



ExtremeCloud IQ (Classic) v25.8.0 User Guide

System Configuration and Management

9041054-00 Rev AA
March 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/>

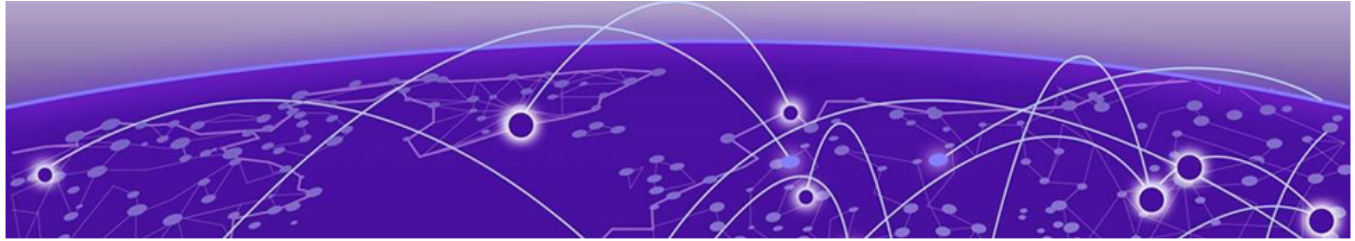


Table of Contents

Abstract.....	xi
Preface.....	12
Text Conventions.....	12
Documentation and Training.....	13
Open Source Declarations.....	14
Training.....	14
Help and Support.....	14
Subscribe to Product Announcements.....	15
Send Feedback.....	15
Release Notes.....	16
Welcome to ExtremeCloud IQ.....	17
Register for an ExtremeCloud IQ Account.....	17
Unified Login Page.....	18
Extreme Applications and the 9-dot Menu.....	19
Log in to ExtremeCloud IQ.....	20
Navigate ExtremeCloud IQ.....	20
Unified Logout.....	21
Onboarding.....	22
Add Devices Overview.....	22
Universal AP Boot and Onboarding Process.....	23
Quick Add Devices.....	28
Quick Add Tunnel Concentrators.....	31
Add Locally Managed Devices.....	32
Add Devices with Advanced Onboarding.....	34
About Digital Twin.....	36
Wireless AP Overview.....	36
AP3000 Series Radios and 6 GHz Support.....	37
AP4000/AP4000-1 Radios and 6 GHz Support.....	39
AP5000 Series Radios and 6 GHz Support.....	41
AFC Overview.....	43
Indoor/Outdoor AFC Support.....	44
Anchor and Non-Anchor APs.....	46
6 GHz Radio Power AFC.....	47
6 GHz Radio — Standard Power Operation without AFC Approval.....	48
GeoLocation Agent.....	49
GeoLocation Coordinates.....	50
AP Placement for AFC.....	52
Administration.....	54
About Global Settings.....	55

Manage Account Details.....	55
Enable ExtremeCloud IQ Classic.....	56
Account Management.....	57
Add or Edit an Administrator Account.....	58
Account Management Settings.....	58
Delete an Administrator Account.....	60
Add a Credential Distribution Group.....	61
Enable Two-Factor Authentication.....	62
Manage Licenses and Subscriptions.....	63
Entitlements.....	63
NAC Entitlements.....	64
Legacy Entitlements.....	65
Link Your Extreme Networks Portal Account.....	65
Manage Licenses.....	66
Set a Device Default Password.....	67
Manage the Virtual IQ.....	68
Enable Single Sign On (SSO).....	70
Add an IdP Profile.....	70
Manage IdP Profile Certificates.....	74
Manage IdP Profiles.....	74
Set Email Notifications.....	77
Manage API Access Tokens.....	78
Generate API Access Tokens.....	79
Add an API Presence and Data Location Feed.....	80
Add a Third-Party API Token.....	81
Download Logs.....	81
Audit Logs.....	81
GDPR Audit Log.....	83
KDDR Logs.....	83
Authentication Logs.....	84
Accounting Logs.....	85
Credential Logs.....	86
Email Logs.....	86
SMS Logs.....	87
Enable SSH Availability.....	88
Enable Supplemental CLI.....	88
Configure Users.....	89
Add a User.....	90
User Settings.....	90
Bulk Create Users.....	92
Bulk Create Settings.....	92
Add a User Group.....	93
Cloud User Group Settings.....	93
Local User Group Settings.....	95
Add a User to a User Group.....	98
Bulk Add Users to a User Group.....	98
Configure a Private Client Group.....	98
Unlock Users.....	99
Perform a RADIUS Test.....	99

Unbind a Device.....	100
Configuration—Network Policies.....	101
Add a Network Policy.....	102
Configure Policy Settings.....	103
Configure DNS Server Policy Settings.....	104
Configure NTP Server Policy Settings.....	105
Configure SNMP Server Policy Settings.....	106
Configure Syslog Server Policy Settings.....	107
Configure Device Credentials Policy Settings.....	108
Configure the Device Time Zone.....	109
Configure HIVE Policy Settings.....	109
Configure Management and Native VLAN Policy Settings.....	109
Configure IP Tracking Policy Settings.....	110
Configure LLDP/CDP Policy Settings.....	111
Configure Management Options.....	111
Configure Traffic Filters Policy Settings.....	112
Configure MGT IP Filter Policy Settings.....	112
Deploy a Network Policy.....	113
Configure the SSID for a Standard Wireless Network.....	113
SSIDs.....	117
SSID Usage in Standard Wireless Networks.....	118
Configure a Client Mode AP Profile using a Wired Connection and a Device Template.....	126
Captive Web Portals.....	127
Hotspot.....	137
RADIUS Authentication.....	144
Configure VLAN Settings.....	156
Apply Different User Profiles to Clients and User Groups.....	158
Customize Advanced Access Security Controls.....	159
Customize Wireless Network Optional Settings.....	162
Settings for Multi-Link Operation.....	170
Configure Device Templates.....	171
Configure Classification Rules for a Device Template.....	171
Fabric Attach.....	174
Configure Fabric Attach.....	174
Configure Device Data Collection and Monitoring Options.....	175
Configure the BLE Service.....	177
Configure Presence Analytics.....	180
Configure WIPS.....	180
Configure a Location Server.....	181
Install CA Certificates.....	181
Configure a Layer 2 IPsec VPN Service.....	182
Router Settings.....	182
Configure Network and IP Address Allocation.....	183
Configure a Router Template.....	184
VPN Services.....	188
Configure an SD-WAN Route Group.....	194
Configure a Routing Policy.....	195
Configure Dynamic DNS.....	197

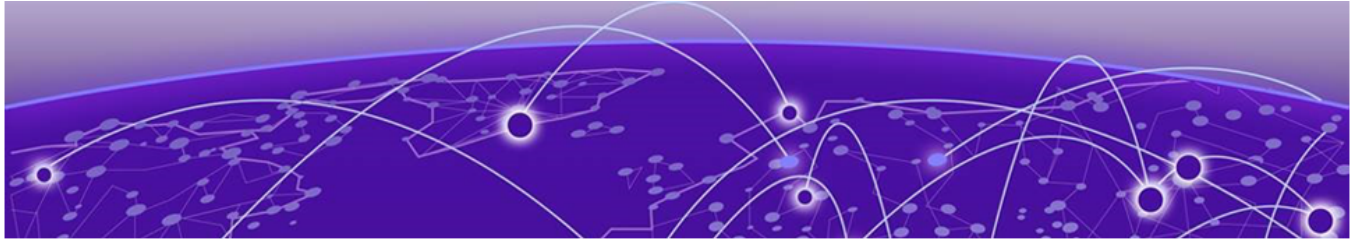
Configure WAN Tracking.....	198
Configuration—Common Objects.....	199
Policy Configuration.....	199
Configure AP Templates.....	200
Configure Auto-Provisioning.....	209
Configure a Bonjour Gateway.....	211
Configure Classification Rules.....	214
Configure Client Monitor Profile Policies.....	216
Add a Cloud Config Group.....	217
Configure a Fabric Attach Profile.....	217
Configure a HIVE Profile.....	218
Configure a Hotspot Profile.....	221
Configure a Hotspot Service Provider Profile.....	221
IoT Profiles.....	221
Manage Port Types.....	228
Instant Port Profiles List.....	228
About Radio Profiles.....	229
Configure an SDR Profile.....	242
Configure a Schedule.....	243
Configure an SSID.....	244
Configure Switch Templates.....	244
Configure URL Filtering Rules.....	280
Add a User Profile.....	281
Basic Configuration.....	287
Add Application Sets.....	288
Client Mode Profiles.....	288
Configure DHCP Servers and DHCP Relay Agents.....	291
Configure a DNS Service.....	293
Configure IP Objects and Host Names.....	294
Configure a MAC Object and MAC OUI.....	298
Configure a Notification Template.....	299
Configure OS Objects.....	300
Configure a VLAN Object.....	300
Configure a VLAN Group Object.....	301
Configure Supplemental CLI.....	302
Security Configuration.....	303
Add AirDefense Policies.....	303
Add IP Firewall Policies.....	303
Add MAC Firewall Policies.....	304
Configure MGT IP Filters.....	305
Configure Traffic Filters.....	307
Add a WIPS Policy.....	309
QoS Configuration.....	313
Quality of Service.....	313
Classifier Maps.....	315
Configure Marker Maps.....	318
Configure Rate Limiting and Queuing.....	319
Management Configuration.....	320
Configure a DNS Server.....	320

Configure an NTP Server.....	321
Configure an SNMP Server.....	322
Configure a Syslog Server.....	325
Network Configuration.....	327
Configure an Access Console.....	328
Configure ALG Services.....	329
Configure LLDP and CDP.....	329
Configure an IP Tracking Group.....	331
Configure Layer 2 IPsec VPN Services.....	332
Configure Location Servers.....	338
Configure Management Options.....	341
Configure Tunnel Concentrator Services.....	352
Configure Tunnel Policies.....	356
Configure an sFlow Receiver.....	358
Configure Network Services.....	359
Add a Subnetwork Space.....	360
Configure a Firewall Policy.....	364
Configure VPN Services.....	365
Authentication Configuration.....	366
Clone an AAA Server Profile.....	366
Clone an Active Directory Server.....	367
Clone or Edit a Captive Web Portal.....	367
Clone or Edit an External RADIUS Server.....	367
Clone or Edit an Extreme Networks A3 RADIUS Server.....	368
Clone an LDAP Server.....	368
Certificate Configuration.....	370
Create a Certificate and Key.....	370
Create an ExtremeCloud IQ Certificate of Authority.....	371
Create a CSR for a Server.....	372
Concatenate an Existing Certificate and Private Key.....	374
Create a Self-Signed Certificate.....	374
Import a Certificate or Key.....	375
Create a Certificate Bundle.....	376
Manage.....	377
Summary.....	378
Use the Filter Sidebar.....	379
Real Time Maps.....	381
Device Summary and Actions Menu.....	385
View Client Roaming Trail.....	393
Add a Floor Plan.....	394
View Device Inventory.....	396
Import a Third-Party RF Heatmap.....	397
View Antenna Patterns.....	397
Edit a Real Time Floor Map.....	398
Planning.....	401
Location Tree Changes.....	403
Add a Site Group.....	404
Add a Site.....	404
Import a Map.....	405

Add a Building.....	405
Move a Building.....	406
Draw a Building Perimeter.....	406
Add Interior Walls and Obstructions.....	407
Add a Floor.....	407
Plan Devices.....	409
View Heat Maps.....	411
Devices.....	412
Manage Devices.....	412
Filter the Device List.....	416
Device List Views.....	416
Device Status Icons.....	435
Utilities.....	440
Actions Menu Overview.....	449
Device Details Panel.....	454
Clients.....	496
Clients Health.....	496
Client Connection Details Panel.....	497
Client Tools (Wireless).....	502
Real-Time Troubleshooting.....	505
Users.....	506
View Connected Users.....	507
Connected Users List.....	507
User Details.....	508
Events.....	508
Alerts.....	509
Manage Alerts.....	509
View Legacy Alarms.....	514
Alert Policy.....	515
Manage Notifications.....	523
Reports.....	526
Create a Network Summary Report.....	527
Generate a PCI DSS 3.2 Report.....	528
Generate a WIPS History Report.....	528
Generate a Wi-Fi Statistics Summary.....	529
Generate a Client Tracking Report.....	529
Generate a Switch Summary Report.....	530
Time Range for Reports.....	530
Applications.....	531
Applications List.....	532
Add a Custom Application.....	533
Application Detection Rules Settings.....	533
Rogue APs.....	534
Classify Rogue APs.....	536
Mitigate Rogue APs.....	536
Rogue Clients.....	536
Classify Rogue Clients.....	537
About Client Monitor.....	537
Search for Clients.....	538

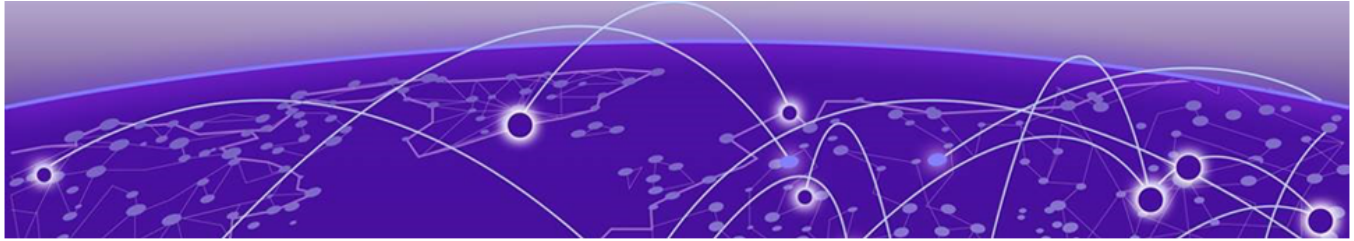
About the Issue List Table.....	538
About Diagnosis.....	540
Timeline.....	540
Card.....	540
Events Associated with an Issue.....	541
Email Notification on Change of Status.....	541
Perform a Change Status Email Notification.....	542
Packet Capture.....	542
Manage Packet Capture Sessions.....	543
Add and Start a Packet Capture Session.....	546
VPN Management.....	551
Set the Time Frame for Captured Data Displays and Reports.....	551
ML Insights.....	553
Network 360 Monitor Overview.....	553
Status Cards.....	554
Device View.....	555
Zone View.....	556
Topology Tab.....	556
Map Tab.....	557
Network Scorecard.....	558
Device Health Scoring.....	558
Client Health Scoring.....	560
WiFi Health Scoring.....	561
Network Health Scoring.....	563
Services Health Scoring.....	564
About Client 360.....	564
Connection Details Panel (Wireless).....	565
Session Details (Wireless).....	570
Device Details Panel (Wireless).....	573
Client Alias.....	573
Thread Monitoring.....	574
Thread Network Details.....	575
Topology View.....	575
Inventory.....	576
Node Details.....	578
Essentials.....	579
ExtremIoT Essentials in ExtremeCloud IQ.....	579
Extreme AirDefense Essentials in ExtremeCloud IQ	580
ExtremeGuest Essentials in ExtremeCloud IQ.....	582
ExtremeLocation Essentials in ExtremeCloud IQ.....	583
CoPilot Dashboard.....	584
Connectivity Experiences.....	585
Quality Index for Wireless Devices Widget.....	586
Quality Index for Wired Devices Widget.....	586
Connectivity Experiences Table.....	587
Connectivity Experiences Panel (Wireless).....	588
Client Association (Wireless).....	589
Client Authentication (Wireless).....	591

Time to Obtain IP Address (Wireless).....	593
Connectivity Experiences Panel (Wired).....	594
Port Errors.....	595
Anomalies.....	596
Instant Anomaly Detection.....	597
Top Anomalies by Site Widget.....	598
Anomalies by Severity Widget.....	598
Top Anomalies by Type Widget.....	599
Anomalies Table.....	608
Anomaly Trends.....	611



Abstract

This user guide for ExtremeCloud IQ (Classic) version 25.8.0 provides comprehensive technical instructions for onboarding, configuring, securing, and managing Extreme Networks access points, switches, and SD-WAN devices in cloud-driven and hybrid deployments. It details device registration, DHCP-based discovery, CAPWAP connectivity, region and country fingerprinting, firmware orchestration, persona conversion for Universal APs, and enhanced onboarding workflows including Digital Twin simulation. The guide explains unified network policy configuration for wireless, switching, and routing, covering SSID authentication (WPA3, PPSK, MAC auth), VLAN assignment, RADIUS integration, protected management frames, captive portal options, and advanced services such as NTP/DNS/Syslog, IP tracking, LLDP/CDP, traffic filters, and Fabric Attach. Deployment scenarios include 6 GHz Wi-Fi 6E/7 operation, AFC-controlled spectrum, geolocation services, and indoor/outdoor placement guidelines. Additional sections describe administrative controls, licensing, SSO, API integration, diagnostics, ML-driven insights, CoPilot anomaly detection, and reporting capabilities for enterprise-scale operations.



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

Table 3: Command syntax

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

Documentation and Training

Find Extreme Networks product information at the following locations:

[Current Product Documentation](#)

[Release Notes](#)

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

[Extreme Optics Compatibility](#)

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

Open Source Declarations

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

Training

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

Help and Support

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

[Extreme Portal](#)

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

[The Hub](#)

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

[Call GTAC](#)

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

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

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

Subscribe to Product Announcements

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

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

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

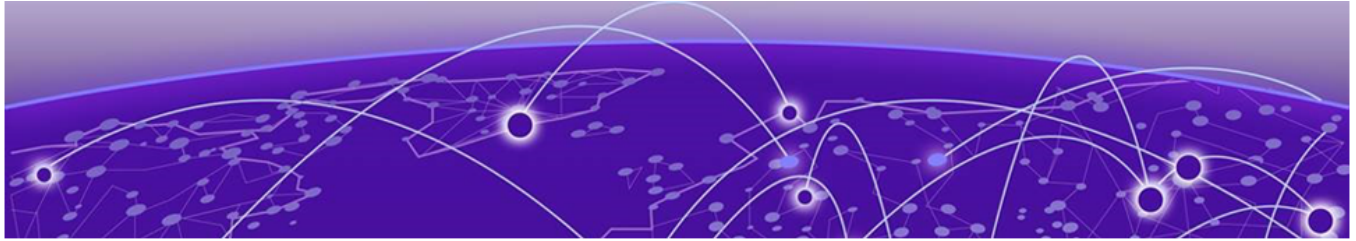
Send Feedback

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

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

To send feedback, email us at Product-Documentation@extremenetworks.com.

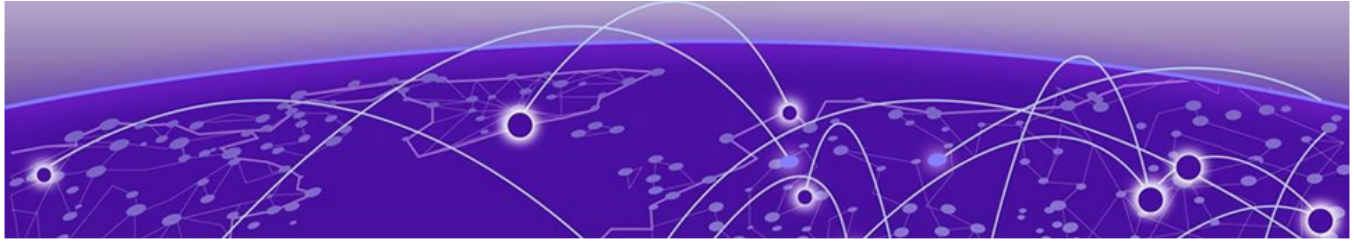
Provide as much detail as possible including the publication title, topic heading, and page number (if applicable), along with your comments and suggestions for improvement.



Release Notes

Consult the [Release Notes](#) for details about changes in the current release of ExtremeCloud IQ.

For release notes information about device firmware and other related products, see the Extreme Networks [Product Documentation](#) website.



Welcome to ExtremeCloud IQ

[Register for an ExtremeCloud IQ Account](#) on page 17

[Unified Login Page](#) on page 18

[Log in to ExtremeCloud IQ](#) on page 20

[Navigate ExtremeCloud IQ](#) on page 20

[Unified Logout](#) on page 21

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

ExtremeCloud IQ (Classic) 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.

For more information, consult the [ExtremeCloud IQ \(Classic\) documentation](#).



Note

All instances of ExtremeCloud IQ in this document refer to ExtremeCloud IQ (Classic).

Related Links

[Onboarding](#) on page 22

Register for an ExtremeCloud IQ Account

Registration requires a valid email address, to which you have access. ExtremeCloud IQ restricts registrations from generic email and business addresses. For more information, see [Article Number: 000118501](#).

Use this task to register for an ExtremeCloud IQ account.

1. Using your web browser, go to <https://www.extremenetworks.com/solutions/cloud-management/extremecloud-iq-registration>.

2. Complete the registration form as follows:

Table 4: ExtremeCloud IQ Registration Form

Field	Description
FIRST NAME	(Required) Type the first name of the new account holder. Only letters Aa–Zz are accepted.
LAST NAME	(Required) Type the last name of the new account holder. Only letters Aa–Zz are accepted.
EMAIL ADDRESS	(Required) Type the email address of the new account holder.
COMPANY	(Required) Type the company name.
JOB TITLE	(Required) Type the job title of the new account holder.
PHONE	(Required) Type the phone number of the new account holder.
COUNTRY	(Required) Select the country from the list.
PARTNER OR EXTREME NETWORKS REPRESENTATIVE EMAIL	To send a copy of the registration to your Extreme Networks partner or representative, type their email address.
I UNDERSTAND THAT FAILURE TO PROVIDE COMPLETE AND/OR ACCURATE INFORMATION MAY RESULT IN MY ACCOUNT BEING SUSPENDED AND/OR TERMINATED (Required) Select the check box.	

3. Select **Register**.

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.

For more information about other applications and the 9-dot menu, see [Extreme Applications and the 9-dot Menu](#) on page 19.

Related Links

[Extreme Applications and the 9-dot Menu](#) on page 19

Extreme Applications and the 9-dot Menu

The following table lists the applications available on the 9-dot menu, according to subscription type, including applications available for trial.



Note

Connect VIQs are not linked to an Extreme Portal Account. Therefore, Connect accounts do not have access to Extreme Platform ONE Networking. If Connect users are added to other accounts as external users, they can use the ExtremeCloud IQ (Classic) account switcher to switch between the external accounts to which they have access.

Table 5: ExtremeCloud IQ 9-dot menu

Subscription types	Available applications	Available for trial
Pilot	ExtremeCloud IQ (New)	• Extreme Platform ONE Networking • Extreme Platform ONE Security • ExtremeCloud SD-WAN
Pilot + EP1 Standard OR EP1 Standard	Extreme Platform ONE Networking	• Extreme Platform ONE Security • ExtremeCloud SD-WAN
Pilot + EP1 Standard OR EP1 Standard + Extreme Platform ONE Security + ExtremeCloud SD-WAN	• Extreme Platform ONE Networking • Extreme Platform ONE Security • ExtremeCloud SD-WAN • ExtremeCloud IQ (Classic)	None available
Pilot + ExtremeCloud SD-WAN	• Extreme Platform ONE Networking • ExtremeCloud SD-WAN	Extreme Platform ONE Security
Pilot + Extreme Platform ONE Security	• Extreme Platform ONE Networking • Extreme Platform ONE Security	ExtremeCloud SD-WAN

Table 5: ExtremeCloud IQ 9-dot menu (continued)

Subscription types	Available applications	Available for trial
Pilot + ExtremeCloud SD-WAN + Extreme Platform ONE Security	• Extreme Platform ONE Networking • Extreme Platform ONE Security • ExtremeCloud SD-WAN	None available
Pilot + ExtremeCloud SD-WAN + Extreme Platform ONE Security + Extreme Intuitive Insights	• Extreme Platform ONE Networking • Extreme Platform ONE Security • ExtremeCloud SD-WAN • Extreme Intuitive Insights	None available

Log in to ExtremeCloud IQ

Use this task to log in to ExtremeCloud IQ.

1. In a web browser, go to <https://extremeplatformone.com>, and enter your ExtremeCloud IQ credentials.
2. Select **Log In**



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. You can use the 9-dot menu to switch to ExtremeCloud IQ (Classic)

3. If you have access to multiple VIQs, select **Manage My Network** to manage your primary account, or select another account.

This dialog appears only if you have multiple accounts.



Note

Connect VIQs are not linked to an Extreme Portal Account. Therefore, Connect accounts do not have access to Extreme Platform ONE Networking. If Connect users are added to other accounts as external users, they can use the ExtremeCloud IQ (Classic) account switcher to switch between the external accounts to which they have access.

Navigate ExtremeCloud IQ

Log in to ExtremeCloud IQ.

After you log in, ExtremeCloud IQ displays the **Manage > Devices** page.

1. Use the left-hand navigation bar to select one of the tabs, and then make a selection from the navigation drawer.
2. Hover over  to open the ExtremeCloud IQ menu and select a link.

To do this	Select
Configure Global Settings. For more information, see About Global Settings on page 55.	Global Settings
Change the Virtual IQ (VIQ) account you are connected to. This option is available only to SSO users whose IDP/Domain is integrated with multiple VIQs.	Switch My Network
Change the ExtremeCloud IQ account that you are managing. This option is available only if you have been defined as an external administrator in one or more different VIQs.	Switch ExtremeCloud IQ
Learn about ExtremeCloud IQ.	About ExtremeCloud IQ
Check for communications about ExtremeCloud IQ.	Communications
Read about Cloud Security.	Cloud Security Information
Log out of ExtremeCloud IQ.	Logout

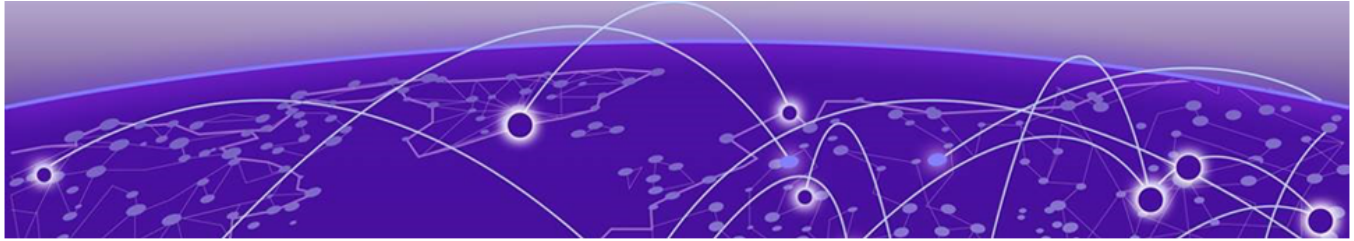
Related Links

[About Global Settings](#) on page 55

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



Onboarding

- [Add Devices Overview](#) on page 22
- [Quick Add Devices](#) on page 28
- [Add Devices with Advanced Onboarding](#) on page 34
- [About Digital Twin](#) on page 36
- [Wireless AP Overview](#) on page 36
- [AFC Overview](#) on page 43

Use Onboarding to set up a basic network structure for your interactions with ExtremeCloud IQ. Then use the following tabs in the left-hand navigation space to navigate ExtremeCloud IQ:

- **Configure:** Create advanced network structures when necessary. Configure users, network policies, and common objects.
- **Manage:** View user or device status, customize device configurations at the device level, and assign devices to existing locations.
- **ML Insights:** Monitor your network on a daily basis.

Add Devices Overview

There are two ways to onboard real or simulated devices:

- [Quick Add Devices](#) is a simplified way to add devices to your network. If you choose to manage your devices directly from the cloud, you can onboard real or simulated devices to your network. When you create simulated devices with this method, you can also create Digital Twin devices. Create simulated devices to help you prepare your network for real devices. You can create up to 20 Digital Twins, each with a lifespan of 4 hours. For more information about the Digital Twin feature, see [About Digital Twin](#). If you choose to manage your devices locally, with an on-premise controller, you can select ExtremeWireless WiNG, ExtremeXOS/Switch Engine, or VOSS/Fabric Engine devices. All you need is the device serial number.
- [Advanced Onboarding](#) is a guided process to add manually managed real devices or cloud-managed real or simulated devices, assign locations, and either assign an existing network policy or create and assign a new network policy.

ExtremeCloud IQ supports many families of devices and each family is sufficiently distinct from others to make onboarding them together complicated. Multiple devices

of the same family can always be onboarded together. The following items **cannot** be onboarded with devices from a different device family:

- Any AP device family with any switch or router family
- Switch Engine Switches
- Fabric Engine Switches
- Universal Hardware Switches
- ExtremeWireless WiNG Controller
- ExtremeCloud IQ Controller
- ExtremeCloud IQ Site Engine
- Universal Appliances
- Tunnel Concentrator instances

When an AP is powered on for the first time, it begins a sequence of steps to connect to the network. For more information, see the [Universal AP Boot and Onboarding Process](#).

Related Links

[Quick Add Devices](#) on page 28

[Quick Add Tunnel Concentrators](#) on page 31

[Add Devices with Advanced Onboarding](#) on page 34

[Add Locally Managed Devices](#) on page 32

[Wireless AP Overview](#) on page 36

[About Digital Twin](#) on page 36

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.
- [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](#): 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 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. 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:
 - 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, hover over  to open the ExtremeCloud IQ menu and select **About ExtremeCloud IQ** to find the link to your **Firewall Configuration Guide**.

Universal/Worldwide SKU Region and Country Fingerprinting

1. ExtremeCloud IQ 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 in the UI.
 - If fingerprinting fails, ExtremeCloud IQ 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, hover over  to open the ExtremeCloud IQ menu and select **About ExtremeCloud IQ** 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 and always engage with ExtremeCloud IQ 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.

From ExtremeCloud IQ, onboard and register the Universal AP using either **Local Management** or **Cloud Management**.

If local network configuration (DHCP or DNS) is not available to assist the AP to find ExtremeCloud IQ Controller, Enhanced Discovery from ExtremeCloud IQ is supported. The AP takes the IP address or FQDN of ExtremeCloud IQ Controller. For more information, see [Enhanced Discovery](#) on page 33.

If locally onboarded, ExtremeCloud IQ 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 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

If onboarded to ExtremeCloud IQ (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, hover over  to open the ExtremeCloud IQ menu and select **About ExtremeCloud IQ** 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.
 - 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 25.
- If the AP is unable to complete a firmware upgrade or complete configuration, ensure port TCP 443 is 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 Utility](#) on page 447.

Quick Add Devices

**Note**

- For information about adding a Tunnel Concentrator, see [Quick Add Tunnel Concentrators](#) on page 31.
- For information about onboarding access points, see [Add Devices Overview](#) on page 22.
- For information about adding switches, see the [ExtremeCloud IQ Universal Switch Deployment Guide](#).

Use this task to quickly add devices to ExtremeCloud IQ from the **Manage > Device List** page.

1. Go to **Manage > Devices**.
2. Select , then select **Quick Add Devices**.

3. Select **Manage your devices directly from the cloud.**

If you intend to manage your devices locally through an on-premise controller, see [Add Locally Managed Devices](#) on page 32 for instructions before you proceed to the next step.

4. For **Device Type**, select **Real** or **Simulated**.

- For **Real** devices: For **Entry Type**, either select **Manual** and enter device serial numbers in the field, or select **CSV** to import a **.csv** file with a list of device serial numbers or service tags. If you select **Manual**, ExtremeCloud IQ tries to detect your device automatically when you submit the serial numbers and displays the detected device make in a separate field. If it cannot detect the device make from the serial number, it prompts you to select a device make manually.



Note

To onboard a Universal Hardware Switch, for the **Device OS**, choose **Switch Engine** or **Fabric Engine**.

Your CSV file must have at least one field containing serial numbers or service tags. Add a second field for the model numbers of the devices. For example:

Serial Number:

01234567890123

01234567890124

01234567890125

Serial Number and Model Number:

01234567890123, AP3000

01234567890124, AP410

01234567890125, AP5050



Note

Avoid using spreadsheet applications such as Excel to create or modify a **.csv** file. Excel formats serial numbers that contain preceding zeros incorrectly. Many applications interpret the serial number as a numeric value, which can cause the preceding zeros to be lost and the value to be represented in scientific notation, requiring you to use special functions or convert the cell content type. Instead, use a text editor that does not format the contents.

- For **Simulated** devices: In the **Device Model** drop-down list, choose a model, and enter the number of devices to add. Repeat this step to add different models.
- For **Digital Twin** devices: Use to create a simulated Switch Engine Switch. Select **Switch Engine** from the **OS Persona**, then select the **Device Model** and **OS Version**. Proceed to **Step 4**.



Note

You can only add Digital Twin devices if you are also using ExtremeCloud IQ CoPilot.

5. For **Location**, select a location from the pick list.

**Note**

You cannot create a new location in the Quick Add process; you can select an existing location.

6. From the **Policy** menu, select an existing network policy.
7. Select **Add Devices** or **Launch Digital Twin**.

**Note**

To add a device that was previously onboarded using an earlier version of ExtremeCloud IQ or Extreme Management Center, you must first delete the device from the older version. In these instances, you see an alert.

Related Links

[Add Devices Overview](#) on page 22

[Quick Add Tunnel Concentrators](#) on page 31

[Wireless AP Overview](#) on page 36

Quick Add Tunnel Concentrators

Deploy the Tunnel Concentrators instances. For more information, see the documentation for [Extreme Tunnel Concentrator](#).

Use this task to quickly add Tunnel Concentrator instances as devices and register the serial number for each instance.

1. Go to **Manage > Devices**.
2. Select , then select **Quick Add Devices**.
3. Select **Manage your devices directly from the cloud**.
4. For **Device Type**, select **Real**.
5. For **Entry Type**, select **Manual**.
6. Type the **Serial Number** of the device.
7. From the **Device Make** menu, select **Tunnel Concentrator**.
8. (Optional) From the **Policy** menu, select an existing network policy.
If you do not already have an existing policy configured for this purpose, skip this step and add the policy later.
9. Select **Add Devices**.

After you complete this procedure, you can open the Tunnel Concentrator application from ExtremeCloud IQ.

Select a Tunnel Concentrator from the **Devices** page to view the device details. To open the Tunnel Concentrator application, go to one of the following locations:

- **Device Details > Monitoring > Overview**
- **Device Details > Monitoring > System Information**

Related Links

[Configure Tunnel Concentrator Services](#) on page 352

[Quick Add Devices](#) on page 28

Add Locally Managed Devices



Note

Onboard locally managed devices to monitor them from ExtremeCloud IQ. You cannot use ExtremeCloud IQ to adjust the device configuration for locally managed devices.

For information about supported switches, see [ExtremeCloud IQ Release Notes](#).

Use this task to onboard supported switches that you intend to manage locally, with an on-premise controller. This option applies to WiNG, Switch Engine, or Fabric Engine devices.

1. Go to **Manage > Devices**.
2. Select **+**, then select **Quick Add Devices**.
3. Select **Manage your devices locally**.
4. To enter the devices manually, select **Manual** and enter the associated serial numbers.

If you select **Manual**, ExtremeCloud IQ tries to detect your device automatically when you submit the serial numbers and displays the detected device make in a separate field. If it cannot detect the device make from the serial number, it prompts you to select a device make manually.



Note

Insert serial numbers that are part of the same platform family.

5. To use a CSV file to enter the devices, select **CSV**.
6. Select the device make from the drop-down list.

7. Drag or choose a **.csv** file with a list of device serial numbers or service tags, and a second field for the model numbers of the devices.

For example:

Serial Number :

12345678901234

12345678901235

12345678901236

Serial Number and Model Number:

12345678901234, AP3000

12345678901235, AP410

12345678901236, AP5050

Optionally, you can specify the IP addresses for local controllers by using the fields *Controller1* and *Controller2*. For more information, see [Enhanced Discovery](#) on page 33.

Serial Number, Model Number, Controller1, and Controller2:

12345678901234, AP350, 192.0.2.1, 192.0.2.2

12345678901235, AP410, 192.0.2.3, 192.0.2.4

12345678901236, AP630, 192.0.2.5, 192.0.2.6



Note

Avoid using spread sheet applications such as Excel to create or modify a CSV file. Excel formats serial numbers that contain preceding zeros incorrectly. Many applications interpret the serial number as a numeric value, which can cause the preceding zeros to be lost and the value to be represented in scientific notation, requiring you to use special functions or convert the cell content type. Instead, use a text editor that does not format the contents.

Related Links

[Enhanced Discovery](#) on page 33

[Add Devices Overview](#) on page 22

[Add Devices with Advanced Onboarding](#) on page 34

[Quick Add Devices](#) on page 28

Enhanced Discovery

Enhanced Discovery can be used to enhance support of onboarding for Local Management (within ExtremeCloud IQ) providing an option to define the list of primary and secondary controllers running ExtremeCloud IQ Controller.

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.

With Enhanced Discovery, the user assigns a selection of APs to be managed by a specific controller (or high availability pair) as part of the conversion to local operating system. Once the AP boots into the local WiNG operating system, if the discovery override is defined, the AP automatically connects to the indicated controller, bypassing the traditional discovery methods.

Universal APs are configured for cloud management by default. To manage these APs locally, select **Local Management** when onboarding the APs in ExtremeCloud IQ.

In a remote deployment, you can configure the IP addresses or FQDNs of the primary and secondary controllers for local management. First, the AP uses a REST API call to connect to ExtremeCloud IQ. The API response includes the configured controller IP addresses. After the AP successfully adopts to ExtremeCloud IQ Controller, the access point reboots to the local management persona.

Enhanced Discovery is supported when manually onboarding devices or when importing devices with a .csv file.

**Note**

Enhanced Discovery is supported on AP3000 and ExtremeCloud IQ Controller.

Related Links

[Add Locally Managed Devices](#) on page 32

[Enhanced Discovery Action](#) on page 454

Add Devices with Advanced Onboarding

Use this task to add devices to ExtremeCloud IQ from the **Manage > Device List** page. Use **Advanced Onboarding** when you want to create a new location or a new network policy for the device.

For more information about adding switches, see the [ExtremeCloud IQ Switch Deployment Guide](#).

Use this task to add devices using Advanced Onboarding.

1. Go to **Manage > Devices**.
2. Select  and then select **Advanced Onboarding**.

3. On the **Onboard your devices** tab, select the **Device Type: Real** or **Simulated**.

- **For simulated devices:** In the device model drop-down list, choose a model, and enter the number of devices to add. Repeat this step to add different models.
- **For real devices:** Either manually enter the serial numbers in the first field, separated by commas, or import a CSV file by either dragging the file into the second field, or browse for a file by selecting **Choose**.

**Note**

To onboard a Universal Hardware Switch, for the **Device OS**, choose **Switch Engine** or **Fabric Engine**.

Your .csv file must have at least one field containing serial numbers. Add a second field for the model numbers of the devices. For example:

Serial Number :

01221234567890

01221234567891

01221234567892

Serial Number, and Model Number:

01221234567894, AP3000

01221234567895, AP410

01221234567896, AP5050

**Note**

Avoid using spread sheet applications such as Excel to create or modify a .csv file. Excel formats serial numbers that contain preceding zeros incorrectly. Many applications interpret the serial number as a numeric value, which can cause the preceding zeros to be lost and the value to be represented in scientific notation, requiring you to use special functions or convert the cell content type. Instead, use a text editor that does not format the contents.

4. For **Assign a network policy** (optional): Select an existing network policy from the drop-down list or [create a new network policy](#).
5. Select **Next**, and then **Finish**.

Related Links

[Add a Network Policy](#) on page 102

[Add Devices Overview](#) on page 22

[Add Locally Managed Devices](#) on page 32

[Quick Add Devices](#) on page 28

[Wireless AP Overview](#) on page 36

About Digital Twin

Digital Twin allows you to create simulated devices to help you prepare your network for real devices. You can perform multiple actions to see how the devices will function in your networks in the same way as you would with actual devices.

You can have a maximum of 15 Digital Twins with every ExtremeCloud IQ CoPilot account, with a maximum of 5 of these 15 in an active or running state at the same time. Digital Twins have a maximum uptime of 24 hours, after which they are automatically shut down. To continue using a Digital Twin that has been shut down, you must manually re-launch it.

Digital Twin devices appear in the device list and are identified by an icon showing two masks—. Select the **Hostname** to see more details and make modifications, just as you would for a real device. Many of the same monitor and configuration options that apply to real devices are available for twins.

Select the check box for a **Digital Twin** device in the **Device** list to activate the **Actions** drop-down list above the table.

Select the check box for a **Digital Twin** device to activate the **Update** option above the table. In the dialog box, you can select **Perform Update** to update the network policy and configuration.

Wireless AP Overview

ExtremeCloud IQ access points (APs) use 802.11 wireless standards (802.11a/b/g/n/ac/ax/be) for network communications, and bridge network traffic to an Ethernet LAN.

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

ExtremeCloud IQ supports the following Universal APs.

Table 6: ExtremeCloud IQ Supported Universal APs

AP Class	Supported Universal APs
Wi-Fi 7 Universal World-Wide APs ExtremeCloud IQ	• AP4020/AP4020X/AP4020FX • AP4060/X • AP5020
Wi-Fi 6E Universal World-Wide APs ExtremeCloud IQ	• AP3000/X • AP4000 • AP4000-1 • AP5010 • AP5050U/AP5050D
Wi-Fi 6 Universal APs ExtremeCloud IQ	• AP302W • AP305C/CX • AP305C-1 • AP410C • AP410C-1 • AP460C/S6C/S12C • AP510C/CX

Related Links

[AP3000 Series Radios and 6 GHz Support](#) on page 37

[AP4000/AP4000-1 Radios and 6 GHz Support](#) on page 39

[AP5000 Series Radios and 6 GHz Support](#) on page 41

[Add Devices Overview](#) on page 22

[Quick Add Devices](#) on page 28

[Add Devices with Advanced Onboarding](#) on page 34

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.

The AP3000 series APs offer two radios in three modes:

Table 7: 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 requires that your 6 GHz radio network assignment be WFA 6E compliant. ExtremeCloud IQ 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.



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.

Related Links

[Wireless AP Overview](#) on page 36

AP4000/AP4000-1 Radios and 6 GHz Support

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

Table 8: AP4000/AP4000-1 Radio Modes

Radio	Radio Modes
Radio 1	• b/g • g/n • b/g/n • g/n/ax • client-bridge
Radio 2	• a/n/ac • a/n/ac/ax • client-bridge
Radio 3	• 2x2 WLAN Service 6.0 GHz, Or • 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 9: AP4020/AP4020X/AP4020FX Radio Modes

Radio	Radio Modes
Radio 1	• b/g • g/n • b/g/n • g/n/ax • client-bridge
Radio 2	• a/n/ac • a/n/ac/ax • client-bridge
Radio 3	• 2x2 WLAN Service 6.0 GHz, Or • 2x2 WLAN 2.4 GHz, dual 5.0 GHz, 6.0 GHz
Radio 4	• Dedicated sensor mode. • Performs full-time scanning and sensing across all available wireless channels (2.4 GHz, 5 GHz, and 6 GHz). • Does not serve client devices. 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.

**Note**

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

ExtremeCloud IQ 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 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 requires that your 6 GHz radio network assignment be WFA 6E compliant. ExtremeCloud IQ 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.

**Note**

AP4000-1 models do not support IoT.

Related Links

[Wireless AP Overview](#) on page 36

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
- AP5050U — Indoor/Outdoor AP Wi-Fi 6E
- AP5050D — Indoor/Outdoor AP Wi-Fi 6E with selectable narrow and wide angle built in directional antennas.

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.

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

For AP5020 devices, ExtremeCloud IQ uses GPS-based location information when determining AFC spectrum assignments. When an AP5020 connects, ExtremeCloud IQ automatically sends a GPS query to the device. After the AP reports its GPS coordinates, ExtremeCloud IQ 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 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

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 causes a radio reset.

Table 10: AP5000 Series Radio Modes

Radio	Radio Modes
Radio 1: • 4x4 WLAN Service 2.4 GHz • 2x2 WLAN Tri-Band Sensor, 2.4 GHz, 5.0 GHz, 6.0 GHz	• sensor • b/g • g/n • b/g/n • g/n/ax • g/n/ax/be (AP5020 only) • client-bridge
Radio 2: • WLAN Service 5.0 GHz • 4x4 WLAN Service 5.0 GHz	• a/n/ac • a/n/ac/ax • a/n/ac/ax/be (AP5020 only) • client-bridge
Radio 3: • 4x4 WLAN Service 6.0 GHz • 2x2 WLAN Service 2.4 GHz	• ax6 • ax6/be (AP5020 only) • client-bridge

Related Links

[Wireless AP Overview](#) on page 36

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.

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 on behalf of eligible ExtremeCloud IQ 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 specifying over which channels and at which power levels the AP can operate.

ExtremeCloud IQ 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 supports AFC with the AP5050 and AP5020. 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 offers AFC with Geo-Location Agent support. The AP5020 supports 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 uses GPS-based location information when determining AFC spectrum assignments. When an AP5020 connects, ExtremeCloud IQ automatically sends a GPS query to the device. After the AP reports its GPS coordinates,

ExtremeCloud IQ applies the standard AFC filtering criteria to determine whether spectrum can be assigned to the AP.

Table 11: 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 44

[Anchor and Non-Anchor APs](#) on page 46

[6 GHz Radio Power AFC](#) on page 47

[6 GHz Radio — Standard Power Operation without AFC Approval](#) on page 48

[GeoLocation Agent](#) on page 49

[GeoLocation Coordinates](#) on page 50

[AP Placement for AFC](#) on page 52

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 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 supports the following indoor AFC devices:

- AP4020/AP4020X/AP4020FX
- AP4060/AP4060X
- AP5020
- 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.

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 outdoor APs operate safely and legally by coordinating spectrum use with licensed incumbents in the 6 GHz band.

ExtremeCloud IQ 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 43

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 assigns geo-location coordinates to all APs under its control.

- The AP4020 and AP5020 are non-anchor APs that supports 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 43

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.

AP4020/AP5020

You can configure the AP4020/AP5020 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 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 43

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 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 12](#).

Table 12: 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 43

GeoLocation Agent

The GeoLocation Agent within ExtremeCloud IQ 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/AP4020/AP5010/AP5020/AP5050 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 43

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/AP5050), 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.

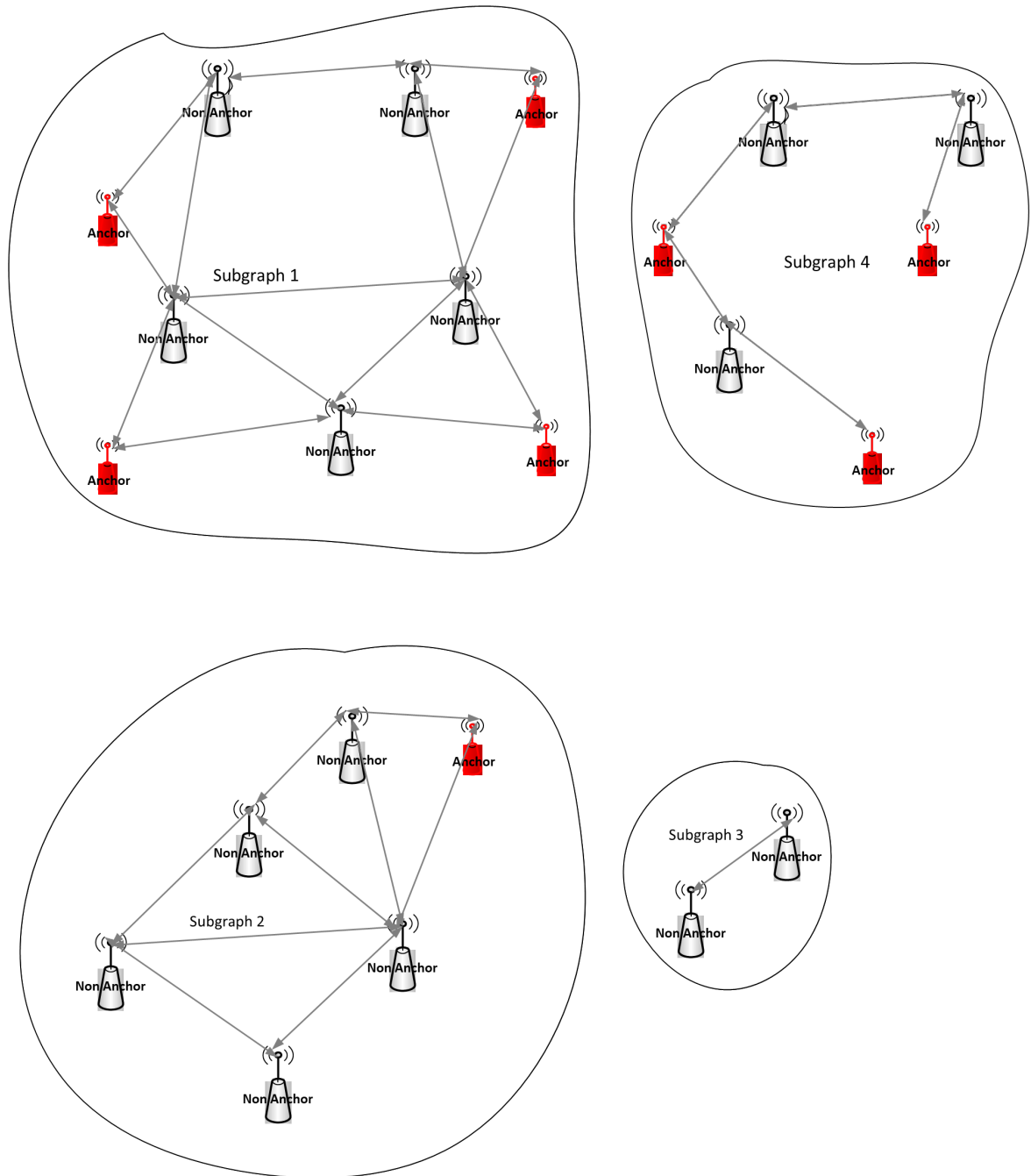


Figure 1: Example Subgraph Scenarios

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 43

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 53.

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 53.

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, and AP5050 can be used as a non-anchor AP.

Related Links

[AFC Overview](#) on page 43

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
- GnssLogger

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.

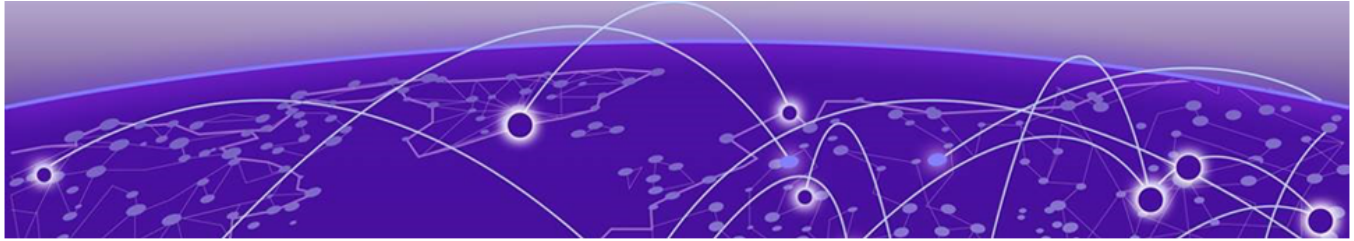
1. Position the phone at the proposed AP placement area and wait up to 30 minutes for GPS lock.

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 52



Administration

[About Global Settings](#) on page 55
[Manage Account Details](#) on page 55
[Enable ExtremeCloud IQ Classic](#) on page 56
[Account Management](#) on page 57
[Add a Credential Distribution Group](#) on page 61
[Enable Two-Factor Authentication](#) on page 62
[Manage Licenses and Subscriptions](#) on page 63
[Set a Device Default Password](#) on page 67
[Manage the Virtual IQ](#) on page 68
[Enable Single Sign On \(SSO\)](#) on page 70
[Set Email Notifications](#) on page 77
[Manage API Access Tokens](#) on page 78
[Add an API Presence and Data Location Feed](#) on page 80
[Add a Third-Party API Token](#) on page 81
[Download Logs](#) on page 81
[Enable SSH Availability](#) on page 88
[Enable Supplemental CLI](#) on page 88

Administration provides access to various ExtremeCloud IQ settings as follows:

- **Global Settings:** Define criteria that affects the entire system. For example, license and subscription management, device settings, email notifications, API settings, and viewing activity logs.
- **Switch My Network:** Switch between multiple Virtual IQ accounts.
- **Switch ExtremeCloud IQ Accounts:** Switch between multiple ExtremeCloud IQ accounts.

About Global Settings

Global Settings affect the entire ExtremeCloud IQ management system as follows:

- **Account Details:** View personal and organizational information about the administrator that is currently logged in to this account. [Manage Account Details](#) on page 55
- **Account Management:** Add, delete, or edit accounts. [Add or Edit an Administrator Account](#) on page 58
- **Credential Distribution Groups:** Add, delete, or edit credential distribution groups. [Add a Credential Distribution Group](#) on page 61
- **License Management:** View and add license and entitlement objects. [Manage Licenses](#) on page 66
- **Device Management Settings :** View and modify the default device management password. [Set a Device Default Password](#) on page 67
- **VIQ Management:** Manage the Virtual ExtremeCloud IQ. [Manage the Virtual IQ](#) on page 68
- **Email Notifications:** View, add, and modify email notification rules for status changes. [Set Email Notifications](#) on page 77
- **API:** View, add, modify, and delete API data management objects, and enable and disable presence and location data feeds. [Add an API Presence and Data Location Feed](#) on page 80, [Add a Third-Party API Token](#) on page 81, [Generate API Access Tokens](#) on page 79
- **Logs:** View and sort logs. Download log entries for any or all admin accounts. [Download Audit Logs](#) on page 82
- **SSH:** Provide temporary remote access to your network for troubleshooting purposes. [Enable SSH Availability](#) on page 88

Manage Account Details

Use this task to edit your personal and company information.

1. Hover over , and then select **Global Settings**.
2. From the **Accounts** menu, select **Account Details**, and then configure the settings for your account.

Table 13: Account Details Settings

Setting	Description
Personal Information	
Name	The name of the account. Select  , type the new value, and then select  .
Role	Information only—you cannot edit the Role .
Email	The primary email address for your account. Select  , type the new value, and then select  .

Table 13: Account Details Settings (continued)

Setting	Description
Proactive license warning email messages	Select the toggle to change the setting. Set to ON to receive emails about upcoming license and subscription expiration dates.
Alternate Email	An alternate (optional) email address for your account. Select  , type the new value, and then select  .
Phone Number	The phone number for your account. Select  , type the new value, and then select  .
Job Title	Your job title. Select  , type the new value, and then select  .
Password	The password for your account. Select CHANGE PASSWORD, type the current password, and then type the new password twice: New Password and Confirm New Password. Select SAVE. Note: After you change your password, you can continue your current administrative session or navigate through the GUI. After you log out of your current session, you must enter your new password the next time you log in. To change your password at the log in prompt, select Forgot Password and follow the instructions.
Select Language	Select your preferred language from the menu, and then select APPLY. Note: You must log out for the change to take effect.
Organization Information	
Organization Name	The name of the organization. Select  , type the new value, and then select  .
Industry	Select an industry from the drop-down list and then select Apply. Note: The industry that you identify here indicates the group that submits data for CoPilot global analytics.
Address	Select  , type the new value, and then select  .

Related Links

[About Global Settings](#) on page 55

Enable ExtremeCloud IQ Classic

Use this task to link your devices directly to the ExtremeCloud IQ Classic version:

1. Hover over , and then select **Global Settings**.
2. From the **Accounts** menu, select **ExtremeCloud IQ Classic Account**.

3. Toggle the **Status** switch to **ON**.
4. Enter your user name.
5. Enter your password.
6. Select **Get Organization**.

Related Links

[About Global Settings](#) on page 55

Account Management

The **Admin Accounts** page displays a list of existing administrator accounts in a table format.

The table displays the following information about administrator accounts:

- User Name
- Email Address
- Role
- MFA Status
- Location

Select a column header to sort the table according to that value.

The table features controls for adding, editing, and deleting administrator accounts. Use the **MFA Status** filter to display accounts as follows:

All

Show all accounts, regardless of multifactor authentication (MFA) status.

Enabled

Show only the accounts for which MFA is enabled.

Not Enabled

Show only the accounts for which MFA is not enabled.

Unknown

Show only the accounts for which the MFA status is unknown.

If the list is long, you can select the number of results to display per page and use the page controls to navigate the list. Use the **Search** feature to find a specific account. To download the list of administrators in CSV file format, select **DOWNLOAD**.

Related Links

[Add or Edit an Administrator Account](#) on page 58

[Account Management Settings](#) on page 58

Add or Edit an Administrator Account

Use the following task to add a new administrator account or to edit an existing account.

1. Hover over , and then select **Global Settings**.
2. From the **Accounts** menu, select **Account Management**.
3. Select an existing account, and then select , or select .
Use the **Search** field to help locate an existing account.
4. To configure the account, see [Account Management Settings](#) on page 58.
5. Select **SAVE & CLOSE**.

Related Links

[Account Management](#) on page 57

[Account Management Settings](#) on page 58

[About Global Settings](#) on page 55

Account Management Settings

For a new account, specify whether the new admin is internal to your organization, or external:

- **Create a new admin account:** Select to create an account for an admin within your organization.
- **Grant access to an external admin:** Select to grant access to administrators outside of your organization. These administrators include personnel from Extreme Networks resellers, distributors, technical support, and sales.



Note

External administrators must have an ExtremeCloud IQ account before they can be added.

Table 14: Account Management Settings

Field	Description
Email Address	The email address of the administrator.
Name	The name of the administrator (internal admin only).
Idle Session Timeout	The number of minutes before a session times out (internal admin only).
Choose a Role —Assign a role to each admin.	

Table 14: Account Management Settings (continued)

Field		Description
	Installer	Designed to work with the mobile app, and has limited privileges based on the built-in limitations of the app. If you log into ExtremeCloud IQ as an admin with Installer privileges using the standard web interface, the Management , Insights , and Configuration tools are read-only with the following exceptions: • Onboard, update, reboot, and delete devices • Assign network policies • Assign locations • CLI access • Flash LEDs
	Guest Management	Has access only to the guest management admin interface. This is mainly for employees who need to create user accounts for guests, contractors, and employee personal devices to enable access to the wireless network.
	Application Operator	Can view status information about client devices and supported APs and change roles for a client device. this role cannot see other menus, or make configuration changes to the network.
	Observer	Has read-only access to most of the ExtremeCloud IQ interface. This role does not have access to the account and license or subscription management functions. The difference between Observer and Monitor is the Monitor role has write access to the Tools tab and read access to the rest of the network. The Observer has read-only access.
	Monitor	Has full read-write access to system Tools located at Manage > Devices > Utilities > Tools and restricted (read-only) access to the remaining tabs. With full access to the Tools tab, the monitor role can diagnose client issues, escalate issues, and mark issues as resolved.
	Administrator	Has full read-write access to ExtremeCloud IQ and your network. This is the only role that can create and manage administrators and ExtremeCloud IQ licenses.
	Help Desk	Has full access to the Tools tab. They can diagnose client issues, escalate issues, and mark issues as resolved, and search by user name to see details for a user, or by MAC address to see details for a client.

Table 14: Account Management Settings (continued)

Field		Description
	Operator	Has full write access, but cannot manage accounts and licensing. An operator can also update the network map (located on the Manage > Planning tab) to add a building or a floor to any location, unless they are restricted to a single location. Note: Local operators cannot view alarms for locations they cannot access.
Access Scope —Available only when the site isolation feature is enabled for the VIQ. Assign the locations to which the administrator has access. Access restrictions by location are based on the locations defined in your network map. This scope applies to all roles.		
	All Sites	The administrator can create and edit objects for all sites (global).
	Custom	The administrator can create objects only for specified sites. Select the down arrow to display the Assign Sites menu. Select the sites to which the administrator will have access. Clear the corresponding check box to remove access to a site. To specify global read only access for the administrator, select Read Only , under Global Permissions .
Global Permissions —Available only when you select Custom for the Access Scope , and the site isolation feature is enabled for the VIQ.		
	Read & Write	The administrator can edit global objects.
	Read Only	The administrator can view the settings for global objects, but cannot make changes.

Related Links

[Account Management](#) on page 57

[Add or Edit an Administrator Account](#) on page 58

[Manage the Virtual IQ](#) on page 68

Delete an Administrator Account

Use the following task to delete administrator accounts that are no longer required.

1. Hover over , and then select **Global Settings**.
2. From the **Accounts** menu, select **Account Management**.
3. Select the corresponding check boxes for the accounts that you want to delete, and then select .
4. Select the check box to confirm you understand that all data associated with the selected administrator accounts will be deleted.
5. Select **Yes**.

Related Links

[Account Management](#) on page 57

Add a Credential Distribution Group

Use this task to create Credential Distribution Groups for members of your organization who are permitted to distribute log in credentials to visitors.



Note

When defining Credential Distribution groups, the required details for **Admin Account** depend on the specific type of administrative account.

In most cases, you enter the email address associated with the Guest Management account in [Account Management Settings](#). However, if the Guest Management account was created automatically by Self-Service SSO (and has a blue SSO badge), you must use the automatically generated saml.login user ID (such as, abcdefg12345@saml.login). This value must be obtained by the GET /users XAPI call. For more information, see the [ExtremeCloud IQ XAPI Swagger](#) or [ExtremeCloud IQ API Reference](#).

1. Hover over , and then select **Global Settings**.
2. From the **Accounts** menu, select **Credential Distribution Groups**.
3. Select an existing group, and then select , or select .
4. Configure the settings.

Setting	Description
Group Name	(Required) Type a name for the group.
Admin Account	(Required) From the menu, choose Active Directory User or Guest Management Role User .
Member Of	Active Directory User only Enter the Active Directory user group for the account. If the account is a member of multiple groups, type the name of the first group, press Enter , and then enter the next group name.
Guest Management User	(Required) Guest Management Role User only Enter the access control role to assign to a group member.
Credential Restriction	Select Restrict the number of credentials per employee to , and then select the number of credentials that group members can distribute.
Registration Operation	Select Email Approval .
Enable User Groups	Add existing user groups to add to this credential distribution group either by selecting Select All , or by selecting the check boxes for individual user groups.

5. Select **SAVE**.

Related Links

[About Global Settings](#) on page 55

Enable Two-Factor Authentication

Use these steps to configure ExtremeCloud IQ to require multi-factor authentication at log in. When this feature is enabled, to log in, enter your VIQ account admin name and password credentials, and then enter a six-digit key generated by an authentication app. Authentication apps generate time-based one-time keys and run on iOS and Android devices.

**Note**

ExtremeCloud IQ Two-Factor Authentication is not supported when using Single-Sign On (SSO).

To enable two-factor authentication:

1. Hover over , and then select **Global Settings**.
2. From the **Accounts** menu, select **Multi-Factor Authentication**.
3. Toggle the **Status** switch to **ON**.
4. Install an authenticator app on your iOS or Android smart device.
5. Open the authenticator app, select **Scan Barcode**, and scan the on-screen QR code.

Alternately, you can open the authenticator app, select **Manual Entry**, enter the email address you use as your admin name when logging into ExtremeCloud IQ, and enter the secret key that ExtremeCloud IQ displays. After you scan the QR code or enter a valid email address and secret key, the authenticator app displays a six-digit code, which changes every 30 seconds.

6. Enter the six-digit code in the **Step 2** text box in the **Setup Multi-Factor Authentication** window.
7. Select **Confirm** to activate multi-factor authentication for yourself.

**Note**

For legibility, the authenticator app includes a space between the first three digits and the second three digits in its display. Do not include this space when you enter the six-digit code.

When administrators log in, they enter their admin name and password, the authenticator app code, and select **Submit**. If authorized sessions were active using earlier authentication, an informational message alerts the user of this state. Verify this message to terminate these sessions after successful enforcement of MFA authentication.

Related Links

[About Global Settings](#) on page 55

Manage Licenses and Subscriptions

The first time that you log into ExtremeCloud IQ, you are redirected to the Extreme Portal and prompted for your credentials. If you do not have an Extreme Portal account, you must register for one before you can continue.



Note

If you are partner, distributor, or reseller, and are setting up an account for a customer, you can create the account and then instruct the customer to log into their new ExtremeCloud IQ instance and proceed through the prompts.

After you enter your credentials, ExtremeCloud IQ retrieves the license and subscription information from your Extreme Portal account and applies it to your ExtremeCloud IQ account. See [Manage Licenses](#) on page 66.



Note

The terms *Licenses* and *Entitlements* appear throughout the ExtremeCloud IQ interface. These terms are not interchangeable. For more information, see *Extreme Platform ONE Networking and ExtremeCloud IQ Subscription and Licensing Guide*. For clarity, this guide does not use the term *License* to refer to a subscription, unless the term is used in the user interface to refer to a subscription.

Entitlements

The **Entitlements** table displays the following information about your current subscriptions and licenses:

Type

The possible values are: **Subscription**, **Permanent**, or **Evaluation**.

Total

The total number of licenses or subscriptions of that type. **Available + Activated = Total**

License Name

The name of the license or subscription. Some subscriptions add device management capabilities, while others enable specific features. Examples of subscription types:

- XIQ-PIL-S-C—ExtremeCloud IQ Pilot
- XIQ-NAV-S—ExtremeCloud IQ Navigator
- XIQ-COPILOT-S-C—ExtremeCloud IQ CoPilot

Available

The number of licenses or subscriptions that are available for use.

Activated

The number of used licenses or subscriptions.

Start Date

The date the license or subscription became valid. This column can be sorted. The date is in the UTC time zone.

End Date

The date the license or subscription expired. This column can be sorted. The date is in the UTC time zone.

Description

A description of the license or subscription, if one was entered.



Note

ExtremeCloud IQ sends aggregated information for each license or subscription type to ExtremeCloud IQ Site Engine.

ExtremeCloud IQ Site Engine displays a table listing the licenses and subscriptions purchased: XIQ-PIL-S-C, XIQ-NAV-S-C, and XIQ-NAC-S. A single line displays the **Contract Start Date**, **Contract End Date**, and **Feature**. The **Quantity** is the total number of licenses or subscriptions purchased of that type, similar to what ExtremeCloud IQ displays.

NAC Entitlements

Network Access Control (NAC) uses a set of protocols to secure devices when they access the network. The 802.1X standard is a basic form of NAC.

Universal NAC subscriptions are available for ExtremeCloud A3 and ExtremeControl.

NAC controls access using pre-admission endpoint security checks and post-admission controls over access levels and permissions that devices exercise in the network.

The total number of NAC subscriptions available appears above the **NAC Entitlements** table, and is based on the number of NAC subscriptions specified in your contracts.



Note

An MSP operator can define **Total NAC Entitlements** for the VIQ. If defined, the system uses the defined value rather than the number of NAC subscriptions that you see in the license pool.

The **NAC Entitlements** table lists the following information about NAC entitlement allocations:

- **Entitled Serial Number:** The serial number of the NAC device associated with this entitlement. The device can be running ExtremeCloud IQ Site Engine version 21.9 and newer, or ExtremeCloud A3 version 4.0 and newer.
- **Name:** The name of the NAC device.
- **Allocated %:** The percentage of the total allocations that are available to this device. You can modify this number as needed. To confirm and save your changes, click **Save**.
- **Allocated Entitlements:** The maximum number of entitlements that can be used by this device.

Legacy Entitlements

The information that this table displays depends on whether you entered an evaluation or permanent entitlement key. If you entered an evaluation key, the number of days remaining until the entitlement key expires and the number of devices licensed appears at the top of the window. If you entered a permanent key, the table displays only the number of licensed devices.

You can use unused entitlements in addition to any active licenses. For more information, see, [Manage Licenses](#) on page 66.

The **Legacy Entitlements** table displays the following information:

- **Current State:** Can be active or expired. Use the drop-down list above the column to filter these values.
- **Evaluation Period:** For evaluation keys, this column displays the number of days remaining in the evaluation period. For permanent licenses, the column displays **N/A**.
- **Entitlement Key:** The 30-character string that you received from Sales or Support. To remove or deactivate a key, select the check box for it and then select **Remove/Deactivate**. If you deactivate an active key, you can add it back later.
- **Type:** The type can be evaluation or permanent.
- **Devices:** The number of devices the entitlement key supports. The total number of devices you can manage is the sum of all the numbers associated with active keys.
- **Subscription Start and End Dates:** The start and end dates for this entitlement key. These columns can be sorted. The date is in the UTC time zone.
- **Support End Date:** The date on which the support contract expires. This column can be sorted. The date reflects the time zone setting in your browser.
- **Activation Date:** The date on which the entitlement key was activated. This column can be sorted.
- **Description:** The entitlement key description, if one was entered.

Related Links

[Link Your Extreme Networks Portal Account](#) on page 65

[Manage Licenses](#) on page 66

Link Your Extreme Networks Portal Account

Use this task to link your Extreme Networks Portal account so that when you enter your credentials, ExtremeCloud IQ retrieves the license and subscription information from your Extreme Networks Portal account and applies it to your ExtremeCloud IQ account.

1. Hover over , and then select **Global Settings**.
2. From the **Administration** menu, select **License Management**.
3. Select **Link My Extreme Portal Account**.

4. Enter your Extreme Networks Portal credentials.
- The license and subscription information appears in the **Entitlements** or the **NAC Entitlements** table.

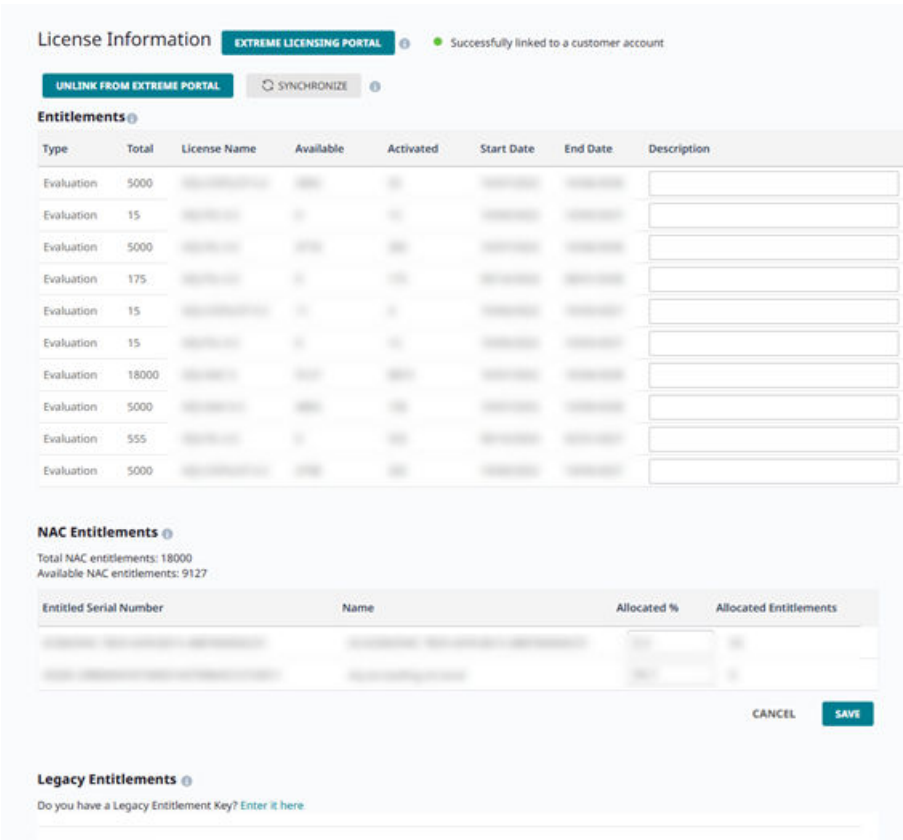


Figure 2: ExtremeCloud IQ License Information Page



Note

The information is cached. The refresh interval depends on the location of your ExtremeCloud IQ account. To update the cached information from the license pool on the **License Information** page, select **Synchronize**. Alternatively, you can unlink from and relink to the Extreme Portal using your Extreme Portal credentials.

Manage Licenses

Use this task to manage your device licenses and subscriptions in ExtremeCloud IQ.

1. Hover over , and then select **Global Settings**.
 2. From the **Administration** menu, select **License Management**.
 3. To change the number of devices that you manage, select **Contact Sales**.
 4. If you have a NAC device that does not appear in the **NAC Entitlements** table, onboard the NAC device to ExtremeCloud IQ.
- If the NAC device is compatible, it appears in the table automatically.

5. For **NAC Entitlements**, to modify the percentage allocated for a NAC device, select the serial number of the device and enter a new number in the **Allocated %** column.
6. To save changes to **NAC Entitlements**, select **SAVE**.
7. For **Legacy Entitlements** only, to enter an entitlement key, select **Enter it here**, enter the entitlement key text string in the **Enter Entitlement Key** field, select **Submit**, and accept the end user license agreement.

**Tip**

Legacy Entitlement Keys are not compatible with the upcoming licensing schema and new features. When Legacy Entitlement Keys are present and your Extreme Portal Account is linked, you cannot perform the following actions:

- Add new devices.
- Change the managed state for a device from Unmanaged to Managed.

**Note**

Perpetual Legacy Entitlement Keys are not compatible with ExtremeCloud IQ.

For more information, see this [Extreme Portal Article](#).

8. To remove or deactivate a Legacy Entitlement Key, select the corresponding check box and then select **Remove/Deactivate**.
If you deactivate an active key, you can add it back later.
9. For **Legacy Entitlements** only, select **DOWNLOAD** to download the **Legacy Entitlements** table into a CSV file.

Related Links

[Manage Licenses and Subscriptions](#) on page 63

Set a Device Default Password

Use this task to set the default password for Extreme Networks devices.

1. Hover over , and then select **Global Settings**.
2. From the **Administration** menu, select **Device Management Settings**.
3. For **Default Password**, enter the password the root admin 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.
4. **Confirm** the new password.
5. (Optional) Select **Show Password**.
6. For Switch Engine or EXOS switches, select **Enable device management settings for EXOS switches**.

This setting enables you to set **Device Credentials** at the device level for these switch series.

7. Select **Save**.

Related Links

[About Global Settings](#) on page 55

Manage the Virtual IQ

ExtremeCloud IQ administrators with read and write permission can perform the following administrative tasks:

- Manually back up and restore Virtual IQ (VIQ) account data.
- Delete data to reset the Virtual IQ database.
- Export and import Virtual IQ data.
- Toggle SSH (see [Enable SSH Availability](#) on page 88)
- Toggle the supplemental CLI tool.
- Toggle the verification of APs using the out-of-the-box wireless onboarding feature.

Use this task to manage the VIQ.

1. Hover over , and then select **Global Settings**.
2. From the **Global Settings** menu, select **VIQ Management**.
3. To perform a manual backup, select **Backup Now**.

To ensure data integrity, ExtremeCloud IQ suspends activity in the Virtual IQ during both the backup and the restore process. The **Current Status** changes from **ACTIVE** to **SUSPENDING** during these processes. When a backup is complete, ExtremeCloud IQ displays the backup event in the **Backup History** table at the bottom of the page.

4. To restore a backup, choose a backup file from the **Backup History** table, and then select **Restore**.



Note

You must restore the Virtual IQ to the same version of ExtremeCloud IQ from which you performed the backup. If the versions are different, the system displays a compatibility error message (`Version Mismatch`).

5. Select **Reset VIQ** to delete the Virtual IQ database.

This step resets the VIQ to its initial state before any inventory or configurations were added.

6. To export Virtual IQ data:

- a. Select **Export Virtual IQ** and follow the instructions in the dialog boxes.

ExtremeCloud IQ suspends the Virtual IQ during the export operation and displays a progress report showing its status. When it is complete, a message displays stating that the Virtual IQ was successfully exported. A link to the exported .tar.gz file is displayed to the right of the **Export Virtual IQ** button.

- b. Select the link to download and save the **.tar.gz** file to a local directory on your management system.

The tarball contains numerous files for different areas of the Virtual IQ, such as certificate files in PEM format, captive web portal files in HTML, JavaScript, and graphic image file formats, background image files for topology maps, and configuration objects and Virtual IQ settings in XML format.

**Note**

Global Settings > VIQ Management > Download is not available for trial VIQs.

7. To import Virtual IQ data:
 - a. Select **Import Virtual IQ**.
 - b. Select either **Import Virtual IQ from ExtremeCloud IQ** or **Import Virtual IQ from HM Classic**, depending on the source of the data.
 - c. Either drag the **.tar.gz** file into the first field at the top or select **Choose** to navigate to the location of the file and select it.
 - d. Select **Import Now**.

Optionally, you can change the import timeout, which is 30 minutes by default, and the action to take if an error occurs; abort (default) or continue.
8. To enable SSH, toggle **SSH Availability** to **ON**.

**Note**

Enabling SSH availability potentially gives others direct access to your devices during the time that 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, because SSH FTP assumes that it is running over a secure channel. For more information, see [Enable SSH Availability](#) on page 88.

9. To enable Supplemental CLI, 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. You can access this feature in multiple places in the GUI, after you enable it for the Virtual IQ.
10. To enable the Virtual IQ to permit APs to respond to mesh-join requests, toggle **AP Out-of-the-box Wireless Onboarding** 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.
11. To allow the staging of configuration push jobs to offline devices, toggle **Auto Config Push** to **ON**.

Related Links

[About Global Settings](#) on page 55

Enable Single Sign On (SSO)

Single Sign On (SSO) simplifies the login process, allowing users to log in to a service provider (SP) application, such as ExtremeCloud IQ, using their credentials from an existing SAML-enabled identity provider (IdP).

Key features of SSO:

- **Unified Access:** Log in once and gain access to all integrated services without repeated logins.
- **Improved Security:** Using 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 by removing users from the IdP.

This task provides an overview of all the SSO management options available in ExtremeCloud IQ.

1. Hover over , and then select **Global Settings**.
2. From the **ADMINISTRATION** menu, select **Enable Single Sign On (SSO)**.
3. To enable SSO, you must create an Identity Provider (IdP) profile in ExtremeCloud IQ, see [Add an IdP Profile](#).
4. To manage an existing IdP profile, from the list of IdP profiles, find the row of the profile you want to manage, select , and then from there you can:
 - a. Manage certificates, see [Manage IdP Profile Certificates](#).
 - b. Edit an existing IdP Profile, see [Manage IdP Profiles](#).
 - c. Enable or disable an IdP profile. Select **Enable**, or select **Disable** and then select **Disable** again to confirm.



Note

If disabled, users of the domain defined in the IdP profile will not be able to log in to ExtremeCloud IQ.

- d. Delete an IdP profile. Select **Delete**, and then select **Delete** again to confirm.

Related Links

[Add an IdP Profile](#) on page 70

[Manage IdP Profiles](#) on page 74

[Manage IdP Profile Certificates](#) on page 74

Add an IdP Profile

An Identity Provider (IdP) profile defines how your system 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.

The following IdPs are supported by ExtremeCloud IQ:

- 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. Hover over , and then select **Global Settings**.
2. From the **ADMINISTRATION** menu, select **Enable Single Sign On (SSO)**.
3. Select **Add IdP Profile**.
4. Select a **Type**, enter a **Domain** and **Description**, and then select **Continue**.

**Note**

Only the domain specified will allow login. If your IdP employs sub-domains, separate IdP profiles are required for each sub-domain.

For more information, including step-by-step integration with Microsoft Entra ID or Okta, see the [ExtremeCloud IQ Self-Service Single Sign On, Entra ID SAML Integration Guide](#).

5. Configure IdP Metadata for the IdP Connection, see [IdP Connection Settings](#).
6. Select **Continue**.
7. Configure [Attribute Map Settings](#), and then select **Save**.

Related Links

[Enable Single Sign On \(SSO\)](#) on page 70

IdP Connection Settings

Identity Provider (IdP) Metadata provides structured information 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:

- **IdP Entity ID:** A unique identifier for an IdP used to identify the IdP to a SP.
- **SSO URLs:** Endpoints where the SP sends authentication requests.
- **Binding Methods:** Methods used for communication between the IdP and SP.
- **Certificates:** Used for signing and encrypting SAML assertions.

This Metadata can be provided as a file ([Import Metadata](#)), as a URL ([Import from URL](#)), or you can [Manually Enter](#) the Metadata.

Import Metadata

1. Select **Import Metadata**.
2. Select **Browse Files**, then select the Metadata file from your local folder.

Import from URL

1. Select **Import From URL**.
2. Enter an **IdP Metadata URL**, and then select **Import**.

Manually Enter

1. Select **Manually Enter**.
2. Configure the IdP Metadata settings, see [IdP Metadata Settings](#).

Table 15: IdP Metadata Settings

Setting	Description
IdP Entity ID	The IdP unique identifier URL. URLs must begin with <code>https</code> .
SSO Binding	Select HTTP POST to send messages within the body of an HTTP POST request. 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 <code>https</code> .
SSO Sign Request	Select SSO Sign 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. Select HTTP POST to send messages within the body of an HTTP POST request. 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 <code>https</code> .
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 <code>https</code> .
Verification Certificate	The digital certificate used to verify the authenticity and integrity of messages exchanged between the IdP and SPs. Choose an existing certificate from the drop-down list, or select Import a new Certificate .

Related Links

[Add an IdP Profile](#) on page 70

Attribute Map Settings

Table 16: Attribute Mapping Settings

User Profile Attribute	SAML Attribute
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 Name Mapping	Specifies how group names from the IdP are translated, or mapped, to the corresponding group names in ExtremeCloud IQ: • Select the IdP Group, ExtremeCloud IQ Group, and Site(s) for each group name map. • Select Add a group name mapping to add a new group map row. • Select  to delete a group map. • Select  and drag the row to reorder the group mappings. The first group that the user matches the rule, in the order, the process stops. Rules are enforced top down, once a user is in the first group in a rule, the Determine what action ExtremeCloud IQ should take for users that do not match a defined group name mapping: • Deny user login. • Allow user login and assign a default user group (select a default group). Note: When defining Group Mappings for the Operator, Monitor, Help Desk, Observer, and Installer roles you must define sites to view managed devices. Administrators have global oversight, so site-specific group mappings are ignored. Sites are ignored for Guest Management accounts. However, Guest Management accounts must be added to a Credential Distribution group to view and create guest accounts.

Related Links

[Add an IdP Profile](#) on page 70

[Manage IdP Profiles](#) on page 74

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 **Manage Certificates** window for an IdP profile, you can:

- View a list of certificates associated with the IdP profile, including certificate name, expiration date, and status.
- Select a certificate to view details, including 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. From the list of IdP profiles, locate the profile you want to manage.
2. In the corresponding row, select , and then select **Manage Certificates**.
3. To deactivate a certificate, select the active certificate, and then select **Make Inactive**.
4. To add a new certificate, select **Import New Certificate**, and then select **Browse Files** to browse to your local folder and select the certificate.
5. Select **Back to IdP Profiles** to return to the **Single Sign-On Identity Provider (IdP) Profiles** window.

Related Links

[Enable Single Sign On \(SSO\)](#) on page 70

Manage IdP Profiles

Use this task to manage existing Identity Provider (IdP) profiles.

1. From the list of IdP profiles, locate the profile you want to manage.
2. In the corresponding row, select , and then select **Edit**.
3. Configure [IdP Profile Settings](#), and then select **Save**.
4. Select **ExtremeCloud (SP) Connection** to obtain the SP Metadata:
 - Select **Download SP Metadata** for IdPs that support Metadata files.
 - To manually add SP Metadata into the IdP, select  to copy the URL to your clipboard, and then paste into your IdP. Repeat this process for each URL.
 - Select **Download Certificate** to acquire the signing certificate.

Related Links

[Enable Single Sign On \(SSO\)](#) on page 70

*Manage IdP Profile Settings***Table 17: Profile Settings**

Setting	Description
Domain	The domain used by the IdP to manage and authenticate user identities.
Description	A brief summary of the IdP profile.

Table 18: IdP Connection Settings

Setting	Description
IdP Entity ID	The IdP unique identifier URL. URLs must begin with <code>https</code> .
SSO Binding	Select HTTP POST to send messages within the body of an HTTP POST request. 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 <code>https</code> .
SSO Sign Request	Select SSO Sign 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. Select HTTP POST to send messages within the body of an HTTP POST request. 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 <code>https</code> .

Table 18: IdP Connection Settings (continued)

Setting	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 <code>https</code> .
Verification Certificate	The digital certificate used to verify the authenticity and integrity of messages exchanged between the IdP and SPs. To update the verification certificate for this IdP profile, select X, and then choose an existing certificate from the drop-down list. Alternatively, select Manage IdP Profile Certificates on page 74 to import a new certificate.

Table 19: Attribute Mapping Settings

User Profile Attribute	SAML Attribute
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.

Table 19: Attribute Mapping Settings (continued)

User Profile Attribute	SAML Attribute
Group	The URL or endpoint where the IdP provides the user's group memberships.
Group Name Mapping	Specifies how group names from the IdP are translated, or mapped, to the corresponding group names in ExtremeCloud IQ: • Select the IdP Group, ExtremeCloud IQ Group, and Site(s) for each group name map. • Select Add a group name mapping to add a new group map row. • Select  to delete a group map. • Select  and drag the row to reorder the group mappings. The first group that the user matches the rule, in the order, the process stops. Rules are enforced top down, once a user is in the first group in a rule, the Determine what action ExtremeCloud IQ should take for users that do not match a defined group name mapping: • Deny user login. • Allow user login and assign a default user group (select a default group). Note: When defining Group Mappings for the Operator, Monitor, Help Desk, Observer, and Installer roles you must define sites to view managed devices. Administrators have global oversight, so site-specific group mappings are ignored. Sites are ignored for Guest Management accounts. However, Guest Management accounts must be added to a Credential Distribution group to view and create guest accounts.

Set Email Notifications

Before you can activate the switch port email notification function, you must activate **Port Status Reports** for the monitored ports. You can do this in the **Manage Devices** section.



Note

Email Notification is a legacy function. Extreme Networks recommends using Alerts. For more information, see [Manage Alerts](#) on page 509.

If you have permission, you can configure ExtremeCloud IQ to send email notifications for changes of device status. After you activate an email notification rule and save the settings, ExtremeCloud IQ automatically sends notification emails when the configured conditions are met.

For APs, ExtremeCloud IQ averages the AP status over five-minute periods (by default) to minimize unnecessary repetitions of the same notification email. For switches, ExtremeCloud IQ sends a notification email after all port up and down events.



Note

To view a graphical representation of alerts, select **Try the new Alerts Management feature**. You can also configure alert policies.

1. Hover over , and then select **Global Settings**.
2. From the **Administration** menu, select **Email Notifications**.
3. Configure the alert settings as follows:

Setting	Description
AP Status	(Not supported for WiNG devices) Toggle the setting ON to receive notifications for the selected events: Alert if Up , Alert if Down .
Hardware CPU	Toggle the setting ON to receive notification when the CPU usage of an AP is greater than 80 percent. ExtremeCloud IQ polls the AP every 60 seconds to check the CPU threshold and sends an email at a specified interval, reporting how long the AP exceeded the threshold.
Hardware Memory	Toggle the setting ON to receive notification when the memory usage of an AP exceeds a high (10.2 MB) threshold or dips below a low (10.1 MB) threshold. ExtremeCloud IQ polls APs every 60 seconds to check the memory threshold and sends an email at a specified interval, stating how long an AP exceeded the threshold.
Switch (Port) Up/Down Status	(Applicable only when an Extreme Networks Aerohive switch model SR22/23xx enables the up/down status as an alert.) Toggle the setting ON to receive notification when a switch port, with authorized email notifications configured, goes up or down.
Aerohive Port Security Violation	(Applicable only when an Extreme Networks switch enables port security violation as alert.) Toggle the setting ON to receive notification when a switch port, with authorized email notifications configured, encounters a security violation.

4. Enter the **To Email** addresses, each separated by a comma.
5. Select **SAVE SETTINGS**.

Related Links

[Alerts](#) on page 509

Manage API Access Tokens

Global Settings > API Token Management

The **API Access Tokens** window displays a table containing the following information for the API access tokens that have been added to ExtremeCloud IQ:

- **Application:** The name of the application that can use the API token, from the **My Profile** section on the developer portal
- **Access Token:** The text string of the access token
- **Grantor:** The admin who granted access to the application or who generated the access token
- **Generated On:** The date that the access token was created
- **Expiration:** The date that the access token expires in the year-month-day hour: minutes: seconds format

For tokens that are already expired, ExtremeCloud IQ replaces the date with **Expired**.

- **Refresh Token:** A token for temporary use, to provide time to obtain a new access token with a new expiration date

Use the table to view the access tokens added to ExtremeCloud IQ. You can sort the results by column. To delete an access token, select the corresponding check box, and then select .



Note

The API tokens created in ExtremeCloud IQ are only used with the legacy v1 API. For information on using the current v2 API, see [ExtremeCloud IQ API](#) and [ExtremeCloud IQ API Reference](#).

Related Links

[Generate API Access Tokens](#) on page 79

Generate API Access Tokens

Use this task to generate API access tokens that applications use to make REST API calls to ExtremeCloud IQ. For more information about API Tokens, see [Manage API Access Tokens](#) on page 78.



Note

The API tokens created here are only used with the legacy v1 API. For information on using the current v2 API, see [ExtremeCloud IQ API](#) and [ExtremeCloud IQ API Reference](#).

1. Hover over , and then select **Global Settings**.
2. From the **API** menu, select **API Token Management**.
3. Select .
4. Enter a valid **Client ID**.

The client ID is the **Credentials** value from **My Profile > Your API Developer Application** in the Extreme Networks **Developer Portal**. This step connects the token you generate with your developer account.

5. Select an **Expiration Setting** for the access token:

- **Expires in 30 days**
- **Time from enrollment**

Enter the number of days, months, or years, after which the access token expires.

- **Date**

Use the calendar control to select a specific date for the access token expiration.

6. Select **GENERATE**.

Related Links

[Manage API Access Tokens](#) on page 78

Add an API Presence and Data Location Feed

Using the presence and location API feature, Extreme Networks wireless devices can detect the presence of clients (such as smart phones) and obtain location data for all connected and unconnected clients.

Use this task to configure a Presence and Data Location feed to stream raw presence and location data from the ExtremeCloud IQ Cloud Services platform to an external server.

1. Hover over , and then select **Global Settings**.
2. From the **API** menu, select **API Data Management**.
3. Select .
4. Enter the **Post URL** for the server to receive presence and location-based services.

The Extreme Networks Cloud Services platform streams real-time presence and location data through a webhook to this URL.



Note

Because client MAC addresses and positions are being transmitted, an HTTPS connection is strongly recommended. If you use an SSL certificate, ensure that it is well known and contains the entire CA certificate chain because ExtremeCloud IQ will not connect to a server if it cannot validate its certificate.

5. Enter an access token, which is either automatically generated when you create a new application in the Develop Portal or which you manually generate (see [Generate API Access Tokens](#) on page 79).
6. Select a **Message Type**:
 - **Client-Centric** presents a single view of a client device and shows the Access Points observing it.
 - **AP-Centric** sent for each Access Point that observes client devices. If a client device is observed by multiple access points, information about the device will appear in multiple messages, one for each AP observation. This feature does not scale for customers with high density environments.
7. Select **Enable**.

8. Select **SAVE**.

Related Links

[Generate API Access Tokens](#) on page 79

[Manage API Access Tokens](#) on page 78

Add a Third-Party API Token

Use this task to add a third-party API token for applications to use to make REST API calls to ExtremeCloud IQ. For more information, see [Manage API Access Tokens](#) on page 78.

1. Hover over , and then select **Global Settings**.
2. From the **API** menu, select **3rd Party API Connections**.
3. Select an existing token, and then select , or select .
4. Type the character string for the **API Token**.
5. Select **SAVE**.

