distribute. |

3. Select **Add**.

# Configure the Idle Session Timeout

Use this task to specify the idle period, after which an inactive session automatically times out, for all user accounts with **Enforce Idle Session Timeout** enabled. See Create a New User on page 580.

**Note**
If a user account has **Enforce Idle Session Timeout** disabled, sessions for that account do not time out. To change this setting, edit the user account.

1. Go to **Administration & Settings** > **Access Management**, and then select the **Access Settings** tab.
2. Select **Timeout Duration**, and select the hour and minutes for duration from the **HH** and **MM** menus, respectively.
3. Select **Save**.

Related Links

Create a New User on page 580
Edit, Disable, or Delete a User Account on page 583

# Administration & Settings | Alert Policies

Global Policy on page 714
Site Policy on page 714

**Note**
The Observer role does not have access to Alert Policies.

## Global Policy

Use the **Global Policy** screen to enable or disable **Alert Rules**, and edit alert rule parameters.

The alert rule categories include **ExtremeCloud IQ**, **Extreme Vendor Specific**, **Extreme Platform ONE Security**, **ExtremeCloud SD-WAN**, and **WIPS**. Select a rule category to see alert rules for that type. Alert rule parameters can be enabled or disabled by selecting the alert rule, then toggle the enable/disable radio button for the event or metric. To edit alert rule parameters, select  for the rule.

**Note**

Alert rules can be filtered. To filter rules, select  then select **Enable** or **Disabled**. Only rules that match the filter setting are displayed.

## Site Policy

### Add a Site Policy

Use this task to add a site policy.

**Note**
The Observer role does not have access to Alert Policies.

1. Go to **Administration & Settings** > **Alert Policies**, and select **Site Policies**.
2. Select **Add Site Policy**.
3. Complete the following:
   - Provide the **Alert Policy Name**.
   - Select **Sites**.
4. Select **Next**.
5. Select an **Alert Rule** and optionally edit, enable, or disable the rule parameters.

6. Select **Apply Rules**.
7. To edit or delete the site policy, from the 3-dot menu, select **Edit** or **Delete**.

# Administration & Settings | External Notifications

Add Email Recipient on page 716
Add Webhook on page 717
Add ServiceNow Account on page 718
Add a Rule for Subscriptions on page 718
Add a Rule for Contracts on page 719

External notifications involve configuring recipients and rules. From the **Recipients** tab, you can perform the following tasks:

- Add Email Recipient on page 716
- Add Webhook on page 717
- Add ServiceNow Account on page 718

From the **Rules** tab, you can perform the following tasks:

- Add a Rule for Subscriptions on page 718
- Add a Rule for Contracts on page 719

To configure external notifications, go to **Administration and Settings** > **External Notifications**, then select either **Recipients** or **Rules**.

## Add Email Recipient

Use this task to add email recipients.

1. Go to **Administration and Settings** > **External Notifications** > **Recipients** select **Email Recipients**.

2. Select **Add Email Recipient** and configure the settings in Table 249.

**Table 249: Email Recipient Configuration Settings**

| Field | Description |
|---|---|
| Business Email | Enter a valid email address. |
| Notification Type and Notification Rule | The following Notification Types and associated rules are available for email recipients:<br>• Alert - Select one or more **Application**, **Severity**, and **Alert Policy** from the drop-down list.<br>**Note:** By default, **Select All** is selected for severity, application, sites and policy drop down values.<br>**Note:**<br>To use global policy to generate an email notification when there is no site-specific policy, select **Global Policy**.<br>If a site-specific policy exists, and you select Global Policy, the system does not send a notification.<br>• Subscription - Select at least one **Subscription** from the drop-down list.<br>• Contract - Select at least one **Contract Rule** from the drop-down list. |
| Enable Notifications | Select the toggle to enable notifications. |

3. Select **Save**.
4. Type in the **Search** field to view specific email recipients.
5. Apply the following filters for email recipients:
   - All
   - Verified
   - Not Verified

## Add Webhook

A Webhook is an automatic, event-driven HTTP request that sends, or pushes, real-time data between applications. You can configure a Webhook to integrate with external systems that benefit from an Extreme Platform ONE Networking alert such as a client lockout alert.

Use this task to add Webhooks.

1. Go to **Administration and Settings** > **External Notifications.** > **Recipients** select **Webhooks**:
2. Type in the **Search** field to view specific Webhook alerts.

