



ExtremeCloud IQ User Guide

June 2023



Copyright © 2023 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: www.extremenetworks.com/company/legal/trademarks

Open Source Declarations

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

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



Table of Contents

Preface.....	ix
Conventions.....	ix
Text Conventions.....	ix
Documentation and Training.....	xi
Send Feedback.....	xi
Help and Support.....	xi
Subscribe to Product Announcements.....	xii
AP Regulatory Information.....	xii
Welcome to ExtremeCloud IQ.....	13
Onboarding.....	14
Add Devices Overview.....	14
Quick Add Devices.....	15
Add Locally Managed Devices.....	17
Add Devices with Advanced Onboarding.....	18
Administration.....	20
About Global Settings.....	20
Manage Account Details.....	21
Enable Two-Factor Authentication.....	21
Enable ExtremeCloud IQ Classic.....	22
Add a Credential Distribution Group.....	22
Add an Organization.....	23
Add an Admin Account.....	23
View Licenses.....	25
Manage Licenses.....	27
Set a Device Default Password.....	28
Manage the Virtual IQ.....	28
Set Email Notifications.....	30
Generate API Access Tokens.....	31
Add an API Presence and Data Location Feed.....	32
Add a Third-Party API Token.....	33
Alert Notifications.....	33
Download Log Information.....	34
Enable SSH Availability.....	39
Configure Applications and Users.....	40
Add a Custom Application.....	40
User Management.....	40
Add a User Group.....	41
Add Users to a User Group.....	42
Configure a Cloud User Group.....	43
Configure a Local User Group.....	45

Configure a Private Client Group.....	46
Locked Users.....	47
RADIUS Test.....	48
Unbind Device.....	49
Configure Network Policies.....	50
Add a Network Policy.....	51
Configure Policy Settings.....	52
Deploy a Network Policy.....	53
Configure a Standard Wireless Network (SSID).....	53
About SSID Usage in Standard Wireless Networks.....	56
Customize Wireless Network Optional Settings.....	60
Configure MAC Authentication.....	62
Customize Broadcast and Multicast Handling Settings.....	63
Customize DoS Prevention.....	64
Configure Voice Enterprise Options.....	65
Configure a Classification Rules Network Policy.....	66
Customize Advanced Access Security Settings.....	68
About RADIUS Authentication.....	70
Add a RADIUS Server Group.....	70
Configure RADIUS Server Settings.....	70
Configure an Extreme Networks Device as a RADIUS Proxy.....	72
Configure a RADIUS Proxy Server Realm.....	72
Configure Realm Settings.....	73
Add Approved RADIUS Clients.....	74
Configure an Extreme Networks Device as a RADIUS Server.....	74
Add an Active Directory Server.....	75
About Router Settings.....	76
Configure a Router Template.....	77
Configure Network and IP Address Allocation.....	80
About VPN Services.....	81
Configure an SD-WAN Route Group.....	87
Configure a Routing Policy.....	88
Configure URL Filtering Rules.....	90
Configure Dynamic DNS.....	91
Configure WAN Tracking.....	92
Configure Device Templates.....	92
Configure a Hive Profile.....	93
Configure Device Data Collection and Monitoring Options.....	95
Configure iBeacon Service.....	97
Configure Presence Analytics.....	98
Configure Common Objects.....	99
Configure AP Templates.....	101
Assign an Ethernet Port Profile.....	101
Configure Storm Control Settings.....	102
Configure STP Settings.....	103
Configure Wireless Interfaces for an AP Template.....	104
Configure Wired Interfaces for an AP Template.....	105
SES-Imagotag.....	106

Configure AP Device Template Advanced Settings.....	109
Fabric Attach.....	110
Configure Auto-Provisioning.....	111
Configure a Bonjour Gateway.....	113
Configure a Classification Rules Common Object.....	114
Add a Cloud Config Group.....	116
Configure Port Types.....	116
About Radio Profiles.....	117
Add a Radio Profile.....	118
About Radio Settings.....	119
Configure Backhaul Failover.....	121
About Channel Selection.....	121
Configure Neighborhood Analysis.....	124
About Client SLA Settings.....	124
Optimize Radio Usage.....	125
Configure Sensor Mode Scan Settings.....	126
Configure Outdoor Deployment.....	126
Configure RF Interface Reports.....	127
Configure WMM QoS Settings.....	127
Configure an SDR Profile.....	128
About SSIDs.....	128
About SSID Usage in Standard Wireless Networks.....	129
Add an Availability Schedule for User Profiles.....	133
Configure Switch Templates.....	134
Configure Switch Common Settings.....	135
Port Type Settings.....	136
Create a New Port Type.....	137
Configure Individual Ports.....	140
Configure Port Details.....	140
Configure Port Settings Parameters.....	141
Configure PSE Parameters.....	142
Configure Storm Control.....	143
Configure STP Parameters.....	143
Aggregate LAG and LACP Ports.....	144
Configure Supplemental CLI.....	144
Configure Switch STP Settings.....	145
About Switch Stacks.....	146
Configure Switch Device Template Advanced Settings.....	149
Configure URL Filtering Rules.....	150
Add a User Profile.....	152
Configure User Profile Security Settings.....	152
Configure Availability Schedule Settings.....	153
Configure User Profile Client SLA Settings.....	154
Configure User Profile Access Restrictions.....	154
Configure User Profile Traffic Tunneling Settings.....	155
Configure User Profile QoS Settings.....	156
Add Application Sets.....	157
About Client Mode Profiles.....	157

Configure a Client Mode AP Profile using a Wired Connection and a Device Template.....	158
Configure a Client Mode AP using a Wireless Connection and a Device Template.....	158
Configure a Client Mode AP using a Wired Connection and Auto Provisioning.....	160
Configure a Client Mode AP using a Wireless Connection and Auto Provisioning.....	161
Configure a Client Mode Profile.....	162
Configure DHCP Servers and DHCP Relay Agents.....	164
Add a DNS Service.....	166
Add IP Objects and Host Names.....	168
Add a MAC Object and Host Name.....	168
Add a Notification Template.....	169
Configure OS Objects.....	169
Configure VLAN Settings.....	170
Add a VLAN Group.....	171
Configure Supplemental CLI.....	172
Add IP Firewall Policy Rules.....	172
Add a Network Service Object.....	173
Add MAC Firewall Policy Rules.....	174
Traffic Filters.....	175
Configure MGT IP Filters.....	176
Add a WIPS Policy.....	177
Configure Rogue AP Detection.....	177
About QoS.....	180
About Classifier Maps.....	182
Configure Marker Maps.....	185
Configure Rate Limiting and Queuing.....	186
Configure a DNS Server.....	187
Configure an NTP Server.....	188
Configure an SNMP Server.....	189
Configure a Syslog Server.....	190
Configure an Access Console.....	191
Configure ALG Services.....	192
Configure a Router Firewall Policy.....	193
Configure an IP Tracking Group.....	194
Configure Layer 2 VPN Services.....	195
Configure IPsec VPN Authority Settings.....	196
About Server-Client Credentials.....	197
Configure Advanced Server Options.....	198
Configure Advanced Client Options.....	199
Configure LLDP and CDP Settings.....	200
Configure Location Servers.....	201
Configure Track Client Location Using an AeroScout Location Server.....	202
Configure Track Client Location Using an Extreme Location Server.....	203
Configure Track Client Location Using the Tazmen Protocol.....	204
Add Management Options.....	205
About Management Options.....	205
Configure Forwarding Engine Control Management Options.....	210
Configure System Settings Management Options.....	211
Configure Authentication Settings Management Options.....	213

Configure External RADIUS Server Settings.....	214
Configure Network Services.....	215
Configure an sFlow Receiver.....	216
Add a Subnetwork Space.....	217
Configure Subnetwork Space Advanced Settings.....	219
Configure Tunnel Policies.....	221
Configure an AAA Server Profile.....	222
Configure AAA Server Security Options.....	223
About Captive Web Portals.....	224
Customize and Preview Cloud-based Captive Portal Settings.....	224
Customize and Preview Device-based Captive Web Portal Settings.....	226
Import Captive Web Portal HTML Files.....	229
Configure an Extreme Networks A3 Server.....	230
Configure an LDAP Server.....	230
Create a Certificate and Key.....	232
Create an ExtemeCloud IQ Certificate of Authority.....	232
Create a Server CSR.....	233
Concatenate an Existing Certificate and Private Key.....	235
Create a Self-signed Certificate.....	236
Import a Certificate or Key.....	236
Manage.....	238
Use the Filter Sidebar.....	239
An Overview of Your Network.....	239
Plan your Network.....	240
Add a Location.....	241
Add a Building.....	242
Draw a Building Perimeter.....	242
Add Interior Walls and Obstructions.....	243
Add Floors.....	243
Plan Devices.....	245
View Heatmaps.....	247
Device List Views.....	248
About Digital Twin.....	250
Device List Views.....	250
Default Device Columns.....	250
Device List Functions.....	252
Device Status Icons.....	253
Utilities.....	257
About Actions.....	264
Device Details Overview.....	267
Device Details Monitor Functions.....	268
Device Details Configuration Tasks.....	271
Reports.....	288
Create a Network Summary Report.....	289
Generate a PCI DSS 3.2 Report.....	290
Generate a WIPS History Report.....	290
Generate a WiFi Statistics Summary.....	291
Generate a Client Tracking Report.....	291
Manage Users.....	292

View Connected Users.....	292
View User Details.....	293
Manage Events.....	293
Alerts Management.....	294
Configure an Alert Policy.....	294
Manage Active Alarms.....	295
Rogue APs.....	295
Classify Rogue APs.....	296
Mitigate Rogue APs.....	296
Rogue Clients.....	297
Classify Rogue Clients.....	297
Manage Network Applications and Application Groups.....	298
About Client Monitor.....	298
Search for Clients.....	299
About the Issue List Table.....	300
About Diagnosis.....	302
Timeline.....	302
Card.....	302
Events Associated with an Issue.....	303
Email Notification on Change of Status.....	303
Perform a Change Status Email Notification.....	303
VPN Management.....	304
Set the Time Frame for Captured Data Displays and Reports.....	304
ML Insights.....	307
Network 360 Monitor Overview.....	307
Network 360 Monitor - Device View.....	309
Network 360 Monitor - Zone View.....	309
Network Scorecard.....	309
About Client 360.....	310
Client Alias.....	310
Essentials.....	312
ExtremeIoT Essentials in ExtremeCloud IQ.....	312
Extreme AirDefense Essentials in ExtremeCloud IQ.....	313
ExtremeGuest Essentials in ExtremeCloud IQ.....	314
ExtremeLocation Essentials in ExtremeCloud IQ.....	315
CoPilot Dashboard.....	317
CoPilot Widget Tools.....	318
CoPilot Adverse Traffic Patterns Widget.....	319
The CoPilot DFS Recurrence Widget.....	319
CoPilot PoE Stability Widget.....	320
CoPilot Port Efficiency Widget.....	321
CoPilot Wi-Fi Capacity Widget.....	321
Submit a Support Ticket.....	321
Configure ExtremeCloud IQ to Submit a Support Ticket.....	321
Wireless Connectivity Experience Widget.....	322
Wired Connectivity Experience.....	323



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.

Conventions

To help you better understand the information presented in this guide, the following topics describe the formatting conventions used for notes, text, and other elements.

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 ExtremeSwitching switches or SLX routers, the product is referred to as *the switch* or *the router*.

Table 1: Notes and warnings




Icon	Notice type	Alerts you to...
	Tip	Helpful tips and notices for using the product
	Note	Useful information or instructions
	Important	Important features or instructions

Table 1: Notes and warnings (continued)



Icon	Notice type	Alerts you to...
	Caution	Risk of personal injury, system damage, or loss of data
	Warning	Risk of severe personal injury

Table 2: Text

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

Table 3: Command syntax

Convention	Description
bold text	Bold text indicates command names, keywords, and command options.
<i>italic text</i>	Italic text indicates variable content.
[]	Syntax components displayed within square brackets are optional. Default responses to system prompts are enclosed in square brackets.
{ x y z }	A choice of required parameters is enclosed in curly brackets separated by vertical bars. You must select one of the options.
x y	A vertical bar separates mutually exclusive elements.
< >	Nonprinting characters, such as passwords, are enclosed in angle brackets.

Table 3: Command syntax (continued)

Convention	Description
...	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 white papers, data sheets, and case studies

Extreme Networks offers product training courses, both online and in person, as well as specialized certifications. For details, visit www.extremenetworks.com/education/.

Send Feedback

The Information Development 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, do either of the following:

- Access the feedback form at <https://www.extremenetworks.com/documentation-feedback/>.
- Email us at documentation@extremenetworks.com.

Provide the publication title, part number, and as much detail as possible, including the topic heading and page number if applicable, as well as your suggestions for improvement.

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.

AP Regulatory Information

For regulatory information for the ExtremeCloud IQ supported access point models and appliances, refer to the appropriate *Installation Guide*.



Welcome to ExtremeCloud IQ

ExtremeCloud IQ 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 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 on the [Release Notes](#) and ExtremeCloud IQ documentation, see the Extreme Networks documentation site at [ExtremeCloud IQ documentation](#).

Related Topics

[Onboarding](#) on page 14



Onboarding

[Add Devices Overview](#) on page 14

[Quick Add Devices](#) on page 15

[Add Devices with Advanced Onboarding](#) on page 18

Use Onboarding to set up a basic network structure for your interactions with ExtremeCloud IQ. Afterwards, use the following tabs in the lefthand navigation space to navigate ExtremeCloud IQ:

- **Administration:** Define Global Settings for ExtremeCloud IQ.
- **Configure:** Create advanced network structures when necessary.
- **Manage:** View 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. You must use an existing location. When you create simulated devices with this method, you can also create **Digital Twin** devices. Digital Twin allows you to 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](#) on page 250. If you choose to manage your devices locally, with an on-premise controller, you can select WiNG, Switch Engine/EXOS, or Fabric Engine/VOSS devices. All you need is the device's 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
- WiNG Controller
- XCC Controller
- Site Engine
- Universal Appliances

Quick Add Devices

About This Task

Use this task to add devices to ExtremeCloud IQ from the **Manage > Device List** page. See [Add Devices Overview](#) on page 14 for more information about onboarding devices. For more information about adding switches, see the [ExtremeCloud IQ Switch Deployment Guide](#).

Procedure

1. Select the add icon, then **Quick Add Devices**.
2. Select **Manage your devices directly from the cloud** or **Manage your devices locally**.

If you intend to manage your devices locally via an on-premise controller, see [Add Locally Managed Devices](#) on page 17 for instructions. Otherwise, proceed to **Step 3**.

3. 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** and 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. When you are done, proceed to **Step 4**.