Related Links

[Manage API Access Tokens](#) on page 78

Download Logs

ExtremeCloud IQ uses logs to record and display information for the following categories:

- [GDPR Audit Log](#) on page 83
- [KDDR Logs](#) on page 83
- [Authentication Logs](#) on page 84
- [Accounting Logs](#) on page 85
- [Credential Logs](#) on page 86
- [Email Logs](#) on page 86
- [SMS Logs](#) on page 87

Audit Logs

The **Audit Logs** table contains a historical record of the administrative operations performed on ExtremeCloud IQ. The maximum page size is 500 entries per page. You can see the following information for each operation:

- **Organization:** Your network organization.
- **Timestamp:** The time when the operation was performed.
- **Category:** The type of operation.
- **Admin User:** The email address of the admin who performed the operation.
- **Description:** A description of the operation.

Sort entries by selecting any of the column headers. The **Timestamp** column sorts entries chronologically, and the other columns sort alphabetically. Select the same column header again to reverse the sorting direction.

By default, ExtremeCloud IQ displays audit logs for 24 hours.

Choose from the following actions to customize the display:

- Use the calendar controls to display logs for a specified time period, up to a maximum of 30 days history.
- Use the **Category** menu to narrow the logs list to those associated with a specific function.
- Use the Admin User drop-down list to narrow the logs list to those associated with a specific user.

Related Links

[Download Audit Logs](#) on page 82

Download Audit Logs

Administrators with full access can download the entire log or only the entries pertaining to a specific administrator, which is important for compliance with GDPR (General Data Protection Regulation). If administrators are EU citizens working in the EU, they have the right to access PII (personally identifiable information) gathered about them. This includes personal information collected by ExtremeCloud IQ and contained in the log. If an administrator leaves the company and asks for this information, you can sort for log entries pertaining to that administrator, and then download and save them in a CSV (comma-separated values) file.

Use this task to download an entire log, or only the log entries for a specific administrator.

1. Hover over , and then select **Global Settings**.
2. From the **LOGS** menu, select **Audit Logs**.
3. Select a **Category**:
 - ALL
 - ADMIN
 - SYSTEM
 - DEPLOYMENT
 - CONFIG
 - MONITOR
 - ALARM

Select **All** to display and download the logs for all categories.

4. From the **Admin User** menu, select an administrator or select **All** to display and download the logs for all administrators.
5. Select .
6. Select **OK**.

ExtremeCloud IQ generates a file in CSV format.

7. Select .

Related Links

[Audit Logs](#) on page 81

GDPR Audit Log

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.

The **GDPR Audit Log** table displays the following information about logged tasks, such as preparing client data for download, and deleting user, client, and admin data:

- **Start:** The time the process to download or delete data started.
- **End:** The time the process ended.
- **Status:** Whether the process is currently in progress, completed, or failed.
- **Log ID:** The download or deletion process ID number.
- **Category:** The task type.
- **MAC:** The MAC address of the client.
- **Admin:** The admin who initiated the data download or deletion.
- **Description:** A descriptive note about the task status.

Related Links

[Download the GDPR Audit Log](#) on page 83

Download the GDPR Audit Log

Use this task to download the GDPR audit log.

1. Hover over , and then select **Global Settings**.
2. From the **LOGS** menu, select **GDPR Audit Log**.
3. Select  **DOWNLOAD**.

Related Links

[GDPR Audit Log](#) on page 83

KDDR Logs

Kernel Diagnostic Data Recorder (KDDR) logs record failures or interruptions of ongoing processes. The KDDR log format is binary. Generally these logs are for more advanced troubleshooting. Extreme Networks support might ask for these logs for troubleshooting unexplained reboots or crashes.

You can view the following information:

- **File Name:** The KDDR log file name.
- **Size:** The KDDR log file size.
- **Timestamp:** The time the unexpected event occurred.
- **Device Name:** The device where the unexpected event occurred.
- **Device MAC:** The MAC address of the device.

Related Links

[Download KDDR Logs](#) on page 84

Download KDDR Logs

Use this task to download KDDR logs.

1. Hover over , and then select **Global Settings**.
2. From the **LOGS** menu, select **KDDR Logs**.
3. Select a file name link to download a KDDR log.

Related Links

[KDDR Logs](#) on page 83

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.

The table displays the following information about successful network authentication attempts:

- **Auth Status:** The status of the authentication.
- **User Name:** The name of the cloud-based PPSK or RADIUS user, or the email address of a user authenticating through a cloud-hosted captive web portal.
- **SSID:** The SSID associated with this authentication.
- **Auth Type:** The method of authentication:
 - Private PSK
 - Enterprise (for RADIUS)
 - One of the social log in options: Google, LinkedIn



Note

To remove an existing login button that has already been deployed, you must resave the CWP and the Network Policy, and then redeploy the respective network policy to the device.

- PIN
- **Client Device:** The MAC address of the authenticated client device.

- **Reject Reason:** The reason why an authentication attempt failed.
- **NAS Device:** The MAC address of the AP running guest management and serving as the network portal.
- **NAS Identifier:** The network name for the NAS device
- **Auth Date:** The date of the authentication attempt.

**Note**

These entries are not real-time, but are historical records showing when individuals were authenticated. Entries are automatically deleted after seven days.

Related Links

[Download Authentication Logs](#) on page 85

Download Authentication Logs

Use this task to download authentication logs.

1. Hover over , and then select **Global Settings**.
2. From the **LOGS** menu, select **Authentication Logs**.
3. Select  **DOWNLOAD**.

Related Links

[Authentication Logs](#) on page 84

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.

The table displays the following information about cloud-based PPSK and RADIUS user sessions on your network:

- **Start Time:** The session start time.
- **Stop Time:** The session end time.
- **Session Time:** The session duration.
- **User Name:** The cloud-based PPSK or RADIUS user name
- **Client Device:** The MAC address of the device.
- **SSID:** The SSID over which this session was conducted.
- **Usage:** The amount of data transmitted during the session.
- **NAS Device:** The MAC address of the Extreme Networks AP client.
- **NAS Identifier:** The host name of the Extreme Networks AP.

Related Links

[Download Accounting Logs](#) on page 86

Download Accounting Logs

Use this task to download accounting logs.

1. Hover over , and then select **Global Settings**.
2. From the **LOGS** menu, select **Accounting Logs**.
3. Select  **DOWNLOAD**.

Related Links

[Accounting Logs](#) on page 85

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.

The table displays the following credentials information:

- **Time Expired:** The time that the credentials expired.
- **User Name:** The user name associated with the expired credentials.

Related Links

[Download Credential Logs](#) on page 86

Download Credential Logs

How to download credential logs.

1. Hover over , and then select **Global Settings**.
2. From the **LOGS** menu, select **Credential Logs**.
3. Select  **DOWNLOAD**.

Related Links

[Credential Logs](#) on page 86

Email Logs

The **Email Logs** table displays information about email notifications to users who requested network access. ExtremeCloud IQ creates email log entries for the following events:

- When an email message is sent to a visitor
- When an email message is sent for employee approval
- When an administrator approves user credentials

To filter the display, use the **Start**, **End**, and **Time** controls at the top of the page. You can also search for email messages sent to a specific address by using the **Search** field above the table.

The table displays the following information:

- **Time Sent:** The time the SMS was sent.
- **User Name:** The user name associated with the sent credentials.
- **Approver Email:** The email address of the approving employee.
- **Status:** Whether or not approval is required for the visitor.

Related Links

[Download Email Logs](#) on page 87

Download Email Logs

Use this task to download email logs.

1. Hover over , and then select **Global Settings**.
2. From the **LOGS** menu, select **Email Logs**.
3. Select  **DOWNLOAD**.

Related Links

[Email Logs](#) on page 86

SMS Logs

The **SMS Logs** table displays information about SMS notifications sent to users who request network access. ExtremeCloud IQ creates SMS log entries for the following events:

- SMS notifications sent to visitors.
- User credentials approved by an administrator.

To filter the display, use the **Start**, **End**, and **Time** controls at the top of the page. You can also search for SMS messages sent to a specific phone number in the **Search** field above the table.

The table displays the following information:

- **Time Sent:** The time the SMS was sent.
- **Phone Number:** The text message phone number.
- **Status:** The SMS message transmission status.

Related Links

[Download SMS Logs](#) on page 87

Download SMS Logs

Use this task to download SMS logs.

1. Hover over , and then select **Global Settings**.
2. From the **LOGS** menu, select **SMS Logs**.
3. Select  **DOWNLOAD**.

Related Links

[SMS Logs](#) on page 87

Enable SSH Availability

ExtremeCloud IQ provides a way to access devices remotely using the SSH protocol. Because best practices suggest that SSH access to internal devices be blocked from external access, ExtremeCloud IQ uses an SSH proxy server to mediate the end-to-end connection between an external device that manages files on your client device.

**Note**

Enabling SSH Availability potentially gives others direct access to your devices during the time that 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, because SSH FTP assumes that it is run over a secure channel.

Use this task to enable SSH Availability.

1. Hover over , and then select **Global Settings**.
2. From **Administration** menu, select **VIQ Management**.
3. Toggle the **SSH Availability** setting **ON**.

Navigate to **Manage > Devices > host_name > Additional Device Settings > SSH**, select the length of time during which you want to make SSH available, and then select **Enable SSH**. ExtremeCloud IQ then creates an SSH session for the specified length of time between the SSH proxy server and the external device.

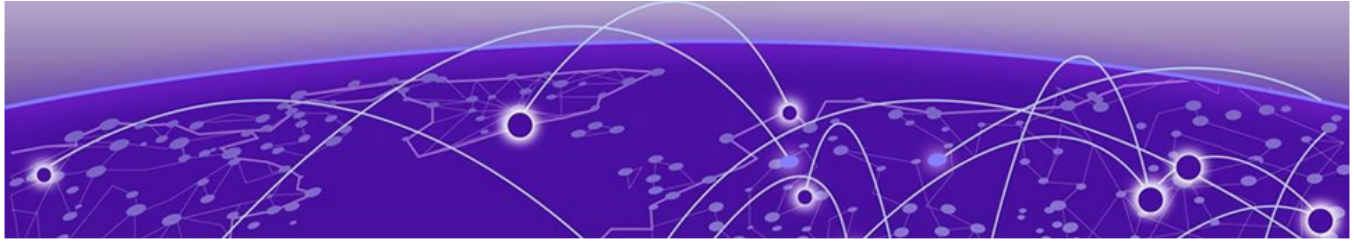
Enable Supplemental CLI

Use this task to enable supplemental CLI for ExtremeCloud IQ.

1. Hover over , and then select **Global Settings**.
2. From the **Administration** menu, select **VIQ Management**.
3. Toggle the **Supplemental CLI** setting **ON**.

Related Links

[Configure Supplemental CLI](#) on page 302



Configure Users

- [Add a User](#) on page 90
- [Bulk Create Users](#) on page 92
- [Add a User Group](#) on page 93
- [Add a User to a User Group](#) on page 98
- [Bulk Add Users to a User Group](#) on page 98
- [Configure a Private Client Group](#) on page 98
- [Unlock Users](#) on page 99
- [Perform a RADIUS Test](#) on page 99
- [Unbind a Device](#) on page 100

After you complete **Onboarding**, your ExtremeCloud IQ system is ready for daily use.

Add users and assign them to user groups to manage which SSIDs they access, what their access limitations are, and how they access your network. Administrators and operators can configure user groups with limited access privileges for VIPs and non-employees such as guests, visitors, and contractors who request network access.

Create user groups for a selected network policy or for all network policies. Add users before you create user groups, or add them when you create the user group.

On the **Configure > User Management > Users** page, you can view, add, sort, select, modify, and delete user groups and user accounts.



Note

For existing user groups, some settings are not available to edit. This limitation prevents issues with creating passwords. To modify these settings, you must create a new user group.

You can also create and assign Private Pre-Shared Key (PPSK) users for use in private client groups.

For information about user profiles, see [Add a User Profile](#) on page 281.

Related Links

- [Onboarding](#) on page 22
- [Add a User Profile](#) on page 281

Add a User

You must first create the user group to which you want to assign the user.

Use this task to add a new user and assign an existing user group.



Note

You cannot edit the user group for an existing user.

1. Go to **Configure > User Management > Users**.
2. Select **+** and then configure the settings.
See [User Settings](#) on page 90.
3. Select **SAVE**.

Related Links

[User Settings](#) on page 90

User Settings

Table 20: Settings for new user accounts

Setting	Description
Create account in user group	(Required) Select a user group from the menu.
Name	Type the name of the user. 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> . Note: Required only if you select Name from the User Name menu.
Organization	Type the name of the organization for the user. For permanent users, leave this field empty.
Purpose of Visit	Type the purpose of the user's visit. For permanent users, leave this field empty.
Email Address	Type the user's email address. Note: Required only if you select Name from the User Name menu.

Table 20: Settings for new user accounts (continued)

Setting	Description
Phone Number	Type the user's phone number, and use the menu to set the international dialing code. Note: Required only if you select Phone Number from the User Name menu.
User Name	From the menu, select a field to use as the User Name. Choose from the following options: • Name • Email Address • Phone Number • Other If you select Other, type a user name for the account. Example: jsmith
Password	(Required) Type a password, or select Generate to automatically generate a password for the user. To see the password, select Show Password. Note: For either method, the password must conform to the password rules configured for the associated user group.
Description	(Optional) Type a description for the user account.
VLAN Override	Specify a VLAN ID to override the default VLAN assignment for the user. When configured, the user traffic is placed on the specified VLAN instead of the VLAN assigned by the user group or network policy.
Deliver Password	Select a password delivery method: • Email Address 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. • Text Message 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 90

[Add a User Group](#) on page 93

[Add a User to a User Group](#) on page 98

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 **Configure > User Management > Users**.
2. Select **Bulk Create** and configure the settings.
See [Bulk Create Settings](#) on page 92.
3. Select **SAVE**

Related Links

[Bulk Create Settings](#) on page 92

[Add a User Group](#) on page 93

Bulk Create Settings

Table 21: 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. 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 to send the user credentials.

Related Links

[Bulk Create Users](#) on page 92

[Bulk Add Users to a User Group](#) on page 98

Add a User Group

Administrators and operators can configure ExtremeCloud IQ user groups with limited access privileges for VIPs and non-employees such as guests, visitors, and contractors who request network access.



Note

For existing user groups, some settings are not available to edit. This limitation prevents issues with creating passwords. To modify these settings, you must create a new user group.

- In the **User Groups** section of a Wireless Network (SSID) when you want to store them in the ExtremeCloud IQ Authentication Service cloud database.
- In **Configure > User Management > User Groups > Add** and then reference them in AAA server profiles that you apply to APs configured as RADIUS servers when you want to store users there. See [RADIUS Authentication](#) on page 144.

ExtremeCloud IQ supports user groups for Private Pre-Shared Key (PPSK) users and RADIUS users. Configure PPSK user groups in the **User Groups** section of a Wireless Network (SSID). Configure RADIUS user groups in one of two places in ExtremeCloud IQ, depending on where you intend to store the RADIUS users:

Use this task to create user groups for a selected network policy or for all network policies.

1. Go to **Configure > User Management > User Groups**.

2. Select **+**, and then configure the settings.

For a cloud-based user group, see [Cloud User Group Settings](#) on page 93.

For a local user group, see [Local User Group Settings](#) on page 95.

3. Select **SAVE**.

Related Links

[RADIUS Authentication](#) on page 144

[Cloud User Group Settings](#) on page 93

[Local User Group Settings](#) on page 95

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 22: 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.

Table 22: Settings for Cloud User Groups (continued)

Setting	Description
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. Available only if a captive web portal is enabled for this SSID.
PCG Use	(Optional) Available only for the PPSK password type. Select Enable use for Private Client Group .
Password Settings	
Generate Password Using	(Required) 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: • All selected character types • Any selected character types • Only one character type
PSK Generation Method	Available only for the PPSK password type. 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. 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 Use this string to generate PPSKs as User name + Character String + Password. For example, if you enter <code>Extreme</code> , as the string, then the generated PPSKs are <code><User name>Extreme<Password></code> .
Expiration Settings	

Table 22: Settings for Cloud User Groups (continued)

Setting	Description
Account Expiration	Select one of the options from the menu: • Never Expire • Valid During Dates Use the calendar and time controls to specify the Start and End dates and times. • Valid For Time Period 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. 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. • Daily Use the Start and End controls to specify the daily time period.
Action at Expiration	Not available for accounts set to never expire. Select Access Rejected to have ExtremeCloud IQ block users from renewing their credentials. Select Show Expiration Message to have ExtremeCloud IQ 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: • Text Messages (SMS) • Email Use the menus to select an email template for each method.

Related Links

[Add a User Group](#) on page 93

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 local on all SSID APs. The following settings are available when you configure a local-based user group.

Table 23: 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. 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. 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). Range: 0-15, 0 = no limit
PCG Use	(Optional) Available only for the PPSK password type. Select Enable use for Private Client Group .
PPSK Classification Use	(Optional) Available only for the PPSK password type. Select Enable user for PPSK Classification only to create a single SSID and distribute unique guest passwords for each location. Use this option with a Private Pre-Shared Key SSID Authentication network policy. See Configure Private Pre-Shared Key SSID Authentication on page 123 for more information.
Password Settings	
Generate Password Using	(Required) 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: • All selected character types • Any selected character types • Only one character type

Table 23: Settings for Local User Groups (continued)

Setting	Description
PSK Generation Method	Available only for the PPSK password type. 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. 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 Use this string to generate PPSKs as User name + Character String + Password. For example, if you enter <code>Extreme</code> , as the string, then the generated PPSKs are <code><User name>Extreme<Password></code> .
Expiration Settings	
Require Authentication After	To force re-authentication after a session is inactive for a period of time, select Require Authentication After and enter a time in the minutes field.
Account Expiration	Select an option from the menu: • Never Expire • Valid During Dates (Available only for PPSK.) 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. Select Access Rejected to have ExtremeCloud IQ block users from renewing their credentials. Select Show Expiration Message to have ExtremeCloud IQ 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: • Text Messages (SMS) • Email Use the menus to select an email template for each method.

Related Links

[Add a User Group](#) on page 93

Add a User to a User Group

You must first create the associated user group.

Use this task to add a single user by editing an existing user group.

1. Go to **Configure > User Management > User Groups**.
2. Select an existing user group, and then select , or select .
3. Expand the **Add Users** section.
4. Select  and then configure the settings.
See [User Settings](#) on page 90.
5. Select **DONE**.

Related Links

[User Settings](#) on page 90

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 **Configure > User Management > User Groups**.
2. Expand the **Add Users** section.
3. Select **Bulk Create** and configure the settings.
See [Bulk Create Settings](#) on page 92.
4. Select **DONE**.

ExtremeCloud IQ 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.

If you are configuring a network policy, continue with that configuration.

Related Links

[Bulk Create Settings](#) on page 92

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 123.

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 **Configure > User Management > Private Client Groups**.
2. Select a **Network Policy** from the menu.
3. 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**.

4. Select **+** to add rooms for AP-based groups, or users for key-based groups.
5. 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.

Alternately, for key-based groups, you can bulk add users by selecting **IMPORT** and uploading a CSV file.

6. Repeat steps 4–5 until you finish adding groups or users.
7. Select **SAVE CHANGES**.

Related Links

[Configure Private Pre-Shared Key SSID Authentication](#) on page 123

Unlock Users

ExtremeCloud IQ 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 **Configure > User Management > Locked Users**.
2. Select entries in the locked users list.
3. 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 **Configure > User Management > RADIUS Test**.
2. 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.
3. 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.
4. 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.
5. Select **Test**.

Results appear under **Test Result**. A successful test result is shown below.

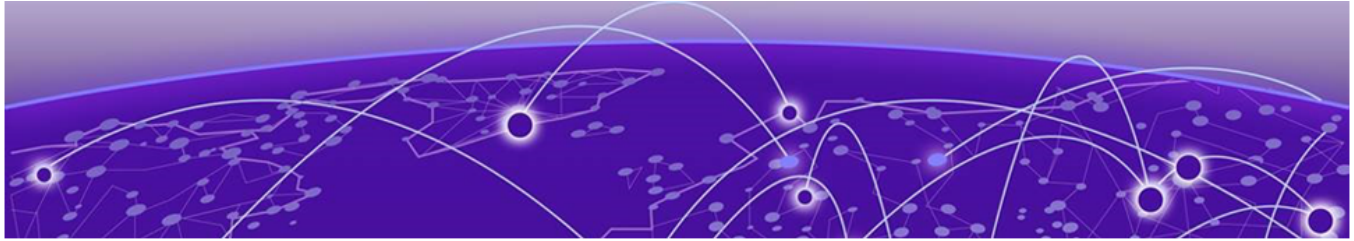
RADIUS server is reachable. Get attributes from RADIUS server: User-Group-ID:0=13; VLAN-ID:1=1; Session-Timeout=1800

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 **Configure > User Management > Unbind Device**.
2. Select the method for unbinding from the drop-down list.

Choose **MAC address**, **PPSK**, or **MAC address and PPSK**.
3. Enter the MAC address, the PPSK, or both.
4. Select **Unbind**.



Configuration—Network Policies

- [Add a Network Policy](#) on page 102
- [Configure Policy Settings](#) on page 103
- [Deploy a Network Policy](#) on page 113
- [Configure the SSID for a Standard Wireless Network](#) on page 113
- [Configure Device Templates](#) on page 171
- [Configure Classification Rules for a Device Template](#) on page 171
- [Fabric Attach](#) on page 174
- [Configure Device Data Collection and Monitoring Options](#) on page 175
- [Configure the BLE Service](#) on page 177
- [Configure Presence Analytics](#) on page 180
- [Configure WIPS](#) on page 180
- [Configure a Location Server](#) on page 181
- [Install CA Certificates](#) on page 181
- [Configure a Layer 2 IPsec VPN Service](#) on page 182
- [Router Settings](#) on page 182

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 any 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), **SR/Dell Switching** (Legacy switches), **Branch Routing**, or any combination of these. See [Configure Policy Settings](#) on page 103.
- **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.

- [Router Settings](#): Define wired or wired and wireless router templates, assign port usage settings, and specify authentication.
- [Deploy Policy](#): Push the configuration to your network devices.

**Note**

The assigned **Access Scope** determines an administrator's access to **Common Objects**. Administrators not assigned global access can only see and work with policy objects created for the sites to which they are assigned. For more information about this assignment, see [Account Management Settings](#) on page 58.

Related Links

[Add a Network Policy](#) on page 102

[Configure Policy Settings](#) on page 103

[Configure the SSID for a Standard Wireless Network](#) on page 113

[Configure a RADIUS Server Group](#) on page 145

[Configure Device Templates](#) on page 171

[Router Settings](#) on page 182

[Deploy a Network Policy](#) on page 113

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 ExtremeCloud IQ. Switches do not use CAPWAP connections. Extreme Networks routers and APs run IQ Engine and communicate with ExtremeCloud IQ using CAPWAP on UDP port 12222 or CAPWAP-over-HTTP on TCP port 80. This is true whether they communicate with ExtremeCloud IQ on premises or in the cloud. Other supported devices communicate with ExtremeCloud IQ using HTTPS on TCP port 443.

The network policy configuration process is defined by sequential workflow tabs at the top of the page. Depending on where you are in the process, the related tab appears blue. These tabs are 1 Policy Details, 2 Wireless, 3 Switching, 4 SR/Dell Switching, 5 Branch Routing, and 6 Deploy Policy.

Use this task to add a new network policy.

1. Go to **Configure > Network Policies**.

Network policies appear 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 any 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 103, 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 113.

Related Links

[Configure Policy Settings](#) on page 103

[Configure the SSID for a Standard Wireless Network](#) on page 113

[Configure Device Templates](#) on page 171

[Deploy a Network Policy](#) on page 113

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 **Configure > Network Policies**.
2. Select an existing network policy, and then select , or select  to create a new policy.
3. Configure the **Policy Settings**.
 - a. [Configure DNS Server Policy Settings](#) on page 104.
 - b. [Configure NTP Server Policy Settings](#) on page 105.
 - c. [Configure SNMP Server Policy Settings](#) on page 106.
 - d. [Configure Syslog Server Policy Settings](#) on page 107.
 - e. [Configure Device Credentials Policy Settings](#) on page 108.
 - f. [Configure the Device Time Zone](#) on page 109.
 - g. [Configure HIVE Policy Settings](#) on page 109.
 - h. [Configure Management and Native VLAN Policy Settings](#) on page 109.

- i. [Configure IP Tracking Policy Settings](#) on page 110.
- j. [Configure LLDP/CDP Policy Settings](#) on page 111.

**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 111.
 - b. [Configure Traffic Filters Policy Settings](#) on page 112.
 - c. [Configure MGT IP Filter Policy Settings](#) on page 112.
5. Select **SAVE**.
6. Select **Policy**, and then select **NEXT**.

Related Links

[Configure Classification Rules for a Device Template](#) on page 171

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 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.

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 on UDP port 53.

Use this task to configure **DNS Server Policy Settings** for a network policy.

1. Go to **Configure > Network Policies**.
2. Select an existing network policy, and then select , or 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 321.
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**.
9. Select **SAVE DNS SERVER**.

Related Links

[DNS Server Settings](#) on page 321

[Configure Policy Settings](#) on page 103

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 and related services and to ensure alerts and events have the correct timestamp.

Out of the box, and 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 will automatically attempt 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.



Note

If using a Windows server as your NTP server, your Windows server must in turn synchronize with an upstream NTP server for Extreme Networks APs to trust and accept responses from the Windows NTP server.

1. Go to **Configure > Network Policies**.
2. Select an existing network policy, and then select , or select  to create a new policy.

3. From the **Policy Settings** menu, select **NTP Server**.
4. Toggle the **NTP Server** setting to **ON**.
5. (Optional) To use existing NTP server settings, choose an NTP object from the  menu.
6. Configure [NTP Server Settings](#) on page 322.
7. To add a new NTP server to the list, select .
 - a. To use an existing NTP server, select it from the  menu.
 - b. To add a new NTP server, select , and then select **IP Address** or **Host Name**.
 - c. Type a **Name** for the new IP object.
 - d. (Optional) If you want to change your previous selection, select **IP Address** or **Host Name** from the menu.
 - e. Select **SAVE IP OBJECT**.
 - f. Select **ADD**.

ExtremeCloud IQ accesses NTP servers in order, from the top down. Use the up and down arrows to rearrange them if necessary.

8. If you want to use classification, select **Apply NTP servers to devices via classification**.
9. Select **SAVE NTP SERVER**.

Related Links

[NTP Server Settings](#) on page 322

[Configure Policy Settings](#) on page 103

Configure SNMP Server Policy Settings

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 **Configure > Network Policies**.
2. Select an existing network policy, and then select , or select  to create a new policy.
3. From the **Policy Settings** menu, select **SNMP Server**.
4. Toggle the **SNMP Server** setting to **ON**.
5. (Optional) To use existing SNMP server settings, choose an SNMP server from the  menu.
6. Configure the [SNMP Server Settings](#) on page 324.
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.
10. (Optional) If you want to change your previous selection, select **IP Address** or **Host Name** from the menu.
11. Select **SAVE IP OBJECT**.

12. Select the version of SNMP that is running on the management station you intend to use from the **Version** menu.
13. 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.
 - **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.
14. 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.
15. Select **ADD SNMP SERVER**.
16. If you want to use classification, select **Apply SNMP servers to devices via classification**.
17. Select **SAVE SNMP SERVER**.

Related Links

[SNMP Server Settings](#) on page 324

[Configure Policy Settings](#) on page 103

Configure Syslog Server Policy Settings

This task is part of the network policy configuration workflow. Use this task to configure **Syslog Server Policy Settings** for a network policy.

1. Go to **Configure > Network Policies**.
2. Select an existing network policy, and then select , or select  to create a new policy.
3. From the **Policy Settings** menu, select **Syslog Server**.
4. Toggle the **Syslog Server** setting to **ON**.
5. (Optional) To use existing syslog server settings, choose a syslog server from the  menu.
6. Configure the [Syslog Server Settings](#) on page 326.
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 an existing syslog IP Address or host name from the  menu, or select .
9. For **Severity**, select the log level.
10. Type the **Port** number.
11. Select **ADD**.

12. (Optional) Select **Assign Syslog servers via Classification**.
13. Select **SAVE SYSLOG SERVER**.

Related Links

[Syslog Server Settings](#) on page 326

[Configure Policy Settings](#) on page 103

Configure Device Credentials Policy Settings

ExtremeCloud IQ 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 **Configure > Network Policies**.
2. Select an existing network policy, and then select , or select  to create a new policy.
3. From the **Policy Settings** menu, select **Device Credentials**.
4. Configure the following settings:

Table 24: 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 103

Configure the Device Time Zone

This task is part of the network policy configuration workflow. Use this task to configure **Device Time Zone** for a network policy.

1. Go to **Configure > Network Policies**.
2. Select an existing network policy, and then select , or select  to create a new policy.
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 103

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 **Configure > Network Policies**.
2. Select an existing network policy, and then select , or 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 218.
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 103

[HIVE Profile Settings](#) on page 218

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 **Configure > Network Policies**.
2. Select an existing network policy, and then select , or select  to create a new policy.
3. From the **Policy Settings** menu, select **Management and Native VLAN**.

4. Select an **MGT Interface VLAN** from the  menu, or 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. If you want to use classification, select **Apply VLANs to devices using classification**.
See [Configure Classification Rules](#) on page 214.
6. Select an **Native (Untagged) VLAN** *For IQ Engine devices only* from the  menu, or 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. If you want to use classification, select **Apply VLANs to devices using classification**.
See [Configure Classification Rules](#) on page 214.
8. Select **SAVE VLAN**.

Related Links

[Configure Classification Rules](#) on page 214

[Configure Policy Settings](#) on page 103

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 **Configure > Network Policies**.
2. Select an existing network policy, and then select , or 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 332.
7. Select **SAVE**.

Related Links

[IP Tracking Group Settings](#) on page 332

[Configure Policy Settings](#) on page 103

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. In IQ Engine, LLDP was previously off by default. 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. Select an existing network policy, and then select , or select  to create a new policy.
2. From the **Policy Settings** menu, select **LLDP/CDP**.
3. Toggle the **LLDP/CDP** setting to **ON**.
4. (Optional) To use existing LLDP/CDP settings, choose an LLDP/CDP object from the  menu.
5. Configure the settings.
See [LLDP and CDP Settings](#) on page 330.

Related Links

[Configure Policy Settings](#) on page 103

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 **Configure > Network Policies**.
2. Select an existing network policy, and then select , or 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 342.
9. Select **SAVE**.

Related Links

[Management Options](#) on page 342

[Configure Policy Settings](#) on page 103

Configure Traffic Filters Policy Settings

After you enable **Traffic Filter** in the network policy, you can re-use 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 **Configure > Network Policies**.
2. Select an existing network policy, and then select , or select  to create a new policy.
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 select an existing filter from the  menu.
6. Configure the [Traffic Filter Settings](#) on page 308.
7. Select **SAVE**.

Related Links

[Traffic Filter Settings](#) on page 308

[Configure Policy Settings](#) on page 103

Configure MGT IP Filter Policy Settings

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 **Configure > Network Policies**.
2. Select an existing network policy, and then select , or select  to create a new policy.
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 306.
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 306.
8. Select **SAVE MGT IP FILTER**.

Related Links

[MGT IP Filter Settings](#) on page 306

[Configure Policy Settings](#) on page 103

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 pushes all configuration uploads as complete uploads. This 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 **Configure > Network Policies**.
2. Select an existing policy, and then select , or 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.
6. Select **Enable Distributed Image Upgrade** when WAN speed and traffic usage are concerns.

When ExtremeCloud IQ updates the IQ Engine firmware for multiple, same-model APs, it can send the first upgrade to one device and enable the other devices using the same firmware to get their image from that first updated (seed) device.

7. Select **PERFORM UPDATE**.

Related Links

[Configuration—Network Policies](#) on page 101

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 **Configure > Network Policies**.
2. Select an existing network policy, and then select , or 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 214

**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 from the  menu, or select .
6. Type a **Name** for the wireless network SSID.

ExtremeCloud IQ 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 Wi-Fi2 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 25: 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 119. - 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 120. - 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 123. - 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. - 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. 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 126.

10. 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 26: 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.

Table 26: Protected Management Frames Settings (continued)

Setting	Description
Use 802.11w protection for broadcasts/multicasts	If you select WPA2 level of security, 802.11w is disabled by default, with option to enable.
Enable Beacon Protection	Enhances Wi-Fi security by safeguarding beacon frames against tampering. Note: Enable Beacon Protection is supported on AP4020/AP5020 only.

11. To enable Multi-Link Operation (MLO), turn on **Enable MLO**. See [Settings for Multi-Link Operation](#) on page 170.
12. To create a captive web portal for open authentication, see:
 - [Customize and Preview Cloud-based Captive Portal Settings](#) on page 135
 - [Customize and Preview Device-based Captive Web Portal Settings](#) on page 128
 - [Import Captive Web Portal HTML Files](#) on page 136
13. 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 146 to add a wireless network (SSID)-specific RADIUS object. See [Configure an External RADIUS Server](#) on page 148 to add an external RADIUS common object.

To use classification, select **Apply RADIUS server groups to devices via classification**.

14. If you intend to authenticate via user groups (Enterprise only), turn on **Authentication with ExtremeCloud IQ Authentication Service**.
15. If you intend to use Zero Trust Network Access (ZTNA), turn on **Authentication with ExtremeCloud Universal ZTNA**.

**Note**

Authentication with ExtremeCloud IQ Authentication Service and **Authentication with ExtremeCloud Universal ZTNA** are mutually exclusive settings.

16. Either select an existing User group from the current list or select **+** to [Add a User Group](#) on page 93.
17. Use the existing **Default User Profile**, select a profile from the list, or select **+** to [Add a User Profile](#) on page 281.
18. (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 158.
19. To customize the **SSID Availability Schedule**, select the **Restrict the availability of this SSID to selected schedules** check box to enable SSID schedules.

20. Select **Customize**.

To create a new schedule, see [Configure an Availability Schedule | User Profile](#) on page 285.

21. To customize **Advanced Access Security Controls**, see [Customize Advanced Access Security Controls](#) on page 159.

22. To customize **Optional Settings** (not available for 6 GHz), see [Customize Wireless Network Optional Settings](#) on page 162.

23. Toggle **Client Monitor ON** (default) to enable a device to detect client issues, and report client connection activities and problems to ExtremeCloud IQ.

24. Toggle **Client Monitor ON** (default) to

25. Select **SAVE**.

Continue configuring the network policy.

Related Links

[Configure Classification Rules for a Device Template](#) on page 171

[Configure Enterprise SSID Authentication](#) on page 119

[Configure Personal SSID Authentication](#) on page 120

[Configure Private Pre-Shared Key SSID Authentication](#) on page 123

[Customize and Preview Device-based Captive Web Portal Settings](#) on page 128

[Import Captive Web Portal HTML Files](#) on page 136

[Configure MAC Authentication](#) on page 126

[Configure RADIUS Server Settings](#) on page 146

[Configure an External RADIUS Server](#) on page 148

[Add a User Group](#) on page 93

[Add a User Profile](#) on page 281

[Apply Different User Profiles to Clients and User Groups](#) on page 158

[Configure an Availability Schedule | User Profile](#) on page 285

[Customize Advanced Access Security Controls](#) on page 159

[Customize Wireless Network Optional Settings](#) on page 162

[Configure the SSID for a Standard Wireless Network](#) on page 113

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 113.

To view a list of configured SSIDs, go to **Configure > Network Policies**, 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 113

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 119.
- **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 120.
- **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 123.
- **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 are allowed to 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 126.

Related Links

[Configure the SSID for a Standard Wireless Network](#) on page 113

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 113.

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, or WBA Open Roaming.
IQ Engine v10.7.4 is required. For more information, see [Configure a Hotspot](#) on page 138 or [Configure WBA Open Roaming](#) on page 144.
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. 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).

6. Toggle **Transition Mode if Applicable** on.

802.11w settings might have been changed. See [Customize Advanced Access Security Controls](#) on page 159 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, so Protected Management Frames will be set to Mandatory.

For more information, see [Transition Mode Overview](#) on page 122.

7. Select **SAVE**.

Related Links

[Configure the SSID for a Standard Wireless Network](#) on page 113

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 113.

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 122.

3. 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 (Wi-Fi 7 Only)** checkbox to ensure compatibility and compliance with 802.11be.



Note

Applies only to AP4020, AP4060, and AP5020 devices.

4. 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 supports TKIP only for AP3000, AP3000X, AP4000, AP5010, AP5050D, AP5050U models.

5. Select an **SAE Group**.

6. 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 122.

7. For **Key Value**, enter the pre-shared key and **Confirm** it.

The **Key Type** is **ASCII Key**.

8. (Optional) To show the **Key Value**, select **Show Password**.
9. Select **SAVE**.

Related Links

[Configure the SSID for a Standard Wireless Network](#) on page 113

Transition Mode Overview

Transition Mode eases the transition for an organization from WPA2 to WPA3 Wi-Fi security. This mode connects newer client hardware with the latest security standards, while still allowing 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 available 802.11w setting available, so Protected Management Frames will be 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 information element in the open network's 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 27: 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 113

[Configure Enterprise SSID Authentication](#) on page 119

[Configure Personal SSID Authentication](#) on page 120

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 113.

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 125.

5. Select **PPSK Classification Options** to use this network policy with the associated local user groups.

See [Add a User Group](#) on page 93 for more information.

**Note**

It is not recommended practice to mix cloud and local PPSK user groups in the same SSID.

Related Links

[Configure Private Client Group Options](#) on page 125

[Add a User Group](#) on page 93

[Configure the SSID for a Standard Wireless Network](#) on page 113

Configure Private Client Group Options

First, [Configure Private Pre-Shared Key SSID Authentication](#) on page 123.

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 123

[Configure a Private Client Group](#) on page 98

[Configure the SSID for a Standard Wireless Network](#) on page 113

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.

1. Go to **Configure > 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 113.

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  to add a RADIUS Server Group, or select  and then select an existing RADIUS Server Group.

For more information, see [Configure an AAA Server Profile](#) on page 150

Continue configuring a standard wireless network.

Related Links

[Configure an AAA Server Profile](#) on page 150

Configure a Client Mode AP Profile using a Wired Connection and a Device Template

There must be at least one client mode profile configured before you can define a LAN-side AP radio for client mode. See [Configure a Client Mode Profile](#) on page 289.

You can set a radio on some AP models to client mode, which allows 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 **Configure > Network Policies**.
2. Select an existing network policy, and then select , or 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 118.

Related Links

[Configure a Client Mode Profile](#) on page 289

[SSID Usage in Standard Wireless Networks](#) on page 118

Captive Web Portals

Extreme Networks supports two types of captive web portal (CWP):

- AP hosted portals on built-in web servers
- Extreme Networks hosted portals on cloud web servers

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 CWP also has a simpler set of configuration options.

After defining a CWP, you must take one of two actions for your changes to take effect:

- For an AP hosted CWP, upload the configuration, web page files, and certificates (for secure communications using HTTPS) to your devices.
- For a cloud-based CWP, upload the configuration to your devices. ExtremeCloud IQ 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 CWP and the Network Policy, and then redeploy the respective network policy to the device.

ExtremeCloud IQ can include multiple CWPs.

Related Links

[Customize and Preview Cloud-based Captive Portal Settings](#) on page 135

[Customize and Preview Device-based Captive Web Portal Settings](#) on page 128

[Import Captive Web Portal HTML Files](#) on page 136

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 **Configure > Network Policies**.
2. Select an existing policy with open access security, and then select , or select .
3. On the **Wireless** tab, select an existing SSID, and then select , or select .
4. In the **SSID Usage** section, toggle the **Enable Captive Web Portal** setting **ON**.
5. Select **Captive Web Portal**, and then select the features.

Table 28: 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. 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.

6. Select **SELECT** to use an existing CWP, or select **ADD**.
7. Enter a **Name** for the CWP.

8. If you selected **Return Aerohive Private PSK**, configure the **PPSK Settings**.

Table 29: 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.

9. Select **CUSTOMIZE AND PREVIEW > CUSTOMIZATION AND PREVIEW**.
Alternately, you can import HTML files. See [Import Captive Web Portal HTML Files](#) on page 136.
10. [Preview and Customize the Landing Page](#) on page 133.
11. [Preview and Customize the Use Policy Acceptance Page](#) on page 134.
12. [Preview and Customize the Success Page](#) on page 134.
13. [Preview and Customize the Error Page](#) on page 134.
14. Enable or disable the **Success Page**.
15. Enable or disable **Redirect clients after a successful login attempt**.
When enabled, ExtremeCloud IQ sends successful clients to either the login page or to a specified URL.
16. Enable or disable the **Failure Page**, and choose the page to display the failure message.
When enabled, ExtremeCloud IQ displays the failure message on either the login page or the standard failure page. See [Preview and Customize the Error Page](#) on page 134.
17. Enable or disable **Redirect clients after a failed login attempt**.
When enabled, ExtremeCloud IQ sends unsuccessful clients to either the login page or to a specified URL.
18. Configure the default language, and additional languages.

Table 30: 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 adds the files required for the selected languages to the default CWP directory when you save the CWP.

19. Expand the **Advanced Configuration** section, and configure the settings.

Table 31: Advanced configuration settings

Setting	Description
Session Timer	Select Display session timer alert before session expires to display the session timer in the client browser. 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. Select Customize to enter an IPv4 address and netmask for each of the interfaces.
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. Select + to add a new VLAN ID.
DHCP and DNS servers > Use Extreme Network Devices	
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 CWP. 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. 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. 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.

Table 31: Advanced configuration settings (continued)

Setting	Description
Renewal Response	From the menu, choose how you want the AP to respond to a DHCP lease renewal request for a nonexistent lease. • 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. • 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. • 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	
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. 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 CWP uses for HTTPS. The domain name must be a valid domain name that a DNS server can resolve to the IP address of the interface hosting the CWP. This option allows you to use a server certificate from a CA that supports domain names as CNs, but not IP addresses. 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 <code>cwp.aerohive.com</code> 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	

Table 31: Advanced configuration settings (continued)

Setting	Description
Enable HTTPs	Select Enable HTTPs to enable HTTPS on the CWP.
HTTPS certificate	Select Default-CWPCert.pem for preloaded CWPs. The AP hosting the CWP then uses HTTPS to secure traffic between the client and its CWP server. The certificate file must have the following properties: • The file format must be PEM (Privacy Enhanced Mail). • It must contain a server private key stored in an unencrypted format. • 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	
Use HTTP 302	Select Use HTTP 302 to redirect code as the redirection method instead of JavaScript. 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 CWP 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 CWP displays the failure page before initiating the redirection. Type a value in seconds. 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.

20.To create a walled garden, select , and configure the settings.

Table 32: Walled garden settings

Setting	Description
Service Type	Select one of the following options: • Web: Permit client access only to the World Wide Web. • All: Permit client access to the World Wide Web and all other servers. • Advanced: Permit client access only to the admin-defined IP object or host name. If you selected Web or All, paste IP addresses or host names separated by commas into the Service Type text box. Then select ADD. 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.
Protocol Number	(Protocol service only) Type a protocol number (from 0 to 255).
Port	(Protocol service only) Type a port number to define the type of service you want to permit.

21. 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 136

[Configure the SSID for a Standard Wireless Network](#) on page 113

Preview and Customize the Landing Page

This task is part of the [Customize and Preview Device-based Captive Web Portal Settings](#) on page 128 task. 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 134.

Related Links

[Customize and Preview Device-based Captive Web Portal Settings](#) on page 128
[Preview and Customize the Use Policy Acceptance Page](#) on page 134

Preview and Customize the Use Policy Acceptance Page

This task is part of the [Customize and Preview Device-based Captive Web Portal Settings](#) on page 128 task. 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 134

Related Links

[Customize and Preview Device-based Captive Web Portal Settings](#) on page 128
[Preview and Customize the Success Page](#) on page 134

Preview and Customize the Success Page

This task is part of the [Customize and Preview Device-based Captive Web Portal Settings](#) on page 128 task. 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 134.

Related Links

[Customize and Preview Device-based Captive Web Portal Settings](#) on page 128
[Preview and Customize the Error Page](#) on page 134

Preview and Customize the Error Page

This task is part of the [Customize and Preview Device-based Captive Web Portal Settings](#) on page 128 task. 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 128

Customize and Preview Cloud-based Captive Portal Settings

To configure a cloud-based captive web portal (CWP), you must first create a wireless network SSID with **Open** access security. For more information, see [Captive Web Portals](#) on page 127.

Extreme Networks provides two types of cloud-hosted CWPs. 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. Both CWP types are available in ExtremeCloud IQ and ExtremeCloud IQ Connect.

This task is part of the network policy configuration workflow. Use this task to configure a cloud-based CWP.

1. Go to **Configure > Network Policies**.
2. Select an existing policy with open access security, and then select , or select .
3. On the **Wireless** tab, select an existing SSID, and then select , or 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 sends a randomly generated PIN to authenticate the user.

7. Select an existing CWP or select **ADD**.
 - a. If you selected **ADD**, enter a new **Name** for the CWP.
 - b. Enter the length of time that the PIN remains valid.

The validity period begins when ExtremeCloud IQ receives the PIN request and can last from 1 to 24 hours.
 - c. Enter an email address where you want ExtremeCloud IQ to send daily reports about successfully authenticated users on this CWP.

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 sends a separate email for when there are no entries to report.
 - d. Set the hour and minute when ExtremeCloud IQ generates a daily report of successful user authentications.

ExtremeCloud IQ reports the time in UTC, and the report contains events for the previous 24 hours.
 - e. Use the default CWP 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.

**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.

8. Select **Use a different captive web portal for various clients** to use other CWPs 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 171.

Return to the Wireless Network page to complete the network policy configuration.

Related Links

[Configure Classification Rules for a Device Template](#) on page 171

[Configure the SSID for a Standard Wireless Network](#) on page 113

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 **Configure > Network Policies**.
2. Select an existing policy, and then select , or select .
3. On the **Wireless** tab, select an existing SSID, and then select , or 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 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.

Return to the **Wireless Network** page to complete the network policy configuration.

Related Links

[Configure the SSID for a Standard Wireless Network](#) on page 113

Hotspot

ExtremeCloud IQ 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 138

[Hotspot WBA OpenRoaming](#) on page 143

Configure a Hotspot

IQ Engine v10.7.5 or later is required.



Note

AP3000, AP4020, AP5010, AP5020, 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 139.
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 140.
6. On the **Network Characteristics** tab, configure the settings.
For more information, see [Network Characteristics](#) on page 142.
7. Select **SAVE**.

Related Links

[Hotspot Settings](#) on page 139

Hotspot Settings

- [Hotspot Identification](#)
- [Service Provider Identification](#) on page 140
- [Network Characteristics](#) on page 142

Hotspot Identification

On the **Hotspot Identification** tab, configure the settings to uniquely identify the hotspot and specify the languages for the venue.

Table 33: Hotspot Identification settings

Setting	Description
Name	(Required) Type a name for the hotspot.
HESSID	Type the Homogenous Extended Service Set Identifier (HESSID) for the Hotspot 2.0 network. 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) Type the Fully-Qualified Domain Name (FQDN) for the Hotspot 2.0 network. (Default: empty string) 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.
Venue Info	Describe the venue. From the lists of predefined values, first select the category of the venue, and then select the subtype. Example: Institutional, Hospital Select  , configure the settings, and then select ADD .
Operator Name	(Required) Type the name of the venue operator.
Venue Name	(Required) Type the name of the venue.
Language	(Required) 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. For more information, see [Configure a Hotspot Service Provider Profile](#) on page 221.



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 34: 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. • 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. • Add a realm for the PLMN ID. This is the cellular network identity based on public land mobile network (PLMN) information. Select + and configure the settings.	
Realm	(Required) Type the Fully-Qualified Domain Name (FQDN) of the service provider. Wildcards are supported for realm. For example, you can enter *.extreme.area120.com, instead of entering specific realms.
EAP Method	From the list, select the Extensible Authentication Protocol (EAP) authentication type. 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. Although optional, descriptions can be helpful when you are 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. Select +, configure the settings for the Roaming Consortium, and then select ADD.	

Table 34: Service Provider Profile Settings (continued)

Setting	Description
Consortium	(Required) Type the Roaming Consortium Organization Identifier (RCOI). Specify up to eight identifiers unique to the organization that are part of the MAC address.
Description	Type a description for the consortium. Although optional, descriptions can be helpful when you are 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. Select  , configure the settings for a 3rd Generation Partnership Project (3GPP) mobile network, and then select ADD .	
MCC	(Required) Type the mobile country code (MCC).
MNC	(Required) Type the mobile network code (MNC).
Description	Type a description for the 3GPP mobile network. Although optional, descriptions can be helpful when you are troubleshooting your network.
Advanced Settings	Select the arrow to expand this section and configure the following settings: • NAI Realm • Roaming Consortium • 3GPP CellularNetwork 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 35: Network Characteristics settings

Setting	Description
Access Network: From the list, select the type of access network: • Private network—An enterprise network with user accounts. • Private network with guest access—An enterprise network providing guest access. • Chargeable public network—(Default) Open to anyone but access requires payment. • 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: • Not Available • Public • Port Restricted • Single NAT • Double NAT • Port Restricted Single NAT • Port Restricted Double NAT • Unknown
IPv6	From the list, select the type of IPv6 address: • Not Available • Available • 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 . 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 35: Network Characteristics settings (continued)

Setting	Description
Port Number	Type the port number.
Status	From the list, select a status. (Open, Closed, or Unknown)

Related Links

[Configure a Hotspot](#) on page 138

[Configure a Hotspot Profile](#) on page 221

[Configure a Hotspot Service Provider Profile](#) on page 221

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 3: 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.

Related Links

[Configure WBA Open Roaming](#) on page 144

[Hotspot](#) on page 137

Configure WBA Open Roaming

First, obtain the CA, CERT, and KEY files from your Access Network Provider (ANP), and import them into ExtremeCloud IQ. 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 375. 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 119.
2. For **Hotspot** (in the SSID configuration) select **WBA Open Roaming**.
3. In the **WBA OpenRoaming Configuration** dialog configure the settings:

Table 36: 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 143

[Hotspot](#) on page 137

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 via Supplemental CLI.

Related Links

[Configure a RADIUS Server Group](#) on page 145

[Configure RADIUS Server Settings](#) on page 146

[Configure an External RADIUS Server](#) on page 148

[Configure an Extreme Networks RADIUS Server](#) on page 149

[Configure a RADIUS Proxy Server Realm](#) on page 154

[Configure an Extreme Networks RADIUS Server](#) on page 149

[Add an Active Directory Server](#) on page 152

[Add an LDAP Server](#) on page 153

[Add a User Group](#) on page 93

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 configure a RADIUS server group for an SSID, as part of a network policy.

1. Go to **Configure > Network Policies**.
2. Select an existing policy, and then select , or 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. Select an existing RADIUS sever group from the  menu, or select .
6. Type a **RADIUS Server Group Name**.
7. (Optional) Type a **RADIUS Server Group Description**.

Although optional, entering a description is helpful for troubleshooting and for identifying the RADIUS server group.

8. Configure the RADIUS server settings for IQ Engine devices.

See [Configure RADIUS Server Settings](#) on page 146.

9. 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 148
EXTREME NETWORKS A3	Configure an Extreme Networks A3 Server on page 149
EXTREME NETWORKS RADIUS SERVER	Configure an Extreme Networks RADIUS Server on page 149
EXTREME NETWORKS RADIUS PROXY	Configure an Extreme Networks RADIUS Proxy on page 154

Select up to four existing servers to add to your wireless network (SSID) RADIUS server group.

10. 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 146

Configure RADIUS Server Settings

First begin configuring a RADIUS server group. See [Configure a RADIUS Server Group](#) on page 145.

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. Range: 60–100000000 (seconds) Default: 600 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. Range: 10–100000000 (seconds) Default: 600 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. 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. Select Aggressive or Custom (Range 1-5) . Set the First retry interval . (Default: 1) Set the Max-retries value, which is the maximum number of 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 145

Configure an External RADIUS Server

First begin configuring a RADIUS server group. See [Configure a RADIUS Server Group](#) on page 145.

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 server, or select .
3. Type a **Name** for the server.
4. (Optional) Type a **Description** for the server.
5. Select the **IP/Host Name** for the server.

If you do not see the IP address that you need, select  to define a new one (IPv4 or IPv6).

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.

6. For **Server Type**, choose the RADIUS server role:
 - **Authentication:** As an authentication server, the RADIUS service requests that the client device demonstrate its identity.
 - **Port:** Set the RADIUS authentication port.
 - **Accounting:** As an accounting server, the RADIUS service tracks client-server session details.
 - **Port:** Set the RADIUS accounting port number.
7. Type the **Shared Secret** for authenticating communications with the RADIUS server.
8. (Optional) Select **Show Password**.
9. Select **SAVE EXTERNAL RADIUS**.

Finish configuring the RADIUS server group.

Related Links

[Configure a RADIUS Server Group](#) on page 145

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 145.

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 145

Configure an Extreme Networks RADIUS Server

First begin configuring a RADIUS server group. See [Configure a RADIUS Server Group](#) on page 145.

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 150.

Related Links

[Configure an AAA Server Profile](#) on page 150

Configure an AAA Server Profile

First, configure an Extreme Networks RADIUS Server. See [Configure an Extreme Networks RADIUS Server](#) on page 149.

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 an existing user group from the  menu.
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 152.
LDAP Server	See Add an LDAP Server on page 153.
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 151.
17. Select **Approved RADIUS Clients**, and then [Add Approved RADIUS Clients](#) on page 155.
18. Select **SAVE RADIUS SERVER**.

Continue configuring the RADIUS server profile.

Related Links

[Configure an Extreme Networks RADIUS Server](#) on page 149
[Add an Active Directory Server](#) on page 152
[Add an LDAP Server](#) on page 153
[Configure AAA Server Security Options](#) on page 151
[Add Approved RADIUS Clients](#) on page 155

Configure AAA Server Security Options

Configure an Extreme Networks device as a RADIUS Server.

Use this task to add increased security to the AAA Server Profile. For more information, see [Configure an AAA Server Profile](#) on page 150.



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 150.

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, select an existing AD server from the  menu, or 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 automatically populates the Active Directory Server and the base distinguished name (BaseDN) parameters. Go to Step 9 on page 153.
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 150

Add an LDAP Server

First, configure an AAA server profile. See [Configure an AAA Server Profile](#) on page 150.

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, select an existing LDAP server from the  menu, or select **+**.
2. Configure the settings.
See [LDAP Server Settings](#) on page 369

Continue configuring the RADIUS server.

Related Links

[LDAP Server Settings](#) on page 369
[Configure an AAA Server Profile](#) on page 150

Configure an Extreme Networks RADIUS Proxy

First begin configuring a RADIUS server group. See [Configure a RADIUS Server Group](#) on page 145.

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, entering a description is helpful for troubleshooting and for identifying the proxy server.
5. For the **Realms** section, see [Configure a RADIUS Proxy Server Realm](#) on page 154.
6. For the **Approved RADIUS Clients** section, see [Add Approved RADIUS Clients](#) on page 155.
7. For the **Realm Settings** section, see [Configure Realm Settings](#) on page 156.
8. Select **SAVE RADIUS PROXY**.

Related Links

[Configure a RADIUS Server Group](#) on page 145
[Configure a RADIUS Proxy Server Realm](#) on page 154
[Add Approved RADIUS Clients](#) on page 155
[Configure Realm Settings](#) on page 156

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 154.

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 145.
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 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 154

[Configure a RADIUS Server Group](#) on page 145

Add Approved RADIUS Clients

Configure an Extreme Networks device as a RADIUS proxy server. See [Configure an Extreme Networks RADIUS Proxy](#) on page 154.

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. Select an existing **IP/Host Name/Network** for a client, from the  menu, or 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 156.

Related Links

[Configure an Extreme Networks RADIUS Proxy](#) on page 154

[Configure Realm Settings](#) on page 156

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 154
- [Configure a RADIUS Proxy Server Realm](#) on page 154

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 154

[Configure a RADIUS Proxy Server Realm](#) on page 154

Configure VLAN Settings

This task is part of configuring an SSID. Use this task to set the default user profile and configure the VLAN settings.

1. Go to **Configure > Network Policies**.
2. Select an existing network policy, and then select , or select .
3. After you save the **Policy Details**, select **NEXT** or **2 Wireless**.
4. Select an existing SSID and then select , or select .

5. Scroll to **User Access Settings**, select the **Default User Profile**, and configure the settings.
 - To edit the selected **Default User Profile**, select the link and configure the settings.

Typically, the default VLAN is 1.



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.

- To choose a new default user profile, select one from the  menu.
- To create a new user profile, select .

Table 37: User profile settings

Setting	Description
User Profile Name	Type a User Profile Name .
Connect to	a. Select VLAN or VLAN Group . b. Select an existing VLAN object from the  menu, or select  . For more information, see VLAN Object Settings on page 158 and VLAN Group Object Settings on page 158. To edit an existing VLAN object, select it and then select  .
SECURITY	See Configure Security User Profile on page 282.
TRAFFIC TUNNELING	See Configure User Profile Traffic Tunneling on page 283.
QOS	See Configure QoS User Profile on page 284.
AVAILABILITY SCHEDULE	See Configure an Availability Schedule User Profile on page 285.
CLIENT SLA	See Configure Client SLA User Profile on page 286.
DATA/TIME LIMIT	See Configure Access Restrictions User Profile on page 287.

6. Select **SAVE USER PROFILE**.

Continue the SSID configuration.

Related Links

[Add a User Profile](#) on page 281

[VLAN Group Object Settings](#) on page 158

[Configure Classification Rules for a Device Template](#) on page 171

VLAN Object Settings

Configure the following settings, and then select **SAVE VLAN**.

Table 38: Settings for VLANs

Setting	Definition
Name	(Required) Type a name for the new VLAN.
VLAN ID	(Required) 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.

VLAN Group Object Settings

VLAN groups combine multiple VLANs as a single common object. Configure the following settings, and then select **SAVE**.

Table 39: Settings for VLAN group objects

Setting	Definition
Name	(Required) Type a name for the new VLAN group object.
VLANs	(Required) Specify individual VLANs or ranges. Indicate a range with a hyphen. Separate VLAN entries with commas, for example, 1-30, 100-200, 500. Range: 1–4094
Description	(Optional) Type a description to identify the VLAN group. Although optional, descriptions can be helpful when you are troubleshooting your network.

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 113.

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 **Configure > Network Policies**.
 2. Select an existing policy, and then select , or 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. Select  to choose an existing user profile, or select  to add a new profile.
 6. To add an existing user profile assignment rule, select .
 - a. Select one of the existing rules.
 - b. Select **Link**.
 7. To add a new user profile assignment rule, select .
 - a. Type a **Name** for the user profile assignment rule.
 - b. (Optional) Type a description.
 - c. Select  and choose a category.
 - d. Complete the configuration for the selected category.
See [Configure Classification Rules](#) on page 214.
- 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 113
[Configure Classification Rules](#) on page 214

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 **Configure > Network Policies**.
2. Select an existing policy, and then select , or select .
3. After you save the **Policy Details**, select **NEXT** or **2 Wireless**.
4. Select an existing SSID, and then select , or 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 40: 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. 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 EAPOL-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. 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.
GTK Timeout Period	Type the time interval (in Milliseconds) that the device waits for client replies during the handshake process. 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). If you enable PTK rekeying, an interval between 2 and 10 minutes (120 and 600 seconds) is the best practice recommendation, which is short enough to thwart the known TKIP exploit. Enable this option only if you know that the clients using the SSID support it. In addition, you might need to configure PTK rekeying on the clients. 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.

Table 40: Settings for Advanced Access Security Controls (continued)

Setting	Description
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. 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. 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.
Local TKIP Countermeasure	(Available only when the encryption method is Auto-TKIP or CCMP (AES) or TKIP) Select to enable the deauthentication of all clients when the local device detects message integrity check failures during TKIP operations. 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) Select to deauthenticate all previously authenticated clients when a client reports MIC failures during TKIP operations. The distinction between the local and remote countermeasure options is where the discovery occurs: • Local—A device discovered the failure. • 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 102 task.

When you configure 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 **Configure > Network Policies**.
2. Select an existing policy, and then select , or 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 162.
6. [Customize DoS Prevention](#) on page 163.
7. [Customize Traffic Filters](#) on page 164.
8. [Customize the User Profile Application Sequence](#) on page 164.
9. [Customize Voice Enterprise Options](#) on page 165.
10. [Customize Wi-Fi Multimedia™](#) on page 166.
11. [Customize Broadcast and Multicast Handling Settings](#) on page 167.
12. [Customize Client Related Network Settings](#) on page 168.
13. [Customize Other Options](#) on page 169.
14. Select **SAVE OPTIONAL SETTINGS**.

Continue configuring the wireless network policy.

Customize Radios and Rates Settings

Complete the [Add a Network Policy](#) on page 102 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 **Configure > 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 configuring **Optional Settings** in the **Wireless Networks** configuration window. Select **SAVE OPTIONAL SETTINGS** to save your changes.

Related Links

[Add a Network Policy](#) on page 102

[Customize Wireless Network Optional Settings](#) on page 162

Customize DoS Prevention

Complete the [Add a Network Policy](#) on page 102 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 **Configure > 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 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 configuring **Optional Settings** in the **Wireless Networks** configuration window. Select **SAVE OPTIONAL SETTINGS** to save your changes.

Related Links

[Add a Network Policy](#) on page 102

[Customize Wireless Network Optional Settings](#) on page 162

Customize Traffic Filters

Complete the [Add a Network Policy](#) on page 102 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 **Configure > 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 configuring **Optional Settings** in the **Wireless Networks** configuration window. Select **SAVE OPTIONAL SETTINGS** to save your changes.

Related Links

[Add a Network Policy](#) on page 102

[Customize Wireless Network Optional Settings](#) on page 162

Customize the User Profile Application Sequence

Complete the [Add a Network Policy](#) on page 102 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 that have different components in the SSID referencing different user profiles.

1. Go to **Configure > 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 configuring **Optional Settings** in the **Wireless Networks** configuration window. Select **SAVE OPTIONAL SETTINGS** to save your changes.

Related Links

[Add a Network Policy](#) on page 102

[Customize Wireless Network Optional Settings](#) on page 162

Customize Voice Enterprise Options

Complete the [Add a Network Policy](#) on page 102 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 **Configure > 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 102

[Customize Wireless Network Optional Settings](#) on page 162

Customize Wi-Fi Multimedia™

Complete the [Add a Network Policy](#) on page 102 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 **Configure > 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 configuring **Optional Settings** in the **Wireless Networks** configuration window. Select **SAVE OPTIONAL SETTINGS** to save your changes.

Related Links

[Add a Network Policy](#) on page 102

[Customize Wireless Network Optional Settings](#) on page 162

Customize Broadcast and Multicast Handling Settings

Complete the [Add a Network Policy](#) on page 102 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 **Configure > 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 configuring **Optional Settings** in the **Wireless Networks** configuration window. Select **SAVE OPTIONAL SETTINGS** to save your changes.

Related Links

[Add a Network Policy](#) on page 102

[Customize Wireless Network Optional Settings](#) on page 162

Customize Client Related Network Settings

Complete the [Add a Network Policy](#) on page 102 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 **Configure > 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 configuring **Optional Settings** in the **Wireless Networks** configuration window. Select **SAVE OPTIONAL SETTINGS** to save your changes.

Related Links

[Add a Network Policy](#) on page 102

[Customize Wireless Network Optional Settings](#) on page 162

Customize Other Options

Complete the [Add a Network Policy](#) on page 102 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 **Configure > 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 enables this feature by default. If you turn off 6 GHz radio, ExtremeCloud IQ disables this feature.
9. Select **SAVE OPTIONAL SETTINGS** to save your changes.

Finish configuring the network policy.

Related Links

[Add a Network Policy](#) on page 102

[Customize Wireless Network Optional Settings](#) on page 162

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 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 be enabled simultaneously

Configure Device Templates

Create a network policy.

A device template allows you 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 specific device template, you can:

- assign various port types to the device ports, then apply this device template and its 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 200.
2. To add a switch template to the network policy, select **3 Switching** in the workflow and proceed to [Configure Switch Templates](#) on page 244.
For legacy and Dell switch models, select **4 SR/Dell Switching** in the workflow.
3. To add a branch router template to the network policy, select the **5 Branch Routing** step in the workflow and proceed to [Configure a Router Template](#) on page 184.

Continue configuring the network policy.

Related Links

[Configure AP Templates](#) on page 200

[Configure Switch Templates](#) on page 244

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 supports multiple classification rules for DNS servers, VLANs, RADIUS servers, device templates, user groups, and private client groups (PCGs).

- 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.

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 **Configure > Network Policies**.
2. Select an existing policy, and then select , or select .
3. After you save the **Policy Details**, select **NEXT** or **2 Wireless**.
4. From the **Configuration Settings** menu, select **AP Template**.
5. From the  menu, select the desired default template.

Default templates apply to all of the devices of the selected template type, which 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, in the main AP template window. The **Classification Rules** column for the template contains the controls for configuring classification rules.
9. To assign an existing classification rule, in the **Classification Rules** column, select .
 - a. Select an existing classification rule.
 - b. Select **Link**.
10. To create and assign a new classification rule, in the **Classification Rules** column, select .
 - a. Type a **Name** for the rule.
 - b. Type a **Description**.

Although optional, entering a description is helpful for troubleshooting and for identifying the rule.

- c. Select , and then select the rule type to configure.
Choose from the following rule types:

Table 41: Rule types

Selected rule type	Do this
Device Location	- Drill down until you reach the location level at which the device resides. - Select Select. The location appears in the Classification Rules table.
Cloud Config Group	- Select the Match Type. - Select an existing group from the  menu, or select . For more information, see Add a Cloud Config Group on page 217. - Select CLOUD CONFIG GROUP. - Select CONTINUE.
IP Address	- From the Match Type menu, select Contains or Does Not Contain. - Select , or select an existing IP address from the  menu. If you do not see the IP address that you want, select New to create a new IP address. - Select SAVE IP. - Select CONTINUE.
IP Subnet	- From the Match Type menu, select Contains or Does Not Contain. - Select , or select an existing IP subnet from the  menu. If you do not see the IP subnet that you want, select New to create a new IP subnet. - Select SAVE SUBNET. - Select CONTINUE.
IP Range	- From the Match Type menu, select Contains or Does Not Contain. - Select , or select an existing IP range from the  menu. If you do not see the IP range that you want, select New to create a new IP range. - Select SAVE IP. - Select CONTINUE.

11. 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 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.
12. Select **SAVE RULE**.

Related Links

[Add a Cloud Config Group](#) on page 217

[Configure the SSID for a Standard Wireless Network](#) on page 113

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 APs support the following functions:

- Discover the Fabric Attach Server upon start up.
- 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.
- 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 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 174

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 174.

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 **Configure > Network Policies**.
2. Select an existing network policy, and then select , or 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. Select  next to the **Fabric Attach** field.
Alternately, select an existing profile from the menu. To edit the selected profile, select . See [Configure a Fabric Attach Profile](#) on page 217.
7. Type a **Name** for the new profile.
8. (Optional) Type a description for the new profile.
Although optional, entering a description is helpful for troubleshooting and for identifying the profile.
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 174

[Configure a Fabric Attach Profile](#) on page 217

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 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 **Configure > Network Policies**.
 2. Select an existing policy, and then select , or 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**:

- Enable **RADIUS Authentication** to create synthetic traffic.
- 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.

- Adjust the check **Interval** if necessary.

Related Links

[Configure the SSID for a Standard Wireless Network](#) on page 113

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 **Configure > Network Policies**.
2. Select an existing policy, and then select , or 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 42: 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. 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. The default value is 60 seconds.
Batch Reporting (Required for Generic BLE scan)		Toggle ON to submit iBeacon reports in batch files. 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 42: 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. (String, valid URL format, max 255 characters)

9. Configure the **iBeacon Filter** settings (iBeacon Filter only).

Table 43: iBeacon Filter settings

Setting		Description
	Min RSS(dBm)	The minimum Received Signal Strength (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. 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 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 44: 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	
	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 .

11. Select **Save**.

Related Links

[Configure the SSID for a Standard Wireless Network](#) on page 113

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.

1. Go to **Configure > Network Policies**.
2. Select an existing policy, and then select , or 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**.
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 period of time that aggregation will occur for the presence profile.

Related Links

[Configure the SSID for a Standard Wireless Network](#) on page 113

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 **Configure > Network Policies**.
2. Select an existing network policy, and then select , or 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 309.

To reuse WIPS settings, choose a WIPS policy object from the  menu.

6. Select **SAVE**.

Related Links

[WIPS Policy Settings](#) on page 309

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 **Configure > Network Policies**.
2. Select an existing network policy, and then select , or 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 choose an existing location server from the  menu.

Table 45: Location server settings

Setting	Description
Name	(Required) 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.
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: • Extreme Networks Location Server • AeroScout Location Server • Tazmen Sniffer Protocol (Ekahau, etc...)

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 **Configure > Network Policies**.
2. Select an existing network policy, and then select , or 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  to open the **Certificate Management** page. For more information, see [Certificate Configuration](#) on page 370.

Related Links

[Certificate Configuration](#) on page 370

Configure a Layer 2 IPsec VPN Service

First configure a VPN service. See [Configure VPN Services](#) on page 365.

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.

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 **Configure > Network Policies**.
2. Select an existing network policy, and then select , or 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 the **Layer 2 IPsec VPN Service** setting **ON**.
6. Select an existing service from the  menu, or select .
7. Configure the [Layer 2 VPN Services Settings](#) on page 333.

Related Links

[Configure VPN Services](#) on page 365

[Layer 2 VPN Services Settings](#) on page 333

Router Settings

As part of a network policy that applies to multiple devices, you can configure the following router settings:

Network Allocation

You can add or import subnetwork allocations, and allocate VLANs to subnetwork spaces defining management, internal, and guest networks. When ExtremeCloud IQ uploads the network policy to routers with these VLANs assigned to their Ethernet ports, it also assigns the subnetwork space to those ports.

Router Templates

A router template is a diagram of the physical ports for a specific Extreme Networks router model. Use the template to assign port types to the device ports, which defines the function of the ports.

VPN Service

Layer 3 IPsec VPN tunnels securely send traffic between Extreme Networks routers and one or two Extreme Networks VGVAs (VPN Gateway Virtual Appliances).

ExtremeCloud IQ applies Layer 3 IPsec VPNs to routers and Layer 3 VPN gateways through a network policy that supports routing.

SD-WAN

Enable SD-WAN to configure policies that make routing decisions based on Layer 7 application service sets, user profiles, incoming LAN interfaces, or source and destination addresses. An SD-WAN route group is a list of prioritized WAN ports that you can use as a forwarding action in a routing policy.

Routing Policy

Use policy-based routing to assign route priorities to traffic based on various factors, including Layer 7 application service sets, user profiles, incoming LAN interfaces, and source and destination addresses. There are three general configurations for policy-based routing: split tunnel, tunnel all, and custom. When routing is enabled in the network policy and SD-WAN is disabled, you can use any of these routing policy types. When both routing and SD-WAN are enabled, you can only define custom routing rules.

URL Filtering

Some routers support HTTP URL filtering rules, which define URL filtering by allowed list, blocked list, and category, and can be assigned to one or more user profiles.

Firewall

A network firewall policy is a set of up to 2048 rules that a router uses to permit or deny traffic to and from the networks it controls. For more information, see [Configure a Firewall Policy](#) on page 364.

Dynamic DNS

The DNS translates human-friendly domain names into IP addresses. You can supply external DNS server IP addresses or use Extreme Networks routers to provide proxy DNS services for every local network under their control.

WAN Tracking

Configure one or two WAN tracking destination IP addresses in a network policy so that routers can send probe packets to the destination IPs to check WAN availability.

Configure Network and IP Address Allocation

Create a **Network Policy** and select **5 Branch Routing** in the workflow.

You can allocate VLANs to subnetwork spaces, defining management, internal, and guest networks. When ExtremeCloud IQ uploads the network policy to routers with these VLANs assigned to their Ethernet ports, it also assigns the subnetwork space to those ports.

This task is part of the network policy configuration workflow. Use this task to configure network and IP address allocation settings for a network policy.

1. Go to **Configure > Network Policies**.
2. Select an existing network policy, and then select , or select .

3. After you save the **Policy Details**, select **5 Branch Routing**.
4. From the **Router Settings** menu, select **Network Allocation**.
5. In the **Network Allocation** section, select  to create a new VLAN-to-subnetwork mapping.
Alternately, select **Import** to use a CSV file.
6. Choose a VLAN from the corresponding  menu, or select **New** to define one.
To add a VLAN, see [Configure VLAN Settings](#) on page 156.
7. Choose an existing subnetwork from the corresponding  menu, or select **New** to define one.
To add a subnetwork, see [Add a Subnetwork Space](#) on page 360.
8. To map a VLAN to more than one subnetwork, select , and then either choose an existing subnetwork or define a new one.
This action is helpful if your deployment expands beyond your original estimates and you must add a new subnetwork for the additional branch sites. By keeping the VLAN the same, you maintain the same user profile-to-VLAN relationship in your existing configuration, regardless of differing IP address spaces. ExtremeCloud IQ assigns address scopes to branch sites from the next subnetwork after it uses all of those from the previous one.
9. Select **SAVE**.
10. In the **IP Allocation** section, select  to configure IP allocation settings.
11. Select a **Branch ID** for the router from the corresponding  menu.
12. Select the **Serial Number** of this device from the corresponding  menu.
ExtremeCloud IQ automatically displays the host name for the router.
13. Select a subnet entry from the corresponding  menu.
14. Continue to configure **BRANCH ROUTING** settings, or select **NEXT** to apply the network policy.

Related Links

[Router Settings](#) on page 182

Configure a Router Template

A router template is a diagram of the physical ports for a specific Extreme Networks router model. Use router templates to assign port types to the device ports. A port type defines how the ports assigned to it will function. You can add one or more templates for the router models to which the network policy applies. To use more than one template for the same router model, you must use classification rules to distinguish which template to apply, to which device. You can select a previously defined template to use as is, or copy it and modify the settings in the copy to customize it for a particular policy. When you modify a device template that is used in multiple network policies, your changes are applied to that template everywhere. If you do not want to change the template in other network policies, make a copy, save it with a different name, and modify the new template for use in a single policy.

This task is part of the network policy configuration workflow. Use this task to configure a router template.

1. Go to **Configure > Network Policies**.
2. Select an existing network policy, and then select , or select .
3. After you save the **Policy Details**, select **5 Branch Routing**.
4. From the **Router Settings** menu, select **Device Template**.
5. Select  and choose the appropriate device template for the device model.
6. Type a **Template Name** for the template.
7. In the device template, assign ports with the connection types that you want them to provide: access, 802.1Q, and WAN.
8. To assign an existing port type:
 - a. Highlight one or more ports in the router template, and then select **Assign > Choose Existing**.
 - b. Select the type you want for the selected port or ports:
 - **Access port**: for a port connected to an individual host
 - **WAN port**: for a port connected to the WAN
 - **Trunk port**: for a port connected to a forwarding device such as an AP and switch that supports multiple VLANs
9. To create a new port type, select **Assign > Create New** and configure the following in the **New Port Type** section:
 - a. Type a port type name.
 - b. Type an optional description.
 - c. Toggle the **Port Status ON** to enable the port, or **OFF** to disable it.
 - d. For **Port Usage**, select **Access Port** for ports connected to individual hosts, **Trunk Port** (802.1Q VLAN Tagging) for ports providing network access through forwarding devices such as APs and switches that support multiple VLANs, or **WAN Port** for a port acting as a backup WAN interface.
 - e. Configure parameters for the port type you selected.

10. For **Access Port**:

- a. For **Port Usage Settings**, select one of four possibilities for authentication:
 - **No user authentication and no MAC authentication.** This is the default and is common for sites where you know all connections will come from trusted devices so no authentication is necessary. An employee home offices is one example.
 - **User authentication for clients with a RADIUS supplicant running on them but no MAC authentication.** Use this option to authenticate users before allowing network access, if you know that permitted devices will have a RADIUS supplicant running on them, and if your infrastructure is set up for RADIUS user authentication.
 - **MAC authentication for clients without a RADIUS supplicant but no user authentication.** Use this option to control network access when you know that permitted devices connecting to the port will not have a RADIUS supplicant and your RADIUS infrastructure is set up to authenticate them by MAC address.
 - **User authentication for clients with a RADIUS supplicant or MAC authentication for clients without.** This option is useful for situations where you cannot know in advance if a device connected to the access port will have a RADIUS supplicant, perhaps when users at different branch sites connect devices with different RADIUS capabilities to the port.
- b. For **Wired Connectivity**, Toggle **OFF** to enable clients to connect to the port without requiring user authentication, and **ON** to enable user authentication through EAP/802.1X and RADIUS.
- c. Configure a default RADIUS server group and, if you want different APs to use different RADIUS servers based on their location, select **Apply RADIUS server groups to devices via classification** and select or configure additional RADIUS server groups.

See [Configure RADIUS Server Settings](#) on page 146 for more information about RADIUS server settings.

- d. For **MAC Authentication**, toggle **OFF** to allow clients to connect to the port without requiring MAC authentication, and **ON** to enable device authentication using the MAC address as both user name and password.

When a client without a RADIUS supplicant connects, the RADIUS server tries MAC authentication, also referred to as MAB (MAC authentication bypass).

- e. For **Authentication Protocol**, choose **PAP** (Password Authentication Protocol), **CHAP** (Challenge Handshake Authentication Protocol), or **MS CHAP V2** (Microsoft CHAP Version 2), depending on which protocol the RADIUS authentication server supports.

If you are using an Extreme Networks RADIUS server, use the default choice: **PAP**. For an external RADIUS authentication server, choose the protocol that it supports. The Extreme Networks device functioning as the RADIUS authenticator uses the chosen protocol to authenticate communications between itself and the RADIUS server when submitting client credentials (MAC address) for authentication.

If you already enabled **User Authentication** on the **Wired Connectivity** tab and configured one or more RADIUS server groups for it, those servers will also perform MAC authentication. If you enable only MAC authentication on the access port, then you must define a default RADIUS server group and optionally other groups via classification.

- f. For **Multiple Clients**, select **Allow multiple clients connected to the same port on the same VLAN**.

Only the first device needs to authenticate successfully for all others to connect as well.

- g. For **Primary authentication using**, when both **Wired Connectivity** and **MAC Authentication** are enabled, this option enables you to control which authentication method is attempted first.

For example, if you select **Primary authentication using 802.1X**, the RADIUS authentication server first attempts to prompt the client for a user name and password. If the client has a RADIUS supplicant, it must submit a valid user and password to pass authentication. If the client does not have a RADIUS supplicant, the RADIUS server then tries to authenticate the client using the MAC address as both user name and password. If one of the authentication methods succeeds, the client is allowed on the network. If neither succeeds, the client is denied network access. To change the authentication sequence so that MAC authentication is attempted first, select **Primary authentication using MAC**.

11. For **User Access Settings**:

- a. For **Default User Profile**, set the user profile that you want the router to apply by default to users connecting to the port.
- b. Either select and choose an existing user profile, or select the plus sign and create a new one.

See [Add a User Profile](#) on page 281 for more information about creating user profiles.

- c. Select **Apply a different user profile to various clients and user groups** and add one or more user profiles for different categories of users that you expect to make wired connections to the access port.

If a single device, such as a printer, is always connected to this port, leave the check box cleared and just apply the default user profile for infrastructure devices like printers. If you expect different types of users, such as employees, consultants, and visiting VIPs, to use the port as needed to connect their computers to the network, then select the check box and set up [classification rules](#) to govern when to apply different user profiles.
 - d. For **Traffic Filter Management**, select which management and diagnostic services—SSH, Telnet, Ping, and SNMP—to enable access to the mgt0 interface through the access port.
12. Configure the following settings for **Trunk Ports** connected to network forwarding devices such as switches and APs that support multiple VLANs on trunk ports:
- a. For **VLAN Object**, set the native (untagged) VLAN and all VLANs that you want the port to support.
 - **Native VLAN:** The native (untagged) VLAN is the 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.
 - **Allowed VLANs:** Type the VLANs—including the native VLAN—that you want the trunk port to enable. You can list the VLANs individually, separated by commas, or as a range of VLANs using a hyphen. Alternatively, you can type the word `all` to support all existing VLANs previously configured in the network policy. When you type `all`, the router allows all VLANs configured in the network policy, not all VLANs from 1 to 4094.
 - b. For **Traffic Filter Management**, select which management and diagnostic services—SSH, Telnet, Ping, and SNMP—to enable access to the mgt0 interface through the trunk port.
13. For **WAN Ports**, because the ETH0 and USB ports are always enabled as WAN links, they must be set as primary, backup1, backup2, or backup3, therefore, you can set one or more Ethernet ports as WAN links.
14. **Port Types In Use** provides an overview of the port settings and configuration options available from the port settings tabs:
- **Port Details:** View information about the interfaces on the router, add or modify the port type assigned to each interface, and modify the WAN priority settings.
 - **Port Settings:** Displays the physical interface names, and allows you to select the transmission types and speeds.
 - **PSE:** Choose the PSE (power sourcing equipment) power settings for the router to provide to PDs (powered devices) through the ETH1 and ETH2 ports.

Related Links

[Router Settings](#) on page 182

VPN Services

VPN Services consist of configurations for Layer 3 IPsec VPNs, used for communication between routers, and Layer 2 IPsec VPNs, used for communication between access

points (APs). Go to **Manage > VPN Services** to view the existing VPN services in your network configuration.

Layer 3 IPsec VPNs

Layer 3 IPsec VPN tunnels securely send traffic between Extreme Networks routers and one or two Extreme Networks VGVA's (VPN Gateway Virtual Appliances). Each router functions as a VPN initiator and does a route look up to determine whether to send traffic from hosts in its sub-network through an IPsec tunnel to destinations in different subnets on the other side of the gateway, and which functions as a VPN terminator. When using a hub-and-spoke design, the destination might lie on the other side of a second tunnel that connects the Layer 3 VPN gateway to another router at a different remote site. ExtremeCloud IQ applies Layer 3 IPsec VPNs to routers and Layer 3 VPN gateways through a network policy that supports routing. For information about configuring Layer 3 IPsec VPNs, see [Configure Layer 3 VPN Services](#) on page 190.

Layer 2 IPsec VPNs



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 not be able to ping local servers because ICMP does not use port numbers. For information about configuring Layer 2 IPsec VPNs, see [Configure Layer 2 IPsec VPN Services](#) on page 332.

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, then 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.

Related Links

[Server-Client Credentials](#) on page 192

[Router Settings](#) on page 182

Configure Layer 3 VPN Services

Create a Layer 3 VPN Services profile that makes use of all the default settings, choose the VPN gateway and define its external IP address, and then configure the default routing policy and policy exceptions.

This task is part of the network policy configuration workflow. Use this task to configure Layer 3 IPsec VPNs.

1. Go to **Configure > Network Policies**.
2. Select an existing network policy, and then select , or select .
3. After you save the **Policy Details**, select **5 Branch Routing**.
4. From the **Router Settings** menu, select **VPN Service**.
5. Toggle **Enable VPN Service** to **ON**.
6. Select **ADD** to add a new VPN Service, or **SELECT** to specify an existing VPN service.
7. Configure the [VPN Services Settings](#) on page 365.
8. Select **GENERATE** to create client credentials for servers and clients.
For more information, see [Server-Client Credentials](#) on page 192.
9. For the remaining optional settings see:
 - [Configure IPsec VPN Authority Settings](#) on page 190 (Extreme Networks VPN Gateway only)
 - [Configure Advanced Server Options](#) on page 192
 - [Configure Advanced Client Options](#) on page 193
10. Select **SAVE**.

After you apply a VPN gateway, ExtremeCloud IQ automatically displays the WAN and LAN IP addresses, and indicates whether the VPN gateway uses dynamic routing protocols to learn routes from routing peers on its local network.

Related Links

[VPN Services Settings](#) on page 365

[Router Settings](#) on page 182

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 332.

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 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.

This task is part of the network policy configuration workflow. Use this task to configure IPsec VPN Authority settings.

1. Go to **Configure > Network Policies**.
2. Select an existing network policy, and then select , or select .
3. After you save the **Policy Details**, select **5 Branch Routing**.
4. From the **Router Settings** menu, select **VPN Service**.
5. In the **Optional Settings** section, expand **IPsec VPN Authority Settings**.
6. If you do not have a certificate or key that you want to use, select **Import**.
7. 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.

8. 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 192.

Related Links

[Server-Client Credentials](#) on page 192

[Configure Layer 2 IPsec VPN Services](#) on page 332

[Router Settings](#) on page 182

Server-Client Credentials

After you save the Layer 2 IPsec VPN service configuration, ExtremeCloud IQ populates the table with randomly generated 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 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 192.

Related Links

[Router Settings](#) on page 182

Configure Advanced Server Options

This task is part of the network policy configuration workflow. Use this task to configure the **Advanced Client Options** for a VPN service when you configure **Router Settings**.

1. Go to **Configure > Network Policies**.
2. Select an existing network policy, and then select , or select .
3. After you save the **Policy Details**, select **5 Branch Routing**.
4. From the **Router Settings** menu, select **VPN Service**.
5. Select an existing Layer 2 IPsec VPN service, and then select , or select .
6. In the **Optional Settings** section, expand **Advanced Server Options**.
7. 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).
8. 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)**.

9. Select **Enable peer IKE ID validation** to enable VPN clients to validate the IKE ID that the VPN gateway sends them, and choose the type of IKE ID to use.

When you create a server certificate, you have the option to define one or more of these subject alternative names: IP address, FQDN (fully-qualified domain name), user FQDN. You can use any of them as the IKE ID for the VPN gateway. You can also use the ASN.1 DN (Abstract Syntax Notation One Distinguished Name), which is automatically created by concatenating various values in the certificate— including the common name, different organizational units, and the email address.

When you update the configured devices with a configuration that includes a VPN services profile that references this server certificate, ExtremeCloud IQ pushes the server certificate and the specified IKE ID type to the VPN gateway. At the same time, ExtremeCloud IQ also pushes the CA certificate, IKE ID type, and IKE ID string to all the VPN clients. In this way, the VPN clients are ready to authenticate the VPN server certificate and its IKE ID when the time comes to do so during IKE negotiations.

10. Select **SAVE**, or continue configuring the VPN service.

Next, configure **Optional Settings > Advanced Client Options**, see [Configure Advanced Client Options](#) on page 193.

Related Links

[Configure Layer 2 IPsec VPN Services](#) on page 332

Configure Advanced Client Options

First, [Configure Layer 3 VPN Services](#) on page 190.

This task is part of the network policy configuration workflow. Use this task to configure the **Advanced Client Options** for a VPN service when you configure router settings.

1. Go to **Configure > Network Policies**.
2. Select an existing network policy, and then select , or select .
3. After you save the **Policy Details**, select **5 Branch Routing**.
4. From the **Router Settings** menu, select **VPN Service**.
5. Select an existing VPN service, and then select , or select .
6. In the **Optional Settings** section, expand **Advanced Client Options**.
7. Select **Enable NAT Traversal** to enable VPN traffic to traverse NAT devices.
8. Configure the **DPD (Dead Peer Detection) Settings**.

The DPD and tunnel heartbeat settings control when to fail over from the primary to the secondary VPN server. The DPD messages verify the presence of an IKE peer, and AMRP (Advanced Mobility Routing Protocol) tunnel heartbeats verify communications through the GRE and VPN tunnel. The failure of either mechanism can trigger a failover.

- 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 times to retry sending a DPD R-U-There message when it does not elicit a response.

- c. Set the amount of time between retries.
9. Select **SAVE**.

Related Links

[Configure Layer 3 VPN Services](#) on page 190

[Router Settings](#) on page 182

Configure an SD-WAN Route Group

Before you can enable SD-WAN, you must assign a branch ID to the router, and have one or two Extreme Networks VGVAs configured as part of a **VPN Service**. Then create a network policy and configure the **Router Settings**.

An SD-WAN route group is a list of prioritized WAN ports used as a forwarding action in a routing policy. Enable SD-WAN in a network policy to configure policies that make routing decisions based on Layer 7 application service sets, user profiles, incoming LAN interfaces, or source and destination addresses.

This task is part of the network policy configuration workflow. Use this task to configure an SD-WAN route group.

1. Go to **Configure > Network Policies**.
2. Select an existing network policy, and then select , or select .
3. After you save the **Policy Details**, select **5 Branch Routing**.
4. From the **Router Settings** menu, select **SD-WAN**.
5. Select **Enable SD-WAN**.
6. Select .
7. Enter a **Group Name**.
8. Enter an optional description.
9. Set the **WAN Priority** for the following WAN links on routers:
 - **WAN0**: The highest prioritized Ethernet link in the router template.
 - **WAN1**: The second highest prioritized Ethernet link in the router template.
 - **USB**: The WAN link of a connected USB LTE modem.
10. For **Routing Decision Rule**, define the following responses to operational faults for your SD-WAN routing decisions:
 - **Include Jitter**: Select **ON** to have jitter considered for WAN path changes.
 - **Packet Loss**: Select an aggressive, normal, or moderate response to packet losses.
 - **Latency**: Select an aggressive, normal, or moderate response to detected latency.
 - **Jitter**: (Only if **Include Jitter** is set to **ON**): Select an aggressive, normal, or moderate response to jitter.

Continue configuring the network policy.

Configure a Routing Policy

Create a Network Policy. For more information about router policies, see [Router Settings](#) on page 182.

There are three **Policy Types** for policy-based routing: **Split Tunnel**, **Tunnel All**, and **Custom**. When routing is enabled and SD-WAN is disabled, you can use any of these routing policy types. When both routing and SD-WAN are enabled, you must define custom routing rules. The **Split Tunnel** or **Tunnel All** options involve fewer routing considerations. If you configure the router to use **Split Tunnel**, the router applies the split tunnel template to the traffic, forwarding corporate traffic through the VPN tunnel and forwarding Internet traffic through the preferred interface to the Internet. If you configure the router to use **Tunnel All**, the router forwards corporate traffic through the VPN interface, but drops Internet traffic.

This task is part of the network policy configuration workflow. Use this task to configure a routing policy.

1. Go to **Configure > Network Policies**.
2. Select an existing network policy, and then select , or select .
3. After you save the **Policy Details**, select **5 Branch Routing**.
4. From the **Router Settings** menu, select **Routing Policy**.
5. Toggle **Enable Routing Policy** to **ON**.
6. If not selecting an existing policy, select **ADD**.
7. Type a **Name** for the routing policy.
8. (Optional) Type a **Description** for the routing policy.

Although optional, descriptions can be helpful when you are troubleshooting your network.

9. Select a **Policy Type**:
 - **Split Tunnel**: Use the **Forwarding Action** drop-down list to choose the forwarding interface to drop or forward traffic to the Internet. Choose a **Backup Forwarding Action** secondary interface from the drop-down list to drop or forward traffic to the Internet in the event that the primary interface goes down.
 - **None**: Takes no forwarding action.
 - **Primary WAN**: Routes traffic through the interface designated as the primary WAN interface in the device template. By default, the primary WAN interface on an Extreme Networks branch router is ETH0.
 - **Backup WAN-1**: Routes traffic through the interface designated as the backup WAN interface in the device template.
 - **Backup WAN-2**: Routes traffic through the interface designated as the secondary backup WAN interface when there are three interfaces in WAN mode. By default, the Backup WAN-2 interface on a router is the wireless USB modem.

- **VPN:** Routes traffic through the tunnel interface on a router that connects a branch site to the corporate site through an IPsec VPN tunnel.
- **Drop:** Drops traffic rather than forwarding it.

**Note**

The routes for **Forwarding Action** and **Backup Forwarding Action** cannot be the same.