3. To add a webhook alert, select **Add Webhook** and configure the settings in Table 250.

**Table 250: Webhook Alerts Configuration Settings**

| Field | Enter |
|---|---|
| POST URL | Enter a valid URL |
| Access Token (optional) | Provide access token details. |
| Sites | Select at least one site or all sites. |
| Applications | Select at least one application or all applications. |
| Severity | Select at least one severity or all severity levels. |
| Alert Policy | Select at least one alert policy or all alert policies. |

   a. Select the **Enable Notifications** toggle.
   b. Select **Save**.

## Add ServiceNow Account

Use this task to add a ServiceNow account.

1. Go to **Administration and Settings** > **External Notifications.** > **Recipients** select **ServiceNow**:
2. Type in the **Search** field to view specific ServiceNow alerts.
3. To add a ServiceNow alert, select **Add Account** and configure the settings in Table 251.

**Table 251: Add ServiceNow Alerts Configuration Settings**

| Field | Description |
|---|---|
| ServiceNow Email | Enter a valid email address |
| Sites | Select at least one site or all sites. |
| Applications | Select at least one application or all applications. |
| Severity | Select at least one severity or all severity levels. |
| Alert Policy | Select at least one alert policy or all alert policies. |

   a. Select the **Enable Notifications** toggle.
   b. Select **Save**.

## Add a Rule for Subscriptions

Use this task to add a rule for subscriptions.

1. Go to **Administration and Settings** > **External Notifications** > **Rules** select **Subscriptions**:

2. Select **Add Rule** and configure the settings in Table 252.

**Table 252: Subscription Rule Configuration Settings**

| Field | Enter |
|---|---|
| Rule Name | Enter a rule name. |
| Applications | Select the check boxes for the applications that apply from the drop-down menu. |
| Timeline Rules | Select the check boxes for the timeline rules that apply from the drop-down menu. |
| Event Rules | Select the check boxes for the event rules that apply from the drop-down menu. |

3. Select **Save**.
4. Type in the **Search** field to view specific rules.

## Add a Rule for Contracts

Use this task to add a rule for contracts.

1. Go to **Administration and Settings** > **External Notifications** > **Rules** select **Contracts**:
2. Type in the **Search** field to view specific rules.
3. Select **Add Rule** and configure the settings in Table 253.

**Table 253: Contracts Rule Configuration Settings**

| Field | Enter |
|---|---|
| Rule Name | Enter a rule name. |
| Timeline Rules | Select the check boxes for the timeline rules that apply. |

4. Select **Save**.

# Administration & Settings | Global Settings

Service Management on page 720
Backup & Restore on page 721
Integrations on page 723

Global settings apply across the ExtremeCloud IQ (New) instance.

## Service Management

On the **Service Management** tab, you can enable and manage the following optional wireless services for your network:

- Enable Wireless Client Tracking on page 720
- Enable WIPS (Wireless Intrusion Prevention System)
- Enable Guest Services

Go to **Administration & Settings** > **Global Settings** > **Service Management**.

### Enable Wireless Client Tracking

Before enabling Wireless Client Tracking, ensure the following conditions are met:

- **Presence Analytics** must be enabled on the Network Policy associated with the APs that will participate in client tracking. For more information, see Configure Presence Analytics on page 445.
- The Network Policy must include supported APs. For more information, see Wireless Client Tracking | Supported Devices on page 721.
- The required configuration must be pushed to the participating devices. ExtremeCloud IQ (New) will prompt you to navigate to **Monitoring** > **Network Devices** > **Wireless** to select the devices and push the required configuration when you enable the service.

Wireless Client Tracking is a location-based service that enables ExtremeCloud IQ (New) to determine and display the physical location of wireless clients on floor plan maps. When enabled, this service activates the following capabilities:

- Client Location — Displays the real-time and last known location of wireless clients on floor plan maps.
- Client Path — Shows the historical path a client has taken across a floor, available from the Clients inventory panel in Maps.

- Client Density Map — A new map type that displays a heatmap-style grid showing areas of high and low client density on a floor. This map type is only available when Wireless Client Tracking is enabled.

For more information on maps, see Heat Map View on page 46.

Use this task to enable wireless client tracking.

1. Go to **Administration & Settings** > **Global Settings** > **Service Management**.
2. Toggle **Wireless Client Tracking** to **ON**.

**Note**
Wireless client tracking requires Network Policy settings. To configure device network policies, select **Configure**. From the **3-dot Menu** (⋮) at the end of a row for each device that requires Network Policy configuration, select **Configure** > **Device**.