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 :

01221234567890

01221234567891

01221234567892

Serial Number and Model Number:

01221234567894, AP350

01221234567895, AP410

01221234567896, AP630



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.

- 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. Proceed to **Step 3**.
- For **Digital Twin** devices: Use to create a simulated Fabric or Switch Engine switch. Select one of these for 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 CoPilot.

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

**Note**

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

5. For **Policy**(optional): To assign an existing network policy, choose one from the **Add Policy** drop-down list.
6. 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 will see an alert.

Add Locally Managed Devices

About This Task

Use this task to add devices to your network that you intend to manage with an on-premise controller. This option applies only to WiNG, Switch Engine or Fabric Engine devices.

Procedure

1. Select the add icon, then **Quick Add Devices**.
2. Select **Manage your devices locally**.
3. 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.

4. To enter devices via a CSV file, select **CSV**.
5. Select the device make from the dropdown list.

6. 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 :

01221234567890

01221234567891

01221234567892

Serial Number and Model Number:

01221234567894, AP350

01221234567895, AP410

01221234567896, AP630



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.

Add Devices with Advanced Onboarding

About This Task

Use this task to add devices to ExtremeCloud IQ from the **Manage > Device List** page. For more information about adding switches, see the [ExtremeCloud IQ Switch Deployment Guide](#).

Procedure

1. Select the add icon and then select **Advanced Onboarding**.

2. For **Device Type**, select **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, AP350

01221234567895, AP410

01221234567896, AP630



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.

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



Administration

[About Global Settings](#) on page 20

Administration provides access to various ExtremeCloud IQ settings as follows:

- **Global Settings:** Define criteria that affects the entire system. For example, license management, device settings, email notifications, API settings, and viewing activity logs.
- **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 21
- **Account Management:** Add, delete, or edit accounts. [Add an Admin Account](#) on page 23
- **Credential Distribution Groups:** Add, delete, or edit credential distribution groups. [Add a Credential Distribution Group](#) on page 22
- **License Management:** View and add license and entitlement objects. [Manage Licenses](#) on page 27
- **Device Management Settings :** View and modify the default device management password. [Set a Device Default Password](#) on page 28
- **VIQ Management:** Manage the Virtual ExtremeCloud IQ. [Manage the Virtual IQ](#) on page 28
- **Email Notifications:** View, add, and modify email notification rules for status changes. [Set Email Notifications](#) on page 30
- **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 32, [Add a Third-Party API Token](#) on page 33, [Generate API Access Tokens](#) on page 31

- **Logs:** View and sort logs. Download log entries for any or all admin accounts. [Download Log Information](#) on page 34
- **SSH:** Provide temporary remote access to your network for troubleshooting purposes. [Enable SSH Availability](#) on page 39

Manage Account Details

About This Task

Use these steps to edit personal and company information.

Procedure

1. To make changes, select the edit icon next to any of your **Personal Information** items.



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 will be required to 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.

2. To change the **Industry**, select a different industry from the drop-down list and then select **Apply**.

See [Add an Organization](#) on page 23 to add an organization.



Note

The industry you identify here indicates the group that submits data for CoPilot global analytics.

3. Opt into **CoPilot global analytics** to compare characteristics of your deployment with those of similar deployments.

24 hours after opting in, your VHM begins submitting normalized data to its local ExtremeCloud IQ, which gathers this data from various VHMs to create a large set of network measurements. After that, you can compare elements of your network with measurements submitted by other VHMs. These comparisons give you insight into how some aspects of your deployment are functioning with respect to others.

Related Topics

[About Global Settings](#) on page 20

Enable Two-Factor Authentication

About This Task

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 the Google Authenticator app. (Google Authenticator generates time-based one-time keys and runs on iOS and Android devices.)

Procedure

1. Toggle the **Status** switch to **On**.
2. Install the **Google Authenticator** app on your iOS or Android smart device.
3. Open **Google Authenticator**, select **Scan Barcode**, and scan the on-screen QR code.
Alternately, you can open **Google Authenticator**, 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, **Google Authenticator** displays a six-digit code, which changes every 30 seconds.
4. Enter the six-digit code in the text box in the **Multi-Factor Authentication** window.
5. Select **Confirm** to activate multi-factor authentication for yourself.



Note

For legibility, **Google Authenticator** 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.

What to Do Next

When administrators log in, they enter their admin name and password, the **Google 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.

Enable ExtremeCloud IQ Classic

About This Task

Link your devices directly to the ExtremeCloud IQ Classic version using these steps:

Procedure

1. Turn on **ExtremeCloud IQ Classic**.
2. Enter your user name.
3. Enter your password.
4. Select **Get Organization**.

Add a Credential Distribution Group

About This Task

Create Credential Distribution Groups for members of your organization who are allowed to distribute log in credentials to visitors. Use these steps to create a new group:

Procedure

1. Enter a **Group Name**.

2. For **Admin Account**, choose **Active Directory User** or **Guest Management Role User** from the drop-down list.
3. For an **Active Directory User**, enter the account's Active Directory user group.
If the account is a member of multiple groups, then enter the name of the first group, press **Enter**, and add additional groups.
4. For a **Guest Management Role User**, enter the access control role to assign to a group member.
5. Select **Credential Restriction** and enter a number to limit the number of credentials group members can distribute.
6. Select **Registration Operation** to require email approval by the credentials manager before the guest gains access.
7. For **Enable User Groups**, add existing user groups to add to this employee group by either choosing **Select All**, or by selecting individual user groups.
8. Select **Save**.

Add an Organization

About This Task

The administrator can create separate, fully-managed organizations.

Procedure

1. Select the plus sign.
2. Enter a name.
3. Select a color from the drop-down list or create a custom color.
4. Select **Add**.



Note

ExtremeCloud IQ automatically assigns an Organization ID.

What to Do Next

To add an Admin to this organization, see [Add an Admin Account](#) on page 23.

Add an Admin Account

Before You Begin

Create the organization to which this admin will be assigned.

About This Task

Use this task to create a new admin account and set parameters, such as read/write privileges, and device management restrictions based on deployment locations.

Procedure

1. Determine whether the new admin is within 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 engineering.



Note

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

2. Enter the admin email address.
3. Enter the admin name (internal admin only).
4. For **Organization**, assign an admin to an existing organization.
5. For **Idle Session Timeout**, enter the number of minutes before a session times out (internal admin only).
6. Assign a role to each admin.
 - An **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.
 - An **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.

- A **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.
- The **Help Desk** role 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.
- The **Guest Management** role 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.
- An **Observer** has read-only access to most of the ExtremeCloud IQ interface. This role does not have access to the account and license 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.
- The **Installer** role is designed to work with the mobile app, and so has limited privileges based on the in-build limitations of the app. If you log into

ExtremeCloud IQ as an admin with Installer privileges using the standard web interface, then 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
- An **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.
7. Assign the locations to which the admin has access.
Access restrictions by location are based on how you have defined your network map.
 8. Select **Save & Close**.

View Licenses

About Licensing

The first time 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 licensing prompts.

When you enter your credentials, ExtremeCloud IQ retrieves the license information from your Extreme Portal account and applies it to your ExtremeCloud IQ account.

If you already have an Extreme Portal account, in **Global Settings > Administration > License Management**, select **Link My Extreme Portal Account**. Enter your **Extreme Portal** credentials.

For information about how to manage your licenses, see [Manage Licenses](#) on page 27.

Entitlements

The **Entitlements** table contains information about your current licenses. The following information displays:

- **Type:** Licenses can be evaluation or permanent.
- **Devices:** The number of devices your entitlement key supports. The total number of devices you can manage is the sum of all of the numbers associated with active keys.

- **Start Date:** The date the entitlement key and license became valid. This column can be sorted. The date reflects the time zone setting in your browser.
- **End Date:** The date the entitlement key and license expired. This column can be sorted. The date reflects the time zone setting in your browser.
- **Description:** A description of the license, if one was entered.

NAC Entitlements

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

Universal NAC licenses 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 entitlements available is displayed above the **NAC Entitlements** table, and is based on the number of NAC subscriptions you have purchased.

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 will be 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 displayed in this table depends on whether you have entered an evaluation or permanent entitlement key. If you have entered an evaluation key, the number of days remaining until the entitlement key expires and the number of devices licensed are displayed at the top of the window. If you have entered a permanent key, only the number of licensed devices is displayed.

You can use unused entitlements in addition to any active licenses. For more information, see, [Manage Licenses](#) on page 27.

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 licenses, the number of days remaining in the evaluation period displays here. For permanent licenses, N/A displays.

- **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 license 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 reflects the time zone setting in your browser.
- **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 license was activated. This column can be sorted.
- **Description:** The license description, if one was entered.

Manage Licenses

About This Task

Use these steps to link your Extreme Portal account so that when you enter your credentials, ExtremeCloud IQ retrieves the license information from your Extreme Portal account and applies it to your ExtremeCloud IQ account. For more information about ExtremeCloud Licensing, see https://documentation.extremenetworks.com/XIQ/ExtremeCloud_IQ_Licensing/GUID-70BCF935-1DAE-4DF3-8FEC-6B7E6765EDAE.shtml.

Procedure

1. Select **Link My Extreme Portal Account**.
2. Enter your Extreme Portal credentials.
The license information is displayed in the **Entitlements** or the **NAC Entitlements** table.
3. If you need to change the numbers of devices you manage, select **Contact Sales**.
4. If you have a NAC device and it does not display in the NAC Entitlements table, onboard the NAC device to ExtremeCloud IQ.
If the NAC device is compatible, it displays 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. 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.
7. For **Legacy Entitlements** only, to remove or deactivate an Entitlement Key, select the check box and then select **Remove/Deactivate**.
If you deactivate an active key, you can add it back in later.
8. For **Legacy Entitlements** only, select **DOWNLOAD** to download the entire Legacy Entitlements table into a CVS file.

Related Topics

[View Licenses](#) on page 25

Set a Device Default Password

About This Task

Use these steps to set basic parameters for Extreme Networks devices.

Procedure

1. 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.
2. **Confirm** the new password.
3. 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.

Manage the Virtual IQ

About This Task

ExtremeCloud IQ administrators with read/write permission can perform the following administrative tasks from the **VIQ Management** menu:

- Manually back up and restore Virtual IQ account data.
- Delete data to reset the Virtual IQ database.
- Export and import Virtual IQ data.
- Enable and disable SSH (see [Enable SSH Availability](#) on page 39)
- Enable and disable the supplemental CLI tool.
- Enable and disable the verification of APs using the out-of-the-box wireless onboarding feature.

Procedure

1. 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 this page.
2. To restore a backup, select **Restore** for the backup event in the **Backup History** table.



Note

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

3. Select **Reset VIQ** to delete the Virtual IQ database.
This resets it to its initial state before any inventory or configurations were added.

4. 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.

5. 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.

6. Slide the **Enable CoPilot feature for this VIQ** toggle to **ON** to enable it.

The CoPilot feature requires a CoPilot license. If CoPilot is disabled for this VIQ, the CoPilot features will not be available, and the administrator will not receive ML/AI-driven insights and proactive follow-ups.

7. Slide the **SSH Availability** toggle to **ON** to enable it.



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, as SSH FTP assumes that it is run over a secure channel. For more information, see [Enable SSH Availability](#) on page 39.

8. Slide the **Supplemental CLI** toggle to **ON** to enable it.

The **Supplemental CLI** tool allows you 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, but for this feature to be visible, you must first enable it at the global level here.

9. To enable the Virtual IQ to permit APs to respond to mesh-join requests, slide the **AP Out-of-the-box Wireless Onboarding** toggle to **ON**.

This setting permits or prohibits AP responses to mesh-join requests. When this setting is off, the Virtual IQ prohibits managed APs from responding even if the serial number of the requesting AP is listed in the Virtual IQ.

Set Email Notifications

Before You Begin

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.

About This Task

If you have permission, you can configure ExtremeCloud IQ to send email notifications for changes of device status. When you have activated an email notification rule and saved its settings, ExtremeCloud IQ automatically sends notification emails when your 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, a notification email is sent 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 define alert policies from [here](#).

Procedure

1. ExtremeCloud IQ enables you to activate and deactivate email notifications for the following individual alerts:
 - **AP Status:** Activate to notify when an AP goes up or down.
 - **Hardware CPU:** Activate to notify 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:** Activate to notify 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:** Activate to notify when a switch port, with authorized email notifications configured, goes up or down.
2. Enter the **To Email** addresses, each separated by a comma.
3. Select **Save Settings**.

Alerts Management

This page provides a graphical representation of event and metric alerts for a specified time range. Use **Alert Policy** to view currently configured policies and enable them, view unconfigured policies and configure them, and create brand new alert policies. For more information, see [Configure an Alert Policy](#) on page 31.

Configure an Alert Policy

About This Task

Use this task to define and configure an alert policy for reporting events and metrics.

For information about how to manage alerts, see [Alerts Management](#) on page 30.

Procedure

1. Select **Alert Policy** from the **Alert Dashboard** page.

You can now view **Configured Polices** and **Unconfigured Polices**.

- a. For **Configured Polices**, use the check boxes to enable and disable alerts in bulk or individually.
- b. Select whether you want alerts sent to an email or SMS.



Note

Before you can select SMS, you need to define a valid phone number to receive alerts. You can do so from **Global Settings**. For more information, see [Manage Account Details](#) on page 21.

- c. Use the filter option to customize the alerts displayed.
 - d. For **Unconfigured Polices**, highlight a policy, select the plus sign in the **Action** column, and proceed to **Step 2**.
2. Choose the type of alert this policy will report: **Event** or **Metric**.
 - For a **Device** event: Select **Device** events or **Security** events. For a Device event, select the type of device event to report an alert.
 - For a **Metric** event: Use the dropdown menus to define the metric.
 3. Select the **Trigger Type** for the frequency of alerts.
Specify dates and times for **Deferred** and **Repeated**.
 4. Select the type of alert to report: **Information only**, **Warning** or **Critical**.
 5. Enter an optional description.
 6. Select **Save**.
 7. The saved alert then displays in the **Configured Policies** list.
 8. Select whether to report this alert via email or SMS.
 9. Enable the alert.
 10. To define a brand new alert policy, select **Add New Policy** and follow **Steps 2-9**.

Generate API Access Tokens

About This Task

Use these steps to generate API access tokens that applications use to make REST API calls to ExtremeCloud IQ. For more information about API Tokens, see [API Access Tokens](#) on page 32.

Procedure

1. Navigate to **Global Settings > API Token Management**.

2. Select the plus sign.
3. 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 connects the token you generate with your developer account.
4. Select an **Expiration Setting** for the Access Token.
5. Select **Generate**.

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 access token text string

Grantor: The admin who granted access to the application or who generated it

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. If the token is already expired, the date is replaced with Expired.

Refresh Token: The refresh token can be used temporarily before the current one expires so that you have time to obtain a new access token with a new expiration date.