- **Tunnel All:** Read-only.
10. If you choose the **Custom Policy Type**, select **Add**, and select these options:
- a. Choose a **Source Type**:
 - **Any:** Use when you want a routing policy rule to apply to traffic from any source.
 - **Network:** Use when you want a rule to apply to traffic from an entire subnetwork, such as a network reserved for contractors and guests.
 - **IP Range:** Use when you want a rule to apply to traffic from a range of IP addresses, such as the addresses in a DHCP pool reserved for a specific group of users.
 - **Interface:** Use when you want to apply a rule to all traffic arriving at a specific interface.
 - **User Profile:** Use when you want to apply rules to specific types of users.
 - **Application Service Set:** Use to apply rules to specific application types.
 - b. Choose a traffic **Destination**.
 - **Any:** The rule applies to any traffic destination.
 - **Network Address:** Sets a specific host name, subnet, or IP address range as the destination.
 - **Private:** The rule applies to traffic destined to the corporate network (VPN).
 - c. Select **Forwarding Actions** and **Backup Forwarding Actions** as described under **Split Tunnel** above.
11. To configure **Path MTU Discovery**, see [Path MTU Discovery Settings](#) on page 197.
12. Select **SAVE**.

For more information, see [Configure a Firewall Policy](#) on page 364, [Configure Dynamic DNS](#) on page 197, and [Configure URL Filtering Rules](#) on page 280.

Continue configuring the network policy.

Related Links

[Router Settings](#) on page 182

Path MTU Discovery Settings

With **Path MTU Discovery**, the router can monitor the value set in the MSS option in TCP SYN and SYN-ACK messages, which enables it to reduce the MSS value below the TCP-MSS thresholds.

Table 46: Settings for Path MTU Discovery

Setting	Description
Enable Path MTU Discovery	Select Enable Path MTU Discovery to enable the Extreme Networks router to learn the maximum packet size, or maximum transmission unit (MTU), that can be sent between two hosts without fragmentation.
Monitor the MSS Option in TCP SYN and SYN-ACK Messages and Perform Clamping if the MSS Threshold is Exceeded	Select Monitor the MSS Option in TCP SYN and SYN-ACK Messages and Perform Clamping if the MSS Threshold is Exceeded to monitor the MSS option in TCP SYN and SYN-ACK messages and, if necessary, reduce the MSS value as determined by one of the following TCP-MSS thresholds.
MSS Threshold for All TCP Connections	Type the TCP-MSS threshold for all TCP connections passing through the device. If you do not specify a threshold value, TCP-MSS clamping uses Path MTU (40 bytes) for the IP and TCP headers.
MSS Threshold for TCP Connections Through the VPN Tunnel	Type the TCP-MSS threshold for TCP connections that pass through a Layer 3 VPN tunnel. If you do not specify a threshold value, the device uses the value set for the MSS threshold for all TCP connections.

Related Links

[Configure a Routing Policy](#) on page 195

Configure Dynamic DNS

Dynamic DNS (DDNS) automatically and periodically updates your DNS server IPv4 or IPv6 information when your IP address changes.

This task is part of the network policy configuration workflow. Use this task to to configure DDNS as part of a network policy.

1. Go to **Configure > Network Policies**.
2. Select an existing network policy, and then select , or select .
3. After you save the **Policy Details**, select **5 Branch Routing**.
4. From the **Additional Router Services** menu, select **Dynamic DNS**.
5. Toggle **Enable Dynamic DNS** to **ON**.
6. Select a DDNS provider.
7. Type a **Username**.
8. Type a **Password**.
9. (Optional) Select **Show Password** to see the password.
10. Type the **Domain Name**, which must be the full router name and domain name.
The router host name must be unique.

11. Select **SAVE**.

Configure WAN Tracking

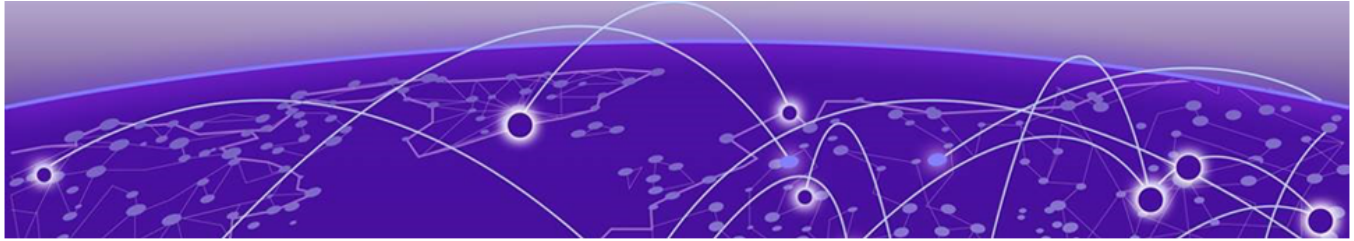
This task is part of the network policy configuration workflow. Use this task to configure WAN tracking as part of a network policy. Configure one or two WAN tracking destination IP addresses in a network policy so routers can check WAN availability by sending probe packets to these destination IPs.

1. Go to **Configure > Network Policies**.
2. Select an existing network policy, and then select , or select .
3. After you save the **Policy Details**, select **5 Branch Routing**.
4. From the **Router Settings** menu, select **WAN Tracking**.
5. To change the default, type a different **Primary IP Target**.
The default primary IPv4 target is 8.8.8.8, which is the Google Public DNS, a free domain name system (DNS). This DNS is available from anywhere in the world.
6. (Optional) Type a **Secondary IP Target**.
7. Type the **Number of Retries** before the router marks the link as unavailable.
8. For the **Measurement Interval**, type the number of seconds between retries.
9. To return settings to the factory defaults, select **Reset to Default**.
10. Select **SAVE**.

Continue configuring the network policy.

Related Links

[Router Settings](#) on page 182



Configuration—Common Objects

[Policy Configuration](#) on page 199
[Basic Configuration](#) on page 287
[Security Configuration](#) on page 303
[QoS Configuration](#) on page 313
[Management Configuration](#) on page 320
[Network Configuration](#) on page 327
[Authentication Configuration](#) on page 366
[Certificate Configuration](#) on page 370

Use the information and procedures in this chapter to define objects for use throughout the configuration process, in particular when you are configuring network policies.

Policy Configuration

The topics in this section provide details about policy configuration objects, such as AP Templates, Auto Provisioning, Bonjour Gateways, Client Monitor Profiles, Cloud Config Groups, Fabric Attach Profiles, Hives, Port Types, Radio Profiles, SDR Profiles, Schedules, and Classification Rules.

Related Links

[Configure AP Templates](#) on page 200
[Configure Auto-Provisioning](#) on page 209
[Configure a Bonjour Gateway](#) on page 211
[Configure Classification Rules](#) on page 214
[Configure Client Monitor Profile Policies](#) on page 216
[Add a Cloud Config Group](#) on page 217
[Configure a Fabric Attach Profile](#) on page 217
[IoT Profiles](#) on page 221
[Manage Port Types](#) on page 228
[Instant Port Profiles List](#) on page 228
[About Radio Profiles](#) on page 229
[Configure an SDR Profile](#) on page 242
[SSIDs](#) on page 117
[Configure Switch Templates](#) on page 244

[Configure URL Filtering Rules](#) on page 280

[Add a User Profile](#) on page 281

Configure AP Templates

Before you begin, create a network policy for the APs (see [Configure Device Templates](#) on page 171). You can also configure an AP template directly from the **Common Objects** tab.

Create AP device templates with default settings for all APs, and settings that ExtremeCloud IQ 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 device templates and auto-provisioning rules (see [Configure Auto-Provisioning](#) on page 209) are both in place for an AP when it is onboarded, the auto-provisioning rules are applied and the device template is ignored.

Use this task to configure an AP device template.

1. Go to **Configure > Common Objects > Policy > AP Template**.
2. Select an existing AP Template, and then select , or select .
To delete the selected template, select .
3. For a new template, enter a name, and for an existing template, edit where necessary.
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 201.
6. To configure **Wireless Interfaces**, see [Configure Wireless Interfaces for an AP Template](#) on page 202.
7. To configure **Wired Interfaces**, see [Configure Wired Interfaces for an AP Template](#) on page 203.
8. To configure **SES-imagotag**, see [Configure Electronic Shelf Labeling](#) on page 205.
9. To configure **Advanced Settings**, see [Configure AP Device Template Advanced Settings](#) on page 208.
10. Select **SAVE TEMPLATE**.

Continue configuring the network policy.

Related Links

[Configure Device Templates](#) on page 171

[Configure Auto-Provisioning](#) on page 209

[Policy Configuration](#) on page 199

Assign an Ethernet Port Profile

Use an Ethernet port profile to 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.

Use this task to assign a port profile to device ports.

1. Go to **Configure > Common Objects > Policy > AP Template**.
2. Select an existing AP Template, and then select , or select  to create a new template.
3. 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**.
4. 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.
5. For **Wired Connectivity**, enable **User Authentication**.
6. See [Configure an External RADIUS Server](#) on page 148 if you are not selecting an existing RADIUS Server Group.
7. Enable **MAC Authentication**, see [Configure MAC Authentication](#) on page 126.
8. For **QoS Settings**, see [Configure Marker Maps](#) on page 318.
9. For **User Access Settings**, to add a new User Profile, see [Add a User Profile](#) on page 281.
10. For **Traffic Filter Management**, see [Configure Traffic Filters](#) on page 307.
11. For **Port Settings**, see [Configure LLDP and CDP](#) on page 329.
12. For **STP Settings**, see [Enable STP—Device Configuration](#) on page 251.
13. For **Storm Control Settings**, see [Configure Storm Control](#) on page 258.

Continue configuring the AP template.

Related Links

[Configure Port Types](#) on page 201

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**.

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.

1. Go to **Configure > Common Objects > Policy > AP Template**.
2. Select an existing AP Template, and then select , or select .
3. To assign an existing port type, select the port and then select **Assign**.
4. To create a new port type and assign it to a port at the same time, highlight an interface port, then select **Assign** and **Create New** from the drop-down list.
5. Enter a **Name** for the port type.
6. (Optional) Enter a brief **Description** for the port type.
7. Turn the port off or on.
8. Select **Save**.

Related Links

[Assign an Ethernet Port Profile](#) on page 201

[Manage Port Types](#) on page 228

Configure Wireless Interfaces for an AP Template

Use this task to configure the Wi-Fi 0, Wi-Fi 1, Wi-Fi 2, Wi-Fi 3, and IoT 0 ports for an AP template.

1. Go to **Configure > Common Objects > Policy > AP Template**.
2. Locate a **Device Model** and select an existing **Template**, or a default template.
3. Scroll down to the **Wireless Interfaces** pane.

4. Select an **Operating Mode** from the drop-down list.
 - 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
5. Select either the **WiFi0**, **WiFi1**, **WiFi2**, **WiFi3**, or **IoT0** tab.

**Note**

- The **WiFi3** tab applies only to AP4020/AP4020X/AP4020FX and AP4060/AP4060X models.
- The **IoT0** tab applies only to AP5010/AP5020 models.

6. Set the **Radio Status** to **On**.
7. Select a **Radio Profile**—or **IoT Profile** if applicable—from the drop-down list.

You can also add a new [Radio Profile](#) or [IoT Profile](#) here, or clone and modify an existing profile.
8. 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.
9. Continue configuring the AP template, or select **Save Interface Settings**.

Configure Wired Interfaces for an AP Template

Create or edit an AP template.

Use this task to configure wired interfaces on the AP.

1. Go to **Configure > Common Objects > Policy > AP Template**.
2. Locate a **Device Model** and select an existing **Template**, or a default template.
3. Scroll down to the **Wired Interfaces** pane.
4. Set the Interface State to **ON** to activate the Ethernet port, or set to **OFF** to deactivate.

5. 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.
6. 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 171.
7. 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 171.
8. 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.
9. 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.
10. Select the **Speed** the Ethernet port uses to communicate with the connected device.
11. Select **Green Ethernet** for AP4020 and AP5020 devices to enable Energy-Efficient Ethernet (EEE).
 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.
12. 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.

13. Select **CDP** for devices to advertise an IP address that can send and receive SNMP traps.
14. 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.
15. 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.

16. (Optional) Toggle **Enable Imagotag** to **ON**.

To configure SES-Imagotag in the device template, see [Configure Electronic Shelf Labeling in a Device Template](#) on page 206.

Continue configuring the AP template.

Configure Electronic Shelf Labeling

Electronic Shelf Labeling (ESL) consists of the following components:

- ESL tags, which are 2.4 GHz RF based battery powered devices
- An ESL communicator used to communicate with the ESL tags
- A server that provides the configuration and updates to the ESL tags

The following access points support Electronic Shelf Labeling:

- AP305C
- AP410C
- AP4020
- AP5010
- AP5020

Configure ESL on a device template or for an individual AP override.

**Note**

Consider the following for ESL support.

- An ESL Server behind a NAT (Network Address Translation) or firewall is not supported.
- Do not make configuration changes during ESL configuration.

Related Links

[Configure Electronic Shelf Labeling in a Device Template](#) on page 206

[Configure Electronic Shelf Labeling as a Device Override](#) on page 207

[Electronic Shelf Labeling Setup](#) on page 206

[Configure AP Templates](#) on page 200

Electronic Shelf Labeling Setup

Use this task to enable Electronic Shelf Labeling (ESL).

1. Prepare the AP device:
 - a. Ensure that the access point is getting 3AT/3AT+ power.
 - b. Connect ESL communicator to access point USB port.
 - c. Ensure that the LED on the ESL communicator is red.
2. In ExtremeCloud IQ, [Configure Electronic Shelf Labeling in a Device Template](#) on page 206 or [Configure Electronic Shelf Labeling as a Device Override](#) on page 207 for a supported AP model.

The following access points support Electronic Shelf Labeling:

- AP305C
 - AP410C
 - AP4020
 - AP5010
 - AP5020
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

[Configure Electronic Shelf Labeling](#) on page 205

[Configure Electronic Shelf Labeling in a Device Template](#) on page 206

[Configure AP Templates](#) on page 200

[Configure Electronic Shelf Labeling as a Device Override](#) on page 207

[Electronic Shelf Labeling Settings](#) on page 207

Configure Electronic Shelf Labeling in a Device Template

Use this task to configure Electronic Shelf Labeling (ESL) in a device template.

1. Go to **Configure > Common Objects > Policy > AP Template**.

2. Select an AP template for one of the supported AP models.
The following access points support Electronic Shelf Labeling:
 - AP305C
 - AP410C
 - AP4020
 - AP5010
 - AP5020
3. Scroll down to the **Electronic Shelf Labeling** section and select **Enable ESL**.
4. Configure the Electronic Shelf Labeling settings.

Related Links

[Electronic Shelf Labeling Settings](#) on page 207

[Configure Electronic Shelf Labeling as a Device Override](#) on page 207

[Configure Electronic Shelf Labeling](#) on page 205

[Electronic Shelf Labeling Setup](#) on page 206

Configure Electronic Shelf Labeling as a Device Override

Use this task to configure Electronic Shelf Labeling (ESL) as a device override.

1. Go to **Manage > Devices**
2. Select one of the supported AP models.
The following access points support Electronic Shelf Labeling:
 - AP305C
 - AP410C
 - AP4020
 - AP5010
 - AP5020
3. From the left pane, select **Configure > Interface Settings**.
4. Scroll down to the **Electronic Shelf Labeling** section and select **Enable ESL**.
5. Configure the Electronic Shelf Labeling settings.

Related Links

[Electronic Shelf Labeling Settings](#) on page 207

[Configure Electronic Shelf Labeling in a Device Template](#) on page 206

[Configure AP Templates](#) on page 200

[Configure Electronic Shelf Labeling](#) on page 205

[Electronic Shelf Labeling Setup](#) on page 206

Electronic Shelf Labeling Settings

Configure the following settings for Electronic Shelf Labeling (ESL):

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 select the communications channel.

Port

The port associated with the defined rule. Enter the port number to explicitly specify the port number. Traffic from this port is subject to the defined rule.

VLAN

The VLAN used to route ESL traffic.

Related Links

[Configure Electronic Shelf Labeling in a Device Template](#) on page 206

[Configure Electronic Shelf Labeling as a Device Override](#) on page 207

[Configure Electronic Shelf Labeling](#) on page 205

[Electronic Shelf Labeling Setup](#) on page 206

Configure AP Device Template Advanced Settings

ExtremeCloud IQ can update device firmware and reboot the device during onboarding.

Use this task to configure **Advanced Settings** for an AP device template.

1. Go to **Configure > Common Objects > Policy > AP Template**.
2. Select an existing AP Template, and then select , or select .
3. Select the **Advanced Settings** tab.
4. For **Upload device firmware upon device authentication**, turn the setting **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.
5. To **Reboot after uploading**, turn the setting **On**.



Note

As a best practice, disable the reboot option when deploying devices in a meshed environment.

6. For **Antenna Location Type**, select a location from the drop-down list.



Note

You must have IQ Engine Version 10.2r2 or higher. The 6 GHz radio is supported Low Power Indoor (LPI) only.



Note

Antenna Location Type does not apply to AP5020.



Note

A full config push is required as different radio tables are used.

7. To enable or disable **Supplemental CLI**, see [Configure Supplemental CLI](#) on page 302.
8. 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.

9. Enable **Override MGT0 MTU** to manually enter a maximum transmission unit (MTU) value, ranging from 100-1500 Bytes. Default value is 1500 Bytes.
10. Enable **POE Profile Override** (AP5010 only), and select the override option from the menu.

Hover over the **i** to view the corresponding override table.

Finish configuring the device template.

Configure Auto-Provisioning

Although AP device templates function similarly to auto-provisioning rules, the best-practice recommendation is to use AP device templates rather than auto-provisioning rules to configure APs as they are onboarded.

**Note**

If AP device templates and auto-provisioning rules are both in place when the AP is onboarded, ExtremeCloud IQ ignores the AP device 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 **Configure > Common Objects > Policy > Auto Provisioning**.
2. Select an existing rule, and then select , or select .
3. Enter a **Name** for the rule.
4. (Optional) Enter 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 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 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 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 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 202 for general instructions.

21. Configure Wired interface. See [Configure Wired Interfaces for an AP Template](#) on page 203 for general instructions.

22. When the auto-provisioning rule configuration is complete, select **Save** to commit the changes, or select **Cancel**.

Configure a Bonjour Gateway

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 **Configure > Common Objects > Policy > Bonjour Gateway Settings**.
2. Select an existing Bonjour Gateway, and then select , or select .
3. Configure the following settings.

Table 47: 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. 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 213.
6. Select **Save**.

Related Links

[Bonjour Filter Rule Settings](#) on page 213

*Bonjour Filter Rule Settings***Table 48: Bonjour Filter Rule Settings**

Field	Description
Service	Choose the name of a previously defined Service from the drop-down list, or enter the name of the service in the field. To add a new Service: 1. Select . 2. Enter the service Name. 3. Enter the Type. 4. Select Save.
From VLAN Group	Choose the VLAN group from which to share services. 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. To add a new From VLAN Group: 1. Select . 2. Enter the service Name. 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. 4. Enter an optional Description. 5. Select Save.
To VLAN Group	Choose the VLAN group to which services are advertised. 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. To add a new To VLAN Group: 1. Select . 2. Enter the service Name. 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. 4. Enter an optional Description. 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 48: 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. 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. Note: By default, the Bonjour Gateway detects and retransmits from the selected VLAN group.

Related Links

[Configure a Bonjour Gateway](#) on page 211

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 common object. ExtremeCloud IQ supports multiple classification rules for DNS servers, VLANs, RADIUS servers, device templates, user groups, and private client groups (PCGs).

1. Go to **Configure > Common Objects > Policy > Classification Rules**.
2. Select an existing rule, and then select , or 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 49: Rule types

Selected rule type	Do this
Device Location	- Drill down until you reach the location level at which the device resides. - Select Select. The location appears in the Classification Rules table.
Cloud Config Group	- Select the Match Type. - Select an existing group from the  menu, or select . For more information, see Add a Cloud Config Group on page 217. - Select CLOUD CONFIG GROUP. - Select CONTINUE.
IP Address	- From the Match Type menu, select Contains or Does Not Contain. - Select , or select an existing IP address from the  menu. If you do not see the IP address that you want, select New to create a new IP address. - Select SAVE IP. - Select CONTINUE.
IP Subnet	- From the Match Type menu, select Contains or Does Not Contain. - Select , or select an existing IP subnet from the  menu. If you do not see the IP subnet that you want, select New to create a new IP subnet. - Select SAVE SUBNET. - Select CONTINUE.
IP Range	- From the Match Type menu, select Contains or Does Not Contain. - Select , or select an existing IP range from the  menu. If you do not see the IP range that you want, select New to create a new IP range. - Select SAVE IP. - Select CONTINUE.

6. Select **SAVE RULE**.

Related Links

[Add a Cloud Config Group](#) on page 217

Configure Client Monitor Profile Policies

Use this task to configure client monitor profile policies.

1. Go to **Configure > Common Objects > Policy > Client Monitor Profiles**.
2. Select an existing client monitor profile, and then select , or select .
3. Configure the settings for the Client Monitor Profile policy.
See [Client Monitor Profile Settings](#) on page 216.
4. Select **Save**.

Related Links

[Client Monitor Profile Settings](#) on page 216

Client Monitor Profile Settings

Table 50: 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 Monitor Profile Policies](#) on page 216

Add a Cloud Config Group

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 create a new group.

1. Go to **Configure > Common Objects > Policy > Cloud Config Groups**.
2. Select an existing group, and then select , or select .
3. Enter a **Name** for the new group.
4. (Optional) Enter a **Description** for the new group.
5. Select real and simulated devices to have their host names display 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 a Fabric Attach Profile

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 174.

Use this task to configure Fabric Attach profiles that you can assign to network policies.

1. Go to **Configure > Common Objects > Policy > Fabric Attach Profiles**.
2. Select an existing profile, and then select , or 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 174

[Configure Fabric Attach](#) on page 174

Configure a HIVE Profile

Use this task to configure a HIVE profile object.

1. Go to **Configure > Common Objects > Policy > Hives**.
2. Select an existing hive profile, and then select , or select .
3. Apply MAC filters to restrict devices that can join the hive.
You can select existing filters from the table, or add new filters.
4. 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.
5. Select **SAVE**.

Related Links

[HIVE Profile Settings](#) on page 218

HIVE Profile Settings

Table 51: 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. 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 any 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) 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 . Disable Encryption Protection to have ExtremeCloud IQ derive a default password from the hive name.
Encryption Password	Choose between Auto Generate and Manual . 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 51: HIVE profile settings (continued)

Setting	Description
MAC-based DoS Prevention Rules	Select Hive or Client, and modifying the settings in the dialog box. Extreme Networks devices ship with the default hive- and SSID-lever DoS detection settings for a number of frame types that are commonly used when launching DoS attacks. You can raise the thresholds to avoid receiving too many false alarms or lowering them to receive more alarms indicative of spikes in certain types of traffic. • 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. • 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. 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 see if any 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 a value in bytes. This is the maximum frame size in bytes that requires the device to first send an request to send (RTS (request to send) message before sending a large frame. The default setting is 2346 bytes.
Fragment Threshold	Type a value in bytes. This is the maximum IEEE 802.11 frame size in bytes that the device uses when sending control traffic over the wireless backhaul link to other members. If the device needs to send a frame that is larger, it first breaks it into smaller 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 51: HIVE profile settings (continued)

Setting	Description
Signal Strength Threshold	Use the slider to specify a signal strength between 90 dBm and - 55 dBm. 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 a value for the time interval from 1 to 60 minutes for polling the signal strength of neighboring members. A lower interval increases traffic on the network slightly, especially in environments where there are lots of members, however it also increases the responsiveness of members to changes in signal strength. A higher interval reduces responsiveness to signal strength changes, which can be preferable in an environment where severe and frequent signal strength fluctuations would cause members to continually drop and re-establish connections. The default is every 60 seconds.
Client Roaming > Detect neighbor devices	
Devices send keepalive heartbeats every	Type a value and select a unit of time from the menu to set the interval between keepalive heartbeats. 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. Using the default settings, 10 seconds (interval) x 5 (missed keepalives), a neighbor ages out after 50 seconds.
Remove neighbor if the number of missed keepalive heartbeats exceeds	Type the number of the number of missed heartbeats before ExtremeCloud IQ removes a neighbor.
Client Roaming > Share connected client information(Roaming cache)	
Devices send client information every	Type a value and select a unit of time from the menu to specify how often devices send client information. The default is 60 seconds.
Remove cached client information when absent from updates after	Type the number of missed updates, after which ExtremeCloud IQ 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) From the menu, select IPv4 or IPv6 .

Related Links

[Configure HIVE Policy Settings](#) on page 109

[Configure a HIVE Profile](#) on page 218

Configure a Hotspot Profile

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 138.

1. Go to **Configure > Common Objects > Policy > Hotspot Profiles**.
2. Select an existing Hotspot Profile, and then select , or select .
3. Configure the [Hotspot Settings](#) on page 139.

Related Links

[Hotspot Settings](#) on page 139

[Configure a Hotspot](#) on page 138

Configure a Hotspot Service Provider Profile

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 138.

You can also configure a Hotspot Service Provider when you [configure a Hotspot Profile object](#).

1. Go to **Configure > Common Objects > Policy > Hotspot Service Provider Profiles**.
2. Select an existing Hotspot Service Provider, and then select , or select .
3. Configure the [Table 34](#) on page 140.

Related Links

[Hotspot Settings](#) on page 139

[Configure a Hotspot](#) on page 138

[Configure a Hotspot Profile](#) on page 221

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 uses IoT profiles to support IoT applications.

Related Links

[Manage IoT Profiles](#) on page 223

[Thread Application](#) on page 222

[Configure IoT Profile Settings](#) on page 224

[Configure the Thread Commissioner](#) on page 226

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, 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 IoT Thread application is supported on AP5010/AP5020 only. IoT Thread is not supported on simulated devices.

With ExtremeCloud IQ, 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 specifying the behavior of the Commissioner for the Thread network, including its credentials, timeout, and list of allowed devices.
- Optionally configuring 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 221

[Configure IoT Profile Settings](#) on page 224

[Configure the Thread Commissioner](#) on page 226

Manage IoT Profiles

The **IoT Profiles** list displays the following information:

Table 52: IoT Profiles List Column Headings

Column Heading	Description
Name	Displays the name assigned to the profile.
IoT Application	Indicates the type of IoT application for which the profile is used.
Used By	Indicates at which device configuration level the profile is assigned: Device Template or Device Configuration .

Use this task to add a new IoT profile to the list, or to edit, clone, or delete existing IoT profiles.

1. Go to **Configure > Common Objects > Policy > IoT Profiles**.

2. Select an existing profile, and then select , or select .

See [Configure IoT Profile Settings](#) on page 224.

- To clone an existing IoT profile, select the profile in the list, then select . In the **Clone** pop-up window, enter a new profile name in the **Save As** field, then select **Clone**.
- To delete an existing IoT profile, select the profile in the list, then select .

Related Links

[IoT Profiles](#) on page 221

Configure IoT Profile Settings

Before you begin, configure a network policy. See [Add a Network Policy](#) on page 102.

Use this task to configure an AP5010/AP5020 to function as a Backbone Border Router in a Thread network.

1. Go to **Configure > Common Objects > Policy > IoT Profiles**
2. Select an existing profile, and then select , or select .
3. Configure the settings as described in [Table 53](#) on page 224 or [Table 54](#) on page 225.
4. Select **Save**.
5. (Optional) Select **Customize** to [Configure the Thread Commissioner](#) on page 226.

Proceed to [Configure Wireless Interfaces for an AP Template](#) on page 202 to enable the Thread **IoT0** radio interface of the AP.

You can override the AP Template IoT0 radio interface settings by configuring the settings under **Manage > Devices > Configure > Interface Settings > Wireless Interfaces > IoT0**.

Related Links

[IoT Profiles](#) on page 221

[Thread Application](#) on page 222

IoT Profile Settings

- [Thread Profile Settings \(Single IoT Application\)](#)
- [Thread Profile Settings \(Multiple IoT Applications\)](#)

Table 53: 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 53: 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. Note: Thread channel 25 is only supported if the country supports IEEE 802.11 channels 12, 13, or 14. 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. To create a new user profile, see Add a User Profile on page 281. 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 54: 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 54: Thread Profile Settings (Multiple IoT Applications) (continued)

Setting	Description
Destination	Select Cloud Reporting, Batch Reporting, or both. Specify the interval in seconds. For Batch Reporting, specify the destination URL. To remove duplicate entries reported for the Batch Reporting interval, keeping only the latest entry for each BLE tag, toggle Remove Duplicates to ON. 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. Note: If you select Custom for the Vendor, type the Company Name and the Company ID.

Related Links

[IoT Profiles](#) on page 221

Configure the Thread Commissioner

Before you begin this task, complete procedure [Configure IoT Profile Settings](#) on page 224.

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. Go to **Configure > Common Objects > Policy > IoT Profiles**.
2. Select an existing Thread Application profile, and then select , or select .
3. Scroll down to **Commissioner**, and select **CUSTOMIZE**.
4. (Optional) Type the **Commissioner Credential** consisting of 6 to 250 alphanumeric characters.

5. (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. See [Actions Menu Overview](#) on page 449.

6. 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 7.
 - To add devices in bulk, proceed to step 8.

**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 in accordance with steps 7.b and 7.c, then select **Save**. When editing is complete, proceed to step 9.
 - Delete entries in the Allow List. Select one or more entries, then select . Proceed to step 9.
 - 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 PSKd in the search field, then select .
7. 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 7.a through 7.d for each device added.
 - f. Proceed to step 9.

8. 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.
9. Select **Save** to save settings, 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 **Stop Thread Commissioner** and reassign the Commissioner role to another AP. See [Actions Menu Overview](#) on page 449 for details.



Note

The **Start Thread Commissioner** and **Stop Thread Commissioner** actions appear only when the AP is running an HOS version earlier than 10.8.6.0. These options are not available for APs running HOS 10.8.6.0 or later.

Related Links

[IoT Profiles](#) on page 221

[Thread Application](#) on page 222

[Actions Menu Overview](#) on page 449

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 **Configure > 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 201

Instant Port Profiles List

The Instant Port Profiles (IPP) feature in ExtremeCloud IQ 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.

The **Instant Port Profiles List** displays the configured Instant Port Profiles in your network. Configure IPP as part of a switch template configuration or a device template configuration. To delete a profile from the IPP list, select the corresponding check box, and then select .

Related Links

[Configure an Instant Port Profile](#) on page 260

About 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 171.

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 171

[Configure a Radio Profile](#) on page 230

[Configure Neighborhood Analysis](#) on page 231

[About Channel Selection](#) on page 231

[Configure Dynamic Channel Switching](#) on page 234

[Optimize Radio Usage](#) on page 235

[Radio Settings](#) on page 236

Configure a Radio Profile

Use this function 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 [About Radio Profiles](#) on page 229.

**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 **Configure > Common Objects > Policy > Radio Profiles**.
2. Select an existing profile, and then select , or select .
3. Type the radio profile **Name**.
4. Type a **Description**.
Although optional, descriptions can be helpful when you are 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

[About Radio Profiles](#) on page 229

[Configure Device Templates](#) on page 171

[Configure Neighborhood Analysis](#) on page 231

[About Channel Selection](#) on page 231

[Configure Dynamic Channel Switching](#) on page 234

[Optimize Radio Usage](#) on page 235

[Radio Settings](#) on page 236

Configure Neighborhood Analysis

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.

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. Go to **Configure > Common Objects > Policy > Radio Profiles**.
2. and then select , or select .
3. In the **Neighborhood Analysis** section, toggle **Background Scan ON** or **OFF**.
Background scanning is necessary for WIPS and Layer 3 roaming to function.
4. Set the interval between background scans of all radio channels.
Perform Background Scan Every: The range is 1 to 1440 minutes (24 hours).
5. 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.
6. Select **SAVE RADIO PROFILE**.

Related Links

[Configure Channel Selection](#) on page 233

[Configure a Radio Profile](#) on page 230

About 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). For more information, see [AP5000 Series Radios and 6 GHz Support](#) on page 41.

Related Links

[Configure Channel Selection](#) on page 233

Configure Channel Selection

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.

Channel selection is dimmed and set to **Auto**. Perform channel selection at the device level.

1. Go to **Configure > Common Objects > Policy > Radio Profiles**.
2. Select an existing radio profile, and then select , or select .
3. 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)**
4. To manually exclude channels, select a specific channel.
5. 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.

- c. 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.
6. To manually set **Transmission Power**, select **Manual** and then use the slider to select a dBm setting.
7. Enable **Enable client transmission power control (802.11h)**.
8. To manually enable client transmission power control (802.11h), use the slider to select a dBm setting.
9. 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.
10. Enable **Use the last known power and channel during the AP boot up process**.
11. Select **SAVE RADIO PROFILE**.

Related Links

[About Channel Selection](#) on page 231

[Configure Dynamic Channel Switching](#) on page 234

[Configure a Radio Profile](#) on page 230

Configure Dynamic Channel Switching

Enable Dynamic Channel Switching (DCS) to dynamically select and switch channels based on specified criteria.

1. Go to **Configure > Common Objects > Policy > Radio Profiles**.
2. Select an existing radio profile, and then select , or select .
3. Enable **Dynamic Channel Switching**.
4. 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.

5. 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**
6. Select **SAVE RADIO PROFILE**.

Related Links

[Optimize Radio Usage](#) on page 235

[Configure a Radio Profile](#) on page 230

Optimize Radio Usage

Management frames such as beacons, and probe and association requests and responses, consume airtime that might otherwise be used to transmit user data. Configure the following settings 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. Go to **Configure > Common Objects > Policy > Radio Profiles**.
2. Select an existing radio profile, and then select , or select .
3. 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.
4. 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.
5. 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** select the add icon to add a new MAC OUI.

See [Configure a MAC Object and MAC OUI](#) on page 298.



Note

The suppression setting is disabled by default when high-density WLAN optimization is enabled.

6. Enable **Band Steering** and select a mode from the menu.

7. Use the slider to set the **Allowed percentage distribution of 2.4 and 5.0 GHz clients**.
8. Enable **Client Load Balancing** and configure the threshold settings.

Table 55: Load balance clients based on

Airtime	Number of clients
Ignore probe and association requests per device when threshold exceeds: • CRC Error Rate • RF Interference • Average Airtime Per Client	Ignore probe and association requests from clients associated with other Extreme Networks devices until: • Anchor Period Elapses • Query neighbors about client load every
Ignore probe and association requests from clients associated with other Extreme Networks devices until: • Anchor Period Elapses • Query neighbors about client load every	

9. Enable **Radio Load Balancing** and specify the **Number of Connection Attempts**.
10. Enable **Weak Signal Probe Request Suppression** and specify the **Signal-to-Noise Threshold** in dB.
11. Enable **Safety Net** and specify the time elapse, in seconds or minutes, before a device again responds to association requests after an overload incident.
12. Configure [Configure Radio Settings](#) on page 237.
13. Select **SAVE RADIO PROFILE**.

Related Links

[Configure a MAC Object and MAC OUI](#) on page 298
[Configure Radio Settings](#) on page 237
[Configure a Radio Profile](#) on page 230

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 237

Configure Radio Settings

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 236.



Note

Extreme Networks provides defaults for each item in this section. The following steps are optional.

1. Go to **Configure > Common Objects > Policy > Radio Profiles**.
2. Select an existing radio profile, and then select , or 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

[Optimize Radio Usage](#) on page 235

[Configure Backhaul Failover](#) on page 238

[Configure a Radio Profile](#) on page 230

Configure Backhaul Failover

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. Go to **Configure > Common Objects > Policy > Radio Profiles**.
2. Select an existing radio profile, and then select , or select .
3. Enable **Backhaul Failover**.
4. 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.
5. Select **SAVE RADIO PROFILE**.

Related Links

[Configure Outdoor Deployment](#) on page 239

[Configure a Radio Profile](#) on page 230

Configure Outdoor Deployment

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. Go to **Configure > Common Objects > Policy > Radio Profiles**.
2. Select an existing radio profile, and then select , or select .
3. Set a distance (between 300 and 10,000 meters) over which to support the radio.
4. Select **SAVE RADIO PROFILE**.

Related Links

[Configure RF Interface Reports](#) on page 239

[Configure a Radio Profile](#) on page 230

Configure RF Interface Reports

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. Go to **Configure > Common Objects > Policy > Radio Profiles**.
2. Select an existing radio profile, and then select , or select .
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 Client SLA Definitions](#) on page 240

[Configure a Radio Profile](#) on page 230

Configure Client SLA Definitions

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 802.11a/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.

1. Go to **Configure > Common Objects > Policy > Radio Profiles**.
2. Select an existing radio profile, and then select , or select  and then select .
3. 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.
4. Select **SAVE RADIO PROFILE**.

Related Links

[Configure WMM QoS Settings](#) on page 240

[Configure a Radio Profile](#) on page 230

Configure WMM QoS Settings

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 Wi-Fi Multimedia.

1. Go to **Configure > Common Objects > Policy > Radio Profiles**.
2. Select an existing radio profile, and then select , or select .
3. If necessary, modify the default settings in the **Contention Window Minimum**, **Contention Window Maximum**, and **AIFS** columns.
4. If necessary, modify the default setting in the **TXOP Limit** column to determine how long bursts of traffic last before relinquishing the medium.
5. 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.
6. Select **SAVE RADIO PROFILE**.

Related Links

[Configure Sensor Mode Scan Settings](#) on page 241

[Configure a Radio Profile](#) on page 230

Configure Sensor Mode Scan Settings

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. Go to **Configure > Common Objects > Policy > Radio Profiles**.
2. Select an existing radio profile, and then select , or select .
3. If necessary, modify the **Dwell Time**.
4. Deselect **Scan All Channels** and set individual channel numbers to collect client probe request data.

5. Select **SAVE RADIO PROFILE**.

Related Links

[Configure a Radio Profile](#) on page 230

Configure an SDR Profile

Before you begin, you must create radio profiles. For more information, see [Configure a Radio Profile](#) on page 230.

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).

1. Go to **Configure > Common Objects > Policy > SDR Profiles**.
2. Select an existing profile, and then select , or select .
3. Type a **Name** for the profile.
4. (Optional) Type a **Description** for the profile.

Although optional, entering a description is helpful for troubleshooting and for identifying 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 a Radio Profile](#) on page 230

Configure a Schedule

Use this procedure to configure a schedule as a common object for reuse.

1. Go to **Configure > Common Objects > Policy > Schedules**.
2. Select an existing schedule, and then select  , or select .
3. Configure the settings.
See [Schedule Settings](#) on page 243.
4. Select **SAVE SCHEDULE**.

Related Links

[Schedule Settings](#) on page 243

Schedule Settings

Table 56: Settings for a One Time Schedule

Setting	Description
Name	Type a name for the schedule.
Description	(Optional) Type a description for the schedule.
One Time	Select to apply this schedule one time only.

Table 56: Settings for a One Time Schedule (continued)

Setting	Description
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 57: Settings for a Recurring Schedule

Setting	Description
Name	Type a name for the schedule.
Description	(Optional) 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

[Schedule Settings](#) on page 243

[Configure an Availability Schedule | User Profile](#) on page 285

Configure an SSID

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 118.

Use this task to configure a new SSID object for reuse in network policies.

1. Go to **Configure > Common Objects > Policy > SSIDs**.
2. Select an existing SSID, and then select , or select .
3. Configure the settings.
For more information, see [SSID Usage in Standard Wireless Networks](#) on page 118.
4. Select **SAVE**.

Related Links

[SSID Usage in Standard Wireless Networks](#) on page 118

Configure Switch Templates

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, see the ExtremeCloud IQ Universal Switch Deployment Guide.

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. With the Switch Template Override feature, you can create and manage switch templates based on common settings for the SwitchEngine, ExtremeXOS, Fabric Engine, and VOSS platforms. 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.

To make changes to a switch template at the device level, go to **Manage > Devices** and select a device name.

Use this task to configure a switch template.

1. Go to **Configure > Common Objects > Policy > Switch Template**.
2. Select an existing switch template, and then select , or 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 267.

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 an Instant Port Profile](#) on page 260.
 - To **Configure Ports in Bulk**, see [Create a New Port Type](#) on page 248
 - To **Configure Ports Individually**, see [Configure Individual Ports](#) on page 252
15. For **sFlow Control**, see [Configure an sFlow Receiver](#) on page 358.
16. For **Supplemental CLI**, see [Configure Supplemental CLI](#) on page 302.
17. For **Advanced Settings**, see [Configure Switch Device Template Advanced Settings](#) on page 279.
18. Select **Save**.

Continue configuring the network policy. To create a switch stack template, see [Manually Create a Switch Engine Stack](#) on page 277.

Configure Switch Common Settings

This section contains configuration elements applicable to all Switch Engine, EXOS, Fabric Engine, and VOSS switches assigned to a specific network policy.

Use this task to configure common settings for switches.

1. For **Management Servers** (Switch Engine/EXOS only), select **VR-Default** or **VR-mgmt** to apply the correct routing instance to defined network policy DNS, NTP, SNMP, and Syslog server settings.
2. For **STP Configuration**, see *Configure STP Settings* in the *ExtremeCloud IQ Universal Switch Deployment Guide*.
3. 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.

4. For **IGMP Settings**, if necessary, toggle to **On** and make the following selections:
 - **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.
5. For **Extreme Loop Recovery Protocol Settings**, select **Configure ELRP client periodic packet transmission for VLAN(s) assigned to port type to detect and prevent loops. ELRP must also be enabled within switch template.**

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.

Or

Select **Configure ELRP Port Duration** to enable the ability to define how many seconds a port stays disabled before re-enabling when ELRP detects a loop (15-600 seconds).

6. For **DHCP Snooping Settings**, toggle to **On**.
 - **Drop Rogue Packets Action:** Instructs the switch to drop all packets marked as rogue.
7. 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.
8. For **PSE Settings**, toggle to **On** to configure maximum power thresholds to generate alerts to ExtremeCloud IQ about exceeding maximum power levels.

9. For **Management Interface Settings** (Switch Engine devices only), select one of the following options:
 - **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.

Port Type Settings

Use **Port Types** to manage Switch Engine (EXOS) and Fabric Engine (VOSS) SKU port types within the network policy. View, create, edit, clone and delete switch port types from the **Port Types** menu item under **Switch Settings**. Use the plus sign to add a new port type. See [Create a New Port Type](#) on page 248 for more information about port type configuration.



Note

You cannot delete a port type if it is currently assigned to a switch associated to any network policy.

The table displays information about the port device family, usage, status, and VLAN. For the **Used by** column, hover over, select the number (Total number of usages), and the Device configuration, Device Template, and Network Policy this port type is being used in displays on the right. For example:

- Device Template
- 2ndSlot_5720_copied
- AVM-5720-Stack-2
- Network Policy
- Edge_IOT_Policy

Other columns display based on a filter that enables you to view Switch Engine, EXOS or Fabric Engine, VOSS, or both.

Related Links

[Create a New Port Type](#) on page 248

Create a New Port Type

Create or modify a port type.

Use this task to create ports in bulk.

1. Either 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**).
2. If this template applies to a 5570 or 5520 switch, define the VIM Port Channelization ports; otherwise, proceed to Step 3.
 - a. Under **Configure Ports in Bulk**, choose **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**.

**Note**

If 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 171 for more information about classification rules.

- d. Select one or more of these VIM ports and continue to Step 3.
3. Type a **Name**.
 4. (Optional) Edit the associated **Description**.
 5. Toggle the port **ON** or **OFF**.
 6. 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.
 7. Select **Next**.
 8. 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 156.
 9. Select **Next**.
 10. 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.
 11. Select **Next**.
 12. 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 148.
 13. For **Authentication Method Priority**, use the up or down arrows to determine the authentication method use order.

14. 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 318.

15. Select **Next**.

16. 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.
- **LLDP Receive:** Enables the switch to receive LLDPDU frames.

17. Select **Next**.

18. 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.

19. Select **Next**.

20. 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.
21. 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.
22. 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.
23. Select **SAVE**.
24. 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.
25. For **PSE**, select an existing profile or select the plus sign to add a new one.
- See [Configure PSE Settings](#) on page 259.
26. Review all the port settings in the **Summary** section and select **Save** when complete.

Enable STP—Device Configuration

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 Individual Ports

Use this task to configure or modify settings for individual ports.

1. Go to **Configure > Common Objects > Policy > Switch Template**
2. Select an existing template, and then select , or select  and configure a new template.
3. From the **Configuration** menu, select **Port Configuration** or **Port/VLAN Configuration**.
4. For **Port Name & Usage** and **VLAN**, see [Configure Port Details](#) on page 252.
5. For **User Authentication**, see [Configure User Authentication](#) on page 254.
The **User Authentication** tab is part of the taskflow for older Dell and SR-based devices.
6. For **QoS**, see [Configure QoS Settings](#) on page 255.
7. For **Transmission Settings**, see [Configure Port Transmission Settings](#) on page 256.
8. For **STP**, see [Configure STP Settings](#) on page 257.
9. For **Storm Control**, see [Configure Storm Control](#) on page 258.
10. For **PSE**, see [Configure PSE Settings](#) on page 259.
11. Review the settings on the **Summary** tab, and then select **SAVE**

Continue configuring the switch template.

Configure Port Details

Create or modify a switch template, and then open it for configuration. See [Configure Individual Ports](#) on page 252.

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 266.

- **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. In the **Configure Ports Individually** section, select **+**, or select  for an existing port.
2. 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**.
3. 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.
4. Select **NEXT** to open the **VLAN** tab.
5. Select an existing VLAN from the  menu, or select **+** to create a new VLAN object.
6. Select **NEXT**, or select the **User Authentication** or **QoS** tab, and continue configuring the port.

For older Dell and SR-based devices, the taskflow includes the **User Authentication** tab. See [Configure User Authentication](#) on page 254.

See [Configure QoS Settings](#) on page 255.

Related Links

[Configure Individual Ports](#) on page 252

[Configure User Authentication](#) on page 254

[Configure QoS Settings](#) on page 255

Configure User Authentication

First configure the **Port Name & Usage** and **VLAN** tabs. See [Configure Port Details](#) on page 252.



Tip

These settings appear in the **Authorization** section of the **Summary** tab.

Use this task to configure the settings for a new port, on the **User Authentication** tab.



Note

The **User Authentication** tab is part of the taskflow for older Dell and SR-based devices.

1. Under **Authentication Options**, toggle **User Authentication** to **ON** or **OFF**.
2. Toggle **MAC Authentication** to **ON** or **OFF**.
3. Select an **Authentication Protocol** from the list.
4. Configure the settings for the additional tabs required for each selection:
The additional tabs depend on which authentication options you enable.

Table 58: Additional tabs

If you enabled	Configure these additional tabs
User Authorization only	• Radius Settings • User Profile
MAC Authorization only	Radius Settings
Both	• Radius Settings • Auth Priority • User Profile

- a. Select the **Radius Settings** tab, and configure the settings.

Table 59: Radius settings

Setting	Description
Default RADIUS Server Group	Select an existing RADIUS server group from the  menu, or select + . For more information, see RADIUS Authentication on page 144.
Apply RADIUS server groups to devices via classification	Select to use classification. For more information, see Configure Classification Rules on page 214.

- b. Select the **User Profile** tab, and configure the settings.

Table 60: User profile settings

Setting	Description
Default User Profile	Select an existing user profile from the  menu, or select  .
User profile to use when authentication fails	Select an existing user profile from the  menu, or select  .

- c. Select the **Auth Priority** tab, and use the up and down arrows to change the order of the authentication methods.
 5. Select **REVIEW** and verify the **Authorization** settings.
 6. Select the **QoS** tab, and continue configuring the port.
- See [Configure QoS Settings](#) on page 255.

Related Links

[Configure QoS Settings](#) on page 255

[Configure Port Details](#) on page 252

Configure QoS Settings

First configure [Configure Port Details](#) on page 252.



Tip

These settings appear in the **QoS** section of the **Summary** tab.

Use this task to configure custom QoS settings for a new port, on the **QoS** tab.

1. To customize the QoS settings, toggle **Use Custom QoS Settings** to **ON**.
If you toggle the setting **OFF**, go to Step .
2. Configure the **Quality of Service (QoS) Settings**.

Table 61: QoS settings

Setting	Description
QoS Traffic Class	
Trusted Traffic Source	a. Select this option to map all incoming traffic into the Extreme Networks classification system. b. Then select a marker: DSCP (Diffserve Codepoint) or 802.1p from the list.

Table 61: QoS settings (continued)

Setting	Description
Untrusted Traffic Source	- Select this option to map all incoming traffic into the Extreme Networks classification system. - Then select a classification system from the list.
Traffic Marking	- Select Mark the outgoing traffic with priority markers, to map Extreme Networks QoS classes to priority markers and mark outgoing traffic using. - Then select a marker: DSCP (Diffserve Codepoint) or 802.1p from the list. - Select For unmarked incoming traffic, use Extreme Networks class, and then select an Extreme Networks class from the list.

3. Select **NEXT**, or select the **Transmission Settings** tab, and continue configuring the port.

See [Configure Port Transmission Settings](#) on page 256.

Related Links

[Configure Port Transmission Settings](#) on page 256

[Configure Port Details](#) on page 252

Configure Port Transmission Settings

First, [Configure QoS Settings](#) on page 255.



Tip

These settings appear in the **QoS** section of the **Summary** tab.

Use this task to configure the settings for a new port, on the **Transmission Settings** tab.

1. Type the maximum transmission unit value for **MTU Settings**, to define the largest packet size that can be transmitted through your system.
2. For **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.
3. 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.
4. Select the **Speed** the switch port uses to communicate with the connected device.
5. Select **LLDP Transmit** to enable the switch to transmit LLDPDU frames.
6. Select **LLDP Receive** to enable the switch to receive LLDPDU frames.

7. Select **Client Reporting** to display learned switch port client MAC addresses on ExtremeCloud IQ monitoring screens.

When client reporting is disabled, client MAC addresses are not displayed. It is disabled when **CDP Receive** is turned off.

8. Select the **NEXT**, or select the **STP** tab, and continue configuring the port.

See [Configure STP Settings](#) on page 257.

Related Links

[Configure STP Settings](#) on page 257

[Configure QoS Settings](#) on page 255

Configure STP Settings

First [Configure Port Transmission Settings](#) on page 256.



Note

Extreme Networks and Dell EMC recommend that you enable STP for Dell EMC switches.

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**, 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.
 - **Disabled**: Turns off BPDU Protection.
4. If this port is an STP edge port, select a port priority for STP from the drop-down list. You can manually designate a port to act as a root bridge by assigning port priorities.
5. Toggle **BPDU Restrict** to **ON**.
6. For BPDU recovery timeout, input a time between 60-600 seconds.

**Note**

After the time expires ExtremeCloud IQ re-enables the port automatically.

7. Select **NEXT**, or select the **Storm Control** tab, and continue configuring the port. See [Configure Storm Control](#) on page 258.

Related Links

[Configure Port Transmission Settings](#) on page 256

[Configure Storm Control](#) on page 258

Configure Storm Control

First [Configure STP Settings](#) on page 257.

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. For **Thresholds**, select **Byte Based** or **Packet Based**.
3. For **Rate Limit Type**, select **Kbps** or **Percentage** if you selected **Byte Based**, and **PPS** if you selected **Packet Based**.

4. Type the **Rate Limit Value** for discarding traffic of the selected types.
5. Select **NEXT**, or select the **PSE** tab, and continue configuring the port.

See [Configure PSE Settings](#) on page 259.

Related Links

[Configure STP Settings](#) on page 257

[Configure PSE Settings](#) on page 259

Configure PSE Settings

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**.

Instant Port Profiles

The Instant Port Profiles (IPP) feature in ExtremeCloud IQ 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:

- Create an Instant Port Profile
- Create Instant Port Device Type

For more information about IPP, see [ExtremeCloud IQ Universal Switch Deployment Guide](#).

Related Links

[Configure an Instant Port Profile](#) on page 260

[Create an Instant Port Device Type](#) on page 261

Configure an Instant Port Profile

Add or edit an Instant Port Profile (IPP) in a switch template.

1. Go to **Configure > Network Policies** and select a device template for the switch.
2. On the switch template page, select **Port Configuration** and then choose one of the following actions:

Add a new IPP

Select , and then go to Step 3.

Edit a new IPP

Select an existing IPP from the drop-down menu, select  and then go to Step 3.

3. Configure the profile settings.

See [Instant Port Profile Settings](#) on page 260.

Related Links

[Instant Port Profile Settings](#) on page 260

[Delete an Instant Port Profile](#) on page 261

Instant Port Profile Settings

Configure the following Instant Port Profile (IPP) settings.

Table 62: IPP Settings

Field	Description
Name	Enter a Name for the IPP.
Description	Enter a Description for the IPP.
Non-Forwarding VLAN	From the menu, select a VLAN to use for the detection of attached devices; this VLAN will not forward traffic. The non-forwarding VLAN cannot be utilized within a port type assigned to the switch.

Table 62: IPP Settings (continued)

Field	Description
Default Port Type	From the menu, select the default port type: • Access Port—Use for a port connected to an individual host. • Trunk Port—Use for a port connected to a forwarding device such as an AP and switch that supports multiple VLANs. Ports assigned with an IPP inherit the selected port type settings, such as type, speed, STP, MAC locking, ELRP, and PSE port settings.
Non-Match Action	Select one of the options: • Non-Forwarding VLAN—Does not forward traffic for devices that do not match an assignment rule. • Use Default Port Type VLAN—Assigns the VLANs associated with the port type. 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. See IPP Device Type Settings on page 262

Related Links

[Configure an Instant Port Profile](#) on page 260

[IPP Device Type Settings](#) on page 262

Delete an Instant Port Profile

You can delete Instant Port Profiles (IPPs) that you no longer use.

1. Go to **Configure > Common Objects > Policy > Instant Port Profiles**.
2. Select the corresponding check boxes for the IPPs that you want to delete, and then select .

Create an Instant Port Device Type

Configure a Network Policy with a Switch Template and an Instant Port Profile (IPP).

The Instant Port device type is part of the IPP. When a device connects to a switch port, ExtremeCloud IQ 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 the settings.
See [IPP Device Type Settings](#) on page 262.
3. Select **Save** to commit changes, or select **Cancel**.

Related Links

[IPP Device Type Settings](#) on page 262

[Configure an Instant Port Profile](#) on page 260

IPP Device Type Settings

Configure the following Instant Port Profile (IPP) device type settings.

Table 63: IPP Device Type Settings

Field	Description
Name	Enter a Name for the device type.
Description	Optionally, enter a Description of the device type.

Table 63: IPP Device Type Settings (continued)

Field	Description
Match Category	Use the drop-down menu to choose a Match Category. Options are: • 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. • 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. • LLDP Capability — Matches the device based on the LLDP capability from the source LLDP PDU. Options are: • 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. If you choose MAC Learning or LLDP Src MAC, configure the following fields: • MAC Address/OUI ◦ Select  and choose a MAC address. ◦ Select  to add a custom MAC Address or MAC OUI. ◦ Select  to edit a custom MAC Address or MAC OUI. • MAC Mask ◦ Enter a custom MAC mask format. ◦ Select the Edit MAC Mask check box, then edit the entry in the MAC Mask field. If you choose LLDP Capability, use the drop-down menu to choose one of the following options: • Avaya Phone • Gen Tel Phone • Router • Bridge • Repeater • WLAN Access Pt • Docsis Cable Ser • Station Only • Other If you choose LLDP Src MAC + LLDP Capability, configure the parameters as described above.
PORT USAGE tab	
Port Usage	Select a Port Usage option, as follows: • Access Port • Trunk Port (802.1Q VLAN Tagging) • Phone with a Data Port
VLAN tab	

Table 63: IPP Device Type Settings (continued)

Field	Description
VLAN	This field appears if Port Usage is configured as Access Port. Choose from the following actions: • Select  and choose a VLAN. • Select  to add a custom VLAN. Optionally, select the Apply VLANs to devices using classification check box. • Select  to edit a custom VLAN.
Native VLAN	This field appears if Port Usage is configured as Trunk Port (802.1Q VLAN Tagging). Choose from the following actions: • Select  and choose a Native VLAN. • Select  to add a custom Native VLAN. Optionally, select the Apply VLANs to devices using classification check box. • 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: • Select  and choose a Voice VLAN. • Select  to add a custom Voice VLAN. Optionally, select the Apply VLANs to devices using classification check box. • 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: • Select  and choose a Data VLAN. • Select  to add a custom Data VLAN. Optionally, select the Apply VLANs to devices using classification check box. • Select  to edit a custom Data VLAN.
STORM CONTROL tab	
Broadcast	Select Broadcast to include traffic that is forwarded to all destinations simultaneously.
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 for the selected types.

Related Links

[Create an Instant Port Device Type](#) on page 261

Instant Secure Port Profiles

Use Instant Secure Port Profiles (ISPP) to configure user authentication and MAC authentication per port and to specify a radius server to use.

**Note**

The ISPP feature requires a Extreme Platform ONE Security subscription. If you do not have a Extreme Platform ONE Security subscription, the **Instant Secure Port Profiles** section under **Switch Settings** is not visible.

For additional information about ISPP, see [ExtremeCloud IQ Universal Switch Deployment Guide](#).

Universal Port Stacking Support Mode

Switch Engine 4000 Series hardware allows for the configuration of Universal Port Stacking Support Mode. When Stacking Support Mode is **disabled**, Universal Ports U1 and U2 will operate as non-stacking ports. Once stacking ports are no longer defined as stacking, then all ExtremeCloud IQ supported port configurations apply, including configuration by port type and configurations associated with ports such as Instant Port configurations.

**Note**

Changing the stacking support mode will require a reboot to be performed during configuration update.

Universal Port Mode

Stacking Support Mode



When Stacking Support Mode is disabled, Universal Ports U1 and U2 will operate as non-stacking ports. Changing the stacking support mode will require a reboot to be performed during configuration update.

CANCEL

APPLY

Figure 4: Universal Port Stacking Support Mode

To enable or disable Universal Port Stacking Support Mode:

1. Go to **Configure > Network Policies**, to edit or create a new policy.
2. Select **Switch Template**.
3. From the Details page, select **Switching > Port/VLAN Configuration**.
4. Select  beside the Universal Ports.
5. Choose your Stacking Support Mode with the **Toggle**.
6. If the device is a Switch Engine 4120 series, additional channelization options appear. Select the Channelization options for both Universal Ports.



Note

The default value selected for the 4120 SKUs is 1x100G.

7. Select **Apply**.



Note

Universal Port Stacking Support Mode can also be configured at the device-level, within the **Port / VLAN Configuration** page. Device level configuration overrides the template configuration.

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.

1. Select the ports you want to aggregate on the switch template, and then select **Assign > Advanced Actions > Aggregate**.
2. Enter an optional description.
3. Add or remove ports from the LAG.
4. For **Inherit Port Settings**, select the appropriate settings from the drop-downs.

**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.

Continue configuring the switch template.

Configure Switch STP Settings

Before you begin this task, create or modify a switch template.

By default, STP is disabled. Use this task to toggle it on and configure the settings. Extreme Networks and Dell EMC recommend you enable STP for Dell EMC switches.

1. Toggle **STP (Spanning Tree Protocol)** to **ON**, and 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.

2. 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.

3. 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.

Assign an sFlow Receiver to a Switch Template

Before you can assign an sFlow receiver to a switch template, you must first configure an sFlow receiver as a common object. See [Configure an sFlow Receiver](#) on page 358.

**Note**

sFlow is only available for SR/Dell switch models.

Use the following steps to assign sFlow receivers that you have configured as common objects to switch templates.

1. Go to **Configure > Common Objects > Policy > Switch Template**.
2. Select an existing switch template and then select , or select  to create a new template.
3. Select the **sFlow Receivers** tab.
The sFlow Receivers feature is available only for supported switches.
4. Type a **Name** for the template.
5. Select .
6. Select a receiver object from the **Available sFlow Receivers** menu.
7. Enable **sFlow Receiver**.
8. Enable **Interface Packet Sampling**.
9. Move interfaces you want to sample from the **Available** column to the **Selected Interfaces** column using the arrows.
10. Enable **Counter Polling**.
11. Move interfaces you want polled from the **Available** column to the **Selected Interfaces** column.
12. Select **Save**.
13. Select **Save sFlow Receivers**.

Related Links

[Configure an sFlow Receiver](#) on page 358

Routing

The Routing feature in ExtremeCloud IQ allows for configuration of IPv4 forwarding, DHCP Relay, and Static Routing for Universal Hardware running Switch Engine or x435 devices.

Network Allocation within the Network Policy Switching Section allows for an IPv4 Subnetwork to be defined with a VLAN created from VLAN attributes with a defined local IP Address Subnetwork space, IP address of the IPv4 interface, and DHCP Relay Server configuration.

SWITCHING

Common Settings

Switch Engine and EXOS

Fabric Engine and VOSS

Switch Settings

Port Types

VLAN Attributes

Instant Port Profiles

Switch Templates

Routing

→ Network Allocation

Network Allocation

Network Allocation allows the creation of IP Subnetwork configuration. A subnetwork with a selected VLAN can be applied to a device within the Routing section.
Note: A VLAN defined within Instant Port Profiles as Non-Forwarding cannot be used to create a subnetwork.

Name	Description	IPv4 Subnetwork	Clients Per Subnet	DHCP Relay	VLAN Name	VLAN ID	VLAN Used By
Office		10.1.0.0/24	254	DHCP-Relay	v800	800	1
Test		10.1.0.0/16	65534	DHCP-Relay	v802	802	1

Routing

Routing allows an IP Subnetwork to be assigned to a device.
Note: A VLAN defined within Instant Port Profiles as Non-Forwarding cannot be used to create a routing interface.

Device Serial Number	Device Host Name	IPv4 Address / Subnet Mask	IPv4 Subnetwork Allocation Name	VLAN Name	VLAN ID	IPv4 Forwarding	Routing Instance
PA082323G-00001	4220-4MW-39P-4X-SwitchEngine	10.1.0.1/24	Office	v800	800	Disabled	VR-Default
1924G-00128	X435-24T-45-Floor-1	10.1.255.1/16	Test	v802	802	Enabled	VR-Default
00496C6022	X435-8P-2T-W	10.1.255.253/16	Test	v802	802	Enabled	VR-Default

Static Routes

Static Routes allows a static route to be assigned to a device.

Static Route Name	Device Serial Number	Device Host Name	Routing Instance	Destination Subnetwork	Next Hop IP	Ping Protection	Metric
Name for Static Route	1924G-00128	X435-24T-45-Floor-1	VR-Default	10.1.1.0/24	10.1.0.1	ON	1

EXIT

NEXT

Figure 5: Network Allocation

The IPv4 interface assigned to a device allows the ability to define IPv4 forwarding, VLAN loopback, and DHCP relay assignment.

IPv4 Static routes can also be defined with the destination subnetwork, next hop IP, next hop IP ping protection, and metric.

Network Allocation

Network Allocation allows the creation of IP subnetwork configuration. A subnetwork with a selected VLAN can be applied to a device within the Routing section.



Note

A VLAN defined within Instant Port Profiles as Non-Forwarding cannot be used to create a subnetwork.

On the **Network Allocation** page, you can add, edit, or delete Network Allocation configurations. The table includes the following parameters:

- Name
- Description
- IPv4 Subnetwork
- Clients Per Subnet
- DHCP Relay
- VLAN Name
- VLAN ID
- VLAN Used By

To configure Network Allocation:

1. Go to **Configure > Network Policies**.
2. Create or select a Network Policy.

3. Select **Switching > Routing > Network Allocation**.
4. Select  to add or  to edit.
5. Enter the IPv4 Network Allocation Attributes according to the table below:

Table 64: Network Allocation Attributes

Field	Description
VLAN Attribute (Mandatory)	Only VLAN attributes created from VLAN Attributes tab within Switching/Routing section of the same policy can be selected from the drop-down list. Note: The user can create multiple entries for the same VLAN ID within the same policy.
Name (Mandatory)	The name of your subnetwork.
Description (Optional)	A description of your subnetwork.
Local IP Address Space (Mandatory)	Define the local IP address space using CIDR notation, such as 10.1.0.0/16. This must be a subnet address. The user can create multiple entries for different VLAN IDs with overlapping subnet space within the same policy.
Clients Per Subnet (Read-only)	Shows the number of clients per subnetwork.
Select One	- Use the first IP address of the local IP address space for the IPv4 interface - Use the last IP address of the local IP address space for the IPv4 interface Note: Use the first/last IP address of the local IP address space as default value when creating an IPv4 interface using this subnetwork.
Enable DHCP Relay	Enables/disables DHCP Relay. If enabled, the user can select, create or edit a DHCP Relay Common Object.

**Note**

The entries from the Network Allocation table don't generate delta by themselves. They must be used to create entries in Routing table in order to generate delta.

Configure IPv4 Network Allocation

New Subnetwork

Select VLAN associated with network allocation

VLAN Attribute * 3 / VLAN-3

Name * Subnet3

Description

Local IP Address Space * 10.3.0.0/16
Example: 10.1.0.0/16

Clients Per Subnet 65534

☐ Use the first IP address of the local IP address space for the IPv4 interface

☒ Use the last IP address of the local IP address space for the IPv4 interface

☐ Enable DHCP Relay

CANCEL
SAVE

Figure 6: Adding a new subnetwork

Network Allocation | Routing

Routing allows an IP subnetwork to be assigned to a device.



Note

A VLAN defined within Instant Port Profiles as Non-Forwarding cannot be used to create a routing interface.

To configure routing:

1. Go to **Configure > Network Policies**.
2. Create or select a Network Policy.
3. Select **Switching > Routing > Network Allocation** and scroll to the Routing table.
4. Select + to add or ✎ to edit.

5. Enter the Routing Attributes according to the table below:

Table 65: Routing Attributes

Field	Description
Device (Mandatory)	Select a Device from the drop-down menu. Only standalone or stack EXOS/ Switch Engine switches with this policy assigned can be selected.
Network Allocation (Mandatory)	Select a Network Allocation from the drop-down menu. Note: You cannot assign a device to the same subnetwork twice or multiple subnetworks referencing the same VLAN ID or subnetworks with overlapping subnet space.
VLAN Attribute (Read-only)	Select a VLAN Attribute from the drop-down menu. Note: This field displays <VLAN ID> / <VLAN name> / <VLAN attribute created from>. For IPv4 interfaces created from a network policy, it will display the VLAN ID and VLAN name from the selected subnetwork and "POLICY" as the source for the VLAN attribute.
IPv4 Address / Subnet Mask (Mandatory)	Shows the assigned IP Address, such as 10.1.0.0/16. Note: IPv4 address must be a host address within the same subnet space as the selected subnetwork.
Routing Instance (Read-only)	Shows the Routing Instance. Note: IPv4 interfaces can only be created within VR-Default.
IPv4 Forwarding	Enables/disables IPv4 forwarding.
VLAN Loopback	Enable or Disable VLAN Loopback.
DHCP Relay (Read-only)	DHCP Relay configured within the selected subnetwork or allows overriding DHCP Relay from subnetwork with a custom configuration.

Static Routes

Static route configuration in a Network Policy allows you to create one static route entry and assign that static route entry to multiple devices. The device is required to have the corresponding directly connected interface present in the routing section.

If adding a static route configuration at device-level, then the device is still required to have a corresponding directly connected interface present in the device-level routing section.

To configure Static Routes:

1. Go to **Configure > Network Policies**.
2. Create or select a Network Policy.
3. Select **Switching > Routing > Network Allocation** and scroll to the Static Routes table.
4. Select  to add or  to edit.
5. Enter the Static Route Attributes according to the table below:

Table 66: Static Route Attributes

Setting	Description
Device (Mandatory)	Select a Device from the drop-down menu . Only standalone or stack EXOS/Switch Engine switches having this policy assigned can be selected.
Static Route Name (Mandatory)	Enter the name of the Static Route.
Destination Subnet (Mandatory)	Enter the desired subnet address, such as 10.1.0.0/16.
Next Hop IP (Mandatory)	Enter the desired IP Address for the next Hop, such as 123.321.132.312. Must be in the same subnetwork with at least one of the IPv4 interfaces configured for the device. Next hop IP cannot be configured with the same IPv4 address as that of the interface configured for device.
Next Hop IP Ping Protection (Mandatory)	Enable or Disable Next Hop IP Ping Protection. Note: Enabling Ping Protection will generate a Ping Protection Status tool tip when viewing your device within Manage > Devices > Monitoring > Routing .
Metric (Mandatory)	Enter your desired metric value from 1 to 255.
Routing Instance (Read-only)	Shows the Routing Instance. Note: IPv4 static routes can only be created within VR-Default.

You cannot configure the same static route twice for the same device. A static route is defined by the following parameters: destination subnetwork, next hop IP, and routing instance.

IPv4 Static Routes

Failed to add IPv4 static route: duplicate static route

Device *

2037G-00255 - 5420F-245-4XE-SwitchEngine

Static Route Name *

Route3

Destination Subnetwork *

12.1.0.0/16

Example: 10.1.0.0/16

Next Hop IP *

10.2.0.12

Next Hop IP Ping Protection

☐

Metric *

1

Routing Instance

VR-Default

CANCEL

SAVE

By selecting a device when creating an IPv4 static route, routing feature allows device-level configuration to be performed from a network policy. The entries from Static Routes table will generate delta only for those devices selected when the IPv4 static routes have been created.

- Device-level IPv4 static route configuration can also be performed also from page of each device which has a policy assigned: go to **Manage > Devices** and select the supported device. Select **Configure > Network Allocation > Routing Configuration**.



Note

All IPv4 static routes created from a network policy for a specific device are displayed and can be edited also from the device-level page of that device and vice-versa.

7. Since every IPv4 static route is linked to an IPv4 interface, when deleting an IPv4 interface all static routes linked to, you must confirm the actions.

Routing

Routing allows an IP Subnetwork to be assigned to a device. Ensure that each switch is assigned to the network policy before initiating network allocation.
Note: A VLAN defined within Instant Port Profiles as Non-Forwarding cannot be used to create a routing interface.

+ ✎ 🗑

Device Serial Number	Device Host Name	VLAN ID	IPv4 Forwarding	Routing Instance
☐ 2037G-00123	E-1-0123	2	Disabled	VR-Default
☐ 2037G-00123	E-1-0123	3	Disabled	VR-Default
☒ 2037G-00255	5420F-245-4XE-SwitchEngine	2	Disabled	VR-Default
☐ 2037G-00255	5420F-245-4XE-SwitchEngine	3	Enabled	VR-Default
☐ 2037G-00255	5420F-245-4XE-SwitchEngine	5	Enabled	VR-Default
☐ 2037G-00255	5420F-245-4XE-SwitchEngine	6	Enabled	VR-Default

Multiple static routes might be associated with the selected interfaces. Do you want to continue deleting?

NO YES

Static Routes

Static Routes allows a static route to be assigned to a device.

+ ✎ 🗑

Static Route Name	Device Serial Number	Device Host Name	Routing Instance	Destination Subnetwork	Next Hop IP	Ping Protection	Metric
☐ Route2	2037G-00255	5420F-245-4XE-SwitchEngine	VR-Default	12.1.0.0/16	10.2.0.12	ON	10
☐ Route3	2037G-00255	5420F-245-4XE-SwitchEngine	VR-Default	13.1.0.0/16	10.2.0.13	OFF	1

Routing

Routing allows an IP Subnetwork to be assigned to a device. Ensure that each switch is assigned to the network policy before initiating network allocation.
Note: A VLAN defined within Instant Port Profiles as Non-Forwarding cannot be used to create a routing interface.

+ ✎ 🗑

Device Serial Number	Device Host Name	IPv4 Address / Subnet Mask	IPv4 Subnetwork Allocation Name	VLAN Name	VLAN ID	IPv4 Forwarding	Routing Instance
☐ 2037G-00123	E-1-0123					Disabled	VR-Default
☐ 2037G-00123	E-1-0123					Disabled	VR-Default
☒ 2037G-00255	5420F-245-4XE-SwitchEngine					Disabled	VR-Default
☐ 2037G-00255	5420F-245-4XE-SwitchEngine					Enabled	VR-Default
☐ 2037G-00255	5420F-245-4XE-SwitchEngine					Enabled	VR-Default
☐ 2037G-00255	5420F-245-4XE-SwitchEngine	10.6.0.1/16	N/A	VLAN-6	6	Enabled	VR-Default

You are going to delete '2' static routes. Are you sure you want to continue deleting all associated routes?

NO YES

Static Routes

Static Routes allows a static route to be assigned to a device.

+ ✎ 🗑

Static Route Name	Device Serial Number	Device Host Name	Routing Instance	Destination Subnetwork	Next Hop IP	Ping Protection	Metric
☐ Route2	2037G-00255	5420F-245-4XE-SwitchEngine	VR-Default	12.1.0.0/16	10.2.0.12	ON	10
☐ Route3	2037G-00255	5420F-245-4XE-SwitchEngine	VR-Default	13.1.0.0/16	10.2.0.13	OFF	1



Note

When editing an IPv4 static route, only Next Hop IP Ping Protection and Metric fields can be changed. To change the other fields, create a new static route after deleting the existing one.

8. When editing an IPv4 interface which is linked to an IPv4 static route (next hop IP of a static route is in the same subnet as the IPv4 address of the routing interface), IPv4 address field cannot be changed anymore. The rationale behind this restriction is to not invalidate existing static routes.



Note

The default route defined within Management Interface Settings using Static Address option is displayed as read only in IPv4 static routes tables from both the device-level configuration page and network policy. In the device-level configuration page, the default static route name has a hyperlink to Management Interface Settings from the Device Configuration tab.



Note

When creating an IPv4 static route, next hop IP cannot be default gateway defined within Management Interface Settings using Static Address option.

IPv4 Static Routes ×

Failed to add IPv4 static route: next hop IP cannot be default gateway (loopback address '10.106.0.254'). ×

Static Route Name *

Destination Subnetwork *
Example: 10.1.0.0/16

Next Hop IP *

Next Hop IP Ping Protection ☐

Metric *

Routing Instance

CANCEL SAVE

Switch Stacks

ExtremeCloud IQ can manage switch stacks. You can instantly create a Switch Engine switch stack or manually create it.

- To instantly create Switch Engine switch stacks, see [Instantly Create a Switch Engine Stack](#) on page 276.
- To manually create a switch stack, see [Manually Create a Switch Engine Stack](#) on page 277.

Instantly Create a Switch Engine Stack

To instantly create a stack, onboard the switches into ExtremeCloud IQ via the ExtremeCloud IQ MobileApp. Unbox the switches, connect the stacking/power/uplink cables, and push the **Mode** button until the **STK LED** lights up. Depress the **Mode** button for at least 5 seconds. All of the front panel ports LED will flash. The stack forms

automatically, all the slots reboot, and ExtremeCloud IQ detects the newly formed stack.

Use this task to instantly configure a Switch Engine switch stack in ExtremeCloud IQ.

1. Go to **Manage > Devices**.
2. Find the new stack in the **Devices List** and select its check box.
3. In the **Template** column, select **Assign/Create Template**.
4. Select the **Create template based on currently selected device**.
5. Select an existing stack template from the dropdown.
6. Select **Assign**.

The assigned template now displays in the **Policy** column.

Manually Create a Switch Engine Stack

The following prerequisites for creating a switch stack template must be met:

- You must have an ExtremeCloud IQ license key for every switch in the physical stack. As a best practice, onboard keys for the primary, then the standby, and then the remaining stack members.
- Onboard each switch. Ensure that you have followed the procedures in [Configure Switch Templates](#) on page 244 before you complete the cable connections and power on the switches to form the physical stack.
- Ensure the switches are cabled and powered on in the required stack configuration order (primary, standby, and members).

After you have onboarded the switches in your stack, you must create a stack template in ExtremeCloud IQ that exactly matches the physical stack.

1. Select the add icon.
2. Select the switch models for the switch stack from the drop-down list.
3. Enter a name for your template and select the first switch model to add from the drop-down list.
4. Select **Add** to add each switch to the stack.
5. Continue to add switches to the template until you have added all of the switches in your physical stack.

Make sure the template switch numbers match the numbers of the physical switches.

6. Select **Save**.

Push a network policy to the stack. For more information, see [Manage Switch Stacks](#) on page 277.

Manage Switch Stacks

Create a switch stack template. See [Switch Stacks](#) on page 276.

After you create a template for a stack, you can edit each stack member switch template to reconfigure the ports. If you change your physical stack, add or remove switches, you must create a new stack template to match the new physical stack.

When you create a new stack template, you must also perform a configuration update. If the template does not match the physical stack exactly, the configuration update will fail. The following are examples of common changes that can occur to a stack, with the actions you need to take for each example.

1. When the primary and standby switches reverse roles:

If the primary and standby switches change their roles (for example, as the result of a CLI command), after a delay of approximately 3 minutes, the Devices List updates to show the new primary and standby switches. To display the Devices List, navigate to **Manage > Devices**. See [Devices](#) on page 412 for more information.

2. If you remove the primary switch from a stack, the stack retains the MAC address of the removed primary, resulting in duplicate MAC addresses for the stack and the standalone former primary switch.

If you need to remove the primary switch from a stack, you must perform the following steps to prevent duplicate MAC addresses:

- a. Delete the entire stack from ExtremeCloud IQ.
- b. Perform the following CLI command:

no member {n} where *n* is the unit number of the primary switch.

- c. Enter the serial numbers of the stack members and the standalone switch in ExtremeCloud IQ.
 - d. Recreate the stack template to reflect the change.
3. Add a new switch to an existing stack:

To add a new switch to an existing stack, click **Add** underneath the template name, and add another device to the stack.

4. Add an existing switch to a stack:

You must cable the switch to the physical stack, then use the previous step to add an existing switch to a stack.

5. Remove a switch from one stack and add it to another stack:

To move a switch from one stack to another stack, you must disconnect the switch from the original stack, then re-cable it in the new stack. Create two new stack templates, one to match the diminished stack configuration, and one to match the new stack configuration.

6. When a stack member goes offline:

If a stack member is offline (is powered down but remains a member of the stack), ExtremeCloud IQ updates the Devices List to show that member as **Disconnected**. When the offline stack member comes back online, the Devices List is updated to show it as **Connected**. To display the Devices List, navigate to **Manage > Devices**.

7. Manage a switch that has been uncabled from a stack:

If a stack member is uncabled, ExtremeCloud IQ updates the Devices List to show that member as **Disconnected**. This action alerts you that there might be a problem with this switch. If this switch has been accidentally or inadvertently uncabled, you can then re-cable it. ExtremeCloud IQ updates the Devices List to show the switch is working correctly.

8. Remove a switch from a stack in ExtremeCloud IQ:
 - a. To remove stack members from the ExtremeCloud IQ database (but not from the actual physical stack), select **Remove Stack Members** from the **Actions** drop-down list in the Devices List window.
 - b. Select the check box for the stack member or members that you want to remove and then select **Remove**.

See [Devices](#) on page 412 for more information.



Note

If you accidentally remove a primary stack member, you have only removed it from ExtremeCloud IQ. It remains as the operational physical primary of the stack, and you can onboard it again.

9. Split stacks:

When you reconfigure a physical stack so that some of the switches become independent stacks, you create a split stack. If no CLI commands are issued to explain the change, the stack still reports having the original number of switches, with the removed switches showing as not connected. For example, Stack A has Switches 1, 2, 3, 4, 5, and 6. Then someone creates a split stack by cabling Switches 5 and 6 into their stack, Stack B. At this point, both Stack A and Stack B think that all six switches belong to them. A show switch command on Switch 1 shows six members (two with a management status of **Disconnected**). A show switch command on Switch 5 shows six members (four with a management status of **Disconnected**).

If the primary of the new smaller 2-member stack tries to communicate with ExtremeCloud IQ as an independent stack, ExtremeCloud IQ ignores this communication because it still recognizes the service tag for this switch as belonging to the original stack. Any communication from this switch is ignored because this new primary switch has a different MAC Address. If the 3rd and 4th stack members rejoin the original stack, they again display as valid and healthy stack members in the Devices List. .

- a. If you want the stacks to remain split, in the Devices List, select **Remove Stack Members** from the **Actions** drop-down list.
- b. Select the check boxes for the stack members to remove from the stack, and select **Remove**.

The switches you removed display in the Devices List as a separate stack. See [Devices](#) on page 412 for more information.

If necessary, create a new switch stack template to reflect any of the above changes.

Configure Switch Device Template Advanced Settings

Create or edit a switch template.

ExtremeCloud IQ can update device firmware and reboot the device during onboarding.

1. Select the **Advanced Settings** tab.

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 302.

Complete configuring the device template.

Configure URL Filtering Rules

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 filters to that rule, and then associate the rule with a user profile.

1. Go to **Configure > Common Objects > URL Filtering**.
2. Select the add icon.
3. Enter a name for the rule.
4. Enter an optional description.
5. Select an existing URL filter from the table.

To create a new URL filter, select the add icon above the table.



Note

Allowed lists and blocked lists can be applied to both HTTP and HTTPS, but there are some differences. For HTTPS, you can only get the domain name (for example, `www.google.com`), so if you configure the URL as `www.google.com/xxxx`, HTTPS cannot match it, but if you configure the URL as `www.google.com` or `*.google.com`, then HTTPS can match it. This does not apply to HTTP.