3. To disable wireless client tracking, toggle **Wireless Client Tracking** to **OFF**, and then select **Disable**.

**Note**
This will stop tracking client location and movement on the floor plan.

*Wireless Client Tracking | Supported Devices*

Wireless Client Tracking is supported on the following ExtremeCloud IQ (New) APs:

- AP302W
- AP305C/305CX
- AP310C
- AP310CX
- AP410C
- AP460C
- AP460S
- AP510C
- AP510CX
- AP4000
- AP4000U
- AP4020/4020X/4020FX
- AP4060/4060X
- AP650
- AP650X
- AP3000
- AP3000X
- AP5010
- AP5010U
- AP5020
- AP5022
- AP5050U/D
- AP5060U/D

# Backup & Restore

On the **Backup & Restore** tab, you can manage Virtual IQ (VIQ) account data and configuration, and set the default device password.

## VIQ Management

The **VIQ Management** screen supports the following functions:

- Manually back up and restore Virtual IQ account data.
- Delete data to reset the Virtual IQ database.
- SSH Availability.
- Supplemental CLI.

- AP Out-of-the-box Wireless Onboarding.
- Import and Export VIQ data.

Use this task to manage the Virtual IQ.

1. Go to **Administration & Settings** > **Global Settings** > **Backup & Restore** > **VIQ Management**.
2. To perform a manual backup, select , and then select **Backup VIQ**.

   To ensure data integrity, activities are suspended in the VIQ during both the backup and the restore process. When a backup is complete, the backup event is added to the Backup History table at the bottom of the page.
3. To restore a backup, choose a backup file from the **Backup History** table, and then select **Restore**.
4. To delete the VIQ database, select , and then select **Reset VIQ**.

   This step resets the VIQ to its initial state before configuration and the addition of inventory.
5. Toggle **SSH Availability** to **ON**.

   Enabling SSH availability potentially gives others direct access to your devices while SSH access is available. While active, SSH Availability exposes your device to the public Internet through an SSH proxy, protected only by the device administrator credentials, as SSH FTP assumes that it is run over a secure channel.
6. Toggle **Supplemental CLI** to **ON**.

   Use the Supplemental CLI tool to append CLI commands to a network policy when you upload the configuration to managed devices.
7. To enable the VIQ to permit APs to respond to mesh-join requests, slide the **AP Out-of-the-box Wireless Onboarding** toggle to **ON**.

   This setting permits or prohibits AP responses to mesh-join requests. When this setting is off, the Virtual IQ prohibits managed APs from responding even if the serial number of the requesting AP is listed in the Virtual IQ.
8. To export VIQ data:
   a. Select **Export VIQ**.
   b. (Optional) Provide **Export Timeout (in minutes)**.
   c. Select **Export**.
9. To import VIQ data:
   a. Select **Import VIQ**.
   b. Select **Import VIQ from ExtremeCloud IQ**.
   c. Either drag the .tar.gz file or select **Browse Files** to navigate to the location of the file and select it.
   d. Complete the following Optional Settings:

   - Enable or disable **Resend Cloud PPSK/RADIUS password via Email/SMS**
   - Provide **Import Timeout** (in minutes)
   - Instructions on handling errors during VIQ import: **Abort the import operation** or **Continue the import Operation**.
   - Select **Import**.

### Set Default Device Password

The device default password is applied to devices when their network policies are uploaded. Use this task to set the default device password.

1. Go to **Administration & Settings** > **Global Settings** > **Backup & Restore** > **Default Device Password**.
2. For **Default Password**, enter the password the administrator uses to log in to a new device.

   The password must be an alphanumeric string containing at least one number and one uppercase character, and cannot be the same as the user name or a previously used password.
3. For EXOS and VOSS switches, select **Enable device management settings for Switch Engine (EXOS)/Fabric Engine (VOSS) switches**.

   Enable this setting to set device credentials at the device level for these switch series.
4. (Optional) Select **Change Password**.

## Integrations

**Administration & Settings** > **Global Settings** > **Integrations** provides administrators with tools to create and manage API keys. An API key is a unique alphanumeric code used to identify and authenticate when communicating with the API. The **Integrations** table displays the following information for the API keys that have been added to ExtremeCloud IQ (New):

- **Name**: The name of the API key.
- **Expire At**: The expiration date of the API key.
- **Key Hash**: A partial representation of the API key used for reference without exposing the full key.
- **Description**: A short description of the API key.