Add an API Presence and Data Location Feed

About This Task

The presence and location API feature lets Extreme Networks wireless devices detect the presence of clients (such as smart phones) and obtain location data for all connected and unconnected clients. Use the following steps 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.

Procedure

1. Navigate to **Global Settings > API Data Management**.
2. Select the plus sign on the **API Data Management** page.

3. 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.

4. 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 31).
5. 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.
6. Select **Enable**.
7. Select **Save**.

Add a Third-Party API Token

About This Task

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 [API Access Tokens](#) on page 32.

Procedure

1. Navigate to **Global Settings > 3rd Party API Connections**.
2. Select the plus sign and then enter the **API Token** character string.
3. Select **Save**.

Alert Notifications

Use these options to define [Webhooks](#) for viewing alerts about events and metrics in real time, and [Emails](#) for receiving alerts. [User Subscriptions](#) contains information about users subscribed to email and SMS alerts.

Add Webhooks

About This Task

Use this task to hook into the alert data stream and digest in real time.

Procedure

1. Select the plus sign to add a new webhook.
2. Enter the **Post URL** from your API from <http://ExtremeCloud%20IQ.com>.
Look for it under **Notifications**.
3. Enter an optional **Access Token** that you created [here](#).
4. Enter an optional **Description**.
5. To receive information about all events, select **Send Me Everything**.
6. To receive only certain events, select **Alert Policy List** and one or both of the following options.
 - **Device up**: Sends a list of devices currently up and running.
 - **Device SSH login failed**: Sends a list of failed device logins.
7. Select **Enable**.
8. Select **Save**.

An an Email Alert

About This Task

Use this task to add an email for alert notifications.

Procedure

1. Enter the email address.
2. Enter an optional description.
3. To receive information about all events, select **Send Me Everything**.
4. To receive only certain events, select **Alert Policy List** and one or both of the following options.
 - **Device up**: Sends a list of devices currently up and running.
 - **Device SSH login failed**: Sends a list of failed device logins.
5. Select **Enable**.
6. Select **Save**.

About User Subscriptions

This page contains information about users subscribed to email and SMS alerts.

Download Log Information

About This Task

If you are logged in as an admin with full access (administrator role), you can download the entire log or just the entries pertaining to a specific admin, 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 any PII (personally identifiable information) gathered about them. This includes personal information collected by ExtremeCloud IQ and contained in the log. If an admin leaves their company and asks for this information, you can sort for log entries pertaining to that admin and download and save them in a .csv (comma-separated values) file.

Procedure

1. Select **Download**,
2. Select the name of the person requesting data from the **Admin Name** drop-down list in the dialog box.
3. Select **Ok**.

ExtremeCloud IQ generates a file in CSV format.

4. Select one of the following options.

Select either **file_name.csv** or **Download**. The file contains only log entries for the chosen admin.

5. To download the complete log, follow these steps but select **All** from the **Admin Name** drop-down list.

For more information about the types of logs available see:

- For Audit logs, see [About Audit Logs](#) on page 36
- For GDPR logs, see [About GDPR Audit Logs](#) on page 37
- For KDDR logs, see [About KDDR Logs](#) on page 38
- For Authentication logs, see [About Authentication Logs](#) on page 36
- For Accounting logs, see [About Accounting Logs](#) on page 35
- For Credential logs, see [About Credential Logs](#) on page 37
- For Email logs, see [About Email Logs](#) on page 37
- For SMS logs, see [About SMS Logs](#) on page 38

About Accounting Logs

The Accounting Logs table displays information about cloud-based PPSK and RADIUS user sessions on your network. To set a time range in which to view user sessions, select start and end dates and times in the fields at the top of the window. 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.

For information about how to download Accounting logs, see [Download Log Information](#) on page 34

About Audit Logs

The audit log contains an historical record of the administrative operations performed on ExtremeCloud IQ. 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.

For information about how to download Audit logs, see [Download Log Information](#) on page 34

About Authentication Logs

This window 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 authentication events displayed in the table appear for a time range that you define using start and end dates and times in the fields at the top of the window. 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: Facebook, Google, LinkedIn
 - 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.

For information about how to download Authentication logs, see [Download Log Information](#) on page 34

About Credential Logs

This window displays information about cloud-based RADIUS user credentials that have expired. To set a time range to view expired user credentials, select start and end dates and times in the fields at the top of the window. You can also search for log entries for a specific user in the **Search** field above the table.

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.

For information about how to download Credential logs, see [Download Log Information](#) on page 34

About Email Logs

Email logs display 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 user credentials are approved by an employee

To filter the display, select start and end dates and times in the fields at the top of the window. You can also search for email messages sent to a specific address in 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.

For information about how to download Email logs, see [Download Log Information](#) on page 34

About GDPR Audit Logs

GDPR (General Data Protection Regulation) audit logs display 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 these logs to track actions that are currently being processed, those that have been completed, and those that have failed.

The table displays the following information about 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.

For information about how to download GDPR logs, see [Download Log Information](#) on page 34

About KDDR Logs

A KDDR (Kernel Diagnostic Data Recorder) log captures run-time statistical data about unexpected events and unpredictable or unwanted situations that might occur with ongoing processes and services of an Extreme Networks device. Extreme Networks Support analyzes the log files for troubleshooting.

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.

For information about how to download Audit logs, see [Download Log Information](#) on page 34

About SMS Logs

This window displays information about SMS notifications to users who requested network access. ExtremeCloud IQ creates SMS log entries for the following events:

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

To filter the display, select start and end dates, and times in the fields at the top of the window. 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.

For information about how to download SMS logs, see [Download Log Information](#) on page 34

Enable SSH Availability

About This Task

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 will manage 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, as SSH FTP assumes that it is run over a secure channel.

Use these steps to enable SSH.

Procedure

1. From **Administration > Global Settings**, select **VIQ Management**.
2. Toggle **ON SSH Availability**.

What to Do Next

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.



Configure Applications and Users

[Add a Custom Application](#) on page 40

[User Management](#) on page 40

After you complete **Onboarding**, your ExtremeCloud IQ system is ready for daily use. You can adjust default settings for applications and users as follows:

- **Applications:** Manage custom applications.
- **Users:** Manage Users and User Groups.

Add a Custom Application

About This Task

Use these steps to create a custom application definition, including an application group, optional descriptions, and application detection rules.

Procedure

1. Select **Add Custom**.
2. Enter a name for the new application.
3. Enter an optional description.
4. Select an existing **Application Category** from the drop-down list or create a new one by selecting the plus sign.
 - a. If you add a new group, enter a group name.
 - b. Select **Save**.
5. Add **Application Detection Rules**.
6. Select **Save**.

User Management

Users are assigned 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. You can create user groups for a selected network policy or for all network policies. You can view, add, sort, select, modify, and delete user groups and user accounts. However, after a user group has been configured, you can only modify the name and description, which

prevents issues with creating passwords. To modify other settings, you must create a new user group.

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

For information about User Profiles, see [Add a User Profile](#) on page 152.

Add a User Group

Before You Begin

Extreme Networks supports user groups for PPSK (Private Pre-Shared Key) 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:

- 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 > Users > 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 [About RADIUS Authentication](#) on page 70.

About This Task

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



Note

After a user group has been configured, you can only modify the name and description. This prevents issues with creating passwords. To modify other settings, you must create a new user group.

Procedure

1. Enter the user group's name.
2. For **Password DB Location**, select **Cloud** when you want the password database to reside in the cloud, and **Local** when you want the login credentials to be stored on all APs using this SSID.
You must select **Local** when you are creating a private client group in this user group (see [Classification Rules Overview](#)).
3. If you selected **Cloud**, see [Configure a Cloud User Group](#) on page 43 for more information.
4. If you selected **Local**, see [Configure a Local User Group](#) on page 45 for more information.
5. Select **SAVE** after completing Step 3 or 4.

What to Do Next

If this is part of creating a network policy, return to complete that configuration.

Add Users to a User Group

Before You Begin

You must first create the associated user group.

About This Task

As part of creating a user group either on its own or associated with a network policy, you need to populate that user group with users. You can either add one user at a time or add several in bulk. This task walks you through both options.

Procedure

1. To add a single user, select the plus sign in the **Add Users** section of the **New User Group** window.
2. Enter or select the following:

- Enter the user's name. This name displays in any messages sent to the email address in the **Deliver Password** section. The email messages, which contain login credentials and wireless connection instructions, begins with `Welcome <this_name>`. When you choose **Name** in the **User Name** drop-down list, this field is required. Otherwise, it is optional and if left empty, whatever you define as the user name—email address, phone number, or other—is used in the email message.



Note

When an Extreme Networks device is used as RADIUS server and local database is selected, the following special characters are not allowed to be in the usernames:

`- /@(.+)\. (.+)\$/ - / \ [] : ; | = , + * ? < > @ " */ ^`

- Enter the user's organization. For permanent users, leave this empty.
- Enter the purpose of the user's visit. For permanent users, leave this empty.
- Enter the user's email address. This is only required if you choose **Email Address** in the **User Name** drop-down list.
- Enter the user's mobile phone number, including international dialing code. This is only required if you choose **Phone Number** from the **User Name** drop-down list.
- Choose a **User Name** identifier from the drop-down list: **Email Address**, **Name**, **Phone Number**, or **Other**. If you select **Other**, you must enter another type of user identifier, such as Jane's iPhone, Guest, or `<organization_name>` in the additional field that displays.

- Enter a password for this user. The password must conform to the password rules configured in the associated user group.

**Note**

Only administrators can view and change passwords. Other ExtremeCloud IQ admin roles will not see or be able to edit this parameter.

- Enter an optional user description.
 - For **Deliver Password/Email Address**, select and enter the email address that receives the user credentials when you select the envelope icon in the **Delivery** column. This field is auto-populated if you have already entered an email address above. This option only displays if you selected **Email** in the associated user group's **Delivery Settings** section.
3. Select **DONE**.
 4. To add a multiple users, select **Bulk Create** in the **Add Users** section of the **New User Group** window.
 5. Enter or select the following:
 - Enter a prefix for these users' names. Bulk-created user names will have this prefix added in front of the digits for each user, starting with 1. For instance, if the user name prefix is 1250, then the first bulk-created user is 12501, the second user is 12502, and so on.
 - Enter the number of users to add, between 1 and 1000.
 - Enter the email address that receives the user credentials.
 6. Select **DONE**.

This saves your changes, creates the requested user accounts, and emails the bulk-created login credentials to the saved email addresses in CSV file format. The CSV file contains the SSID, user ID, user name, user group, access key, and expiration date for each bulk-created user.

What to Do Next

Return to the **New User Group** window to see the newly added users and continue configuring the network policy.

Configure a Cloud User Group

Before You Begin

Select **Cloud** as the password database location on the **New User Group** screen.

About This Task

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. Use this task to configure a cloud-based user group.

Procedure

1. Configure **Password Settings** as follows:
 - **Password Type:** Select **PPSK** or **RADIUS**.
 - **Description:** Enter an optional description for this user group.
 - Select the **Enable CWP Register** check box to require users in this user group to log in using a captive web portal. (Only available if a captive web portal is enabled for this SSID.)
 - **Generate Password Using:** Select any combination of characters that you want to include in the password (**Letters**, **Numbers**, and **Special Characters**).
 - You can then enforce password complexity by choosing **All selected character types**, **Any selected character types**, or **Only one character type** from the drop-down list.
 - For **PSK Generation Method**, choose **Password Only** or **User String Password**. The User String Password option lets you include the user name and a string of characters in front of the generated Private PSKs.
 - Enter the length of automatically-generated passwords for this user group.
 - 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**, then the maximum passphrase for the Private PSK can be between eight and 31 characters.
 - The **Concatenating String** field displays if you selected **User String Password** above. This string is used to generate PPSKs as User name + Character String + Password. For example, if you enter `Extreme`, as the string, then the generated PPSKs are `<User name>Extreme<Password>`.
2. Configure Expiration Settings as follows:
 - Select **Require Authentication After** to enforce re-authentication after a session has been inactive for a period of time.
 - For **Account Expiration**, select an option from the drop-down list and complete any fields that ExtremeCloud IQ displays based on your selection. These fields describe the time frame during which the account is valid.
 - **Action at Expiration:** (Not available for accounts that are 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 send users an on-screen prompt that they can use to renew their credentials.
3. Configure a delivery method as follows:
 - For **Deliver Access Key by**, select the notification delivery method for members of this user group. You can select **Text Messages (SMS)**, or **Email**, or both.
 - Select **Add Users** to see the **Add new users to this User Group** section. The table includes the number of users assigned to this user group, showing their name, user name, and organization.
4. Select **Add User** to add a single user to this user group or **Bulk Create** to add multiple users at the same time.

For more information, see [Add Users to a User Group](#) on page 42.

5. Select **SAVE**.

What to Do Next

If this is part of creating a network policy, return to complete that configuration.

Configure a Local User Group

Before You Begin

Select **Local** as the password database location on the New User Group screen.

About This Task

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. Use this task to configure a local user group.

Procedure

1. Fill in the following fields:
 - For **Password Type**, select **PPSK**.
 - Enter an optional user group description.
 - 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). Multiple per-user PPSK limits can be set in the same (SSID).
 - Select **Enable use for Private Client Group** when you are creating a private client group (PCG) in this user group.
 - Select one of the following PCG operating modes:



Note

After you select the PCG operating mode, you cannot change your selection because the different modes create non-transferrable passwords.

- **AP-Based:** An 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:** A key-based PCG requires one password used by the entire group of devices. Key-based PCGs do not need room assignments, and no traffic tunneling is used on anchor APs.
- **Both:** Supports both AP-based and key-based modes.



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.

2. 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 58 for more information.
3. Configure password settings as follows:
 - Select any combination of characters to use for the password: **Letters, Numbers, and Special Characters**). To enforce password complexity, select **All selected character types, Any selected character types, or Only one character type** from the drop-down list.
 - For **PSK Generation Method** select **Password Only** or **User String Password**. The User String Password option lets you include a string of characters in the generated Private PSKs.
 - Enter the length of automatically-generated passwords for this user group. If the generation method is **Password Only**, then the PPSK password can be between eight and 63 characters. If the generation method is **User + String + Password**, then the maximum passphrase for the Private PSK can be between eight and 31 characters.
 - If you selected **User String Password** above, enter a character string from 0 to eight alphanumeric characters. This string will be used to generate Private PSKs in the form `User name + Character String + Password`. For example, if you enter `Extreme`, the generated Private PSKs are `<user name>Extreme<Password>`.
4. Configure **Expiration Settings** as follows:
 - To force re-authentication after a session has been inactive for a period of time, select **Require Authentication After** and enter a time in the minutes field.
 - For **Account Expiration**: Select **Never Expire** or **Valid During Dates** from the drop-down list. If you select **Valid During Dates**, complete the displayed fields, which define the time frame during which the account is valid.
 - **Action at Expiration**: (Not available for accounts that are set to never expire.)
 - Select **Access Rejected** to block users from renewing their credentials.
 - Select **Show Expiration Message** to send users an on-screen prompt that they can use to renew their credentials.
5. Select **Text Messages (SMS)**, or **Email**, or both to define the user group's notification method.
6. Select **Add User** to add a single user to this user group or **Bulk Create** to add multiple users at the same time.
For more information, see [Add Users to a User Group](#) on page 42.
7. Select **SAVE**.