6. Select the **Whitelist** tab.
 - a. Manually enter up to 32 allowed URLs.
 - b. You can also import a `.csv` file containing up to 32 URLs by dragging the file into the field or searching for an existing `.csv` 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
```

7. Select the **Blacklist** tab.
 - a. Manually enter up to 32 allowed URLs.

You can also import a .csv file containing up to 32 URLs by dragging the file into the field or searching for an existing .csv file.
8. Select the **Categories** tab.
9. Choose the categories this rule blocks.
10. Schedule when this filter is actively applied to the rule.
 - a. Select an existing **Schedule**.
 - b. Select **Add** to create a new **Schedule**.
 - Enter a name and an optional description.
 - Select one time or recurring.
 - For one time, enter a start and end date and time.
 - For recurring, choose to have this report generated daily, or customize using the day and time range option. You can also add multiple time ranges to this schedule. To limit the recurrence of this schedule, select the calendar icons to insert dates into the **Start** and **End** fields.
 - c. Select **Save Schedule**.
11. Select **Save Detail**.
12. Continue adding filters if needed.
13. Select **Save URL Rule**.
14. Select user profiles to associate with this rule or create new profiles.

To create a new user profile, see [Add a User Profile](#) on page 281.

Add this **URL Filtering Rule** to a network policy **Router Settings**.

Add a User Profile

Use this task to create user profiles that 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.

1. Go to **Configure > Common Objects > Policy > User Profiles**.
2. Select **+**.
3. Type a **Name** for the profile.
4. Select **VLAN** or **VLAN Group** for the profile.
5. Select a VLAN or VLAN group from the menu, or select **+**.

See [Configure VLAN Settings](#) on page 156 for more information.
6. On the **Security** tab, apply IP or MAC firewall rules.

For more information, see [Configure Security | User Profile](#) on page 282.
7. On the **Traffic Tunneling** tab, enable generic routing encapsulation (GRE) traffic tunneling for a user profile.

For more information, see [Configure User Profile Traffic Tunneling](#) on page 283.

8. On the **QoS** tab, set rate limits and traffic forwarding rules for each traffic class.
For more information, see [Configure QoS | User Profile](#) on page 284.
9. On the **Availability Schedule** tab, define user profile availability for specific dates, days, and times.
For more information, see [Configure an Availability Schedule | User Profile](#) on page 285.
10. On the **Client SLA** tab, enable devices to monitor client throughput and take action if the actual throughput is below the targeted minimum level.
For more information, see [Configure Client SLA | User Profile](#) on page 286.
11. On the **Date/Time Limit** tab, configure access restrictions for users based on the user's assigned profile.
For more information, see [Configure Access Restrictions | User Profile](#) on page 287.
12. Select **Save User Profile**.

Related Links

[Configure VLAN Settings](#) on page 156
[Configure Security | User Profile](#) on page 282
[Configure User Profile Traffic Tunneling](#) on page 283
[Configure QoS | User Profile](#) on page 284
[Configure an Availability Schedule | User Profile](#) on page 285
[Configure Client SLA | User Profile](#) on page 286
[Configure Access Restrictions | User Profile](#) on page 287

Configure Security | User Profile

First create a new user profile, or select an existing user profile to edit. Go to:

Configure > Network Policies or to

Configure > Common Objects > Policy > User Profiles.

Use this task to apply IP or MAC firewall rules to a user policy.

1. On the **SECURITY** tab, 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 a **Name** for the firewall rule.
 - 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. Select an existing IP firewall rule or select the add icon to create a new rule.
See [Add IP Firewall Policies](#) on page 303.

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 304.
4. Continue configuring the user profile, or select **SAVE USER PROFILE**.

Related Links

[Add IP Firewall Policies](#) on page 303

[Add MAC Firewall Policies](#) on page 304

[Add a User Profile](#) on page 281

Configure User Profile Traffic Tunneling

First create a new user profile, or select an existing user profile to edit. Go to:

Configure > Network Policies or to

Configure > Common Objects > Policy > User Profiles.

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.

Configure the following options based on your tunnel policy requirements. These options are mutually exclusive.

1. On 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.
To add a new IP address or host name, see [Configure IP Objects and Host Names](#) on page 294.
- b. **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 and Host Names](#) on page 294.
- 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.
To add a new IP address or host name, see [Configure IP Objects and Host Names](#) on page 294.
 - b. **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 156.
 - c. **Tunnel Mode Access Mode:** type, select, edit, or add the VLAN ID.
To add a VLAN ID, see [Configure VLAN Settings](#) on page 156.
 - d. **Tunnel Failover:** type, select, edit, or add the IP address or host name of the secondary GRE tunnel endpoint. The secondary tunnel is used automatically if the primary tunnel goes down and traffic fails back to the primary tunnel when it is available.
 - e. **Keep Alive Interval:** Enter the interval (in seconds) used to monitor the failover tunnel.
 - f. **Keep Alive Retries:** Enter the number of retry attempts before the failover tunnel is considered down.
6. **Tunnel Concentrator:** select up to three tunnel concentrator services to act as the Primary (required) Secondary (optional) and Tertiary (optional) tunnel destinations.
- You can add a new Tunnel Concentrator service by selecting , or select  to modify an existing instance. For more information, see [Configure Tunnel Concentrator Services](#) on page 352.
7. Continue configuring the user profile, or select **SAVE USER PROFILE**.

Related Links

[Configure IP Objects and Host Names](#) on page 294
[Configure VLAN Settings](#) on page 156
[Configure Tunnel Concentrator Services](#) on page 352
[Add a User Profile](#) on page 281

Configure QoS | User Profile

First create a new user profile, or select an existing user profile to edit. Go to:

Configure > Network Policies or to

Configure > Common Objects > Policy > User Profiles.

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 318.
7. Continue configuring the user profile, or select **SAVE USER PROFILE**.

Related Links

[Configure Marker Maps](#) on page 318

[Add a User Profile](#) on page 281

Configure an Availability Schedule | User Profile

First create a new user profile, or select an existing user profile to edit. Go to:

Configure > Network Policies or to

Configure > Common Objects > Policy > User Profiles.

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.

1. On the **AVAILABILITY SCHEDULE** tab, turn on **Availability Schedule**.

2. Select  and configure the settings.
See [Schedule Settings](#) on page 243.
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 119.

Related Links

[Schedule Settings](#) on page 243

[Configure Enterprise SSID Authentication](#) on page 119

[Add a User Profile](#) on page 281

Configure Client SLA | User Profile

First create a new user profile, or select an existing user profile to edit. Go to:

Configure > Network Policies or to

Configure > Common Objects > Policy > User Profiles.

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 are not getting the expected level of throughput, you can see the results in graphs in the ExtremeCloud IQ 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 Extreme Networks devices are being 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 281

Configure Access Restrictions / User Profile

First create a new user profile, or select an existing user profile to edit. Go to:

Configure > Network Policies or to

Configure > Common Objects > Policy > User Profiles.

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 281

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

[Add Application Sets](#) on page 288

[Client Mode Profiles](#) on page 288

[Configure DHCP Servers and DHCP Relay Agents](#) on page 291

[Configure a DNS Service](#) on page 293

[Configure IP Objects and Host Names](#) on page 294

[Configure a MAC Object and MAC OUI](#) on page 298

[Configure a Notification Template](#) on page 299

[Configure OS Objects](#) on page 300

[Configure VLAN Settings](#) on page 156

[VLAN Group Object Settings](#) on page 158

[Configure Supplemental CLI](#) on page 302

Add Application Sets

Along with predefined sets of Layer 7 applications, ExtremeCloud IQ allows administrators to define sets of custom applications. An admin can choose to identify multiple sets of applications and feed them through an SD-WAN route group to support application-based routing policies. Use this task to create one or more custom application sets. Application sets are available as common objects for all SD-WAN routing policies.

1. Go to **Configure > Common Objects > Basic > Application Sets**.
2. 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.
Search results appear in the **Application Name and Category table**.
6. In the **Application Name and Category table**, select applications for your application set.
ExtremeCloud IQ automatically adds your selections to the **Selected Applications** box.
7. Select **SAVE**.

Related Links

- [Applications](#) on page 531
- [Applications List](#) on page 532
- [Add a Custom Application](#) on page 533

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.

Go to the **Client Mode Profiles** page using one of the following navigation paths:

- **Configure > Common Objects > Policy > AP Template > Device Configuration > Wireless Interfaces > Client Mode > Client Mode Profile**
- **Configure > Common Objects > Basic > Client Mode Profiles**

The **Client Mode Profiles** page includes:

- A list of Client Mode Profiles.
- Tools that allow users to manage Client Mode Profiles.

By default, the **Client Mode Profiles** window displays all configured profiles in tabular form. [Table 67](#) describes the type of information displayed under each column and the actions that a user can employ.

Table 67: Client Mode Profile List Column Headings

Column Heading	Description
Name	Displays the Name assigned to the Client Mode Profile.
Description	Displays the Description assigned to the Client Mode Profile.
Local Web	Indicates the status of Enable Local Web Page option. Possible values are On or Off .
DHCP Server Scope	Displays the reserved IP address or the first in a range of IP addresses used for DHCP client connections.
Used By	Identifies the number of Device Templates currently using a Client Mode Profile. Hover over the number to view the list of Device Templates.

Related Links

[Manage Client Mode Profiles](#) on page 289

[Configure a Client Mode Profile](#) on page 289

[Configure a Client Mode AP Profile using a Wired Connection and a Device Template](#) on page 126

Manage Client Mode Profiles

Use this task to manage Client Mode Profiles.

1. Go to **Configure > Common Objects > Basic > Client Mode Profiles**.
2. Choose from the following actions:

- To add a new Client Mode Profile, select .
- To edit a Client Mode Profile, select the profile in the list, then select .
- To clone a Client Mode Profile, select the profile in the list, then select .

In the **Clone** dialog, enter a new profile name in the **Save As** field, then select **CLONE**.

- To delete a Client Mode Profile, select the profile from the list, then select .

Related Links

[Client Mode Profiles](#) on page 288

Configure a Client Mode Profile

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. As a best practice, use a wired interface to configure client-mode APs. The wired configuration process is much faster than with a wireless backhaul.

Use this task to configure a Client Mode Profile.

1. Go to **Configure > Common Objects > Basic > Client Mode Profiles**.
2. Select an existing Client Mode Profile, and then select , or select .
3. Type a **Client Mode Profile Name**.
4. (Optional) Type a **Description**.

Although optional, descriptions can be helpful when you are 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. 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 from the dropdown list.
7. 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**.
8. When configuration of the Client Mode Profile settings is complete, select **Save**.

Related Links

[Client Mode Profiles](#) on page 288

[Configure DHCP Servers and DHCP Relay Agents](#) on page 291

[Configure Wireless Interfaces for an AP Template](#) on page 202

[Configure a Client Mode AP Profile using a Wired Connection and a Device Template](#) on page 126

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.

The DHCP Server and Relay Objects table displays the following information:

- **Name:** The name of the object.
- **Interface:** The management interface. For example, mgt0.
- **IP Address/Netmask:** The IP address and netmask that defines the subnet.
- **Used By:** The number of network policies to which this DHCP server and relay object applies. Hover over the number in this column to see a list.

Use this task to add a new DHCP Server and Relay object.

1. Go to **Configure > Common Objects > Basic > DHCP Server and Relay**.
2. Select an existing object, and then select , or 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 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 still 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 the plus sign, 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:** Enter the IP address of the default gateway or the subnet to which the addresses in the IP pool belong.
- **DNS Server1 IP:** Enter 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:** Enter 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:** Enter 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:** Enter the IP address of the POP3 server for clients to use (DHCP option 70).
- **SMTP Server IP:** Enter the IP address of the SMTP server for clients to use (DHCP option 69).
- **WINS Server1 IP:** Enter the IP address of the primary WINS server for NetBIOS name-to-address resolution (DHCP option 44).
- **WINS Server2 IP:** Enter the IP address of the secondary WINS server for NetBIOS name-to-address resolution (DHCP option 44).
- **Lease Time:** Enter 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:** Enter the netmask defining the subnet to which the addresses in the IP pool belong.
- **Domain Name:** Enter 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:** Enter 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:** Enter the IP address of the secondary NTP server with which DHCP clients can synchronize their clocks (DHCP option 42).
 - **Log Server IP:** Enter 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:** Enter 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 a Secondary DHCP Server (optional).
9. Select **Save**.

Configure a DNS Service

Add or modify a subnetwork space. For more information, see [Add a Subnetwork Space](#) on page 360. It is also helpful to have configured your DNS Servers. See [Configure a DNS Server](#) on page 320.

Extreme Networks routers use DNS services in their subnetwork configurations (see [Configure Subnetwork Space Advanced Settings](#) on page 362). 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 **Configure > Common Objects > Basic > DNS Services**.
2. Select an existing DNS Service object, and then select , or select .

3. Type a **Name**.
4. (Optional) Type a **Description**.

Although optional, descriptions can be helpful when you are 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**.

Next, [Configure Subnetwork Space Advanced Settings](#) on page 362.

Configure IP Objects and 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 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 148.

Use this task to configure an IP object and Host name.

1. Go to **Configure > Common Objects > Basic > IP Objects / HostNames**.
2. Select an existing IP object or host name, and then select , or select .



Note

You cannot change the object type of an existing IP object or host name.

- To delete an IP object and host name, select the object(s) and then select .
 - To clone an existing IP object and host name, select .
3. Type a **Name** for the new object.
 4. Select an object type from the menu, and then configure the settings.

Table 68: Object Types

Object Type	Description
IP Address	Define an IP Address for a host. Note: When you select IP Address, ExtremeCloud IQ 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. 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: • Subnet IP: 10.1.1.0 • 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 68: Object Types (continued)

Object Type	Description
Wildcard	When creating an IP object/host name using a Wildcard Mask, the mask 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. 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 10.1.0.255.255.0.255. 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 devices at those sites. 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	

5. To add a classification rule:

a. Select .

**Important**

Classification rules for IP objects are currently only supported when IP objects are used to create firewall rules.

b. To create and assign a new classification rule, select , type a **Name** and a **Description** for the rule, select to select a rule type, and then select **Save Rule**.

Select  for each new rule you want to include. Select  to edit, or  to delete, an existing rule. Use the up and down arrows in the **Order** column to define the order in which the rules appear.

Table 69: Rule types

Selected rule type	Do this
Device Location	- Drill down until you reach the location level at which the device resides. - Select Select. The location appears in the Classification Rules table.
Cloud Config Group	- Select the Match Type. - Select an existing group from the  menu, or select . For more information, see Add a Cloud Config Group on page 217. - Select CLOUD CONFIG GROUP. - Select CONTINUE.
IP Address	- From the Match Type menu, select Contains or Does Not Contain. - Select , or select an existing IP address from the  menu. If you do not see the IP address that you want, select New to create a new IP address. - Select SAVE IP. - Select CONTINUE.

Table 69: Rule types (continued)

Selected rule type	Do this
IP Subnet	- From the Match Type menu, select Contains or Does Not Contain. - Select , or select an existing IP subnet from the  menu. If you do not see the IP subnet that you want, select New to create a new IP subnet. - Select SAVE SUBNET. - Select CONTINUE.
IP Range	- From the Match Type menu, select Contains or Does Not Contain. - Select , or select an existing IP range from the  menu. If you do not see the IP range that you want, select New to create a new IP range. - Select SAVE IP. - Select CONTINUE.

- To assign an existing classification rule, select , select an existing classification rule, and then select **Link**.
 - Select the arrow in the **Assignment Description** column to view a summary of the linked classification rules.
- Select **SAVE IP OBJECT**.

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. For more information about firewall policies, see [Add MAC Firewall Policies](#) on page 304. In QoS traffic classification and marking policies, you can prioritize traffic based on its OUI.

Use this task to configure a MAC object and MAC OUI.

- Go to **Configure > Common Objects > Basic > MAC Objects / MAC OUIs**.
- Select .
- Select **MAC Address**.
- Type a **Name**.
- Type the **MAC Address**.
- Select **SAVE**.
- Select .

8. Select **MAC OUI**.
9. Type a **Name**.
10. Type the first six digits of the Mac address, for the **MAC OUI**.
11. Select **SAVE**.

Related Links

[Add MAC Firewall Policies](#) on page 304

Configure a Notification Template

There are two default notification templates available in ExtremeCloud IQ; 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 **Configure > Common Objects > Basic > Notification Templates**.
2. Select an existing template, and then select , or select .
To delete a selected template, 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 70: 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 71: 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
- 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 **Configure > Common Objects > Basic > OS Objects**.
2. Select an existing object, and then select , or select .

To delete a selected OS object, select .

3. Type a **Name** for the object.
4. Enter a **Description** for the object.
5. Select either **DHCP Option** or **HTTP Agent**.

Although optional, descriptions can be helpful when you are troubleshooting your network.

6. Select .
7. Select the **OS Type** from the  menu.

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 a VLAN Object

Although you can manage VLANs from **Common Objects**, it is a best practice that you configure them inside a network policy workflow. For more information, see [Configure VLAN Settings](#) on page 156.

Use this task to configure a VLAN object.

1. Go to **Configure > Common Objects > Basic > VLANs**.
2. Select an existing VLAN, and then select , or select .
3. Type a **Name** for the new VLAN.
4. Type a **VLAN ID**.
5. (Optional) Select **Apply VLANs to devices using classification**.

For more information, see [Apply VLANs to Devices Using Classification](#) on page 301.

6. Select **SAVE**.

Related Links

[Configure VLAN Settings](#) on page 156

[Apply VLANs to Devices Using Classification](#) on page 301

Apply VLANs to Devices Using Classification

First, [Configure a VLAN Object](#) on page 300 and select **Apply VLANs to devices using classification**.

This task is part of VLAN object configuration. Use this task to apply VLANs to devices by using classification.

1. Go to **Configure > Common Objects > Basic > VLANs**.
2. Select an existing VLAN, and then select , or select .
3. Select **Apply VLANs to devices using classification**.
4. Add or select classification rules.
 - a. To choose an existing classification, select , and then select **LINK**.
 - b. To add a new classification rule, select .
 - c. Configure the settings for the rule.

See [Configure Classification Rules](#) on page 214.
5. Select **SAVE**.

Related Links

[Configure a VLAN Object](#) on page 300

[Configure Classification Rules](#) on page 214

Configure a VLAN Group Object

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 156, and [VLAN Group Object Settings](#) on page 158.

Use this task to configure a VLAN Group object.

1. Go to **Configure > Common Objects > Basic > VLAN Group**.
2. Select an existing VLAN Group, and then select , or 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 troubleshooting your network.

6. Select **SAVE**.

Related Links

[Configure VLAN Settings](#) on page 156

[VLAN Group Object Settings](#) on page 158

Configure Supplemental CLI

To use the supplemental CLI (sCLI) tool, first go to **Global Settings > VIQ Management**, and enable **Supplemental CLI**.

After you save supplemental CLI 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 attempts to update only the configuration deltas. If a full update is required, the system prompts you to select **Complete Configuration Update**. 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. Go to **Configure > Common Objects > Basic > Supplemental CLI Objects**.

2. Select an existing Supplemental CLI object, and then select , or select .

3. Type a **Name**.

4. (Optional) Type an optional **Description**.

Although optional, descriptions can be helpful when you are 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

[Enable Supplemental CLI](#) on page 88

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

- [Add IP Firewall Policies](#) on page 303
- [Add MAC Firewall Policies](#) on page 304
- [Configure MGT IP Filters](#) on page 305
- [Configure Traffic Filters](#) on page 307
- [Add a WIPS Policy](#) on page 309

Add 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 **Configure > Common Objects > Security > AirDefense Policies**.
2. Select an existing AirDefense policy object and then select , or select .
3. Enter a **Name** for the new policy.
4. Enter an optional **Description**.
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 303

Add IP Firewall Policies

Use the following procedure to create IP firewall policy objects and rules that determine how the device manages traffic based on network or application services, and source and destination IP addresses.

1. Go to **Configure > Common Objects > Security > IP Firewall Policy Rules**.
2. Select an existing IP firewall policy rule and then select , or select .
3. Enter a **Name** for the new policy.
4. Enter an optional **Description**.
5. Select  to add a new rule.
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 the add icon to

create a new network service. For more information, see [Configure Network Services](#) on page 359.

- 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 continue to add rules to a policy, 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 359

[Security Configuration](#) on page 303

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 the following procedure to add MAC firewall policy objects and rules.

1. Go to **Configure > Common Objects > Security > MAC Firewall Policies**.
2. Select an existing IP firewall policy and then select , or select .
3. Enter a **Name** for the new policy.
4. Enter an optional **Description**.
5. Select  to add a new rule.
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 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

[Security Configuration](#) on page 303

Configure MGT IP Filters

Before you begin, enable **MGT IP Filter** in the network policy settings. See [Configure MGT IP Filter Policy Settings](#) on page 112.

By default, ExtremeCloud IQ 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 **Configure > Common Objects > Security > MGT IP Filters**.
2. Select an existing MGT IP Filter and then select , or select .
3. Configure the settings.
See [MGT IP Filter Settings](#) on page 306.
4. To add a new IP Object, select **Add Another IP Object**, configure the settings, and then select **SAVE SUBNET**.
See [Table 73](#) on page 307.
5. Select **SAVE MGT IP FILTER**.

Related Links

[MGT IP Filter Settings](#) on page 306

[Security Configuration](#) on page 303

MGT IP Filter Settings

Table 72: Settings for MGT IP Filters

Setting	Description
Name	Type a Name for the filter.
Description	(Optional) Type a Description for the filter. Although optional, entering a description is helpful for troubleshooting and for identifying the filter.
Permitted Management Traffic Source	

Table 72: Settings for MGT IP Filters (continued)

Setting	Description
Available IP Objects	IP objects in this list are preconfigured. To add to the list, select ADD ANOTHER IP OBJECT. See Table 73 on page 307. 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. 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. 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. Use the double arrow >> to move all available IP addresses.

Table 73: Settings for IP Objects

Setting	Description
Name	(Required) Type a Name for the new IP object.
Subnet	(Required) Type the new IP Address and Subnet .

Configure Traffic Filters

Before you begin, enable **Traffic Filters** in the network policy settings. See [Configure Traffic Filters Policy Settings](#) on page 112.

The Traffic Filter table displays services (SSH, Telnet, ping, and SNMP) that Extreme Networks devices permit between connected clients. The table displays the name of the traffic filter, a description (if one was configured), and identifies the SSID using the filter (Used by). Hover over a number in the Used by column to see more information.

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.

You can clone, modify, and delete traffic filters using the icons above the table.

Use this task to configure a new Traffic Filters object.

1. Go to **Configure > Common Objects > Security > Traffic Filters**
2. Select an existing Traffic Filter, and then select , or select .
3. Configure the settings.
See [Traffic Filter Settings](#) on page 308.
4. Select **SAVE**.

Related Links

[Traffic Filter Settings](#) on page 308

[Security Configuration](#) on page 303

Traffic Filter Settings

Table 74: 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	
Control the following types of traffic to devices	Select the corresponding check boxes to enable the selected types of traffic. • Enable SSH: Permit an SSH connection to the mgt0 interface. By default, SSH is enabled. • Enable Telnet: Permit a Telnet connection to the mgt0 interface. By default, Telnet traffic is disabled. • Enable Ping: Permit ICMP echo requests (pings) to reach the mgt0 interface. By default, pinging mgt0 is allowed. • Enable SNMP: Permit an SNMP connection to the mgt0 interface. By default, SNMP is disabled. • 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. • Enable Telnet: Permit a Telnet connection to the mgt0 interface. By default, Telnet traffic is disabled. • Enable Ping: Permit ICMP echo requests (pings) to reach the mgt0 interface. By default, pinging mgt0 is allowed. Does not apply to N1100 series devices.

Related Links

[Configure Traffic Filters](#) on page 307

[Configure Traffic Filters Policy Settings](#) on page 112

Add a WIPS Policy

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 an Extreme AirDefense Essentials 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.

1. Go to **Configure > Common Objects > Security > WIPS Policies**.
2. Select an existing WIPS policy object, and then select , or select .
3. Configure the settings.
For more information, see [WIPS Policy Settings](#) on page 309.
4. Select **SAVE**.

Related Links

[Security Configuration](#) on page 303

[WIPS Policy Settings](#) on page 309

WIPS Policy Settings

Table 75: Settings for WIPS policy

Setting	Description
Name	Type a Name for the new policy.
Description	(Optional) Type a Description . 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 . By default, AirDefense Essentials is ON (enabled). 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.

Table 75: Settings for WIPS policy (continued)

Setting	Description
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. 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 assumed 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.
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. Choose an existing MAC OUI from the  menu, or select + , and then 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. Select + , and then choose one of the following: 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. • Select an SSID—Select the SSID from the menu. • Enter an SSID Name—Type the SSID name. 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. 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	

Table 75: Settings for WIPS policy (continued)

Setting	Description
Mitigation Mode	Select one of the following: • 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. 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. • Automatic: APs automatically mitigate rogue APs and their clients, starting and stopping the mitigation process without any administrator involvement. 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.
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. 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). 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).

Table 75: Settings for WIPS policy (continued)

Setting	Description
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). 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.
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.) 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 180

Add a WIPS Policy on page 309

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 313

[Classifier Maps](#) on page 315

[Configure Marker Maps](#) on page 318

[Configure Rate Limiting and Queuing](#) on page 319

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.

The Rate Limits table lists the following information:

- **Name:** The name of the user profile in which traffic policing and rate limiting are enabled.



Note

Extreme Networks devices apply airtime-based scheduling to traffic assigned to admin-defined user profiles but not to traffic assigned to a predefined user profile "default-profile". To apply airtime-based scheduled QoS to client traffic, make sure that the SSIDs reference only user profiles that you or another admin created.

- **Used By:** Hover over any number in the Used By column to see the user names of devices that are using this rate limit

You can use the icons above the table to add, modify, or clone rate limits. To delete a rate limit, select the check box for the rate limit and then select the delete icon.

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 incoming traffic according to 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 313.

When a device applies a classifier map, it checks incoming packets for settings matches in the map, 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 Map Services](#) on page 315.

Related Links

[Quality of Service](#) on page 313

[Configure Classifier Map Services](#) on page 315

Configure Classifier Map Services

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.

1. Go to **Configure > Common Objects > QOS > Classifier Maps > Services** tab.
2. Select an existing map and then select , or select .
3. Type a **Name** for the Classifier Map.
4. Type an optional **Description**.
5. To add a new service, select .
6. 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) that you want 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