To create a new API key, select **Create New API Key**. To edit an existing API key, select ⋮ at the end of the corresponding row, and then select **Edit Key**. To delete an API key, select **Delete Key**.



**Note**

- After generating a key, it cannot be modified.
- External administrators are not permitted to create API keys.

### Create a New API Key

Use this task to create a new API key.

1. Go to **Administration & Settings** > **Integrations** > **Create New API Key**.

2. Configure the settings in Table 254.

**Table 254: API Key Settings**

| Field | Description |
|---|---|
| Name | A descriptive label to identify the API key. |
| Description | A short description of the API key. |
| Expiration Date | The date the API key automatically becomes inactive. |

3. Select **Generate Key**.
4. Select **Copy API Key**, and then select **Close**.



**Important**
Make sure to copy your API key now. For security reasons, you won't be able to see it again once you close the window.

Related Links

Integrations on page 723

# Administration & Settings | Logs

Delete KDDR (Kernel Diagnostic Data Recorder) Logs on page 726

Use logs to detect anomalies in the system and track past activity. To access Extreme Platform ONE Networking logs, go to **Administration and Settings** > **Logs**.

Logs capture the following activities:

- **Accounting Logs**

  The Accounting Logs table displays information about cloud-based PPSK and RADIUS user sessions on your network. The table includes authentication events for the time range that you define using the Start, End, and Time controls at the top of the page. Use the Search field above the table to search for a specific client or user name.
- **Audit Logs**
  - Administrative activity: For example, creating or deleting a user account or changing, suspending, or deleting role-based user access.
  - Data access and modification: When a user views, creates, or modifies data
  - User denials or login failures: Captures when a user is unable to login to a system due to invalid credentials or is denied access to resources such as a specific URL
  - Configuration changes: Captures when a configuration change is made to a device.
  - Access requests: When a user requests access to resources.
  - System changes: Captures system activity. Audit logs must be compliant with all Extreme Network standards, for example, HIPPA, PCI, NIST.
- **Authentication Logs**

  The Authentication Logs table displays information about successful authentication attempts involving cloud-based PPSK and RADIUS users, and users authenticating through a cloud-hosted captive web portal using either social log in credentials or a PIN. The table includes authentication events for the time range that you define using the Start, End, and Time controls at the top of the page. Search for a specific client or user name in the Search field above the table.
- **Credential Logs**

  The Credential Logs table displays information about cloud-based RADIUS user credentials that have expired. To set a time range to view expired user credentials, use the Start, End, and Time controls at the top of the page. Use the Search field above the table to search for a specific client or user name.
- **Email Logs**

The Email Logs table displays information about email notifications to users who requested network access.

- **Event Logs**

  The Event Logs table displays information about events on devices on the network.

- **GDPR Logs**

  The General Data Protection Regulation (GDPR) audit log displays information about download tasks performed on client data, and deletion tasks performed on user, client, and admin data to support compliance with GDPR requirements for EU citizens. Use this log to track actions that are currently being processed, that are complete, or that have failed.

- **Security Logs**

  The Security Logs table displays detailed information about security-related events within the network.

Use this task to work with logs.

1. Go to **Administration and Settings** > **Logs.**
2. Select the **Log** and **Date** and **Time** pickers to do the following:
   - View logs for up to 13 months (390 days).
   - View logs for last week, last month or last quarter.
   - Select an end time.
   - Reset to default.
   - Use arrows to select a specific month.
   - To view a logs for a specific date, select the date directly from the calendar.
3. You can also search and filter by column heading.
4. Select the **Date/Time** column to sort in ascending or descending order.
5. Select **Column** to add, hide, and reposition columns on the screen.
6. To refresh the screen and get the latest audit logs, select .

## Delete KDDR (Kernel Diagnostic Data Recorder) Logs

Use this task to delete KDDR logs.

1. Go to **Administration and Settings** > **Logs**.
2. Select **KDDR Logs** from the **Logs** drop down list.
3. Select the KDDR logs you want to delete using one of these methods:
   - **Select individual logs:** Select the check box next to each KDDR log row you want to delete.
   - **Select all logs on the current page:** Select the check box in the column header. All visible logs on the current page are automatically selected.
   - **Select all logs across all pages:** Select () next to the header check box to open the selection drop down list. Select **All** to select all KDDR logs in the table, including logs on other pages.
4. Select **Delete** and select **Delete** again to confirm the deletion of the KDDR logs.