Configure a Private Client Group

Before You Begin

Create a Private Pre-share Key Standard Wireless Network.

About This Task

When Private Client Groups (PCGs) are enabled, they can be designated 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.

Procedure

1. **Enable Private Client Group Options.**
2. Select **AP-Based** or **Key-Based**.
3. If you selected Key-Based, fill in the following **Private Client Groups Traffic Filtering** options.
 - **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 and grayed out. If you do not select **Multicast Filtering**, you can independently select mDNS and SSDP filtering. This capability is solely dependent upon site requirements.

What to Do Next

Continue configuring the Standard Wireless Network.

Locked Users

About This Task

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 clients in the sandbox.

To unlock a client, use the following steps:

Procedure

1. Select a client from the locked clients list.
2. Select **Unlock**.

RADIUS Test

Before You Begin

This 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.

About This Task

To test the connectivity between a RADIUS authenticator and a RADIUS server, perform the following steps:

Procedure

1. Select the type of RADIUS server 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.
2. 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.
3. 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.
4. Select **Test**.

Results

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

Example

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

Unbind Device

About This Task

Use this to unbind a cloud-based PPSK from a client device to free up that key and/or device. You can unbind the client MAC address, the PPSK, or both.

Procedure

1. Select the method for unbinding from the drop-down list.
Choose **MAC address**, **PPSK**, or **MAC address and PPSK**.
2. Enter the MAC address, the PPSK, or both.
3. Select **Unbind**.



Configure Network Policies

- [Add a Network Policy](#) on page 51
- [Configure Policy Settings](#) on page 52
- [Deploy a Network Policy](#) on page 53
- [Configure a Standard Wireless Network \(SSID\)](#) on page 53
- [Configure a Classification Rules Network Policy](#) on page 66
- [Customize Advanced Access Security Settings](#) on page 68
- [About RADIUS Authentication](#) on page 70
- [About Router Settings](#) on page 76
- [Configure Device Templates](#) on page 92
- [Configure a Hive Profile](#) on page 93
- [Configure Device Data Collection and Monitoring Options](#) on page 95
- [Configure iBeacon Service](#) on page 97
- [Configure Presence Analytics](#) on page 98

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. The [Policy Settings](#) section offers links to Common Object configuration options.
- [Standard Wireless Networks:](#) Define the wireless network (SSID) and the bands on which to broadcast each SSID, plus SSID usage, 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.

Add a Network Policy

About This Task

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 DeployPolicy.

To add a new network policy, do the following:

Procedure

1. Select **Add** above the Network Policies table, or select **Add Network Policy**.
2. In the **New Policy** window, select a policy type: (Wireless, Switching, SR/Dell Switching, Branch Routing, or any combination, including all them).
3. Enter a name for the policy.
4. Enter an optional description.
5. 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 nav bar, under Application Management, select **Presence Analytics**. This is where you configure analytics settings, such as trap interval, aging time, and aggregate time.

6. Select **Save**.

The highlighted tab changes from 1 Policy Details to 2 Wireless Networks, 3 Switching, 4 SR/Dell Switching, 5 Branch Routing and 6 Deploy Policy, depending on your configuration choices.

What to Do Next

Proceed to configuring a Wireless Network ([Configure a Standard Wireless Network \(SSID\)](#) on page 53, Device Templates ([Configure Device Templates](#) on page 92), Router Settings ([Configure a Routing Policy](#) on page 88), or Additional Settings, as necessary. When you are done, deploy the policy ([Deploy a Network Policy](#) on page 53).

Configure Policy Settings

About This Task

The following configuration settings are optional, depending upon your requirements. For example, choose which default routing instance will be used for NTP, DNS, Syslog, and SNMP for a switch.

- DNS Server (Switches only)
- NTP Server (Switches only)
- SNMP Server (Switches only)
- Syslog Server Settings (Switches only)
- Device Credentials
- Device Time Zone
- HIVE
- Management & Native VLAN
- IP Tracking
- LLDP/CDP (Switches only)
- Management Settings
 - Management Options
 - Traffic Filter
 - MGT IP Filter

Procedure

1. Navigate to **Configure > Network Policies**.
2. Select the existing network policy and **Edit**.
3. [Configure a DNS Server](#) on page 187.
4. [Configure an NTP Server](#) on page 188.
5. [Configure an SNMP Server](#) on page 189.
6. [Configure a Syslog Server](#) on page 190.
7. [Configure Device Credentials](#) on page 279.
8. [Configure a Classification Rules Network Policy](#) on page 66.
9. [Configure a Hive Profile](#) on page 93.
10. [Configure VLAN Settings](#) on page 170.
11. [Configure an IP Tracking Group](#) on page 194.
12. [Configure LLDP and CDP Settings](#) on page 200.



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.

13. [Add Management Options](#) on page 205.
14. Configure [Traffic Filters](#) on page 175.
15. [Configure MGT IP Filters](#) on page 176.

16. Select **Save**.

Deploy a Network Policy

Before You Begin

Create a complete the network policy configuration.

About This Task

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 that will operate under the policy. 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).

Procedure

1. To upload a network policy to all of the devices in the devices list, select the check box in the top left side of the table header.
This automatically selects the check boxes for all of the devices.
2. Select **Upload**.
3. To upload your network policy to specific devices only, select the check box for those devices, and then select **Upload**.
You can filter the devices displayed with the **Assigned**, **Eligible** and **Filtered** options.
4. 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.
5. 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.
6. Select **Perform Update**.

Configure a Standard Wireless Network (SSID)

About This Task

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 set of authentication and encryption services that wireless clients and access point devices use when communicating with each other. This topic describes how to configure a standard-access wireless network.

Procedure

1. Select the plus sign below the Wireless Networks heading.
2. Select **All other Networks (standard)** from the drop-down.

3. Enter 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.

4. Enter 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.

5. Select SSID radio broadcast bands:

- **WiFi0 Radio (2.4 GHz or 5 GHz):** Broadcast the SSID based on the configuration of the WiFi0 radio.
- **WiFi1 Radio (5 GHz only):** Broadcast the SSID on the WiFi1 radio operating in the 5 GHz band. Most Extreme Networks devices have two radios: radio 1 is bound to WiFi 0 and radio 2 is bound to WiFi1. 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 WiFi0 and WiFi1 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.

- **WiFi2 Radio (6 GHz only):** This option currently supports only Enterprise WPA3, Personal WPA3, and Open Enhanced. When you select this check box, a message reminds you that you will only be able to access the items available for 6 GHz.
6. Select an SSID Authentication method and complete the fields.
 - Select **Enterprise WPA/WPA2/WPA3** to require users to authenticate by entering a user name and password, and validating against a RADIUS server. Only WPA3 is supported for 6 GHz devices. See [Configure Enterprise SSID Authentication](#) on page 56.
 - Select **Personal WPA/WPA2/WPA3** to require users to enter a shared PPSK to authenticate. Only Personal WPA3 is supported for 6 GHz devices. See [Configure Personal SSID Authentication](#) on page 57.
 - Select **Private Pre-Shared Key** to require 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 58.
 - Select **WEP** to require users to use EAP/802.1X for user authentication and two keys for encryption; one for multicast traffic and another for unicast traffic (not available for 6 GHz) See [Configure WEP SSID Authentication](#) on page 131.
 - Select **Open** (not available for 6 GHz) or **Enhanced Open** so users do not use any form of authentication, but can be directed to a captive web portal before they are allowed to access other network resources. Enhanced Open is available only for 6 GHz devices. If you select open authentication and need to create a captive web portal, complete Steps 7 - 11 below. Otherwise, proceed to Step 12.

7. Select **On** to enable a captive web portal for this wireless network.
This option requires users to register before they are assigned user profile settings for network access beyond their associated device. (Not available for 6 GHz.)
8. Select an existing captive web portal, or select **Add** to create a new one.
9. Enter a name for the captive web portal.
10. Customize and preview your login page, authentication method, and optional success and failure pages as described in [Customize and Preview Device-based Captive Web Portal Settings](#) on page 226.
11. Import, upload, and remove login page files, and optional success and failure page HTML files in an admin-defined directory as described in [Import Captive Web Portal HTML Files](#) on page 229.
12. If you intend to use MAC Authentication, see [Configure MAC Authentication](#) on page 62.
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 70 to add a wireless network (SSID)-specific RADIUS object. See [Configure External RADIUS Server Settings](#) on page 214 to add an external RADIUS common object.
14. If you intend to authenticate via user groups (Enterprise only), turn on **Authentication with ExtremeCloud IQ Authentication Service**.
15. Either select an existing User group from the current list or select the plus sign to add a new group.
See [Add a User Group](#) on page 41.
16. Either use the existing **Default User Profile** from the current display or select the plus sign to add a new profile.
See [Add a User Profile](#) on page 152.
17. To customize the **SSID Availability Schedule**, select the **Restrict the availability of this SSID to selected schedules** check box to enable SSID schedules.
18. Select **Customize**.
To create a new schedule, see [Configure Availability Schedule Settings](#) on page 153.
19. To customize **Advanced Access Security Controls**, see [Customize Advanced Access Security Settings](#) on page 68.
20. To customize **Optional Settings**, see [Customize Wireless Network Optional Settings](#) on page 60.
(Not available for 6 GHz).
21. Turn **Client Monitor On** (default) to enable a device to detect client issues, and report client connection activities and problems to ExtremeCloud IQ.
22. Select **Save**.

What to Do Next

Continue configuring your network policy.

About SSID Usage in Standard Wireless Networks

As part of configuring a standard wireless network, you need to 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 56.
- **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 57.
- **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 58.
- **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 62.

Configure Enterprise SSID Authentication

Before You Begin

Create a standard wireless network policy. For more information, see [About SSIDs](#) on page 128.

About This Task

Use these steps to configure Enterprise SSID authentication options.

Procedure

1. Select **Enterprise-802.1X**.

This requires users to authenticate themselves by entering a user name and password, which are checked against a RADIUS authentication server.

2. Select the required **Key Management** and **Encryption Method** options from their respective drop-down menus or leave them at the default values.

Key Management options:

- **WPA3-802.1X** uses 192-bit encryption, and simultaneous authentication of equals (SAE) instead of PSK exchanges. If all wireless clients support WPA3, it is a better choice than WPA2.
- **WPA2-802.1X** supports PMK caching and preauthentication (WPA does not). If the wireless clients support WPA2, it is the better choice over WPA, and is the default.
- **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.
- Choose **Auto-(WPA or WPA2) 802.1X** to negotiate the use of WPA2 or WPA with clients based on which version they support.

For **Encryption Method** Option:

CCMP (AES) (Counter Mode-Cipher Block Chaining Message Authentication Code Protocol) 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).

Configure Personal SSID Authentication

Before You Begin

Create a standard wireless network policy. For more information, see [About SSIDs](#) on page 128.


About This Task

This option requires all users to authenticate themselves by entering the same pre-shared key. Select the required **Key Management**, **Encryption Method**, and **Key Type** entries from their respective drop-down menus or leave them at their default values, and enter a required value in the **Key Value** text box.

Procedure

1. Select **Personal** SSID Authentication.

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. WPA2 supports PMK caching and pre-authentication, whereas WPA does not.
 - Select **WPA-(WPA or Auto)-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 support WPA (not WPA2), this option allows the Extreme Networks device to support them.
 - **Auto-(WPA or WPA2)-PSK** to negotiate the use of WPA2 or WPA with clients based on the version they support.
 3. For **Encryption Method** (WPA or WPA2 only): Choose **CCMP (AES)**.

CCMP (AES) (Counter Mode-Cipher Block Chaining Message Authentication Code Protocol) is a security protocol that 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).
-  **Note**
When the SSID is configured for WPA3 (SAE), the encryption method is always set to 128-bit encryption.
4. To define the **Key Type** (WPA or WPA2 only) value with ASCII characters, choose **ASCII Key**.
 5. For **Key Value**, enter the pre-shared key and **Confirm** it.

Configure Private Pre-Shared Key SSID Authentication

Before You Begin

Create a Standard Wireless Network configuration.

About This Task

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. Use these steps to configure Private Pre-Shared Key SSID authentication options.



Note

ExtremeCloud IQ Connect does not support Private Pre-Shared Keys.

Procedure

1. Choose one of the following **Key Management** options:
 - **WPA3 (SAE)** to negotiate using WPA3 with clients. If all the wireless clients support WPA3, it is a better choice than WPA2.
 - **WPA2-(WPA2 Personal)-PSK** to use WPA2 for key management. WPA2 supports PMK caching and pre-authentication, whereas WPA does not.
 - **WPA-(WPA or Auto)-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 support WPA (not WPA2), this option allows the Extreme Networks device to support them.
 - **Auto-(WPA or WPA2)-PSK** to negotiate the use of WPA2 or WPA with clients based on the version they support.
2. For **Encryption Method** (WPA or WPA2 only): Choose **CCMP (AES)**.

CCMP (AES) (Counter Mode-Cipher Block Chaining Message Authentication Code Protocol) is a security protocol that uses AES (Advanced Encryption Standard) encryption. CCMP provides message integrity by combining counter mode with CBC (cipher block chaining) to produce a MAC.



Note

When the wireless network (SSID) is configured for WPA3 (SAE), the encryption method is always set to 128-bit encryption.

3. Enter the maximum number of simultaneous clients allowed for each PPSK user, from 1 through 15, or 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.

4. If necessary, select **MAC binding**.

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.

- a. Choose an Extreme Networks AP from the list to define it as a PPSK server.

A PPSK server stores PPSK users, binds multiple client MAC addresses to a PPSK, and automatically updates and tracks PPSK-to-MAC address bindings. It must be an AP that is at the network policy's site. Extreme Networks APs (PPSK authenticators) at the same site contact this server when checking and requesting a user-submitted PPSK binding to the user's client MAC address.

**Note**

Only APs that you previously configured with static network settings appear in the PPSK server list.

5. To configure **Private Client Group Options**, see [Configure a Private Client Group](#) on page 46.
6. Select **PPSK Classification Options** to use this network policy with associated Local User Groups.

See [Configure a Local User Group](#) on page 45 for more information.

What to Do Next

Continue configuring the Standard Wireless Network.