```
show logging buffered
```

 command, or you can configure the device to send event logs to a syslog server and view them there.
 - e. Select **Save**.

As an alternative, you can select services individually.
8. Select **Save**.

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 **Configure > Common Objects > QOS > Classifier Maps > MAC OUIs** tab.
2. Select an existing map and then select , or select .
3. Type a **Name** for the Classifier Map
4. Type an optional **Description**.
5. To add a new MAC OUI, 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 **Configure > Common Objects > QOS > Classifier Maps > SSIDs** tab.
2. Select an existing map and then select , or 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 **Configure > Common Objects > QOS > Classifier Maps > 802.1p/DiffServ/802.11e** tab.
2. Select an existing map and then select , or 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 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.



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. Go to **Configure > Common Objects > QOS > Marker Maps**.
2. Select an existing map and then select , or 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 always include 802.11e priority marking in the L2 headers of wireless frames automatically, 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.

Configure Rate Limiting and 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 procedures to configure rate limiting and queuing profiles for network traffic.

1. Go to **Configure > Common Objects > QOS > Marker Maps**.
2. Select an existing map and then select , or select .
3. Enter a **Name** for the rate limiting 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. Enter 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 802.11ac/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: 54,000 Kbps for 802.11a/b/g, 1,000,000 for 802.11n, 2,000,000 for 802.11ac/ax.
- 2 - Best Effort 1: 54,000 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, 1,000,000 for 802.11n, 2,000,000 for 802.11ac/ax.

10. Select **Save**.

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 a DNS Server](#) on page 320
- [Configure an NTP Server](#) on page 321
- [Configure an SNMP Server](#) on page 322
- [Configure a Syslog Server](#) on page 325

Configure a DNS Server

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 **Configure > Common Objects > Management > DNS Servers**.
2. Select an existing DNS server profile object, and then select , or select .
3. Configure the [DNS Server Settings](#) on page 321.

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 321

[Management Configuration](#) on page 320

DNS Server Settings

Table 76: Settings for DNS server profiles

Setting	Description
Name	(Required) 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 104

[Configure a DNS Server](#) on page 320

Configure an NTP Server

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 in the Common Objects area first, before creating Network Policies and the VGVA's that reference them.

1. Go to **Configure > Common Objects > Management > NTP Servers**.
2. Select an existing NTP Server, and then select , or select .
3. Configure the [NTP Server Settings](#) on page 322.
4. To add an NTP server, select .
 - a. To use an existing NTP server, select it from the  menu.
 - b. To add a new NTP server, select , and then select **IP Address** or **Host Name**.
 - c. Type a **Name** for the new IP object.
 - d. (Optional) To change your previous selection, select **IP Address** or **Host Name** from the menu.

- e. Select **SAVE IP OBJECT**.
- f. Select **ADD**.

Related Links

[Configure NTP Server Policy Settings](#) on page 105
[Management Configuration](#) on page 320

NTP Server Settings

Table 77: Settings for NTP server profiles

Setting	Description
Name	Type a Name for the NTP server.
Domain Name	(Optional) 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). 2. From the Switch Sync Interval , select a value.

Related Links

[Configure NTP Server Policy Settings](#) on page 105
[NTP Server Settings](#) on page 322

Configure an SNMP Server

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.

The **SNMP Server Profiles** table displays information about SNMP server profiles and their assignments to network policies and VGVAs (VPN Gateway Virtual Appliances), including the server profile name, a description, and the number of network policies or VGVAs that reference the SNMP server profile. Hover over any non-zero number to see the names of the policies and VGVAs.

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 **Configure > Common Objects > Management > SNMP Servers**.
2. Select an existing SNMP Server, and then select , or select .
3. Configure the [SNMP Server Settings](#) on page 324.
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 it from the **SNMP Server** menu.
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 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 SNMP SERVER**.

Related Links

[SNMP Server Settings](#) on page 324

[Management Configuration](#) on page 320

*SNMP Server Settings***Table 78: Settings for SNMP servers**

Setting	Description
Name	Type a Name for the server.
Description	(Optional) 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. 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.

Table 78: Settings for SNMP servers (continued)

Setting	Description
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: • 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.
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 106

[Configure an SNMP Server](#) on page 322

Configure a Syslog Server

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 an NTP Server](#) on page 321.

Use this task to configure a syslog server object.

1. Go to **Configure > Common Objects > Management > Syslog Servers**.

2. Select an existing Syslog Server, and then select , or select .
3. Configure the [Syslog Server Settings](#) on page 326.
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 an existing syslog IP Address or host name from the  menu, or select .
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 326

[Management Configuration](#) on page 320

Syslog Server Settings

Table 79: Settings for Syslog servers

Setting	Description
Name	Type a Name for the syslog server.
Description	(Optional) 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. 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.

Table 79: Settings for Syslog servers (continued)

Setting	Description
Syslog Group	Select the arrow to expand the Syslog Group section, and use the menus to select the log level for each category. • Emergency • Alert • Critical • Error • Warning • Notification • Info • Debug 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 107

[Configure a Syslog Server](#) on page 325

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, sFlow receivers, network services, subnet space, firewalls, and VPN services.

Related Links

[Configure an Access Console](#) on page 328

[Configure ALG Services](#) on page 329

[Configure LLDP and CDP](#) on page 329

[Configure an IP Tracking Group](#) on page 331

[Configure Layer 2 IPsec VPN Services](#) on page 332

[Configure Location Servers](#) on page 338

[Configure Management Options](#) on page 341

[Configure Tunnel Concentrator Services](#) on page 352

[Configure Tunnel Policies](#) on page 356

[Configure an sFlow Receiver](#) on page 358

[Configure Network Services](#) on page 359

[Add a Subnetwork Space](#) on page 360

[Configure a Firewall Policy](#) on page 364

Configure an Access Console

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 only supported by IQ Engine APs and cannot be used with other devices.

1. Go to **Configure > Common Objects > Network > Access Consoles**.

2. Select an existing Access Console and then select , or select .

3. Enter a **Name** for the Access Console.

4. Enter an optional **Description**.

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 6.1r5; and for Extreme Networks devices introduced in ExtremeCloud IQ 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**.

Configure ALG Services

You can configure ALG services from inside the network policy or as common objects.

Complete the following steps to configure ALG services.

1. Select the add icon.
2. Enter a name for the ALG service.
3. Enter an optional description for the service.
4. From the table, select check boxes to enable the protocols you want to associate with this ALG service.
5. Select the quality of service to apply to each protocol for which QoS is available.
6. Enter the 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.
7. Enter the maximum session length for FTP, SIP, and TFTP.
The range is 1 to 7200 minutes, and defaults vary by protocol.
8. Select **Save**.

Configure LLDP and CDP

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 **Configure > Common Objects > Network > LLDP/CDP**.

2. Select an existing LLDP/CDP object, and then select , or select .
3. Toggle **LLDP/CDP** to **ON**, and then configure the settings.

See [LLDP and CDP Settings](#) on page 330.

To reuse LLDP/CDP settings, choose an existing setting from the  menu.

Related Links

[LLDP and CDP Settings](#) on page 330

[Network Configuration](#) on page 327

LLDP and CDP Settings

Table 80: Settings for LLDP and CDP

Setting	Description
Name	Type a Name for the new LLDP/CDP object.
Description	(Optional) 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. 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) 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. 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)
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.

Table 80: Settings for LLDP and CDP (continued)

Setting	Description
CDP (Cisco Discovery Protocol)	Toggle CDP ON to enable devices to receive and cache CDP advertisements. Note: You can enable LLDP and CDP concurrently. 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 111[Configure LLDP and CDP](#) on page 329

Configure an IP Tracking Group

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 **NTP Server** policy settings for a network policy.

1. Go to **Configure > Common Objects > Network > IP Tracking Groups**.
2. Select an existing IP tracking group, and then select , or select  to create a new group.
3. Configure the settings.
See [IP Tracking Group Settings](#) on page 332.
4. Select **SAVE**.

Related Links

[IP Tracking Group Settings](#) on page 332[Network Configuration](#) on page 327

*IP Tracking Group Settings***Table 81: Settings for IP Tracking Groups**

Setting	Description
Name	Type a Name for the group.
Description	(Optional) 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) Type the tracking interval for this group. Default: 6
Tracking Retries	(Required) 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 110

[Configure an IP Tracking Group](#) on page 331

Configure Layer 2 IPsec VPN Services

First configure a new VPN service. See [Configure VPN Services](#) on page 365.

To configure a Layer 3 IPsec VPN service, see [Configure Layer 3 VPN Services](#) on page 190.

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 **Configure > Common Objects > Network > Layer 2 IPsec VPN Services**.
2. Select an existing Layer 2 IPsec VPN service and then select , or select .
3. Configure the [Layer 2 VPN Services Settings](#) on page 333.
4. Select **SAVE**, or configure **Optional Settings**.

Configure **Optional Settings > IPsec VPN Authority Settings**, see [Configure IPsec VPN Authority Settings](#) on page 190.

Related Links

[Configure VPN Services](#) on page 365

[Layer 2 VPN Services Settings](#) on page 333

[Configure IPsec VPN Authority Settings](#) on page 190

[Configure Layer 3 VPN Services](#) on page 190

Layer 2 VPN Services Settings

Table 82: Settings for Layer 2 VPN services

Setting	Description
Name	Type a name for the service.
Description	(Optional) 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. 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. Note: If the VPN server is behind a NAT device, enter the address of the MIP address on the NAT device. If there is no NAT device in front of the VPN server, enter the mgt0 IP address of the server.

Table 82: Settings for Layer 2 VPN services (continued)

Setting	Description
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. 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 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 182

[Configure Layer 2 IPsec VPN Services](#) on page 332

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 332.

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 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.

This task is part of the network policy configuration workflow. Use this task to configure IPsec VPN Authority settings.

1. Go to **Configure > Network Policies**.
2. Select an existing network policy, and then select , or select .
3. After you save the **Policy Details**, select **5 Branch Routing**.
4. From the **Router Settings** menu, select **VPN Service**.
5. In the **Optional Settings** section, expand **IPsec VPN Authority Settings**.
6. If you do not have a certificate or key that you want to use, select **Import**.
7. 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.

8. 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 192.

Related Links

[Server-Client Credentials](#) on page 192
[Configure Layer 2 IPsec VPN Services](#) on page 332
[Router Settings](#) on page 182

Server-Client Credentials

After you save the Layer 2 IPsec VPN service configuration, ExtremeCloud IQ populates the table with randomly generated 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 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 192.

Related Links

[Router Settings](#) on page 182

Configure Advanced Server Options

First, create a Layer 2 IPsec VPN service. For more information, see [Configure Layer 2 IPsec VPN Services](#) on page 332.

Use this task to configure the **Advanced Server Options** for a new Layer 2 IPsec VPN object.

1. Go to **Configure > Common Objects > Network > Layer 2 IPsec VPN Services**.
2. Select an existing VPN service, and then select , or 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 332.

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 **Configure > Common Objects > Network > Layer 2 IPsec VPN Services**.
2. Select an existing VPN service, and then select , or 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. Configure the **DPD (Dead Peer Detection) Settings**.

The DPD and tunnel heartbeat settings control when to fail over from the primary to the secondary VPN server. The DPD messages verify the presence of an IKE peer, and AMRP (Advanced Mobility Routing Protocol) tunnel heartbeats verify communications through the GRE and VPN tunnel. The failure of either mechanism can trigger a failover.

- 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 times to retry sending a DPD R-U-There message when it does not elicit a response.
- c. Set the amount of time between retries.

7. For **Tunnel Heartbeat Settings**:

- 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 332

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, they send information to ExtremeCloud IQ, AeroScout location servers, or location services such as Ekahau that use Tazmen Sniffer Protocol (TZSP) to be monitored and tracked.

1. Toggle **Location Server ON**.
2. Use the **Re-use Location Server Settings** option to select a previously configured location server profile.

If you are not choosing this option, complete the next steps.

3. Enter a name.
4. Enter an optional description.
5. Toggle **Client Location Tracking ON** to enable location tracking and reporting to the location processing engine.

6. For **Track Client Location Using**:

Extreme Networks Location Server: See [Configure Track Client Location Using an Extreme Location Server](#) on page 340.

AeroScout Location Server: See [Configure Track Client Location Using an AeroScout Location Server](#) on page 339.

Tazmen Sniffer Protocol (Ekahau, etc...): See [Configure Track Client Location Using the Tazmen Protocol](#) on page 340.

Continue configuring the network policy.

Configure Track Client Location Using an AeroScout Location Server

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.

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 and Host Names](#) on page 294.

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.

Continue configuring a network policy.

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 and Host Names](#) on page 294.
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 342.

Use these settings to control how administrators are authenticated and how they access the devices they manage.

1. Go to **Configure > Common Objects > Network > Management Options**.
2. Select an existing management object, and then select , or select .
3. Enter a **Name**.
4. Enter an optional **Description**.
5. Configure [Forwarding Engine Control Management Options](#).
6. Configure [System Settings Management Options](#).
7. Configure [Authentication Settings Management Options](#).
8. After you have completed all the relevant sections, select **SAVE**.

Related Links

[Management Options](#) on page 342

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 83: Forwarding Engine Control Settings

Setting	Description
Forwarding Engine Control	
GRE Tunneling Selective Multicast Forwarding	Select one of the following options: • Block All—Prohibits forwarding multicast and broadcast traffic through tunnels. • Allow All—Enables forwarding multicast and broadcast traffic through tunnels. ExtremeCloud IQ 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. By default, devices do not enforce MAC or IP session limits per station. By default, devices do not enforce IP session limits per station.
Limit IP Sessions per Station	Select Limit IP Sessions per Station to enable the feature, and type the maximum number of sessions per station. 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.

Table 83: Forwarding Engine Control Settings (continued)

Setting	Description
Enable TCP Maximum Segment Size	Select Enable TCP Maximum Segment Size to enable the feature, and then type the maximum segment size. 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. 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. 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.
DHCP Shield	Disable DHCP Shield to turn off the built-in ability for IQ Engine to prevent attached clients from impersonating a DHCP server. 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. Disabling DHCP Shield results in no changes to access points running IQ Engine 6.5, switches, routers, or Virtual Gateway appliances.

Table 83: Forwarding Engine Control Settings (continued)

Setting	Description
Proxy ARP	Proxy ARP requests enable learning MAC addresses and proxy replies to ARP requests. Select one of the following slider bar options: • 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. • Legacy: Not recommended, but is available for legacy Wi-Fi 4 APs. • 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. • 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. 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.
Enable legacy HTTP redirect	Select Enable legacy HTTP redirect to enable redirects to legacy HTTP sites. 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	

Table 83: Forwarding Engine Control Settings (continued)

Setting	Description
Log	Select the corresponding check boxes to enable the generation of logs for the following scenarios: • Drop packets that are denied by IP or MAC firewall policies • 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: • Fragmented IP Packets • 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 84: 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.
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. 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.

Table 84: System Settings (continued)

Setting	Description
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 (%). 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. The following detection methods are available: • Use DHCP option 55 contents: Select to use the DHCP option 55 parameter list. • Use HTTP user agent IDs: Select to use the contents of the HTTP user agent ID within the HTTP headers. • 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 84: 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. Disabling the console port on a device that is deployed in a publicly accessible location is a good security precaution. Disabling the console port means that all administrative access must flow over the network, and if there are any connectivity issues with the network or if the device is configured to use only DHCP to get an IP address and cannot get its network settings from a DHCP server, attempts to log in to the device fail. Note: Disabling the console port means that all administrative access must flow over the network, and if there are any connectivity issues with the network or if the device—if configured to use only DHCP to get an IP address—cannot get its network settings from a DHCP server, you will not be able to log into the device.

Table 84: System Settings (continued)

Setting	Description
Enable Smart PoE	To enable Smart PoE, select the check box. 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. 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: • 20 W or higher: No adjustments are needed when the power level is 20 W or higher. • 18 - 20 W: The device disables the ETH1 interface. • 15 – 18 W: The device switches from 3x3 MIMO (Multiple In, Multiple Out) to 2x3. • 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. • 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. 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.
Accept ICMP Redirect Message	Enable this feature to accept ICMP redirect messages from routers on their subnet. Select the check box. By default, devices reject ICMP redirects because crafted ICMP redirect messages can be maliciously used to cause a victim host to send traffic to an attacker's host or even back to the victim itself, which is what occurs during a WinFreeze attack. However, you can enable this feature if you believe that your network is safe from such threats and you want multiple routers on the local subnet to be able to update the routing table on devices.

Table 84: System Settings (continued)

Setting	Description
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, where the information is logged as an event. 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. To use this setting, you must first define the iBeacon service in the associated network policy and then turn it on via the Device Management page.

Authentication Settings Management Options

Authentication settings specify the database location for storing administrator accounts, and control authentication for administrators.

Table 85: 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: • Local—Stores admin accounts locally on the APs. • RADIUS—Stores admin accounts remotely on RADIUS authentication servers. • Both—Stores admin accounts both locally and remotely. 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. 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. 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. 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: • Delimiter—Choose the type of delimiter: Colon (:), Dash (-), or Dot (.). • Style—Choose No delimiters, Two delimiters, or Five delimiters. • Case Sensitivity—Choose between Lower Case and Upper Case. 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

Table 85: Authentication Settings (continued)

Setting	Description
	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. 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: Colon, no delimiter, upper case: 0016CF8D55BC Colon, two-delimiter, upper case: 0016:CF8D:55BC Colon, five-delimiter, upper case: 00:16:CF:8D:55:BC Dash, five-delimiter, upper case: 00-16-CF-8D-55-BC Dot, five-delimiter, upper case: 00.16.CF.8D.55.BC

Related Links

[Configure Management Options](#) on page 111

[Configure Management Options](#) on page 341

[Configure Forwarding Engine Control Management Options](#) on page 351

[Configure System Settings Management Options](#) on page 352

[Configure Authentication Settings Management Options](#) on page 352

Configure Forwarding Engine Control Management Options

The forwarding engine controls the type of traffic being forwarded between interfaces, GRE tunnels, and sets logging features. Extreme Networks devices can selectively block or enable broadcast and multicast traffic through GRE tunnels to reduce traffic congestion. This task is part of creating or modifying a Management Option and applies only to APs.

1. Go to **Configure > Common Objects > Network > Management Options**.
2. Select an existing management object, and then select , or select .
3. Configure the settings for **Forwarding Engine Control**.
See [Forwarding Engine Control Management Options](#) on page 342.
4. To add an entry to the **Exception IP List**, select .
 - a. In the dialog box, enter the destination **IP Address** and the **Netmask**.
You can also enter an IPv6 address.
 - b. Select **ADD**.
5. Select **SAVE**.

Continue to [Configure System Settings Management Options](#) on page 352.

Related Links

[Forwarding Engine Control Management Options](#) on page 342

[Configure Management Options](#) on page 341

Configure System Settings Management Options

Use **System Settings** to adjust various device-level functions, including device health alarm thresholds, VoIP features, and client OS detection types. This task is part of creating or modifying a Management Option.

1. Go to **Configure > Common Objects > Network > Management Options**.
2. Select an existing management object, and then select , or select .
3. Configure the **System Settings**.

See [System Settings Management Options](#) on page 345.

Continue to [Configure Authentication Settings Management Options](#) on page 352.

Related Links

[System Settings Management Options](#) on page 345

[Configure Management Options](#) on page 341

Configure Authentication Settings Management Options

Use this procedure to configure a database location for storing administrator accounts, set the PPSK (Private PSK) save list, and the MAC address format.

1. Go to **Configure > Common Objects > Network > Management Options**.
2. Select an existing management object, and then select , or select .
3. Configure the **Authentication Settings**.

See [Authentication Settings Management Options](#) on page 350.

4. Select **SAVE**.

Related Links

[Authentication Settings Management Options](#) on page 350

[Configure Management Options](#) on page 341

Configure Tunnel Concentrator Services

Add the Tunnel Concentrator as a device type. See [Quick Add Tunnel Concentrators](#) on page 31.

Perform this procedure to configure a new Tunnel Concentrator service.

1. Go to **Configure > Common Objects > Network > Tunnel Concentrator Services**.
2. Configure the settings for the Tunnel Concentrator Service.

See [Single Tunnel Concentrator Services Settings](#) on page 353 or [Redundant Tunnel Concentrator Services Settings](#) on page 354.

3. Select **Save**.

Related Links

[Quick Add Tunnel Concentrators](#) on page 31

[Single Tunnel Concentrator Services Settings](#) on page 353

[Redundant Tunnel Concentrator Services Settings](#) on page 354

*Single Tunnel Concentrator Services Settings***Table 86: Single Tunnel Concentrator**

Field	Description
Name	(Required) Type a name to identify the new Tunnel Concentrator service.
Description	(Optional) Provide a description that might be helpful when troubleshooting.
Single Tunnel Concentrator	(Required) Select this option to create a single Tunnel Concentrator without redundancy.
Tunnel IP Address/CIDR	(Required) Type the IP Address for the tunnel (CIDR).
Gateway	(Optional) Type the IP address of the gateway.
Native VLAN ID	(Required) Type the Native VLAN ID. The Native VLAN is untagged.
Device Tunnel Concentrator	(Required) Select a Tunnel Concentrator from the menu.
Tunnel Port	(Required) Select a port from the menu.
VLAN ID	(Required) Type the VLAN ID. (Optional) For an untagged VLAN, select the corresponding check box.
Bridge Port	(Required) 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.

Table 86: Single Tunnel Concentrator (continued)

Field	Description
Block Non- Essential Broadcast	Select or clear the check box. Essential Broadcasts are ARP and DHCP
ARP Proxy	Select or clear the check box. Caution: Disabling the ARP Proxy option can lead to undesired traffic.

Related Links

[Configure Tunnel Concentrator Services](#) on page 352

*Redundant Tunnel Concentrator Services Settings***Table 87: Redundant (Primary and Backup) Tunnel Concentrators**

Field	Description
Name	(Required) Type a name to identify the new Tunnel Concentrator service.
Description	(Optional) Provide a description that might be helpful when troubleshooting.
Redundant Tunnel Concentrator	(Required) Select this option to create a redundant Tunnel Concentrator.
Tunnel IP Address/CIDR	(Required) Type the IP Address for the tunnel (CIDR).
Gateway	(Optional) Type the IP address of the gateway.
VRRP Router ID	(Required) Type the ID for the VRRP router. 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) Type the Native VLAN ID. The Native VLAN is untagged.
Device Tunnel Concentrator	(Required—Primary and Backup) Select a primary Tunnel Concentrator from the menu. Select a backup Tunnel Concentrator from the menu.

Table 87: Redundant (Primary and Backup) Tunnel Concentrators (continued)

Field	Description
Tunnel Port	(Required—Primary and Backup) Select a port for the tunnel from the menu for the primary Tunnel Concentrator from the menu. Select a port for the tunnel from the menu for the backup Tunnel Concentrator from the menu.
VLAN ID	(Required—Primary and Backup) Type the VLAN ID for the primary and for the backup Tunnel Concentrators. (Optional) For an untagged VLAN, select the corresponding check box.
IP Address	(Required—Primary and Backup) Type the IP address for the primary and the backup Tunnel Concentrators.
Bridge Port	(Required—Primary and Backup) Select a bridge port for the tunnel from the menu for the primary Tunnel Concentrator. 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. 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. Possible values: 1 to 60 seconds 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. 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. Possible values: 1 to 10 retries 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.

Table 87: Redundant (Primary and Backup) Tunnel Concentrators (continued)

Field	Description
Add Pre-defined Rule	Select and choose a pre-defined rule from the menu.
Block Non- Essential Broadcast	Select or clear the check box. Essential Broadcasts are ARP and DHCP
ARP Proxy	Select or clear the check box. Caution: Disabling the ARP Proxy option can lead to undesired traffic.

Related Links

[Configure Tunnel Concentrator Services](#) on page 352

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. 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.

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.

Configure the following options based on your tunnel policy requirements. These options are mutually exclusive.

1. Go to **Configure > Common Objects > Network > Tunnel Policies**.
2. Select the plus sign.
3. Enter a name for this policy.
4. Enter an optional description for the policy.

Although optional, descriptions can be helpful when you are 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. **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 and Host Names](#) on page 294.
 - b. **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 and Host Names](#) on page 294.
 - c. **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. **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 and Host Names](#) on page 294.
 - b. **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 156.
 - c. **Tunnel Mode Access Mode:** type, select, edit, or add the VLAN ID.
To add a VLAN ID, see [Configure VLAN Settings](#) on page 156.
 - d. **Tunnel Failover:** type, select, edit, or add the IP address or host name of the secondary GRE tunnel endpoint. The secondary tunnel is used automatically if the primary tunnel goes down and traffic fails back to the primary tunnel when it is available.
 - e. **Keep Alive Interval:** Enter the interval (in seconds) used to monitor the failover tunnel.
 - f. **Keep Alive Retries:** Enter the number of retry attempts before the failover tunnel is considered down.
8. Select **Tunnel Concentrator** and then select up to three tunnel concentrator services to act as the Primary (required) Secondary (optional) and Tertiary (optional) tunnel destinations.

You can add a new Tunnel Concentrator service by selecting , or select  for an existing instance. For more information, see [Configure Tunnel Concentrator Services](#) on page 352.

9. Select **Save**.

The **Tunnel Policies** table displays the following information for the configured tunnel policies in your network:

- **Name:** The name of the tunnel policy.
- **Description:** An optional description of the policy.
- **Used by:** The number of network policies to which the tunnel policy is applied. Hover over a number in this column to see the names of the network policies.

Related Links

[Configure Tunnel Concentrator Services](#) on page 352

[Configure User Profile Traffic Tunneling](#) on page 283

Configure an sFlow Receiver

Use sFlow receivers to provide visibility into your switch traffic patterns. Configure sFlow receivers as common objects that you can assign to specific devices. Use the following procedure to configure an sFlow receiver as a common object.



Note

sFlow is only available for SR/Dell switch models.

1. Go to **Configure > Common Objects > Network > sFlow Receivers**.
2. Select an existing sFlow Receiver, and then select , or select , and then select **Switch** from the menu.
3. Type a **Name**.
4. Type an optional **Description**.
5. Type the IP address of the receiver, to which the accumulated data will be sent.
6. Select a **UDP Port Number**.

This is the UDP port number of the sFlow receiver where the data will be sent. The default UDP port number is 6343. (Range: 1-65535).

7. Select a **Maximum Datagram Size**.

This is the maximum number of data bytes that can be sent in a single sFlow diagram. Select a value that avoids datagram fragmentation.

8. The **Owner String** is an identity string required for the sFlow receiver configuration to take affect.

This is usually the same as the receiver name.

9. Select a timeout value.

This is the time, in seconds, before the sFlow sampler stops sending data to the receiver. A zero receiver timeout displays the sFlow receiver configuration in the running config.

10. Select a sampling rate (number of packets) and sample size (in bytes).

A higher sampling rate lowers the CPU burden on the device, and helps ensure that all collected samples can be sent to the receiver.

11. Select an interval for the sFlow receiver.

12. Select **SAVE SFLOW RECEIVERS**.

You can delete a single sFlow receiver or multiple receivers. Select the corresponding check boxes for the receivers and then select the delete icon.

You can add a new sFlow receiver by creating a clone of an existing receiver and then renaming it. Select the check box for the sFlow receiver that you want to clone and then select the clone icon. Type the new **Name** and then select **Clone**.

Related Links

[Assign an sFlow Receiver to a Switch](#) on page 488

[Assign an sFlow Receiver to a Switch Template](#) on page 268

Configure Network Services

Network service objects identify Layer 4 traffic by protocol and port number. ExtremeCloud IQ provides a number of predefined services and you can create custom network services to use when defining firewall policies (see [Configure a Firewall Policy](#) on page 364) and QoS traffic classification and marking policies (see [Classifier Maps](#) on page 315 and [Configure Marker Maps](#) on page 318).

The Network Services table displays the following information about predefined and custom network service objects:

- **Name:** The name of the network service object.
- **Protocol Number:** The type of protocol (followed by its standard protocol number) that the service uses. 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)
- **Port Number:** The standard destination port number of the service. The receiving device uses the port number to map the service to a particular processor.
- **Service Idle Timeout:** The amount of time (in seconds) after which the device terminates an inactive session using this service. (For IP firewall policies, this field is only supported by APs.)
- **ALG Type:** An ALG (application layer gateway) links certain port numbers to a service so that the device can apply the proper QoS (Quality of Service) and firewall policies. For example, the TFTP service has a control stream and data stream that each use different port numbers. The port number for the TFTP control stream is static (port 69 by default), but the port number for the TFTP data stream is dynamic and is negotiated within the control session. The TFTP ALG links these two streams together logically so that the device can apply the proper QoS and firewall policies to both TFTP streams. You can apply different QoS settings to the TFTP control and data sessions, for example, to ensure high reliability but tolerate high latency, or to ensure accept a medium level of reliability but require low latency.

- **Description:** An optional description for the object. Descriptions can be very useful when troubleshooting or managing a complex network.
- **Virtual IQ:** The name of the Virtual IQ (virtual ExtremeCloud IQ) to which the service belongs. All predefined services are marked as global to indicate that they belong to all Virtual IQs. This column only appears when you are logged in to "All Virtual IQs" with super-user privileges.

Use the following procedure to configure a network service:

1. Select the plus sign.
2. Enter a name for the service.
3. 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.
4. 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.
5. Enter the standard destination port number of 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.
6. Select an ALG type from the drop-down list.
ALG is supported for APs and routers only. If the service you are defining needs to use an ALG, select DNS, FTP, HTTP, SIP, or TFTP, from the drop-down list. Otherwise, leave this empty.

Add a Subnetwork Space

When you create a subnetwork for branch sites, you have a choice between making 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. Select the plus sign.
2. Enter an optional description.

3. Choose a network type from the drop-down list as follows:
 - **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.
4. **Create a unique subnetwork at each site**, as follows:
 - **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.

5. **Replicate the same subnetwork at each site**, as follows:

- **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.

6. Select **SAVE** or proceed to [Configure Subnetwork Space Advanced Settings](#) on page 362.

Configure Subnetwork Space Advanced Settings

Create or modify a subnetwork space. For more information, see [Add a Subnetwork Space](#) on page 360.

This task contains the next set of optional steps for creation of a new subnetwork space.

1. Select **Enable DHCP** to enable branch routers to dynamically provide client devices with network settings.
2. Enable the DHCP server on the routers to remove the necessity for additional hardware at remote sites.

When you select this option, additional configuration items appear.

- a. Use the controls to select where you want your DHCP pool of addresses 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.

- b. Enter the DHCP address lease time.

- c. Enter the NTP server's IP address that clients use to synchronize their system clocks.
- d. Enter your network domain name.
- e. Select **Use ARP to check IP address conflicts** to enable Extreme Networks routers functioning as DHCP servers to check if an IP address is in use before offering to lease it to a DHCP client.

Clear 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.

- f. For **Custom Options**, enter 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.

- g. Select **Enable DHCP Relay** to support a centralized DHCP server on a branch router.

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 branch router's DHCP server function. This 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.

3. Choose the **DNS Service** profile from the drop-down list.

If you do not see a service profile that you want to use, select the plus sign to create a new one. For more information about adding a DNS Service, see [Configure a DNS Service](#) on page 293.

**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.

4. 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. Enter the number of branch sites you want to replicate.
- b. Enter 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.

5. Select **SAVE**.

Configure a Firewall Policy

If you intend to use a User Profile as a source, create one first. See [Add a User Profile](#) on page 281.

You can add a firewall policy to control the traffic crossing routers, defining rules that either permit or deny traffic based on its source, destination, and network service type.

1. Go to **Configure > Common Objects > Network > Firewalls**.
2. To add a new firewall policy, select **+**.
To edit an existing firewall policy, select the corresponding check box, and then select .
3. Enter a **Name** for the policy.
4. Enter an optional **Description**.
5. To add and configure a new source, select **+**.
6. Choose the traffic **Source** from the drop-down list as follows:
 - **Any**: Applies to traffic from any source.
 - **Network Address**: Applies to traffic from an IP address. Depending on the netmask, this could indicate the address of a single host or an entire subnetwork; for example, as a network reserved for one or more types of users, such as contractors and guests. Choose an existing network address or define a new one.
 - **User Profile**: Applies to specific types of users. Choose an existing user profile or define a new one.
 - **VPN**: Applies to all traffic forwarded through an L3 IPsec VPN tunnel. For example, you might want to apply a rule to traffic tunneled from the main and other branch sites through the router firewall, to destinations at the branch site behind the router.
7. Choose the traffic **Destination** from the drop-down list as follows:
 - **Any**: Applies to traffic from any source.
 - **Network Address**: Applies to traffic from an IP address. Depending on the netmask, this could indicate the address of a single host or an entire subnetwork; for example, as a network reserved for one or more types of users, such as contractors and guests. Choose an existing network address or define a new one.
 - **VPN**: Applies to all traffic forwarded through an L3 IPsec VPN tunnel. For example, you might want to apply a rule to traffic tunneled from the main and other branch sites through the router firewall, to destinations at the branch site behind the router.
8. Select **Any** or an existing **Network Service** from the drop-down list, or create a new network service.
9. Choose **Permit** to pass traffic through the firewall or **Deny** to block it.
10. Turn logging **ON** or **OFF** for instances when the rule is enforced.

11. Select **Add** and repeat these steps for each new rule.

**Note**

The router applies firewall rules in order from the top. To reposition a rule, select it in the table and use the up and down arrows in the **Order** column.

12. Select **SAVE FIREWALL**.

Related Links

[Add a User Profile](#) on page 281

[Network Configuration](#) on page 327

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 other IQ Engine device acting as a tunnel head-end.

1. Go to **Configure > Common Objects > Network > VPN Services**.
2. Configure the [VPN Services Settings](#) on page 365.
3. Select **GENERATE** to create client credentials for servers and clients.
For more information, see [Server-Client Credentials](#) on page 192.
4. For the remaining optional settings, see:
 - [Configure IPsec VPN Authority Settings](#) on page 190 (Extreme Networks VPN Gateway only)
 - [Configure Advanced Server Options](#) on page 336
 - [Configure Advanced Client Options](#) on page 193
5. Select **SAVE**.

Related Links

[VPN Services Settings](#) on page 365

[Network Configuration](#) on page 327

VPN Services Settings

Table 88: Settings for VPN services

Setting	Description
Name	Type a Name for the new VPN service.
Description	(Optional) Type a Description for the new VPN service. Although optional, descriptions can be helpful when you are 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	

Table 88: Settings for VPN services (continued)

Setting	Description
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. 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.
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, AD servers, captive web portals, external RADIUS servers, Extreme Networks A3, and LDAP servers.

Related Links

- [Clone an AAA Server Profile](#) on page 366
- [Clone an Active Directory Server](#) on page 367
- [Clone or Edit a Captive Web Portal](#) on page 367
- [Clone or Edit an External RADIUS Server](#) on page 367
- [Clone or Edit an Extreme Networks A3 RADIUS Server](#) on page 368
- [Clone an LDAP Server](#) on page 368

Clone an AAA Server Profile

First, create an AAA Server Profile as part of a network policy. For more information, see [Configure an AAA Server Profile](#) on page 150.

Use this task to create a copy of an AAA Server Profile.

1. Go to **Configure > Common Objects > Authentication > AAA Server Settings**.
2. Select a server profile from the table.

3. Select .
4. Type a new name in the **Save As** field, and then select **CLONE**.

Related Links

[Configure an AAA Server Profile](#) on page 150

Clone an Active Directory Server

First, create an Active Directory (AD) server object as part of a network policy. For more information, see [Add an Active Directory Server](#) on page 152.

Use this task to clone an AD server object.

1. Go to **Configure > Common Objects > Authentication > AD Servers**.
2. Select an AD server object from the table.
3. To clone the AD server object, select .
4. Type a new name in the **Save As** field, and then select **CLONE**.

Related Links

[Add an Active Directory Server](#) on page 152

Clone or Edit a Captive Web Portal

First, create a captive web portal (CWP) as part of a network policy.



Note

If the table is empty, select . For more information, see [Captive Web Portals](#) on page 127.

Use this task to clone, or to edit the settings, for a CWP object.

1. Go to **Configure > Common Objects > Authentication > Captive Web Portals**.
2. Select a CWP object from the table.
3. To edit the settings for the CWP object, select  and configure the settings.
For more information, see [Captive Web Portals](#) on page 127.
4. To clone the CWP object, select .
5. Type a new name in the **Save As** field, and then select **CLONE**.

Related Links

[Captive Web Portals](#) on page 127

Clone or Edit an External RADIUS Server

First, create an External RADIUS Server object.

If the table is empty, select . For more information, see [Configure an External RADIUS Server](#) on page 148.

Use this task to clone, or to edit the settings, for an External RADIUS Server object.

1. Go to **Configure > Common Objects > Authentication > External RADIUS Servers**.
2. Select an External RADIUS Server object from the table.
3. To edit the settings for the External RADIUS Server object, select  and configure the settings.
For more information, see [Configure an External RADIUS Server](#) on page 148.
4. To clone the External RADIUS Server object, select .
5. Type a new name in the **Save As** field, and then select **CLONE**.

Related Links

[Configure an External RADIUS Server](#) on page 148

Clone or Edit an Extreme Networks A3 RADIUS Server

First, create an Extreme Networks A3 RADIUS server object.

If the table is empty, select . For more information, see [Configure an Extreme Networks A3 Server](#) on page 149.

Use this task to clone, or to edit the settings, for an Extreme Networks A3 RADIUS server object.

1. Go to **Configure > Common Objects > Authentication > Extreme Networks A3 RADIUS Servers**.
2. Select an Extreme Networks A3 RADIUS Servers object from the table.
3. To edit the settings for the Extreme Networks A3 RADIUS Server object, select  and configure the settings.
For more information, see [Configure an Extreme Networks A3 Server](#) on page 149.
4. To clone the External RADIUS Server object, select .
5. Type a new name in the **Save As** field, and then select **CLONE**.

Related Links

[Configure an Extreme Networks A3 Server](#) on page 149

Clone an LDAP Server

First, create an LDAP Server Profile as part of a network policy.

Use this task to create an LDAP server with AAA Server profiles for devices configured as RADIUS servers.

1. Go to **Configure > Common Objects > Authentication > LDAP Servers**.
2. Select a server from the table.



Note

If the table is empty, you must first create an LDAP server inside of a network policy workflow.

3. Select .
4. Type a new name in the **Save As** field, and then select **CLONE**.
5. Select **SAVE**.

Related Links

[LDAP Server Settings](#) on page 369

LDAP Server Settings

Table 89: Settings for LDAP servers

Setting	Description
Name	Type a Name for the new or cloned server.
LDAP Server	Select an IP Address or Host Name from the  menu, or select  .
Description	(Optional) 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. Note: ExtremeCloud IQ 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 LAPDS 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) Enter the LDAP server Destination Port .

Table 89: Settings for LDAP servers (continued)

Setting	Description
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) Select the default certification authority digital certificate type from the list.
LDAP Client Certificate	(Required) Select the default LDAP client digital certificate type from the list.
Client Key File	(Required) Select the default client key digital certificate type from the list.
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: • Try (on first authorization or authentication) • Never • Demand (as required, on demand)

Certificate Configuration

The topics in this section provide details about certificate configuration objects, including how to create certificates and keys, and how to import them.

Related Links

[Create a Certificate and Key](#) on page 370

[Create an ExtremeCloud IQ Certificate of Authority](#) on page 371

[Create a CSR for a Server](#) on page 372

[Concatenate an Existing Certificate and Private Key](#) on page 374

[Create a Self-Signed Certificate](#) on page 374

[Import a Certificate or Key](#) on page 375

Create a Certificate and Key

Before generating a certificate, make sure 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 certificate and key.

1. Select the plus sign.

2. Create one of the following types of certificates:
 - **ExtremeCloud IQ CA:** Select to generate your own Certificate Authority (CA) certificate. See [Create an ExtremeCloud IQ Certificate of Authority](#) on page 371.
 - **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 372.
 - **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 374.
 - **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 374.
3. Select **Save**.
4. You can also import a certificate or key.
See [Import a Certificate or Key](#) on page 375.

Create an ExtremeCloud IQ Certificate of Authority

Before generating a certificate, make sure 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 generate your own Certificate Authority (CA).

1. Go to **Configure > Certificate > Certificate Management**.
2. Select .
3. On the **Create Certificate/Key** page, select **ExtremeCloud IQ CA**.
4. Enter a descriptive name or the domain name of the ExtremeCloud IQ appliance or Virtual IQ that you will use to sign server certificates.
This name will later be used to verify server certificates to authenticate participants in AAA exchanges. Examples: SophiaCA, HiltonCA, Extreme NetworksCA.
5. Enter the name of the ExtremeCloud IQ organization.
Examples: Sophia University, Hilton Hotel, Extreme Networks.
6. Enter the name of the ExtremeCloud IQ division.
Examples: Marketing, Engineering, Sales.
7. Enter the ExtremeCloud IQ location.
8. Enter the ExtremeCloud IQ State or Province.

9. Enter the ExtremeCloud IQ two-character country code.
10. Enter an optional contact email address.
11. Enter 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. 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. Enter the corresponding password for encrypting and decrypting the private key linked to the public key in the CA.
14. Select **Save**.

ExtremeCloud IQ saves the CA with the file name `Default_CA.pem` and the accompanying private key as `Default_key.pem`.

Create a CSR for a Server

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 Certificate Signing Request (CSR).

1. Go to **Configure > Certificate > Certificate Management**.
2. On the **Create Certificate/Key** page, select **Server CSR**.
3. For **Common Name**, type a descriptive name or the domain name of the ExtremeCloud IQ appliance or Virtual IQ that you will use to sign server certificates.
The appliance or VIQ name you assign is used to verify the server certificates when they are used to authenticate participants in AAA exchanges. Examples: SophiaCA, HiltonCA, Extreme NetworksCA.
4. For **Organization Name**, type the name of the ExtremeCloud IQ organization.
Examples: Sophia University, Hilton Hotel, Extreme Networks
.
5. Type the name of the ExtremeCloud IQ division.
Examples: Marketing, Engineering, Sales.
6. For **Locality Name** type the location.
7. For **State/Province Name**, type the State or Province.
8. Type the two-character **Country Code**.
9. Type an optional contact email address.

10. Type an optional **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`.

11. 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.

12. Type the corresponding password for encrypting and decrypting the private key linked to the public key in the CA.

13. Type a **CSR Name** to identify the CSR file.

14. Select **Save**.

ExtremeCloud IQ saves the CA certificate with the file name `Default_CA.pem` and the accompanying private key as `Default_key.pem`.

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 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.

After the CA returns the signed certificate and private key file, import the certificate into ExtremeCloud IQ. See [Import a Certificate or Key](#) on page 375.

Related Links

[Certificate Configuration](#) on page 370

Concatenate an Existing Certificate and Private Key

Before generating a certificate, make sure 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 new file containing a concatenation of a server certificate and an unencrypted private key.

1. Go to **Configure > Certificate > Certificate Management**.
2. On the **Create Certificate/Key** page, select **Concatenate an existing certificate and private key**.
3. Enter a **Name** for the concatenated certificate/private key file.
4. Enter an optional note about the certificate for later reference.
5. Select the certificate you want to use from the drop-down list.

You can also select **Import** to import a certificate. See [Import a Certificate or Key](#) on page 375.

6. Select a private key method from the drop-down list.

You can also select **Import** to import a key. See [Import a Certificate or Key](#) on page 375.

7. Enter the corresponding password for encrypting and decrypting the private key linked to the public key in the CA.
8. Select **Save..**



Note

Although you cannot change the certificate and private key in a concatenated file, you can modify the 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. Select the name of the file, modify the **Certificate Name** and **Description** fields, and then select **Update**.

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 **Configure > Certificate > Certificate Management**.

2. Select an existing certificate or key file and then select , or select  to add a new one.

**Note**

You cannot edit a default certificate or key file.

3. On the **Create Certificate/Key** page, select **Self-signed certificate**.

4. Type a **Name**.

5. Enter the ExtremeCloud IQ organization name.

Examples: Sophia University, Hilton Hotel, Extreme Networks.

6. Enter the ExtremeCloud IQ division name.

Examples: Marketing, Engineering, Sales.

7. Enter ExtremeCloud IQ location.

8. Enter ExtremeCloud IQ State or Province.

9. Enter ExtremeCloud IQ two-character country code.

10. Enter an optional contact email address.

11. Enter 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. Choose an optional 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. Select **Save**.

Import a Certificate or Key

Use the following procedure to import certificate and key files:

1. Go to **Configure > Certificate > Certificate Management**.

2. Select the import icon.

3. Use **Select** to navigate to the location of the certificate file.

4. Select **Open**.

5. Select **Import**.

6. Select whether the file is a certificate or key.

Extreme Networks devices support PEM-formatted certificates. To import certificates in PFX or DER formats, you must first use the conversion tool to reformat them as PEM files. See [Step 6](#) or [Step 7](#), depending on the file format.

7. To import a PFX-formatted file, which contains a certificate and private key combined, first convert it:

- a. Select **Convert the certificate format from PFX to PEM**.

- b. Enter the password that was used to encrypt the PFX file.

- c. Select **Save**.

**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.
 - a. Select **Save**.
9. Select **Save**.

Create a Certificate Bundle

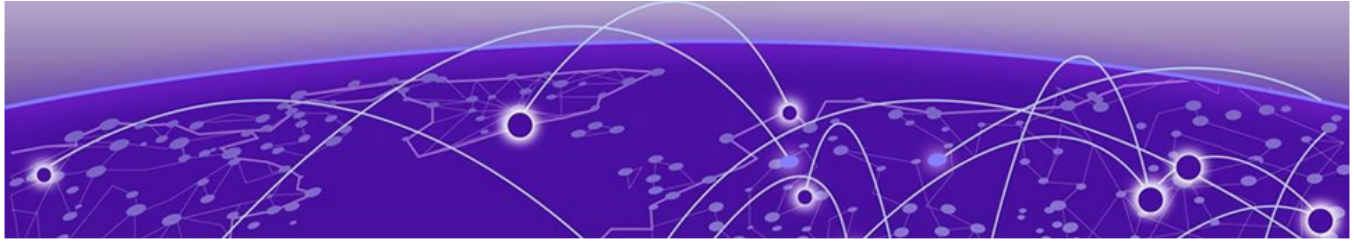
Import the CA, CERT, and KEY files. See [Import a Certificate or Key](#) on page 375. Use this task to create a new certificate bundle:

1. Go to **Configure > Certificate > Certificate Bundle**.
2. Select an existing certificate bundle and then select , or select  to add a new one.
3. Configure the settings.

Table 90: 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**.



Manage

[Summary](#) on page 378
[Real Time Maps](#) on page 381
[Planning](#) on page 401
[Devices](#) on page 412
[Clients](#) on page 496
[Users](#) on page 506
[Events](#) on page 508
[Alerts](#) on page 509
[Reports](#) on page 526
[Applications](#) on page 531
[Rogue APs](#) on page 534
[Rogue Clients](#) on page 536
[About Client Monitor](#) on page 537
[About Diagnosis](#) on page 540
[Packet Capture](#) on page 542
[VPN Management](#) on page 551
[Set the Time Frame for Captured Data Displays and Reports](#) on page 551

Use **Manage** to monitor real-time network statistics, manage devices, and reports as follows:

- [Summary](#): Presents a summary of traffic on your network and the number of access points, routers, and switches. It also provides a summary of the number of unique wired/wireless devices on your network.
- [Planning](#): View and modify your network by adding locations, buildings, floors, and network zones. Place simulated devices to help determine where you might need to add or redistribute devices for the best wireless network capability. View heat map data and modify floor plans to include obstructions that can affect your wireless signal strength.
- [Devices](#): View, add, and update managed and unmanaged devices, check connections to a RADIUS server, and perform other management actions.
- [Users](#): View details about active users in your network; information about all users, or by authentication type: RADIUS users, PPSK, or Others.
- [Events](#): All of the above statistics displayed on one page.

- [Alerts](#) on page 509: View a graphical representation of event and metric alerts, and configure new alerts.
- [Reports](#): Configure and generate reports.
- [Applications](#): View information about the applications that are most active in your network.
- [Security](#): View Rogue APs and Clients.
- [Client Monitor](#) and [Diagnosis](#): View and sort client objects, including IoT clients, plus historical and real-time client data.
- [VPN Management](#): Manage keys for VPNs. You can assign keys, revoke keys, and change keys for VPNs that appear in this list.

Summary

The ExtremeCloud IQ Pilot dashboard gives you a comprehensive overview of how your network is performing. Here you can see details about application usage, the number of connected clients and users, network alarms, and security issues.

Use the **Time Range** controls to specify the time frame for which you want to display captured data. Select any blue item to display more details about that item. Select **Create Report** to generate and distribute customized reports in HTML format. Download report data in **.csv** format.

The dashboard contains eight data widget. Select the  icon within each widget to download widget data in **.csv** format. Use the filter sidebar to filter the information displayed in the widgets. For more information, see [Use the Filter Sidebar](#) on page 379.

Each widget presents the following information:

- **Network Summary**: Provides a summary of traffic on your network and the number of access points, routers, and switches. It also provides a summary of the number of unique wired/wireless devices on your network. The data updates hourly.
- **Top Application Groups**: Provides top **Application Groups** usage and associated users. The detailed data displays in a drop-down format sorted from highest to lowest application group type for both data usage and users. You can download the data details in a spreadsheet.



Note

Because the dashboard refreshes data hourly, no data displays for the first hour after new ExtremeCloud IQ Pilot accounts become active.

- **Top Applications**: Provides top usage in **Top Applications Groups**. The top application types are displayed in selectable, sorted format showing data usage, number of users and clients. You can download the data details in a spreadsheet.
- **Top Usage**: Provides top data usage for clients or users. The data for displays in sortable table format. Top client usage data includes the client ID, data usage, # of apps, top app, and top app group ID. Top user data includes user name, # of apps, usage level, user profile and top associated application. You can download the data details in a spreadsheet.

- **Wi-Fi Clients by OS:** Provides a listing of Wi-Fi clients by OS type. You can customize the information to show the frequency band distribution (2.4 GHz, 5 GHz, or both). You can download the data details in a spreadsheet.
- **Top Wired:** Displays top usage by clients with a wired connection. This information displays in a tabular format that includes port name, network usage volume and %. You can download the data details in a spreadsheet.
- **Top (switches or access points) by (clients or usage):** Provides top-ranked usage access points or switches by user or client. This data is presented as a bubble graph to indicate the magnitude by usage or client. You can download the data details in a spreadsheet.
- **Max Number of Simultaneous Connections:** Displays a bar graph showing the simultaneous client types within the selected period. You can download the data details in a spreadsheet.

Related Links

[Set the Time Frame for Captured Data Displays and Reports](#) on page 551

[Use the Filter Sidebar](#) on page 379

Use the Filter Sidebar

The filter sidebar lets you customize what information is displayed in the Devices list and other ExtremeCloud IQ tables. You can save and reuse custom-defined filters. The filters that are available to you vary depending on the window you are in. For example, for the devices list, you can filter based on location, network policy, device type, etc. To see all available options, in the Filter area, select **More**, or select **Less** to see fewer items.

Filter By > Devices > Locations includes an **Unassigned** option. Select this option to list devices without a location assignment and see their current health status. As a best practice, assign a location to all devices.

Filter By > Devices > Network Policies includes an **Unassigned** option. Select this option to list all devices that are not assigned to a network policy.

The Toggle Filter icon changes depending on whether a filter is applied. When there are no filters applied, the original icon is shown. When one or more filters are applied, the icon contains a colored dot and the sidebar lists the filters under **Applied Filters**.

You can save individual filters or a list of filters. The sidebar displays saved filters under **My Saved Filters**.

Table 91: Sidebar Filter Options

Filter	Description
Devices	
Locations	To view location associated devices. Select Unassigned to list devices without a location assignment and see their current health status. As a best practice, assign a location to all devices.

Table 91: Sidebar Filter Options (continued)

Filter	Description
Network Policies	To view network policy associated devices. Select Unassigned to list all devices that are not assigned to a network policy. Note: Select  to view a summary of the network policy. Select Edit to modify the network policy. For more information, see Configure Policy Settings on page 103.
Device Types	Filter options include All , Digital Twin Devices , Plan Devices , Real Devices , and Simulated Devices .
Device Connection State	Filter options include All , Connected , Disconnected , Pre-Provisioned , and Undetermined .
Device Audit Status	Filter options include All , Config Audit Match , Config Audit Mismatch , and Config Override .
Device Update Status	Filter options include All , Update Successful , and Update Unsuccessful .
Device Management State	Filter options include All , Managed , New , Setting up , and Unmanaged .
Device Managed By	View the devices managed by your selection.
Device Function	View the devices associated with the selected device functions. Note: Select Unknown to view unclassified devices.
Device Product Type	View the devices associated with the selected product types.
Device Software Version	View the devices associated with the selected software versions.
Cloud Config Groups	View the devices associated with the selected cloud config groups.
GeoLocation Status	Filter options include All , Available , and Not Available .
AFC Status	Filter options include All , AFC Available , AFC Grace Period , and AFC Pending .
Network	
SSID Name	View the devices associated with the selected SSID Name(s).
IoT Profiles	View the devices associated with the selected IoT Profile(s).
Users	
User Profiles	View the devices associated with the selected user profile(s).
License	

Table 91: Sidebar Filter Options (continued)

Filter	Description
CoPilot	Filter options include All , All CoPilot Eligible Devices , CoPilot Active , CoPilot None , and CoPilot Unlicensed .
Device License	Filter options include All , Advanced Tier A Device License , Advanced Tier B Device License , Advanced Tier C Device License , Advanced Tier D Device License , Legacy Device License , Navigator Device License , None Device License , Not Licensed , Not Required Device License , Pilot Device License , Standard Tier A , Standard Tier B , Standard Tier C , and Standard Tier D .

Real Time Maps

Real-time network heat 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.

ExtremeCloud IQ supports the following map type views:

- [Wi-Fi Map](#)
- [IoT Map](#)



Note

Maps generated within the **Manage > Planning** section are visible in real-time maps.

With ExtremeCloud IQ real-time network heat maps, you can:

- [Rotate the heat map](#)
- [View a detail summary for a selected device](#) (including uploading installation photos)
- [Perform actions on a selected device](#)
- [View the summary details of clients connected to an AP](#) (including client location, Client 360 details, roaming paths, and real-time troubleshooting)
- [View the heat map in 3D](#)
- [Filter devices by client connection type](#)
- [Adjust thresholds](#)
- [Change color schemes](#)

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

1. Go to **Manage > Real Time Maps**.

2. From the **Global View** location list, select a floor or use the **Search** field to search for a specific site, building, or floor.

**Note**

The **Search** field helps you find a specific location in a large network. Enter the first few characters to see a list of locations. The more characters you enter, the more precise the search results will be.

**Note**

The selected floor must include a floor plan. For more information, see [Add a Floor Plan](#) on page 394.

3. From the floor view pane, select **View Map Type**:
 - a. To view the heat map for Wi-Fi devices, select **Wi-Fi**, configure the following Wi-Fi map settings.

Table 92: Wi-Fi Map Settings

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
Co-channel Interference	2.4 GHz, 5 GHz, or 6 GHz

- b. To view the heat map for IoT devices, select **IoT**, configure the following IoT map settings.

Table 93: IoT Map Settings

Map Type	Radio Frequency
RSSI	2.4 GHz

**Note**

IoT heat maps support **2.4 GHz** radio frequencies only.

- c. To display clients on the map, select the **Show Clients on the Map** checkbox. Clients will appear on the map. To open a client list, select . A client list appears. To close the list, click anywhere outside of the list.
4. To rotate the map, select and drag the slider in the top right corner in the desired direction.

**Note**

Select the arrow icon to reset the map rotation.

5. To view [device details](#), select a device on the map.

6. To view summary details for the clients connected to an AP, select the number of connected clients displayed above the AP.

- The **Inventory > Clients** pop-up window appears.
- To view client locations on the heat map, select the checkbox next to a **Hostname**. Clients are displayed as white circles on the map. When you hover over a **Hostname**, the client icon changes to purple, indicating its location.

**Note**

Clients connected to an AP with a known location are displayed by default. Clients without location information cannot be displayed on the heat map.

**Important**

To view client locations:

- Presence Analytics must be enabled on the network policy. For more information, see [Configure Presence Analytics](#) on page 180.
 - ExtremeLocation Essentials must be enabled. For more information, see [ExtremeLocation Essentials in ExtremeCloud IQ](#) on page 583.
- Select a **Hostname** to view client **Summary** and **Actions**:
 - The **Summary** tab displays the Host Name, OS, Uptime, IP Address, MAC Address, Connected to, VLAN, SSID, Captive Web Portal, User, User Profile, Radio, and Channel information for the selected client.
 - From the **Actions** tab:
 - To access Client 360 details, select **Client 360 View**. This opens a new pop-up window displaying the Client 360 information. To return to the client summary, close the pop-up window.
 - To view the roaming trail of the client, select **Client Roaming**. For more information, see [View Client Roaming Trail](#) on page 393.
 - To troubleshoot client APs in real-time, select **Real-Time Troubleshooting**. For more information, see [Real-Time Troubleshooting](#) on page 505.
 - Select **Disconnect** to deactivate the device.

7. 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 396.

**Note**

Administrator privileges are required to hide a device from the heat map.

8. 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

9. 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 the  and  icons 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.

10. Select one of the following icons to filter devices on the map by their connection type:

-  : All
-  : Wi-Fi
-  : Thread

11. Select  to set Wi-Fi coverage thresholds, configure threshold settings, and then select **Apply**.

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

Table 94: Wi-Fi Coverage Threshold Settings

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

12. To change the color scheme, select  and select a new color scheme.



Note

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

13. Select + to zoom in, and - to zoom out. Select and drag the map to move within the window.

**Note**

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

Related Links

[Add a Floor Plan](#) on page 394

[Import a Third-Party RF Heatmap](#) on page 397

[Edit a Real Time Floor Map](#) on page 398

[Device Summary and Actions Menu](#) on page 385

[View Device Inventory](#) on page 396

[View Antenna Patterns](#) on page 397

Device Summary and Actions Menu

In a Real Time Map, select a device to display device summary information and a list of available actions.

AP Device Summary

The **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 Installation Height:
 - AP Installation Height
 - 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**.

- Radio Band details:
 - Power
 - Channel
 - 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 **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.

Actions

From the **Actions** tab, you can perform the following actions on a selected device:

- [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](#) on page 392

Related Links

[Real Time Maps](#) on page 381

[Switch VLAN Probe Utility](#) on page 448

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 **Manage > Real Time Maps**.

2. From the **Global View** location list, select a floor or use the **Search** field to search for a specific site, building, or floor.

**Note**

The **Search** field helps you find a specific location in a large network. Enter the first few characters to see a list of locations. The more characters you enter, the more precise the search results will be.

**Note**

The selected floor must include a floor plan. For more information, see [Add a Floor Plan](#) on page 394.

3. Select a connected device from the floor plan, and then select the **Actions** tab.
4. Select **Locate AP (blinking lights)** or **Locate Switch**, configure the Locate Device settings, and then select **Submit**.

Table 95: 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 will flash to help you find the AP: • Amber • White • Off
AP	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: • Fast • Slow • Steady
Switch	LED Timeout	Select a number of seconds between 0 (until disabled) and 604800 (one week).

**Note**

Select **Return to normal LED operations**, and then select **Submit**, to stop the blinking lights used for locating the device.

Related Links

[Real Time Maps](#) on page 381

[Device Summary and Actions Menu](#) on page 385

Reboot the Selected Device

Use this task to restart the selected device. Restarting momentarily disconnects any connected clients.

1. Go to **Manage > Real Time Maps**.
2. From the **Global View** location list, select a floor or use the **Search** field to search for a specific site, building, or floor.

**Note**

The **Search** field helps you find a specific location in a large network. Enter the first few characters to see a list of locations. The more characters you enter, the more precise the search results will be.

**Note**

The selected floor must include a floor plan. For more information, see [Add a Floor Plan](#) on page 394.

3. Select a connected device from the floor plan, and then select the **Actions** tab.
4. Select **Reboot**, and then select **Yes** to confirm.

**Note**

The current configuration will not be saved before the reboot.

Related Links

[Real Time Maps](#) on page 381

[Device Summary and Actions Menu](#) on page 385

VLAN Probe from Real Time 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.

Use this task to verify the VLAN probe results and status of VLAN for selected device.

1. Go to **Manage > Real Time Maps**.

- From the **Global View** location list, select a floor or use the **Search** field to search for a specific site, building, or floor.

**Note**

The **Search** field helps you find a specific location in a large network. Enter the first few characters to see a list of locations. The more characters you enter, the more precise the search results will be.

**Note**

The selected floor must include a floor plan. For more information, see [Add a Floor Plan](#) on page 394.

- Select a connected device from the floor plan, and then select the **Actions** tab.
- Select **VLAN Probe** or **Switch VLAN Probe**, and configure the VLAN Probe settings.

Table 96: VLAN Probe Settings

Field	Description
VLAN Range	The start and end VLAN Range to probe. 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 (AP devices only)	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.

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

Related Links

[Real Time Maps](#) on page 381

[Device Summary and Actions Menu](#) on page 385

[Switch VLAN Probe Utility](#) on page 448

Reset a Device to Factory Defaults

Use this task to reset the selected device to their default configuration. A warning statement displays after you select this option. If you select **Yes**, the operation restores factory settings and reboots the device.

**Important**

This operation will remove all existing settings from the selected device and reboot it into the factory default configuration state. It will then reconnect to ExtremeCloud IQ as a new device.

- Go to **Manage > Real Time Maps**.

2. From the **Global View** location list, select a floor or use the **Search** field to search for a specific site, building, or floor.

**Note**

The **Search** field helps you find a specific location in a large network. Enter the first few characters to see a list of locations. The more characters you enter, the more precise the search results will be.

**Note**

The selected floor must include a floor plan. For more information, see [Add a Floor Plan](#) on page 394.

3. Select a connected device from the floor plan, and then select the **Actions** tab.
4. Select **Reset to factory defaults**, and then select **Yes** to confirm.

Related Links

[Real Time Maps](#) on page 381

[Device Summary and Actions Menu](#) on page 385

Upgrade Device Firmware

Use this task to manually upgrade the selected device from a real-time map.

**Note**

LLDP is on by default in ExtremeCloud IQ. In IQ Engine, LLDP was previously off by default. 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 **Manage > Real Time Maps**.
2. From the **Global View** location list, select a floor or use the **Search** field to search for a specific site, building, or floor.

**Note**

The **Search** field helps you find a specific location in a large network. Enter the first few characters to see a list of locations. The more characters you enter, the more precise the search results will be.

**Note**

The selected floor must include a floor plan. For more information, see [Add a Floor Plan](#) on page 394.

3. Select a connected device from the floor plan, and then select the **Actions** tab.
4. Select **Upgrade firmware**.

5. In the **Device Update** dialog box, select an update type.

Table 97: 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 only updates the device deltas. This action will avoid 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 configuration settings. Note: Only supported on devices running HOS or IQE Firmware.
Upgrade IQ Engine and Extreme Network Switch Images:	
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 to from the drop-down list. To add a new version (local image), select Add/Remove: - To add a new local image, select , and then select Choose to upload an image file from your computer. 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. - To delete an existing local image, select an image, and then select . - Select Close. 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.
Activation Time for Extreme Networks Devices Running Images:	
Activate at next reboot (requires rebooting manually)	Activation takes affect the next time the AP is rebooted.

Table 97: Update AP Device Settings (continued)

Field	Description
Activate after xx seconds	The delay before activation, in seconds.
Activate/reboot on this schedule based on your local system time	Schedule a Date and Time to activate.

Table 98: 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 ExtremeCloud IQ.	
Upgrade IQ Engine and Extreme Network Switch Images	

6. To update the select device immediately, select **Perform Update**, or select **Save as Defaults** to keep these settings for future use.

Related Links

[Add a Floor Plan](#) on page 394

[Import a Third-Party RF Heatmap](#) on page 397

[Edit a Real Time Floor Map](#) on page 398

Configure AP Radio and Power Settings

1. Go to **Manage > Real Time Maps**.
2. From the **Global View** location list, select a floor or use the **Search** field to search for a specific site, building, or floor.



Note

The **Search** field helps you find a specific location in a large network. Enter the first few characters to see a list of locations. The more characters you enter, the more precise the search results will be.



Note

The selected floor must include a floor plan. For more information, see [Add a Floor Plan](#) on page 394.

3. Select a connected device from the floor plan, and then select the **Actions** tab.
4. Select **Radio & Power configuration**.

5. Select the Wi-Fi interface, configure the radio and power settings, and then select **Apply**.

Table 99: Radio and Power Configuration Settings

Field	Description
Radio Status	Toggle to turn on/off the Radio Status .
Channel	Select a specific channel. Select Auto to have ExtremeCloud IQ select the channel.
Transmission Power	Set the transmission power for the selected device (1 to 20 dBm). Select Auto to have ExtremeCloud IQ select the transmission power.

Related Links

[Real Time Maps](#) on page 381

[Device Summary and Actions Menu](#) on page 385

View Client Roaming Trail

Viewing the roaming trail of a connected client to an access point (AP) on a real-time map has many 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 **Manage > Real Time Maps**.
2. From the **Global View** location list, select a floor or use the **Search** field to search for a specific site, building, or floor.



Note

The **Search** field helps you find a specific location in a large network. Enter the first few characters to see a list of locations. The more characters you enter, the more precise the search results will be.



Note

The selected floor must include a floor plan. For more information, see [Add a Floor Plan](#) on page 394.

3. Select the purple halo above a device.
The purple halo shows the number of connected clients on the device.

4. Select an available client, and then select **Client Roaming**.

A split window displays:

- **Left Pane:** This pane displays the map and showcases how the client roamed.
- **Right Pane:** This pane displays the roaming view details, including the Client Name, Roaming Time, and Total Number of Roaming Events. The graph illustrates the roaming events and trails. Hover over a client or trail line to see a small pop-up with roaming details.

5. 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).
6. To narrow the roaming time frame, from the right pane, select the **Date & Time Range** drop down, 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 reset back to the default time frame.

7. To exit the roaming view and return to the real-time map, select **X** in the bottom pane.

Related Links

[Real Time Maps](#) on page 381

Add a Floor Plan

Use this task to add a floor plan to a building.

1. From the **Global View** location list, expand a location and select **+**.

To delete a floor plan, expand the building and select **✖** next to the floor to remove.

2. Configure floor details and then select **Next**.

Table 100: Add Floor Configuration Details

Field Name	Description
Name	The floor name.
Associated with	Select a building to associate with the floor.

Table 100: Add Floor Configuration Details (continued)

Field Name	Description
Environment Type	Floor environmental conditions can influence network behaviour. Select one of the following environment types: • Auto • Outdoor Free Space • Outdoor Suburban • Outdoor Dense Urban • Office • Obstructed in Building • Warehouse
Floor Attenuation	The impact (in dB) of physical obstacles (such as walls, doors, and glass) on wireless signal strength within the floor.
AP Installation Height	The installation height of the access point (AP).
Unit	The AP Installation Height unit of measurement (meters or feet).

3. To Upload a Floor Plan, from **Background image for floor plan**, select **Choose background image**.
4. To use an existing floor plan:
 - a. Select **Choose from Library**.
 - b. Select a floor plan image.
 - c. Select **Next**.
5. To upload a new floor plan:
 - a. Select **Upload New**.
 - b. Select **Choose**, navigate to the location of the file, and then select it.
 - c. If applicable, select the **Override floor plan images with same names** checkbox.
 - d. To select a specific area of the floor plan, in the floor plan preview, use the selection box to highlight the area, and then select **Upload selected area**.
 - e. To use the entire floor plan, select **Upload all**.
6. To scale the floor plan:
 - a. Zoom in to the floor plan to get a clear view of the area you want to measure.
 - b. Identify two points that represent the distance you want to measure, and then select a Point A to Point B.
 - c. Enter the distance (meters).
7. Select **Save**.

Related Links

[Real Time Maps](#) on page 381

[Import a Third-Party RF Heatmap](#) on page 397

[Edit a Real Time Floor Map](#) on page 398

View Device Inventory

The **Device Inventory** displays a list of **Access Points**, **Switches**, or **Clients** currently being monitored on a heat map.

The **Access Points** and **Switches** inventory 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 your network's real-time status.

The **Clients** inventory 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 **Manage > Real time maps**.
2. Select a floor from the location list.



Note

The selected floor must include a floor map. For more information, see [Add a Floor Plan](#) on page 394.

3. Select the  icon.



Note

You can use the **Search** field to find a specific device if your device list is long.

4. Select an Inventory Type.
 - Access Points
 - Switches
 - Clients
5. To hide an **Access Point** or **Switch**, select the corresponding  icon.
6. To show a hidden **Access Point** or **Switch**, select the corresponding  icon.
7. To filter **Client** types, select  and activate a filter option.

Import a Third-Party RF Heatmap

ExtremeCloud IQ supports the following third-party radio frequency (RF) heatmaps:

- Ekahau
- Hamina

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

1. Go to **Manage > Real time maps** and select the  icon.
2. 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 real-time maps you can only import building floors. To import a site, site folder, or a building, go to **Manage > Planning**.

- d. If the configuration is custom, select the **Import Custom AP Configuration** checkbox.
 - e. To select a floor plan(s), double-click an **Available floor** to move it to **Selected floors**.

To move all available floors, select the applicable arrow.
 - f. Select **Import**.
3. 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

[Real Time Maps](#) on page 381

[Add a Floor Plan](#) on page 394

[Edit a Real Time Floor Map](#) on page 398

View Antenna Patterns

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

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

- **Azimuth Plane:** A top-down view of the antenna's 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 antenna's 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 antenna's 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 **Manage > Real time maps**.
2. Select a floor from the location list.

**Note**

The selected floor must include a floor map. For more information, see [Add a Floor Plan](#) on page 394.

3. Select the  icon.

**Note**

You can use the **Search** field to find a specific device if your device list is long.

4. Select a device tab.

Edit a Real Time Floor Map

A heatmap provides a visual representation of device signal strength across a floor plan. By editing the heatmap, 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 supports the following real-time floor map editing functions:

- [Draw Inner Walls](#)
- [Add a Device to a Floor Plan](#)
- [Move a Device to a New Location on a Floor Plan](#)
- [Remove a Device from a Floor Plan](#)
- [Layer Opacity Adjustment](#)
- [Resize the Heat Map](#)

Use this task to edit a floor map.

1. Go to **Manage > Real time maps**.
2. Select a floor from the location list.



Note

The selected floor must include a floor map. For more information, see [Add a Floor Plan](#) on page 394.

3. Select the  icon.
4. To draw inner walls:
 - a. Select **Walls**.
 - b. Select a wall type.

Table 101: Floor Plan Wall Types

Wall Colour	Description
	Bookshelf 5dB
	Cubicle 2dB
	Dry Wall 3dB
	Brick Wall 5dB
	Concrete 15dB
	Elevator Shaft 10dB
	Thin Door 4dB
	Thick Door 10dB
	Thin Window 1dB

Table 101: Floor Plan Wall Types (continued)

Wall Colour	Description
	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. Note: Custom materials are created for imported maps that incorporate materials not already available. Note: Duplicate names, colors, or attenuation values are not permitted. Delete an existing custom material by selecting the material and pressing the Delete key on your keyboard. Note: Custom materials can only be deleted after all associated references to the them have been removed.

- c. Select each corner of an inner wall on the floor plan to draw a wall boundary.
- d. 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.

- e. To disable the pen tool, press the **ESC** key on your keyboard.
5. To add a device to the floor plan, select **Devices**:
 - a. Select a device, or use the **Search** field to find a device.
 - b. Hover your cursor 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 floor plan, 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.

8. 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.

9. To resize the heat map, follow these steps:
 - a. Select **Resize**.
 - b. Click on your starting point on the map.
 - c. Drag the cursor to your desired endpoint.
 - d. Click again to close the line.
 - e. Add a new Add a measurement for the line distance.

Related Links

[Real Time Maps](#) on page 381

[Add a Floor Plan](#) on page 394

[Import a Third-Party RF Heatmap](#) on page 397

Planning

Network locations are organized into 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. There is no default site; at account creation, only the global (org) level exists. Sites can have, but do not require addresses.

Sites replace locations as the parent container for buildings and serve the following purposes:

- Column picker
- Configuration applicability
- Monitoring unit
- Troubleshooting and health score unit

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 it must be associated with a site.

The physical address format is adjusted for the selected country, that is USA or international format.

Building names must be unique within the parent site.

Floor

Floors are physical subdivisions of buildings. A floor is the parent container for zones.

Floor names must be unique within the parent building.

Zone

Zones are defined areas of building floors.

For more information about changes to the location hierarchy after upgrading to this release, see [Location Tree Changes](#) on page 403.

Use the **Manage > Planning** page to view and modify your network locations. Define [site groups](#), [sites](#), [maps](#), [buildings](#), [floors](#), and [network zones](#). Place simulated devices to help determine where you might need to add or redistribute devices for the best wireless network capability. View heat map data and modify floor plans to include obstructions that can affect your wireless signal strength.



Note

Because complex factors affect radio signals in the real world, Extreme Networks cannot guarantee that actual radio coverage will match the estimated coverage results.

This page contains the following features:

- **Search Maps** helps you find a specific location in a large network. Enter the first few characters of a building or site name here to see a list of locations. The more characters you enter, the more precise the search results will be.
- **Google Maps** also provides location search functionality.
- **Global View** provides an overall view of your network in the map. The **Global View** location tree lists the names of all site groups (🏢), sites (📍), buildings (🏠), and floors (🏠). You can add multiple buildings to a site, and multiple floors to a building by importing floor plans or by drawing your own floor plan. ExtremeCloud IQ supports the PNG file format.
- **Location Maps:** On the top-level map (the network location map) a building icon indicates your network location. The location map contains **Import Map** and **Add Building** buttons, an option to choose between map or satellite view, and a zoom option.
- **Building Maps:** Select a building in the hierarchy to open the corresponding building map. A building map contains a floor plan of the building. Building maps include **Import Map** and **Add Floor** buttons, an expand screen option, and a **Details** panel, which shows the number of devices, alarms, and active clients at this location. To drill down for more specific network information, select any blue text in the expanded **Details** panel. If a building has multiple floors, you can toggle between them to see floor plans and device deployment.
- **Floor Maps:** Select a floor name in the hierarchy to open the corresponding floor map. A floor map should contain at least one floor perimeter and information about the types of walls and obstructions that appear on the floor. Floor map tabs let you plan and view your network deployments:
 - **Edit Floor Plan:** Upload a floor plan, and draw, change, or remove building parameters and walls. A details panel displays the number of devices installed on the floor.
 - **Plan Devices:** [Manually](#) or [automatically](#) add simulated and real devices, and change plan parameters for the floor.

- **View Heat Map:** See coverage details for simulated and real devices on this floor. For more information, see [View Heat Maps](#) on page 411 and [Real Time Maps](#) on page 381.
- **Zones:** Create and name zones. Zones help you track roaming clients and enable you to identify groups of APs on floors where their locations must be clearly defined and differentiated from each other.
- Each item in the network hierarchy panel contains **Delete**, **Move**, **Export**, **Clone**, **Edit**, and **Add** tools.
- Use **Network Summary** to view the current status of each network hierarchy item.

Related Links

[Location Tree Changes](#) on page 403
[Network 360 Monitor Overview](#) on page 553
[Add a Site Group](#) on page 404
[Add a Site](#) on page 404
[Import a Map](#) on page 405
[Add a Building](#) on page 405
[Move a Building](#) on page 406
[Add a Floor](#) on page 407
[Zone View](#) on page 556
[Manually Add Simulated Devices](#) on page 410
[Automatically Add Simulated Devices](#) on page 409
[View Heat Maps](#) on page 411
[Real Time Maps](#) on page 381

Location Tree Changes

During the upgrade from the previous release, most existing locations will migrate to the new site concept. Some cases require manual resolution. The following scenarios illustrate both successful migrations, and migrations that require administrator action to complete:

Scenario 1: Location > Building > Floor

Migrates to **Site > Building > Floor**

Scenario 2: Location > Location > Building > Floor

Migrates to **Site Group > Site > Building > Floor**

Scenario 3: Location > Location > Location > Building > Floor

Migrates to **Site Group > Site Group > Site > Building > Floor**

Scenario 4: Location > Location > Location > Location > Building > Floor

Migrates to **Site Group > Site Group > Site Group > Site > Building > Floor**. However, the site cannot be edited and you cannot make changes within the third nested site group.

Manually move the affected sites so that they have no more than two levels of nested site groups. ExtremeCloud IQ supports two levels of site groups.

Scenario 5: Building > Floor

Migrates to **Building > Floor**. As a best practice, Extreme Networks recommends that you manually define a site and associate the building to the new site.



Important

Initially, locations migrated to sites are not editable because they do not have the country code specified. The country code is required; manually specify the country code for each migrated site.

Related Links

[Planning](#) on page 401

Add a Site Group

Use the following procedure to add a new site group folder to your network plan.

1. Go to **Manage > Planning > Global View**, and select **Add**.
To add a new site group to an existing site group folder, select the corresponding **Add** button for the site group.
2. On the **Site Group** tab, enter the **Name** of the new site group folder.
3. From the **Associated With** menu, choose the global org level, or another **Site Group**.
This menu is available only when you add a new site group to an existing site group. At the Global level, the menu appears dimmed.
4. Select **SAVE**.

Related Links

[Planning](#) on page 401

Add a Site

Use the following procedure to add a new site to your network plan.

1. Go to **Manage > Planning > Global View**, and select **Add Site Group**.
To add a new site to an existing site group folder, select the corresponding **Add** button for the site group.
2. Select the **Site** tab and enter the **Name** of the new site.
3. Select the **Country**.
4. (Optional) Enter an **Address** and **City**, and then select the **State** from the drop-down menu.
Only the United States (country code 840) follows the US address format. All other countries follow the international address format: **Address, Address 2, Province/State/Town, City, Postal Code**.
5. From the **Associated With** menu, choose the global org level, or an existing **Site Group**.

This menu is available only when you add a new site to an existing site group. At the Global level, the menu is dimmed.

6. Toggle **AFC Schedule Update** to **ON** and set the **Time** and **Timezone** to configure a preferred time to query the AFC server.

**Note**

Service outages can occur after AFC spectrum refresh.

7. (Optional) For an **Outdoor Location**, set the toggle to **ON** and specify the following:
 - a. Choose an **Environment** type that most closely matches your installation.
 - b. Enter the most common **AP Installation Height**, in feet or meters.
 - c. Enter the **Map Size** (Width x Height), in feet or meters.
 - d. Enter a **background Image for floor plan** from your library.

Choose an image from your library, or upload a new image. For more information about floor plans, see [Add a Floor](#) on page 407.
8. Select **Save**.

Related Links

[Planning](#) on page 401

[Network 360 Monitor Overview](#) on page 553

Import a Map

Use the following procedure to add a new map to your network plan.

1. Go to **Manage > Planning** and select the corresponding **Import Map** button for a site, building, or floor.

Or, go to **ML Insights > Device View**.
2. Select **Import Map**.
3. Select **Choose**, then browse to your local folder and select the map. Select **Open**.

**Note**

You can import a single .xml file or a package with floor plan images exported from ExtremeCloud IQ.

4. Select **Import**.

Related Links

[Planning](#) on page 401

[Network 360 Monitor Overview](#) on page 553

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.

1. Go to **Manage > Planning**.
2. Locate the site to which you want to add the building, and select .

3. In the **Add Building** dialog, type a **Name** for the new building.
4. Type the building **Address** and **City**, and then select the **State**.

Alternately, use Google Maps search to automatically populate the address. If you manually adjust the marker on the map, the address updates automatically.

While sites do not require addresses, it is expected that buildings have addresses.

**Note**

While **State** is a required field for the US address format, the **Province/State/Region** field is optional for the international address format.

5. Select **SAVE**.

Related Links

[Planning](#) on page 401

[Network 360 Monitor Overview](#) on page 553

Move a Building

Use this task to move a building from one site to another indoor site.

1. Go to **Manage > Planning**.
2. Locate and expand the site that includes the building that you want to move.
3. Locate the building and select  .
4. In the dialog, from the **Associated With** menu, select the site to which you want to move the building.

**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 prompts you to rename the building before the move.

5. Select **MOVE**.

Draw a Building Perimeter

You must have a site that includes at least one building before you can draw a building perimeter.

It is a good practice to define the building perimeter before you add internal walls, windows, doors, and other RF obstructions. The perimeter helps estimate how much radio signal passes outside the walls of the building.

1. Select **Draw Perimeter**.
2. Select a corner of the building and drag to the next corner.
3. Before you reach the last corner, double-select to close the shape and exit drawing mode.

4. To change the perimeter wall type, highlight the perimeter and select **Change Wall Type**.

You can draw multiple perimeters on the same map to define different buildings or buildings with open spaces, such as courtyards. To draw a second perimeter on a map, select **Draw Perimeter** again and draw the new perimeter. You can draw perimeters inside each other, or two or more non-intersecting perimeters. The only invalid combination is a perimeter that intersects another perimeter.

5. Select a wall type from the drop-down list.
6. To remove a perimeter, highlight a perimeter line and select **Remove**.

The next step is to add internal walls and obstructions to the floors in your building. See [Add Interior Walls and Obstructions](#) on page 407

Related Links

[Planning](#) on page 401

[Add a Floor](#) on page 407

[Add Interior Walls and Obstructions](#) on page 407

Add Interior Walls and Obstructions

Use the drawing tools to add physical obstructions to floor plans. Specifying internal obstructions helps ExtremeCloud IQ estimate the amount of coverage needed for your deployment. From **EDIT FLOOR PLAN**, you can draw in physical elements directly onto your floor plan images. These elements can include elevator shafts, concrete walls, bookcases, and other obstructions. Specifying internal obstructions helps to estimate the amount of coverage needed for your deployment.

1. To change the default wall line color and line type assignments, select the gear icon.
2. Select **Planning Tool** from the drop-down list.
3. To change a wall type, position your cursor on a line segment to highlight it and select **Change Wall Type**.

The drop-down list next to **Draw Wall** contains a variety of obstruction types. The number following each obstruction type indicates the estimated amount of path loss in decibels (dB) when the radio signal strikes the object at a 90° angle. Each line type displays in a different color.

4. To move a wall or object, position your cursor on a line segment to highlight it.
5. Select **Move**.
6. To clone a wall or object, position your cursor in a line segment to highlight it.
7. Select **Clone**.
8. To remove all walls, select the - icon.

Add a Floor

Your network hierarchy must contain at least one building before you can add floors.

Use this task to add a floor to a building.

1. Go to **Manage > Planning**.

2. Locate the building, to which you want to add a floor, and select .
3. In the **Add Floor** dialog, type a **Name** for the new floor.
4. From the **Associated With** menu, select a building.
5. If the floor uses 6 GHz standard power, select **Enable 6 GHz**.
6. From the **Environment** menu, choose the environment type that most closely matches your installation.
7. From the **Floor Attenuation** menu, select the noise level of the floor.
8. Enter the **Height Above Ground** and **Accuracy Range**.

**Note**

Available only if **Enable 6 GHz** is set to on.

9. Enter the installation height (the distance from floor to ceiling) and accuracy range 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.

**Note**

Accuracy Range is available only if **Enable 6 GHz** is set to on.

10. Specify the dimensions of the floor plan.
11. To specify a background image for the floor plan, select **Choose from Library**.
12. Select **SAVE**.

Related Links

[Draw a Floor Plan](#) on page 408

[Size a Floor Plan](#) on page 409

[Planning](#) on page 401

Draw a Floor Plan

If you do not have a floor plan image to upload, you can draw a floor plan using the drawing tools.

**Note**

Floor plans can only be added to floors, not to buildings or locations.

1. Use the single line tool to draw a single line.
2. Use the **Open Shape** tool to draw walls and partitions that are joined at corners.
3. Use the **Closed Shape** tool to draw walls and partitions such as elevator shafts and stairwells.
4. To exit a drawing tool, double-select anywhere on the map.
5. To change a wall type, position your cursor on a line segment to highlight it, right-select and select **Change Wall Type**.
6. To move a wall or object, highlight a line segment, right-select and select **Move**.