Customize Wireless Network Optional Settings

Before You Begin

Configure a standard wireless network.

About This Task

When you configure an SSID, you can configure and apply radio rates, DoS prevention settings, traffic filters, and other options.

Procedure

1. Select **Optional Settings CUSTOMIZE** under **Additional Settings**.
2. For **Radios and Rates**, select the radio frequency and set the basic (mandatory) and optional data rates per SSID.

By default, Extreme Networks devices advertise support for all rates on their SSIDs. 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 your SSID, which can help increase average data transfer rates.
3. See [Customize DoS Prevention](#) on page 64 for **DoS Prevention** customization instructions.

4. Select **Traffic Filters** to control which management and diagnostic services an AP is permitted to receive and whether it allows traffic between clients connected to the AP by selected traffic filters.
 - a. Select the appropriate check boxes to permit specific types of management and diagnostic access to the mgt0 interface, and enable traffic between clients connected to the AP.
 - b. Clear the check boxes to deny access.

**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.

5. Use **Choose User Profile Application Sequence** in cases where different components in the SSID reference different user profiles.

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 what 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.

6. For **Voice Enterprise**, see [Configure Voice Enterprise Options](#) on page 65.
7. Select **Enable WWM** to enable WiFi Multimedia™ to prioritize network traffic.
 - a. Select **Voice** to enable admission control algorithms for voice traffic.
 - b. Select **Video** to enable admission control algorithms for video traffic.
 - c. Select **Enable Unscheduled Automatic Power Save Delivery** to enable stations to request queued traffic at any time, rather than receiving queued traffic scheduled with the beacon.
8. For the **Broadcast and Multicast Handling** section, see [Customize Broadcast and Multicast Handling Settings](#) on page 63.
9. In the **Client Related Network Settings** section, define client usage parameters to 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.
 - **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.

- **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.
 - **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.
 - **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.
10. Select **Ignore broadcast probe request** to enable Extreme Networks devices hosting this SSID to ignore probe requests from wireless clients.
 11. 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 provides very little protection against anything but the most casual intrusion efforts.

12. Select **Save**.

What to Do Next

Continue configuring the wireless network policy.

Configure MAC Authentication

Before You Begin

Create a standard wireless network (SSID).

About This Task

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.

Procedure

1. Select **MAC Authentication** and toggle the switch to **On**.
2. 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.

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.

What to Do Next

Continue configuring a standard wireless network.

Customize Broadcast and Multicast Handling Settings

Before You Begin

Select **Optional Settings CUSTOMIZE** under **Additional Settings** in the **Configure Standard Wireless Networks** window.

About This Task

This task is part of a series of optional settings for configuring a standard wireless network. 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 i 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.

Procedure

1. For the **Convert IP Multicast to Unicast** option, select one of the following settings:
 - **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.

2. Set the **Channel Utilization Threshold** from 1 to 100%.
3. Set the **Membership Count Threshold** from 1 to 30.
4. Select **Enable Non-Essential Broadcast Filtering** to reduce unnecessary broadcast and multicast traffic forwarding (such as LLC, STP, and MDNS) from APs with no registered listeners.
5. Select **Enable Multicast Drop** to drop selected multicasts. You can then select multicasts to drop or to exclude from the drop:
 - **DHCPv4**: Clear the check-box to drop Dynamic Host Configuration Protocol version 4. (Selected by default.)
 - **DHCPv6**: Clear the check box to drop Dynamic Host Configuration Protocol version 6. (Selected by default.)
 - **ARP**: Clear the check box to drop Address Resolution Protocol. (Selected by default.)
 - **IGMP-query**: Clear the check box to drop Internet Group Management Protocol queries. (Selected by default.)
 - **IPv6-Discovery**: Clear the check box to drop Internet Control Message Protocol router discovery messages. (Selected by default.)
 - **MDNS**: This check box is not selected by default. Select this check box to drop multicast DNS frames. (Not selected by default.)

What to Do Next

Continue configuring Optional Settings in the Standard Wireless Networks configuration window.

Customize DoS Prevention

Before You Begin

Select **Optional Settings Customize** under **Additional Settings** in the **Configure Standard Wireless Networks** window.

About This Task

This task is part of a series of optional settings for configuring a standard wireless network policy. In the **DoS Prevention** section, configure defensive settings to protect against Denial of Service (DoS) attacks, and configure SSID access filters based on MAC addresses.

Procedure

1. Under **MAC-based Dos Prevention rules for**, select **SSID** 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.

2. Select **Client** 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.

3. Under **IP-based Dos Prevention rules for**, select **SSID** to protect 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.

4. **Enable MAC-Based filters** and select whether to **Deny** or **Permit** an action.

Choose **Permit** to enable traffic from clients that do not match one of the selected filters, or choose **Deny** to block traffic from clients that do not match any of the selected MAC filters.

What to Do Next

Continue configuring Optional Settings in the Standard Wireless Networks configuration window.

Configure Voice Enterprise Options

Before You Begin

Navigate to **Optional Settings CUSTOMIZE** under **Additional Settings** in the **Configure Standard Wireless Networks** window.

About This Task

This task is part of a series of optional settings for configuring a standard wireless network. Use this task to configure Voice Enterprise options.



Note

To enable Voice Enterprise or 802.11r, the SSID must be configured to use WPA2 key management.

Procedure

1. Select **Enable Voice Enterprise** to enable all options that are required for full voice enterprise support.
2. Select **Custom** and choose from 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 both 2.4 GHz and 5 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.

What to Do Next

Continue configuring Optional Settings.

Configure a Classification Rules Network Policy

Before You Begin

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. You should also create cloud config groups, IP addresses, and IP subnets.

About This Task

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.

Procedure

1. Select the plus sign on the appropriate default AP template screen.
2. Enter the new AP template name.
3. Select **Save Template**.

The new template is displayed on the main AP template window. The **Classification Rules** column for this template now contains a plus sign and arrow sign. Use the arrow sign to assign an existing rule and the plus sign to create new rules.

4. In the **Classification Rules** column, select the arrow sign to assign an existing classification rule.
5. Select **Link**.
6. Select the plus sign in the **Classification Rules** column to add a new classification rule.
7. Enter a name for the rule.
8. Enter an optional description.
9. Select the plus sign and the rule type to configure.
10. If you selected **Device Location**, perform the following steps:

- a. Open each location level until you reach the level where the device resides.
- b. Choose **Select**.

The location is displayed in the Classification Rule table.

11. If you selected **Cloud Config Group**, perform the following steps:

- a. Select the **Match Type**.
- b. Select an existing group from the drop-down list.

To add a new group, select the add icon. For more information, see [Add a Cloud Config Group](#) on page 116.

- c. Select **Save Rule**.

12. If you selected **IP Address**, perform the following steps:

- a. Select the **Match Type**.
- b. Select an existing IP address from the drop-down list.

To add a new IP address, select the add icon.

- c. Select **Save IP**.

13. If you selected **IP Subnet**, perform the following steps:

- a. Select the **Match Type**.
- b. Select an existing IP subnet from the drop-down list.

To add a new IP subnet, select the add icon.

- c. Select **Save Subnet**.

14. If you selected **IP Range**, perform the following steps:
 - a. Select the **Match Type**.
 - b. Select an existing IP range from the drop-down list.
To add a new IP range, select the add icon.
 - c. Select **Save IP**.
15. 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.
These objects are considered using a top-down, first-match, stop-on-match method, so if a device is a member of more than one matching object for an element, only the first match is applied.
16. Select **Save Rule**.

Customize Advanced Access Security Settings

About This Task

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, manage and set up Pairwise Transient Keys.

Procedure

1. For **Generate new Group Master Key (GMK) after**, enter the time interval until a new GMK is generated.
The GMK is a large random number that an Extreme Networks device chooses. From the GMK, the device derives a GTK (Group Temporal Key), which it then sends to all associated clients within EPOL-key messages. The Extreme Networks device and clients use the GTK to encrypt and decrypt broadcast or multicast traffic transmitted between themselves.
2. For **Generate New Group Temporal Key (GTK) after**, enter the time interval until a new GTK is generated.
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.
3. For **GTK Timeout Period**, set the interval 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.
4. For **Number of GTK Retries**, set the maximum number of times the device will retry sending GTK messages.

5. Select **Generate a new Pairwise Transient Key (PTK) after** 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 to configuring PTK rekeying on devices, it might also need to be enabled 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 it is not possible to 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.

6. For **PTK timeout period**, set the interval 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.

7. For **Number of PTK retries**, set the maximum number of times the device will retry sending PTK messages.
8. For **Replay window**, set 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.

9. Select **Local TKIP Countermeasure** (available when the encryption method is Auto-TKIP or CCMP (AES) or TKIP) to enable or disable the deauthentication of all clients when the local device detects message integrity check failures during TKIP operations.

Even if just 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 its existing keys and maintain currently connected clients after detecting MIC failures.

10. Select **Remote TKIP Countermeasure** (available when the encryption method is Auto-TKIP or CCMP (AES) or TKIP) 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 of the failure occurs: local = the device discovered it, remote = the client discovered—and reported—it.

11. Deselect **Refresh GTK when client disassociates from the SSID** to refresh the GTK whenever a client disassociates from the SSID.

About RADIUS Authentication

RADIUS authentication is used for 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 their 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.

Related Topics

[Add a RADIUS Server Group](#) on page 70

[Configure RADIUS Server Settings](#) on page 70

[Configure External RADIUS Server Settings](#) on page 214

[Configure an Extreme Networks Device as a RADIUS Proxy](#) on page 72

[Configure a RADIUS Proxy Server Realm](#) on page 72

[Configure an Extreme Networks Device as a RADIUS Server](#) on page 74

[Add an Active Directory Server](#) on page 75

[Configure an LDAP Server](#) on page 230

Add a RADIUS Server Group

About This Task

RADIUS servers offer two different types of services:

- Authentication for user credentials (usually on port 1812)
- Accounting (logging) (usually on port 1813)

Security on RADIUS servers is handled with simple passwords. One is configured on the server and the other on each of the clients.

Procedure

1. Enter the group's name.
2. Enter an optional description.
3. Enter the group's **IP/Hostname**.
4. Accept the defaults or enter specific **Server Type** ports.
5. Enter an optional password.
6. Select **ADD**.

Configure RADIUS Server Settings

Before You Begin

You must 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.

About This Task

Extreme Networks devices use the 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 group based on their location or other parameters. 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. Use this task for your configuration.

Procedure

1. Choose a RADIUS server group profile name.
2. Enter an optional server group description.
3. Select **Settings** next to the description field and enter or select the following:
 - **Retry Interval:** Enter an unresponsive primary RADIUS server Access-Request retry time. The device retries the primary server after the interval elapses, even if the current backup server is responding.



Note

You cannot enter commas in this field. 100,000,000 must be entered as 100000000.

- **Accounting Interim Update Interval:** Set the interval for sending RADIUS accounting updates to report the client session status and cumulative length.



Note

You cannot enter commas in this field. 100,000,000 must be entered as 100000000.

- **Permit Dynamic Change Of Authorization Messages (RFC 3576):** Enable the RADIUS server to dynamically change a user's authorization 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's 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 message that the Extreme Networks RADIUS authenticators send to the RADIUS authentication server. This attribute's 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.
- **Message Authenticator attribute:** The Message Authenticator is used to authenticate the RADIUS server's reply, and encrypt passwords.

4. From the **RADIUS server lists**, select up to four existing servers to add to your wireless network (SSID) RADIUS server group.
 - If there are no RADIUS servers available, see [Configure External RADIUS Server Settings](#) on page 214.
 - If there are no Extreme Networks A3 Servers available, see [Configure an Extreme Networks A3 Server](#) on page 230.
 - If there are no Extreme Networks RADIUS Servers available, see [Configure an Extreme Networks Device as a RADIUS Server](#) on page 74.
5. Select **Save RADIUS Settings** and **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.

What to Do Next

Return to the Wireless Network screen to complete the Network Policy configuration.

Configure an Extreme Networks Device as a RADIUS Proxy

Before You Begin

Before you can perform this task, you must have a network policy with an SSID with Enterprise (WPA/WPA2 802.1X) access security, and a default RADIUS server group.

About This Task

Use this task to configure RADIUS proxy server parameters, including the parameters for realms, a RADIUS server group, approved RADIUS clients, and other realm settings.

Procedure

1. Select the device to configure as a proxy server.
2. Enter a name.
3. Enter an optional description.
4. For the **Realms** section, see [Configure a RADIUS Proxy Server Realm](#) on page 72.
5. For the **Approved RADIUS Clients** section, see [Add Approved RADIUS Clients](#) on page 74.
6. For the **Realm Settings** section, see [Configure Realm Settings](#) on page 73.
7. Select **SAVE RADIUS PROXY**.

Configure a RADIUS Proxy Server Realm

Before You Begin

Configure an Extreme Networks Device as a RADIUS proxy server.

About This Task

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. The following steps are part of the Realms section of the RADIUS Proxy Server page.

Procedure

1. For **Add a RADIUS Server Group**, see [Add a RADIUS Server Group](#) on page 70
2. Select the **Default Realm** from the drop-down list.
3. Select whether or not the **Default Realm** strips the realm name from proxied access requests.
4. Select the **NULL Realm** from the drop-down list.
5. Select the plus sign to create new Realm.
6. Enter a name.
7. Select a RADIUS server group from the drop-down list.
8. Select whether or not the new realm strips the realm name from proxied access requests.
9. Select **ADD**.

What to Do Next

Continue configuring the Proxy server.

Configure Realm Settings

Before You Begin

Configure an Extreme Networks Device as a RADIUS proxy server and create a Realm.

About This Task

Use this task to optimize Realm configurations.

Procedure

1. 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.
2. Enter the delay between retries.
3. Enter the count for number of retries before declaring failure.
4. Enter the dead time before declaring failure.
5. Select whether or not to inject an operator-named attribute.

What to Do Next

Continue configuring the Proxy server.

Add Approved RADIUS Clients

Before You Begin

Configure an Extreme Networks Device as a RADIUS proxy server.

About This Task

You can assign one or more approved RADIUS clients to each configured realm associated with a RADIUS Proxy Server.

Procedure

1. Select the **Approved RADIUS Clients** section.
2. Select the plus sign.
3. Select the client's **IP/Host Name/Network**.
4. If required, select the plus sign to create a new **IP Address, Host Name or Network**.
5. Enter the associated password.
6. Enter an optional description.
7. Select **ADD**.

What to Do Next

Continue configuring the server.

Configure an Extreme Networks Device as a RADIUS Server

Before You Begin

Before you can perform this task, you must have a network policy with an SSID with Enterprise (WPA/WPA2 802.1X) access security, and a default RADIUS server group.

About This Task

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.

Procedure

1. Select a **User Database Type** from the drop-down list or select the plus sign.
2. If you selected the plus sign, select a device to configure as a RADIUS Server.
3. Continue to the Configure AAA Server Profile section and see [Configure an AAA Server Profile](#) on page 222.

4. If you selected Active Directory in your AAA Server Profile, see [Add an Active Directory Server](#) on page 75.
5. If you selected LDAP Server in your AAA Server Profile, see [Configure an LDAP Server](#) on page 230.
6. Select **SAVE RADIUS SERVER**.

Add an Active Directory Server

Before You Begin

Configure an Extreme Networks device as a RADIUS Server.

About This Task

Use this task to add an Active Directory to an Extreme Networks device acting as a RADIUS Server.

Procedure

1. Enter a name.
2. Enter the Windows domain name that the RADIUS authentication server and Active Directory server both belong to, including parent domains, such as .com, .net, and .org
3. Select **Auto** to enable the Active Directory and ExtremeCloud IQ to automatically supply the Active Directory Server and the base distinguished name parameters.
4. 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.

5. Enter the base distinguished name, or the starting point for directory server searches, and the point in the directory tree structure where the server stores user accounts.
6. If you selected **Manual**, enter a **Short Domain Name**.
7. If you selected **Manual**, enter the **Realm** name that corresponds to the user account location, which is often the same as the domain name.
8. 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. Because you might 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`.

9. Select **Enable TLS Encryption** to encrypt the user look-up requests that the Extreme Networks RADIUS server sends to the Active Directory server.
10. Select **NEXT**.

11. Select a **DNS Server** or select plus to create a new one.
12. Select **NEXT**.

What to Do Next

Continue configuring the server.

About 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 and allows you to assign port types to the device ports, which defines how the ports assigned to it will function.
- **VPN Service** - Layer 3 IPsec VPN tunnels securely send traffic between Extreme Networks routers and one or two Extreme Networks VGVA's (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** - Policy-based routing enables you 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 whitelist, blacklist, 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 Router Firewall Policy](#) on page 193.
- **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** - You can 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 a Router Template

About This Task

A router template is a diagram of the physical ports for a specific Extreme Networks router model and allows you 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.

Procedure

1. Select **ADD** and choose the appropriate device template your model.
2. In the device template, assign ports with the connection types that you want them to provide: access, 802.1Q, and WAN.
3. Enter a template name.
4. 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
5. To create a new port type, select **Assign > Create New** and enter the following in the **New Port Type** section:
 - a. Enter a port type name.
 - b. Enter 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.

6. 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 70 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**.

7. 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 152 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.
8. 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:** Enter 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 enter the word `a11` to support all existing VLANs previously configured in the network policy. When you enter `a11`, 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.
 9. 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.
 10. **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.

Configure Network and IP Address Allocation

Before You Begin

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

About This Task

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.

Procedure

1. Select **Add** to create a new VLAN-to-subnetwork mapping.
2. Choose **Select** and either choose a VLAN from the drop-down list or select **New** to define one.
To add a VLAN, see [Configure VLAN Settings](#) on page 170.
3. Choose **Select** to choose an existing subnetwork from the list or select **New** to define one.
To add a subnetwork, see [Add a Subnetwork Space](#) on page 217.
4. 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 need to add a new subnetwork for the additional branch sites. By keeping the VLAN the same, you can 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 when it has used all of those from the first one.
5. Select **Save**.
6. Select the add icon to add IP allocation settings.
7. Select a branch name for the router from the drop-down list.
8. Select the serial number of this device from the drop-down list.
The host name for the router is automatically displayed.
9. Select a subnet entry from the dropdown list.
10. Select **Next**.

What to Do Next

Configure DNS settings.

About 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).

Layer 3 IPsec VPNs

Layer 3 IPsec VPN tunnels securely send traffic between Extreme Networks routers and one or two Extreme Networks VGVA (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 82. Use **Manage > VPN Services** to view the existing VPN services in your network configuration.

Layer 2 IPsec VPNs

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.

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.

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 VPN Services](#) on page 195.



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.

Configure Layer 3 VPN Services

Before You Begin

Enable VPN Services for the router in the **Router Settings** section of the network policy.

About This Task

Use this task to configure Layer 3 IPsec VPNs. You can 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 configure the default routing policy and any policy exceptions.

Procedure

1. Select to add a new VPN Service.

2. Enter a name for this service.
3. Enter an optional description.
4. Select either **Extreme Networks VPN Gateway** or **Third Party Gateway**.
5. If you selected **Extreme Networks VPN Gateway**, configure the following information:
 - a. Enter the number of branch sites that you expect will build tunnels to the VPN gateway.
 - b. Enter the maximum tunnels per gateway.
 - c. Select whether to have VPN tunnel addressing be automatic or use a WAN interface IP address.
 - d. Select the add icon below **VPN Gateway Settings** and then **Select** a VPN Gateway from the drop-down list.

The VGVA's that display in this list have been added to the network as Layer 3 VPN gateways. To change a VGVA's setting, go to **Manage > Devices**.
6. Select **Auto** to have IP addresses automatically generated, or **WAN Interface IP addresses** to use a specific address.
7. If you selected **Third Party Gateway**, configure the following information:
 - a. Select a vendor from the drop-down list.
 - b. Enter the IP address of the third-party VPN gateway.
 - c. For the **VPN Access List** at the bottom of the page, select the plus sign and enter the required source and destination networks in the respective VPN access list text boxes.
8. Select **Generate** to create credentials for servers and clients.
9. For the remaining optional settings see:
 - [Configure IPsec VPN Authority Settings](#) on page 83
 - [Configure Advanced Server Options](#) on page 85
 - [Configure Advanced Client Options](#) on page 86

Results

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

Configure IPsec VPN Authority Settings

Before You Begin

Create a Layer 2 IPsec VPN service. For more information, see [About Server-Client Credentials](#) on page 84.

About This Task

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 their format from DER to PEM.

**Note**

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.

Procedure

1. If you do not have a certificate or key that you want to use, select **Import**.
2. 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.
3. 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 to each other.

About Server-Client Credentials

As soon as you save the Layer 2 IPsec VPN service configuration, ExtremeCloud IQ populates this 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 a device is configured as a VPN client, ExtremeCloud IQ allocates one of the credentials to it. The name of the VPN client displays 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.

Configure Advanced Server Options

Before You Begin

Create a Layer 2 IPsec VPN service. For more information, see [About Server-Client Credentials](#) on page 84.

About This Task

Use this task to change the IKE Phase 1 and Phase 2 options.

Procedure

1. For **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 are automatically refreshed 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).
2. For **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.
3. 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.

Configure Advanced Client Options

Before You Begin

Create a Layer 2 IPsec VPN service.

For more information, see [About Server-Client Credentials](#) on page 84.

About This Task

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. Use this task to specify which type of management traffic you want VPN clients to send through the tunnel and which to forward locally.

Procedure

1. 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.
2. Select **Enable NAT Traversal** to enable VPN traffic to traverse NAT devices encountered along its data path.
 3. For **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.
4. 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.

Configure an SD-WAN Route Group

Before You Begin

Before you can enable SD-WAN, you must assign a branch ID to the router, and have one or two Extreme Networks VGVA's configured as part of a **VPN Service**. Then create a Network Policy with Router Settings.

About This Task

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.

Procedure

1. Select **Enable SD-WAN**.
2. Select **Add**.
3. Enter a **Group Name**.
4. Enter an optional description.
5. 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.
6. 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.

What to Do Next

Continue configuring the network policy.

Configure a Routing Policy

Before You Begin

Create a Network Policy. For more information about router policies, see [About Router Settings](#) on page 76.

About This Task

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 can only 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.

Procedure

1. Select **Enable Routing Policy** under the **Router Settings** tab.
2. If not selecting an existing policy, select **ADD**.
3. Enter a name.
4. Enter an optional description.
5. 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.

6. 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.
7. To configure **Path MTU Discovery**, see [Configure Path MTU Discovery](#) on page 89.
8. For more information, see [Configure a Router Firewall Policy](#) on page 193, [Configure Dynamic DNS](#) on page 91, and [Configure URL Filtering Rules](#) on page 90.

What to Do Next

Continue configuring the network policy.

Configure Path MTU Discovery

Before You Begin

Create a **Network Policy** and a **Routing Policy**.

About This Task

Path MTU Discovery allows the router to 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.

Procedure

1. Select **Enable Path MTU Discovery** to enable the Extreme Networks router to learn the maximum packet size that can be sent between two hosts without fragmentation.

2. 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:** Set the TCP-MSS threshold for all TCP connections passing through the device. If you do not enter 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:** Set the TCP-MSS threshold for TCP connections that pass through a Layer 3 VPN tunnel. If you do not enter a threshold value, the device uses the value set for the MSS threshold for all TCP connections.

What to Do Next

Continue configuring the network policy.

Configure URL Filtering Rules

Before You Begin

First create the user profiles to be associated with your URL filtering rules.

About This Task

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.

Procedure

1. Select the add icon.
2. Enter a name for the rule.
3. Enter an optional description.
4. 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.