The appearance of the line changes, indicating that you can now move it in the map.

7. To clone a wall or object, highlight a line segment, right-select and select **Clone**.
A copy of the original line or object displays on the map.
8. To remove a line segment, highlight it, right-select and select **Remove**.
9. To remove all walls, select the **Remove All** icon.
You can only modify, move, clone, or remove individual line segments. Even if you drew an object consisting of multiple lines with the open-shape or closed-shape tool, you can only change the wall type or remove the lines of an object one segment at a time.

Size a Floor Plan

When you import a floor plan with a background image, you need to scale the floorplan. Use the following steps.

1. Select the **Resize** icon.
2. Select **Rescale**.
3. Enter the map dimensions, or use the red crosshairs on the map to enter the size manually.
4. Select the width and height.
5. Move the cross hairs to the end points of a known distance on the image.
For example, a standard-sized doorway (2.5 feet or 76 cm).
6. Enter that distance in the field.
7. Select **Apply**.

When you toggle between the width and height icons, the cross hairs in the map reposition appropriately.

Plan Devices

The following options appear at the top of the **Plan Devices** tab when you are adding a floor:

- **Choose Devices:** Displays the number of devices available to deploy. Use this option to assign real, simulated, and planned devices to the floor plan.



Note

You must first [Onboard](#) the devices before you can assign them to a floor.

- **Auto Plan For:** After you select the location wireless coverage type (basic, high-speed, voice, or location tracking), select **Auto Place** to [automatically](#) place the devices in the optimal locations for the selected wireless coverage type.
- **Add Devices:** [Manually](#) place devices based on radio band (5 GHz or 2.4 GHz), device model, signal strength, channel, and power. Select **More** to see additional settings for this function.

After you have placed simulated or planned devices on a map, or after you have onboarded real or simulated devices, you can view the [Heat Map](#) for all devices.

Automatically Add Simulated Devices

Create a network hierarchy with at least one location, building, and floor.

Use this task to automatically add simulated devices to your network to plan deployment and determine future needs. To manually place devices, see [Manually Add Simulated Devices](#) on page 410.

1. Select the type of connectivity you want from the drop-down list under **AUTO PLAN FOR**.
2. Select **AUTO PLACE**, or enter more parameters by expanding the **More** tab.
If you select a connectivity type and then select **AUTO PLACE**, ExtremeCloud IQ calculates the number and placement of devices and the radio band, channel width, device type, and signal strength settings based on the type of connectivity you selected. Expand the **More** tab, to enter these settings yourself and have ExtremeCloud IQ calculate based on your choices.
3. Select **AUTO PLACE**.
Target coverage is one factor that determines the number of devices ExtremeCloud IQ automatically places. For example, for coverage with a signal strength of -50 dBm, ExtremeCloud IQ places multiple devices on the map to ensure adequate coverage. A lower signal strength, such as -70 dBm, requires fewer devices.

ExtremeCloud IQ places simulated devices on your floor plan in the locations determined to be optimal for the type of wireless network you selected. You can now move these devices around, add known obstructions, and view heat maps for each device.

Manually Add Simulated Devices

Create a network hierarchy with at least one location, building, and floor.

Use this task to manually add simulated devices to your network to plan deployment and determine future needs. To have ExtremeCloud IQ automatically plan for you, see [Automatically Add Simulated Devices](#) on page 409.

1. From a floor plan in a building at a network location, select **PLAN DEVICES**.
2. Select the type of connectivity you need from the drop-down list under **AUTO PLAN DEVICES**.
3. In the **ADD DEVICES** section, enter the number of devices you want to add.
4. Expand the **More** tab.
5. Select the **RADIO** band.
The Channel selections available to you in the next step will change depending on whether you select 2.4 GHz or 5 GHz.
6. Select the **Channel Width**.
Channel width options vary depending on the radio band setting.
7. Select the simulated **DEVICE** model that you want to place.
8. Select the RF **SIGNAL STRENGTH**.
9. Select the **CHANNEL**.
If you select **Auto**, ExtremeCloud IQ automatically selects the channel for you.
10. Select a **POWER** setting.
This is the transmission power for the devices. The range is 1 - 20 dBm.

Icons for the simulated devices appear in the upper left corner of your floor plan. Drag them to various locations, add known obstructions to your floor plans ([Add Interior](#)

[Walls and Obstructions](#) on page 407), and view heat maps ([View Heat Maps](#) on page 411) to calculate the best deployment sites.

View Heat Maps

Populate your maps with real devices, simulated devices, or a combination.

Use this task to view device heat maps to see data about your wireless network coverage, including RSSI, SNR, channels, data rates, and interference.

1. From **Radio**, select 2.4 GHz or 5 GHz.
2. From **Devices**, choose to show heat maps for all devices on a map, only for real devices, or only for simulated devices.

If you choose to show only real devices, you can also show clients, rogues, meshed, and Ethernet devices.

3. From **Show on Heat Map** select the type of heat map.

For any option besides **None**, a panel displays the multiple floors icon, a legend to explain the colored areas on the map, and a drop-down list where you can change the power setting. For any active heat map, you can change the signal strength by selecting from a range of -40 dBm to -90 dBm in the dBm.

4. Select **None** to clear heat maps.

Heat maps display the following information:

- **RSSI:** The RSSI color bar indicates the strength of the signals, with red being the strongest and light blue the weakest. When you raise the signal strength threshold toward -40 dBm, the color bar shows only colors representing signal strength levels strong enough to pick up clients at or above that threshold. When you lower the threshold closer to -90 dBm, the color bar shows more colors, indicating more signal strength levels at which clients can connect. Hover your cursor over the color bar to see the RSSI values represented by colors.
- **SNR Heat Map:** SNR (signal-to-noise ratio) is the difference between the RSSI and the noise (low-level background radio signals that can interfere with a wireless network) in the RF environment. A high SNR means that the potential for interference is slight. A low SNR means that there is a greater potential for interference. For good wireless performance, the SNR should be at least 25 dB and never lower than 20 dB.
- **Channels Heat Map:** ExtremeCloud IQ dynamically assigns channels when you add devices either manually or automatically. Channels are displayed in different colors so that you can easily identify which channel each device is using. You can adjust the lower end of the RSSI range to change the area of coverage depicted.



Note

Channels and RSSI heat maps both display channel and RSSI values. The difference is in the emphasis that each map places on different types of data. The Channels option also shows RSSI data, but uses a single color per device to make it easier to see which channels are in use in any area. The RSSI option also shows channel data, but uses different colors to make it easier to distinguish RSSI values.

- **Data Rates Heat Map:** Set the minimum data rate that you want the APs to provide. Radio cells are colored to show the estimated data rates that are available at various distances from the AP. The colors cover a range from the minimum data rate to a maximum of 270 Mbps.

**Note**

Data rates above 54 Mbps are only possible when the radio mode is 802.11n.

Choose the estimated noise level of the site from -75 to -95 dB in increments of 5 dB to estimate the amount of interference to the RF signal from the APs.

- **Interference:** Identify sources of interference from obstructions inside your building, other electronic devices, or from other wireless networks located nearby. There are many causes of interference, such as microwave ovens, cordless phones, Bluetooth devices, wireless video cameras, and even fluorescent lights. If your network is experiencing a great deal of interference, you can try relocating devices, changing the power levels, and changing the radio band.

Devices

The **Manage > Devices** window is where users land after logging in to ExtremeCloud IQ. It features the following elements:

- A list of configured devices in the network—including controllers and controller-managed devices—along with device status and configuration details
- Filters to narrow the list of devices displayed
- Device management resources

The Devices window displays in Default view. To optimize loading performance, a limited number of Device list table columns display in the Default view. Change the **View** setting to filter the Device list, and to add to or change the informational columns displayed. See [Filter the Device List](#) for details.

Related Links

[Manage Devices](#) on page 412

[Filter the Device List](#) on page 416

[Device List Columns](#) on page 430

[Device Status Icons](#) on page 435

[Inventory View](#) on page 424

[Custom View](#) on page 430

[Utilities](#) on page 440

[Actions Menu Overview](#) on page 449

Manage Devices

The **Manage > Devices** window provides resources to facilitate device management. These resources include:

- [Status indicators](#)
- [Management tools](#)

Status Indicators

Status indicators appear in the Device list and in the banner above the Device list.

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. Some status icons are interactive. For example, select either the Configuration Audit Match  icon or Configuration Audit Mismatch  icon to open a pop-up window detailing device configuration changes that have been made since the last configuration update.



Note

The Configuration Audit icons do not apply to locally managed switches.

See [Device Status Icons](#) for a description of each icon that can appear in the Device list and the actions users can take.

The status indicators in the banner above the Device list display network-level connection information and notifications. This data automatically updates whenever you open the Devices window. [Table 102](#) describes the information each indicator provides and actions users can take:

Table 102: Banner Status Indicators

Status Indicator	Description
Connection Status	Shows the total number of connected devices and how many are online versus offline. Select the adjacent  icon to view how many of the devices are APs versus switches.
Total Apps	Shows the number of applications in use. Select the adjacent  icon to view the Most Active App and the Most Active User . Select the adjacent (non-zero) value to open the Manage > Applications window to view more details about the applications. See Manage Network Applications and Application Groups for more information.
Clients	Shows the number of connected clients. Select the adjacent (non-zero) value to open the ML Insights > Client360 window to view more details about the clients. See About Client 360 for more information.
Users	Shows the number of connected users. Select the adjacent (non-zero) value to open the Manage > Users window to view more details about the users. See Manage Users for more information.

Table 102: Banner Status Indicators (continued)

Status Indicator	Description
Anomaly Detection	The Anomaly Detection indicator shows the number of anomalies detected over the past 24 hours. Hover over the  icon to view a summary of the three most recent anomaly detections, or select View All to open the ExtremeCloud IQ CoPilot Dashboard and view more details about the anomalies.
Alerts	The Alerts indicator shows the number of Unacknowledged Critical alerts raised over the last 24 hours. Hover over the  icon to view a summary of the five most recent Critical alerts. Select View All to open the Alerts dashboard and review details of, and optionally acknowledge, the Critical alerts. See Alerts for more information.

Management Tools

Most of the tasks performed in the Device list require that you first identify the targets of any actions to be taken by selecting the check box associated with the devices in the Device list. You can individually select a target device, or you can select **Select All** and clear the check boxes for devices that you do not want to include.

When there are multiple pages of devices, to select all the devices on all pages, choose **All Pages** above the table. To deselect all the devices on all pages, choose **None**.

**Note**

After you select **All Pages**, the **Actions** menu displays only the following basic management actions:

- Assign Network Policy
- Assign Location
- Clear Audit Flag
- Reboot
- Change Management Status

Only actions applicable to the selected device are available.

The number of devices you select displays in **Showing** *<devices selected>* **of** *<total filtered devices>* **Selected**.

Choose from the following actions:

- To filter the device list:
 - Select a **View** option from the drop-down list. For more information, see [Device List Views](#) on page 416.
 - Use the sidebar filter to customize the information in the device list. For more information, see [Use the Filter Sidebar](#) on page 379.
- Select  to add a new device.

See [Add Devices Overview](#) for information about the different methods you can use to add devices to the ExtremeCloud IQ network.

- To modify an AP or switch configuration at the device level, or to view monitoring data for an AP or switch, choose from the following methods to open the **Device Details** panel where you can find **Monitoring** and **Configuration** resources:
 - Select the target device, then select .

This option is not available for locally-managed devices.

- Select the **Host Name** of a device.
- Select the **MAC** address of a device.
- Select the value under the **Clients** column for the target device.

See [Device Details Overview](#) for details about the Monitoring and Configuration resources available at the device level.

- To download data in .csv format for one or more devices, select each target device in the list, then select .
- To delete one or more devices, select each target device in the list, then select  and confirm the deletion.
- Select one or more devices in the list, then use the drop-down menus to see which [Utilities](#) and [Actions](#) are available for the device(s).



Note

Most device options are **unavailable** if an unmanaged device is selected, either alone or together with managed devices. To change the management status for one or more devices, select each target device in the list, then select [Actions](#) and use the drop-down menu to choose **Change Management Status**.

- To apply configuration changes to one or more devices, select each target device in the list, then select **Update Devices**. Alternatively, to update configuration changes for a single device, select **Update** in the **Device Details** panel.

See [Push the Device-Level Configuration to the Device](#) for details.

- Select  to customize the informational columns that display in the Device list.

See [Device List Columns](#) for further detail.

- Select  to refresh the status indicators and device data displays.
- Select the policy name under the **Network Policy** column to open the Policy configuration window and examine or edit settings.
- Select the path of the target device under the **Location** column to open the **Assign Location** window and view or edit the associated details.

Related Links

[Devices](#) on page 412

[Device Details Panel](#) on page 454

[Device List Views](#) on page 416

[Use the Filter Sidebar](#) on page 379

Filter the Device List

This section describes the options available for filtering the Device list under **Manage > Devices**.

Sidebar Filter

Use the [sidebar filter](#) to customize the information displayed in the Device list. The filter icon changes depending on whether a filter is applied. When there are no filters applied, the icon appears normal. When one or more filters are applied, the icon contains a colored dot. You can save and name multiple filters. Sidebar filter settings persist after logging out.

View Options

Filter the Device list using the **View** drop-down menu. For more information on the different views, see [Device List Views](#) on page 416.

Search Options

Use the **Search** tool to narrow the Device list. Valid search field entries include a device's **Host Name**, **MAC address**, **Serial #**, or **Management IP address**.

Column Picker

Select  to open the Column Picker and select the table columns to include in the Device list view. The options available to choose from depends on the current [View](#). Select **Reset to Defaults** to reset the column selection to the default view.

Related Links

[Use the Filter Sidebar](#) on page 379

[Device List Views](#) on page 416

[Manage Devices](#) on page 412

[Device List Columns](#) on page 430

Device List Views

The device list displays in tabular format, with device provisioning details arranged under various columns. Some columns are displayed by default. Other columns must be selected to appear in the display, using the column picker (.

The columns that appear in the device list by default, and the optional columns users can select with , depends on which of the following **Views** is selected:

- **Default**: Displays a limited set of table columns for optimal page loading performance. You can arrange Default view table columns independently of the other views using the Default column picker.
- **Wireless**: Displays information about only the wireless devices on your network.
- **LAN**: Displays data for LAN devices.
- **WAN**: Displays data for only XR routers.
- **Locally Managed**: Displays universal devices that have been onboarded to ExtremeCloud IQ to set operating system or region/Country as needed, but are not

managed directly through ExtremeCloud IQ. Locally managed devices are managed by a controller or by a ExtremeCloud IQ Site Engine that is not connected to ExtremeCloud IQ.

- **Controller:** Displays all onboarded controllers.
- **Inventory:** Displays device inventory at all sites or a specified site. The Inventory view is distinct from and uses drop down lists to filter the Device list view.
- **AFC Wireless:** Displays the APs that support 6E Standard Power under AFC server control.
- **Site Engine Managed:** Displays devices that are managed by ExtremeCloud IQ Site Engine.
- **Custom:** Displays device list table columns according to selections made with .

Choose from the following options to alter the columns display:

- Rearrange the order of the column headings by selecting a column heading and dragging it horizontally. A dotted line indicates where the heading will be inserted.
- If the columns do not fit the width of the window, scroll horizontally to view all the columns.
- Select and drag the right edge of any column to change the column width.

For more information on the different ways to filter the device list, see [Filter the Device List](#).

The selected **View** persists—even if you change windows—until you log out, after which the view setting reverts to Default view. The exception to this is for the Custom view, which you can set as the default view for the landing page when you log in to ExtremeCloud IQ.

Related Links

[Manage Devices](#) on page 412

[Filter the Device List](#) on page 416

[Device List Columns](#) on page 430

Default View

To optimize loading performance of the **Manage > Devices** landing page, a limited number of columns appear in the **Default** view.

The following columns appear in the **Default** view:

• Status	• Location
• Host Name	• Serial #
• Network Policy	• Model
• Uptime	• OS Version
• MGT IP Address	• Updated ON
	• IPv6

- Clients
- MAC

**Note**

You cannot add new columns to the **Default** view.

For column descriptions, as well actions that users can take, see [Device List Columns](#) on page 430.

Related Links

[Manage Devices](#) on page 412

[Device List Views](#) on page 416

[Filter the Device List](#) on page 416

[Device List Columns](#) on page 430

Wireless View

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

**Note**

For column descriptions, as well actions that users can take, see [Device List Columns](#) on page 430.

Go to **Manage > Devices**, then select **Wireless** from the **View** drop-down list.

The following columns appear by default in the **Wireless** view:

• Status	• Updated On
• Host Name	• WiFi0 Channel
• Network Policy	• WiFi0 Power
• Managed By	• WiFi1Channel
• Uptime	• WiFi1 Power
• MGT IP Address	• WiFi2 Channel
• Default Gateway	• WiFi2 Power
• Clients	• Managed
• MAC	• Country
• Location	• WiFi0 Radio Profile
• Serial #	• WiFi1 Radio Profile
• Model	• WiFi2 Radio Profile
• OS Version	• OS

The following columns are optional. To add these columns to your **Wireless** view, select .

• Last Seen On	• Device Mode
• Device Function	• WAN IP Address
• Template	• Public IP Address

- Cloud Config Groups
- Site
- Feature Liense
- Device License
- CoPilot
- Branch ID
- Service Tag
- VPN Service
- Stack Unit
- Stack Role
- IQAgent
- MGT VLAN
- Make
- IoT0 Profile
- IoT0 EUI-64
- IoT0 Extended MAC
- RADIUS Server
- IPv6
- Eth0 LLDP Port #
- Eth0 LLDP Sys-ID
- Eth0 LLDP Sys-Name
- Eth1 LLDP Port #
- Eth1 LLDP Sys-ID
- Eth1 LLDP Sys-Name
- Description
- Application Status

Related Links

[Manage Devices](#) on page 412

[Device List Views](#) on page 416

[Filter the Device List](#) on page 416

[Device List Columns](#) on page 430

LAN View

The **LAN** view provides a list of Local Area Network (LAN) devices.



Note

For column descriptions, as well actions that users can take, see [Device List Columns](#) on page 430.

Go to **Manage > Devices**, then select **LAN** from the **View** drop-down list.

The following columns appear by default in the **LAN** view:

- Status
- Host Name
- Network Policy
- Managed By
- Uptime
- MGT IP Address
- Default Gateway
- Clients
- MAC
- Location
- Serial #
- Feature License
- Device License
- Service Tag
- Stack Role
- OS Version
- IQAgent
- Updated On
- MGT VLAN
- Make
- Managed
- Eth0 LLDP Port #
- Eth0 LLDP Sys-ID
- Eth0 LLDP Sys-Name
- Eth1 LLDP Port #
- Eth1 LLDP Sys-ID
- Eth1 LLDP Sys-Name

- Model
- Stack Unit
- Description
- OS

The following columns are optional. To add these columns to your **LAN** view, select .

- Last Seen On
- Device Function
- Template
- Cloud Config Groups
- Site
- Feature Liense
- Device License
- CoPilot
- Branch ID
- Service Tag
- VPN Service
- WiFi0 Channel
- WiFi0 Power
- WiFi1 Channel
- WiFi1 Power
- WiFi2 Channel
- WiFi2 Power
- Device Mode
- WAN IP Address
- Public IP Address
- Country Code
- WiFi0 Radio Profile
- WiFi1 Radio Profile
- WiFi2 Radio Profile
- IoT0 Profile
- IoT0 EUI-64
- IoT0 Extended MAC
- RADIUS Server
- IPv6
- Application Status

Related Links

[Manage Devices](#) on page 412

[Device List Views](#) on page 416

[Filter the Device List](#) on page 416

[Device List Columns](#) on page 430

WAN View

The **WAN** view provides a list of Wide Area Network (WAN) devices.



Note

For column descriptions, as well actions that users can take, see [Device List Columns](#) on page 430.

Go to **Manage > Devices**, then select **WAN** from the **View** drop-down list.

The following columns appear by default in the **WAN** view:

- Status
- Host Name
- Network Policy
- Managed By
- Uptime
- MGT IP Address
- Default Gateway
- Branch ID
- Model
- VPN Service
- OS Version
- Updated On
- MGT VLAN
- Mode

- Clients
- MAC
- Location
- Serial #
- Device License
- Managed
- WAN IP Address
- Public IP Address
- Country
- OS

The following columns are optional. To add these columns to your **WAN** view, select .

- Last Seen On
- Device Function
- Template
- Cloud Config Groups
- Site
- Feature Liense
- CoPilot
- Service Tag
- Stack Unit
- Stack Role
- IQAgent
- WiFi0 Channel
- WiFi0 Power
- WiFi1 Channel
- WiFi1 Power
- WiFi2 Channel
- WiFi2 Power
- Make
- WiFi0 Radio Profile
- WiFi1 Radio Profile
- WiFi2 Radio Profile
- IoT0 Profile
- IoT0 EUI-64
- IoT0 Extended MAC
- RADIUS Server
- IPv6
- Eth0 LLDP Port #
- Eth0 Sys-ID
- Eth0 LLDP Sys-Name
- Eth1 LLDP Port #
- Eth1 Sys-ID
- Eth1 LLDP Sys-Name
- Description
- Application Status

Related Links

[Manage Devices](#) on page 412

[Device List Views](#) on page 416

[Filter the Device List](#) on page 416

[Device List Columns](#) on page 430

Locally Managed View

The **Locally Managed** view provides a list of locally managed devices.



Note

For column descriptions, as well actions that users can take, see [Device List Columns](#) on page 430.

Go to **Manage > Devices**, then select **Locally Managed** from the **View** drop-down list.

The following columns appear by default in the **Locally Managed** view:

- Status
- Host Name
- Stack Role
- OS Version

- Network Policy
- Managed By
- Uptime
- MGT IP Address
- Default Gateway
- Clients
- MAC
- Location
- Serial #
- Model
- Stack Unit
- IQAgent
- Updated On
- WiFi0 Channel
- WiFi0 Power
- WiFi1 Channel
- WiFi1 Power
- WiFi2 Channel
- WiFi2 Power
- MGT VLAN
- OS

The following columns are optional. To add these columns to your **Locally Managed View** view, select .

- Last Seen On
- Device Function
- Template
- Cloud Config Groups
- Site
- Feature License
- Device License
- CoPilot
- Branch ID
- Service Tag
- VPN Service
- Make
- Device Mode
- Managed
- WAN IP Address
- Public IP Address
- Country Code
- WiFi0 Radio Profile
- WiFi1 Radio Profile
- WiFi2 Radio Profile
- IoT0 Profile
- IoT0 EUI-64
- IoT0 Extended MAC
- RADIUS Server
- IPv6
- Eth0 LLDP Port #
- Eth0 LLDP Sys-ID
- Eth0 LLDP Sys-Name
- Eth1 LLDP Port #
- Eth1 LLDP Sys-ID
- Eth1 LLDP Sys-Name
- Description
- Application Status

Related Links

[Manage Devices](#) on page 412

[Device List Views](#) on page 416

[Filter the Device List](#) on page 416

[Device List Columns](#) on page 430

Controller View

The **Controller** view provides a list of controller devices.



Note

For column descriptions, as well actions that users can take, see [Device List Columns](#) on page 430.

Go to **Manage > Devices**, then select **Controller** from the **View** drop-down list.

The following columns appear by default in the **Controller** view:

- Status
- Host Name
- Network Policy
- Managed By
- Uptime
- MGT IP Address
- Default Gateway
- Clients
- MAC
- Location
- Serial #
- Model
- Stack Unit
- Stack Role
- OS Version
- IQAgent
- Updated On
- WiFi0 Channel
- WiFi0 Power
- WiFi1 Channel
- WiFi1 Power
- WiFi2 Channel
- WiFi2 Power
- MGT VLAN
- OS

The following columns are optional. To add these columns to your **Controller** view, select .

- Last Seen On
- Device Function
- Template
- Cloud Config Groups
- Site
- Feature License
- Device License
- CoPilot
- Branch ID
- Service Tag
- VPN Service
- Make
- Device Mode
- Managed
- WAN IP Address
- Public IP Address
- Country Code
- WiFi0 Radio Profile
- WiFi1 Radio Profile
- WiFi2 Radio Profile
- IoT0 Profile
- IoT0 EUI-64
- IoT0 Extended MAC
- RADIUS Server
- IPv6
- Eth0 LLDP Port #
- Eth0 LLDP Sys-ID
- Eth0 LLDP Sys-Name
- Eth1 LLDP Port #
- Eth1 LLDP Sys-ID
- Eth1 LLDP Sys-Name
- Description
- Application Status

Related Links

[Manage Devices](#) on page 412

[Device List Views](#) on page 416

[Filter the Device List](#) on page 416

[Device List Columns](#) on page 430

Inventory View

Go to **Manage > Devices**, then select **Inventory** from the **View** drop-down list.

The **Inventory** window includes:

- A [list of devices](#) at all sites or a specified site, along with details about the devices
- [Filters](#) to narrow the list of devices displayed
- [Management tools](#)

Device List Details

The Inventory device list displays in tabular format, with device provisioning details arranged under various columns. The Inventory view displays a fixed set of columns, as follows:

- Device Type
- Managed By
- Device License
- CoPilot
- OS Version
- Country
- Host Name
- Status
- MAC
- Location
- Serial #
- Model

See [Device List Columns](#) for a description of the type of information displayed under these columns.

Filters

Use the **Search** tool to narrow the device list. Valid search field entries include a device's **Host Name**, **MAC address**, **Serial #**, or **Management IP address**.

The following filters are available to refine the list of devices in the Inventory view. Use the filter drop-down menus to select from the available options.

Status

- All
- Connected
- Disconnected
- Pre Provisioned
- Undetermined

Device Type

- All
- Access Point

- Router
- Switch
- Stack

OS Version

- All
- Choose from the list of currently available OS versions.

Managed By

- All
- Choose from the list of currently available management platforms.

Management Tools

Choose from the following actions:

- Select  to refresh the display.
- Select  to download a .csv file containing a record of the devices in the list.
- To exit the Inventory window, choose another option from the **View** menu.

Related Links

[Devices](#) on page 412

[Manage Devices](#) on page 412

[Filter the Device List](#) on page 416

AFC Wireless View

The **AFC Wireless** view shows all access points (APs) that support 6E Standard Power under Automatic Frequency Coordination (AFC) server control. A dashboard summary displays AFC Status, Geo Location, and AFC Mismatch information for the APs.

**Note**

AFC is supported on AP4020/4020X/AP4020FX (indoor), AP4060/AP4060X (indoor/outdoor), AP5020 (indoor), and AP5050 (indoor/outdoor) devices.

AFC Status and Geo Location are not related to the AP's current connection status. They indicate that the AP can function within the region it is connected to. If an AP is no longer connected, the AFC Status and Geo Location are not erased. Both the AFC Status and Geo Location remain unchanged until the expiration time is reached. When the expiration time is reached, the AFC Status changes to "Grace Period" and the Geo Location changes to "Not Available".

Go to **Manage > Devices**, then from the **View** drop-down list, select **AFC Wireless**.

AFC Service Connection Status

Select **AFC Service** to view the AFC service connection status. AFC service status indicates whether the device is successfully connected to the AFC server. The graph shows the AFC service availability for the last 24 hours

Table 103: AFC Service Details

Field	Description
Mode	Indicates if the AFC service is Connected or Not Connected to the AFC server.
Address	Displays the URL or IP address of the connected AFC server.
Country	Displays the country in which the AFC service is operating.
Time Range	The displayed connectivity time range. To change the displayed time range, select 1 Hour , 2 Hours , 4 Hours , 8 Hours , or 24 Hours . 24 Hours is selected by default.
Graph	Displays the connectivity status for the selected Time Range . To see the connection details for a specific moment, hover over the graph timeline. A popup window appears, showing the date, time, and connection status for that particular point.



Note

Select **Clear Selection** to reset back to the default time range.

To save the graph details for future reference, select the **Chart Context Menu** (≡) icon, and then select one of the following options:

- Print chart
- Download PNG image
- Download SVG vector image
- Download JPEG image
- Download PDF document

Graph Details

The **AFC Status** graph displays the status of each AP:

- **Available:** AFC spectrum is available until 24 hours after the AFC server assigned the spectrum.
- **Pending:** The initial state after the AP powers up. The AP waits for “Geo Location Available” and AFC spectrum response from the AFC server.
- **Grace Period:** The AFC spectrum must be renewed every 24 hours. If the AFC server is not reachable, or not responding at the selected time, the status changes to **Grace Period**. The status remains in **Grace Period** until the next midnight UTC. If the AFC server stays down, the status changes to **Pending** and the radios are shut down. After the AFC server recovers, the status changes to **Pending**.

The **Geo Location** graph displays the geo location status of each AP:

- **Available:** The GPS has locked on sufficient satellites to determine the coordinates of the AP. The GPS locks within 2 minutes if the AP is exposed to open sky. If not, the time is unpredictable, depending on signal obstructions.
- **Not Available:** The initial state after the AP powers up.

The **AFC Spectrum Mismatch** graph highlights the number of APs with discrepancies between their expected AFC settings and the actual spectrum usage.



Note

Hover over the graph colors to see the percentage for each individual status.

Device List Details

The Device List displays the following **AFC Wireless** view columns by default:

• Status	• Managed
• Host Name	• Country
• Network Policy	• Geo Location
• Managed By	• WiFi Radio
• Uptime	• AFC Status
• MGT IPAddress	• Expire
• Clients	• Power Mode
• Location	• Channel
• Site	• Req. Channel
• Serial #	• Power
• Model	• Req. Power

See [Device List Columns](#) for column information descriptions.

Management Tools

Choose from the following actions:

- To add a new device, select . For more information, see [Add Devices Overview](#) on page 22.
- To download a .csv file containing a record of the devices in the list, select .
- To delete one or more devices, select the target device in the list, then select and confirm the deletion.
- To filter the device list, see [Filter the Device List](#) on page 416.
- To view which [Utilities](#) and [Actions](#) are available for the device, select one or more devices from the list, then use the associated menu.
- To hide and remove columns, select .



Note

To add new columns, go to **Custom** view.

- To refresh the display, select .
- To exit the **AFC Wireless** view, choose another option from the **View** menu.

Related Links

[Devices](#) on page 412

[Manage Devices](#) on page 412

[Add Devices Overview](#) on page 22

[Filter the Device List](#) on page 416

Site Engine Managed View

The **Site Engine Managed** view shows all Site Engine managed devices in one separate view for easier management and monitoring.

To access this view, go to **Manage > Devices**, then from the **View** drop-down list, select **Site Engine Managed**.

The **Site Engine Managed** view includes a list of devices and their details, filters to narrow the displayed devices, and management tools.

Device List Details

The Device List column display is configurable. The **Site Engine Managed** view displays the following columns by default:

- Last Seen On
- OS
- Status
- Hostname
- Uptime
- Mgt IP Address
- IPv6
- Model
- MAC
- OS version
- Serial #
- Location
- Managed
- Stack Unit
- Stack Role
- Cloud Config Groups

See [Device List Columns](#) for column information descriptions.

Filters

Use the Search tool to find specific device information. The following column values are valid search criteria: Host Name, MAC Address, Serial Number, or Management IP Address.

The following filters are available to refine the list of devices in the Site Engine Managed view. Use the filter drop-down menus to select from the available options.

Table 104: Site Engine Managed view filter options

Filter	Drop-down options
Status	All
	Connected
	Disconnected
	Pre Provisioned
	Undetermined
OS Version	All
	Choose from the list of currently available OS versions.
Managed	All
	New
	Setting up
	Managed
	Unmanaged

Management Tools

Choose from the following actions:

- To refresh the display, select .
- To download a .csv file containing a record of the devices in the list, select .
- To delete one or more devices, select the target device in the list, then select  and confirm the deletion.
- To view which [Utilities](#) and [Actions](#) are available for the device, select one or more devices from the list, then use the associated menu.
- To hide and remove columns, select .



Note

To add new columns, go to Customer view.

- To exit the Site Engine Managed window, choose another option from the **View** menu.

Related Links

[Devices](#) on page 412

[Manage Devices](#) on page 412

[Filter the Device List](#) on page 416

Custom View

Go to **Manage > Devices**.

Use this task to create or edit a Custom view of the device list, and optionally, to set it as the default view for the ExtremeCloud IQ landing page. Only one Custom view can exist per administrator account.



Note

Choosing to make the Custom view the default view for the ExtremeCloud IQ landing page may impact page loading performance.

1. Use the **View** drop-down menu to select **Custom**.
2. Select  adjacent to the **View: Custom** field.
3. In the **Name Custom View** pop-up window:
 - a. Add or edit the name for the Custom view.
 - b. Optionally, select the **Save as default** check box to set the Custom view as the default view when you log in to ExtremeCloud IQ.
4. Select **Save** to commit the changes, or select **Cancel**.
5. Select  to pick the columns you want to display in the device list for the Custom view.

Related Links

[Filter the Device List](#) on page 416

[Device List Columns](#) on page 430

Device List Columns

The [Device List Columns](#) table lists and describes the available columns for the device list views, as well actions that users can take. For more information about the available views, see [Device List Views](#) on page 416.

Table 105: Device List Columns

Column Heading	Description
AFC Status	Indicates the AFC status of the AP. Status options include: • Available • Pending • Grace Period Note: AFC Status is not related to the AP's current connection status. If an AP is no longer connected, the AFC Status remains unchanged until the AP expiration time is reached. When the expiration time is reached, the AFC Status changes to 'Grace Period'.
Application Status	The application status of the device.
Branch ID	The identifier used to allocate specific subnetworks to XR routers.

Table 105: Device List Columns (continued)

Column Heading	Description
Channel	The operating channel of the device.
Clients	The number of clients connected to this device.
Cloud Config Groups	Identifies all associated cloud config groups for this device.
CoPilot	Identifies whether the CoPilot subscription is used by ExtremeCloud IQ. Valid values are: • None—This indicates one of the following conditions: ◦ CoPilot is disabled. ◦ Device is not compatible. ◦ Device is unmanaged. ◦ Customer intentionally revoked CoPilot subscription. • CoPilot Active—CoPilot subscription is active for the device. • Unlicensed—CoPilot subscription has expired.
Country	The device country location code.
Country Code	The device country location code.
Default Gateway	The management interface default gateway of the managed device.
Description	Free form text field available for use on IQ Engine-based devices.
Device Function	The product family of the device.
Device License	Identifies the ExtremeCloud IQ subscription type that is used to manage the device. Valid values are: • Pilot—ExtremeCloud IQ Pilot subscription • Navigator—ExtremeCloud IQ Navigator subscription • Legacy—Legacy entitlement key • Unlicensed—Device without an active subscription • Not Required—Ping Only device reported by ExtremeCloud IQ Site Engine, APs reported by ExtremeCloud IQ Controller, Digital Twin (DT), Simulated, or Unmanaged by user
Device Mode	Identifies the IQ Engine AP role in a wireless mesh.
Eth0 LLDP Port #	The switch port name that the AP is connected to via ETH0.
Eth0 LLDP Sys-ID	The switch port MAC address that the AP is connected to via ETH0.
Eth0 LLDP Sys-Name	The switch host name that the AP is connected to via ETH0.
Eth1 LLDP Port #	The switch port name that the AP is connected to via ETH1.

Table 105: Device List Columns (continued)

Column Heading	Description
Eth1 LLDP Sys-ID	The switch port MAC address that the AP is connected to via ETH1.
Eth1 LLDP Sys-Name	The switch host name that the AP is connected to via ETH1.
Expire	The expiration of the AFC checkin. The AFC requires checkin every 24 hours.
Feature License	Identifies the licensed features the device is using. Valid values are: None, MacSec, Premier. MACsec features require a MACsec license. Feature requirements for a Premier license are platform- and network operating system-specific. For details and ordering information, see the switch datasheet(s).
Geo Location	Indicates if the AP can function within the region it is connected to. Note: Geo Location is not related to the AP's current connection status. If an AP is no longer connected, the Geo Location remains unchanged until the AP expiration time is reached. When the expiration time is reached, the Geo Location changes to 'Not Available'.
Host Name	The host name of the device. Select the host name to open the Device Details panel, which provides monitoring and configuration resources for managing this device. This column is sortable.
IoT0 EUI-64	A unique identifier assigned to a device in a Thread network .
IoT0 Extended MAC	A unique identifier assigned to a device in a Thread network .
IoT0 Profile	The name of the profile assigned to the IoT0 wireless interface.
IPv6	The IPv6 address of the client device.
IQAgent	For switches, the IQ Agent version. IQ Agent enables communication between switches and ExtremeCloud IQ.
Last Seen On	The date and time the device was last connected to ExtremeCloud IQ.

Table 105: Device List Columns (continued)

Column Heading	Description
Location	The location of the device in your network. To assign or change the location, choose one of the following methods: • Select the corresponding checkbox for a device, and then select Actions > Assign Location. • Select the name in the Location column. In the dialog box under Global View, select a new location and then select Assign. Note: For devices managed by ExtremeCloud IQ Site Engine the location is read-only. You can assign the location in ExtremeCloud IQ Site Engine.
MAC	The MAC address of the device.
Make	Extreme Networks: For example, Fabric Engine, Switch Engine, EXOS, VOSS, WiNG. External: For example CISCO.
Managed	Indicates whether the device is currently managed.
Managed By	Identifies which product manages the device, as follows: • ExtremeCloud IQ • ExtremeCloud IQ Site Engine (Site Engine also manages third-party devices) • ExtremeCloud IQ Controller • ExtremeWireless WiNG When devices are managed locally, this column is empty.
MGT IP Address	The IP address of the device.
MGT VLAN	The management VLAN for this device.
Model	The hardware model of the device. The hardware model and serial number appear on a label on the underside of the chassis.
Network Policy	The network policy assigned to this device. If you have not assigned a network policy, you can do so now. Select the check box for the device, and then select Actions > Assign Network Policy. Note: This option is not available for locally managed devices.
OS	The operating system currently running on the device. For example, FABRIC, WiNG, CLOUD-IQ ENGINE.
OS Version	The version that is currently running on the device.
Power	The requested power of the device.
Power Mode	The power mode of the device. The AP5050 is always in Standard Power (SP).

Table 105: Device List Columns (continued)

Column Heading	Description
Public IP Address	For devices managed using an RFC 1918 private address range behind a NAT device, this is the public IP address of the NAT device.
RADIUS Server	Indicates whether the managed device is acting as a RADIUS server. IQ Engine only.
Req. Channel	The AFC requested channel.
Req. Power	The AFC requested power.
Serial #	The serial number of the device.
Service Tag	Asset identification. Managed Dell devices only.
Site	The site assigned to the managed device.
Stack Role	The role (primary, secondary, or member) of a switch in a stack.
Stack Unit	The unit number of a switch in a stack.
Status	Status icons indicate a device's connection status and provide other important device indications. Hover over an icon to view its function or other related information. For details about each icon's purpose, see Device Status Icons on page 435. Note: The Configured at Device Level () icon indicates that a switch or AP uses device-level configuration settings instead of the device template (network policy) configuration. To revert to the device template configuration, select the check box associated with the device, then from the Actions menu, choose Revert Device to Template Defaults.
Template	The template assigned to the device.
Updated On	The last time the configuration on this device was updated. If an update was not successful, ExtremeCloud IQ displays a Device Update Failed error message that includes configuration, firmware, certificate, and signature update issues, reboot timeouts, and error information specific to devices configured using Auto Provisioning. Hover over the error message to see details. To view error message descriptions listed by device and timestamp, select the error message link.
Uptime	The amount of time since the device last rebooted and re-connected.
VPN Service	The Layer 3 VPN assigned to the policy. XR routers only.
WAN IP Address	The WAN IP address obtained by the device. XR routers only.
WiFi Radio	Indicates which WiFi radio is enabled for the AP.

Table 105: Device List Columns (continued)

Column Heading	Description
WiFi0 Channel	The channel currently used by the WiFi0 radio. Refer to the data sheet for your device and your software-defined radio (SDR) configuration to determine the band on which the WiFi0 radio is operating.
WiFi0Power	The power level of the WiFi0 radio.
WiFi1 Channel	The channel currently used by the WiFi1 radio. Refer to the data sheet for your device and your software-defined radio (SDR) configuration to determine the band on which the WiFi1 radio is operating.
WiFi1 Power	The power level of the WiFi1 radio.
WiFi2 Channel	The channel currently used by the WiFi2 radio. Refer to the data sheet for your device and your software-defined radio (SDR) configuration to determine the band on which the WiFi2 radio is operating.
WiFi2 Power	The power level of the WiFi2 radio.
WiFi0 Radio Profile	The radio profile assigned to the WiFi0 interface on an IQ Engine AP.
WiFi1 Radio Profile	The radio profile assigned to the WiFi1 interface on an IQ Engine AP.
WiFi2 Radio Profile	The radio profile assigned to the WiFi2 interface on an IQ Engine AP.

Related Links

[Manage Devices](#) on page 412

[Device List Views](#) on page 416

[Filter the Device List](#) on page 416

Device Status Icons

Go to **Manage > Devices**.

[Device Status Icons](#) describes the icons that can appear under the **Status** column in the Device list. Actions users can take are also described. To display the Device List, go to **Manage > Devices**.

Table 106: 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 . For more information, select the AFC status icon to open the AFC Wireless view of the selected device.
	Provisioned Device	An administrator has provisioned the device, but the device has not yet communicated with ExtremeCloud IQ. 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 Manage Status > Managed Devices menu option.
	Connected Device	Device is actively communicating with ExtremeCloud IQ.
	Disconnected Device	Device is not actively communicating with ExtremeCloud IQ. 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 or when there are misconfigured firewalls or ACL rules. Action: Ensure the device is connected to the network and powered on and ensure that communication can occur through logical barriers such as firewalls.
	No Connection	This device has not yet made a connection with ExtremeCloud IQ. It can take up to 10 minutes for a device to appear after the initial onboarding process. If the device has not successfully connected after 10 minutes.
	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 <i>Device update failed</i> .
	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.
	Undetermined	Device status is undetermined. Cause: This condition can arise when the indicators are ambiguous, unknown, or appear contradictory due to other factors. 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.
	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.

Table 106: Device Status Icons (continued)

Icon	Icon Name	Description
	Configuration Audit Match	The network policy configuration matches the current running configuration. Select the icon to open a pop-up window detailing the configuration changes that occurred since the last Update Devices operation. • Audit tab — lists any modifications made since the previous configuration update. • Delta tab — shows CLI commands that have changed since the previous update. • 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. Note: Not applicable for locally managed switches.
	Configuration Audit Mismatch	The network policy configuration does not match the current running configuration. 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. Action: Upload the network policy to the device. 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. Note: Not applicable for locally managed switches.
	Pending Configuration	Device is currently offline and will receive its latest assigned configuration once it reconnects to the network.
	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.
	Anchor	Device is set as an anchor in an indoor AFC deployment.

Table 106: Device Status Icons (continued)

Icon	Icon Name	Description
	Device Update Unsuccessful	Device did not accept the OS or configuration upload. 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. 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.
	Managed by ExtremeloT	Device is provisioned to function with ExtremeloT.
	Thread Commissioner Running	The AP is designated Commissioner in the IoT Thread network.
	Monitoring Unassociated Clients	Device is using presence analytics to monitor client devices that are not associated to the network, such as passersby.
	Switch Stack	Device is a switch stack. Select the icon to expand the device list view to include details for the switch stack members.
	Switch Stack Warning	One or more stack member switches is not associated to the master stack node. 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. Action: Ensure that the switch slot has power and that the stacking cables are properly connected.
	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 On	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.
	Sensor Mode - Interface Inactive	Device is functioning as a sensor, but the monitoring interface is not active and is not monitoring the RF environment.
	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.
	VPN Server - Tunnel Up	Device is functioning as a VPN server and the VPN tunnel is up, healthy, and operating properly.

Table 106: Device Status Icons (continued)

Icon	Icon Name	Description
	VPN Server - Tunnel 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. 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. Action: Consult the VPN troubleshooting tools in ExtremeCloud IQ. 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 - Tunnels Up and Down	Some of the VPN server tunnels are administratively up but operationally down. Cause: VPN client might be down, or unreachable. Action: Ensure that the VPN clients are powered on, connected to the network, and communicating with ExtremeCloud IQ. In addition, ensure that there is connectivity and communication between the VPN server and clients.
	VPN Client - Tunnels Up	Device is functioning as a VPN client and the VPN tunnel is up, healthy, and operating properly.
	VPN Client - 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. 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. Action: Consult the VPN troubleshooting tools in ExtremeCloud IQ. 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 - Tunnels Up and Down	Some of the VPN client tunnels are administratively up but operationally down. Cause: VPN server might be down, or unreachable. Action: Ensure that the VPN server is powered on, connected to the network, and communicating with ExtremeCloud IQ. In addition, ensure that there is connectivity and communication between the VPN server and client.
	Locally Managed	Device is managed by a platform other than ExtremeCloud IQ, but it is monitored by ExtremeCloud IQ. For example, other platforms can include 3rd party, ExtremeCloud IQ Site Engine, or ExtremeCloud IQ Controller.

Table 106: Device Status Icons (continued)

Icon	Icon Name	Description
	Locally Managed (No ExtremeCloud IQ)	Device or its management platform are not visible in ExtremeCloud IQ. 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 is unaware of the status. 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. Afterward, ensure that any applications that lie in the communication path are receiving, processing, and sending data appropriately.
	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. 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. Action: Ensure that there is connectivity between FA device and server, and that FA server functionality is enabled on the peer switch.
	Digital Twin	Device is a simulated device.
	FIPS Mode	Device is in FIPS mode.

Utilities

Go to **Manage > Devices > Utilities**

The **Utilities** drop-down list offers a variety of useful troubleshooting tools.



Note

Utilities are only available for devices managed by ExtremeCloud IQ; not devices managed by ExtremeCloud IQ Site Engine. Not all utilities are available for all device types. Depending on the type of device you select, you will see a subset of the available utilities.

If you have a large number of devices, use the steps below to help locate a specific device to which you want to apply any of these utilities.

There are a number of **diagnostics** options based on the type of device you choose. For more information on some of the more complicated options, see:

- [Device Diagnostics](#) on page 441
- [Restart Device to Default](#) on page 443
- [Spectrum Intelligence Details](#) on page 443
- [Restart PSE](#) on page 445

Status options include:

- Advanced Channel Selection Protocol
- Interface
- [Wi-Fi Status Summary](#) on page 445

Tools options include:

- [Client Information](#) on page 446
- [Get Tech Data](#) on page 446
- [Locate Device](#) on page 446
- [Neighbor Information](#) on page 446
- [Packet Capture \(for IQ Engine APs\)](#) on page 447
- [Switch VLAN Probe Utility](#) on page 448
- [SSH Availability](#) on page 448

Use the following steps to locate a device:

1. If you know an identifying characteristic (host name, MAC address, or serial number) of a device that you want to troubleshoot and you see it in the table, proceed to Step 2.
 - a. If you know an identifying characteristic but do not see the device in the main table—perhaps because there are a large number of devices—start typing the host name, MAC address, or serial number in the **Enter Client Host Name** or **Mac Address** field.

This field will auto-complete your entry with one or more possibilities, which are displayed in a drop-down list. The more characters you enter, the more specific the result. Choose the item you want from the list.
 - b. If you do not see a device in the main table and do not recall any identifying characteristics, try applying one or more filters until you see the one you want.
2. Select the check box for that device to see the results.

Device Diagnostics

This utility enables you to run CLI commands on a device from inside the ExtremeCloud IQ interface to perform basic network connectivity diagnostics, check status, and diagnose several functions.

1. Select a device to diagnose.

2. Select **Diagnostics**.
3. Select one of the following CLI commands:
 - **Ping**: Have the selected device ping 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 Log**: Displays the event log for the device.
 - **Show Version**: Displays the version running on the device.
 - **Show Running Config**: Displays the configuration running on the device.
 - **Show Startup Config**: Displays the configuration used by the device on reboot.
 - **Show IP Routes**: Displays the IP routing table.
 - **Show MAC Routes**: Displays the MAC forwarding table.
 - **Show ARP Cache**: Displays the ARP cache.
 - **Show Roaming Cache**: Displays 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 DNXp Neighbors**: Displays 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 DNXp Cache**: Displays the DNXp cache, which provides information that the device uses to form an association with a client that has already associated with a DNXp neighbor and that could possibly roam to it.
 - **Show AMRP Tunnel**: Displays information about DNXp, INXP, and VPN tunnels, including tunnel type, the peer IP address, and how long the tunnel has been up.
 - **Show GRE Tunnel**: Displays 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.
 - **Debug AFC Data Exchange**: Displays raw AFC request and response data from the AFC server.
 - **Show Tunnel Clients**: Displays a list of tunnels with their IP address and a list of MAC addresses, tunneled through the corresponding GRE tunnel.
 - **Show IKE Event**: Displays 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**: Displays 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 IPsec SA**: Displays 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 CPU:** Displays total, per user, and per system CPU utilization.
- **Show Memory:** Displays total, free, used, buffered, and cached memory.

**Note**

For Tunnel Concentrator devices, only the following subset of diagnostics is available:

- **Ping**
- **Show GRE Tunnel**
- **Show Tunnel Clients**
- **Show Log**

Restart Device to Default

You can reset one or more selected devices to their default configuration. A warning statement displays after you select this option. If you select **Yes**, the operation removes all existing settings (except bootstrap settings) and reboots the selected devices.

Spectrum Intelligence

(Applies to APs only). Spectrum Intelligence provides a live view of the RF (radio frequency) environment to help you plan for future VLAN deployment or troubleshoot VLAN issues such as high retransmission rates caused by device interference or slow connections due to overuse. There are two main spectrum intelligence functions: providing a graphical rendering of the RF environment in an FFT (fast Fourier transform) trace and swept spectrogram and identifying interfering devices, such as cordless phones and microwave ovens.

**Note**

Spectrum Intelligence is only supported on 2.4 and 5 GHz radios. To use Spectrum Intelligence, you must have at least one SSID configured on your VLAN on at least one AP running ExtremeCloud IQ 11.28 and IQ Engine 8.0 or later.

The AP5020 requires 802.3bt power for Spectrum Intelligence functionality.

1. Select the check boxes for up to five supported APs.
2. Select **Utilities > Spectrum Intelligence**.
3. A message warns you that performing this function can affect performance.
4. Select **Yes** to see the analysis panel, containing a status bar, a graphical analysis feedback section, and the interference reports.

For information about the data panel, see [Spectrum Intelligence Details](#) on page 443.

Spectrum Intelligence Details

The **Spectrum Intelligence** data panel contains the following information:

Status Bar

The **Status Bar** at the top of the panel displays the current analysis parameters, including which AP or APs are running the scan, the channels, run time, and band (2.4 GHz or 5 GHz). You can change these settings for each and then select **Apply**.

Below the Status Bar, on the right side of the panel you will see the time remaining in the current scan. Select **Stop** to end the current analysis.



Note

Spectrum analysis automatically shuts down after 30 minutes.

Data Collect Interval: The data collection interval refers to the time interval between scans of the spectrum. Each time the AP scans the spectrum, it updates the display. If the data collection interval is five seconds, then the AP scans every five seconds and updates the display. You can change the interval from 1 to 30 seconds.

Graphical Analysis Feedback

This area displays graphs of the received signals, arranged by default in a two-by-two array. Use the expand and collapse arrows in the upper right corner of each graph to enlarge or reduce the graph for visibility.

- **Real-time FFT:** The real-time FFT trace indicates the power of a signal (vertical axis) along a domain of frequencies (horizontal axis).
- **FFT Duty Cycle:** The FFT duty cycle is the amount of time as a percent of total time that the AP receives a signal 20 dB or more above the noise floor. The FFT duty cycle is often referred to as channel utilization because it indicates to what extent a channel is actually in use in terms of the relative amount of time the signal is present (vertical axis).
- **Swept Spectrogram:** A swept spectrogram tracks the signal power over time. It produces a color-coded sweep of spectral information that shows the real time FFT in terms of its historical values. The swept spectrogram—also called a heat map—reports the frequency on the horizontal axis, the history (in sweeps) on the vertical axis, and the power encoded as a set of colors.
- **Swept Spectrogram-FFT Duty Cycle:** A swept spectrogram of the FFT duty cycle tracks the duty cycle over time. This spectrogram produces a color-coded sweep of duty cycle information with frequency on the horizontal axis, history (in sweeps) on the vertical axis, and the duty cycle encoded as a set of colors.

Interference Reporting

The Interference Signature table below the graphs displays any sources of RF interference that the spectrum analyzer can identify. This area provides a summary of all interference sources for quick review. This area contains six columns to help identify the affected channels and the approximate position of the interference.

- **Extreme Device Name:** The name of the AP that is reporting the interference. If an interference source is reported by a few APs, but not others, you can use this to approximate the physical location of the interference.
- **Device Function:** Indicates the device type of the interferer, such as a cordless phone, microwave oven, or video bridge. The device type listing can help determine whether the interference source might be a security concern.

- **Discovered:** Shows the date and time that the AP discovered the source of the interference. You can track regular, periodic, and intermittent interference sources using this information.
- **Channel Affected:** When ExtremeCloud IQ identifies an interference source, the channel in which it occurs displays here.
- **Center Frequency:** The center frequency is the midpoint between upper and lower frequency band cutoff.
- **Occupied Bandwidth:** This column displays the bandwidth of the affected range of frequencies.

The last three columns contain redundant information and provide the same information from different perspectives so that you can gain a more a complete understanding of the affected frequencies and channels.

Neighboring APs

A table displays a list of neighbor APs.

Restart PSE

(Applies to switches only.) You can restart the PSE function on PoE switches.

1. Select the switch checkbox.
2. Select **Utilities > Restart PSE**.
3. A warning statement displays after you select this option.
4. Select **Yes**.

The switch briefly stops supplying PoE on all PoE-enabled ports, and then re-applies it. All devices receiving PoE from the switch are power cycled.

Wi-Fi Status Summary

The **Wi-Fi Status Summary** provides an overview of the current wireless network state for the selected wireless device.

Interface Summary

The **Interface Summary** provides `wifi0`, `wifi1`, and `wifi2` details for the selected wireless device.

Station

Station provides the following `wifi0`, `wifi1`, and `wifi2` details about the selected wireless device (station):

• Mac Address	• User Profile Identifier
• IP Address	• Physical Mode
• Channel Number	• LDPC
• Tx Rate	• Tx-STBC
• Rx Rate	• Rx-STBC
• Power (in dBm)	• SM-PS
• Authentication Mode	• Chan-width

- Encryption Mode
- Associated Time
- VLAN
- Authenticated
- Mu-MIMO
- Release
- Station-State

Client Information

Client Information presents an aggregated view of unique historical client connections within the last 30 days.

Get Tech Data

This utility collects technical data about devices to assist in troubleshooting.

1. Select one or more devices.
2. Select **Get Tech Data**.
3. Confirm the number of devices you selected.

You can save the data file to a local directory in the **.tar.gz** file format. To view the data in a text editor, you must first expand it with a file decompression program. A read me file identifies the devices from which information was obtained.

Locate Device

Use the Locate Device utility to alter the status LED on APs and Switch Engine devices so that you or an assistant at a remote site can locate the physical device more easily. You can also turn the LED off, which can be useful when an AP is mounted near a projection screen or is in a location where the light can be distracting.

1. Go to **Manage > Device**, select the check box for a single device, select **Utilities > Tools > Locate Device**.
2. Set the LED timeout, between 10-300 seconds.



Note

The default timeout is 300 seconds.

3. Select **Submit**.
4. To return the LED to normal operation, select **Return to normal LED operations**.

Neighbor Information

This utility lets you see information about the backhaul link between a device and its neighbors.

1. Select a device from the list.
2. Select **Get Layer 2 Neighbor**.

The following information displays:

- **Neighbor Information:** The host name of the neighbor device.
- **MAC Address:** The MAC address of the neighbor to which there is an Ethernet or wireless backhaul link. Some neighbors might appear twice in the table, once to report information about an Ethernet link and again to report information about a wireless link.

- **Connection Time:** The total time that the backhaul link has been up.
- **Link Cost:** The routing cost. The lower the cost, the more preferred the link is for routing.
- **RSSI:** The RF signal strength of the wireless link between the two neighboring devices. The RSSI range is 0 ~ 90.
- **Link Type:** Ethernet or wireless.

Packet Capture (for IQ Engine APs)

ExtremeCloud IQ supports basic Packet Capture capabilities on all APs hosting IQ Engine OS. Additionally, AP5010/AP3000/AP3000X models hosting IQ Engine 10.6.4 or higher, AP5020 models hosting IQ Engine 10.7.3 or higher, and AP4020 models hosting IQ Engine 10.8.1 or higher support Enhanced Packet Capture capabilities.

1. Go to **Manage > Devices**.
2. Select the check box for an AP model.
3. Select **Utilities > Tools > Packet Capture** to add a capture session for the selected AP.

The **New Packet Capture** window opens displaying the packet capture configuration settings available, which depend on the device selected.

Related Links

[Packet Capture](#) on page 542

[Add and Start a Packet Capture Session](#) on page 546

VLAN Probe Utility

The VLAN probe function utilizes DHCP client on the device to check for and display IP connectivity on a specified VLAN. Use this task to locate a VLAN in a complex network with multiple VLANs.

1. Go to **Manage > Devices** select the associated device.
2. Select **Utilities > Tools > VLAN Probe**.
3. Configure the following settings:

VLAN Range

Indicates the range of VLAN IDs to probe. Enter the start and end values. You can enter up to five ranges, separated by commas, up to a total range of 12. Range numbers cannot overlap. For example, 1,2-7,8,9-12.

Probe Retries

Indicates the number of probe retries. Valid values are 1-10.

Timeout

(Optional) Indicates how long to wait for a reply from each probe. Valid values are 5 to 60 seconds.

4. Select **Start** to start a probe.
5. Select **Stop** to stop a probe before it is complete.
6. Select **Clear** to clear entries for a probe.

When the VLAN probe is complete, a table shows the host name, MAC address, available VLANs, unavailable VLANs, and their status.

Switch VLAN Probe Utility

The VLAN probe function utilizes DHCP client on the switch to check for and display IP connectivity on a specified VLAN.



Note

The VLAN probe is skipped when the selected VLAN has a static IP address or is DHCP enabled.

Use this task to locate a VLAN in a complex network with multiple VLANs. You can also trigger VLAN probe for a Switch Engine device through the topology map.

To verify the VLAN probe results for a selected device:

1. Go to **Manage > Devices** select the associated device.
2. Select **Utilities > Tools > Switch VLAN Probe**.
3. Configure the following settings:

VLAN Range

Indicates the range of VLAN IDs to probe. Enter the start and end values. You can enter up to five ranges, separated by commas, up to a total range of 12. Range numbers cannot overlap. For example, 1,2-7,8,9-12.

Probe Retries

Indicates the number of probe retries. Valid values are 1-10.

Timeout

(Optional) Indicates how long to wait for a reply from each probe. Valid values are 5 to 60 seconds.

4. Select **Start** to start a probe.
5. Select **Stop** to stop a probe before it is complete.
6. Select **Clear** to clear entries for a probe.

When the VLAN probe is complete, a table shows the host name, MAC address, available VLANs, unavailable VLANs, and their status.

Related Links

[Device Summary and Actions Menu](#) on page 385

[VLAN Probe from Real Time Maps](#) on page 388

SSH Availability

Before you begin this task, complete procedure [Enable SSH Availability](#) on page 88.

You can use the SSH Availability utility to temporarily enable SSH availability on a device.

1. Select a device.
2. Select **Run**.
3. Select the length of time to make the device available for SSH access.

4. Select **Enable SSH**.

Make a note of the IP address and port number to use when formatting an SSH session with the device. You, or another administrator with remote access to the device can now make an SSH connection and log in to it with root or read-only administrator credentials.

Download Tech Support File

To help with support related issues, you can download a technical support file, gathered from your system.

This action is only supported by one device at a time.

To download the technical support file:

1. Go to **Manage Device**, select a single device, **Utilities > Tools > Get Tech Support File**.
2. Select **Yes** when asked if you want to proceed.
3. Select **Download Tech Support**.

Actions Menu Overview

From the **Manage > Devices > Actions** menu, you can perform a number of actions on a device. The available actions depend on the device type selected. Select one or more device check boxes, then select **Actions**.



Note

Not all actions are available for all device types. Most device options are unavailable for an unmanaged device, either alone or together with managed devices. To change the management status of your device, select **Change Management Status**.

- **Add to Cloud Config Group:** Add the selected devices to an existing **Cloud Config Group** (CCG). In the **Add to Cloud Config Group** panel, select a CCG to assign to the selected devices, and then select **Continue**. If you need to first create a new CCG, see [Add a Cloud Config Group](#) on page 217.
- **Advanced:** This option offers the following actions:
 - **CLI Access:** (Real devices only) Use this feature to enter CLI commands for the selected device or devices without establishing a console cable connected to the device. Enter the command in the **CLI Command** field, and then select **Apply**. The results of the command are displayed below the command entry field.
 - **Bootstrap Configuration:** Use this simple configuration to re-establish a connection between a device and ExtremeCloud IQ. See [Bootstrap Configuration](#) on page 452 for more information.
 - **Update Netdump Settings:** Configure a device to automatically save a core netdump file to a TFTP server on the network when it next boots up after becoming unresponsive. See [Update Netdump Settings](#) on page 453 for more information.
- **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 preset to **FCC** and the country code is preset to **United States**. Select **Save** to reboot the selected devices.

- **Assign Deployment Mode:** Assign the Pre-provisioned or Production deployment mode.
 - **Pre-provisioned:** Indicates that the device is configured for production, but not active.
 - **Production:** Indicates that the device is actively managed in production.
- **Assign Location:** Using the Network Maps feature, assign a location for the selected device.



Note

For devices managed by ExtremeCloud IQ Site Engine the location is read-only. You can assign the location in ExtremeCloud IQ Site Engine.

- **Assign Network Policy:** Assign an existing network policy to the device or devices.
- **Change CoPilot License Status:** This option appears only if the ExtremeCloud IQ CoPilot feature is enabled and you select a ExtremeCloud IQ CoPilot-eligible device. Select **Activate CoPilot License** or **Revoke CoPilot License**.
- **Change Device Mode:** Change the device mode. from AP/device to Router.
- **Change Management Status:** Indicates the management status of the selected devices. Select **Manage Devices** or **Unmanage Devices**.

You can select the **Unmanage** or **Manage** action for a single device or a group of devices. If the device is a stack, it applies to all stack units that are part of the selected stack.



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**.

- **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.
- **Clone Device:** Apply the existing device-level configuration from one device to a new device of the same model. For more information, see [Clone a Device](#) on page 453.
- **Enable FIPS-Mode/Disable FIPS-Mode:** For StateRamp-enabled RDCs only, toggle FIPS-Mode for supported APs. Enabling FIPS-Mode resets the AP to the default settings.
- **Enhanced Discovery:** Enhanced Discovery can be used to enhance support of onboarding for Local Management (within ExtremeCloud IQ) providing an option to define the list of primary and secondary controllers running ExtremeCloud IQ Controller. 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. For more information, see [Enhanced Discovery](#) on page 33.

- **Reboot:** Reboot devices after uploading a configuration. Rebooting momentarily disconnects any associated clients from the SSID, which could be disruptive.
- **Recalculate GPS Location:** Recalculates the GPS coordinates for all selected devices.

**Note**

This feature is available only in AFC Wireless view.

- **Reset IDM Client Certificate:** Select to reset the IDM client certificate for this device.
- **Revert Device to Template Defaults:** Select to return the device settings to the network policy template. This removes any device-level configuration settings.
- **Send AP Range Info:** Sends the selected device parameters, such as geolocation, antenna height, and coverage range, to the AFC system.

**Note**

This feature is available only in AFC Wireless view.

- **Show AFC Spectrum:** Select to display the AFC spectrum results for the selected AP.

**Note**

If the AFC status of the selected AP is **Pending**, the spectrum results do not display.

- **Start Thread Commissioner:** Select to designate an AP as a Thread Commissioner. This option is available for connected APs, configured with an IoT Thread profile, and are not already designated as a Thread Commissioner.

**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.

The **Start Thread Commissioner** pop-up window opens. Optionally, select **Override Timeout** and enter a value in the range of 1-2000000 seconds. Select **Start**.

**Note**

The **Start Thread Commissioner** action appears only when the AP is running an HOS version earlier than 10.8.6.0. This option is not available for APs running HOS 10.8.6.0 or later.

- **Stop Thread Commissioner:** Select to stop the Thread Commissioner running on an AP. This menu item is available only for an AP that is currently designated as Thread Commissioner.

**Note**

The **Stop Thread Commissioner** action appears only when the AP is running an HOS version earlier than 10.8.6.0. This option is not available for APs running HOS 10.8.6.0 or later.

- **Update AFC Spectrum:** Select to refresh AFC data to ensure ExtremeCloud IQ is displaying the latest information.

Bootstrap Configuration

From the **Actions** tab on the **Device Details** page, use this simple configuration to re-establish a connection between a device and ExtremeCloud IQ. The information you enter here allows you to log into a device when running the bootstrap configuration. When there is a bootstrap configuration on an AP, the AP fails over to it when you reset the configuration, or if the current and backup config files fail to load. When there is no bootstrap config file on an AP, it fails over to default configuration settings.

1. Select **Actions > Advanced > Bootstrap Configuration**.
2. Enter the credentials for an admin to access the device after it has loaded a bootstrap configuration.
 - a. Enter the root **Admin Name** (this is required while running the bootstrap configuration for this device).
 - b. Enter the **Password** for this device when running the bootstrap configuration.
 - c. For **Configure the Bootstrap CAPWAP settings**:

ExtremeCloud IQ devices use the CAPWAP protocol to communicate with each other (CAPWAP clients) and or (CAPWAP server). The client sends Discovery Request messages until it receives a Discovery Response from the server. When this happens, the CAPWAP server and client establish a secure DTLS session and mutually authenticate each other using a preshared key derived from a passphrase.

- **Primary CAPWAP Server:** Enter the name of a primary CAPWAP server for this device (found in the Device Credentials window).
 - **Backup CAPWAP Server:** Enter the name of a backup CAPWAP server for this device (found in the Device Credentials window).
 - **VIQ Name:** Enter the name of the VIQ account which manages this device.
 - **CAPWAP UDP Port:** Enter the UDP port for CAPWAP communications. To avoid reconfiguring the firewall, you can configure devices behind the firewall to communicate with ExtremeCloud IQ using HTTP on TCP port 80 instead of CAPWAP UDP port 12222. The default is 12222. The port range is 1024 - 65535.
3. Select **Update**.

Update Netdump Settings

You can configure a device to automatically save a core netdump file to a TFTP server on the network when it next boots up after becoming unresponsive. You can then provide this file to Support to help Extreme Networks diagnose the issue.

1. Select the devices for this netdump.
2. Select **Actions > Advanced > Update Netdump Settings**.
3. Select **Enable Netdump**.
4. Complete the following fields:
 - **TFTP server for saving Netdump files:** Enter the TFTP server IP address to which you want the devices to send the core dump file.
 - **Netdump filename to save:** Enter a Netdump filename.
 - **VLAN for reaching the TFTP server:** Enter the VLAN of the interface from which the device sends the Netdump file to the TFTP server.
 - **Native VLAN of the local Extreme Networks device:** Enter the native VLAN of the device.
 - **DHCP:** Select to have the device bootloader use DHCP to obtain an address on startup.
 - **Static:** Select to have the device bootloader use a static IP address. Enter the required static IP settings that the bootloader must use to connect to the network.
5. Select **Save**.



Note

This feature becomes active after you perform a full configuration update for the selected devices.

Clone a Device

Use this task to apply the existing device-level configuration from one switch to a new switch with the same model. For example, if you need to replace one switch with another, this task describes how to do so and then apply the existing device-level configurations used by the previous switch.



Note

Licensing is not cloned.

1. Go to **Manage > Devices** and select the check box for the device in the **Device List**.
2. Select **Actions > Clone Device**.
3. (Optional) Select the **Perform full configuration clone** check box to clone additional configurations previously performed through supplemental CLI, SSH proxy, or local console saved on the original device with the same software version (minimum of 32.3.1.11).
4. Under **Replacement Device**, if the device is not yet **Onboarded**, select **Quick Onboard**, enter the device serial number and proceed to **Step 6**.
If the device has already been **Onboarded**, proceed to **Step 5**.

5. Under **Replacement Serial Number**, select the appropriate device serial number.

**Note**

To onboard a Universal Hardware Switch, for the **Device OS**, choose **Switch Engine** or **Fabric Engine**.

6. Select **Clone**.
7. Select **Yes**.
8. Select **Perform Update** to push the configuration to all selected cloned devices.

Enhanced Discovery Action

The following is an optional way to specify the primary and backup controllers for Enhanced Discovery.

**Note**

Enhanced Discovery is supported on AP3000 and ExtremeCloud IQ Controller.

1. Select an AP3000 from the **Managed Devices** list.
2. Select **Actions > Enhanced Discovery**.
3. Enter the Primary Controller IP address or FQDN, and the Backup Controller IP address or FQDN.
4. Select **OK**.

Related Links

[Enhanced Discovery](#) on page 33

Device Details Panel

Go to **Manage > Devices**, and then select the host name for a device, from the list.

The sidebar displays the following information:

- Device location, map and floor plan
- Image and model number of the device
- The **Policy** assigned to the device, or a link to **Assign Policy**
- Optional uploaded images or video of the device installation in the **Media Gallery**. See [Upload and Manage Media Gallery Content](#) on page 494.
- Connection state
- Active alarms
- Number of connected clients
- Real-time CPU and memory usage data

Below this information are two tabs:

- **Monitor**: Select to view and monitor the status of the device. See [Device Details Monitor Functions](#) on page 455.

- **Configure:** Select to perform device-level configuration tasks and update your devices directly. See [Device Details Configuration Tasks](#) on page 465.

**Note**

The **Configure** tab is not available for locally managed switches.

**Note**

The menu options that appear for the **Monitor** and **Configure** tabs depend on the selected device.

Related Links

[Device Details Monitor Functions](#) on page 455

Device Details Monitor Functions

You can further monitor the status of devices as follows:

Table 107: Monitor menu options

Menu option/page	Device type	More information
Overview	AP	Provides a high-level view of the device (AP or switch) status. See Overview on page 456.
System Information	AP	Provides details about the system-level configuration for an AP device. See System Information on page 457.
Wireless Interfaces	AP	Provides details about the wireless port configuration for an AP device. See Wireless Interfaces on page 458.
Wired Interfaces	AP	Provides details about wired port configuration for an AP device. See Wired Interfaces on page 459.
Interfaces	Switch	Provides details about port configuration for a switch device. See Interfaces on page 459.
Routing	Switch	Provides detailed routing information for a switch device. See Routing on page 460.
Clients	AP or Switch	Provides details about the Clients on page 461 connected to a device (AP or switch).
Diagnostics	Switch	Provides detailed timeline Diagnostics on page 462 information, such as port transmit and receive traffic, for switch devices.

Table 107: Monitor menu options (continued)

Menu option/page	Device type	More information
Events	AP or Switch	Displays changes to the network, including configuration changes, for which Events on page 463 notifications exist.
Alarms	AP or Switch	Indicates network issues for which Alarms on page 464 exist and require administrator attention.

Overview

Overview for AP Devices

Select the host name of an AP from the **Devices** table, and then go to **Monitor > Monitoring > Overview**. The **Device Details** panel displays the following information for that device:

- At the top of the page, the **Connection Chain** diagram shows how the device connects to the internet and to ExtremeCloud IQ. Hover over the diagram to see the node type, IP address, host name, and VLAN assignments for the AP.
- The timeline below the connection diagram shows connected clients, CPU usage, and memory usage over time. You can customize the time period using the **Time Range** controls above the timeline, or by dragging inside the timeline. The chart lines are interactive—hover over a line to see more data.

To print or download timeline data in a variety of file formats, select .

- The following widgets appear below the timeline graph:
 - **DEVICE HEALTH**
 - **MAXIMUM CLIENT CAPABILITIES**
 - **CONNECTED CLIENTS**
 - **ACTIVE ALARMS**
 - **NETWORK USAGE**
 - **CHANNEL CHANGE EVENTS**
 - **TOP 5 USERS BY USAGE**
 - **TOP 5 APPLICATIONS BY USAGE**



Note

The selected time period applies to the widgets as well as the timeline graph.

Overview for Switch Devices

Select the host name of a switch from the **Devices** table, and then go to **Monitor > Monitoring > Overview**. The **Device Details** panel displays the following information for that device:

- The timeline diagram shows counters for RX and TX, and the average CPU and memory usage over time. You can customize the time period using the **Time Range**

controls above the timeline, or by dragging inside the timeline. The chart lines are interactive—hover over a line to see more data.

To print or download timeline data in a variety of file formats, select .

- An interactive port usage diagram and corresponding table appear below the timeline graph. The following widgets and information appear above the diagram:



Figure 7: Wired Overview widgets and information for switches

- **CPU Usage:** Hover over the half-pie chart to display usage information.
- **Memory:** Hover over the half-pie chart to display memory usage.
- **MAC Table Utilization:** Hover over the half-pie chart to display MAC Table usage.
- **Last Seen:** Hover over  to display the date and time at which the device was last online.
- **Temperature:** Displays the temperature at which the device is running. You can also hover over the  to display the temperature.
- **Power Supply Status:** Hover over  to display detailed information about power supply and PoE status.
- **Fan Status:** Hover over  to display the status of the fans for each tray.
- **IP Address:** Displays the IP address of the device.
- **MAC Address:** Displays the MAC address of the device.
- **Software Version:** Displays the version of the device software.
- **Model:** Displays the model of the device.
- **Serial #:** Displays the serial number of the device.
- **Make:** Displays the make of the device.
- **IQAgent Version:** Displays the IQAgent software version.

Related Links

[Device Details Monitor Functions](#) on page 455

System Information

Select the host name of an AP from the **Devices** table, and then go to **Monitor > Monitoring > System Information**. The **Device Details** panel displays a table that includes the following information for the AP:

- Host Name
- Network Policy
- SSID
- Device Model
- Function
- Device Template
- Configuration Type
- Serial Number
- Mgt0 IPv4 Address
- Mgt0 IPv6 Address
- IPv4 Subnet Mask
- IPv6 Subnet Mask
- IPv4 Default Gateway
- IPv6 Default Gateway
- Mgt0 MAC Address

- IQ Engine
- Device Status
- DNS
- NTP

The **Device Details** panel displays a **GEO Location** table that includes the following information for the AP:

- GPS Last Reported
- Latitude
- Longitude
- Elevation (m)



Note

GEO Location is supported on AP5050 devices only.

Related Links

[Device Details Monitor Functions](#) on page 455

Wireless Interfaces

Select the host name of an AP from the **Devices** table, and then go to **Monitor > Monitoring > Wireless Interfaces**. The **Device Details** panel displays the following information:

- An interactive timeline graph shows channel utilization for WiFi0, WiFi1, and WiFi2, and the number of connected clients.

To customize the time period for the graph, use the **Time Range** controls above the timeline, or drag inside the timeline. The chart lines are interactive—hover over a line to see more data. To show or hide a line on the graph, select the corresponding label at the top of the graph.

To print or download timeline data in a variety of file formats, select .

- The **WIFI HEALTH** widget provides an overview of the Wi-Fi performance for the selected radio channel: 2.4 GHz, 5 GHz, 6 GHz, or for all channels combined.
- Widgets show the number of **Total Clients**, **Clients with Poor Health**, and **Surrounding BSSIDs**, as well as the percentage of **CPU Usage** and **Memory Usage**.
- Summary information tables for **WiFi0**, **WiFi1**, and **WiFi2**.



Note

For AP5050 devices, WiFi2 displays the **AFC Status** of the device:

- Hover over the  icon to view Status, Received, Expire, and Reason details.
- Select the  icon to view the device AFC channel plan. Antenna gain and chain gain are taken into account to only show channels that the AP can use.

- **Channel Utilization** widgets.
- The **Surrounding Access Points** table provides details about surrounding APs.

Related Links

[Device Details Monitor Functions](#) on page 455

Wired Interfaces

Select the host name of an AP from the **Devices** table, and then go to **Monitor** > **Monitoring** > **Wired Interfaces**. The **Device Details** panel displays the following information:

- An interactive timeline graph shows CPU usage, memory usage, and the number of connected clients over a period of time.

To customize the time period for graphs, use the **Time Range** controls above the timeline, or by drag inside the timeline. The chart lines are interactive—hover over a line to see more data. To show or hide a line on the graph, select the corresponding label at the top of the graph.

To print or download timeline data in a variety of file formats, select .

- An interactive timeline graph shows the following details for each interface:
 - The number of bytes transmitted and received
 - The number of transmission and receive errors
 - The number of transmission and receive discards

Select the interface from the list.

- Widgets show the number of **Total Clients** and the **Number of Ports in Use**.
- The **Interface Details** table presents the information for each interface in table format.

Related Links

[Device Details Monitor Functions](#) on page 455

Interfaces

Device Details for Interfaces

Select the host name of a switch from the **Devices** table, and then go to **Monitor** > **Monitoring** > **Interfaces**.

**Note**

The selected switch must be assigned a network policy.

- An interactive port usage diagram and corresponding table appear below the timeline graph. The following widgets and information appear above the diagram:

 65°C
 
 IP Address: 10##### 54
 MAC Address: 00#####300
 Software Version: 32.7.1.9
 Model: Switch Engine 5520-24W
 Serial #: 2#####9
 Make: Switch Engine
 IQAgent Version: 0.7.21

Figure 8: Widgets and information for switches

- **CPU Usage:** Hover over the half-pie chart to display usage information.
- **Memory:** Hover over the half-pie chart to display memory usage.

- **MAC Table Utilization:** Hover over the half-pie chart to display MAC Table usage.
- **Last Seen:** Hover over  to display the date and time at which the device was last online.
- **Temperature:** Displays the temperature at which the device is running. You can also hover over the  to display the temperature.
- **Power Supply Status:** Hover over  to display detailed information about power supply and PoE status.
- **Fan Status:** Hover over  to display the status of the fans for each tray.
- **IP Address:** Displays the IP address of the device.
- **MAC Address:** Displays the MAC address of the device.
- **Software Version:** Displays the version of the device software.
- **Model:** Displays the model of the device.
- **Serial #:** Displays the serial number of the device.
- **Make:** Displays the make of the device.
- **IQAgent Version:** Displays the IQAgent software version.
- The graphic below shows all of the ports on the device. Select a port to display more information.

Provisioned ports that use the VLAN, both tagged and untagged, light up to indicate VLAN usage. Select a port to display the port name, port status, VLAN untagged/tagged status, and port actions.

- Select the **VLAN** tab to display a table containing the following information: VLAN Name, VLAN ID, Active Ports (Enabled port with VLAN assigned), STP Instance, IGMP Snooping, and DHCP Snooping information columns. Select a VLAN in the VLAN table to highlight currently assigned ports.
- Select the **IPv4** tab to display a table containing the following information: VLAN Name, VLAN ID, IPv4 Forwarding, Routing Instance, and IP Address/Subnet information columns. You can select the VLAN when the row is highlighted.

Related Links

[Device Details Monitor Functions](#) on page 455

Routing

Select the host name of a switch from the **Devices** table, and then go to **Monitor > Monitoring > Routing**. The **Device Details** panel displays the following information:



Note

The selected switch must be assigned a network policy.

- An interactive timeline graph shows the number of each route type:
 - Direct Routes
 - Static Routes
 - OSPF Routes
 - Total Routes

To customize the time period for the graph, use the **Time Range** controls above the timeline, or drag inside the timeline. The chart lines are interactive—hover over a line to see more data. To show or hide a line on the graph, select the corresponding label at the top of the graph.

The X axis represents the poll time interval.

The Y axis represents the total number of routes and resizes, based on the chosen routes.



Note

Select the corresponding label to show or hide lines on the graph.

- Within the **IPv4 Routing Table** section, the destination subnetwork, next hop, VLAN Name, VLAN ID, Route Origin, Status, Metric, Route Age, Route Type Priority, and Routing Instance information are all listed. You can filter by the **Route Origin** and **Status**. Select ▼, and then select a filtering option from the menu.



Note

- Up to 100 IPv4 routes are visible within the table. For additional visibility, use an SSH proxy.
- Switch Engine software version 32.6.2.68 or newer is required.

Related Links

[Device Details Monitor Functions](#) on page 455

Clients

Select the host name of an AP or a switch from the **Devices** table, and then go to **Monitor > Monitoring > Clients**. The **Device Details** panel displays the following information:

- 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, use the **Time Range** controls above the timeline, or drag inside the timeline. The chart lines are interactive—hover over a line to see more data.

- The **Total Clients within selected time range** widgets displays the number of clients.
- The **Clients with poor health** widget displays the number of clients.
- A table lists the following details about the clients that are connected during the specified time range:
 - Type of client (wired, wireless, Thread, undetermined)
 - OS type
 - Connection status
 - Health Status
 - Host name

- Alias
- IPv4
- IPv6
- Client MAC address
- Connected port name
- User name
- VLAN to which client is connected
- Client IP address
- SSID
- RSSI
- SNR

You can filter by the **Current Connection Status**, **Connection Type**, and by **OS Type**. Select ▼, and then select the filtering options. You can also use the **Search** field to customize your view.

Related Links

[Set the Time Frame for Captured Data Displays and Reports](#) on page 551

Diagnostics

Select the host name of a switch from the **Devices** table, and then go to **Monitor > Monitoring > Diagnostics**. The **Device Details** panel displays the following information:

- An interactive port usage diagram and corresponding table appear above the **Port Statistics** timeline graph. The following information appears above the diagram:
 - **IP Address:** Displays the IP address of the device.
 - **MAC Address:** Displays the MAC address of the device.
 - **Software Version:** Displays the version of the device software.
 - **Model:** Displays the model of the device.
 - **Serial #:** Displays the serial number of the device.
 - **Make:** Displays the make of the device.
 - **IQAgent Version:** Displays the IQAgent software version.

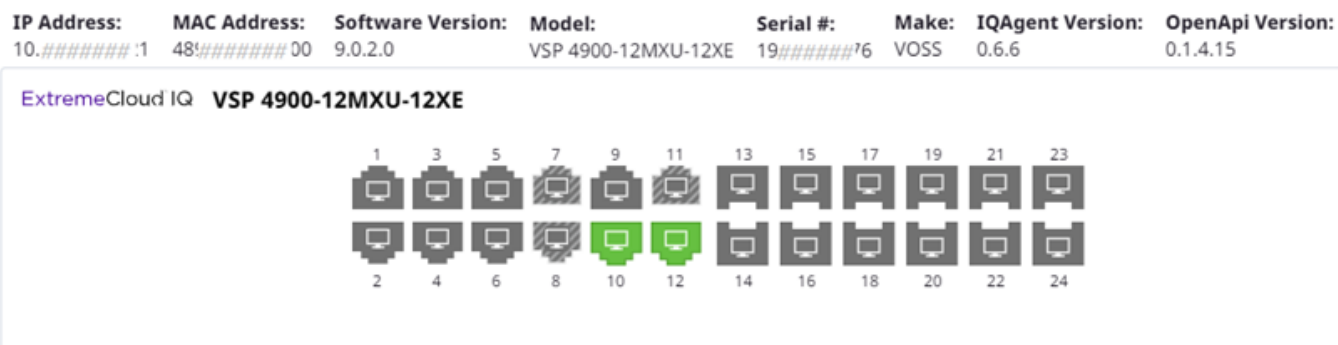


Figure 9: Port diagnostics information for switches

- **Port Statistics:** An interactive timeline graph displays diagnostics statistical data captured for ports, for the specified time frame. By default, the data capture time frame is 24 hours.

To customize the time period for the graph, use the **Time Range** controls above the timeline, or drag inside the timeline. The chart lines are interactive—hover over a line to see more data. To show or hide a line on the graph, select the corresponding label at the top of the graph.

Depending on the type of switching device selected, the graph displays some or all of the following details over a colored timeline:

- Transmit and receive traffic and port utilization
- Transmit and receive errors
- Transmit and receive data usage types (unicast, multicast, broadcast)
- **Port Details:** A table displays detailed information for each port. Select ports to use the **ACTIONS** menu and select: **Bounce Port** or **Bounce PoE**. Select **Start Test** to run a cable test for a port.
- **QoS Statistics:** Interactive timeline graphs shows the number of **QUEUE PKTS** and **QUEUE CONGESTION**.

To customize the time period for the graphs, use the **Time Range** controls, or drag inside the timeline. The chart lines are interactive—hover over a line to see more data. To show or hide a line on the graph, select the corresponding label at the top of the graph.

Related Links

[Set the Time Frame for Captured Data Displays and Reports](#) on page 551

[Device Details Monitor Functions](#) on page 455

Events

Select the host name of an AP or a switch from the **Devices** table, and then go to **Monitor > Monitoring > Events**. The **Device Details** panel displays the following information:

ExtremeCloud IQ records events that occur in the network, and displays the events for the selected device in this window. The table data updates hourly. You can customize the time period using the **Time Range** controls:

- To show events for the current day, select **Day** and then select the number of hours: 1, 2, 4, 8, or 24.
- To show events for the week, select **Week** and then select the number of days: 1, 2, or 7.

There is an **Events** tab and a **Configuration Events** tab above the table. Select **Configuration Events** to show only changes to the device configuration, either from inside a network policy, or at the device level.

Use the predictive search field to search for an event by description. Use the column picker to customize the categories displayed in the table. By default, **Timestamp**, **Severity**, **Category**, and **Description** columns are displayed. Optional columns include **Host Name**, **Device MAC**, and **Client MAC**.

Select a **Severity** level from the list to filter the table. To customize the display, select the column headings. For example, if you want to organize the content by host name, select the **Host Name** heading.

Each entry includes the following elements:

- **Timestamp**: Indicates the time (in the month/day and time-of-day format) that the alarm or event occurred.
- **Severity**: Indicates the severity of the an alarm or event: Major, Info, or Clear.
- **Category**: Indicates the issue category that triggered the alarm or event. Available categories are CAPWAP, channel power, state change, client connection down, client connection change, static route ping protection, and DHCP rogue MAC detection.
- **Description**: Describes the context of an alarm or an event.
- **Host Name**: The host name of the configured device on which the event occurred.
- **Device MAC**: The MAC address of the device that reported the alarm or event.
- **Client MAC**: The MAC address of the client that reported the alarm or event.

To copy the information pertaining to an individual log, hover over the text in the **Description** column to display the complete description in a text box. Select the text, right-click, and then select **Copy**.

You can download table data as a CSV file.

Related Links

[Device Details Monitor Functions](#) on page 455

Alarms

Select the host name of an AP or a switch from the **Devices** table, and then go to **Monitor > Monitoring > Alarms**. The **Device Details** panel displays the following information:

- The **Alarm Details** widget displays the number of alarms for each severity level.
- There are two views available: **Alarm Details** (default view) and **Timeline**.

- The **Alarm Details** table lists all active alarms. Columns include:
 - **Status**: The status of the alarm.
 - **Severity**: Major, minor, or informational.
 - **Category**: The type of alarm, for example Agent alarm, Device disconnected, or Change OS.
 - **Description**: A description of the alarm.
 - **Time Raised**: The date and time when the alarm was reported.
 - **Action**: Actions that can be taken with this alarm.

The following columns are optional:

- **Time Cleared**: The time that the alarm was cleared.
- **Cleared by**: The name of the person who cleared the alarm.
- The Alarms **Timeline** view displays an interactive timeline graph, with color-coded lines showing **ALARMS RAISED**, **ACTIVE ALARMS**, and **CLEARED ALARMS**. By default, the graph displays data captured for a 24-hour time frame. You can customize the time period using the **Time Range** controls:
 - To show events for the current day, select **Day** and then select the number of hours: 1, 2, 4, 8, or 24.
 - To show events for the week, select **Week** and then select the number of days: 1, 2, or 7.

Select **Active** or **Cleared** to display the corresponding table.

For either view, use the **UPDATE** button to apply your changes to the devices. Use the refresh icon to refresh the data. Use the column picker to select which table columns to display. Your column selections persist, if you go to another window and return, and from one session to the next. The table features horizontal scrolling when there are too many columns to fit the display window.

To remove one or more alarms, or remove redundant entries, select the check box next to the alarm, and then select **Clear Selected Alarms**. Cleared alarms then become events, which appear in the **Events** log.

To clear multiple alarms at the same time, either select the check box in the table header to select all alarms, select the check boxes individually, or shift-select to select check boxes for multiple alarms. Then select **Clear Selected Alarms**.

Related Links

[Set the Time Frame for Captured Data Displays and Reports](#) on page 551
[Device Details Monitor Functions](#) on page 455

Device Details Configuration Tasks

Go to **Manage > Devices > <device name> > Configure**.

With ExtremeCloud IQ, you can perform device-level configuration tasks and update your devices at the device level. Settings made at this level apply only to the individual device and override the template settings configured for the network policy. After device-level settings are removed, the device automatically reverts back to the original

network policy and device template configuration. The features that display for this tab vary depending on the type of device you selected.

To configure a switch, see [Configure Switch Devices](#) on page 481. To configure an AP device, see [Configure AP Devices](#) on page 466.

Related Links

[Configure Switch Devices](#) on page 481

[Configure AP Devices](#) on page 466

Configure AP Devices

After you select an **AP** from the Device List, you can create or modify the following:

- [AP Device Configuration](#): Edit device details such as the host name, the description, the device function, IP addresses, and VLAN assignments.
- [AP 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.
- [AP Device Credentials](#): Assign or change network administrator credentials and administrator assignments, and configure CAPWAP and Shared Key settings.
- [Netdump](#): Enable an unresponsive AP to automatically save a core dump file to a TFTP server on the network the next time it boots.
- **Location Information**: Define detailed device location information, see [Location Information Configuration Settings](#) on page 476.
- [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.
- [SSH](#): Temporarily enable SSH to troubleshoot the device.

After you make changes to the configuration, you must [push the configuration changes to the device](#).

Related Links

[Device Details Configuration Tasks](#) on page 465

AP 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 AP.

1. Go to **Manage > Devices** and select the host name of the AP in the **Devices** list.
2. From the **Device Details** left pane, select **Configure > Device Configuration**.

3. Configure **Device Details** settings:

Table 108: 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.
IQ Engine	Lists the IQ Engine firmware version currently installed on the AP.
SNMP Location	The SNMP location name, for example headquarters, building 1.

4. 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.

5. Configure **Management Interface** settings:

- a. Select **Static Address** to enter a static address for this interface, and then configure the following settings:

Table 109: 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)** to have an address automatically assigned by DHCP, and then configure the following settings:

Table 110: Dynamic Address Configuration (DHCP) Settings

Field	Description
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: • 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. • Automatically Generate Interface IP Settings: ◦ 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. ◦ Subnet Mask: Enter the netmask for the subnet to which the mgt0 interface connects. • Static Fallback IP Settings: ◦ 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. ◦ Subnet Mask: Enter 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.

- 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).
6. (Optional) Configure **Supplemental CLI**.
- For more information, see [Device Details Configure Supplemental CLI](#) on page 489.
7. 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.
8. For **Deployment Mode**, select **Pre-Provisioned** or **Production** to indicate whether the device has been pre-provisioned.
9. (AP5010 only) Enable **POE Profile Override**, select the override option from the dropdown, and hover over the **i** icon to view the corresponding override table.

10. For **Antenna Location Type**, select a location from the drop-down list.

**Note**

Antenna Location Type does not apply to AP5020.

11. Select **Save Device Configuration**.
12. To update the device immediately, select **Update** in the upper-right corner of the page.
For information about pushing the updated configuration to the device, see [Push the Device-Level Configuration to the Device](#) on page 494.

Related Links

[Configure Device Templates](#) on page 171

AP 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 **Manage > Devices** and select the host name of the AP in the **Devices** list.
2. From the **Device Details** left pane, select **Configure > Interface Settings**.
3. For **Wireless Interfaces**, select either the **WiFi0**, **WiFi1**, **WiFi2**, **BLE**, or **IoT0** tab.

**Note**

The **IoT0** tab is supported on AP5010/AP5020 models.

4. To configure **WiFi0**, **WiFi1**, **WiFi2**, or **IoT0**, see [Configure WiFi Settings](#) on page 470.
5. To configure **BLE**, see [Configure BLE Service Settings](#) on page 471.
For more information about the BLE service, see [Configure the BLE Service](#) on page 177.
6. For **Wired Interfaces**, see [Configure Wired Interfaces Settings](#) on page 472.
7. Select **Save Interface Settings**.

Related Links

[Configure WiFi Settings](#) on page 470

[Configure BLE Service Settings](#) on page 471

[Configure Wired Interfaces Settings](#) on page 472

[Configure the BLE Service](#) on page 177

[Configure Wireless Interfaces for an AP Template](#) on page 202

[Configure Wired Interfaces for an AP Template](#) on page 203

Configure WiFi Settings

Table 111: 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.
Radio Usage	Select the usage type: • 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. 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. • Client Access: Select for normal client operation. • Backhaul Mesh Link: Select for wireless portal and mesh backhaul operation. • 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. For more information, see Configure an SDR Profile on page 242.
Channel	Select a channel. If you select Auto , ExtremeCloud IQ 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 112: 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.

Table 112: Enable Presence Analytics Settings (continued)

Field	Description
Aggregate Time	The interval (in seconds) for the period of time that aggregation occurs for the presence profile.
Aging Time	The aging time (in seconds) for a given presence profile.

Table 113: 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.
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

[AP Interface Settings](#) on page 469

Configure BLE Service Settings

Table 114: BLE Service Settings

Field	Description
Enable BLE Service	Select to enable the BLE service for the device. Deselect to disable BLE Monitoring for the device. Note: BLE Services must be enabled in the Network Policy before it can be enabled or disabled on the device. For more information, see Configure the BLE Service on page 177.
Service Name	The BLE service name. This field is read only.
iBeacon UUID	The iBeacon UUID. This field is read only.
Settings — Major	The iBeacon major value. Value range is 0 to 65535.
Settings — Minor	The iBeacon minor value. Value range is 0 to 65535.
Settings — Power dBm	The iBeacon signal strength. Value range is -128 to 127 dBm.

Table 114: BLE Service Settings (continued)

Field		Description
BLE Scan — iBeacon		Select iBeacon to enable iBeacon Monitoring for the device. Deselect to disable iBeacon Monitoring for the device. Note: iBeacon must be activated in the Network Policy before it can be enabled or disabled on the device. For more information, see Configure the BLE Service on page 177.
	Enable Cloud Reporting	Select to enable Cloud Reporting for the device. Deselect to disable Cloud Reporting for the device. To change how often iBeacon transmits to ExtremeCloud IQ, you must update the Network Policy. For more information, see Configure the BLE Service on page 177. The default value is 60 seconds. Note: Cloud Reporting must be enabled in the Network Policy before it can be enabled or disabled on the device.
	Enable Batch Reporting	Select to enable Batch Reporting for the device. Deselect to disable Batch Reporting for the device. To change how often iBeacon transmits batch file reports (default is 10 seconds) and the destination URL, you must update the Network Policy. For more information, see Configure the BLE Service on page 177. Note: Batch Reporting must be enabled in the Network Policy before it can be enabled or disabled on the device.
Generic		

Related Links

[AP Interface Settings](#) on page 469

Configure Wired Interfaces Settings

Table 115: 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.

Table 115: Wired Interfaces Settings (continued)

Field	Description
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. 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. 2. For each VLAN, select , and then enter the device's associated VLAN ID and I-SID. 3. Select a VLAN from the list, and then select  to remove the VLAN from the Fabric Attach. 4. Select Save.
Transmission Type	Select one of the following options: • 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.
Speed	The speed the Ethernet port uses to communicate with the connected device.
Green Ethernet (AP4020 and AP5020 Only)	Select for AP5020 devices to allow physical layer transmitters to consume less power when they are in a state of idleness or low data activity.
LLDP	Select for devices to advertise 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.
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

[AP Interface Settings](#) on page 469

Configure AP 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. 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 **Manage > Devices**.
2. Select an AP **Host Name** to see a details panel for that AP.
3. Select the **Configure** tab.
4. Under **Configuration**, select **Device Credentials**.
5. 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.
6. 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.
7. 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.
8. Configure a **Shared Key for Authentication Passphrase**.
9. Select **Save Device Credentials**.

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 **Manage > Devices** and select the host name of the AP in the **Devices** list.
2. From the **Device Details** left pane, select **Configure > Configure Netdump**.
3. Select the check box to **Enable Netdump**.

4. Configure the **Update Settings**.

Table 116: 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.

5. Select the **DHCP** check box to have the device bootloader use DHCP to obtain an IP address at startup.
6. Select the **Static** check box to use a static IP and configure the following network settings that the bootloader must use to connect to the network:

Table 117: 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.

7. Select **SAVE NETDUMP CONFIGURATION**.
8. To update the device immediately, select **UPDATE**.
9. Select the type of update.
10. Select **SAVE AS DEFAULTS**.
11. Select **PERFORM UPDATE**.

The device will send a core dump file to the TFTP server the next time it reboots.

Location Information Configuration Settings

Table 118: Location Information Configuration Settings

Field	Definition
LCI Override	Enable to define the following location information: • Latitude (degrees) • Longitude (degrees) • Altitude (meters)
Z-Subelement Enable	Enable to define the following location information: • Expected to Move (check/clear) • Height Above Floor (meters) • Height Above Floor Uncertainty (meters)
Civic Address Override	Enable to override the existing location civic address and enter an RF 4776 Hex String.

Related Links

[Device Details Configuration Tasks](#) on page 465

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. You can configure both DHCP servers and relay agents here.

1. Go to **Manage > Devices** and select the host name of the AP in the **Devices** list.
2. From the **Device Details** left pane, select **Configure > Additional Settings > DHCP Server and Relay**.
3. Select  to .
4. Enter a **Name**.
5. Enter an optional **Description**.
6. Select the **Platform Supported** from the drop-down list.
7. Select the **Interface** from the drop-down list.
8. Select **DHCP server** or **DHCP relay agent**.

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.

9. 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.

10. 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.
11. Select **Enable NAT Support** if this DHCP server uses NAT.
12. 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**.
13. For **IP Binding**
 - a. Select **+** to add a new IP Binding.
 - b. Enter the **IP Address** and **MAC Address**.
 - c. Select **Add**.
14. To configure each of the required parameters that the DHCP server returns to clients along with an IP address, see [Configure DHCP Server Options](#) on page 478.
15. To define custom DHCP options to provide additional network settings to connected clients, see [Configure Custom DHCP Options](#) on page 477.
16. Select **Save**.

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 the add icon.
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. Choose 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**.
6. Select **Save**.

Update the device from the **Manage > Device** page.

Configure DHCP Server Options

Create basic **DHCP Server and Relay settings**.

Use this task to configure each of the required parameters that the DHCP server relays to clients, along with an IP address.

1. Enter the IP address of the **Default Gateway** for the subnet to which the addresses in the IP pool belong.
2. Enter the primary **DNS server** IP address for clients to contact when resolving domain names to IP addresses.
3. Enter the secondary **DNS server** IP address for clients to contact when resolving domain names to IP addresses.
4. Enter the tertiary **DNS server** IP address for clients to contact when resolving domain names to IP addresses.
5. Enter the **POP3 server** IP address for clients to use.
6. Enter the **SMTP server** IP address for clients to use.
7. Enter the primary **WINS server** IP address for clients to use.
8. Enter the secondary **WINS server** IP address for clients to use.
9. For **Lease Time**, enter the length of time for the DHCP lease to last.
10. Enter the **Netmask** that defines the subnet to which the addresses in the IP pool belong.
11. Enter the DNS name resolution **Domain Name** to assign to DHCP clients.
12. Set the path **MTU** aging timeout in seconds for clients to use.
13. Enter the primary **NTP server** IP address for DHCP client clock synchronization.
14. Enter the secondary **NTP server** IP address for DHCP client clock synchronization.
15. Enter the **Log Server** IP address for DHCP clients.

Save the configuration or continue to **Custom** settings.

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 **Manage > Devices** and select the host name of the AP in the **Devices** list.
2. From the **Device Details** left pane, select **Configure**.
3. Under **Additional Settings**, 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**.
9. To update the device immediately, select **Update**.
10. Select the type of update, and then select **Save as Defaults** to save this option as the default action.
11. To update the device immediately, select **Perform Update**.

Configure Bonjour Gateway Settings

Define Bonjour Gateway settings in the network policy.

Use this task to choose the AP you want to act as your Bonjour Gateway Designated Device (BDD) at the device level. If possible, use the newest model AP you have in a low traffic area.

1. Go to **Manage > Devices** and select the host name of the AP in the **Devices** list.
2. From the **Device Details** left pane, select **Configure**.
3. Under **Additional Settings**, select **Bonjour Gateway Settings**.
4. Set the **Priority** for the AP 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 will act 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**.
7. To update the device immediately, select **Update**.
8. Select the type of update, and then select **Save as Defaults** to save this option as the default action.
9. To update the device immediately, select **Perform Update**.

Push a complete configuration to the BDD, followed by a **Delta** update to all other APs.

Troubleshooting

Use this task to enable Client Monitor so devices can detect client issues, and report client connection activities and problems to ExtremeCloud IQ.

1. Go to **Manage > Devices** and select the host name of the AP in the **Devices** list.
2. From the **Device Details** left pane, select **Configure**.
3. Under **Additional Settings**, 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 216, 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's client monitor policy.
8. For APs 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**.
10. To update the device immediately, select **Update**.
11. Select the type of update, and then select **Save as Defaults** to save this option as the default action.
12. To update the device immediately, select **Perform Update**.

Related Links

[Configure AP Devices](#) on page 466

Configure SSH

Before you can configure SSH access on a device, you must first enable **SSH Availability**. To do this, under your admin name at the top right of the ExtremeCloud IQ window, select **Global Settings > Administration > VIQ Management > SSH > SSH Availability** and enable the feature.

ExtremeCloud IQ 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 device from the device details panel., under **Configuration > Additional Settings > SSH**.

1. Go to **Manage > Devices** and select the host name of the AP in the **Devices** list.
2. From the **Device Details** left pane, select **Configure**.
3. Under **Additional Settings**, select **SSH**.
4. Under **Run Time**, select the length of time that you want SSH to be available for the device.

ExtremeCloud IQ 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 AP Devices](#) on page 466

Configure Switch Devices

After you select a **switch** from the Device List, you can create or modify the following:

- [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.
- [Switch Port Configuration](#): Edit switch ports, STP, Storm, and PSE settings.
- [Device Credentials](#): Assign or change network administrator credentials and administrator assignments.

- [SSH](#): Temporarily enable SSH to troubleshoot the device.
- **Web SSH** (For Digital Twin only): Temporarily enables you to SSH a console into the Digital Twin switch directly in the GUI, without the need for a third-party SSH terminal application.
- [sFlow Receivers](#): (SR Series only): Provide visibility into your switch traffic patterns.

After you make changes to the configuration, you must [push the configuration changes to the device](#).

Related Links

[Device Details Configuration Tasks](#) on page 465

Switch Device Configuration

Making device configuration changes at the switch 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 **Manage > Devices**.
2. Select the host name of the switch in the **Devices** list, and then select the **Configure** tab in the **Device Details** panel.
3. Under the **Configure** 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.
6. Toggle **Management Interface Settings** to **On** or **Off**.

When enabled, Switch Engine management interface settings apply 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**.
7. (Optional) Configure **Supplemental CLI**.

For more information, see [Device Details Configure Supplemental CLI](#) on page 489.
8. Select **Save Configuration**.
9. To update the device immediately, select **Update**.
10. Select the type of update, and then select **Save as Defaults** to save this option as the default action.
11. To update the device immediately, select **Perform Update**.

For more information about how to push updated configuration to the device, see [Push the Device-Level Configuration to the Device](#) on page 494.

Related Links

[Configure Switch Devices](#) on page 481

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 overwrite any changes made at the device level.

**Note**

DNS Server, NTP Server, SNMP Server, and Syslog Server configurations can be managed at the device level for EXOS and Switch Engine devices after unlock. Not all management server tabs are available for all device types.

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 **Manage > Devices**.
2. Select the **HOST NAME** of the device you want to manage.
3. Select **Configure > 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, then select **SAVE CONFIGURATION**.

The changes only apply at the device level. See *Configure Management Server Settings* in the *ExtremeCloud IQ Universal Switch Deployment Guide* for more information about management server configuration.

6. To update the device immediately, select **Update**.
7. Select the type of update, and then select **Save as Defaults** to save this option as the default action.
8. To update the device immediately, select **Perform Update**.

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 details about each option, see [Create a New Port Type](#) on page 248.
- 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 **Manage > Devices**.
2. Select a switch **Host Name** to see a details panel for that switch.
3. Select the **Configure** tab.
4. Under **Configuration**, select **Port/VLAN Configuration**.
5. Select **Unlock** to enable switch-level configuration changes.
6. Select each tab, and edit any accessible field.
7. Select **Save Port Configuration**.

**Note**

BPDU Restrict and BPDU Restrict Recovery Timeout settings are found within the STP settings.

8. To revert back to the network policy switch template, select **Revert to Switch Template**.
9. To update the device immediately, select **Update**.
10. Select the type of update, and then select **Save as Defaults** to save this option as the default action.
11. To update the device immediately, select **Perform Update**.

Related Links

[Configure Switch Devices](#) on page 481

Configure Switch 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 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 switch only. These changes always override the network policy configurations. To revert to the settings in the network policy, from the **Device List**, select the switch 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 **Manage > Devices**.
2. Select a switch **Host Name** to see a details panel for that switch.
3. Select the **Configure** tab.
4. Under **Configuration**, select **Device Credentials**.
5. 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.
6. 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.
7. Select **Save Device Credentials**.
8. To update the device immediately, select **Update**.
9. Select the type of update, and then select **Save as Defaults** to save this option as the default action.
10. To update the device immediately, select **Perform Update**.

Related Links

[Configure Switch Devices](#) on page 481

Configure SSH

Before you can configure SSH access on a device, you must first enable **SSH Availability**. To do this, under your admin name at the top right of the ExtremeCloud IQ window, select **Global Settings > Administration > VIQ Management > SSH > SSH Availability** and enable the feature.

ExtremeCloud IQ 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 device from the device details panel., under **Configuration > Additional Settings > SSH**.

1. Go to **Manage > Devices** and select the host name of the AP in the **Devices** list.
2. From the **Device Details** left pane, select **Configure**.
3. Under **Additional Settings**, select **SSH**.

- Under **Run Time**, select the length of time that you want SSH to be available for the device.

ExtremeCloud IQ creates an SSH session for the specified length of time between the SSH proxy server and the device.

- 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.

- 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 Switch Devices](#) on page 481

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.

- Go to **Manage > Devices**.
- Select a switch **Host Name** to see a details panel for that switch.
- Select the **Configure** tab.
- Under **Network Allocation**, select **Interface Configuration**.
- Select a port icon on the template graphic to view port details, if available.
- Select  to add, or  to edit an Interface.
- Enter the interface attributes according to the table below:

Table 119: 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.

Table 119: Interface Configuration Attributes (continued)

Field	Description
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 .

8. Select **Next**.
9. Confirm **Summary** details, and then select **Save**.
To go back and make changes, select **Previous**.
10. To delete Interfaces, select the Interface(s) and select .
11. To update the device immediately, select **Update**.
12. Select the type of update, and then select **Save as Defaults** to save this option as the default action.
13. To update the device immediately, select **Perform Update**.

Related Links

[Configure Switch Devices](#) on page 481

Routing Configuration

The device must have an IPv4 interface configured. For more information, see [Interface Configuration](#) on page 486.

Use this task to configure IP4 Static Routes for the selected device.

1. Go to **Manage > Devices**.
2. Select the host name of the switch in the **Devices** list, and then select the **Configure** tab in the **Device Details** panel.
3. Under the **Network Allocation** menu, select **Routing Configuration**.
4. Select  to add or  to edit, and then configure the following settings:

Table 120: 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. Note: Enabling Ping Protection will generate a Ping Protection Status tool tip when viewing your device within Manage > Devices > Monitoring > Routing .

Table 120: Static Route Settings (continued)

Field	Description
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. To update the device immediately, select **Update**.
8. Select the type of update, and then select **Save as Defaults** to save this option as the default action.
9. To update the device immediately, select **Perform Update**.

Related Links

[Configure Switch Devices](#) on page 481

Assign an sFlow Receiver to a Switch

Before you can assign an sFlow receiver to a switch, you must first configure an sFlow receiver as a common object. sFlow is not available for all Extreme switch models. See [Configure an sFlow Receiver](#) on page 358.

Use the following steps to assign sFlow receivers that you have configured as common objects to switches at the device level.

**Note**

sFlow assignments made at the device level override assignments made in the network policy device template.

1. Go to **Manage > Devices** and select the host name of a supported device.
2. Select **Configure > sFlow Receivers**
The sFlow Receivers feature is available only for supported switches.
3. Select .
4. Select a receiver object from the **Available sFlow Receivers** menu.
5. Enable **sFlow Receiver**.
6. Enable **Interface Packet Sampling**.
7. Move interfaces you want to sample from the **Available** column to the **Selected Interfaces** column using the arrows.
8. Enable **Counter Polling**.
9. Move interfaces you want polled from the **Available** column to the **Selected Interfaces** column.
10. Select **Save**.
11. Select **Save sFlow Receivers**.

Related Links

[Configure an sFlow Receiver](#) on page 358

Configure Port Router Forwarding

When enabled, port forwarding allows a router to open certain ports to incoming traffic from specified IP addresses. Port forwarding is helpful when you have a server behind your router that needs a port exposed to the Internet, such as an HTTP server that needs to be accessible to people outside the VPN, Branch, or HQ network. For each port, a port forwarding rule applies. You can have up to 128 port rules. You can edit or delete rules from the table. Use the following steps to enable port forwarding and create forwarding rules.

1. Select the user name of the router for which you want to enable port forwarding.
2. On the **Configure** tab, go to **Port Forwarding**.
3. Enable **Port Forwarding**.
4. Select the plus sign to add a new port forwarding rule.
5. Enter a description of how this rule will be used (optional).
6. Select a number for the outside port from the range of 1025-65535 (reserved ports cannot be used).
7. Select a number for the local port from the range of 1-65535.
8. Select **TCP**, **UDP**, or both from the protocol drop-down list.
9. Select a host IP address for the internal device from the drop-down list, or select the plus sign to add a new address.
10. Select **Add**.
11. When you are finished adding rules, select **Save**.

Device Details Configure Supplemental CLI

First go to **Global Settings > VIQ Management**, and 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 update CLI commands to multiple devices simultaneously from ExtremeCloud IQ.

1. Go to **Manage > Devices**.
2. Select the devices to update, and then select .
3. Select an existing supplemental CLI object, or select  to [Add a Supplemental CLI Object](#) on page 490.

4. Select one of these options:
 - **Override Supplemental CLI in the network policy:** Enable the network policy to override supplemental CLI objects for the device.
 - **Keep Supplemental CLI in the network policy and append below at end:** 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.
5. Select one of these options:
 - **UI overrides Supplemental CLI**
 - **Supplemental CLI overrides UI**
6. When you are finished, select **SAVE**.
7. To update the device immediately, select **UPDATE DEVICES** at the top right.
8. In the **Device Update** dialog box, select the type of update, and then select **Save as Defaults**.

To avoid an unnecessary system reboot, select **Delta Configuration Update**. ExtremeCloud IQ attempts to update only the configuration deltas. If a full update is required, the system prompts you to select **Complete Configuration Update**. Examples of CLI commands that require a full configuration update are: **system antenna-type** and **system environment**.
9. To update the device immediately, select **Perform Update**.

Related Links

[Add a Supplemental CLI Object](#) on page 490

Add a Supplemental CLI Object

To use the supplemental CLI tool, go to **Global Settings > VIQ Management**, and enable **Supplemental CLI**.

You can save supplemental CLI objects containing CLI commands, and ExtremeCloud IQ 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 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 **Configure > Common Objects > Basic > Supplemental CLI Objects**.
2. To add a new supplemental CLI object, select .
3. Type a **Name**.
4. Type an optional **Description**.
5. Type the CLI commands.
 - Enter multiple CLI commands, one command per line.
 - Use CLI Commands that contain IP and VLAN objects: `${ip:ip_object_name}` and `${vlan:vlan_object_name}`.
6. Select **SAVE** and perform a configuration update each time you append commands to device configurations.

To avoid an unnecessary system reboot, select **Delta Configuration Update**.

ExtremeCloud IQ attempts to update only the configuration deltas. If a full update is required, the system prompts you to select **Complete Configuration Update**.

Examples of CLI commands that require a full configuration update are: **system antenna-type** and **system environment**.

Related Links

[Device Details Configure Supplemental CLI](#) on page 489

About Digital Twin

Use the Digital Twin feature to create simulated devices for Universal Hardware switch models to help you prepare your network for real devices. For example, Digital Twin can simulate a new switch in the cloud to help you to identify and resolve configuration issues before you install the new device.

Digital Twin devices appear in the **Manage > Devices** list and are identified by the

following icon: . You can perform multiple actions to see how the devices will function in your network. You can assign a location, a network policy, access the CLI, shut down or restart a twin device, and configure device settings in the same way as you would an actual device. From the device list, you have several options:

- Select the hostname of a twin to see the device details. Many of the same monitor and configuration options that apply to real devices are available for their twins.
- Select the check box for the twin device to activate the **Actions** drop-down list above the table.
- Select the check box for a twin device to activate the **Update** option above the table.

Digital Twin requires OS Version 32.6.3 or later. To learn how to create a Digital Twin device, see [Device Details Configure a Digital Twin Device](#) on page 491.

Device Details Configure a Digital Twin Device

You can create up to 20 Digital Twin devices, each with a lifespan of 4 hours. Use this task to configure a Digital Twin device.

1. Go to **Manage > Devices**, and then select .

2. Select **Quick Add Devices > Manage Your Devices Directly from the Cloud**.
3. Under **DEVICE TYPE**, select **Digital Twin**.
4. Select an **OS PERSONA** from the list.
5. Select a **DEVICE MODEL** from the list.
6. Select the **OS VERSION** from the list.
Digital Twin requires OS Version 32.6.3 or later.
7. Select the **EXPANSION MODULE** from the list.
This option appears only for supported device models.
8. Select the **LICENSE TYPE** from the list.
9. Assign a **NETWORK POLICY** from the list.

**Note**

You can do this at a later time if you have not yet configured a network policy.

10. Select **Launch Digital Twin** or **Relaunch Digital Twin**.
The Digital Twin device now appears in the device list.

Related Links

[About Digital Twin](#) on page 491

Device Level WAN Stateful Firewall

WAN stateful firewall is a common feature used in branch networks to provide network level defense, typically by blocking unsolicited traffic from outside of the branch. It can also be used to control of branch traffic into and out of a router, such as allowing or denying traffic between local subnetworks, allowing or denying branch clients from going to a specific IP or range of IPs, or allowing or denying specific network protocols. To enable network policy firewall overrides and make adjustments to the firewall filtering rules for this device, perform the following steps:

1. Select **On** to enable overrides to the network policy firewall settings for a router.
2. Use the up and down arrows to change the order of the existing filtering rules in the table.
Rules are processed in order from top to bottom.
3. Select **Add** to add a new filtering rule.
4. Select a source address from the available options.
5. Select **On** (the default) to support auditing, accounting, and monitoring.
6. Repeat these steps to add additional filtering rules.
Use the up and down arrows to arrange your new rules in the table according to how you want to them to be processed.
7. Select **Save**.
8. To delete firewall rules, select the check box next to the rule, then select the delete icon.

Configure VRRP

To enable VRRP, you must have at least two routers with the same branch ID. VRRP changes require a complete configuration update on the devices

Virtual Router Redundancy Protocol (VRRP) allows multiple routers to function as a single logical routing unit. When using VRRP, routers that each have a different IP address share a VRRP ID and a virtual IP address that other network devices use as the router address. Routers that share a VRRP ID use VRRP to determine the state of other routers with the same VRRP ID. If one becomes unresponsive for a specific amount of time, VRRP uses the priority setting to determine which router will take over routing traffic.

Use the following steps to configure VRRP.

1. Toggle **Enable VRRP** to **On**.
2. Enter the VLAN ID for the routed traffic.
3. Enter the static subnet for the routed traffic.
4. Indicate whether a router in the VRRP routing group is included in the redundancy.
5. Enter the priority of the router.
 - **High:** This router handles the traffic.
 - **Medium:** This router handles the traffic when the high-priority router is offline.
 - **Low:** This router becomes active when the other priority routers are all offline.
6. Enter a numeric VRRP ID.
7. Enter the static virtual IP address that the routers share.
8. Enter the interval that the routers will wait before advertising their availability (the default is one second).
9. Select whether a higher-priority backup router preempts a lower-priority primary router.
10. Select whether the router monitors the state of the WAN connection.

If the primary router WAN connection is unresponsive, VRRP activates a backup router to handle traffic.

Router URL Filtering

Some Extreme Networks routers support HTTP URL filtering rules, which define URL filtering by white list, blocked list, and category, and which can be assigned to one or more user profiles. You can select from existing user profiles or you can create a new user profile in the URL filtering rule table.

Select the host name of a router from the devices list. In the device details window, under the Configure tab, select URL Filtering. After you turn URL Filtering on, you can perform the following steps to configure URL Filtering rules,

1. Go to **Manage > Devices**.
2. Select the host name of a router from the Device list.
3. In the device details window, navigate to **Configure > Additional Settings > URL Filtering**.
4. Toggle **URL Filtering** to **On**.
5. Select an existing rule, or select the add icon to add a new rule.
6. If you are adding a new rule, enter a name and description for the rule.
7. Select the plus sign above the rules table.

8. Add or select a schedule for when this rule applies.
9. Add or import up to 32 URLs for the allowed list and the blocked list.
You can add URLs manually or import them in the form of .csv file.
10. Select categories that you want this URL filter to block.
11. Select **Save Detail**.
12. When you see the new URL rule in the table, select **Save URL Rule**.

Push the Device-Level Configuration to the Device

Perform necessary configuration changes at the device level. After you save these changes, an exclamation mark appears in the device **Status** column, indicating that the device configuration is out of sync with the network policy.

Use this task to push configuration changes made at the device level to the selected devices, and replace the exclamation marks with green checks.

1. Go to **Manage > Devices** and select the devices to update.
Alternately, go to **Manage > Devices > ,** and select the **host_name** for a device. On the **Configure** page, select **Update**. Proceed to step 3.
2. Select **Update Devices**.
3. Select **Delta Configuration Update**.
4. Select **Perform Update**.

To avoid an unnecessary system reboot, select **Delta Configuration Update**.

ExtremeCloud IQ attempts to update only the configuration deltas. If a full update is required, the system prompts you to select **Complete Configuration Update**.

Examples of CLI commands that require a full configuration update are: **system antenna-type** and **system environment**.

The status icon changes from an exclamation mark to a green check.

5. For Universal switches, if you receive an out-of-sync error, hover over the message and review the details to reveal where the local configuration is out of sync.
 - a. Match the out-of-sync local configuration within the network policy, switch template, or device level configuration and perform an update device again.
 - b. If **Step a** is not successful, select **Perform delta configuration update and resolve local device configuration which is out of sync with ExtremeCloud IQ**.



Note

This option requires a minimum version of Switch Engine 32.3 or Fabric Engine 8.9 installed on the Universal switches.

Upload and Manage Media Gallery Content

Go to **Manage > Devices** *<select host name>* **Device Details** panel.

The **Media Gallery** is available only for real devices, and cannot be used with simulated devices.

Use this task to upload and manage images (.png or .jpg) or video (.mp4 or .mov) produced during installation of a device.

**Note**

It is recommended that the image file size be less than 500 KB, and the video file size be less than 5 MB.

1. To view and manage existing media files, or to add media files, select **View Device Media** under **Media Gallery** in the sidebar.
2. To upload an image file or video file:
 - a. Select **Choose File**, then browse to your local folder and select the target image or video. Select **Open**.
 - b. Optionally, select **Change File** if you want to exchange the file you selected in the previous step.
 - c. Select **Upload**
3. Optionally, edit the **Title**, which is automatically populated with the file name of the uploaded image or video file.
4. Optionally, enter a **Description** of the image or video.
5. Optionally, select **Upload New** to add another image. Repeat this step for all images or videos to be added.
6. Choose from the following actions:
 - To rotate an image to get a better view of details, select the image in the sidebar, then select .
 - To delete an image or video, select it in the sidebar, then select  to delete the file. Confirm the deletion.
 - Select  to close the **Media Gallery**.

Related Links

[Device Details Panel](#) on page 454

Manage Active Alarms

When you select the **Host Name** of a device from the **Devices** list and then select **Monitor > Alarms**, the following information is shown for the device:

- At the top of the main section, a diagram shows how the device is connected to the network.
- **Active Alarms View:** In this default view, you can see all active alarms for this device, and select and clear alarms. Use the column picker to select which columns are displayed in the table. Select or clear check boxes to display or hide columns. Your column selections are maintained if you go to another window and return, and when you log out and then log in again. Horizontal scrolling is available for this table when there are too many columns to fit in your display window.
- **Timeline View:** Switch to this view to see a graph with timelines representing alarms data captured within the specified time frame. By default, alarms are displayed for a 24-hour time frame. You can customize the time frame using the **Time Range** controls. Hover over graph lines to see more information. You can also clear alarms in the **Active Alarms** view. Cleared alarms become events and are then displayed in the **Event** log.

Related Links

[Set the Time Frame for Captured Data Displays and Reports](#) on page 551

Clients

Clients Health

The Client Health page shows health information based on the sites and time ranges for the active clients on your network.

To access the information, go to **Manage > Clients**.

Data widgets display the following:

- **Overall Score** - Poor (0-49), Good (50-79), Excellent (80-100) based on:
 - Wi-Fi Health Score
 - Network Health Score
 - Application Health Score
- **Clients** - 2.4 GHz, 5 GHz, 6 GHz
- **Client Issues** - Associated Issues, Auth Issues, Networking Issues

The Healthy and Unhealthy client lists display all associated client details. Use the **Connection Type**, **OS Type**, **Connected Via**, **User Profile**, and **Status** drop-down lists above the table to view real time or historical data.

Real-Time Troubleshooting is available for AP3000, AP3000x, AP5010, and AP5050U/D devices. For more information, see [Real-Time Troubleshooting](#) on page 505.

Table 121: Client List Details

Column	Description
Status	This column contains icons for each client, depending on the health of the connection. • Green indicates a healthy wireless connection. • Grey indicates that the client is not connected. • Red indicates that the wireless connection is in danger of failing. • Yellow indicates a poor-quality wireless connection.
Connection Type	Wired or wireless connection.
Host Name	The name of the device hosting the client.
SNR	If enabled APs consider signal-to-noise ratio to determine when to disassociate.
RSSI	The RF signal strength of the wireless link between the two neighboring devices. The RSSI range is 0-90.
Category Assignment (IoT only)	Operator-defined IoT category, such as printer, camera, thermostat, wireless client, and so on.

Table 121: Client List Details (continued)

Column	Description
Channel Utilization	The client channel utilization.
IPv4	The IPv4 address of the client.
MAC	The MAC address of the client. Select the hyperlink to view the Client Connection Details Panel on page 497 or to access the Client Tools menu.
User Name	The name of the user operating the client.
OS Type	The operating system running on the client as determined by the OS fingerprint. If the combination of requested DHCP parameters does not match an OS type in the client OS list, "unknown".
VLAN	The ID number of the VLAN to which the device assigned the client.
Connected Via	The port through which the client is connected.
User Profile	The user profile to which this client is assigned.

Select  to download the table information in a .csv format.

Related Links

[Connection Details Panel \(Wireless\)](#) on page 565

[Session Details \(Wireless\)](#) on page 570

[Client Tools \(Wireless\)](#) on page 502

Client Connection Details Panel

The connection details panel lists details about the current or last connection in a column to the left of the interactive widgets and tables.

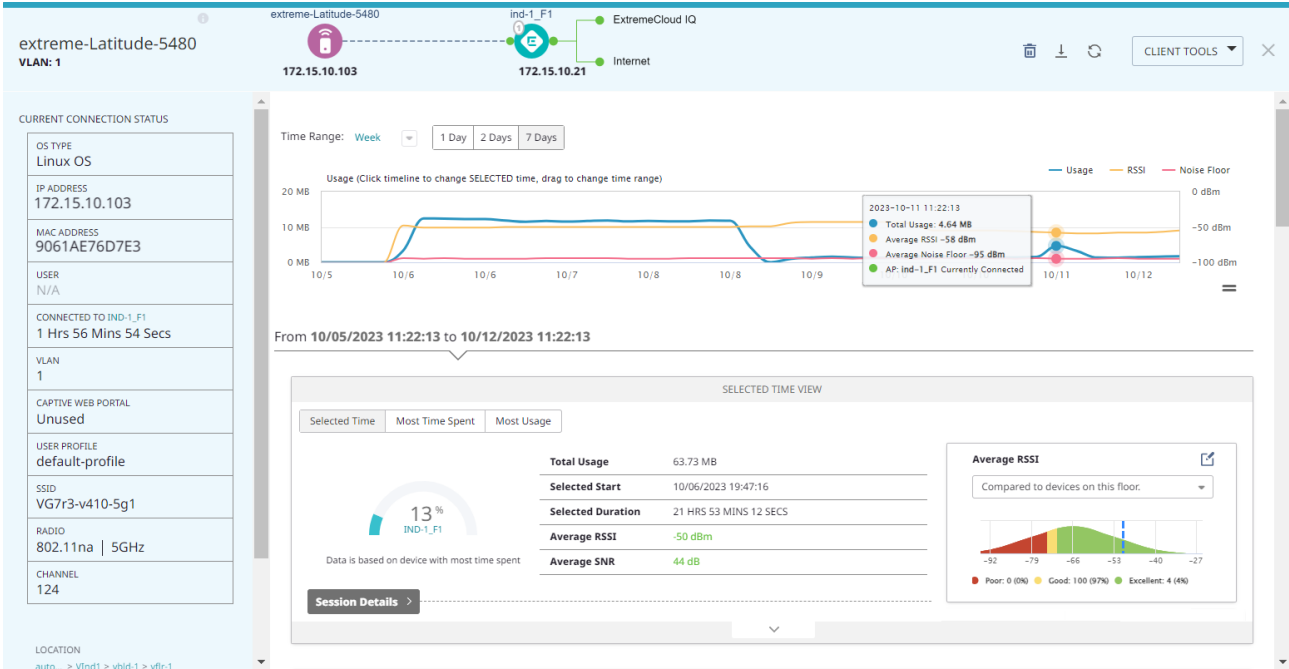


Figure 10: Connection Details Panel

The initial graph displays information about data usage, RSSI, and the noise floor. Use the **Time Range** menu to change the time period. Select from the following options:

- Day (1 Hour, 2 Hours, 4 Hours, 8 Hours, or 24 hours)
- Week (1 Day, 2 Days, 7 Days)
- Month (7 Days, 14 Days, 30 Days, or 90 Days)
- Custom (Use the Calendar controls to select the date range.)

Select one of the tabs to display relevant information:

- Selected Time
- Most Time Spent
- Most Usage

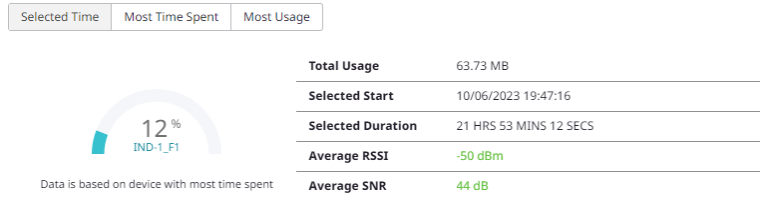


Figure 11: Selected Time

The **CLIENT TRAIL** table displays information about device connections. Display 10, 20, 50, or 100 results per page. Navigate pages by selecting the page number, or enter a page number and select **Go**. Color-coded connection status icons provide at-a-glance status information. Mouse over the icons for descriptions.

CLIENT TRAIL														
DEVICE NAME	FROM	TO	DURATION	AVERAGE RSSI	AVERAGE SNR	USAGE	SSID	ROAM	ASSOC	AUTH	DHCP	DEFAULT GATEWAY	DNS	
> ind-1_F1	2023-10-06 02:15:32	2023-10-06 08:25:08	6 Hrs 9 Mins 36 Secs	-51 dBm	44 dB	19.12 MB	VG7r3-v410-5g1	N/A	●	●	●	●	●	
> ind-1_F1	2023-10-06 08:25:40	2023-10-06 10:17:51	1 Hrs 52 Mins 11 Secs	-51 dBm	44 dB	5.86 MB	VG7r3-v410-5g1	N/A	●	●	●	●	●	
> ind-1_F1	2023-10-06 10:17:54	2023-10-06 17:50:09	7 Hrs 32 Mins 15 Secs	-51 dBm	44 dB	23.11 MB	VG7r3-v410-5g1	N/A	●	●	●	●	●	
> ind-1_F1	2023-10-06 10:17:54	2023-10-06 17:50:09	7 Hrs 32 Mins 15 Secs	-51 dBm	44 dB	23.11 MB	VG7r3-v410-5g1	N/A	●	●	●	●	●	
> ind-1_F1	2023-10-06 17:50:16	2023-10-06 17:50:17	0 Secs				VG7r3-v410-5g1	N/A	●	●	●	●	●	
> ind-1_F1	2023-10-06 17:50:17	2023-10-06 19:46:35	1 Hrs 56 Mins 18 Secs	-50 dBm	45 dB	5.88 MB	VG7r3-v410-5g1	N/A	●	●	●	●	●	
> ind-1_F1	2023-10-06 19:47:16	2023-10-07 17:40:28	21 Hrs 53 Mins 12 Secs	-50 dBm	44 dB	63.73 MB	VG7r3-v410-5g1	N/A	●	●	●	●	●	
> ind-1_F1	2023-10-07 17:41:30	2023-10-07 18:01:09	19 Mins 39 Secs	-50 dBm	44 dB	1.07 MB	VG7r3-v410-5g1	N/A	●	●	●	●	●	
> ind-1_F1	2023-10-07 18:01:42	2023-10-07 18:01:59	17 Secs	-49 dBm	46 dB	19.14 KB	VG7r3-v410-5g1	N/A	●	●	●	●	●	
> ind-1_F1	2023-10-07 18:02:43	2023-10-07 20:46:29	2 Hrs 43 Mins 46 Secs	-50 dBm	44 dB	7.61 MB	VG7r3-v410-5g1	N/A	●	●	●	●	●	
10 20 50 100														
⏮ ⏪ 1 2 3 4 5 ⏩ ⏭ Go														

Figure 12: Client Trail Table

The **TROUBLESHOOT SESSIONS** table displays in-progress and completed troubleshooting sessions.

TROUBLESHOOT SESSIONS				
TIMESTAMP	DESCRIPTION	INITIATED BY	STATUS	
> 2023-10-13 15:23:04		shrisha-ft-2@gmail.com	IN PROGRESS (09:48)	⏏ ⚠
> 2023-10-12 10:09:18		shrisha-ft-2@gmail.com	COMPLETED	⏏

Figure 13: Troubleshoot Sessions Table

The **CLIENTS ISSUES** table displays client issues. Filter the issues with the following options:

- Status
- Issue Type
- Summary
- User Profile
- Site Group
- Detected On

The **CLIENT EVENTS** table displays client events. Filter the events according to phase:

- All
- Association
- Authentication
- IP Assignment

CLIENT EVENTS

Phases

All

Show Probe

DEVICE NAME	TIMESTAMP	DEVICE BSSID	EVENT TYPE	DESCRIPTION
ind-1_F1	2023-10-12 14:03:27	BCF3105D74F4	Basic	Sta(at if=wifi1.1) is de-authenticated because of notification of driver
ind-1_F1	2023-10-12 14:03:27	BCF3105D74F4	Basic	Sta(at if=wifi1.1) is de-authenticated because of notification of driver
ind-1_F1	2023-10-12 14:03:27	BCF3105D74F4	Info	Rx deauth (reason 4 <assoc-leave>, rssi -55dB)

Figure 14: Client Events Table

To download the results as a CSV file, select .

The **NETWORK USAGE** section displays usage information in an interactive graph and **Top 10 Apps** widget. Mouse over points on the graph for details. From the hamburger menu, choose from the following options:

- Print chart
- Download PNG
- Download JPEG
- Download PDF
- Download SVG vector image

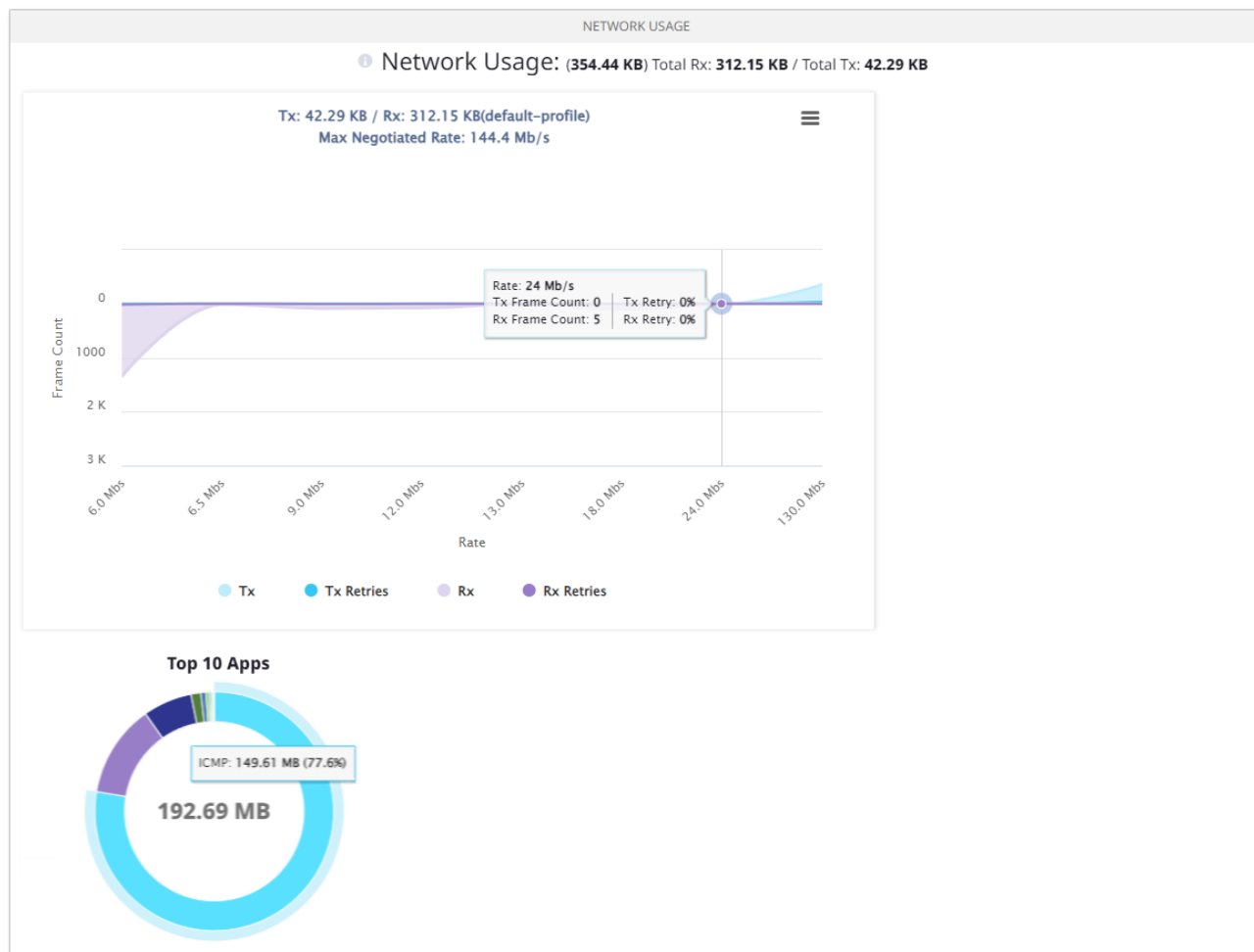


Figure 15: Network Usage Graph and Widget

Mouse over the **Top 10 Apps** widget to display information about app usage.

The **MAXIMUM CLIENT CAPABILITIES** widget displays the maximum client capabilities for all 2.4 and 5 GHz Wi-Fi clients connected to the AP during the selected period.

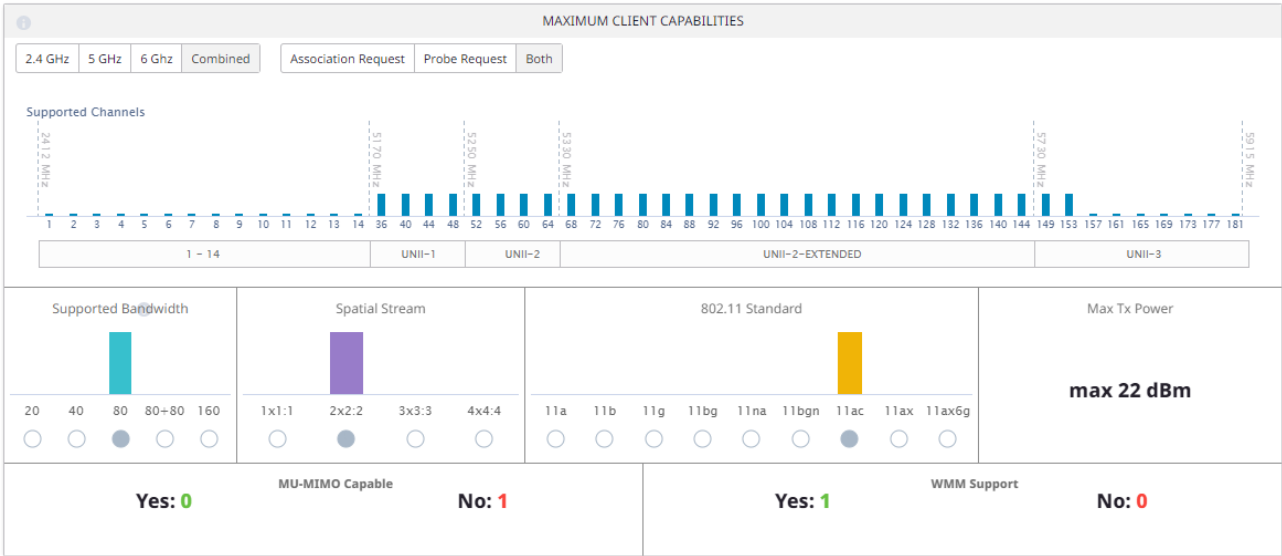


Figure 16: Maximum Client Capabilities Widget

Client Tools (Wireless)

Go to **Manage > Clients > <existing unhealthy client> > Client Tools**, and select one of the tools:

- Troubleshoot Now
- VLAN Probe
- Neighbors

Troubleshoot Now

Selected Client

9061AE76D7E3

Description

Please select this AP to which the client is currently connected.

Select Devices (1 Selected)

☒	Status	Host Name	IPv4 Address	MAC Address	Serial Number	IPv6 Address
☒		ind-1_F1	172.15.10.21	BCF3105D74C0	04102005200894	

OR

SHOW ALL DEVICES

CANCEL

START

Please select up to 10 access points to begin troubleshooting.

Select Devices (1 Selected)

IP Address/MAC Address/Serial Number

Model

ALL

Status

All

Location

☐ Unassigned

☐ auto_location_01

☐ AHQA-PROD

☐ AHQA

☐ AH1003

☐ AH1003-Store

☐ AH1008

☐ AH1009

☐ AH1011

☐ AH1016

☐ AH1018

☐ AH1019

☐ AH1020

☐	Status	Host Name	IPv4 Address	MAC Address	Serial Number	IPv6 Address
☐		Raj-Raj-0075	192.168.23.44	BCF310004400	03051907020075	
☐		Verwav-AP4k	192.0.0.231	B027CF6F0600	64002107010133	
☐		vind2-4th-floor-4k	172.15.10.15	B027CF6F0540	64002107010130	
☐		Pun-Pun-1473	7.7.7.198	BCF3102D51C0	04102003121473	
☒		ind-1_F1	172.15.10.21	BCF3105D74C0	04102005200894	
☐		Del-Del-0044	10.234.143.175	241FBD01FEC0	WM052223W-30044	
☐		ind2-305c-F1	172.15.10.169	BCF3107270C0	03052007030030	
☐		Mum-Mum-1450	7.7.7.195	BCF3102D4C00	04102003121450	

CANCEL

START

Figure 17: Troubleshoot Now Tool

- Troubleshoot Now
- VLAN Probe

Troubleshoot Now

Selected Client

9061AE76D7E3

Description

Please select this AP to which the client is currently connected.

Select Devices (1 Selected)

☒	Status	Host Name	IPv4 Address	MAC Address	Serial Number	IPv6 Address
☒		ind-1_F1	172.15.10.21	BCF3105D74C0	04102005200894	

OR

SHOW ALL DEVICES

CANCEL

START

Please select up to 10 access points to begin troubleshooting.

Select Devices (1 Selected)

IP Address/MAC Address/Serial Number

Model

ALL

Status

All

Location

☐ Unassigned

☐ auto_location_01

☐ AHQA-PROD

☐ AHQA

☐ AH1003

☐ AH1003-Store

☐ AH1008

☐ AH1009

☐ AH1011

☐ AH1016

☐ AH1018

☐ AH1019

☐ AH1020

☐	Status	Host Name	IPv4 Address	MAC Address	Serial Number	IPv6 Address
☐		Raj-Raj-0075	192.168.23.44	BCF310004400	03051907020075	
☐		Verwav-AP4k	192.0.0.231	B027CF6F0600	64002107010133	
☐		vind2-4th-floor-4k	172.15.10.15	B027CF6F0540	64002107010130	
☐		Pun-Pun-1473	7.7.7.198	BCF3102D51C0	04102003121473	
☒		ind-1_F1	172.15.10.21	BCF3105D74C0	04102005200894	
☐		Del-Del-0044	10.234.143.175	241FBD01FEC0	WM052223W-30044	
☐		ind2-305c-F1	172.15.10.169	BCF3107270C0	03052007030030	
☐		Mum-Mum-1450	7.7.7.195	BCF3102D4C00	04102003121450	

CANCEL

START

Figure 18: Troubleshoot Now Tool

Select the connected AP, or **SHOW ALL DEVICES** and select up to 10 APs, and then select **START**. The session appears in the **TROUBLESHOOT SESSIONS** table. See [Connection Details Panel \(Wireless\)](#) on page 565.

CLOSE VLAN PROBE

VLAN:

1

(1-4094)

Probe Retries

1

(1-10)

Timeout

3

(1-60 seconds)

The DHCP Test is complete!

START

STOP

CLEAR

DHCP Test Results

VLAN ID	AVAILABLE	SUBNET
1	Yes	172.15.10.0/24

Figure 19: VLAN Probe

The VLAN Probe tool determines whether VLANs are operational on the wired network and reports the status, including the subnet of each VLAN.

Specify the VLAN or range, the number of **Probe Retries**, and the **Timeout**, and then select **Start**.

Related Links

[Connection Details Panel \(Wireless\)](#) on page 565

[Connectivity Experiences](#) on page 585

[Connectivity Experiences Panel \(Wireless\)](#) on page 588

Real-Time Troubleshooting

Real-Time Troubleshooting is designed to monitor and diagnose client-side issues as they occur in real-time. This functionality is supported on the following devices: AP3000, AP3000x, AP5010, and AP5050U/D.

Real-time client monitoring displays the following insights into client-side issues, allowing for prompt identification and resolution:

- **RSSI (Received Signal Strength Indicator)**: Measures the power level that a device receives from an access point.
- **SNR (Signal-to-Noise Ratio)**: Indicates the quality of the signal relative to background noise.
- **Usage**: Tracks the bandwidth consumption of connected devices.
- **Tx (Transmit) and Tx Retries**: Monitors the number of packets sent and the number of retransmissions required.
- **Rx (Receive) and Rx Retries**: Tracks the number of packets received and the number of retransmissions required.

Client Statistics displays the number of data packets transmitted and retried. **Packet Stream** displays the control packets used to manage the network.

You can run Real-Time Troubleshooting simultaneously on up to 10 access points. This capability is particularly useful for identifying and addressing roaming issues, where clients move between different access points.

By leveraging Real-Time Troubleshooting, network administrators can gain a comprehensive view of network performance and client behavior, enabling them to quickly address any issues that arise.

Use this task to begin Real-Time Troubleshooting.

1. Navigate to **Manage > Clients**.
2. Select an online client, and then select **Real-Time Troubleshooting**.
3. Select a **client from this site (Hostname of MAC)**.
4. Select **one or more APs to track the client**, up to a maximum of 10.

5. Select one of the following **Packet Stream** options view:

- All
- Data Frames
- Management Frames

6. Select **Start**.



Note

Starting up Real-Time Troubleshooting services typically takes about 10-20 seconds.

7. Select **Client Statistics** to see the following detailed information about the transmission (Tx) and reception (Rx) of packets:

- **Tx Packets:** The number of packets sent from the source device.
- **Rx Packets:** The number of packets received by the destination device.
- **Tx Retries:** The number of times packets had to be retransmitted due to errors or failures in the initial transmission.
- **Rx Retries:** The number of times packets had to be re-received due to errors or failures in the initial reception.
- **Total Packets:** The total number of packets sent and received.
- **Total Retries:** The total number of retransmissions and re-receptions due to errors.
- **Total Data Usage:** The overall amount of data transmitted and received, in bytes.

8. Select **Packet Stream** to see the following details for each packet:

- **Time:** The timestamp indicating when the packet was captured.
- **Serial Number:** A unique identifier assigned to each packet for tracking purposes.
- **Source:** The IP address or hostname of the device that sent the packet.
- **Destination:** The IP address or hostname of the device intended to receive the packet
- **Protocol:** The communication protocol used by the packet.
- **Length:** The size of the packet in bytes.

9. Select **Stop** to end Real-Time Troubleshooting.

Users

ExtremeCloud IQ presents the **Connected Users** list in table format. The list provides details about connected users in real time or within a specified time frame. Use the table controls to customize your view.

The following sections describe the types of data related to connected users that ExtremeCloud IQ collects and displays, and how to customize your view.

Related Links

[View Connected Users](#) on page 507

[Connected Users List](#) on page 507

[User Details](#) on page 508

View Connected Users

Use the following procedure to display the **Connected Users** list and customize your view.

1. Go to **Manage > Users**.
2. Use the table controls to customize your view.
 - Choose the time period for which to display data:
 - **Real Time**
 - **Historical**

Historical data is updated hourly. A graph provides a visual representation of the data captured for the specified time frame. You can change the time frame using the **Time Range** controls. See [Set the Time Frame for Captured Data Displays and Reports](#) on page 551.

- Use the **Source** menu to filter information by authentication type:
 - **All**
 - **RADIUS**
 - **PPSK**
 - **Others**
- Select  to update the data.
- Select a user name to view detailed information about that user. See [User Details](#) on page 508.
- Sort table rows alphabetically or numerically by selecting any of the column headings. Select the heading again to sort it in reverse order.
- Select and drag the right edge of any table column to change the column width to display longer entries.
- Select the  to save user data as a file named **monitoring.activeUsers.csv**.

Related Links

[User Details](#) on page 508

[Connected Users List](#) on page 507

[Set the Time Frame for Captured Data Displays and Reports](#) on page 551

Connected Users List

The **Connected Users** list displays the following details for active users in your network:

- **Status:** Connected or disconnected.
- **User Name:** The name by which this user is identified.
- **User Group:** The user group to which this user is assigned, if any. You can configure user groups in the SSID portion of a network policy workflow or in **Configure > User Management > User Groups**. If the user does not belong to a group, N/A is shown in this column.
- **#Clients:** The number of active client devices this user has connected to the network.

- **Usage:** The amount of data this user has transmitted and received on the network during the current session.
- **Source:** The authentication method by which this user device accessed the network.
- **Session Time:** The length of the current session for this user.
- **Expires On:** The expiration date assigned to the account. If the user account does not have an expiration set or is set never to expire, the value is N/A or Never Expire.

Related Links

[View Connected Users](#) on page 507

User Details

When you select a user name from the **Connected Users** table, ExtremeCloud IQ displays the **Summary View** for the user. The summary provides the following information:

- **Connection details:** The time span of the user's current connection.
- **Number of clients:** Hover over **Clients** to see more information about client devices.
- **Applications:** Details about the network applications this user accessed, including the top app and the most used apps.
- **Total Network Usage:** The amount of data that the user transmitted and received. You can download this chart as a PNG, JPEG, or PDF file.
- **Last Known Location:** The location in your network where this user was last connected, or is currently connected. Select any name in the location path to see the location on a map.
- **Timeline:** The graphical timeline reflects peak and low client usage by hour, day, or month. ExtremeCloud IQ displays any alarms that occurred during the specified time range. Hover over an alarm for details.
- **Network Usage:** This information is displayed below the timeline and shows details about network usage by client, SSID, User Profile, and Radio.
- **Top 5 Applications by Usage:** Usage information for the top 5 applications.

To refresh the data display, select .

Related Links

[View Connected Users](#) on page 507

Events

The events log shows events reported by network devices. You can use this information to audit activity or select the download icon to archive it. By default, the events log shows the most recent event at the top and is refreshed hourly.

Use the column picker to customize what appears in the table. Your selections persist if you go to another window and return, and when you log out and then log in again. Horizontal scrolling is available for this table when there are too many columns to fit in your display window. Most column headers in the Event Log are sortable. You

can select and display multiple events at the same time, which can be useful for large-batch operations.

Events log entries contain the following elements:

- **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

ExtremeCloud IQ continually monitors operations, with the following objectives:

- To detect, record, and report details of specific events
- To evaluate performance metrics and report occurrences where specific criteria are met

The specific events detected and metrics evaluated, and the criteria for raising an alert, are stipulated in the **Alert Rules** of an **Alert Policy**, as follows:

- **Global Policy** — This is the default policy. The Alert Rules of this policy apply to all devices at all sites, and can be modified as desired.
- **Site Policy** — Alert Rules for a site policy apply to all devices at the specified site. Site Policy rules override Global Policy rules for the specified site.



Note

Each site can have only one Site Policy; however, you can assign the same Site Policy to multiple sites.

Users can receive alert notifications through email or Webhooks.

Related Links

[Manage Alerts](#) on page 509

[View Legacy Alarms](#) on page 514

[Alert Policy](#) on page 515

[Manage Notifications](#) on page 523

Manage Alerts

Go to **Manage > Alerts**.

The **Alerts** dashboard includes:

- A [list of alerts](#) raised during the specified time range
- Interactive [widgets](#) that summarize, highlight, and logically group the alerts raised during the specified time range

- Tools that allow users to filter the alerts list, manage alerts, and configure alert policies

**Note**

Alerts are supported for devices that are connected directly to ExtremeCloud IQ cloud management only. Devices that appear in ExtremeCloud IQ but are managed by ExtremeCloud IQ Controller, the ExtremeWireless WiNG implementation, or ExtremeCloud IQ Site Engine will not generate alerts.

**Note**

The ExtremeCloud IQ Pilot banner displays a **Notifications** icon  and the total number of **Unacknowledged Critical** alerts raised over the last 24 hours. Hover over the icon to view a summary of the five most recent Critical alerts. Select **View All** to open the Alerts dashboard—from any user interface—and review details of, and optionally acknowledge, the Critical alerts.

Select **Alert Policy** to modify the **Global Policy** or to create or modify a **Site Policy**.

Select **View Legacy Alarms** to view legacy alarms.

Alert Details

By default, the Alerts dashboard displays information about alerts raised at all sites for the last 24 hours. You can filter the **Alert Details** list using either one or a combination of the following methods:

- Use the **Sites** drop-down menu to display alerts associated with a specific site.
- Use the **Time Range** controls to specify a time range—within the last 30 days—for which you want to display alerts.
- Use interactive widget controls to display alerts based on **Severity**, **Alert Category**, or **Top 5 Alert Type**.
- Use the **Status** drop-down list to display **All** (default), **Acknowledged**, or **Unacknowledged** alerts.

**Note**

After you set filters, if you exit the Alerts dashboard, the filters do not persist. You cannot save filter settings.

The **Alert Details** pane lists alerts and related details in tabular form. [Table 122](#) describes the type of information displayed in each column and the tools users can employ.

Table 122: Alert Details List Column Headings

Column Heading	Description
Severity	Displays alert severity levels, as follows: • Critical - red bead  • Warning - yellow bead  • Info - blue bead 
Summary	Provides an interactive description of the alert. Select the description to open the Alert Detail pop-up window, which displays variations of the following information, depending on the source of the alert: • Info ◦ Summary — Summarized alert description. ◦ Detected — The exact time the event was detected. • Source ◦ Type — Possibilities are: - Device - CPU - PSU ◦ Name — Device host name. • Description ◦ Device ID — The identifier assigned to the device. ◦ Device Name — The name assigned to the device. ◦ Admin State — Managed or Unmanaged. ◦ IP Address — The IP address of the device. ◦ Real Device — True or False. ◦ Mac Address — The MAC address of the device. ◦ Model — The AP or switch model. ◦ Serial Number — The device serial number. ◦ Location — The site, building, and floor location of the device. ◦ PSU Number — Power supply identifier. ◦ PSU Capacity — Available power. In the Alert Detail window, choose from the following actions: • Select  to acknowledge the alert. • Select  to close the window. Note: Alerts can apply to specific device models based on the feature support. For example, the alert: <i>Switch SSH Login Failed</i> applies to switches running EXOS (Switch Engine) and VOSS (Fabric Engine) only.

Table 122: Alert Details List Column Headings (continued)

Column Heading	Description
Category	Identifies the category of the alert. Possibilities are: • Device • XIQ • Security • Performance • Client • Anomaly • Static Route Ping Protection • DHCP Snooping Rogue MAC Detection
Source	Displays an interactive device host name. Select the host name to open the Manage > Device > Monitor window to investigate the related alert issue.
Detected	Indicates when the event was detected or the performance metric criteria was met.
Acknowledge	Identifies the acknowledgment status of the alerts, as follows: •  — Unacknowledged alert. •  — Acknowledged alert. Choose from the following actions: • Hover over an alert's  icon to discover which user acknowledged the alert. • Select one or more alert check boxes, then select an  icon to open the Acknowledge Alert? pop-up window. Select OK to confirm acknowledgment, or select Cancel to quit the operation. Note: Multiple alerts of different types and at different sites can be selected and acknowledged simultaneously. Once acknowledgment is confirmed, it cannot be reversed. Acknowledged alerts cannot be deleted. They can be filtered out of the Alert Details list using the Status drop-down menu.

Alerts Summary

Alert widgets provide a graphical summary of alerts and include color-coded refinements based on severity, category, and most prolific types of alerts. Widgets are interactive, allowing users to filter the alerts in the **Alert Details** list based on the refinements.

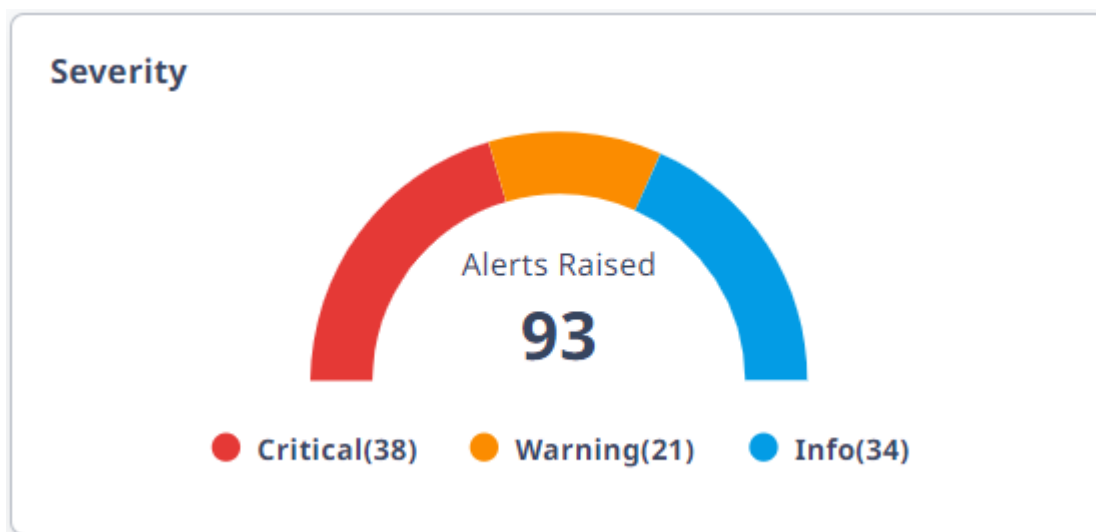


Figure 20: Severity Widget

This 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

Select a colored band in the graphic, or a bead, to filter the **Alert Details** list on the basis of Severity.



Figure 21: Category Widget

This widget displays the total number of **Alerts Raised** in all categories for the specified time range. Colored bands of the graphic and color-matched beads below it represent refinements based on **Alert Category**, as follows:

- Device
- Performance
- Security

Select a colored band in the graphic or a bead to filter the **Alert Details** list on the basis of Alert Category.

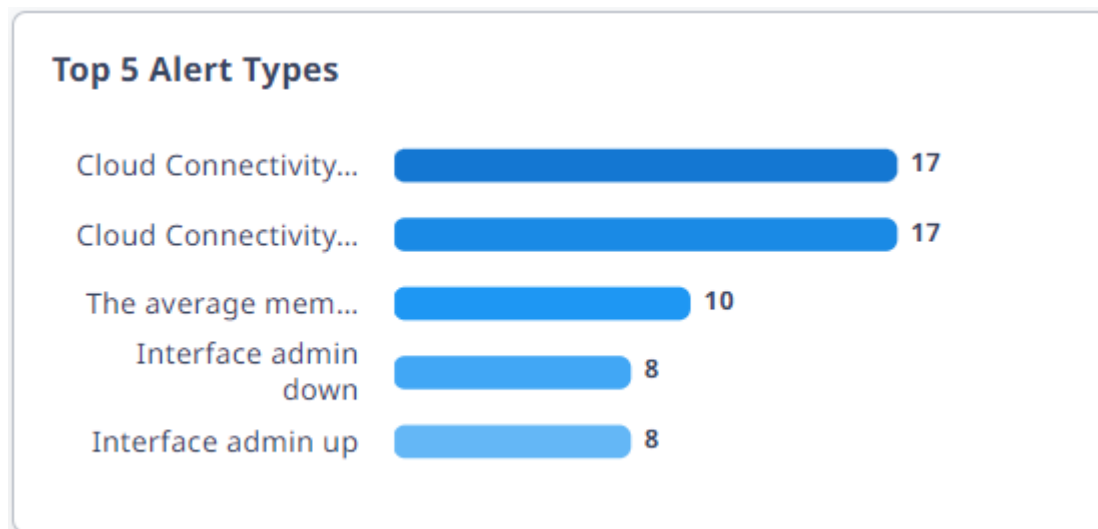


Figure 22: Top 5 Alert Widget

This widget displays the five most prolific alert types raised for the specified time range. Select a colored band in the graphic to filter the **Alert Details** list on the basis of Alert Type.

Related Links

[Alerts](#) on page 509

[Alert Policy](#) on page 515

[Manage Notifications](#) on page 523

View Legacy Alarms



Note

This page will be deprecated in a future release.

Go to **Manage > Alerts > View Legacy Alarms**.

See [Alarms](#) on page 464 for information about the information displayed in this window, and the tools users can employ to filter the view.

Alert Policy

The **Alert Policy** window includes tools that allow users to take the following actions:

- To configure a new Site Policy, select **Add Site Policy**.
- To receive alert notifications through email or Webhooks, select **Notifications**.
- To configure Alert Rules for all devices at all sites, select the **Global Policy** tab, then see [Configure Alert Rules](#) on page 523 for details.
- To manage site policies, select the **Site Policies** tab, then take any of the following actions with configured site policies in the list:
 - Select  associated with a site to remove the assignment of the policy to that site. There must be at least one site assigned to a policy.
 - Select  associated with a site policy to configure the Alert Rules. See [Configure Alert Rules](#) on page 523 for details.
 - Select  associated with a site policy to modify it.
 - Select  associated with a site policy to delete it.

Related Links

[Alert Rules Overview](#) on page 516

[Add or Edit a Site Policy](#) on page 515

[Manage Alerts](#) on page 509

Add or Edit a Site Policy

Before you begin, review the information about managing site policies in [Alert Policy](#) on page 515.

Go to **Manage > Alerts > Alert Policy**.

Use this task to add and assign a Site Policy, or edit an existing policy. You can assign only one Site Policy to a site; however, you can assign a Site Policy to multiple sites.



Note

Site Policy alert rules override Global Policy alert rules for the specified site.

1. Select **Add Site Policy**.
2. Enter or modify the **Policy Name**.
3. Select one or more check boxes associated with the sites to which you want to apply this policy.
4. Use the **Search** field to narrow the list of sites from which to choose.
5. Select **Save** to commit the changes, or select **Cancel**.

Proceed to [Configure Alert Rules](#) on page 523.

Related Links

[Alert Rules Overview](#) on page 516

[Manage Alerts](#) on page 509

Alert Rules Overview

Alert Rules stipulate the specific events detected and metrics evaluated, and the criteria for raising an alert.

Alert Rule settings options and default settings are identical for both Global and Site policies. See [Alert Rules — Settings Options](#) and [Alert Rules — Default Settings](#) on page 517 for details.

Alert Rules — Settings Options

The event and metric alert rule options are as follows:

Event and Metric Alert Rule Options:

Enabled or Disabled

Trigger Type:

- Immediate
- Deferred

days

hours

minutes

seconds

An alert is raised if the condition persists for the configured deferral period.

- Repeated

Occurred — Number of times the event occurs or criteria for the metric is met

days

hours

minutes

seconds

An alert is raised if the condition repeats the configured number of times.

Optionally, users can defer the alert by setting the slider to enable the time setting fields, then configuring the deferral period.

Raise Alert

- Critical
- Warning
- Info

Metric-only Option:

When (the metric is...)

- Operator

>= (greater than or equal to)

> (greater than)

<= (smaller than or equal to)

< (smaller than)

= (equal to)

!= (not equal to)

- Threshold

0 - 100000000 (% , V, Watt, Mw, °C, byte)

Alert Rules — Default Settings

[Table 123](#) describes the event types that ExtremeCloud IQ can detect and the default rule criteria used for raising an alert.

Table 123: Events — Default Alert Rule Settings

Event	Default Alert Rule Settings
Device	
AFC Radio Down - Channel/Power Not Supported	• Disabled • Trigger Type: Immediate • Raise Alert: Warning
AFC Radio Down - No AFC Info	• Disabled • Trigger Type: Immediate • Raise Alert: Warning
AFC Radio Down - Timeout	• Disabled • Trigger Type: Immediate • Raise Alert: Critical
AFC Radio Up	• Disabled • Trigger Type: Immediate • Raise Alert: Info
Cloud Connectivity Established	• Disabled • Trigger Type: Immediate • Raise Alert: Info
Cloud Connectivity Lost	• Enabled • Trigger Type: Deferred 10 minutes • Raise Alert: Info
Interface admin down	• Disabled • Trigger Type: Immediate • Raise Alert: Info
Interface admin up	• Disabled • Trigger Type: Immediate • Raise Alert: Info
Interface operation down	• Disabled • Trigger Type: Immediate • Raise Alert: Info

Table 123: Events — Default Alert Rule Settings (continued)

Event	Default Alert Rule Settings
Interface operation up	• Disabled • Trigger Type: Immediate • Raise Alert: Info
Power supply failed	• Enabled • Trigger Type: Immediate • Raise Alert: Info
Power supply not present	• Disabled • Trigger Type: Immediate • Raise Alert: Info
Power supply recovered	• Enabled • Trigger Type: Immediate • Raise Alert: Info
Power supply unplugged	• Enabled • Trigger Type: Immediate • Raise Alert: Info
Switch fan failed	• Enabled • Trigger Type: Immediate • Raise Alert: Info
Switch fan not present	• Enabled • Trigger Type: Immediate • Raise Alert: Info
Switch fan recovered	• Enabled • Trigger Type: Immediate • Raise Alert: Info
Switch power failed	• Enabled • Trigger Type: Immediate • Raise Alert: Info
Security	
Device SSH login failed	• Disabled • Trigger Type: Immediate • Raise Alert: Info

Table 124 describes the metrics that ExtremeCloud IQ evaluates and the default rule criteria used for raising an alert.



Note

When the configured threshold for an alert rule is exceeded, the system raises a single alert. If performance returns to normal, and then exceeds the threshold again, the system raises a new alert.

Table 124: Metrics — Default Alert Rule Settings

Metric	Default Alert Rule Settings
AP Radio Usage	
Total Channel Usage	• Enabled • When: Total Channel Usage - Operator: >= - Threshold: 80% • Trigger Type: Immediate • Raise Alert: Info
Total Interference Usage	• Disabled • When: Total Interface Usage - Operator: >= - Threshold: 20% • Trigger Type: Immediate • Raise Alert: Info
Total RX Usage	• Disabled • When: Total RX Usage - Operator: >= - Threshold: 80% • Trigger Type: Immediate • Raise Alert: Info
Total TX Usage	• Disabled • When: Total TX Usage - Operator: >= - Threshold: 80% • Trigger Type: Immediate • Raise Alert: Info
CPU & Memory Usage	
Avg CPU Usage	• Enabled • When: Avg CPU Usage - Operator: >= - Threshold: 80% • Trigger Type: Deferred 30 minutes • Raise Alert: Info

Table 124: Metrics — Default Alert Rule Settings (continued)

Metric	Default Alert Rule Settings
Avg Memory Usage	• Enabled • When: Avg Memory Usage - Operator: >= - Threshold: 80% • Trigger Type: Deferred 30 minutes • Raise Alert: Info
Max CPU	• Disabled • When: Max CPU - Operator: >= - Threshold: 80% • Trigger Type: Immediate • Raise Alert: Info
Min CPU	• Disabled • When: Min CPU - Operator: <= - Threshold: 1% • Trigger Type: Immediate • Raise Alert: Info
Device Temp	
Device Temp	• Disabled • When: Device Temp - Operator: >= - Threshold: 45 °C • Trigger Type: Immediate • Raise Alert: Info
Power Consumption	
Available Power	• Disabled • When: Available Power - Operator: >= - Threshold: 350000 Mw ** • Trigger Type: Immediate • Raise Alert: Info
Consumed Power	• Disabled • When: Consumed Power - Operator: >= - Threshold: 100000 Mw *** • Trigger Type: Immediate • Raise Alert: Info

Table 124: Metrics — Default Alert Rule Settings (continued)

Metric	Default Alert Rule Settings
Switch PSU Usage	
Avg Input Volt	• Disabled • When: Avg Input Volt - Operator: >= - Threshold: 120 V * • Trigger Type: Immediate • Raise Alert: Info
Avg Output Power	• Disabled • When: Avg Output Power - Operator: >= - Threshold: 350 Watts ** • Trigger Type: Immediate • Raise Alert: Info
Avg Output Volt	• Disabled • When: Avg Output Volt - Operator: >= - Threshold: 120 V * • Trigger Type: Immediate • Raise Alert: Info
MAX Switch Input Volt	• Disabled • When: MAX Switch Input Volt - Operator: >= - Threshold: 125 V • Trigger Type: Immediate • Raise Alert: Info
MAX Switch Output Power	• Disabled • When: MAX Switch Output Power - Operator: >= - Threshold: 650 Watts ** • Trigger Type: Immediate • Raise Alert: Info
MAX Switch Output Volt	• Disabled • When: MAX Switch Output Volt - Operator: >= - Threshold: 120 V • Trigger Type: Immediate • Raise Alert: Info

Table 124: Metrics — Default Alert Rule Settings (continued)

Metric	Default Alert Rule Settings
MIN Switch Input Volt	• Disabled • When: MAX Switch Input Volt - Operator: <= - Threshold: 115 V • Trigger Type: Immediate • Raise Alert: Info
MIN Switch Output Power	• Disabled • When: MIN Switch Output Power - Operator: >= - Threshold: 100 Watts ** • Trigger Type: Immediate • Raise Alert: Info
MIN Switch Output Volt	• Disabled • When: MIN Switch Output Volt - Operator: >= - Threshold: 120 V * • Trigger Type: Immediate • Raise Alert: Info
Wired Port Usage	
Total RX Byte Count	• Disabled • When: Total RX Byte Count - Operator: >= - Threshold: 10000000 byte • Trigger Type: Immediate • Raise Alert: Info
Total TX Byte Count	• Disabled • When: Total TX Byte Count - Operator: >= - Threshold: 10000000 byte • Trigger Type: Immediate • Raise Alert: Info
Notes: • * Can be 120 or 220 V, depending on SKU/PSU. • ** Recommended approximate setting. Varies across different SKUs. • *** Recommended approximate setting. Varies across different SKUs, and depends on what is connected to the device.	

Related Links

[Configure Alert Rules](#) on page 523

[Alert Policy](#) on page 515

Configure Alert Rules

Before you begin, review the information about alert options and rules in [Alert Rules Overview](#) on page 516.

Use this task to configure Alert Rule settings, establishing the criteria for raising alerts.

1. Go to **Manage > Alerts > Alerts Policy**.
2. Choose from the following options:
 - To modify Global Policy rules, proceed to the next step.
 - To configure Site Policy rules, select the **Site Policies** tab, locate the target Site Policy in the list, then select the associated  to open the Alert Rules cascading menus. Proceed to the next step.
3. Select  or  to navigate the **Event** and **Metric** tabs, which contain the Alert Rules.
4. Use the slider control to **Enable** or **Disable** an Alert Rule.
5. Select  associated with an Event or Metric to open its **Alert Rule** window, then modify the settings.
6. Select **Save** to commit changes, or select **Cancel**.
7. Repeat these steps for each event and metric for which you want to change the settings.

Related Links

[Alert Policy](#) on page 515

Manage Notifications

Go to **Manage > Alerts > Alert Policy > Notifications**.

Users can configure notifications to send alerts to Webhook URLs for viewing alerts in real time or to email addresses for viewing alerts when it is convenient.

The **Notifications** window has two tabs:

- **Manage Emails** — This tab displays a list of configured email notifications.
- **Manage Webhooks** — This tab displays a list of configured Webhook notifications.

Each tab includes management tools that allow users to choose from the following actions:

- To add and configure an email or Webhook notification, select .
- To delete multiple existing email or Webhook notifications, select the check boxes associated with the target entries in the list, then select  located at the top-left of the list.

To delete a single entry in the list, under the **Actions** column, select  associated with the list entry.

Select **OK** to confirm the deletion, or select **Cancel**.

- To edit an existing email or Webhook notification, under the **Actions** column, select  associated with the target item in the list. When editing is complete, select **Save** to commit the changes, or select **Cancel**.

Manage Emails Tab

[Table 125](#) describes the type of information displayed under each column in the Email Notifications list and any actions that a user can take.

Table 125: Email Notifications List Column Headings

Column Heading	Description
Email Address	Email address to which alerts are sent.
Created On	Date on which the notification is created.
Verify	Indicates whether the email address is verified, and allows users to initiate the email verification process, as follows: - Unverified —  - Verified —  To start the verification process, select . The recipient at the configured email address must open the verification email that ExtremeCloud IQ sends, and select Validate Your Email Address within 30 minutes to complete the verification process. If verification is successful,  displays when the window refreshes. To refresh the window, select , or exit and return to the Email tab.
Actions	Choose from the following actions: - Select  to delete the associated list entry. - Select  to edit the associated list entry.

Manage Webhooks Tab

[Table 126](#) describes the type of information displayed under each column in the Webhook Notifications list and any actions that a user can take.

Table 126: Webhook Notifications List Column Headings

Column Heading	Description
Post URL	URL to which the alerts are sent.
Access Token	Access token, if configured.
Created On	Date on which the notification is created.
Actions	Choose from the following actions: - Select  to delete the associated list entry. - Select  to edit the associated list entry.

Related Links

[Add or Edit an Email Notification](#) on page 525

[Add or Edit a Webhook Notification](#) on page 525

Add or Edit an Email Notification

Go to **Manage > Alerts > Alert Policy > Notifications**.

Use this task to set up email notifications for alerts.

1. Select **Manage Emails**.
2. Choose from the following actions:
 - Select  to add a notification.
 - Select  to edit a notification.
3. Add or modify the **Email Address** for the intended recipient.
4. Sending notifications is enabled by default. Deselect **Enable** to disable the sending of notifications to the specified email address.
5. Choose from the following options:
 - To receive notifications of alerts for all alert policies, no action is required. The **Select All Policies** option is enabled by default.
 - To receive notifications of Global Policy alerts or specific Site Policy alerts, or any combination of these, enable **Select Global/Site Policies**, then select the check box associated with the target policies. To narrow the list of policies to select from, use the **Search** tool.

**Note**

A user's assigned role determines which options are available.

6. Select **Save** to commit the changes, or select **Cancel**.

Newly added and modified email addresses must undergo verification. See [Manage Notifications](#) on page 523 for details on how to initiate the verification process.

Related Links

[Alerts](#) on page 509

Add or Edit a Webhook Notification

Go to **Manage > Alerts > Alert Policy > Notifications**.

Use this task to set up Webhook notifications for alerts.

**Note**

Webhook notification is temporarily disabled if three consecutive notifications fail to reach the configured Webhook endpoint. ExtremeCloud IQ stops sending notifications for 10 minutes, then retries sending. This process is repeated until the notifications can be sent to this endpoint again. Any alerts raised during the 10 minute pause window are not sent.

1. Select **Manage Webhooks**.

2. Choose from the following actions:
 - Select  to add a notification.
 - Select  to edit a notification.
3. Add or modify the **Post URL** destination for the notification.
4. Optionally, add an **Access Token**.
5. Deselect **Enable** to disable the sending of notifications to the specified Post URL. Sending notifications is enabled by default.
6. Choose from the following options:
 - To receive notifications of alerts for all alert policies, no action is required. The **Select All Policies** option is enabled by default.
 - To receive notifications of Global Policy alerts or specific Site Policy alerts, or any combination of these, enable **Select Global/Site Policies**, then select the check box associated with the target policies. To narrow the list of policies to select from, use the **Search** tool.
7. Select **Save** to commit the changes, or select **Cancel**.

Related Links

[Manage Notifications](#) on page 523

Reports

The **Reports** table shows all generated reports that you have configured. Select a report name to view details. Select the plus sign to create reports. Schedule up to 500 combined weekly and daily reports. View all of the available types of reports or select a **Report Type** from the drop-down list to see just reports of that type. Filter the reports displayed.

To access **Reports**, go to **Manage > Reports**. ExtremeCloud IQ offers the following report types:

- **Network Summary:** This report provides visibility into how the network is being used by displaying the top applications and wireless clients for a given time period.
- **PCI DSS 3.2:** ExtremeCloud IQ audits current device configuration settings, checks them against those listed in PCI DSS 3.2, and provides a list of changes that you must make to bring non-compliant devices into compliance.
- **WIPS History:** This report summarizes data collected on rogue devices over a period of time, which can help you locate and remove these devices from your network. It can also help your organization adhere to PCI DSS record keeping requirements.
- **WiFi Statistics Summary:** This report provides a list of per-session locations, sublocations, associated VLANs, device MAC addresses, client MAC addresses, session start and end times, client IP addresses, client host names, client OS names, BSSIDs, and SSIDs. Because this report is location-based, to run it, you must first assign a map location to your devices.

- **Client Tracking:** This report provides information about a client connected to your network for a time range that you specify. You can identify the client by MAC address, user name, or host name.
- **Switch Summary:** This report provides switch port summary information. The report also includes switch device name, stack unit, status, total uptime, temperature status, average CPU/memory utilization, power supply/fan stats, PoE power availability, total client count, and total unicast/multicast/broadcast values. The report provides a list of port errors, port operational status, and port TX/RX information.

Related Links

[Create a Network Summary Report](#) on page 527

[Generate a PCI DSS 3.2 Report](#) on page 528

[Generate a WIPS History Report](#) on page 528

[Generate a Wi-Fi Statistics Summary](#) on page 529

[Generate a Client Tracking Report](#) on page 529

[Generate a Switch Summary Report](#) on page 530

[Time Range for Reports](#) on page 530

Create a Network Summary Report

A Network Summary report can display a great deal of information about your network and how it is functioning. You can choose to display a number of report widgets that show top usage, top applications and application groups, top wired clients, unique clients, and more.

Use this task to configure and generate a network summary report.

1. Go to **Manage > Reports**.
2. Select the **Network Summary** tab (selected by default).
3. Select the [time range](#) options for the report.
4. Name the report.
5. Choose which data widgets appear in the report.

Display all widgets, or display them selectively. Select the check box to the left of a widget to include it, and clear the check box to exclude the widget. Many of the widgets are interactive, meaning that you can hover over them to see more information. There are two views: **Access** (the default view) and the **WAN** view.
6. Select the format for the report.
7. Select recurrence options for the report.
8. Share the report with others by entering valid email addresses in the **Share With** field.
9. Select **GENERATE REPORT**.

ExtremeCloud IQ automatically generates the report according to your instructions. You can view it on the **My Reports** page by selecting **My Reports** from the top-left corner of the page.

Related Links

[Reports](#) on page 526

Generate a PCI DSS 3.2 Report

This feature audits current device configuration settings and checks them against those listed in the Payment Card Industry Data Security Standard (PCI DSS) 3.2. The report then provides a specific list of changes that must be followed to bring non-compliant devices into compliance.

Use this task to configure and generate a PCI DSS 3.2 summary report.

1. Go to **Manage > Reports**.
2. Select the **PCI DSS 3.2** tab.
3. Name the report.
4. Select the [time range](#) options for this report.
5. Choose the widgets that you want to display in the report:
By default, the report displays the widgets.
 - To remove a widget, select  to the right of the widget name.
 - To add a widget, select  to the right of the widget name.
6. To share this report with others, enter valid email addresses in the **Share With** field.
7. Select **GENERATE REPORT**.

ExtremeCloud IQ automatically generates the report according to your instructions. You can view it on the **My Reports** page by selecting **My Reports** from the top-left corner of the page.

Related Links

[Reports](#) on page 526

Generate a WIPS History Report

A WIPS History report provides information about rogue and unauthorized devices, and the neighbor APs that reported them. This report can help you improve network security and comply with Payment Card Industry Data Security Standard (PCI DSS) intrusion detection and record-keeping requirements.

Use this task to configure and generate a WIPS History report.

1. Go to **Manage > Reports**.
2. Select the **WIPS HISTORY** tab.
3. Select [time range](#) options for this report.
4. Name the report.
5. Choose the widgets that you want to display.
The report displays the widgets by default.
 - To delete a widget, select  to the right of the widget name.
 - To add a widget, select  to the right of the widget name.

6. Select the recurrence options for the report.
7. Share the report with others by entering valid email addresses in the **Share With** field.
8. Select **GENERATE REPORT**.

ExtremeCloud IQ automatically generates the report according to your instructions. You can view it on the **My Reports** page by selecting **My Reports** from the top-left corner of the page.

Related Links

[Reports](#) on page 526

Generate a Wi-Fi Statistics Summary

The Wi-Fi Statistics Summary provides information about your wireless clients and their connections, availability through your APs, and other wireless details.

1. Go to **Manage > Reports**.
2. Select the **WiFi STATISTICS SUMMARY** tab.
3. Enter a **Name** for the report.
4. Select the [time range](#) options for this report.
5. Share this report with others by entering valid email addresses in the **Share With** field.
6. Select **GENERATE REPORT**.

ExtremeCloud IQ automatically generates the report according to your instructions. You can view it on the **My Reports** page by selecting **My Reports** from the top-left corner of the page.

Related Links

[Reports](#) on page 526

Generate a Client Tracking Report

The Client Tracking report shows information about a client connected to your network for a time range that you specify. You can identify the client by MAC address, user name, or host name.

Use this task to configure a Client Tracking report.

1. Go to **Manage > Reports**.
2. Select the **CLIENT TRACKING** tab.
3. Select the [time range](#) options for this report.
4. Name the report.
5. Select a **Device Identifier** for the client, and then type the MAC address, user name, or host name.
6. Choose a file format for the data.
7. To share this report with others, enter valid email addresses in the **Share With** field.
8. Select **GENERATE REPORT**.

ExtremeCloud IQ automatically generates the report according to your instructions. You can view it on the **My Reports** page by selecting **My Reports** from the top-left corner of the page.

Related Links

[Reports](#) on page 526

Generate a Switch Summary Report

A Switch Summary Report displays information about your switches. You can choose to display a number of report widgets that show switch ports errors, switch ports status reports, and switch ports TX/RX Bps reports.

Use this task to configure and generate a Switch Summary Report.

1. Go to **Manage > Reports**.
2. Select the **SWITCH SUMMARY REPORT** tab (selected by default).
3. Select the [time range](#) options for the report.
4. Name the report.
5. Choose the widgets that you want to display.
The report displays the widgets by default.
 - To delete a widget, select **X** to the right of the widget name.
 - To add a widget, select **+** to the right of the widget name.
6. Select the format for the report.
7. Select recurrence options for the report.
8. Share the report with others by entering valid email addresses in the **Share With** field.
9. Select **GENERATE REPORT**.

ExtremeCloud IQ automatically generates the report according to your instructions. You can view it on the **My Reports** page by selecting **My Reports** from the top-left corner of the page.

Related Links

[Reports](#) on page 526

Time Range for Reports



CREATE REPORT Time Range: Day ▼ 1 Hour 2 Hours 4 Hours 8 Hours 24 Hours

Figure 23: Report Time Range

When generating reports, multiple options exist at the top of the page for you to select the time range for the desired report:

- **Time Range** drop-down menu - Select from Day, Week, or Custom.

- Selection Buttons - Provide context-sensitive options based on your selection from the **Time Range** drop-down menu.
 - Day - 1, 2, 4, 8 or 24 hours
 - Week - 1, 2, or 7 days

When you select the **Custom** option in the **Time Range** drop-down menu a calendar opens on the screen.

The screenshot shows a 'Time Range Calendar' dialog. At the top, it displays the selected time range: 'Apr 2 | 02:00 to Apr 3 | 02:30'. Below this is a calendar for April 2024. The days of the week are labeled S, M, T, W, T, F, S. The dates 2 and 3 are highlighted with blue circles. To the right of the calendar is a vertical list of time slots from 00:00 to 03:00 in 30-minute increments. The 02:30 slot is highlighted with a blue background. At the bottom right, there is an 'OK' button.

Figure 24: Time Range Calendar

To create a custom time range, select the dates and times, broken down into 30-minute segments.

Related Links

[Reports](#) on page 526

Applications

The **Applications** and **Application Groups** windows contain status cards at the top, a filter tool at the left, and data tables in the main window. Use this window as follows:

- Select inside any status card to see more details.
- Use the **Filter** tool to filter the display of application data. You can create and save filters for later use.
- The Applications and Application Groups tables display information about the applications that are most active in your network.

- Select to display the **Top 20** or **Top 100** applications or groups. Most of the columns in this table can be sorted using up and down arrows. The following information is displayed:
 - **Application:** The name of the application or group.
 - **Data Usage (% used):** The percentage of bandwidth used by the application (in GB, MB, or Kbps).
 - **# Clients:** The number of clients that are running the application.
 - **# Users:** The number of users accessing this application:
- Select the download icon to download the table. You can save it to a location or open it in an application such as Word or Excel.
- Select the refresh icon to refresh all of the data in this window at any time.
- Select an application name or application group name in the **Applications** table to see more information, including:
 - Application name and category (application group name)
 - Data usage, unique clients, and unique user summary for the previous hour.
 - Application description, if available.
 - A usage timeline shows data for a time period which you can define using the range options above the graph.
 - Unique clients using this application, sortable by OS, SSID, or user profile.
 - Network usage for this application, sortable by OS, SSID, or user profile.
 - Top locations where the selected application is being used.
 - Top five clients by usage, including MAC address, operating system, and connection information.
 - Top five users by name, location of their most recent connection, and usage.
- Use **MANAGE APPLICATIONS** to create custom applications. For more information, see [Add a Custom Application](#) on page 533.

Related Links

[Add a Custom Application](#) on page 533

[Application Detection Rules Settings](#) on page 533

Applications List

To see a list of configured applications, go to **Manage > Applications > MANAGE APPLICATIONS**.

From this page, you can filter the list of applications any of the following ways:

- Kind
 - Application
 - Category
- Type
- Protocol

Use the search field to find a specific application in the list.

Select an application in the list:

- To edit the application, select .
- To delete an application, select .

**Note**

You cannot edit or delete system-defined applications.

Related Links

[Add a Custom Application](#) on page 533

[Add Application Sets](#) on page 288

Add a Custom Application

Use this task to create a custom application definition, including an application group, optional descriptions, and application detection rules.

1. Go to **Manage > Applications**, and then select **MANAGE APPLICATIONS**.
2. Select **ADD CUSTOM**.
3. Enter an **Application Name** for the new application.
4. Enter an optional **Description**.
5. Select an existing **Application Category** from the drop-down list, or select  to create a new one.
 - a. If you add a new group, enter a **Group Name**.
 - b. Select **Save**.
6. Select  and configure the **Application Detection Rules**.
7. To delete a rule, select the corresponding check box, and then select .
8. Select **SAVE**.

Related Links

[Application Detection Rules Settings](#) on page 533

[Add Application Sets](#) on page 288

Application Detection Rules Settings

The settings depend on the rule **Type** that you select. Choose from the following types:

- [Host Name](#)
- [Server IP Address Settings](#) on page 534
- [Port Number](#) on page 534

*Host Name***Table 127: Host Name Settings**

Setting	Description
Type	Select the type of rule: Host Name , Server IP Address , or Port Number from the menu.
Protocol	Select the protocol: HTTP or HTTPS from the menu.
Host Name	(Required) Type the host name.

*Server IP Address Settings***Table 128: Server IP Address**

Setting	Description
Type	Select the type of rule: Host Name , Server IP Address , or Port Number .
Protocol	Select the protocol: TCP or UDP from the menu.
Server IP Address	(Required) Type the IP address for the server.
Port Number	Type the port number. Range: 1-65535

*Port Number***Table 129: Port Number Settings**

Setting	Description
Type	Select the type of rule: Host Name , Server IP Address , or Port Number .
Protocol	Select the protocol: TCP or UDP from the menu.
Port	(Required) Type the port number. Range: 1-65535

Related Links

[Add a Custom Application](#) on page 533

Rogue APs

When you enable a wireless intrusion prevention system (WIPS) on your network, APs that do not comply with the WIPS are considered rogue and are listed under **Manage > Security > Rogue APs**. If an AP that does not comply with WIPS appears here, and you are sure that it is a valid device, you can remove it. You might also want to reconfigure the WIPS policy settings.

A graph displays a colored timeline representing data captured for rogue APs within the specified time frame. You can change the time frame using the **Time Range** controls. For more information, see [Set the Time Frame for Captured Data Displays and Reports](#) on page 551. Details about the data captured within this time frame are listed in the table below the graph.

View the table as follows:

- Above the table are three viewing options with check boxes:
 - **Rogue:** An unauthorized AP that is connected to your wired network.
 - **Unauthorized:** Any unauthorized AP that is detected, but not necessarily connected to your wired network.
 - **Neighbor:** APs that you have manually classified as neighbors and that do not represent a threat.
- In the table, select and drag the right edge of any column to change the column width. Some columns can also be sorted. Select the column heading to sort column entries.
- The table displays all of the rogue APs that have been detected in your network. You can also choose to show **In-net** rogues, **Unauthorized** rogues, or **Neighbor** rogues that are not a threat.
- If a detected rogue AP is determined to be in the same backhaul network as compliant APs, ExtremeCloud IQ displays **In-net**. If the location of the AP in the network cannot be determined, a dash is displayed. Knowing whether a rogue AP is in the same network can help you decide how swiftly you need to respond to its presence.

By default, the table displays the following information:

- **Classification:** Whether this AP is considered a true rogue or a neighbor AP.
- **Clients:** Shows the number of clients associated with this AP.
- **Rogue AP BSSID:** The BSSID (basic service set identifier, which includes the MAC address) of the rogue AP.
- **SSID:** The SSID that is being announced by the rogue AP beacons.
- **Vendor:** The vendor of the rogue AP, Apple, for example.
- **Approximate Location:** The location of the rogue AP in your network, or the location of the AP that reported the rogue.
- **Reporting Device:** The authorized device in your network that reported the rogue AP.
- **Reason:** The reason the AP has been designated as a rogue. APs can check whether the SSID names and types of encryption other access points advertise match those in a checklist. For example, if your network security policy requires all SSIDs to use WPA or WPA2, any SSID using WPA or WPA2 makes the AP hosting it valid. An AP is categorized as rogue if it hosts an SSID using WEP or no encryption at all (open).
- **First Time Detected:** The first time this AP was detected in your network.
- **Last Time Detected:** The last time this AP was detected in your network.
- **Mitigation:** Displays whether mitigation has been taken against this AP.

Classify Rogue APs

You can change the classification for the rogue APs displayed in this table. Select the check box for an AP and then select **Classify**. Then select one of the following options:

- **Neighbor:** Reclassifies this device as an AP that does not present a threat to your network.
- **Auto-classify:** (For previously manually-classified APs). Use this option to return an AP to the default classification it had when first detected.

Mitigate Rogue APs

You can configure your WIPS policy to mitigate rogue APs manually or automatically. For more information about how to configure mitigation, see [WIPS Policy Settings](#) on page 309.

Related Links

[Set the Time Frame for Captured Data Displays and Reports](#) on page 551

[WIPS Policy Settings](#) on page 309

Rogue Clients

Under **Manage > Security > Rogue Clients**, a table displays details for devices that are enabled with a wireless intrusion prevention system (WIPS) configuration that includes ad hoc network settings. These devices detect wireless clients participating in an ad hoc network.



Note

An ad hoc network (also referred to as an IBSS, or independent basis service set) consists of two or more wireless clients that communicate with each other directly instead of through an access point.

Devices can only detect rogue clients in an ad hoc network if the client uses the same channel as the device access radio, and if the device has background scanning enabled on that radio. View the table as follows:

A graph displays a colored timeline representing data captured for rogue clients within the specified time frame. You can change the time frame using the **Time Range** controls. For more information, see [Set the Time Frame for Captured Data Displays and Reports](#) on page 551. Details about the data captured within this time frame are listed in the table below the graph.

The Rogue Clients table displays all of the rogue clients that have been detected in your network. Select the **Rogue** check box to list in-net rogues. Select the **Unauthorized** check box to list unauthorized rogues, or the rogues that have been removed from your network.

The table has variable-width columns to display longer entries. Select and drag the right edge of any column left or right to change the column width. Some columns

are sortable; select the column heading to sort column entries. By default, this table displays the following information:

- **MAC Address:** The MAC address of the rogue client.
- **Vendor:** The client vendor.
- **Classification:** Whether the client is considered a true rogue, or a neighbor.
- **SSID:** The SSID that is being announced by the client beacons.
- **Approximate Location:** The location of the client or reporting AP in your network.
- **Device Name:** The authorized device that reported the rogue client.
- **First Time Detected :** The first time the client was detected in your network.
- **Last Time Detected:** The last time the client was detected in your network.

Classify Rogue Clients

To classify rogue clients, select the check box for the client and then select **Classify**. From the drop-down list, select **Neighbor**, **Removed**, or **Auto-classify**.

Related Links

[Set the Time Frame for Captured Data Displays and Reports](#) on page 551

About Client Monitor

The client monitor tool helps identify and troubleshoot issues clients typically encounter when associating with an AP, authenticating, and accessing the network.

The **Issue List** window provides a list of all the issues that wireless clients face within the time frame defined in the graph at the top of the window, and the issue type and issue status filters also defined at the top of the table. For each issue, the table shows the following details:

- Client host name and MAC address
- Issue type and summary
- User profile applied to the client
- Host name of the Extreme Networks device with which the client connected
- Client location on a topology map
- Timestamp when the issue was detected



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

You can search for a particular client host name or MAC address by entering a full or partial text string. You can also use the **Filter Toggle** on the left side of the screen to filter the lists by device and location.

Issue cards below the **Unique Clients experiencing issues** header provide a high-level view of the type and number of issues wireless clients are experiencing during the period defined in the timeline. At a glance, you can see how many issues clients are having in the areas of **Association**, **Authentication**, and **Networking**.

Related Links

[Search for Clients](#) on page 538

[About the Issue List Table](#) on page 538

[Troubleshoot an Issue](#) on page 539

[Take Action for a Client Issue](#) on page 539

[Download Issue Lists](#) on page 540

[Set the Time Frame for Captured Data Displays and Reports](#) on page 551

Search for Clients

Open a **Client Monitor** window.

You can search for clients by entering a client host name or MAC address in the search field at the top of the **Issue List**.

1. Enter a client host name or MAC address.
2. Select the name or address from the drop-down list.
3. Select the Search icon.

About the Issue List Table

The **Issue List** table lists issues clients experienced or are still experiencing, along with details that help identify the issue location. From this list, you can select issues for troubleshooting. The **Issue List** table consists of the following columns:

- **Status:** One of three icons display:
 - A red exclamation point - indicates an active issue
 - A green check mark - indicates an issue an admin manually marked as resolved
 - A maroon Up escalator icon - indicates an admin manually escalated the issue
- **Client Host Name:** The client-assigned host name. If the host name is not available, nothing displays.
- **Client MAC:** The MAC address of the wireless client.
- **Issue Type:** An issue classification. It can be Association, Authentication, Networking (DHCP or DNS server), or Unknown. Additional sub-categories are available when you select **Association**, **Authentication**, and **Networking** from the drop-down list. The Summary column displays the specific sub-category issue type for each client issue detected.
- **Summary:** The sub-category for each client issue detected.

- **User Profile:** The user profile applied to the client. If no user profile is applied, nothing displays.
- **Extreme Networks Device:** The Extreme Networks access point's host name associated with the client.
- **Location:** The device location on a topology map.
- **Detected On:** The month, day, and time-of-day the access point detected the issue.

**Note**

To display issues that involve a real-time troubleshooting session initiated by an admin, select **Show User Sessions**. Troubleshooting sessions are indicated by **USER** next to the **Status Icon**.

Troubleshoot an Issue

Go to **Manage > Client Monitor & Diagnosis**.

Use this task to troubleshoot issues listed under the **Client Monitor** tab.

1. Select an issue and **Troubleshoot Selected**.
2. Enter the following information:
 - **Selected Client:** Contains your selected client name.
 - **Troubleshooting Duration:** Select a troubleshooting length of time.
 - **Access Points:** Select the APs to troubleshoot.
3. Filter the list to show APs by location, model, connection status.
 - **Location:** Troubleshoot APs by location.
 - **Model:** Filter APs by model using the drop-down, or choose **All**.
 - **Status:** Filter APs by their connection status or select **All**.
4. Select **Start**.

Take Action for a Client Issue

Open a **Client Monitor** window.

You can act on client issues by escalating them, resolving them, commenting on them, and notifying other administrators about them through email.

1. Select an issue and **Take Action**.
2. Complete the following fields:
 - **Action:** Change the issue status to **Resolved** or **Escalate**.

**Note**

After an issue is marked Resolved, you cannot take further action.

- **Comments:** Add a message describing the issue. This might be a note for yourself or—if you send an email about this to other administrators—to one or more email recipients.
- **Email:** Select the check box and enter one or more email addresses, separating multiple addresses with semicolons.

3. Select **Save**.

The following actions occur:

- The Active icon changes to Resolved or Escalated in the **Issue List Status** column.
- If you entered email addresses, emails are sent to the designated recipients.

Download Issue Lists

Open a **Client Monitor** window by navigating to **Manage > Client Monitor & Diagnoses > Client Monitor**.

You can download the **Issue List**, filtering it first to focus on certain issue types. For example, you might download only unresolved issues for tracking purposes, escalated issues for a team meeting, or resolved issues to include in a report.

1. Select **Download**.
2. Save the file to a local directory.

About Diagnosis

This window provides detailed information about a selected issue or issues associated with a client host name (or MAC address), in the form of a timeline and card.

Timeline

A timeline displays issue detection in a graph. It is useful to see multiple occurrences of the same issue. Each occurrence is represented by a bubble and a flag with a number. Hover your mouse over a bubble to display the month, day, and time-of-day an issue occurred, as well as the issue type: **Association**, **Authentication**, **Networking** (DNS or DHCP server issues), or **Unknown**. The flag shows the number of occurrences of the issue at the time.

Card

Underneath the timeline, the **Diagnosis** card contains data that can help you understand the issue, such as when problems were detected, the location of the connected AP, a description of the issue, and a suggested remedy.

- **AH Device:** The host name of the Extreme Networks device.
- **User:** The name of the user, if known.
- **Location:** The location of the Extreme Networks device.
- **User Profile:** The user profiles assigned to this device.
- **Client MAC:** The MAC address of the wireless client device.
- **Case Number:** A case number for your use. (This number is not linked to Extreme Networks Support.) Select **Assign** to access a dialog box. Enter a case number, and then select **Submit**. The number you entered displays here.
- **Problem Type:** Indicates if the issue was auto-generated by the client or initiated by an admin while troubleshooting the issue.
- **Detected On:** The month, day, year, and time-of-day the issue was first detected.

- **Description:** A detailed description of the issue, such as External RADIUS server could not accept the access request from the client Or DHCP server did not respond to the client.
- If Dynamic Packet Capture has been recorded, it will be appended here. Select **Download Client Trace Support Bundle** to download and view it using your preferred protocol analyzer tool.
- **Last Successful Connection:** The month, day, year, and time-of-day the wireless client last connected successfully to the Extreme Networks device.
- **Suggested Remedy:** A solution to the issue, such as Check RADIUS server log files and verify the authenticating user's credentials Or Ensure DHCP server is properly configured, reachable, and that it has enough leases available.

Events Associated with an Issue

If there are events associated with an issue, the total number of events displays, followed by a timeline that highlights events, and an information card below the timeline that describes each event. Below the card is a table populated with a description of the associated events, such as when a configuration was pushed to a device. (If no events are associated with an issue, the table is empty.) This table provides the following information:

- **Show Phases:** Select **All**, **Association**, **Authentication**, or **IP Assignment** phases from this drop-down menu. Select **Show Probe Requests** to display all probe requests related to this incident.
- **Time Stamp:** The month, day, year, and time-of-day the event occurred.
- **Device Name:** The Extreme Networks device name. By default, the Extreme Networks device name is the host name. If the host name is not available, the device name is the IP address. If the IP address is not available, the device name is the MAC address.
- **Device BSSID:** The AP wireless access interface MAC address.
- **Event Type:** The classification of the event, such as **Auto provisioning**, **Connection Change**, or **Power Mode Change**.
- **Description:** A description of the event, such as Station sent out DHCP REQUEST message.

You can share information about issues with colleagues, escalate issues, or mark them as resolved by selecting **Take Action**. For more information, see [Take Action for a Client Issue](#) on page 539.

Email Notification on Change of Status

To send an email indicating the status of an issue has changed, see [Perform a Change Status Email Notification](#) on page 542.

Perform a Change Status Email Notification

Run **Diagnosis** under **Manage > Tools**.

Use this task to send an email notification when the status of an issue changes.

1. Select the check box next to one or more issues.
2. Select **Take Action**.
3. Fill in the fields as follows:
 - **Action:** The issue status.
 - **Comment:** Add an issue description.
 - **Email:** Select the check box next to this field and supply an email address to enable ExtremeCloud IQ to automatically send an email indicating the status change.

After you mark an issue as resolved, the status icon changes from a red active issue icon to a green resolved check mark on the **Issue List** table. After you mark an issue as resolved, you cannot take further action.



Note

The email notification is for your internal company use. It does not notify Extreme Networks Technical Support.

Packet Capture

Packet Capture is a process by which data packets are intercepted and recorded. Packet Capture operations reveal network performance and integrity issues such as congestion, packet loss, and security threats. Packet Capture results are stored in PCAP files that can be analyzed to obtain information required to address the issues revealed during packet capture operations.



Note

ExtremeCloud IQ stores PCAP files for 14 days. To retain PCAP files longer than 14 days, either download them to local storage or upload them to CloudShark. Uploading files to CloudShark requires an existing account.

ExtremeCloud IQ supports basic Packet Capture and Enhanced Packet Capture capabilities, as follows:

- All APs running IQ Engine OS support basic Packet Capture capabilities, which include:
 - View which packet capture operations are still in progress, and stop a packet capture session, if desired.
 - View all packet captures belonging to the same packet capture session grouped together.
 - Download PCAP files to a desktop PC or laptop.
 - Download PCAP files for each interface involved in a packet capture session, as well as files for the entire session combined.

- AP5010/AP3000/AP3000X models hosting IQ Engine 10.6.4 or higher support basic Packet Capture capabilities as well as Enhanced Packet Capture capabilities. AP4020 models hosting IQ Engine or higher support basic Packet Capture capabilities as well as Enhanced Packet Capture capabilities. Capabilities include:
 - Set various filters to narrow the focus of the packet capture operation.
 - Capture wired and wireless packets simultaneously or independently.
 - If a client is specified, a user can:
 - Select all APs in the same location.
 - Select APs where the client has roamed over the previous 7 days.

Consider the following:

- Packet Capture is not supported on simulated devices.
- A device can participate in only one packet capture session at a time. However, multiple interfaces on the same device may participate in the same packet capture session.
- Each ExtremeCloud IQ license supports a maximum of 10 simultaneous packet capture sessions.
- When capturing data packets from a location, it is recommended that a MAC address filter be specified.
- If a client is specified only one MAC address filter can be used.
- After a packet capture starts, packet capture settings cannot be modified.

Related Links

[Manage Packet Capture Sessions](#) on page 543

[Add and Start a Packet Capture Session](#) on page 546

Manage Packet Capture Sessions

Go to **Manage > Client Monitor & Diagnosis > Packet Capture**.

The **Packet Capture** tab includes:

- A list of Packet Capture sessions.
- Management tools that allow users to perform Packet Capture operations.

Packet Capture is a client monitoring feature where administrator, operator, and help desk roles have full-access. Monitor roles have read-only access to monitoring.

View Packet Capture Sessions

By default, the **Packet Capture** tab displays a list of **all** sessions in tabular form.

Table 130 describes the type of information displayed under each column and any actions that a user can employ.

Table 130: Packet Capture List Column Headings

Column Heading	Description
Status	Indicates the operational status of sessions: • In-progress - grey bead  • Successfully completed - green bead  • Partially completed - yellow bead  • Failed - red bead  Note: Hover over the red bead to view the failure reason description.
Session Name	Displays the name that ExtremeCloud IQ automatically assigns to the session when it starts. The name includes the session start time.
Host Name	Displays the Host Name of the AP targeted for Packet Capture operations.
Interface	Identifies the AP's interface(s) targeted for Packet Capture operations.
Location	Identifies the location of the AP (city, building address, floor number).
Start Time	Displays the time when the session started.

Table 130: Packet Capture List Column Headings (continued)

Column Heading	Description
End Time	Displays the time when the session ended.
Download	This field provides links to PCAP files generated for individual interfaces on an AP that is targeted in a Packet Capture session. The files are uploaded to ExtremeCloud IQ and, if Upload to CloudShark is enabled, the files are uploaded there too. Possible links in this field include the following: • If Upload to CloudShark is enabled, a link to the PCAP file on CloudShark displays. • If Upload to CloudShark is disabled, a link to the PCAP file stored in ExtremeCloud IQ displays. • If the user selects the check box associated with a Packet Capture session and then selects , the system displays a link to a tar file containing all the individual PCAP files generated for a session and uploaded to ExtremeCloud IQ. Links to PCAP files are also provided through the Read Only view of the Packet Capture session configuration. Select a Packet Capture session in the list, then select  to access the links. Note: If the uploading of PCAP files from the AP to ExtremeCloud IQ fails, select  to retry the upload.

To narrow the list of sessions displayed:

- Search for specific sessions. Enter a Session Name, Host Name, or an Interface type in the **Search** field, then select refresh .
- Delete sessions for which PCAP files have been downloaded and stored or uploaded to CloudShark. Select a session, then select . Only one session can be deleted at a time.

To view the settings for a Packet Capture session, select the session in the list, then select .

Add and Stop a Packet Capture Session

Select  to add a **New Packet Capture** session.

Select  to stop a Packet Capture session that is in progress.

Related Links

[Packet Capture](#) on page 542

[Add and Start a Packet Capture Session](#) on page 546

Add and Start a Packet Capture Session

Go to any of the following user interfaces:

- **Manage > Devices** *<select an IQ Engine AP>* **Utilities > Tools > Packet Capture**
- **Manage > Client Monitor & Diagnosis > Packet Capture**
- **ML Insights > Client 360** *<optionally, select an active client>* **Utility > Packet Capture**



Note

If a packet capture is initiated through **Client 360** and an active client is selected, when the **New Packet Capture** window opens, the client's MAC address is prefilled in the **Clients** field, and the client's associated AP is preselected. Add other APs to the packet capture, as required.

Use this procedure to configure Packet Capture parameters and start a Packet Capture session.



Note

After a session starts, package capture parameters cannot be modified.

1. Select  to add a new Packet Capture session.
2. Select one or more target APs from the list. Optionally, narrow the list of APs displayed in the list using the **Location** filter or **Search** field.
3. Configure the Packet Capture settings.
 - For AP5010, AP3000/AP3000X, and AP4020 models, see [Table 131](#) on page 546.
 - For all other IQ Engine APs, see [Table 132](#) on page 550.



Note

If the target APs selected in step 2 include model types that support Enhanced Packet Capture and other model types that support basic Packet Capture, only the [basic Packet Capture](#) parameters are available for configuration.

Table 131: Enhanced Packet Capture Settings

Parameter	Description
Filter Settings	
Direction	Filters packet capture on the basis of the direction of packet flow. Options are: • Both — Capture packets transmitted and received by the AP. This is the default value. • In — Capture packets received by the AP. • Out — Capture packets transmitted by the AP.

Table 131: Enhanced Packet Capture Settings (continued)

Parameter	Description
Clients	Filters packet capture on the basis of packets received from and transmitted to clients associated with the selected AP. Options are: • All — Capture packets from all clients. This is the default value. • Enter the MAC address of a specific client. • Initiate packet capture through ML Insights > Client 360 with an Active client selected, and the client's MAC address automatically appears in this field.
Where has the client recently roamed?	Provides the option to add to the Packet Capture session any APs involved in client roaming over the previous seven days. Select Update Selected APs. In the Select APs from Client Trail pop-up window, select one or more APs, then select OK.
VLANs	Filters packet capture on the basis of packet transmission over specific VLANs. Enter an individual VLAN ID or a range of VLAN IDs. Indicate a range with a hyphen. Separate VLAN entries with commas. Example: 2,4,5-10.
Protocol	Filters packet capture on the basis of protocol. Choose from the following options: • Any (default) • User defined Enter a value in the range of 0-255 representing the IP Protocol number in the <i>Protocol</i> field of an IPv4 header or the <i>Next Header</i> field of an IPv6 header. See IP Protocol Numbers for more information. • ICMP • ICMPv6 • TCP • UDP • GRE • IPSec ESP • IPSec AH
Wireless	

Table 131: Enhanced Packet Capture Settings (continued)

Parameter	Description
Band	Filters packet capture on the basis of radio band. Select Band, then use the drop-down list to choose from of the following options: • All • 2.4 GHz • 5 GHz • 6 GHz Note: ExtremeCloud IQ automatically discovers the radio interface(s) on the target AP that support the selected radio band(s). If there is no radio on the AP to support the configured band, the packet capture session fails.
Interface	Filters packet capture on the basis of radio interface. Select Interface, then use the drop-down list to choose from of the following options: • All (default): All available interfaces. • WiFi0: AP's primary Wi-Fi radio. • WiFi1: AP's secondary Wi-Fi radio. • WiFi2: AP's third Wi-Fi radio. Note: AP3000/AP3000X do not support WiFi2. If target APs include AP3000/AP3000X and model types that do support WiFi2, then the WiFi2 option is available. However, the capture result for the AP3000/AP3000X Wi-Fi 2 interface fails. • IoT: Capture packets from the AP's IoT radio interface. Note: The IoT option is only available on AP5010/U models with an IoT profile installed.
WLANs	Filters packet capture on the basis of the traffic over WLAN(s). Use the drop-down list to choose from of the following options: • Select Any to capture packets transmitted over any WLAN. • Select a pre-configured Broadcast Name associated with a Wireless Network SSID to capture packets from the specified WLAN.

Table 131: Enhanced Packet Capture Settings (continued)

Parameter	Description
Filters	Filters packet capture on the basis of network traffic functions. Select one or more of the following options: • Management • Control • Data • EAPOL • Beacons • Probes
Wired	
Interface	Filters packet capture on the basis of Ethernet port. Use the drop-down list to choose either: • eth0 (default) • eth1 • All — At least one wired interface on each target AP must be enabled. Note: If a target AP has a disabled Ethernet port that is specified here, the packet capture for the interface fails.
Filters	Filters packet capture on the basis of protocol. Select one or more of the following options: • DHCP • Radius • LLDP • ARP • mDNS
Capture Settings	
Duration	Indicates the period of time after Start Capture is selected during which packets are captured. This option is enabled by default. Options are: • Enter a value in the range of 5-604800 seconds. The default value is 30 seconds. The capture operation continues until the specified duration has elapsed or until the maximum allowable size of captured packet data files for the platform is reached. • Deselect Duration to capture packets for an unspecified period of time. The capture operation continues until the maximum allowable size of captured packet data files for the platform is reached.

Table 131: Enhanced Packet Capture Settings (continued)

Parameter	Description
Upload to CloudShark	Indicates whether tar files containing PCAP files from packet capture operations on individual interfaces are uploaded to CloudShark. This option is enabled by default. Note: Uploading files to CloudShark requires an existing account.
CloudShark API Token	Specifies the API access token. Enter a value consisting of 32 hex characters (0-9, a-f).

Table 132: Basic Packet Capture Settings

Parameter	Description
Wireless	
Interface	Filters packet capture on the basis of radio interface. All (default): All available interfaces. WiFi0: AP's primary Wi-Fi radio. WiFi1: AP's secondary Wi-Fi radio. WiFi2: AP's third Wi-Fi radio. Note: AP3000/AP3000X do not support WiFi2.
Capture Settings	
Duration	Indicates the period of time after Start Capture is selected during which packets are captured. This option is enabled by default. Options are: - Enter a value in the range of 5-604800 seconds. The default value is 30 seconds. The capture operation continues until the specified duration has elapsed or until a maximum of 100000 packets are captured. - Deselect Duration to capture packets for an unspecified period of time. The capture operation continues until a maximum of 100000 packets are captured.
Upload to CloudShark	Indicates whether tar files containing PCAP files from packet capture operations on individual interfaces are uploaded to CloudShark. This option is enabled by default. Note: Uploading files to CloudShark requires an existing account.
CloudShark API Token	Specifies the API access token. Enter a value consisting of 32 hex characters (0-9, a-f).

4. Select **Start Capture**.

5. After the configured packet capture session **Duration** has elapsed, select  to refresh the capture session list and view the results of the latest session.

Related Links

- [Packet Capture](#) on page 542
[Manage Packet Capture Sessions](#) on page 543
[About Client 360](#) on page 564

VPN Management

The **VPN Management** window displays VPN management data for your network. VPNs are identified by branch ID, location, the router or WAN, the VPN gateway, status, availability, and usage data, and keys. You can revoke or refresh VPN keys here.

1. Select a VPN from the list.
2. Select an option from the **Manage Keys** drop-down list.

Set the Time Frame for Captured Data Displays and Reports

Navigate to any of the following ExtremeCloud IQ pages:

- **Manage > Summary**
- **Manage > Devices >**
 - **<switch> Hostname > Monitoring > Monitor >**
 - **Overview**
 - **Clients**
 - **Diagnostics**
 - **Alarms > Timeline View**
 - **<access point> Hostname > Monitoring > Monitor >**
 - **Overview**
 - **Wireless Interfaces**
 - **Wired Interfaces**
 - **Clients**
 - **Alarms > Timeline View**
- **Manage > Users > Historical**
- **Manage > Reports > Network Summary** or **Client Tracking**
- **Manage > Security**
- **Manage > Client Monitor & Diagnosis > Client Monitor**
- **ML Insights > Network 360 Monitor** or **Client 360 > Inactive**

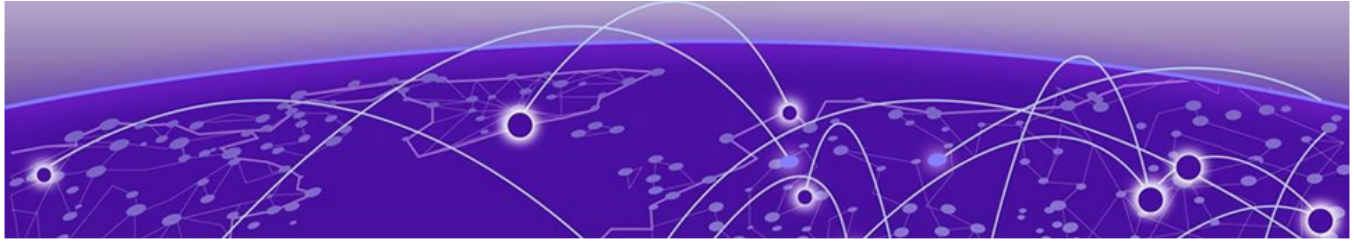
By default, ExtremeCloud IQ presents data captured for a 24-hour time frame, with hourly updates. In most cases, a graph with a colored timeline displays the captured data. The color key for timelines and the type of data captured on a timeline appears above the right-hand side of the time frame. In some cases, ExtremeCloud IQ presents data in other formats, such as reports or other types of graphical representations.

Use this procedure to set the time frame for reports containing captured data for various network operations and events.

1. From the **Time Range** drop-down menu, choose one of the following options:
 - Select **Day** to see the captured data in on an hourly basis. Select an interval of either 1, 2, 4, 8, or 24 hours to narrow the data capture time frame.
 - Select **Week** to see the captured data on a daily basis. Select an interval of either 1, 2, or 7 days to narrow the data capture time frame.
 - Select **Month** to see the data on a weekly or monthly basis. Select an interval of either 7, 14, or 30 days to narrow the data capture time frame.
 - Select **Custom** to open the **Calendar** and set a start date and time, then an end date and time, not exceeding a 30-day time period. Select **OK**.
2. Narrow the time frame using one of the following methods. The specific method available depends on the UI.
 - Select a point inside the graph and drag left or right to define a time frame. The adjusted time frame appears in grey in the graph.
 - Customize the time frame by dragging the left or right slider. Move the time frame as a block to a different part of the timeline by selecting a point within the shaded block.
3. To customize the view for graphs that display data on a timeline, do the following:
 - Select the timeline to view data for a 30 minute period along the timeline. The adjusted time frame appears grey in the graph.
 - Select a point on the timeline to view data captured at a precise time.
4. To reset a narrowed time frame, select either **Clear Selection** (where available), one of the interval controls, or an option from the **Time Range** drop-down menu.
5. Select the **Chart context menu**  to download the graph in your preferred format.

Related Links

[Summary](#) on page 378
[Device Details Monitor Functions](#) on page 455
[Create a Network Summary Report](#) on page 527
[Generate a Client Tracking Report](#) on page 529
[View Connected Users](#) on page 507
[Manage Active Alarms](#) on page 495
[Rogue APs](#) on page 534
[Rogue Clients](#) on page 536
[About Client Monitor](#) on page 537
[About Diagnosis](#) on page 540
[Network 360 Monitor Overview](#) on page 553
[About Client 360](#) on page 564



ML Insights

[Network 360 Monitor Overview](#) on page 553

[Network Scorecard](#) on page 558

[About Client 360](#) on page 564

[Thread Monitoring](#) on page 574

Use machine learning (ML) to monitor network health, clients, devices, wireless, and services, as follows:

- **Network 360 Monitor:** View detailed network health information.
- **Network Scorecard:** View at-a-glance network health information.
- **Client 360:** View and sort client objects, including IoT clients, plus historical and real-time client data.
- **Thread Monitoring:** View detailed thread network information.

Network 360 Monitor Overview

The first time you open this window you are directed to create a network hierarchy. You can either import an existing hierarchy or create a new one from the **Manage > Planning** window. (See [Planning](#) on page 401). After you have created and populated your network, select a location, building, or floor from the list to the left of the map to see data. To see health data for your entire network, select **Global View**. Use the following tools to navigate the window.

- **Where's My Data?:** Because data is collected on an hourly basis, this window might be empty for up to one hour.
- **Search Maps:** For large networks with multiple locations, enter the first few characters of the location name in the type-ahead field to automatically bring up matching items. As you enter more characters, the search results become more precise.
- **Filter:** Use to manage the data that is displayed. When a filter is applied, the filter icon contains a circle in the lower right corner.

Related Links

[Set the Time Frame for Captured Data Displays and Reports](#) on page 551

[Status Cards](#) on page 554

[Device View](#) on page 555

[Zone View](#) on page 556

[Import a Map](#) on page 405
[Add a Site](#) on page 404
[Add a Building](#) on page 405
[Topology Tab](#) on page 556
[Map Tab](#) on page 557
[Network Scorecard](#) on page 558
[About Client 360](#) on page 564

Status Cards

Status cards across the top of the window display information about your network health. When you select a network location, the status card data automatically changes to match your selection. Network health is determined by several factors, including availability, number of reboots, average CPU and memory usage, and average power consumption, indicated by color. Green indicates excellent network health, with scores between 80 and 100. Yellow indicates good network health, with scores between 50 and 79. Red indicates poor network health, with scores between 0-50.

Select anywhere inside a status card to see additional details. From inside the detail panels, you can navigate directly to another status card, refresh data, customize the time frame of the captured data display, print the details on the timeline within the specified time frame, or download the data as a .png, .svg, .jpg, or PDF file. Many of the following data widgets are interactive and let you drill deeper for additional information:

- **Device Health:** The Devices Health timeline displays information about usage, clients, and health. Device widgets display device health, current availability, hardware health, active alarms, top device uptime, configuration and firmware status, channel change events, DFS events, reboots and more. Many sections of the widgets are interactive. For example, if there is a caret icon at the bottom of a widget, you can expand it for more information.
- **Client Health:** Displays overall and wireless health scores, bandwidth usage, issues, channel distribution, supported spatial streams, maximum client capability in the 2.4, 5 and 6 GHz bands, association and probe requests, 802.1x technology, transmit power, and more.

The **Overall Score** is calculated by dividing the sum of the **Client WiFi Experience**, **Client IP Network Experience**, and **Client Application Experience** health scores by three ($(\text{overallWiFiHealthScore} + \text{overallNetworkHealthScore} + \text{overallApplicationHealthScore}) / 3$).

- **WiFi Health:** Displays usage, clients, and the overall Wi-Fi score over time. Widgets display wireless health details, association per radio score, channel utilization, the SNR score, data rates, and retries, and more.
- **Network Health:** Displays network health and usage. Widgets display the overall network health score, WAN, VPN, and gateway Internet availability and latency, multicast and unicast detection, Ethernet interface modes, and more.
- **Services Health:** Displays DHCP, DNS, and RADIUS activity. Widgets display the overall health score, network and authentication services scores, DHCP DNS and

NTP availability, authentication, management, and network service availability, and more.

- **Application Health:** Displays the top applications active in your wireless network. Three applications are shown by default, but you can add an application by typing the first few letters in the type-ahead search field, and then selecting the full name when it displays. To delete an application, select the **X** in the check box next to the application name. Charts and widgets display total usage, top 5 applications, and a table showing the top 20 or top 100 active application groups. You can change the number of applications displayed per window on the lower left, and scroll through the windows on the lower right.
- **Security Health:** Displays network activity involving rogue clients, rogue APs, and traffic violations. Charts and widgets display a security overview, detected Layer 2 DOS (Denial of Service) attempts, rogue APs, and traffic violations.



Note

To see Layer 2 DOS information, you must enable this feature in **SSID Additional Settings Optional Settings**. See [Customize Wireless Network Optional Settings](#) on page 162.

Related Links

[Network 360 Monitor Overview](#) on page 553

[Device View](#) on page 555

[Zone View](#) on page 556

[Import a Map](#) on page 405

[Add a Site](#) on page 404

[Add a Building](#) on page 405

[Topology Tab](#) on page 556

[Map Tab](#) on page 557

Device View

The **Network 360 Monitor Device** view displays your network hierarchy, shown in outline form in the left navigation bar, with maps that correspond to each network location. The following viewing options are available:

- **Show Devices:** View all network devices on a floor, or select a specific device from the drop-down list.
- **Time Lapse:** Create a graphical representation of heat map changes due to client activity over a period of time. Select devices, a time period, and a speed from the drop-down lists. The **Connected Clients** option displays a heat bloom for APs where clients are connected, along with the number of connected clients.

Related Links

[Network 360 Monitor Overview](#) on page 553

[Status Cards](#) on page 554

[Zone View](#) on page 556

[Import a Map](#) on page 405

[Add a Site](#) on page 404

[Add a Building](#) on page 405

[Map Tab](#) on page 557

[Topology Tab](#) on page 556

Zone View

The **Network 360 Monitor Zone** view displays your network hierarchy in outline form in the left navigation bar, with your network zones shown on the map. The following viewing options are available:

- **Show Devices:** View all zones or select a zone from the drop-down to see how many clients are connected to the AP that controls that zone.
- **Time Lapse:** Create a display of heat map changes due to client activity over a period of time. Select devices, a time period, and a speed from the drop-down lists. The **Connected Clients** option displays a heat bloom for APs where clients are connected, along with the number of connected clients.

Related Links

[Network 360 Monitor Overview](#) on page 553

[Status Cards](#) on page 554

[Device View](#) on page 555

[Import a Map](#) on page 405

[Add a Site](#) on page 404

[Add a Building](#) on page 405

[Map Tab](#) on page 557

[Topology Tab](#) on page 556

Topology Tab

The **Topology** tab shows the devices in a given floor-level location, and how they are interconnected. Right-clicking on a Switch Engine device displays a list of VLANs that are currently configured on the device.

Ports configured as an LAG are displayed as a bold green line. Right-clicking an LAG link, displays the ports which are members of the LAG within the **Port Info** view. If multiple ports are connected to a Switch Engine device which are not formed as an LAG, all ports are displayed within the **Port Info** view.

The following details are displayed within each **Port Info** view:

- Port Name
- Type
- Link Aggregation
- LAG Logical Port
- Link Aggregation Status
- Default Port Mode: Access
- Port Status: Connected
- Transmission Mode

- Access VLAN
- Tagged VLAN(s)
- MAC Locking
- LLDP Neighbor
- Traffic Received
- Traffic Sent
- Port Errors
- STP Port State
- Power Used
- Port Speed

Related Links

[Network 360 Monitor Overview](#) on page 553

[Status Cards](#) on page 554

[Device View](#) on page 555

[Zone View](#) on page 556

[Import a Map](#) on page 405

[Add a Site](#) on page 404

[Add a Building](#) on page 405

[Map Tab](#) on page 557

Map Tab

The **Map** tab displays the corresponding map for the selected floor. The floor map displays the floor perimeter and information about the types of walls and obstructions that appear on the floor. Select + to zoom in, and - to zoom out. Use the arrows to move the map within the window.

Related Links

[Network 360 Monitor Overview](#) on page 553

[Status Cards](#) on page 554

[Device View](#) on page 555

[Zone View](#) on page 556

[Import a Map](#) on page 405

[Add a Site](#) on page 404

[Add a Building](#) on page 405

[Topology Tab](#) on page 556

Network Scorecard

The **Network Scorecard** window displays current network health scores by selected location (if you use the locations filter), a 30-day average score for the selected location, and an overall current score for all locations.



Note

Because ExtremeCloud IQ collects data in one-hour segments, when you onboard new devices, or clients first connect to your network, you will not see current score data for the first hour.

Use the filter section to manage the data displayed. When a filter is applied, the filter icon contains a circle in the lower right corner. Use the **Location** filter to display scores for a selected location. Use the **VLAN** filter to display scores for a selected VLAN.

Displayed network scorecards include:

- **Device Health:** Displays current and 30-day average scores for device availability, hardware health, and configuration and firmware.
- **Client Health:** Displays current and 30-day average scores for wireless, network, and application health.
- **WiFi Health:** Displays the current and 30-day average scores for SNR, channel utilization, and association-per-radio score.
- **Network Health:** Displays current and 30-day average scores for Internet availability, Internet performance and network usage.
- **Services Health:** Displays current and 30-day average scores for network, authentication, and management services.

For score calculation details, see:

- [Device Health Scoring](#) on page 558
- [Client Health Scoring](#) on page 560
- [WiFi Health Scoring](#) on page 561
- [Network Health Scoring](#) on page 563
- [Services Health Scoring](#) on page 564

Device Health Scoring

The **Device Health** score is determined based on the following scoring parameters:

- [Device Availability Score](#)
- [Device Hardware Health Score](#)
- [Configuration and Firmware Score](#)

The overall **Device Health** score is calculated based on the following weights applied to the individual scoring parameters:

Overall Device Health Score = (0.3 * availability_score) + (0.5 * hardware_score) + (0.2 * config_firmware_score)

Device Availability Score

For a selected time range and location, the device availability score is calculated by:

- Count of connected devices (X)
- Count of disconnected devices (Y)
- Total devices (T) = X + Y

**Note**

Availability Score = $(X * 100) / T$

Device Hardware Health Score

For a selected time range and location, the device hardware health score is based on the following attributes reported by the periodic device stats from the AP:

- [Average CPU usage](#)
- [Average memory usage](#)
- [Power utilization](#)

**Note**

The overall **Device Hardware Health Score** is calculated as:

Device Hardware Health Score = Power Utilization Score * 0.3 + CPU Usage Score * 0.3 + Memory Usage Score * 0.4

Table 133: Average CPU Score

CPU Usage Average	CPU Usage Score
Less than 85	100
Between 85 and 89	95
Between 90 and 94	90
95 or higher	85

Table 134: Average Memory Score

Memory Usage Average	Memory Usage Score
Less than 80	100
Between 80 and 90	90

Table 134: Average Memory Score (continued)

Memory Usage Average	Memory Usage Score
Between 90 and 94	80
95 or higher	50

Table 135: Average Power Utilization Score

Power Health Criteria	Power Mode	Power Utilization Score
- AP630 - AP650 - AP650X - AP510C - AP510CX - AP1130	802_03_AF	49
- AP250 - AP245X - AP550	802_03_AF	79
Others		100

Configuration and Firmware Score

For a selected time range and location, the configuration and firmware score is calculated based on the following attributes:

- **Config Updated (config_updated):** Count of devices that have configuration in sync with the cloud.
- **Config Pending (config_pending):** Count of devices that have pending configuration updates from the cloud.
- **Firmware Current (firmware_current):** Count of devices that are on latest supported firmware.
- **Firmware Older (firmware_older):** Count of devices that are on an older firmware.

**Note**

The overall **Configuration and Firmware Score** is calculated as:

Configuration Firmware Score = (config_score + firmware_score) / 2

- **config_score** = (config_updated + config_pending * 0.6) * total device count / 100
- **firmware_score** = (firmware_current + firmware_older * 0.8) * total device count / 100

Client Health Scoring

The **Client Health** score is determined based on the following parameters:

- [WiFi Health Score](#)

- [Network Health Score](#)
- [Application Health Score](#)

The **Overall Client Health Score** is the scoring parameter average.

WiFi Health Score

The **SLA Connect** score is calculated and stored for each time period during which a station is connected. Within the selected time range, a station can have multiple connection periods occurring at irregular intervals.

The **WiFi Health Score** is calculated as the weighted average of all clients' SLA Connect scores, where each score is weighted by the duration of all client connections within the selected time range.

Network Health Score

The **IP Network Connectivity** score is calculated and stored for each period during which the station is connected. Within the selected time range, a station can have multiple connection periods occurring at irregular intervals.

The **Network Health** score is the weighted average of all clients' IP Network Connectivity scores, where each score is weighted by the duration of the all client connections within the selected time range.

Application Health Score

The **Application Health** score is calculated and stored for each time period during which a station is connected. Within the selected time range, a station can have multiple connection periods occurring at irregular intervals.

The **Application Health** score is the weighted average of all clients' Application Health scores, where each score is weighted by the duration of all client connections within the selected time range.

WiFi Health Scoring

The **WiFi Health** score is determined based on the following individual scoring parameters:

- SNR Score
- Airtime Utilization Score
- Client Association per Radio Score

Overall WiFi Health Score = (2 * SNR Score) + (1 * Airtime Utilization Score) + (0.5 * Client Association per Radio Score) / 3.5



Note

Individual scores and the overall WiFi Health score are not stored; they are calculated at runtime when the related API calls are made.

SNR Score

Average SNR Score = $((2.46 \text{ averageSNR} * 2.4\text{G totalDocuments}) + (5\text{G averageSNR} * 5\text{G totalDocuments})) / (2.4\text{G totalDocuments} + 5\text{G totalDocuments})$

The overall **SNR Score** is determined based on the average SNR within the specified time range, location, and VHM criteria.

Table 136: Overall SNR Score

Average SNR Score	Overall SNR Score
Greater than 10	35
Between 10 - 15	49
Between 15 - 20	79
20 or higher	100

Airtime Utilization Score

Average Airtime Utilization Score = $((2.46 \text{ averageUtilization} * 2.4\text{G totalDocuments}) + (5\text{G averageUtilization} * 5\text{G totalDocuments})) / (2.4\text{G totalDocuments} + 5\text{G totalDocuments})$

The overall **Airtime Utilization Score** is determined based on the Average Airtime Utilization Score within the specified time range, location, and VHM criteria.

Table 137: Overall Airtime Utilization Score

Average SNR Score	Overall SNR Score
Greater than 70%	35
Between 50 - 70%	49
Between 30 - 50%	79
Between 0 - 30%	100

Client Association per Radio Score

Average Client Association per Radio Score = $((2.46 \text{ client association} * 2.4\text{G totalDocuments}) + (5\text{G client association} * 5\text{G totalDocuments})) / (2.4\text{G totalDocuments} + 5\text{G totalDocuments})$

The overall **Client Association per Radio Score** is determined based on the average clients per radio across all devices within the specified time range, location, and VHM criteria.

Table 138: Overall Client Association per Radio Score

Average SNR Score	Overall SNR Score
Greater than 90	35
Between 60 - 90	49

Table 138: Overall Client Association per Radio Score (continued)

Average SNR Score	Overall SNR Score
Between 30 - 60	79
Between 0 - 30	100

Network Health Scoring

The **Network Health** score is determined based on the following individual scoring parameters:

- [Internet Availability Score](#)
- [Client Network Usage](#)



Note

Individual scores are not stored; they are calculated at runtime when the related API calls are made.

Internet Availability Score

Average Internet Availability Score = (cumulative internet availability / totalDataSamples) * 100

The overall **Internet Availability Score** is determined based on the cumulative internet availability within the specified time range, location, and VHM criteria.

Table 139: Overall Internet Availability Score

Average Internet Availability Score	Overall Internet Availability Score
VHMExcellent (>= 99%)	
100%	100
99%	90
Good (95-98%)	
98%	79
97%	70
96%	60
95%	50
Poor (< 95%)	
90 - 94%	45
70 - 89%	30
60 - 69%	20
50 - 59%	10
< 50%	0

Client Network Usage

Client Network Usage = TX ByteCount + RX ByteCount of all connected clients within the specified time range, location, and VHM criteria.

Services Health Scoring

The **Services Health** score is determined based on the following individual scoring parameters:

- [Network Services Score](#)
- [Authentication Services Score](#)
- [Management Services Score](#)

Overall Services Health Score = (0.65 * Network Services Score) + (0.35 * Authentication Services Score) + (0.05 * Management Services Score)

Network Services Score

Network Services Score = (0.4 * DHCP Score) + (0.3 * DNS Score) + (0.3 * NTP Score)

- **DHCP Score:** The average DHCP service availability percentage across all servers.
- **DNS Score:** The average DNS service availability percentage across all servers.
- **NTP Score:** The average NTP service availability percentage across all servers.

Authentication Services Score

Authentication Services Score = (0.5 * CWP Score) + (0.5 * RADIUS Score)

- **CWP Score** = The average CWP service availability percentage across all servers.
- **RADIUS Score** = The average RADIUS service availability percentage across all servers.

Management Services Score

The **Management Services** score is determined by the Syslog Services score, which is the average Syslog service availability percentage across all servers.

About Client 360

The **Insights Client 360** view shows real time and historical data for active and inactive clients connected to your network.

Use the **Filter** section to manage the data. When a filter is applied to the view, the filter icon shows a small white dot. You can save filters for reuse.

Many of the columns in the table are interactive. Hover over icons or text to see more details.

Choose from the following actions:

- Select  to configure an alias in bulk through .csv.

The .csv file must contain the client MAC address and the alias value. To remove an alias using the .csv file, include the client MAC address and an empty string for the alias value.

- Select  to refresh table data.
- Select  to download data in multiple formats.
- Select  to assign a [Client Alias](#) to one or more active clients.
- Select **Utility > Packet Capture** to [Add and Start a Packet Capture](#) for the selected active client and its associated AP. It is not necessary to select an active client to initiate a Packet Capture session.
- Select  to customize the table columns displayed.

For active clients (the Active tab), when you select a client from the table, a session details section appears. The data that is displayed varies depending on the type of device you have selected.

For inactive clients (the Inactive tab), a timeline enables you to change the time range for which captured client data is displayed.

By default, the window displays 10 clients. Change the number of clients displayed at the bottom left corner of the table. Use the client list to display and select multiple entries at a time, which is useful for large-batch operations.

Related Links

[Set the Time Frame for Captured Data Displays and Reports](#) on page 551

[Packet Capture](#) on page 542

Connection Details Panel (Wireless)

The connection details panel lists details about the current or last connection in a column to the left of the interactive widgets and tables.

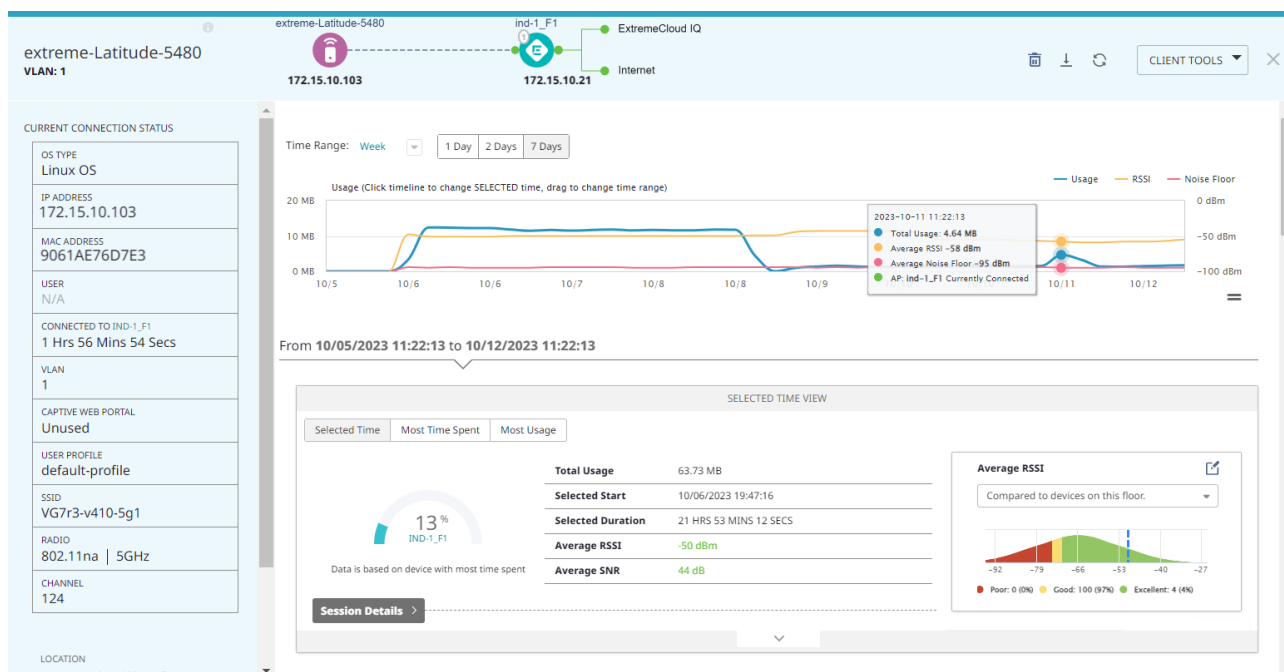


Figure 25: Connection Details Panel

The initial graph displays information about data usage, RSSI, and the noise floor. Use the **Time Range** menu to change the time period. Select from the following options:

- Day (1 Hour, 2 Hours, 4 Hours, 8 Hours, or 24 hours)
- Week (1 Day, 2 Days, 7 Days)
- Month (7 Days, 14 Days, 30 Days, or 90 Days)
- Custom (Use the Calendar controls to select the date range.)

Select one of the tabs to display relevant information:

- Selected Time
- Most Time Spent
- Most Usage

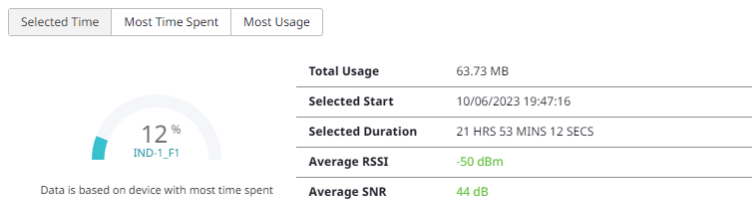


Figure 26: Selected Time

To expand the **SELECTED TIME VIEW** section, select **Session Details >**. For more information, see [Session Details \(Wireless\)](#) on page 570.

The **CLIENT TRAIL** table displays information about device connections. Display 10, 20, 50, or 100 results per page. Navigate pages by selecting the page number, or enter a page number and select **Go**. Color-coded connection status icons provide at-a-glance status information. Mouse over the icons for descriptions.

CLIENT TRAIL

DEVICE NAME	FROM	TO	DURATION	AVERAGE RSSI	AVERAGE SNR	USAGE	SSID	ROAM	ASSOC	AUTH	DHCP	DEFAULT GATEWAY	DNS
> ind-1_F1	2023-10-06 02:15:32	2023-10-06 08:25:08	6 Hrs 9 Mins 36 Secs	-51 dBm	44 dB	19.12 MB	VG7r3-v410-5g1	N/A					
> ind-1_F1	2023-10-06 08:25:40	2023-10-06 10:17:51	1 Hrs 52 Mins 11 Secs	-51 dBm	44 dB	5.86 MB	VG7r3-v410-5g1	N/A					
> ind-1_F1	2023-10-06 10:17:54	2023-10-06 17:50:09	7 Hrs 32 Mins 15 Secs	-51 dBm	44 dB	23.11 MB	VG7r3-v410-5g1	N/A					
> ind-1_F1	2023-10-06 10:17:54	2023-10-06 17:50:09	7 Hrs 32 Mins 15 Secs	-51 dBm	44 dB	23.11 MB	VG7r3-v410-5g1	N/A					
> ind-1_F1	2023-10-06 17:50:16	2023-10-06 17:50:17	0 Secs				VG7r3-v410-5g1	N/A					
> ind-1_F1	2023-10-06 17:50:17	2023-10-06 19:46:35	1 Hrs 56 Mins 18 Secs	-50 dBm	45 dB	5.88 MB	VG7r3-v410-5g1	N/A					
> ind-1_F1	2023-10-06 19:47:16	2023-10-07 17:40:28	21 Hrs 53 Mins 12 Secs	-50 dBm	44 dB	63.73 MB	VG7r3-v410-5g1	N/A					
> ind-1_F1	2023-10-07 17:41:30	2023-10-07 18:01:09	19 Mins 39 Secs	-50 dBm	44 dB	1.07 MB	VG7r3-v410-5g1	N/A					
> ind-1_F1	2023-10-07 18:01:42	2023-10-07 18:01:59	17 Secs	-49 dBm	46 dB	19.14 KB	VG7r3-v410-5g1	N/A					
> ind-1_F1	2023-10-07 18:02:43	2023-10-07 20:46:29	2 Hrs 43 Mins 46 Secs	-50 dBm	44 dB	7.61 MB	VG7r3-v410-5g1	N/A					

10 | 20 | 50 | 100

1

2

3

4

5

Figure 27: Client Trail Table

To download the results as a CSV file, select . To see more detailed information, select a device in the **Device Name** column. See [Device Details Panel \(Wireless\)](#) on page 573.

The **TROUBLESHOOT SESSIONS** table displays in-progress and completed troubleshooting sessions.

TROUBLESHOOT SESSIONS				
TIMESTAMP	DESCRIPTION	INITIATED BY	STATUS	
> 2023-10-13 15:23:04		shrisha-ft-2@gmail.com	IN PROGRESS (09:48)	↓ ⚠
> 2023-10-12 10:09:18		shrisha-ft-2@gmail.com	COMPLETED	↓

Figure 28: Troubleshoot Sessions Table

To download the results for a session, select the corresponding  icon. For more information about troubleshooting sessions, see [Client Tools \(Wireless\)](#) on page 502.

The **CLIENT EVENTS** table displays client events. Filter the events according to phase:

- All
- Association
- Authentication
- IP Assignment

CLIENT EVENTS					↓
Phases All ☐ Show Probe					
DEVICE NAME	TIMESTAMP	DEVICE BSSID	EVENT TYPE	DESCRIPTION	
ind-1_F1	2023-10-12 14:03:27	BCF3105D74F4	Basic	Sta(at if=wifi1.1) is de-authenticated because of notification of driver	
ind-1_F1	2023-10-12 14:03:27	BCF3105D74F4	Basic	Sta(at if=wifi1.1) is de-authenticated because of notification of driver	
ind-1_F1	2023-10-12 14:03:27	BCF3105D74F4	Info	Rx deauth (reason 4 <assoc-leave>, rssi -55dB)	

Figure 29: Client Events Table

To download the results as a CSV file, select .

The **NETWORK USAGE** section displays usage information in an interactive graph and **Top 10 Apps** widget. Mouse over points on the graph for details. From the hamburger menu, choose from the following options:

- Print chart
- Download PNG
- Download JPEG
- Download PDF
- Download SVG vector image

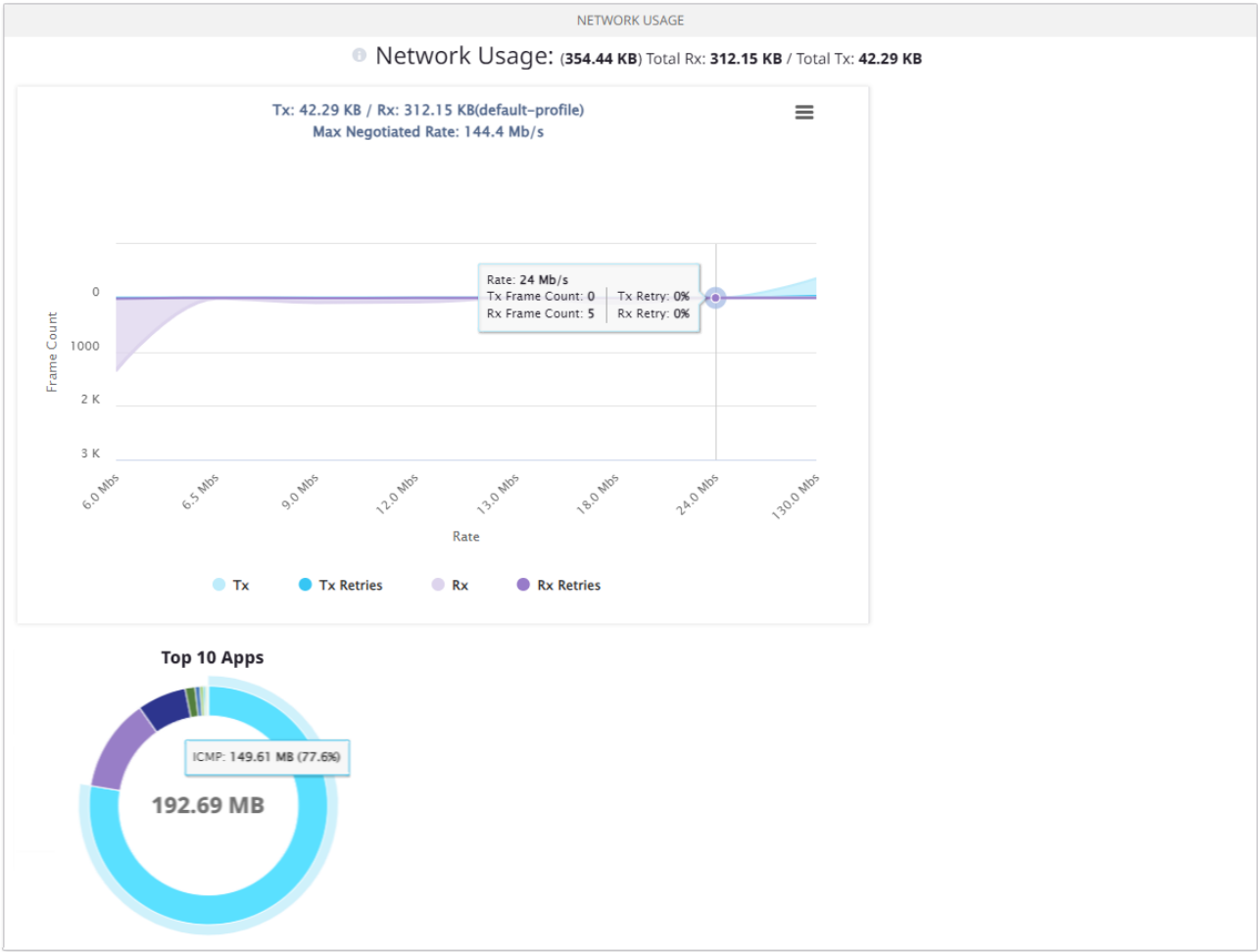


Figure 30: Network Usage Graph and Widget

Mouse over the **Top 10 Apps** widget to display information about app usage.

The **MAXIMUM CLIENT CAPABILITIES** widget displays the maximum client capabilities for all 2.4 and 5 GHz Wi-Fi clients connected to the AP during the selected period.

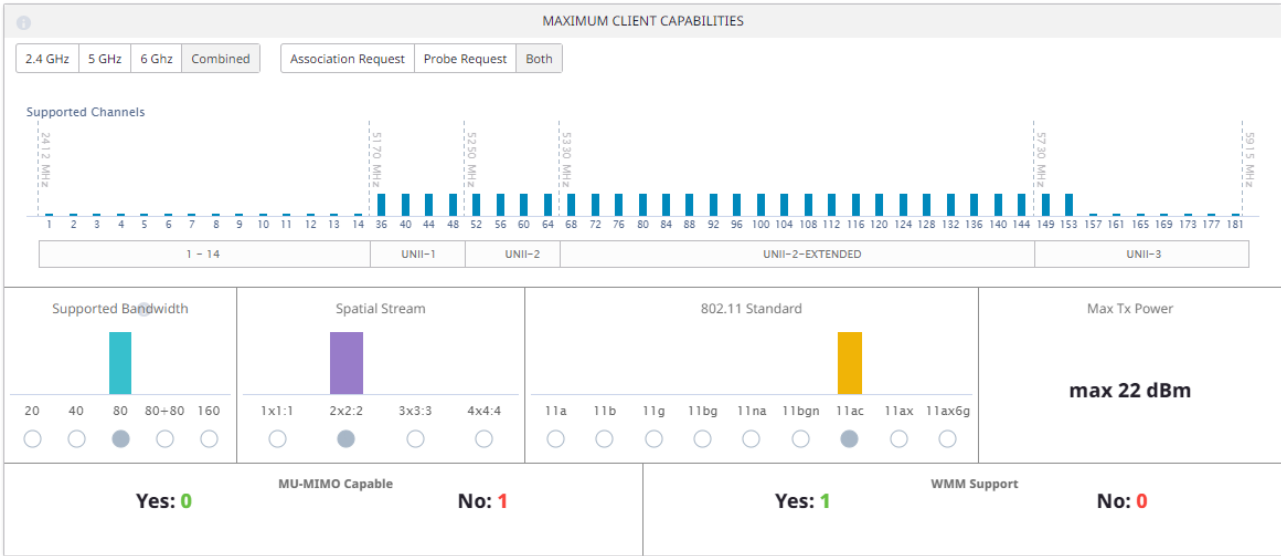


Figure 31: Maximum Client Capabilities Widget

Related Links

- [Session Details \(Wireless\)](#) on page 570
- [Device Details Panel \(Wireless\)](#) on page 573
- [Client Tools \(Wireless\)](#) on page 502
- [Connectivity Experiences Panel \(Wireless\)](#) on page 588
- [Connectivity Experiences](#) on page 585

Session Details (Wireless)

To expand the **SELECTED TIME VIEW** section, select **Session Details**.

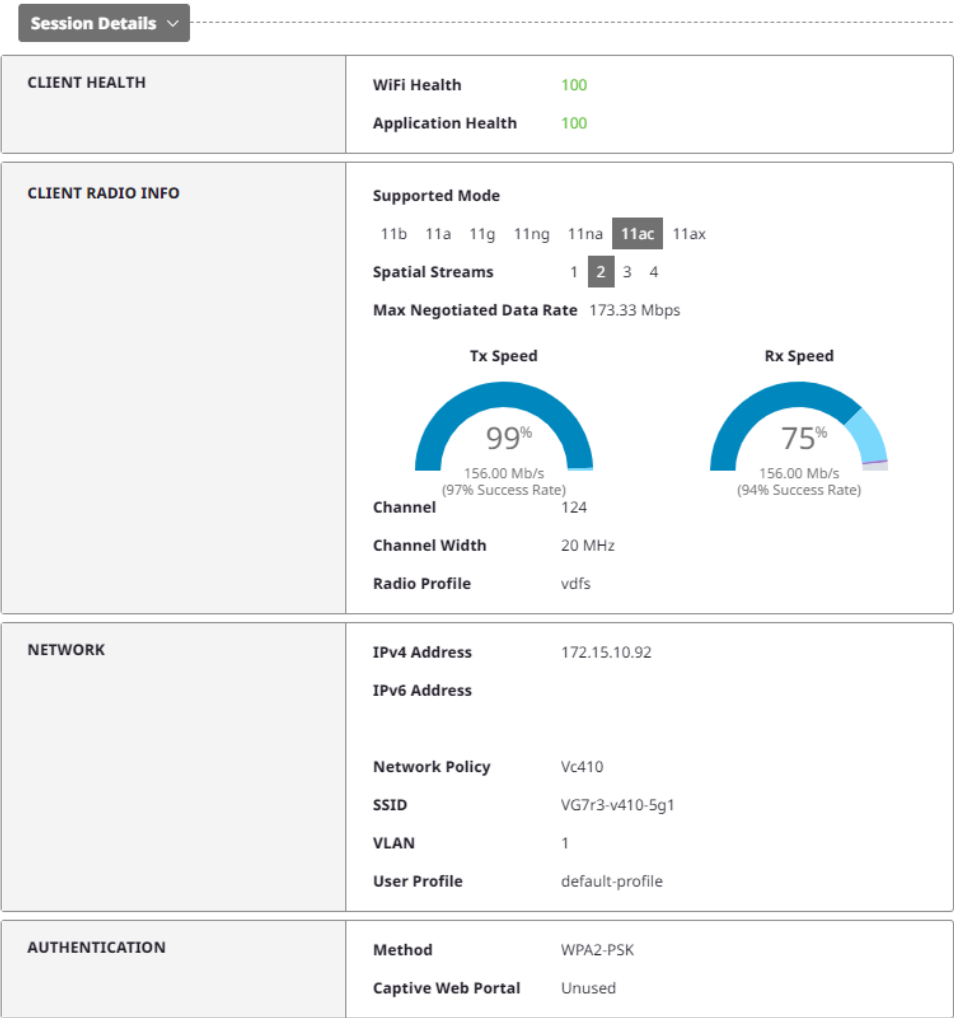


Figure 32: Session Details—Expanded

Mouse over the **Tx Speed** and **Rx Speed** graphs to see the percent for each category.

Interactive widgets appear to the left of the display. You can edit the thresholds and customize the view for the following widgets:

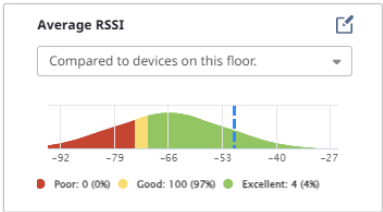


Figure 33: Average RSSI

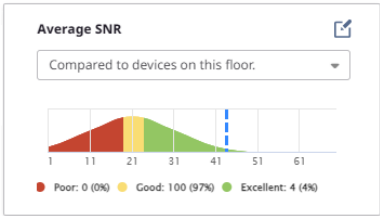


Figure 34: Average SNR

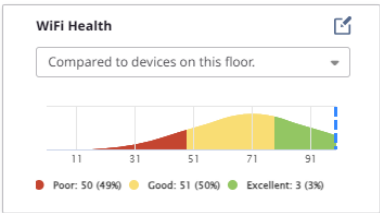


Figure 35: WiFi Health

Use the drop-down menu to choose one of the following display options:

- Compared to devices on this floor.
- Compared to the connect AP.

To edit the thresholds, select .

Edit Health Range

Poor:

0

to

49

Good:

50

to

79

Excellent:

80

to

100

Reset all

Cancel

Save

Figure 36: Edit Health Range

Mouse over a column in the **Supported Mode** widget to see the number of supported devices for that mode.

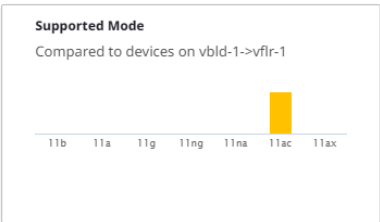


Figure 37: Supported Mode

Related Links

- [Connection Details Panel \(Wireless\)](#) on page 565
- [Connectivity Experiences Panel \(Wireless\)](#) on page 588
- [Connectivity Experiences](#) on page 585

Device Details Panel (Wireless)

To open the details panel for a device, select the device link in the **Device Name** column of the **CLIENT TRAIL** table. Alternately, go to **Manage > Devices** and select a device.

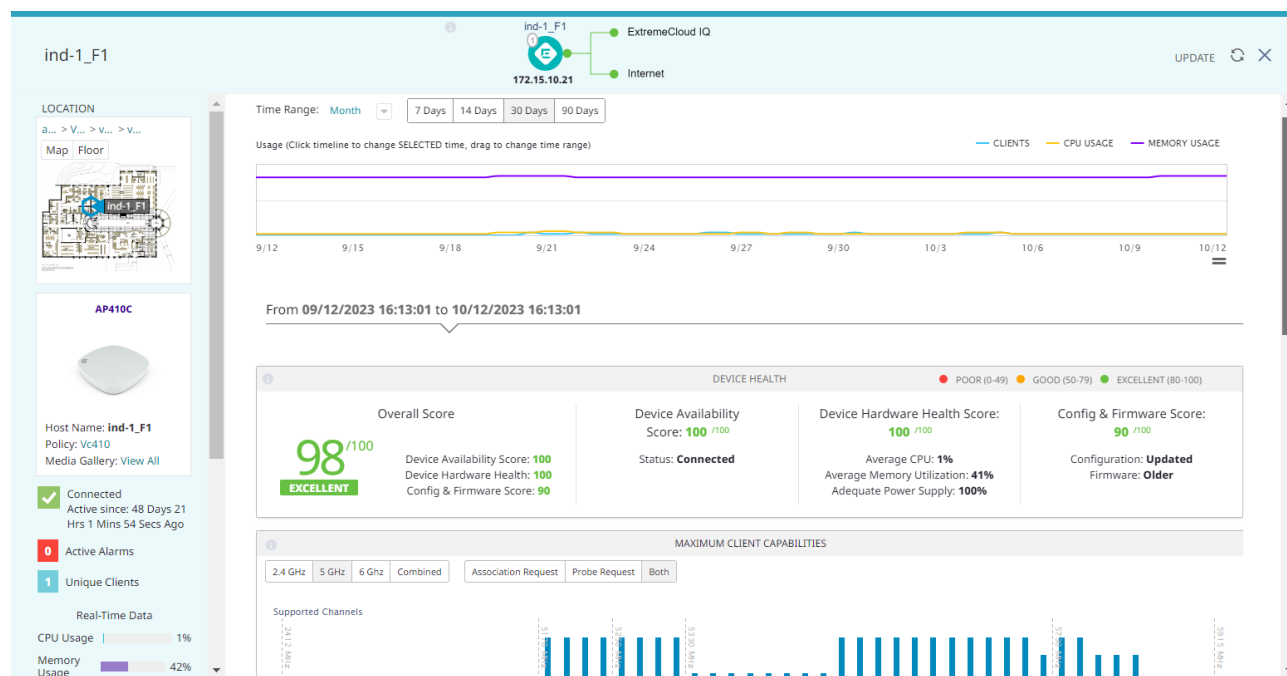


Figure 38: Device Details Panel

The panel organizes information under tabs:

- **Monitor**
- **Configure**

Related Links

- [Device Details Panel](#) on page 454
- [Device Details Monitor Functions](#) on page 455
- [Device Details Configuration Tasks](#) on page 465
- [Connection Details Panel \(Wireless\)](#) on page 565
- [Connectivity Experiences Panel \(Wireless\)](#) on page 588
- [Connectivity Experiences](#) on page 585

Client Alias

Assign a client alias to one or more active clients to easily identify and find clients. After defining a client alias, you can search on the client alias to display all clients with that alias.

Configure Client Alias manually from the user interface, in bulk through .csv, or through the API.

ML Insights > Client 360

1. Go to **ML Insights > Client 360** and select one or more clients from the **Connected Clients List**.
2. Select  to edit.

The **Change Client Alias** dialog displays.

- Enter a Client Alias for the selected clients and select **Save**.
 - To remove an alias from a client, select , then select **Save**.
3. Additionally, you can apply existing filters to restrict the number of clients displayed.

Device Details

View Client Alias from the **Device Details** page:

1. Go to **Manage > Devices**.
2. Select a device to display **Device Details**.
3. Select **Monitoring > Clients**.

The Client Alias column is shown in the list of clients.

Clients Monitor & Diagnosis

View Client Alias from a list of client issues. Go to **Manage > Client Monitor & Diagnosis**. You can search client issues by alias, in addition to hostname and MAC address.

Thread Monitoring

The **Thread Monitoring** view provides an administrator with real-time insight into the health and topology of their Thread networks which is crucial for diagnosing issues, optimizing performance, and understanding network behavior:

- Visualizing the topology of a Thread network provides a clear overview of the network's current state, including device connectivity, router roles, and mesh network dynamics.
- Viewing in real-time when a network segmentation has occurred (new elections).
- Interacting with the different roles to see what they are doing and how they are behaving.

As a Thread network uses a mesh network topology, it allows for multiple paths between devices, which enhances the network's resilience and flexibility to provide reliable and secure wireless communication for IoT end-devices.

- Thread networks are designed to be self-healing. Routers automatically adjust their routing tables and can change their roles (router, leader, or router eligible end-device) based on the network's needs.
- When a new router joins a Thread network the network automatically adjusts its topology to include it, potentially selecting it as a path for data transmission based on its location, signal strength, and the network's current topology.
- When a new client joins a Thread network, the client attempts to connect to the router with the strongest signal strength that has available capacity. Although the addition of thread clients might not change the network topology as significantly

as the addition of thread routers, it still requires the network to adapt, ensuring all devices maintain reliable connectivity.

Due to failures or disruptions in connectivity, dynamic changes in the network topology can lead to network partitions - isolated segments of the network. By visualizing the topology of the Thread network, administrators can easily identify these network partitions, leading to quicker troubleshooting and less downtime, ensuring the network remains operational and dependable.

Go to **ML Insights > Thread Monitoring**.

Thread Network Details

Before you can select a Thread network, you must select the site to which it belongs. Select a **Site** and an available **Thread Network** from the drop-downs to view thread details in the Toplogy view.

Thread networks are defined by configuring the IoT interface of one or more APs with an IoT profile specifying a **Thread Gateway** configuration. Different APs configured with the same IoT profile belonging to different sites belong to different Thread networks, but have the same Thread network settings. For more information, see [Thread Application](#) on page 222.

Topology View

View the topology of the selected Thread network in the topology viewer. The "Legend" drop down describes the meaning of the different icons used in the topology diagram.

Select the **Legend** drop-down to view the different icons used in the topology diagram:

-  **Leader**: Manages the overall operation of the thread network. There is only one active Leader in a thread network at any given time.
-  **Router**: Forwards data packets within the network. However, if a Thread network becomes partitioned due to a communication breakdown between sections of the network, each isolated segment can independently elect a new Leader.
-  **End Device**: Endpoints that interact with the network.



Note

When Thread Commissioner is running on an AP, the  icon appears next to the topology diagram. For example, if the leader AP is running Thread Commissioner, the icon appears as follows:



Select  to collapse and expand the menu to enlarge or reduce the Topology viewer for visibility.

Select **+** to zoom in, and **-** to zoom out. Use the arrows to move the Thread network within the window. Alternatively, scroll the mouse wheel to zoom in and out. Select and drag the diagram to view nodes not displayed on the screen.

Select, or hover over, a router node in the topology viewer to see the following node-specific details appear:

- Host Name
- Serial Number
- EUI64
- RLOC16
- Role
- Services

Select an end-device node in the topology viewer to see the **End Device List** for the end devices connected to the parent router:

- MAC Address
- IPV6
- RLOC16

Inventory

To view device details for all the routers participating in the selected Thread network, go to **Inventory > Routers**.

To see a client view of all the end devices participating in the selected Thread network, go to **Inventory > End-Devices**.

Table 140: Thread Router Details

Parameter	Description
Status	Status icons indicate a router's connection status.
Host Name	The host name of the device.
Serial Number	Device serial number.
EUI64	A unique identifier assigned to a device in a Thread network.
Role	The role (Leader or Router) of the device in a thread.
Extended MAC	A unique identifier assigned to a device in a Thread network.
RLOC16	The RLOC16 reflects the hierarchical structure of the network. All devices in the Thread topology have an RLOC16 that is the combination of their router ID + child ID. Because a router is not a child, the child ID for a router is always 0. All child nodes with the same parent router have the same router ID.
IPv6 Link Local	The IPv6 address of the device.

Table 140: Thread Router Details (continued)

Parameter	Description
Mode	The operational modes of the thread device: • Rx On When Idle: This flag indicates whether the device keeps its radio receiver (Rx) on when it is not actively transmitting (Idle). If this is set to true, the device is constantly listening for incoming messages, which is typical for powered devices such as routers. If it's false, the device powers down its radio when idle to save energy, which is a behavior often seen in battery-operated devices. • Full Thread Device: This flag specifies if the device is a Full Thread Device (FTD). An FTD is capable of performing all Thread protocol functions and can route traffic on behalf of other devices. The radio receiver is on when idle and maintains routing information for the network. If this is true, the device is an FTD; if false, it is a Minimal Thread Device (MTD), which does not route traffic and often operates at a lower power level. • Full Network Data: This flag indicates if the device stores a full copy of the network data. Full network data includes all the operational datasets of the Thread network. Devices with full network data have enough information to function as leaders within the Thread network, if necessary. If this is true, the device maintains a full set of the network data; if false, it only stores what is necessary for its operation as a reduced-function device.
Channel	The thread channel number.
Border Router	The border router's connection status.
Backbone Border Router	The elected state (Primary or Secondary) of the backbone border router.

Table 141: Thread End-Devices Details

Parameter	Description
Status	Status icons indicate a router's connection status.
MAC Address	A unique identifier assigned to a device in a Thread network.
RLOC16	A unique identifier assigned to a device in a Thread network.
Extended MAC Address	A unique identifier assigned to a device in a Thread network.
IPV6 Mesh Local EID	The unique endpoint identifier assigned to a device in a Thread network.
Channel	The thread channel number.

Table 141: Thread End-Devices Details (continued)

Parameter	Description
Average RSSI	The average signal strength of the received radio signal.
Connection Time	The total time that the device has been online.

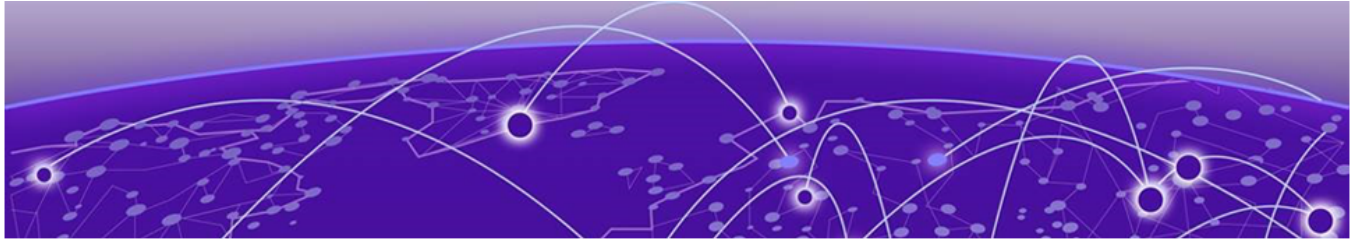
Node Details

Select a node from the Topology viewer for Network, Interface, and Services details. Select an option from the **Node Details** list to display details. The available details are determined by the type of node selected.

Related Links

[Configure IoT Profile Settings](#) on page 224

[Thread Application](#) on page 222



Essentials

[ExtremelOT Essentials in ExtremeCloud IQ](#) on page 579

[Extreme AirDefense Essentials in ExtremeCloud IQ](#) on page 580

[ExtremeGuest Essentials in ExtremeCloud IQ](#) on page 582

[ExtremeLocation Essentials in ExtremeCloud IQ](#) on page 583

Use **Essentials** to access the following Essentials Applications in ExtremeCloud™ IQ:

- ExtremelOT Essentials
- Extreme AirDefense Essentials
- ExtremeGuest Essentials
- ExtremeLocation Essentials

ExtremelOT Essentials in ExtremeCloud IQ



Tip

We are deprecating ExtremelOT™ Essentials™. Existing customers can toggle access via URL, where 10.XXX.XX.49 is the IP for your VIQ:

Enable access:

`https://10.XXX.XX.49/hm-webapp/#/devices?iotEss=true`

Disable access:

`https://10.XXX.XX.49/hm-webapp/#/devices?iotEss=false`

The URL is persistent across sessions.

ExtremelOT™ Essentials provides security management with a simplified configuration work flow, plus traffic and application visibility of connected end devices. ExtremelOT Essentials also facilitates the centralized creation of policies that define network and security settings for groups of IoT devices.



Note

ExtremelOT Essentials is only for the protection of wired IoT end devices. The ExtremelOT Essentials setup creates configuration for wired devices. Administrators can create additional wireless networks through ExtremeCloud IQ.

ExtremelOT Essentials can help you manage IoT devices within ExtremeCloud IQ. The configuration is simplified and steps you through network policy configuration that is associated with the device.

You can use the ExtremeCloud IQ Dashboard Essentials  > icon to list the Essentials applications and choose ExtremelOT Essentials. The ExtremelOT Essentials navigation menu launches in ExtremeCloud IQ.

Access to ExtremelOT Essentials functionality depends on your ExtremeCloud IQ user access level.

**Note**

ExtremelOT Essentials functionality also requires an ExtremeCloud IQ CoPilot™ license.

The following options are available from the **ExtremelOT Essentials** navigation menu:

Dashboard

Monitor your network activity and performance on the dashboard. The dashboard provides a graphical representation of information related to protected devices. Depending on the report, the widget represents historical data or a combination of historical and the latest data from shared memory.

Devices

List of supported access points. The devices view displays data for ExtremelOT Essentials capable devices only.

Clients

List of IoT clients attached to any of the managed devices.

User Profiles

A user profile is a policy role that determines a client's access to the network. Define firewall rules to provide unique treatment of packet types when a user profile is applied.

Policy Groups

Policy groups map a defined user profile to a set of clients. A user profile is a set of network access services that can be applied at various points in a policy-enabled network. All clients in a policy group are subject to the rules defined in the user profile.

Extreme AirDefense Essentials in ExtremeCloud IQ

Extreme AirDefense Essentials is a cloud-based management tool you can use to configure, implement and review security protocols that evaluate and monitor threat detection for devices in your network.

You can use the ExtremeCloud IQ Dashboard Essentials  > icon to list the Essentials applications and choose Extreme AirDefense Essentials. The Extreme AirDefense Essentials Overview launches in ExtremeCloud IQ.

The Extreme AirDefense Essentials Overview launches in ExtremeCloud IQ.

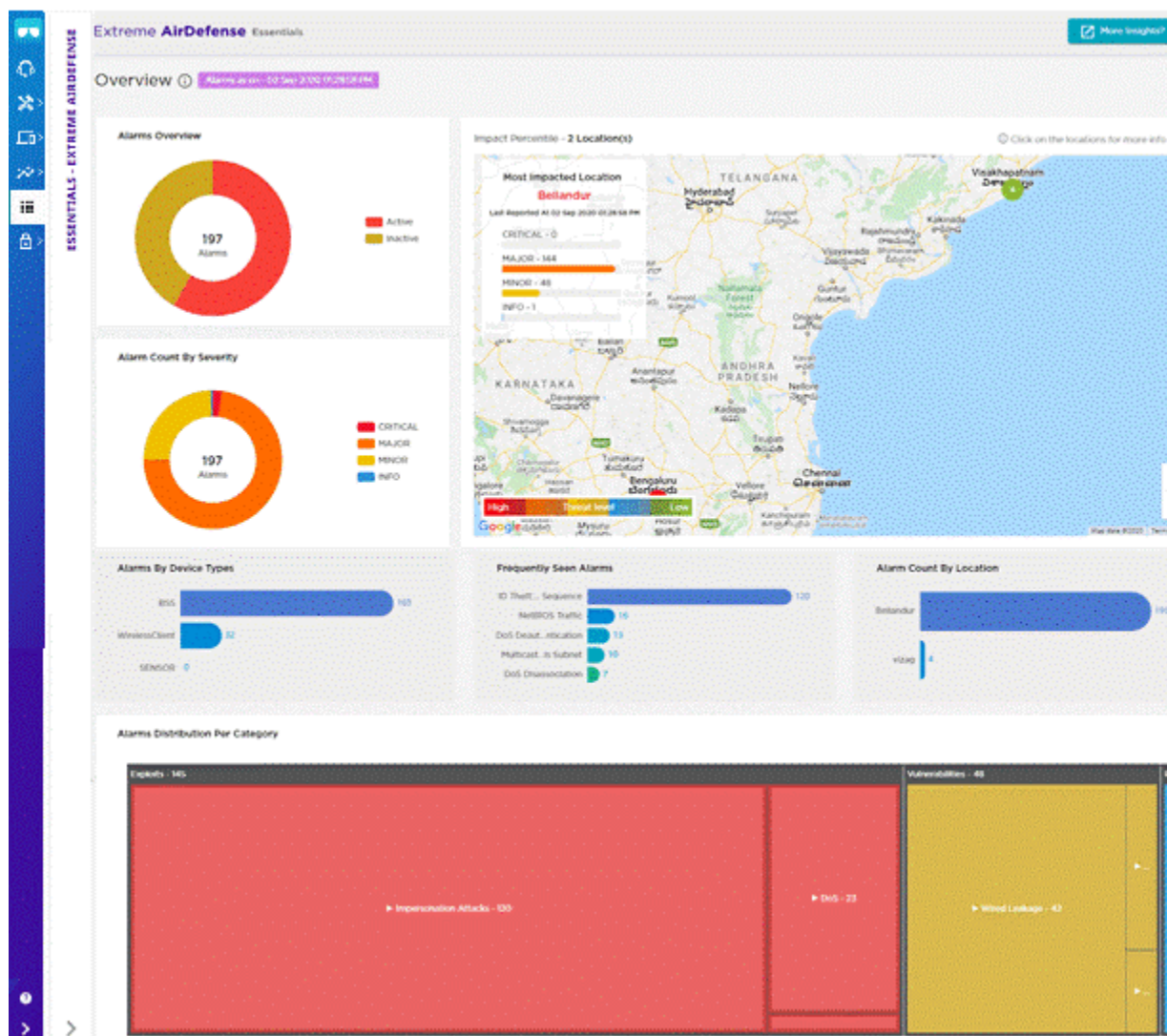


Figure 39: Extreme AirDefense Essentials Overview View in ExtremeCloud IQ

The Extreme AirDefense Essentials Overview in ExtremeCloud IQ includes the following widgets:

- Alarms Overview
- Alarm Count by Severity
- Percentile Map
- Alarms by Device Types
- Frequently Seen Alarms
- Alarm Count by Location

You can select the **More Insights** button at the top right corner of the Overview to access all the features of Extreme AirDefense Essentials and open the application in a separate browser tab.

ExtremeGuest Essentials in ExtremeCloud IQ

ExtremeGuest Essentials is a robust and comprehensive guest management and engagement solution that personalizes engagement by understanding customer behavior and interest, and then tailoring services based on those insights. For example, the number of customers that enter a store, how often they visit, and how much time they spend are all metrics that can be measured through ExtremeGuest Essentials.

ExtremeGuest Essentials can take advantage of social networking behavior to increase patronage, expand brand exposure, and understand client demographics and preferences in a more comprehensive and personal way. Guest onboarding with sponsor approval is supported, allowing a sponsor to approve or deny guest access with a single click.

ExtremeGuest Essentials supports all access point models that are supported with ExtremeCloud IQ.

For documentation on each access point, refer to the AP model number under Extreme Documentation at extremenetworks.com/documentation.

You can use the ExtremeCloud IQ Dashboard Essentials  > icon to list the Essentials applications and choose ExtremeGuest Essentials. The ExtremeGuest Essentials Connection Status launches in ExtremeCloud IQ.

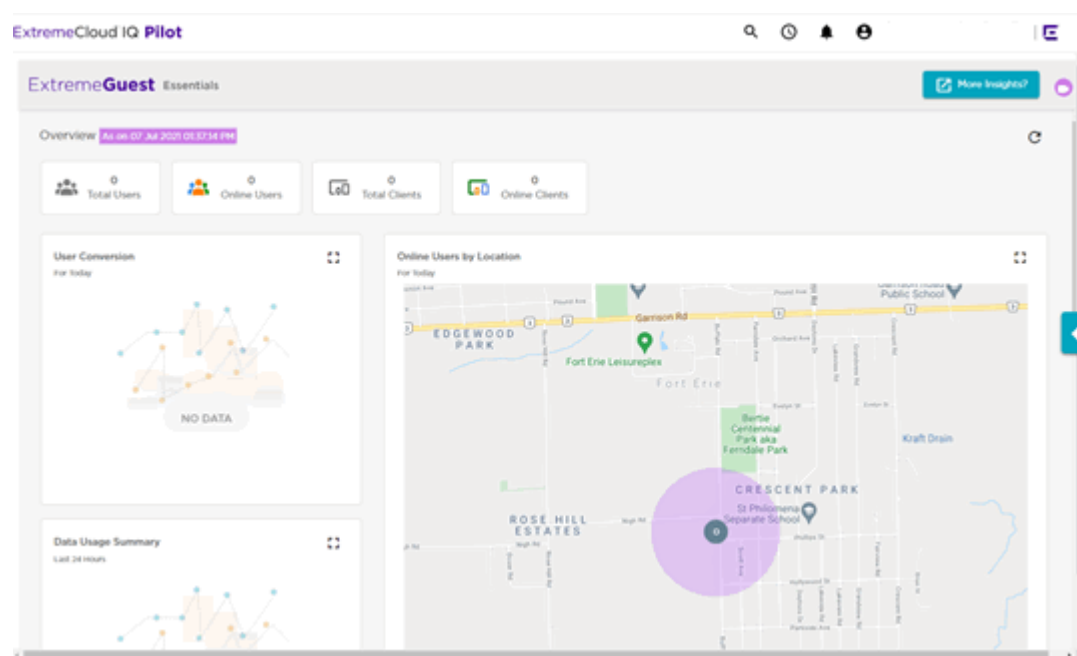


Figure 40: ExtremeGuest Essentials Overview View in ExtremeCloud IQ

You can select the **More Insights** button at the top right corner of the Overview to access all the features of ExtremeGuest Essentials and open the application in a separate browser tab.

ExtremeLocation Essentials in ExtremeCloud IQ

ExtremeLocation Essentials is a resilient, cloud-based location and analytics solutions from Extreme Networks. With real-time location and analytics, you can engage with your customers providing personalized experience for guests and visitors. ExtremeLocation Essentials can also be used to monitor your workflows and assets to improve your overall operation and efficiency.

ExtremeLocation Essentials is accessible from the Extreme Networks cloud-based network management solution ExtremeCloud IQ. ExtremeCloud IQ and Virtual IQ (or VIQ, which is virtual ExtremeCloud IQ) share client data storage functionality. If a client's data is deleted in ExtremeCloud IQ, all configured, cached, Live, and Historical data related to that client is also deleted from ExtremeLocation Essentials.

ExtremeLocation Essentials offers a range of accurate and granular location accuracy to address your deployment scenarios and includes the following functionality:

- Real-time and historical location analysis
- New and repeat visitor tracking
- Engagement time monitoring
- Site or zone specific intelligence
- Assets and employee tracking

Use the ExtremeCloud IQ Dashboard Essentials  > icon to list the Essentials applications and choose **ExtremeLocation Essentials**. The ExtremeLocation Essentials Overview opens in ExtremeCloud IQ.

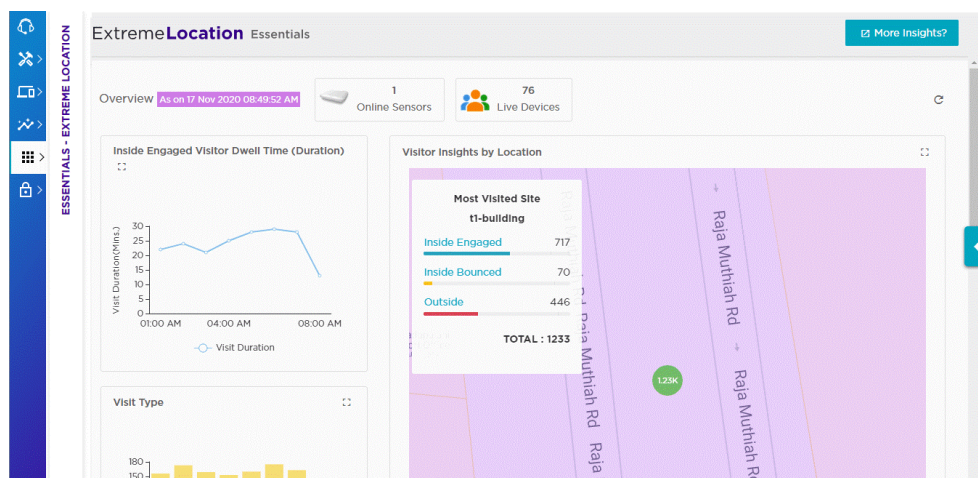
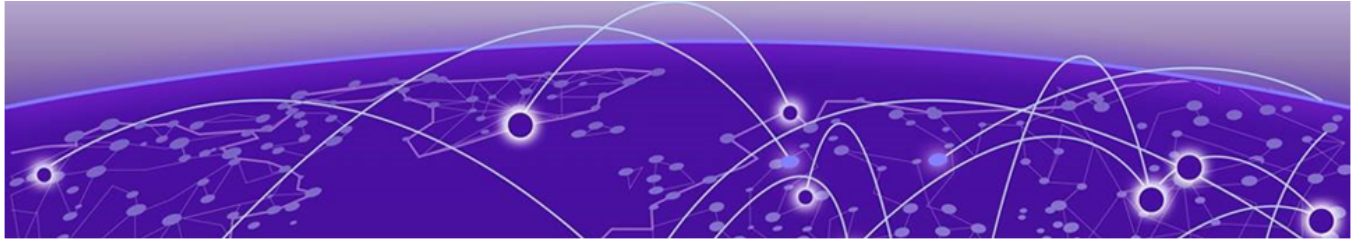


Figure 41: ExtremeLocation Essentials Overview View in ExtremeCloud IQ

To access more ExtremeLocation Essentials features and open the application in a separate browser tab, select **More Insights**.



CoPilot Dashboard

[Connectivity Experiences](#) on page 585

[Anomalies](#) on page 596

ExtremeCloud IQ CoPilot is an AIOps solution that leverages Explainable Machine Learning (ML). With CoPilot, your IT operations teams become more data-driven and proactive. The CoPilot dashboard provides access to in-depth information anomalies and client connectivity for your Extreme Networks cloud-managed wired and wireless networks. Your ExtremeCloud IQ CoPilot subscription provides the following benefits:

- Simplifies troubleshooting by providing auditable recommendations to reduce the number of out-of-context alerts that can waste time and effort
- Identifies anomalies and alerts you, providing an explanation and the best options for resolution
- Reduces risk by proactively looking for patterns ahead of time to identify significant anomalies so IT can address them early
- Utilizes continuous learning and bidirectional communication to provide the best and most accurate recommendations for your network
- Summarizes the client connectivity experience into a single quality index score, and helps you to easily track, identify, and troubleshoot connectivity issues

CoPilot is enabled by default for customers with CoPilot licenses using ExtremeCloud IQ (Classic).

Table 142: Copilot Capabilities Summary

Capability	Wireless Network	Wired Network	Description
Connectivity Experiences	Yes	Yes	Summarizes the client experience into a single quality index score to easily track, identify, and troubleshoot connectivity issues
Wi-Fi Efficiency Anomaly	Yes		Unusually high channel utilization, reporting instances of excessive recurrence and duration
Wi-Fi Capacity Anomaly	Yes		Access points (APs) with unusually high channel utilization, reporting instances of excessive recurrence and duration

Table 142: Copilot Capabilities Summary (continued)

Capability	Wireless Network	Wired Network	Description
PoE Stability Anomaly	Yes	Yes	Access point and SW ports with bad cabling, power supply consistency issues, or insufficient power provided
DFC Recurrence Anomaly	Yes		Access points with excessive channel changes due to external 5Ghz interference, such as radar
Port Efficiency Anomaly	Yes	Yes	Access point and Switch (SW) ports with bad cabling, faulty ports, or auto-negotiation issues
Adverse Traffic Patterns Anomaly	Yes	Yes	Access points and switches with traffic loading issues that cause excessive usage of CPU and memory resources
Hardware Health	Yes	Yes	Devices that have exceeded the threshold for conditions that indicate the state of hardware health
Missing VLANs	Yes		VLANs that are configured on the APs, but missing on the upstream switch

To access the ExtremeCloud IQ CoPilot dashboard, log in to ExtremeCloud IQ and select  from the left navigation panel. The dashboard uses the following tabs to organize the data:

- [Anomalies](#) on page 596
- [Connectivity Experiences](#) on page 585

You can access the dashboard from anywhere, by using the ExtremeCloud IQ Companion mobile app for AIOps.

Connectivity Experiences

The quality index scores client connectivity experiences from 1 (worst) to 10 (best). In an ideal scenario, the quality index is 10 consistently over time, while any decline in the index value indicates a degraded experience. This index is calculated for every client, every time new client metrics are obtained. By default, this interval is every 10 minutes.

Quality index scoring provides more granularity and better control. It can help mitigate the effects of single (random) events.

The global threshold is dynamically calculated based on information from all clients in the Regional Data Center. The system dynamically calculates the local threshold per location and SSID type (PSK vs Open vs Enterprise), and uses the lower threshold.

The **Connectivity Experiences** tab uses the following widgets and a [table](#) to display information about connection quality:

- [Quality Index for Wireless Devices Widget](#) on page 586
- [Quality Index for Wired Devices Widget](#) on page 586

The widgets and table are interactive. Mouse over them to see more details.

To hide the widgets and display a streamlined view of **Sites by Quality Index**, select .

To display the widgets again, select .



Figure 42: Sites by Quality Index Streamlined View

Related Links

- [Quality Index for Wireless Devices Widget](#) on page 586
- [Quality Index for Wired Devices Widget](#) on page 586
- [Connectivity Experiences Table](#) on page 587
- [Connectivity Experiences Panel \(Wired\)](#) on page 594
- [Connectivity Experiences Panel \(Wireless\)](#) on page 588

Quality Index for Wireless Devices Widget

The quality index combines time-to-connect and performance scores, measured against dynamic thresholds. Time to Connect includes association, authentication, and IP acquisition times. Performance score considers packet retry rates. The score, ranging from 1 (worst) to 10 (best), is a time-weighted average, with recent events weighing more.

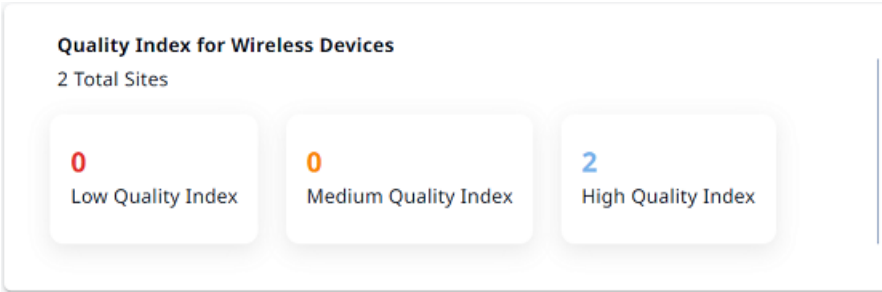


Figure 43: Quality Index for Wireless Devices

The **Quality Index for Wireless Devices** widget shows the number of wireless sites for each quality index category: Low, Medium, and High. Select a quality index category to update the table to show only sites with the selected quality index.

Related Links

- [Connectivity Experiences](#) on page 585

Quality Index for Wired Devices Widget

The quality index for wired devices accounts for port errors on each switch interface. It is a time-weighted average, with recent events weighing more. The score ranges from 1 (worst) to 10 (best), reflecting connectivity health.

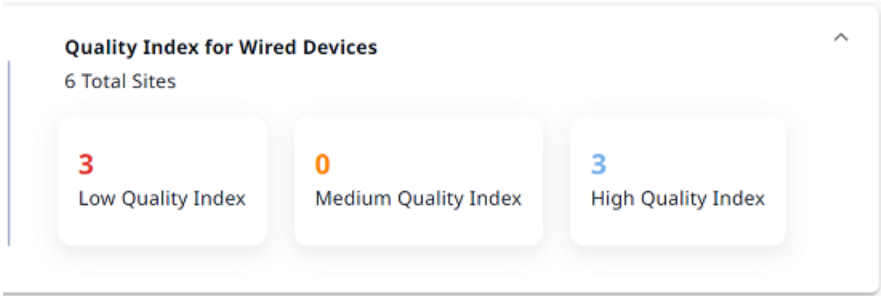


Figure 44: Quality Index for Wired Devices

The **Quality Index for Wired Devices** widget shows the number of wired sites for each quality index category: Low, Medium, and High. Select a quality index category to update the table to show only sites with the selected quality index.

Related Links

[Connectivity Experiences](#) on page 585

Connectivity Experiences Table

The **Connectivity Experiences** table displays connection quality information for the previous 24 hours, and includes the following information for each entry:

- **Site**
- **Connectivity Type**
- **Quality Index**
- **Trend**

The table displays connection quality information for the previous 24 hours. Use the controls found at the top of the page to customize your view of the table:

Site

Display all sites (default) or select a specific site from the menu. Start typing a site name to search the menu for a particular site.

To return to the default view, select **X**.

Connectivity Type

Display all clients (default), or select only wireless, or only wired clients.

To return to the default view, select **X**.

Quality Index

Select Low (1–5), Medium (6–8), or High (8–9). The table updates to display the wired and wireless sites that match your selection.

To return to the default view, select **X**.

Time Range

Use the calendar control to select the time period for which you want to display connection quality trends information. Select the calendar control to open it and then select one of the options:

- Last 24 Hours
- 7 Days
- Custom

Select the start date and time, and then select the end date and time for the period. Select up to 7 days, from 90 days of historical data.

Search by Location

Start typing a site name to search the table for a site. Select **X** to clear the search string and return to the previous table view.

To sort the table results in ascending or descending order according to **Site**. Hover the mouse to the right of the corresponding column label, and select the . To change the sort order again, select the . You can also search for connection quality information by site. Use the **Items per page** menu to specify the maximum number of results to show, per page.

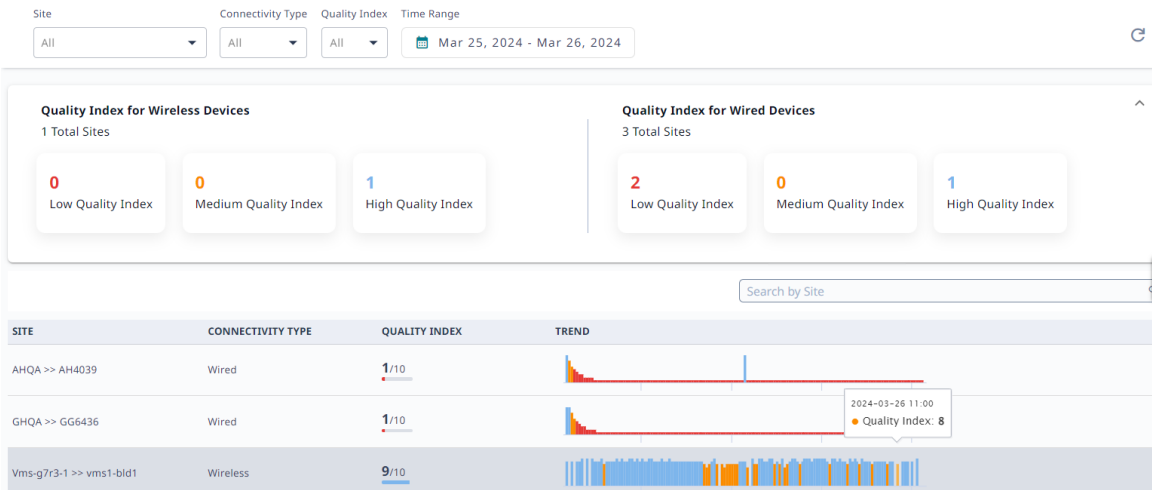


Figure 45: Connectivity Experiences table

Related Links

[Connectivity Experiences](#) on page 585

Connectivity Experiences Panel (Wireless)

To open the **Connectivity Experiences** panel for a site, select the site. Mouse over a point on the graph to display the following metrics at that time:

- Quality Index
- Time to Connect
- Performance

To zoom in, drag and select a time period on the **Quality Index** graph.

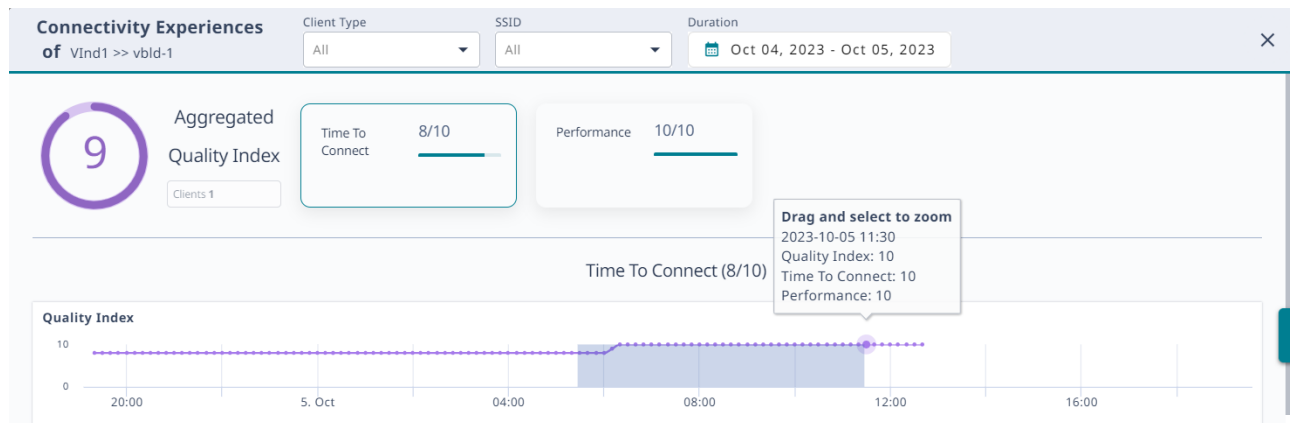


Figure 46: Connectivity Experiences Panel (Wireless)

Your selection and the zoom function apply to all graphs that appear on the site **Connectivity Experiences** panel.

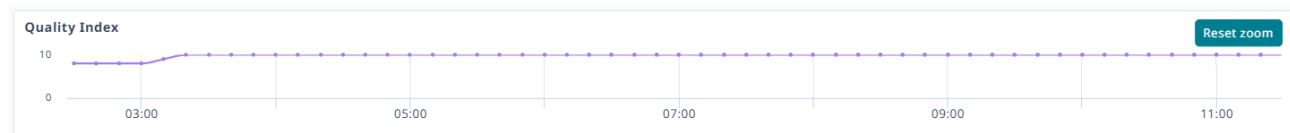


Figure 47: Quality Index Zoom

To see the number of unique clients at a particular time, mouse over a point in the **Client Count** graph.

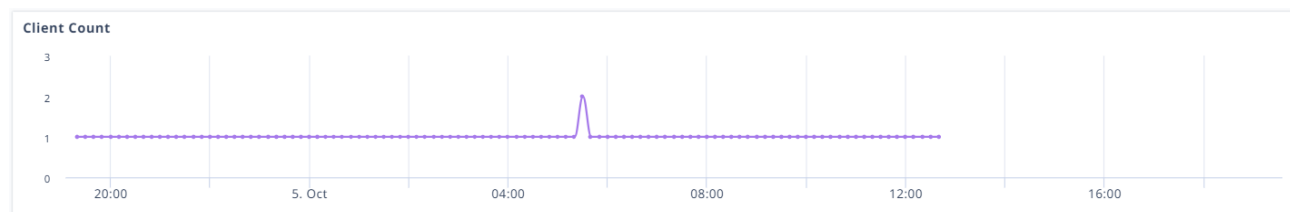


Figure 48: Client Count

Related Links

[Connectivity Experiences](#) on page 585

Client Association (Wireless)

Mouse over a point in the **Client Association** graph to see a summary of the following information:

- Date and time stamp
- Total Unique Clients
- Time to Associate
- Clients Above Association Threshold
- Time to Authenticate

- Clients Above Authentication Threshold
- Time to Obtain IP Address
- Clients Above DHCP Threshold

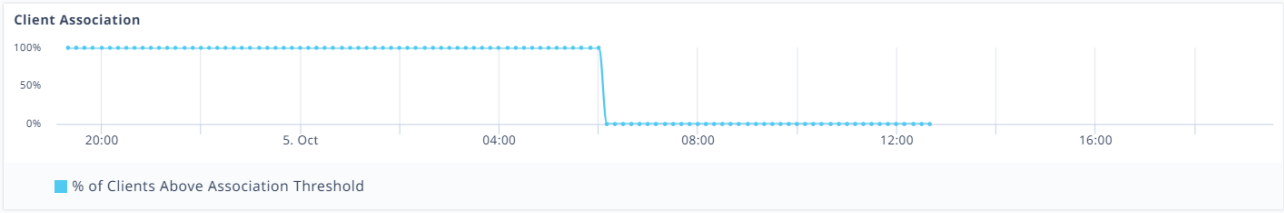


Figure 49: Client Association

To open the **Client Association** panel and see more details, select a point on the graph.

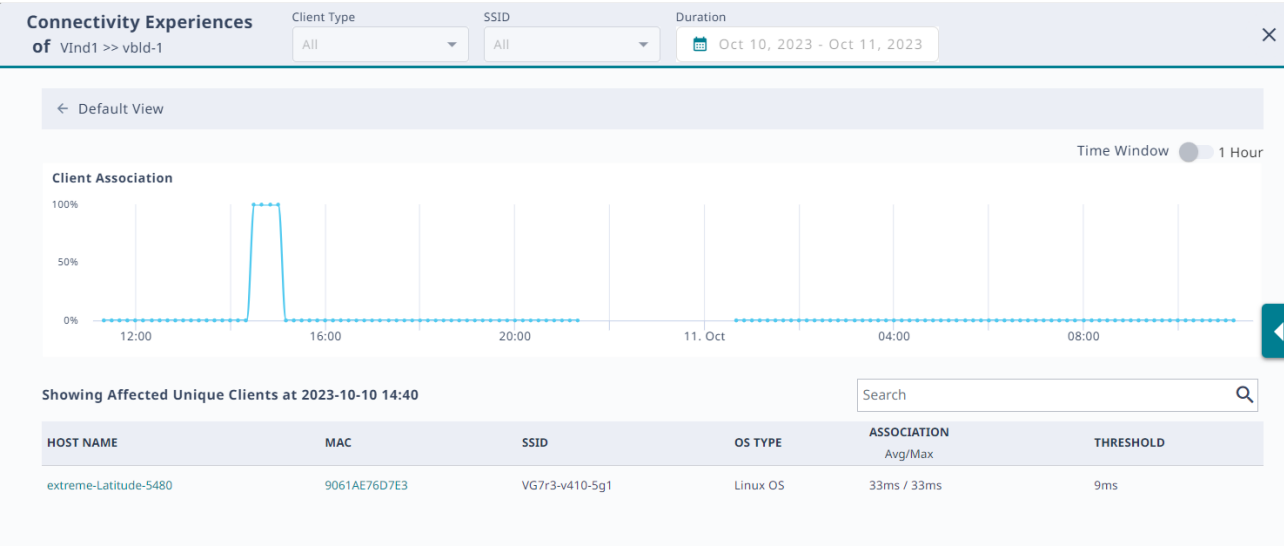


Figure 50: Client Association Panel

To zoom in, drag and select a time period. To zoom back out, select **Reset zoom**. To return to the **Default View**, select the back arrow.

Mouse over a point on the graph to see the following information:

- Date and time stamp
- Total Unique Clients
- Time to Associate
- Clients Above Association Threshold

For more information, select a point on the graph for which there are clients above the association threshold. The table updates to show the affected unique clients. To open the connection details panel, select the link from the **HOST NAME** or the **MAC** column.

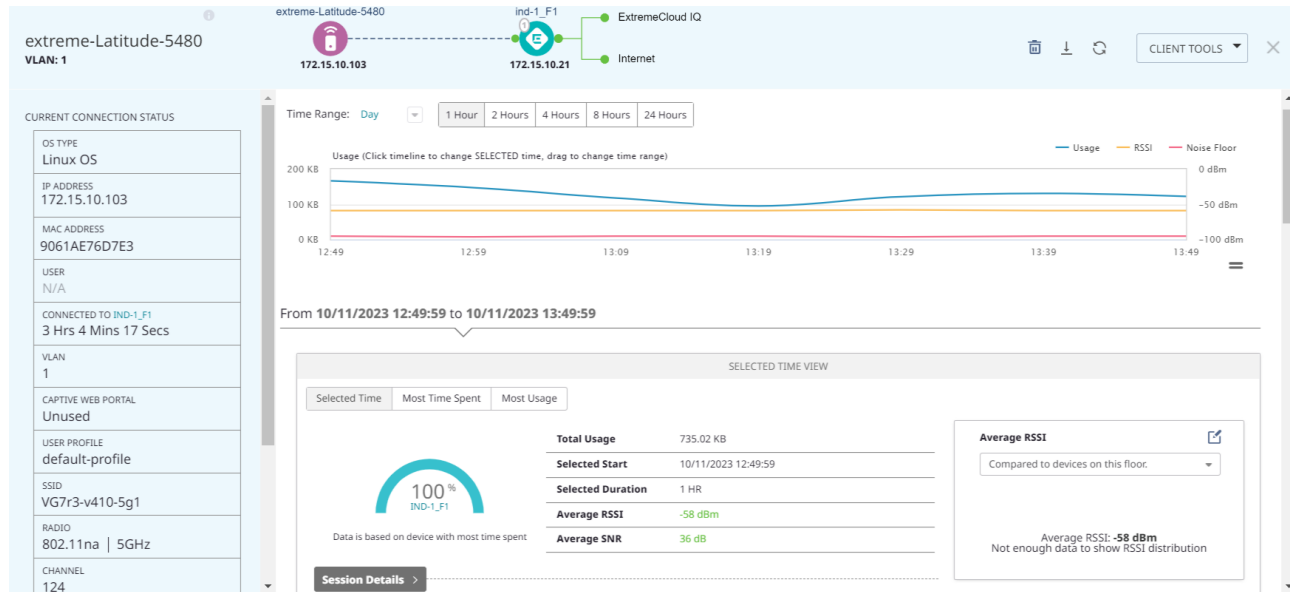


Figure 51: Connection Details Panel

Related Links

[Connectivity Experiences](#) on page 585

[Connectivity Experiences Panel \(Wireless\)](#) on page 588

Client Authentication (Wireless)

Mouse over a point in the **Client Authentication** graph to see a summary of the following information:

- Date and time stamp
- Total Unique Clients
- Time to Associate
- Clients Above Association Threshold
- Time to Authenticate
- Clients Above Authentication Threshold
- Time to Obtain IP Address
- Clients Above DHCP Threshold

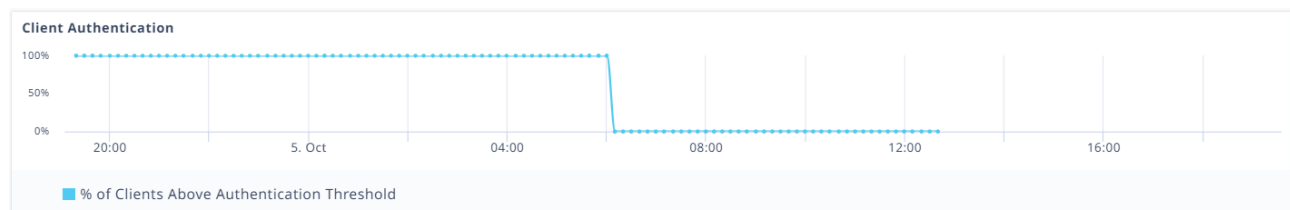


Figure 52: Client Authentication

To open the **Client Authentication** panel and see more details, select a point on the graph.

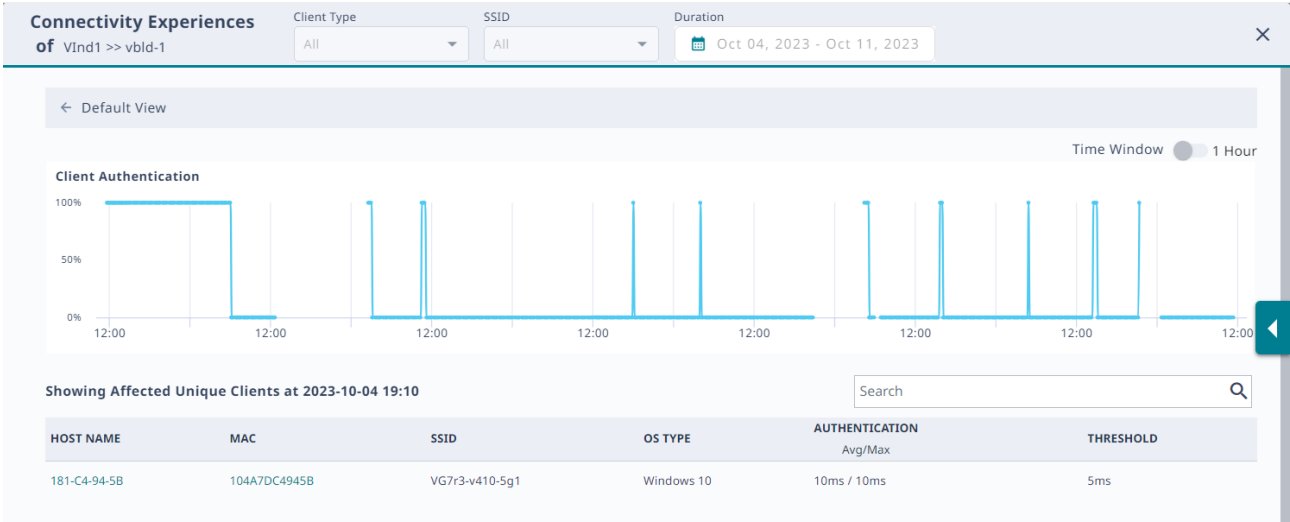


Figure 53: Client Authentication Panel

To zoom in, drag and select a time period. To zoom back out, select **Reset zoom**. To return to the **Default View**, select the back arrow.

Mouse over a point on the graph to see the following information:

- Date and time stamp
- Total Unique Clients
- Time to Authenticate
- Clients Above Authentication Threshold

For more information, select a point on the graph for which there are clients above the association threshold. The table updates to show the affected unique clients. To open the connection details panel, select the link from the **HOST NAME** or the **MAC** column.

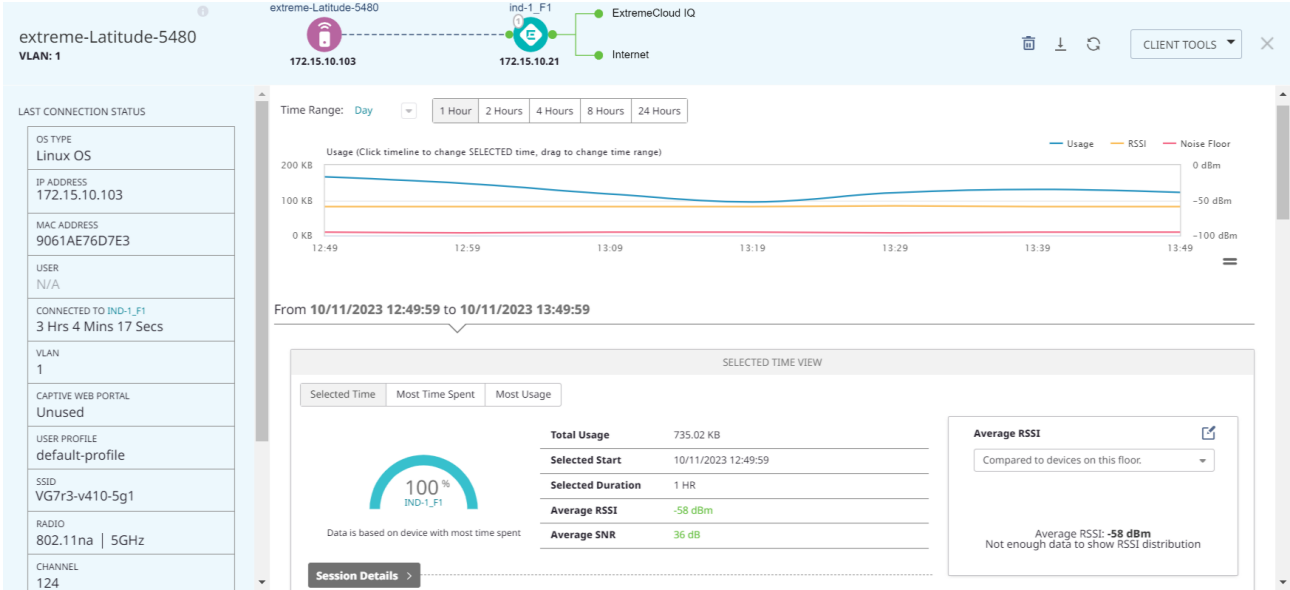


Figure 54: Connection Details Panel

Related Links

- [Connectivity Experiences Panel \(Wireless\)](#) on page 588
- [Connectivity Experiences](#) on page 585

Time to Obtain IP Address (Wireless)

Mouse over a point in the **Time To Obtain IP Address** graph to see a summary of the following information:

- Date and time stamp
- Total Unique Clients
- Time to Associate
- Clients Above Association Threshold
- Time to Authenticate
- Clients Above Authentication Threshold
- Time to Obtain IP Address
- Clients Above DHCP Threshold

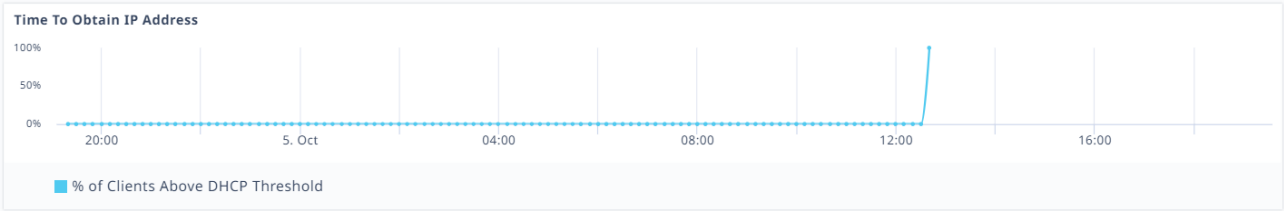


Figure 55: Time To Obtain IP Address

To open the **Time To Obtain IP Address** panel and see more details, select a point on the graph.

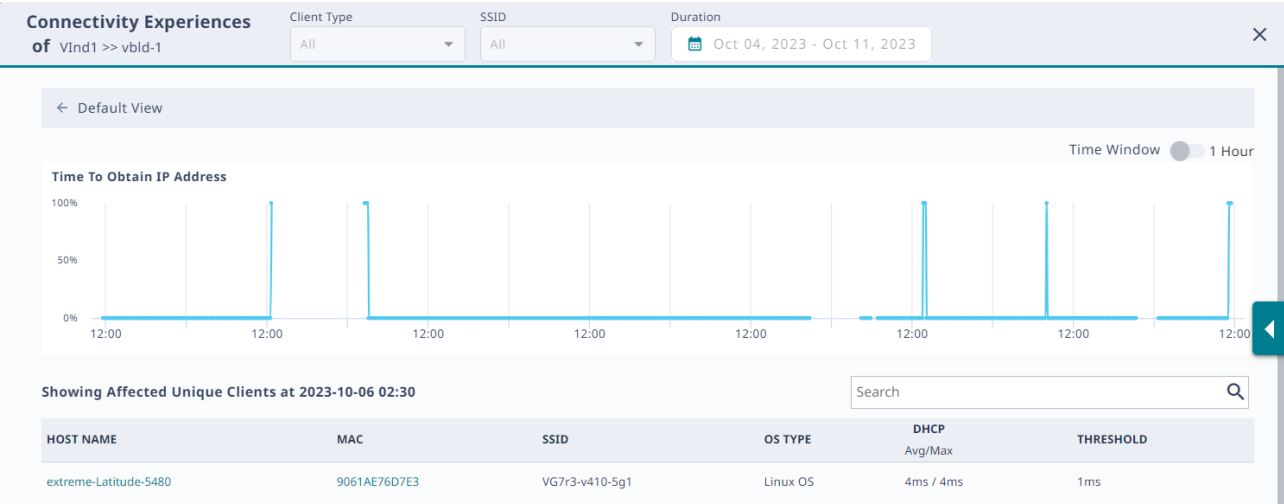


Figure 56: Time To Obtain IP Address Panel

To zoom in, drag and select a time period. To zoom back out, select **Reset zoom**. To return to the **Default View**, select the back arrow.

Mouse over a point on the graph to see the following information:

- Date and time stamp
- Total Unique Clients
- Time to Obtain IP Address
- Clients Above DHCP Threshold

For more information, select a point on the graph for which there are clients above the association threshold. The table updates to show the affected unique clients. To open the connection details panel, select the link from the **HOST NAME** or the **MAC** column.

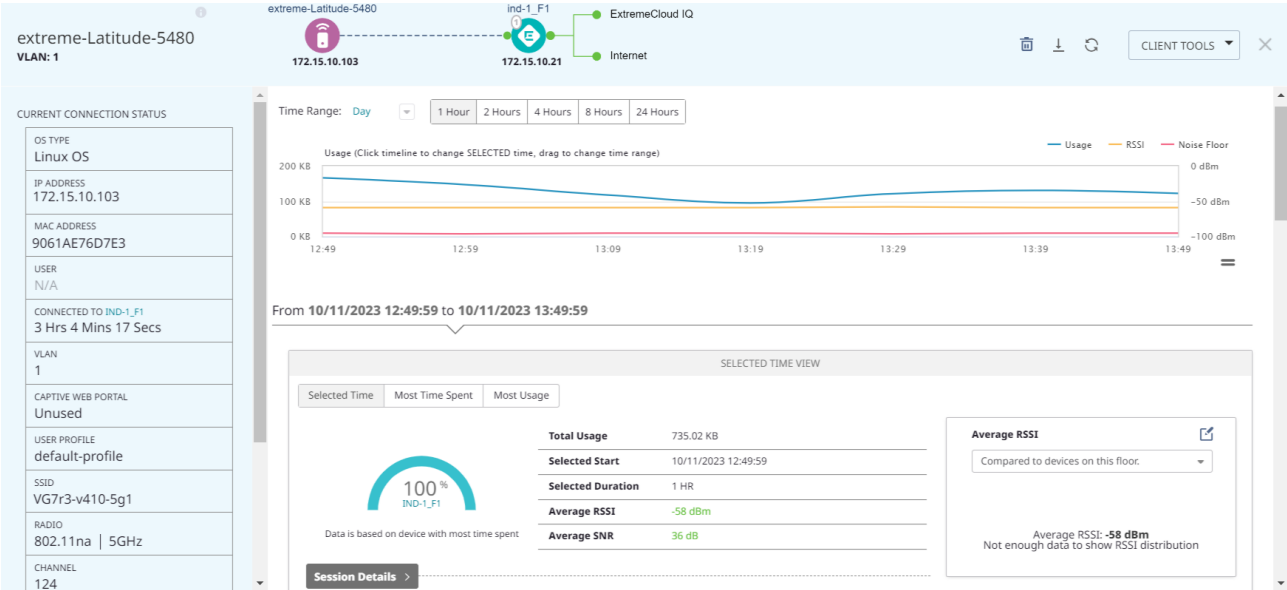


Figure 57: Connection Details Panel

Related Links

[Connectivity Experiences Panel \(Wireless\)](#) on page 588

[Connectivity Experiences](#) on page 585

Connectivity Experiences Panel (Wired)

To open the **Connectivity Experiences** panel for a site, select the site. To zoom in, drag and select a time period on the **Quality Index** graph. To zoom back out again, select **Reset zoom**.

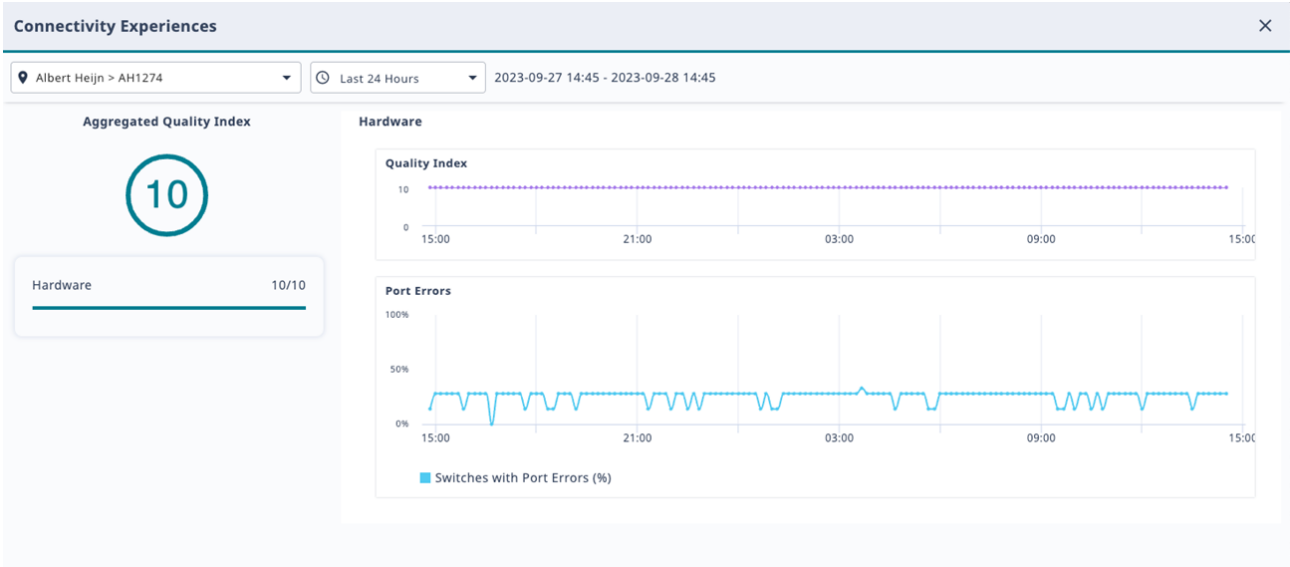


Figure 58: Connectivity Experiences Panel (Wired)

To see high-level information about a port error, mouse over a point in the **Port Errors** graph.

To open the detailed **Port Errors** panel, select the **Port Errors** graph.

Related Links

- [Port Errors](#) on page 595
- [Connectivity Experiences](#) on page 585

Port Errors

To zoom in on the **Port Errors** graph, drag and select a time period.

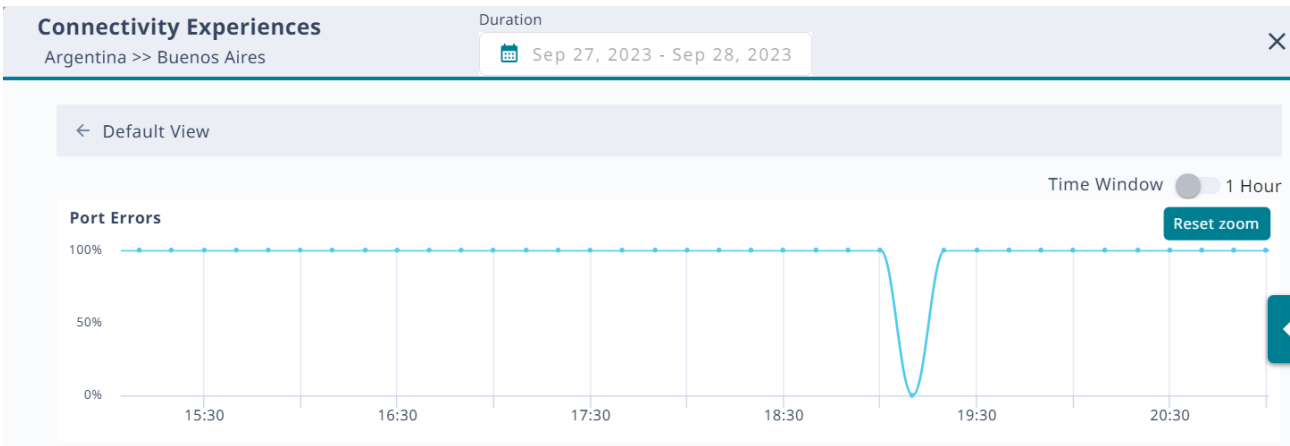


Figure 59: Port Errors

To zoom back out again, select **Reset zoom**. To return to the **Default View**, select the back arrow.

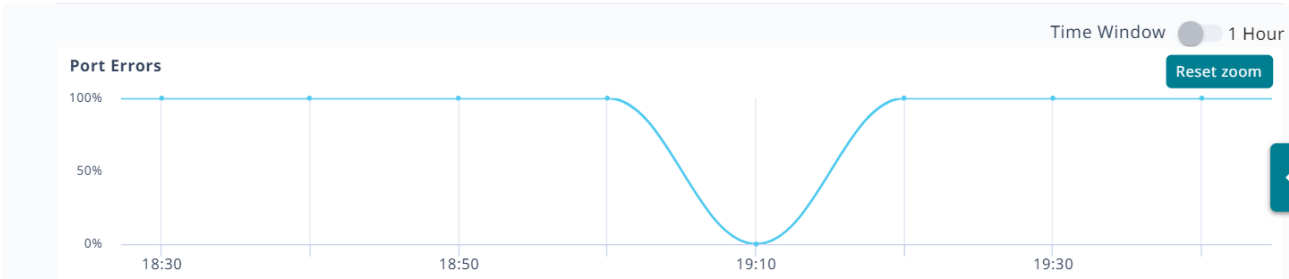


Figure 60: Port Errors Zoom

Select a point on the **Port Errors** graph to update the table with relevant information.

Showing Affected Ports at 2023-09-28 03:40

HOST NAME	SERIAL NUMBER	MGT IP ADDRESS	PORT	IN-ERRORS Avg/Max
Acme1274sw-05	2044N-43364	10.152.236.55	5	0.11% / 0.11%
Acme1274sw-05	2044N-43364	10.152.236.55	6	0.11% / 0.11%
Acme1274sw-04	2044N-43433	10.152.236.54	7	0.27% / 0.27%

Figure 61: Affected Ports Table

The system calculates the metrics that appear in the graph and in the table over a 10-minute period. To change the period to one hour, select the **Time Window** toggle.

Search the table by host name, MAC address, SSID, or operating system (OS).

Related Links

[Connectivity Experiences Panel \(Wired\)](#) on page 594

Anomalies

The **Anomalies** tab uses the following interactive widgets and a [table](#) to display information about anomalies:

- [Top Anomalies by Site Widget](#) on page 598
- [Anomalies by Severity Widget](#) on page 598
- [Top Anomalies by Type Widget](#) on page 599

To hide the widgets and display a streamlined view of **Anomalies by Severity**, select .

To display the widgets again, select .

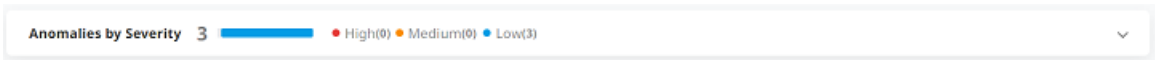


Figure 62: Anomalies by Severity Streamlined View

Use the controls found at the top of the page to customize your view of the widgets and the table:

Site

Display all sites (default) or select a specific site from the menu. You can search the menu for a site.

Severity

Display all severity levels (default) or select a severity level from the menu.

Anomaly Type

Display all anomaly types (default) or select a type of anomaly from the menu.

Duration

Display anomalies for the past 24 hours (default), the past 7 days, or for a custom period. Select up to 7 days, from 90 days of historical data.

Exclude Muted

Toggle to hide or display previously muted anomalies.

Trends

Display the **Anomaly Trends** graph that shows anomalies for all sites and severities for the past 90 days.

Refresh

Refresh the display by selecting .

Related Links

[Top Anomalies by Site Widget](#) on page 598

[Anomalies by Severity Widget](#) on page 598

[Top Anomalies by Type Widget](#) on page 599

[Anomaly Trends](#) on page 611

Instant Anomaly Detection

CoPilot provides instant anomaly detection, so no tuning is required. Instant anomaly detection provides the following benefits:

- Automatically applies and updates the historical data for newly added or licensed devices.
- CoPilot aggregates and correlates historical and latest data streams.
- Algorithms identify normal patterns and establish dynamic baselines.
- To reduce bias and false positives, CoPilot determines dynamic baselines by considering local and regional values.
- CoPilot identifies anomalies at multiple levels: local device, installed location, associated devices, and across multiple sites.

Top Anomalies by Site Widget

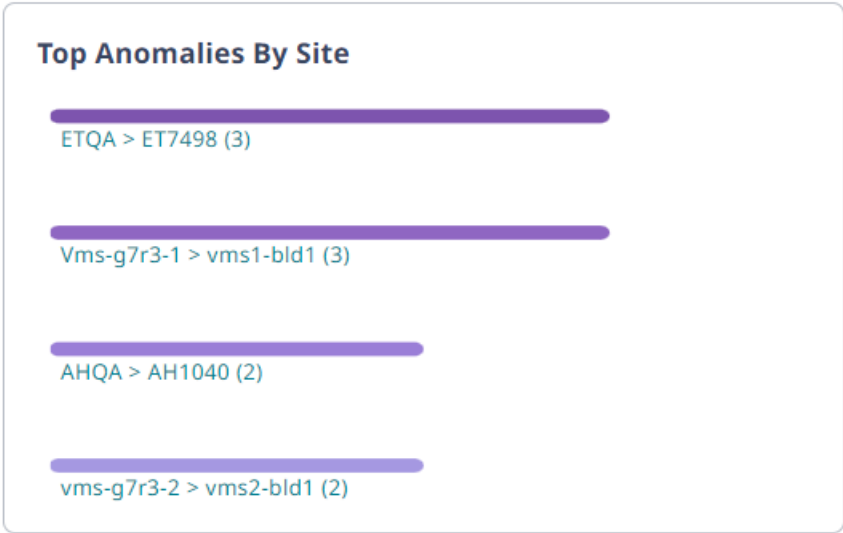


Figure 63: Top Anomalies By Site

The **Top Anomalies By Site** widget shows the sites with the most anomalies. Select a site in the widget to view only the anomalies for that site. The other widgets and the table update to show only the anomalies for the selected site.

Related Links
[Anomalies](#) on page 596

Anomalies by Severity Widget

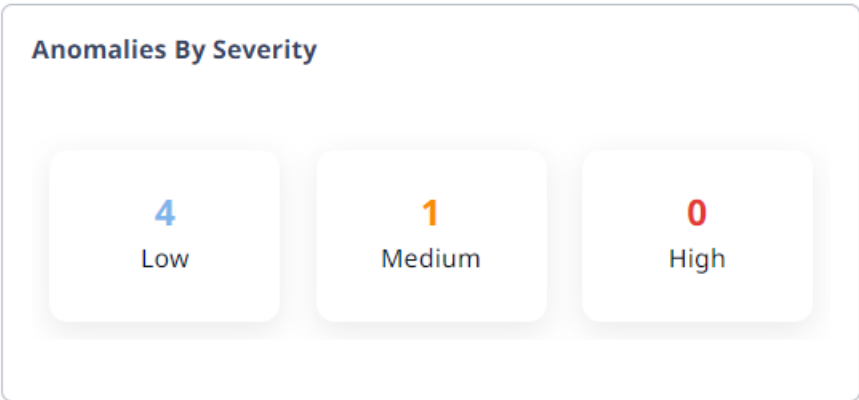


Figure 64: Anomalies By Severity

The **Anomalies By Severity** widget shows the number of anomalies for each severity level. Select a level to display only the anomalies of that severity. The other widgets and the table update to show only anomalies of the selected severity.

Related Links
[Anomalies](#) on page 596

Top Anomalies by Type Widget

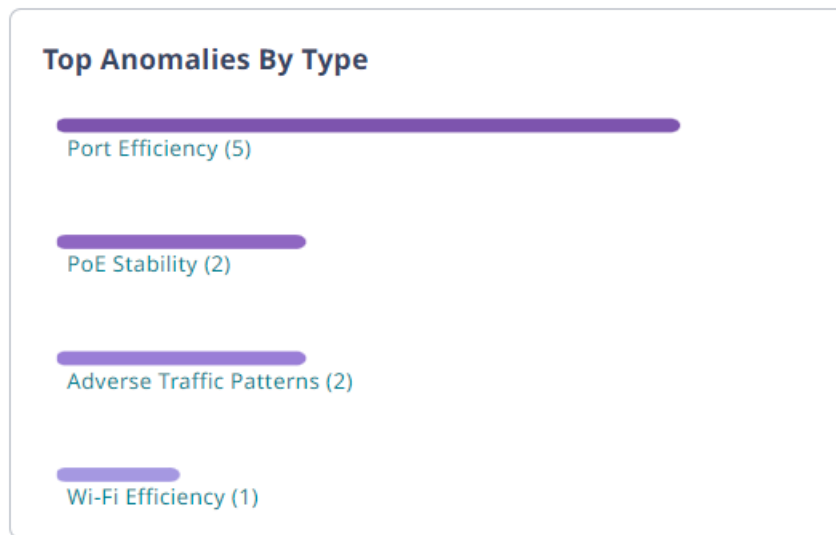


Figure 65: Top Anomalies By Type

The **Top Anomalies By Type** widget shows the most common types of anomalies for your network. From the menu, select an **Anomaly Type** to display only anomalies of that type. The other widgets and table update to display only anomalies of that type.

Related Links

[Wi-Fi Efficiency](#) on page 599
[Wi-Fi Capacity](#) on page 599
[PoE Stability](#) on page 600
[DFS Recurrence](#) on page 604
[Port Efficiency](#) on page 604
[Adverse Traffic Patterns](#) on page 605
[Hardware Health](#) on page 605
[Missing VLANs](#) on page 606
[Anomalies](#) on page 596

Wi-Fi Efficiency

Wi-Fi efficiency anomalies are related to wireless communication between clients and APs. For more information about packet data anomalies, select a location (site) that has a Wi-Fi efficiency anomaly. You can sort the data by location, severity, and most recent occurrence.

Related Links

[Top Anomalies by Type Widget](#) on page 599

Wi-Fi Capacity

Wi-Fi capacity anomalies are related to access point (AP) capacity and airtime usage. You can sort the data by location, severity, and most recent occurrence. This data contains statistical information such as client connection duration and the channel

utilization information related to wireless APs. Wi-Fi capacity anomaly reports include the follow information:

- Total time a channel was in use.
- Total time peak usage for the channel was 80% or higher.
- The total number of peak and non-peak intervals (80% or more) recorded on the channel.
- The average number of clients during peak and non-peak intervals.
- The average total TX and RX usage during peak and non-peak intervals.
- The average interference during peak and non-peak intervals.
- An indication of whether or not the channel is anomalous.
- An indication of the severity of the anomaly (low, medium, high, or null).
- Date and time of the analysis (typically over the last 24 hours).
- The Regional Data Center (RDC) from which the data was obtained.

Related Links

[Top Anomalies by Type Widget](#) on page 599

PoE Stability

Access Points (AP) commonly receive power through an Ethernet backhaul cable connection to an upstream switch. This method is known as Power over Ethernet or PoE. When an AP boots, it selects a power mode based on the available PoE protocols. The AP can start with PoE and move to PoE+ after a brief interval. It uses the selected power mode until it reboots.

Table 143: PoE Standards

Standard	Description
PoE (AF)	IEEE 802.3af
PoE+ (AT)	IEEE 802.3at
PoE++ (BT)	IEEE 802.3bt

PoE stability anomalies are related to sudden changes in power draw. Data is presented over a 48-hour period, and includes date and time details. When an AP negotiates down to AF, even though it requires AT or a higher level for optimal performance and full capacity, CoPilot reports a PoE anomaly.

The severity definitions for PoE anomalies are based on the average number of clients connected to an AP on a given day. If there are fewer than 10 clients, the anomaly severity is considered low. If there are 50 or more clients on a given day, the severity level is considered high. If there are between 10 and 50 clients, the severity level is considered medium.

Occasionally, poorly installed cabling or MDU closet wiring, lack of power on the upstream switch, or a failing power supply on either the AP or the switch might cause APs to cycle through power modes, while never reaching a steady state.

To open the **PoE Stability Anomaly** panel, select a location (site), for which anomalies have been detected, from the table. To view more information about an anomaly, select the corresponding down arrow. The **PoE Stability Anomaly** panel includes the following information:

Header

This section provides general information about the anomaly.

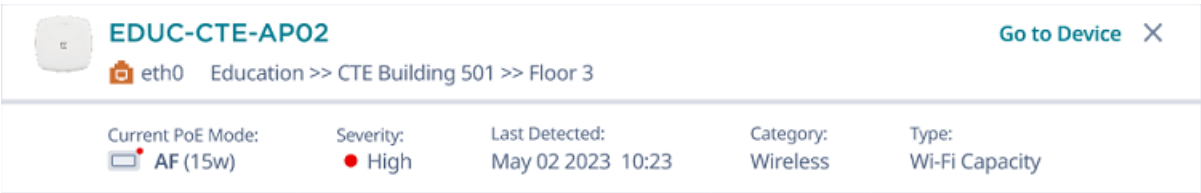


Figure 66: PoE Stability Anomaly Header

The **Current PoE Mode** shows whether the affected device is online and the current power mode—AF, AT or BT. If the AP is offline, the status is **Disconnected**.

To get more information about the device, select **Go to Device**.

Issue

This section provides a description of the problem, including the actual PoE mode and the desired PoE mode.

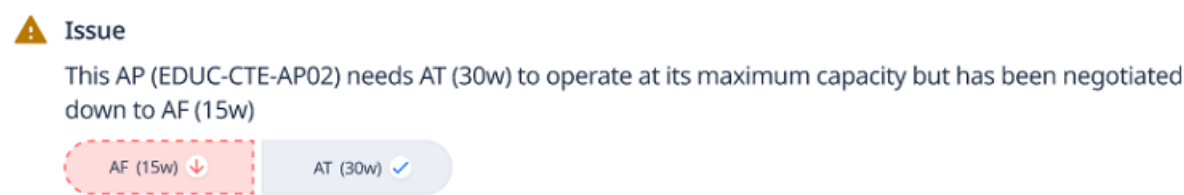


Figure 67: Issue

Impact

This section describes the effect the anomaly has on the system, for example: *Lower coverage and performance in the coverage area*

Recommendation

This section provides steps to resolve the anomaly, for example:

1. Verify whether there is sufficient PoE budget on the upstream switch.
2. Verify that the network cable length is not beyond 100 meters (328 feet), is properly connected to the AP, and that the cable does not have any signs of damage.

PoE Trend

The **PoE Trend** graph shows the pattern of changes in PoE mode for the 48 hours prior to the last detected timestamp. To view the graph, select the down arrow.

The graph indicates the three power modes: AF, AT and BT Type 3. Red indicates a low power mode.

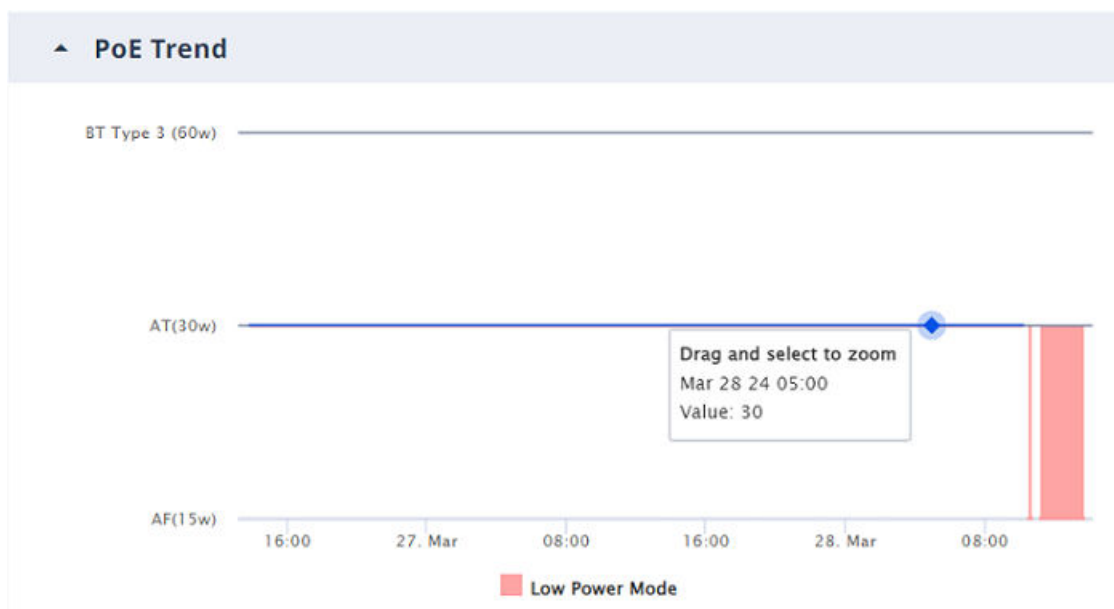


Figure 68: PoE Trend

Select and drag across the timeline to zoom in on a section. Select **Reset zoom** to return to view the entire timeline.

Neighboring Devices

If LLDP is enabled on the AP, the **Neighboring Devices** section provides useful information for troubleshooting power sourcing equipment, and nearby APs connected to the affected AP. To expand this section, select the down arrow.



Note

If LLDP is enabled and the upstream device is an Extreme switch managed by the current VIQ, the **Upstream System Name** value appears as a link that opens the D360 page for the switch.

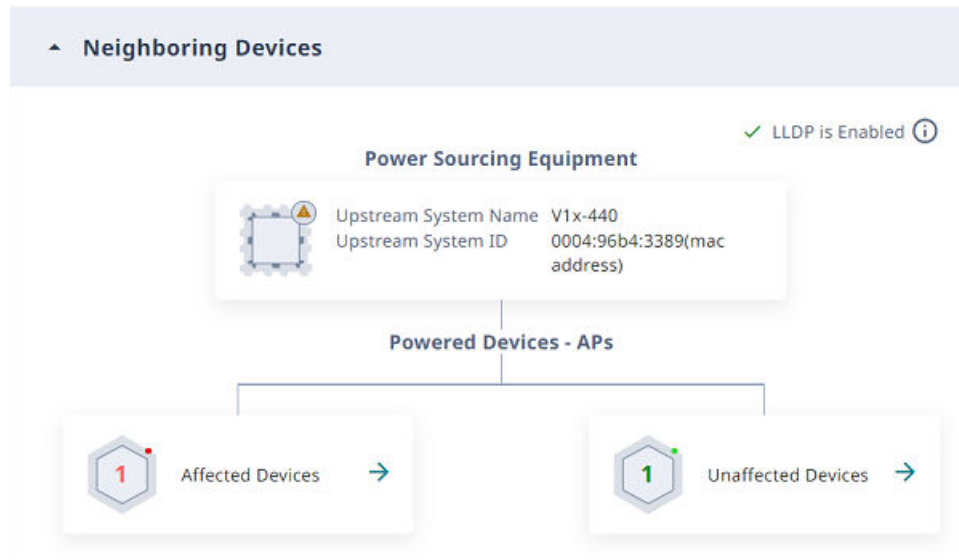


Figure 69: Neighboring Devices

Select **Affected Devices** to view a list of devices affected by the anomaly. ExtremeCloud IQ icons indicate whether the affected device is the current access point, or a neighboring access point.

Select **Unaffected Devices** to view a list of devices not affected by the anomaly.

The device lists include the following details when LLDP is enabled:

- **AP Name** (**Host Name** when LLDP is disabled)
- **AP Model** (**Product Type** when LLDP is disabled)
- **AP Interface** (**Interface** when LLDP is disabled)
- **PSE Port** (**Port** when LLDP is disabled)
- **Last Detected Time** (only for affected devices)

If LLDP is not enabled, ExtremeCloud IQ reports the affected building and the floor, the number of devices affected by the anomaly, and the number of devices not affected.

The device lists include the following details when LLDP is enabled:

- **Host Name**
- **Product Type**
- **Interface**
- **Port**
- **Last Detected Time** (only for affected devices)

Related Links

[Top Anomalies by Type Widget](#) on page 599

DFS Recurrence

Dynamic Frequency Selection (DFS) recurrence anomalies are related to radar-influenced channel changes. When an access point switches channels, the quality of service for connected clients might decrease temporarily, while repeated channel changes might degrade the client experience for extended periods of time.

When an AP detects a radar pulse on the DFS channel it is using, regulations require that it switch to a non-DFS channel for at least 30 minutes. This widget identifies APs that repeatedly switch from a wireless channel within the DFS range (channels 50-144, inclusive) to a channel outside the range because it detects third party radar pulses.

ExtremeCloud IQ records the DFS channels that are affected by radar pulses. Radar is usually not in use across the entire DFS channel range (50-144). If ExtremeCloud IQ determines that only a subset of the range is in use, you can disable only those channels. The AP continues to use DFS channels that are not affected by radar. If ExtremeCloud IQ determines that the entire range of DFS channels is affected, the best practice is to completely disable DFS for the affected AP.

The severity of a DFS anomaly is classified as being:

- High—Many (more than 12) radar events in the past 24 hours
- Medium—Moderate (8-12) number of radar events in the past 24 hours
- Low—Small (5-8) number of radar events in the past 24 hours

Related Links

[Top Anomalies by Type Widget](#) on page 599

Port Efficiency

Port efficiency anomalies identify wired and wireless device interfaces that are not making efficient use of the uplink backhaul connection. This inefficiency might occur in the following scenarios:

- An interface might only use half-duplex communication—only 50% of the available throughput capacity.
- An interface might occasionally flip between full-duplex and half-duplex modes. If this happens too often, it indicates that the interface cannot maintain a full-duplex connection and is considered an anomaly.
- An interface might use an inefficient data rate relative to its capability. Allowable data rates are 10 Mbps, 100 Mbps, 1000 Mbps, 2500 Mbps, 5000 Mbps, and 10000 Mbps. A data rate of 10 Mbps is considered inefficient, while 100 Mbps and higher data rates are considered normal.
- An interface might occasionally flip between data rates, for example, from 2500 Mbps to 1000 Mbps. When this happens on a regular basis, it indicates that there is a wider issue preventing the interface from maintaining the higher data rate.

To display the following graphs, select a site with a **Port Efficiency** anomaly:

- Port Supported Speed and Full/Half Duplex Negotiation

- Number of Changes (Speed or Duplex)



Note

The **Number of Changes** graph appears only for the following anomaly types:

- Wired and wireless duplex mode anomalies
- Wired and wireless data rate inconsistency anomalies
- Anomalies that are a combination of duplex mode or data rate inconsistency and sub-optimal anomalies

Related Links

[Top Anomalies by Type Widget](#) on page 599

Adverse Traffic Patterns

Adverse traffic patterns are caused by TX and RX traffic loads that result in high resource use of multicast and broadcast communications. The use of multicast and broadcast requires devices to clone packets, which reduces CPU availability. This is usually not a problem, unless the traffic load begins to exceed the available CPU capacity. The CPU threshold for APs is 90%. The CPU threshold for switches is 50%. Exceeding the CPU capacity can increase latency and packet loss, and might even bring a device down.

Related Links

[Top Anomalies by Type Widget](#) on page 599

Hardware Health

Each of the following conditions triggers a hardware health anomaly.

Table 144: Anomalous hardware conditions

Condition	Threshold
Non-user initiated reboots	More than 5 in 1 hour
Non-user initiated reboots	More than 10 in 24 hours
CPU utilization	Average CPU usage greater than 90% for 10 minutes
Memory usage	Average memory usage greater than 90% for 10 minutes

To open the **Hardware Anomaly** panel, select a device, for which anomalies have been detected, from the table. The panel includes the following information:

Header

This section provides general information about the anomaly. To get more information about the device, select **Go to Device**.

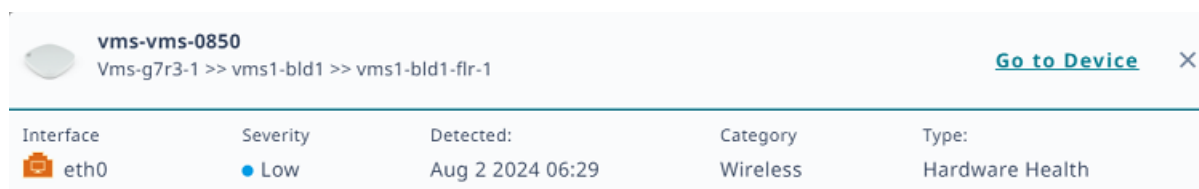


Figure 70: Hardware Health anomaly header

Issue

This section identifies the condition for which the threshold was met, for example:

<name of device> memory utilization is consistently above 90%.

Recommended Actions

This section provides steps to resolve the anomaly, for example:

Identify the process or service causing high memory usage using the CLI command 'show memory detail'.

Time Series Analysis

This section presents relevant synchronized time series graphs. Expand the section to see the graphs. To choose which graphs to display, select **Select Additional Charts**.

Table 145: Additional charts

Chart	Display on hover	Expand on select
Total Throughput	Total throughput	Detailed chart showing: total, unicast tx, rx, broadcast tx, rx and multicast tx, rx traffic
Total Client Count	Total number of clients	Client details: MAC, client hostname, client OS
Reboot	Reboot code and reason	None
PoE Mode	AP PoE power mode	None
Device Temperature	AP temperature	None
CPU Utilization	Percentage of CPU utilization	CLI output for show system process state
Memory Utilization	Percentage of memory utilization	CLI output for show memory detail

Missing VLANs

ExtremeCloud IQ detects VLANs that are configured on the APs, but missing on the upstream switch, even if the upstream switch is not managed. All AP3XXX and AP5XXX models support this feature.

To trigger a Missing VLANs anomaly, clients must attempt to connect to the SSID.

Sometimes VLANs are intentionally missing, for example: black hole VLANs. You can [manually exclude](#) them.

LLDP Enabled

When LLDP is enabled, the anomaly includes the following information:

- The VLAN IDs missing on the APs
- The name of the upstream switch
- The switch ports the APs are connected on
- A **Go to Device** link, if the switch is managed by XIQ

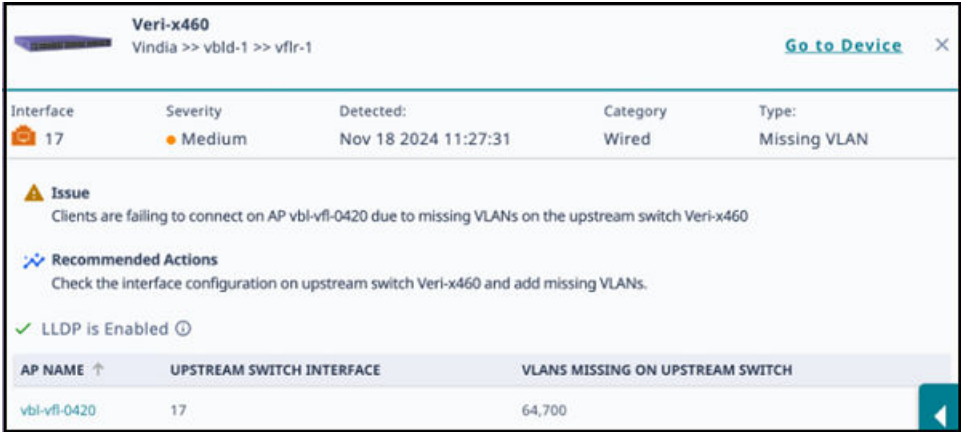


Figure 71: Missing VLAN anomaly with LLDP enabled

LLDP Disabled

When LLDP is disabled, the anomaly includes the following information:

- The VLAN IDs missing on the APs
- The name of the upstream switch approximated from the floor name

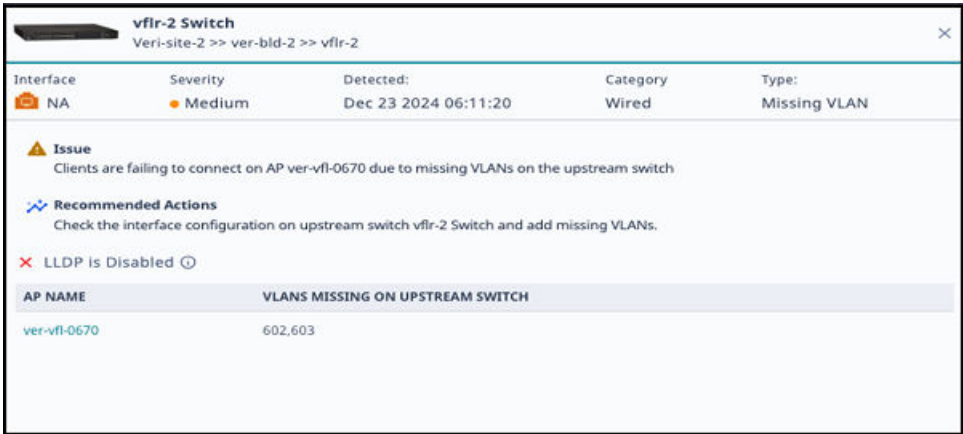


Figure 72: Missing VLAN anomaly with LLDP disabled

Related Links

[Exclude Missing VLANs](#) on page 608

Exclude Missing VLANs

Use this task to manually specify VLANs to exclude from Missing VLANs anomaly detection.

1.

Go to **CoPilot > Anomalies**, and select .
2.

Select an existing Excluded VLAN ID, and then select , or select .
3.

Select **Manual**.

Alternatively, select CSV Import and choose a CSV file. To dismiss existing false positives for the VLAN that you want to exclude, select **Dismiss existing Missing VLANs**.
4.

In the **Excluded VLANs** field, type the VLAN IDs to exclude, separated by a comma after each ID.
5.

From the **Exclude from Sites** menu, select the corresponding check box for each site from which you want to exclude the VLANs specified in Step 4.
6.

Select **ADD**.

Related Links

[Missing VLANs](#) on page 606

Anomalies Table

The **Anomalies** table is interactive, and displays the following information for each anomaly:

- **Device**
- **Interface**
- **Severity**
- **Issue**
- **Site**
- **Category**
- **Type**
- **Muted**



Note
This column appears only when the **Exclude Muted** toggle is off. The possible values for this column are **Yes** and **No**.

- **Last detected**

☐	DEVICE	INTERFACE	SEVERITY	ISSUE	SITE	CATEGORY	TYPE	DETECTED 
☐	AH1-AH1-0015	 eth0	 Low	AH1-AH1-0015 Port Efficiency issue eth0. Anomaly Type : Port negotiated sub-optimal speed - 100. Port negotiated half duplex.	AHQA >> AH1003 >> AH1003-Store	Wireless	Port Efficiency	Apr 15 2024 10:19
☐	v305c-19090	 eth0	 Low	v305c-19090 Port Efficiency issue eth0. Anomaly Type : Port negotiated sub-optimal speed - 100. Port negotiated half duplex.	Vms-g7/3-1 >> vms1-bld1 >> vms1-bld1-flr-1	Wireless	Port Efficiency	Apr 15 2024 10:19
☐	v410-74C0	NA	 Low	This AP v410-74C0 needs at least AT (30w) power to operate at its maximum capacity but has been negotiated down to AF (15w) power.	vms-g7/3-2 >> vms2-bld1 >> vms1-bld1-flr-1	Wireless	PoE Stability	Apr 15 2024 10:19
☐	AH1-AH1-	 5 GHz	 Medium	AH1-AH1-0015 is nearing its wireless capacity on channel 36 in 5 GHz due to high airtime utilization	AHQA >> AH1003 >> AH1003-Store	Wireless	Wi-Fi	Apr 15 2024

Items per page:

50

1 - 5 of 5



Figure 73: Anomalies

You can display the anomalies in ascending or descending order by column, except for the **Interface** column. You can also search for anomalies by device, issue, site, or anomaly type. Use the **Items per page** menu to specify the maximum number of results to show, per page.

To download a CSV file that contains the same information, select .

Some recurring anomalies are not problematic and you can mute or dismiss them. Select the corresponding check boxes for these anomalies, and then select ... > **Mute** or ... > **Dismiss**.

Mute

Hide the selected anomaly when **Exclude Muted** is enabled. To display muted anomalies, disable **Exclude Muted**.



Note

When **Exclude Muted** is enabled, all existing and future anomalies of the selected type and location are hidden. For example, muting a PoE Stability anomaly for Site A hides all current and future anomalies of the PoE stability type for Site A.

Dismiss

Remove the selected anomaly from the table. This action does not affect other current or future anomalies of the same anomaly type.

Related Links

[Anomaly Information for a Device](#) on page 609

[Anomalies](#) on page 596

Anomaly Information for a Device

Select a device to open a panel with detailed information about the anomaly, including a description of the issue and recommended actions for resolution. To open the page for the device, select **Go to Device**.

The panel graphs display up to 3 days worth of data, including the 48 hours prior to the time stamp for the last detected anomaly.

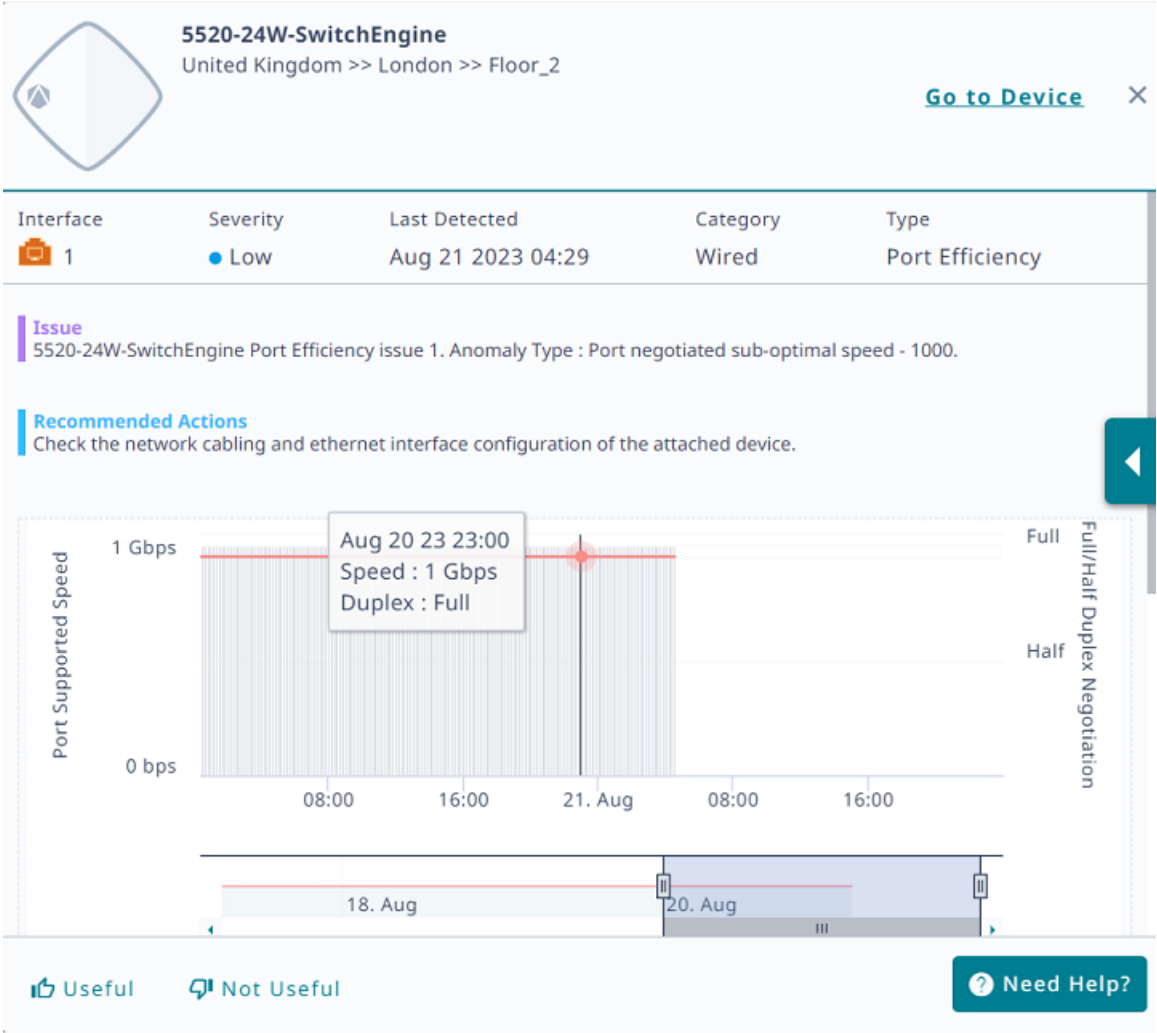


Figure 74: Detailed Information

If you find the detailed information helpful, select **Useful**. If you did not find the information helpful, select **Not Useful**. To get help, select **Need Help**.

Select a bar to see details; select a bar and drag along the timeline to show data for a range of time.

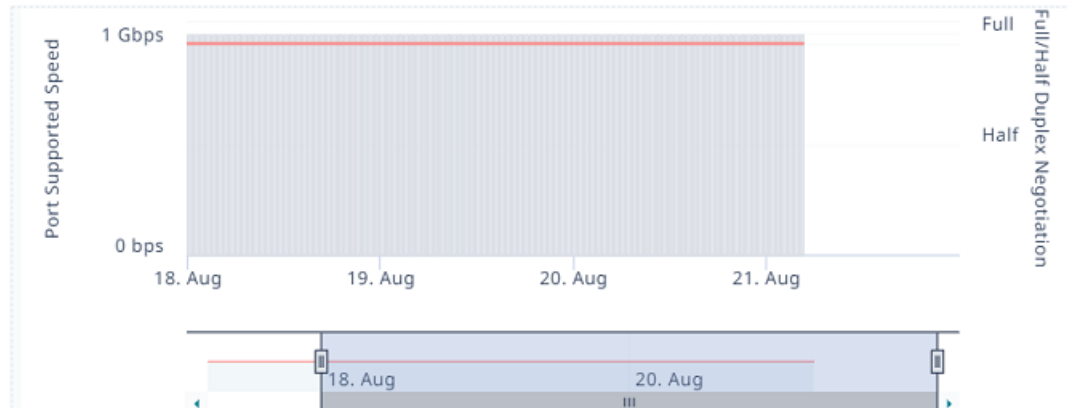


Figure 75: Detailed Information for Specific Days

Related Links

[Anomalies Table](#) on page 608

Submit a Support Ticket

You can trigger ExtremeCloud IQ to open a support ticket if an issue cannot be resolved using the data provided by Insights. ExtremeCloud IQ collects data from the Insight and attaches an output report from the affected device to send to GTAC.

Select **Need Help** and follow the instructions.



Note

This option is only available for devices covered by an ExtremeWorks maintenance contract.

Anomaly Trends

To open the **Anomaly Trends** graph, go to **CoPilot > Anomalies** and select **Trends**.

Mouse over a bar in the timeline to see the date and types of anomalies identified for that day.

View all anomalies (default) or select a specific **Anomaly Type** from the menu. You can drag along the graph to zoom in on a time period, and then select **Reset Zoom** to zoom back out.

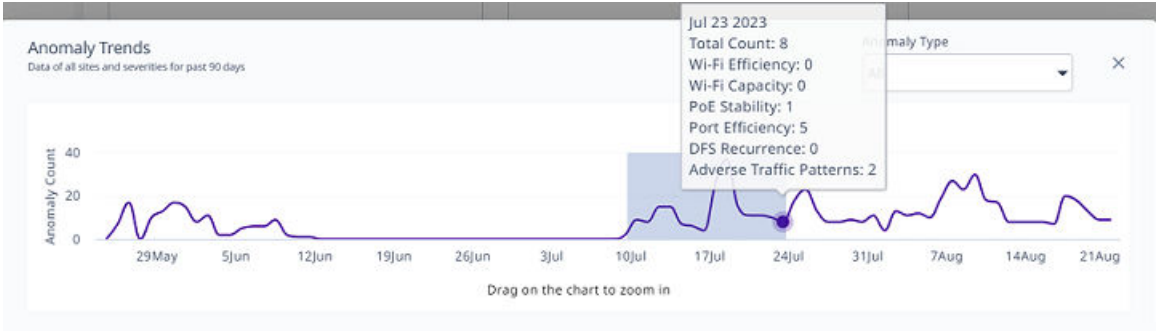


Figure 76: Anomaly Trends graph

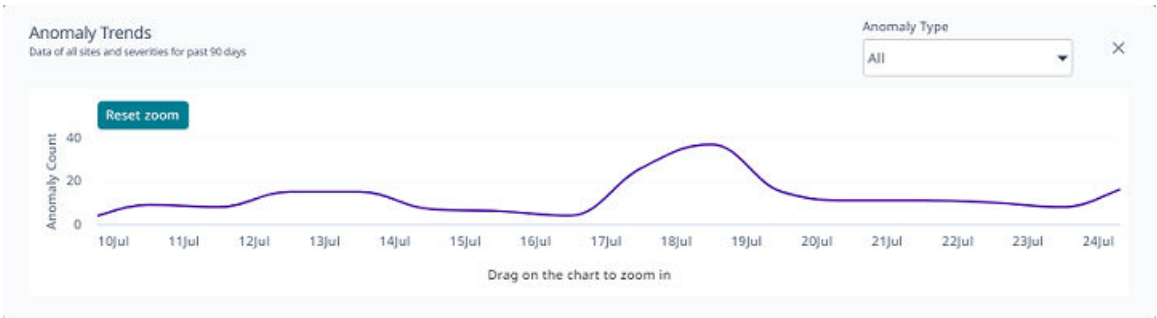


Figure 77: Anomaly Trends graph, zoomed in view

Related Links

[Anomalies](#) on page 596