5. Select the **Whitelist** subtab.
 - 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
```

6. Select the **Blacklist** subtab.
 - 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.
7. Select the **Categories** subtab.
8. Choose the categories this rule blocks.
9. 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**.
10. Select **Save Detail**.
11. Continue adding filters if needed.
12. Select **Save URL Rule**.
13. 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 152.

What to Do Next

Add this **URL Filtering Rule** to a network policy **Router Settings**.

Configure Dynamic DNS

Before You Begin

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

About This Task

Use the following steps to configure DDNS.

Procedure

1. Toggle the Dynamic DNS switch to **On**.
2. Select a DDNS provider.
3. Enter a user name.
4. Enter a password.
5. Enter the domain name, which must be the full router name and domain name.
The router host name must be unique.
6. Select **Save**.

Configure WAN Tracking

Before You Begin

Create a Network Policy with Router Settings.

About This Task

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.

Procedure

1. Enter a different **Primary IP Target** or accept the default.
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.
2. Enter an optional **Secondary IP Target**.
3. Specify the **Number of Retries** before the router marks the link as unavailable.
4. For the **Measurement Interval**, enter the number of seconds between retries.
5. Select **Reset to Default** to return these settings to the factory defaults.

What to Do Next

Continue configuring the network policy.

Configure Device Templates

Before You Begin

Create a network policy.

About This Task

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, apply this device template and its configuration settings to large

numbers of devices of the same type, and 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.

Procedure

1. To add an AP template to the network policy, select **Wireless** in the workflow and proceed to [Configure AP Templates](#) on page 101.
2. To add a switch template to the network policy, select **Switching** in the workflow and proceed to [Configure Switch Templates](#) on page 134.
For legacy and Dell switch models, select **SR/Dell Switching** in the workflow.
3. To add a branch router template to the network policy, select the **Branch Routing** step in the workflow and proceed to [Configure a Router Template](#) on page 77.

What to Do Next

Continue configuring the network policy.

Related Topics

[Configure AP Templates](#) on page 101

[Configure Switch Templates](#) on page 134

Configure a Hive Profile

About This Task

Perform the following steps to configure a hive profile.

Procedure

1. Select the add icon.
2. Enter a name for the hive profile.
3. Select a number for the hive control traffic port.
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 5 digits 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 3005.
4. Enter an optional description.
5. Select to enable or disable CAPWAP delay alarms.
6. Enable **Encryption Protection**, or disable it to have ExtremeCloud IQ derive a default password from the hive name.

7. Select either **Auto Generate a password**, or enter a password manually.

Hive members use this password when authenticating themselves to each other over the wireless backhaul link using WPA-PSK CCMP (AES). To see the text that you entered, clear the **Obscure Secret** check box.
8. Modify DoS prevention rules by selecting either **Hive** or **Client**, and modifying the settings in the dialog box.

Extreme Networks devices ship with the default hive- and SSID-level 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.
9. Select a **Request to Send Threshold** for wireless mesh.

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.
10. Select a **Fragment Threshold** for wireless mesh.

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.

11. Select the check box to require a minimum wireless signal strength for creating wireless mesh, and configure the following settings:
 - Signal strength threshold:** Choose a signal strength between 90 dBm and -55 dBm. This is the minimum signal strength required to enable members to form a wireless backhaul link. The default is -80 dBm.
 - Polling interval:** Set the time interval from 1 to 60 minutes to poll 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 this 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.
12. Configure client roaming settings by first setting the interval between keepalive heartbeats between members.
13. Select the number of missed heartbeats before a neighbor is removed.
 - The default is 10 seconds, and the range is 5 to 360,000 seconds (100 hours). To calculate the length of time required, multiply the keepalive interval by the ageout value. Using the default settings, 10 seconds (interval) x 5 (missed keepalives), a neighbor ages out after 50 seconds.
14. Select how often devices should send client information (default is 60 seconds).
15. Select the interval after which cached client information is removed (default is 60 seconds).
16. Select the check box to update all hive members within radio range, including Layer 3 neighbors.
17. Select the check box to update hive members in the same subnet and VLAN.
18. Select an IP address type.
19. Apply MAC filters to restrict devices that can join the hive.
 - You can select existing filters from the table, or add new filters.
20. Choose the default action for any device whose MAC address or OUI does not match the selected MAC filter.
21. Select **Save**.

Configure Device Data Collection and Monitoring Options

Before You Begin

Create a network policy for these settings.

About This Task

Use this task to set 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.

Procedure

1. Toggle **Application Visibility and Control On** to detect frame application-layer contents.
2. Toggle **Statistics Collection On** to record wireless activity statistics between the device and connected clients.

You can also change the data collection interval.

3. For **Device Wireless Activity Thresholds**, set the following:
 - **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.

4. For **Client Wireless Activity Thresholds**, set the following:
 - 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.
5. Toggle **Kernel Diagnostic Data Recorder On** to capture run-time statistical data about unexpected events.
6. For **Automatic Synthetic Traffic Generation**:
 - a. Enable RADIUS Authentication to create synthetic traffic.
 - b. Turn **Check Radius service connectivity via Status-Server On** to check RADIUS service connectivity.
 - Make sure **Status-Server** is enabled on the RADIUS server.
 - c. Adjust the check **Interval** if necessary.

Configure iBeacon Service

Before You Begin

Configure a network policy.

About This Task

You can configure the embedded iBeacon 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 an iBeacon signal by displaying welcome messages, sale announcements, or coupons.

Procedure

1. Toggle **iBeacon Service On**.
2. Enter a name.
3. Enter an optional description.
4. If your organization already has a UUID number, enter this number in the **iBeacon UUID** field, formatted appropriately with hyphens separating the groups of numbers.
 - You can also automatically create a UUID with an online UUID generator, such as the one at <https://www.uuidgenerator.net/>.
5. Select **Enable iBeacon Monitoring**.

Configure Presence Analytics

Before You Begin

Configure a network policy.

About This Task

Use this task to specify how frequently APs send data to ExtremeCloud IQ. These parameters enable adjustments to accommodate situations where devices are connected over slower links and where the data must be aggregated at different rates.



Note

It is not necessary to change the default values if devices are connected over faster links.

Procedure

1. Toggle **Enable Presence Analytics On**.
2. Enter a name.
3. Enter an optional description.
4. For **Trap Interval**, set 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.
5. Set the **Aging Time** of a given presence profile.
6. Set the **Aggregate Time** interval number for the period of time that aggregation will be done for a given presence profile.



Configure Common Objects

- [Configure AP Templates](#) on page 101
- [Configure Auto-Provisioning](#) on page 111
- [Configure a Bonjour Gateway](#) on page 113
- [Configure a Classification Rules Common Object](#) on page 114
- [Add a Cloud Config Group](#) on page 116
- [Configure Port Types](#) on page 116
- [About Radio Profiles](#) on page 117
- [Configure an SDR Profile](#) on page 128
- [About SSIDs](#) on page 128
- [Configure Switch Templates](#) on page 134
- [Configure URL Filtering Rules](#) on page 150
- [Add a User Profile](#) on page 152
- [Add Application Sets](#) on page 157
- [About Client Mode Profiles](#) on page 157
- [Configure DHCP Servers and DHCP Relay Agents](#) on page 164
- [Add a DNS Service](#) on page 166
- [Add IP Objects and Host Names](#) on page 168
- [Add a MAC Object and Host Name](#) on page 168
- [Add a Notification Template](#) on page 169
- [Configure OS Objects](#) on page 169
- [Configure VLAN Settings](#) on page 170
- [Add a VLAN Group](#) on page 171
- [Configure Supplemental CLI](#) on page 172
- [Add IP Firewall Policy Rules](#) on page 172
- [Add a Network Service Object](#) on page 173
- [Add MAC Firewall Policy Rules](#) on page 174
- [Traffic Filters](#) on page 175
- [Configure MGT IP Filters](#) on page 176
- [Add a WIPS Policy](#) on page 177
- [Configure Rogue AP Detection](#) on page 177
- [About QoS](#) on page 180
- [Configure a DNS Server](#) on page 187

- [Configure an NTP Server](#) on page 188
- [Configure an SNMP Server](#) on page 189
- [Configure a Syslog Server](#) on page 190
- [Configure an Access Console](#) on page 191
- [Configure ALG Services](#) on page 192
- [Configure a Router Firewall Policy](#) on page 193
- [Configure an IP Tracking Group](#) on page 194
- [Configure Layer 2 VPN Services](#) on page 195
- [Configure LLDP and CDP Settings](#) on page 200
- [Configure Location Servers](#) on page 201
- [Add Management Options](#) on page 205
- [Configure External RADIUS Server Settings](#) on page 214
- [Configure Network Services](#) on page 215
- [Configure an sFlow Receiver](#) on page 216
- [Add a Subnetwork Space](#) on page 217
- [Configure Tunnel Policies](#) on page 221
- [Configure an AAA Server Profile](#) on page 222
- [About Captive Web Portals](#) on page 224
- [Configure an Extreme Networks A3 Server](#) on page 230
- [Configure an LDAP Server](#) on page 230
- [Create a Certificate and Key](#) on page 232

Use this section to define objects that you can use throughout the configuration process, in particular when you are configuring network policies. Common object categories include:

- **Policy:** Network policy configuration objects, such as AP Templates, Auto Provisioning, Bonjour Gateways, Cloud Config Groups, Fabric Attach Profiles, Hives, Port Types, Radio Profiles, SDR Profiles, Schedules, and Classification Rules.
- **Basic:** Various categories, such as Application Sets, Client Mode Profiles, DHCP and DNS, IP, MAC, and OS Objects, Notification Templates, and VLANs.
- **Security:** Network security objects, including AirDefense Policies, IP and MAC Firewall Policies, MGT IP and Traffic Filters, and WIPS Policies.
- **QoS:** Classifier and marker maps, and rate control rules.
- **Management:** DNS, NTP, SNMP, and Syslog server objects.
- **Network:** Access consoles, ALG , LLDP/CDP profiles, IP tracking groups, Layer 2 IPsec/VPN services, location servers, management options, tunnel policies, sFlow receivers, network services, subnetwork space, firewalls, and VPN services.
- **Authentication:** Authentication methods, such as AAA servers, AD servers, captive web portals, external RADIUS servers, Extreme Networks A3, and LDAP servers.
- **Certificate:** Certificate management settings.

Configure AP Templates

Before You Begin

Create a network policy for APs (see [Configure Device Templates](#) on page 92). You can also configure an AP template directly from the **Common Objects** tab.

About This Task

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. What you see displayed is based on the device model.



Note

When AP device templates and auto-provisioning rules (see [Configure Auto-Provisioning](#) on page 111) are both in place for an AP when it is onboarded, the auto-provisioning rules are applied and the device template is ignored.

Procedure

1. Select an existing AP Template, or select the plus sign to create a new template.
2. For a new template, enter a name, and for an existing template, edit where necessary.
3. Select a port or interface icon on the template graphic.
 - a. To select or deselect all the ports and interfaces, choose **Select All Ports** or **Deselect All Ports**.
4. To **Assign** an Ethernet port profile, see [Assign an Ethernet Port Profile](#) on page 101.
5. To create a new radio profile for a Wi-Fi port, see [Add a Radio Profile](#) on page 118.
6. To configure **Wireless Interfaces**, see [Configure Wireless Interfaces for an AP Template](#) on page 104.
7. To configure **Wired Interfaces**, see [Configure Wired Interfaces for an AP Template](#) on page 105.
8. To configure **SES-imagotag**, see [SES-Imagotag](#) on page 106.
9. To configure Advanced Settings, see [Configure AP Device Template Advanced Settings](#) on page 109.
10. Select **Save Port Type**.

What to Do Next

Continue configuring the network policy.

Assign an Ethernet Port Profile

Before You Begin

Create or edit an AP template.

About This Task

An Ethernet port profile lets you manage a variety of features such as port status (on or off), port usage (bridge access, bridge 802.1Q, or uplink), wired connectivity, and MAC authentication.

Use the following procedure to assign a port profile to device ports:

Procedure

1. To assign an existing port profile, select one or more Ethernet ports on the AP template graphic.
2. Select **Assign**.
3. Select **Choose Existing**.
4. Choose any of the options from the **Port Type Assignment** list, and select **Save**.
5. To create a new port profile, select **Create New**.
6. Enter a **Port Name** and an optional description.
7. 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.
8. For **Wired Connectivity**, enable **User Authentication**.
9. See [Configure External RADIUS Server Settings](#) on page 214 if you are not selecting an existing RADIUS Server Group.
10. Enable **MAC Authentication**, see [Configure MAC Authentication](#) on page 62.
11. For **QoS Settings**, see [Configure Marker Maps](#) on page 185.
12. For **User Access Settings**, to add a new User Profile, see [Add a User Profile](#) on page 152.
13. For **Traffic Filter Management**, see [Traffic Filters](#) on page 175.
14. For **Port Settings**, see [Configure LLDP and CDP Settings](#) on page 200.
15. For **STP Settings**, see [Configure STP Settings](#) on page 103.
16. For **Storm Control Settings**, see [Configure Storm Control Settings](#) on page 102.

What to Do Next

Continue configuring the AP template.

Configure Storm Control Settings

Before You Begin

Configure an Ethernet port in an AP template.

About This Task

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 configure thresholds for broadcast, multicast, unknown unicast, and TCP-SYN packets as a function of the percentage of interface capacity, number of bits per second, or number of packets per second.

Procedure

1. Adjust access traffic and 802.1Q (VLAN) traffic settings as follows:

Broadcast: Select to include broadcast traffic, traffic that is forwarded to all destinations simultaneously.

Unknown Unicast: Select to include Unicast 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.

2. Use the drop-down list to select **Byte-Based** or **Packet-Based thresholds**.

Byte-Based: Select to enter storm control values measured by the number of bytes a switch processes.

Packet-Based: Select to enter storm control values measured by the number of packets a switch processes.

3. The **Rate Limit** type depends on whether you selected packet-based or byte-based storm control values.

If you chose **Byte-Based**, select values using the number of kilobytes per second (KBps) or as a percentage of total access interface and 802.1Q interface capacities. If you chose **Packet-Based**, select PPS (packets per second).

4. Enter the Rate Limit threshold **Value** the switch uses to discard the selected types of traffic.

What to Do Next

Continue configuring the AP template.

Configure STP Settings

Before You Begin

Create an Ethernet port profile.

About This Task

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. 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 STP BPDU packets are received on a protected port, this feature disables that port and alerts the network admin.

Procedure

1. Toggle the switch to **On** to enable **STP Status**.
2. If you are enabling **BPDU Protection**, toggle the switch to **On** to enable **Edge Port**.
3. Select the **Bridge Protocol Data Units (BPDU) Protection** setting.
 - **Guard**: Controls whether a port explicitly configured as Edge disables itself if it receives 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 will transmit and receive BPDUs.
 - **Disable**: Turn off BPDU Protection.
4. Select a **Priority** for STP from the drop-down list.

What to Do Next

Continue configuring the Ethernet port.

Configure Wireless Interfaces for an AP Template

About This Task

This task provides steps for configuring the WiFi0 and WiFi1 ports on an AP template.

Procedure

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. Turn **Radio Status On**.
5. Select a radio profile from the drop-down list.

You can also add a new radio profile here, or clone and modify an existing radio profile. To add a new radio profile, see [Add a Radio Profile](#) on page 118.
6. 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 create 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.

What to Do Next

Continue configuring the AP template.

Configure Wired Interfaces for an AP Template

Before You Begin

Create or edit an AP template.

About This Task

Use this task to configure wired interfaces on the AP.

Procedure

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 will automatically translate SSDI configurations as well as global native and Management ports to reduce the added need of 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 follow the instructions [here](#).

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 follow the instructions [here](#).

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 **LLDP** for devices to advertise their identities, status, and capabilities to each other.
Devices can transmit data about themselves and receive transmitted data from other devices, but they cannot solicit and retrieve data from other devices.
12. Select **CDP** for devices to advertise an IP address that can send and receive SNMP traps.
13. Select **MCast Filter** to enable Multicast Rate Limiting on the interface for multicast/broadcast traffic, and configure **Multicast Rate Limit** to set the maximum rate (in Kbs) for incoming multicast traffic for the interface.

What to Do Next

Continue configuring the AP template.

NEW SES-Imagotag

SES-Imagotag is a solution for Electronic Shelf Labeling (ESL). The solution consists of the following:

- 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 SES-Imagotag:

- AP305C
- AP410C
- AP5010

Configure SES-Imagotag on a device template or for an individual AP override.



Note

Consider the following for the SES-Imagotag support.

- An ESL Server behind a NAT (Network Address Translation) or firewall is not supported.
- Do not make configuration changes during SES-Imagotag programming and setup.

Related Topics

[Configure SES-imagotag on a Device Template](#) on page 107

[Configure SES-Imagotag on a Device Override](#) on page 108

[SES-Imagotag Setup](#) on page 106

[Configure AP Templates](#) on page 101

NEW! *SES-Imagotag Setup***About This Task**

This topic outlines everything you need to consider when configuring the SES-Imagotag.

Procedure

1. AP device considerations:
 - 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. ExtremeCloud IQ considerations:
 - a. [Enable SES-Imagotag on the AP Device Template](#) or Override for a supported AP model.

The following access points support SES-Imagotag:

- AP305C
- AP410C
- AP5010

- b. Ensure that the LED on the ESL communicator is amber.

Results**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 Topics

[SES-Imagotag](#) on page 106

[Configure SES-imagotag on a Device Template](#) on page 107

[Configure AP Templates](#) on page 101

[Configure SES-Imagotag on a Device Override](#) on page 108

[SES-Imagotag Settings](#) on page 109

NEW! *Configure SES-imagotag on a Device Template*

About This Task

To configure SES-Imagotag on the device template, take the following steps:

Procedure

1. Go to **Configure > Common Objects > Policy > AP Templates**.
2. Select an AP template for one of the supported AP models.
The following access points support SES-Imagotag:
 - AP305C
 - AP410C
 - AP5010
3. Scroll down to the SES-Imagotag pane and select **Enable Imagotag**.
4. Configure the SES-Imagotag settings.

Related Topics

[SES-Imagotag Settings](#) on page 109

[Configure SES-Imagotag on a Device Override](#) on page 108

[SES-Imagotag](#) on page 106

[SES-Imagotag Setup](#) on page 106

NEW! *Configure SES-Imagotag on a Device Override*

About This Task

To configure SES-Imagotag on a device override, take the following steps:

Procedure

1. Go to **Manage > Devices**.
2. Select one of the supported AP models.
The following access points support SES-Imagotag:
 - AP305C
 - AP410C
 - AP5010
3. From the left pane, select **Configure > Interface Settings**.
4. Scroll down to the SES-Imagotag pane and select **Enable Imagotag**.
5. Configure the SES-Imagotag settings.

Related Topics

[SES-Imagotag Settings](#) on page 109

[Configure SES-imagotag on a Device Template](#) on page 107

[Configure AP Templates](#) on page 101

[SES-Imagotag](#) on page 106

[SES-Imagotag Setup](#) on page 106

NEW! SES-Imagotag Settings

Configure the following settings for SES-Imagotag support:

Server

The IP address of the SES-Imagotag server.

Channel

The RF channel used for SES-Imagotag 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.

Related Topics

[Configure SES-imagotag on a Device Template](#) on page 107

[Configure SES-Imagotag on a Device Override](#) on page 108

[SES-Imagotag](#) on page 106

[SES-Imagotag Setup](#) on page 106

Configure AP Device Template Advanced Settings

Before You Begin

Create or edit an AP template.

About This Task

ExtremeCloud IQ can update device firmware and reboot the device during onboarding.

Procedure

1. Select the **Advanced Settings** tab.
2. For **Upload 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 after uploading**, select **On**.



Note

Extreme Networks recommends disabling the reboot option when deploying devices in a meshed environment.

4. To use **Supplemental CLI**, select **On**.

For more information, see [Configure Supplemental CLI](#) on page 144.

5. Select a **Country Code** from the dropdown.

**Note**

For Legacy World and EU SKU devices, the template country code assignment only takes place when a device is initially onboarded.

6. Enable **POE Profile Override** (AP5010 only), select the override option from the dropdown, and hover over the **i** to view the corresponding override table.

What to Do Next

Complete configuring the device template.

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 management command.
- Configure the Fabric Attach Server port with VLAN to I-SID mapping.
- Establish data plane communication path for every configured VLAN.

Related Topics

[Configure Fabric Attach](#) on page 111

Configure Fabric Attach

Before You Begin

Physically connect the device to a Fabric Connect-enabled switch. To perform the following task, you will need the device VLAN ID and I-SID number.

For more information about Fabric Attach, see [Fabric Attach](#) on page 110.

About This Task

Use this task to configure a device connected to an existing Fabric Connect network.

Procedure

1. From within the network policy, navigate to the **Device Template** page and scroll down to the **Wired Interfaces** section.
2. Select the add icon next to the **Fabric Attach** field.
3. Enter the device's associated **VLAN ID** and select its **I-SID#** from the drop down.
4. Select **Save**.

Configure Auto-Provisioning

Before You Begin

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, the auto-provisioning rules are applied and the AP device template is ignored.

About This Task

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 profiles 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.

Procedure

1. Select the add icon.

2. Enter a name.
3. Enter an optional description.
4. Select a **Device Function**.
5. Select a **Device Model**.
The model you choose determines which device functions, interface settings, and radio settings display.
6. Select **Serial Number** to restrict automatic provisioning to particular serial numbers.
7. Choose the **Select Serial Numbers** bar.
8. Add serial numbers from the imported list, import them from a CVS file, or add them manually.
9. Choose **IP Subnetworks** to auto-provision devices by IP subnetworks.
10. Choose **Select IP Subnetworks**.

**Note**

To create an auto provisioning profile that contains IP subnetworks, the devices in the profile cannot have been previously onboarded.

11. Add IP Subnetworks from either a CVS file or manually.
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.
12. Select a **Network Policy** from the drop-down list.
13. 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.
14. 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.

15. For **Select a Location and IP Subnetwork**, select the plus sign.
16. Select a **Subnet** and **Location**.
17. Select **Save**.
18. 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.

19. 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.
20. 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.
21. 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.
22. 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.

Configure a Bonjour Gateway

About This Task

Extreme Networks devices can function as Bonjour Gateways and forward service advertisements across VLAN or subnet boundaries. 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.




Note

You must add at least one filter rule to the Bonjour Gateway profile before you can save it.

Procedure

1. Enter the gateway name for referencing in a network policy.
2. Add an optional description.

3. Enter the VLANs that you want the Bonjour Gateway to scan for service advertisements.
Use commas to separate multiple VLAN IDs (do not include a space after a comma) and dashes to indicate ranges.
4. Select the plus sign to add a Bonjour filter rule.
5. Choose the name of a previously defined **Service** from the drop-down list, or enter the name of the service in the field.
 - a. To add a new service, select the plus sign.
 - b. Enter the service name.
 - c. Enter the type.
 - d. Select **Save**.
6. Choose the VLAN group from which to share services.
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. See [Add a VLAN Group](#) on page 171 for more information.
7. Choose the VLAN group to which services are advertised.
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.
8. Enter the maximum number of management subnet hops between one Bonjour device and another for the recipient to accept service advertisements.
9. Choose the name of an existing **Realm** to apply this rule only to members of that realm.
A realm consists of one or more members within radio range of one another but in different subnets/VLANs. These devices can detect each other automatically. To apply the rule to members of all realms, choose **Any** from the drop-down list.
 **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 configurations.
10. Select **Save**.

Configure a Classification Rules Common Object

Before You Begin

Before you can use classification rules, you must create a network location, along with cloud config groups, IP addresses, and IP subnets.

About This Task

You can create classification rules as part of a network policy or as a common object. 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).

- 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.

Procedure

1. Select the add icon.
2. Enter a name for the rule.
3. Enter an optional description.
4. Select the add icon and the rule type to configure.
5. If you selected **Device Location**, perform the following steps:
 - a. Open each location level until you reach the level where the device resides.
 - b. Choose **Select**.
6. If you selected **Cloud Config Group**, perform the following steps:
 - a. Select the **Match Type**.
 - b. Select an existing group from the drop-down list.

To add a new group, select the add icon. For more information, see [Add a Cloud Config Group](#) on page 116.
 - c. Select **Save Rule**.
7. If you selected **IP address**, perform the following steps:
 - a. Select the **Match Type**.
 - b. Select an existing IP address from the drop-down list.

To add a new IP address, select the add icon.
 - c. Select **Save IP**.
8. If you selected **IP Subnet**, perform the following steps:
 - a. Select the **Match Type**.
 - b. Select an existing IP subnet from the drop-down list.

To add a new IP subnet, select the add icon.
 - c. Select **Save Subnet**.
9. If you selected **IP Range**, perform the following steps:
 - a. Select the **Match Type**.
 - b. Select an existing IP Range from the drop-down list.

To add a new IP IP range, select the add icon.
 - c. Select **Save IP**.

10. Use the up and down arrows in the **Order** column to define the order in which location, cloud config group, IP address, IP subnet, and IP range objects appear. The objects are considered using a top-down, first-match, stop-on-match method, so if a device is a member of more than one matching object for an element, only the first match is applied.
11. Select **Save Rule**.

Add a Cloud Config Group

Before You Begin

You must first configure devices to associate with cloud config groups.

About This Task

Cloud config 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.

Procedure

1. Select the add icon.
2. Enter a name for the new group.
3. Enter an optional description.
4. 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**.
5. Select **Save Cloud Config Group**.

Configure Port Types

About This Task

After you have selected 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 the following steps to assign port types:

Procedure

1. To assign an existing port type to a port, highlight the port and then select **Assign**.
2. 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.
3. Enter a name for the port type.
4. Enter a brief description for the port type.
5. Turn the port off or on.
6. Select **Save**.

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 92).

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, or ax.
- **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.

Add a Radio Profile

About This Task

Use this function to create a new 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 117.



Note

Extreme Networks provides defaults for each item in this section. The following steps are optional, except for the required radio profile **Name**.

Procedure

1. Select the add icon.
2. Enter the radio profile **Name**.
3. Enter an optional description, helpful for troubleshooting and identifying specific radio profiles.
4. Select the proper 802 specification from the **Support Radio Modes** drop-down menu.
5. Use the **Maximum Transmit Power** slider to set the optimal maximum power level.
6. Use the **Transmission Power Floor** slider to set the minimum power level.
7. Use the **Transmission Power Drop** slider to set the maximum value the radio power can drop from the current power level.
8. Use the **Maximum Number of Clients** slider to set the maximum number of wireless clients that can use the radio if the AP is permitted to change channels.

If the number of associated clients is equal to or less than this setting, and if the AP finds a better channel, it can switch to the new channel. Any associated clients will lose their connections and need to reconnect. If the number of clients exceeds this setting, the AP will not switch to the new channel. Whenever a client deauthenticates during the scheduled time range, the AP checks if the number of clients still exceeds this setting. If not, the AP switches channels. If the number of clients exceeds this setting for the entire defined channel switching period, the AP will not change channels.

9. To choose to deny access to legacy interfaces, do the following:
 - a. Select the **Deny connection requests from legacy clients using** check box.
 - b. Select one of the following radio buttons:
 - **802.11b**
 - **802.11a/b/g**



Note

The slower data rates of legacy clients can clog the network when wireless traffic is heavy.

10. Select **Save Radio Profile**.

What to Do Next

Now that you have completed the basic configuration steps, you can continue to modify advanced radio profile settings. Remember to select **Save Radio Profile** after changing any advanced settings.

For more information, see [Configure Radio Settings](#) on page 120, [Configure Neighborhood Analysis](#) on page 124, .

About 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 Topics

[Configure Radio Settings](#) on page 120

Configure Radio Settings

About This Task

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 [About Radio Settings](#) on page 119.



Note

Extreme Networks provides defaults for each item in this section. The following steps are optional.

Procedure

1. Select **Auto (Short/Long)** to enable support for short preambles or **Long** to disable short preamble support.
2. Set the period during which APs send beacons.
3. Set the Guard Interval to 800 nanoseconds by deselecting **Enable Short Guard Interval**.
4. To no longer combine data frames into larger frames before transmission, clear the check box for **Enable MAC Aggregate Protocol Data Units**.
5. 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.
6. Select **Enable Transmit Beamforming** to improve data transfer rates for directional signal transmission processing.
7. Select **Enable MU-MIMO** to enable multiple users to receive data using different simultaneous spatial streams from an AP transmit radio chain.
8. 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.
9. If you are using 802.11ax radios, enable **ODFMA**.
10. If you selected **Enable ODFMA**, select **Uplink** or **Downlink**.
11. If you are using 802.11ax radios, enable **BSS Coloring**.
12. If you selected **Enable BSS Coloring**, enter the numerical value of the new BSS color the AP will transmit after surpassing the beacon threshold.

13. 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**.

For more information, see [Optimize Radio Usage](#) on page 125, [Optimize Radio Usage](#) on page 125, [Configure Outdoor Deployment](#) on page 126, [Configure RF Interface Reports](#) on page 127, [Configure WMM QoS Settings](#) on page 127, [Configure User Profile Client SLA Settings](#) on page 154, and [Configure an SDR Profile](#) on page 128.

Related Topics

[About Radio Settings](#) on page 119

Configure Backhaul Failover

About This Task

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.

Procedure

1. Toggle **On** and 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.
2. Select **Save**.

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

WiFi 6 is the next generation of WiFi based on 802.11ax HE (high efficiency) technology. Currently, AP4000 devices support Wifi 6 on radio 2.

Related Topics

[Configure Channel Selection](#) on page 123

*Configure Channel Selection***About This Task**

Use this section to make changes to the device channel width, Dynamic Frequency Selection (DFS), and Dynamic Channel Switching (DCS). The available settings depend on the **Supported Radio Mode** you selected in the basic configuration section.

**Note**

Extreme Networks provides defaults for each item in this section. The following steps are optional.

Procedure

1. Select a channel from the **Channel** drop-down list.
2. Select a **Channel Width** from the drop-down list.
3. To manually exclude channels, select a specific channel.
4. To manually set transmission power, use the slider to select a dBm setting.
5. Enable **Dynamic Frequency Selection** (DFS) channel selection on APs as required for the regulatory region or country.

DFS is the mechanism that devices use to change to a clear channel when RADAR, such as from military installations, airports, and weather stations, is detected on the current channel.

- a. Select **Enable Manual Channel Return** when a radio is forced off a statically assigned DFS channel due to the presence of radar.

ExtremeCloud IQ now allows the radio profile to be configured to return the affected radio to the original statically assigned DFS channel.

- b. Select **Enable ZeroWait DFS** to enable a device to bypass the clear channel checks when switching to a clear channel.

The device maintains a vetted list of clear channels, and when the device detects RADAR, it switches immediately to a clear channel from the list without delay.

6. To manually enable client transmission power control (802.11h), use the slider to select a dBm setting.
7. Toggle **Limit Channel Selection** on or off 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.
8. Toggle **Dynamic Channel Switching** on to dynamically select and switch channels based on the following criteria:
 - a. Select a **To** and **From** time interval.
 - b. Select the **RF Interference** and **CRC Error** thresholds.

Related Topics

[About Channel Selection](#) on page 121

Configure Neighborhood Analysis

About This Task

Using background scanning, an AP divides a full background channel scan into several shorter partial scans so they do not interfere with the AP's own beacons. 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.

Procedure

1. Toggle **Background Scan** on or off.
Background scanning is necessary for WIPS and Layer 3 roaming to function.
2. Set the interval between background scans of all radio channels.
The range is 1 to 1440 minutes (24 hours).
3. Select **Clients are connected** to enable an AP with connected clients to scan channels.
4. Select **Connected clients are in power save mode** to enable an AP to scan channels when connected clients are in power save mode.
5. 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.

About Client SLA Settings

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 rate 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.

Optimize Radio Usage

About This Task

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**

Extreme Networks provides defaults for each item in this section. The following steps are optional.

Procedure

1. 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.
2. 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.
3. 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 [Add a MAC Object and Host Name](#) on page 168.

**Note**

The suppression setting is disabled by default when high-density WLAN optimization is enabled.

4. Turn **Safety Net** on and select how much time passes before a device will again respond to association requests after an overload incident.

Configure Sensor Mode Scan Settings

About This Task

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.

Procedure

1. If necessary, modify the **Dwell Time**.
2. Deselect **Scan All Channels** and set individual channel numbers to collect client probe request data.

Configure Outdoor Deployment

About This Task

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.

Procedure

1. Set a distance (between 300 and 10,000 meters) over which to support the radio.
2. Select **Save Radio Profile**.

Configure RF Interface Reports

About This Task

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.

Procedure

1. 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%.
2. 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%.
3. Set the short-term average for polling.
The range is 5 to 30 minutes.

Configure WMM QoS Settings

About This Task

WiFi 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.

Procedure

1. If necessary, modify the default settings in the **Contention Window Minimum**, **Contention Window Maximum**, and **AIFS** columns.
2. If necessary, modify the default setting in the **TXOP Limit** column to determine how long bursts of traffic last before relinquishing the medium.
3. 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.

Configure an SDR Profile

Before You Begin

You need to create radio profiles. For more information, see [Add a Radio Profile](#) on page 118.

About This Task

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).

Procedure

1. Select the plus sign.
2. Enter a name for profile.
3. 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.

4. Select **Enable the SDR process during the 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.
5. Select **Enable the SDR process to periodically run in the background while the AP is handling client traffic** 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.
6. 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. If the station number count is 0, the rule will not be applied.
7. Select **Save**.

About SSIDs

An SSID is an alphanumeric string that identifies a wireless or guest network. For information about adding wireless networks, see [Configure a Standard Wireless Network \(SSID\)](#) on page 53.

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.

About SSID Usage in Standard Wireless Networks

As part of configuring a standard wireless network, you need to 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 56.
- **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 57.
- **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 58.
- **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 62.

Configure Enterprise SSID Authentication

Before You Begin

Create a standard wireless network policy. For more information, see [About SSIDs](#) on page 128.

About This Task

Use these steps to configure Enterprise SSID authentication options.

Procedure

1. Select **Enterprise-802.1X**.

This requires users to authenticate themselves by entering a user name and password, which are checked against a RADIUS authentication server.

2. Select the required **Key Management** and **Encryption Method** options from their respective drop-down menus or leave them at the default values.

Key Management options:

- **WPA3-802.1X** uses 192-bit encryption, and simultaneous authentication of equals (SAE) instead of PSK exchanges. If all wireless clients support WPA3, it is a better choice than WPA2.
- **WPA2-802.1X** supports PMK caching and preauthentication (WPA does not). If the wireless clients support WPA2, it is the better choice over WPA, and is the default.
- **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.
- Choose **Auto-(WPA or WPA2) 802.1X** to negotiate the use of WPA2 or WPA with clients based on which version they support.

For **Encryption Method** Option:

CCMP (AES) (Counter Mode-Cipher Block Chaining Message Authentication Code Protocol) 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).

Configure Personal SSID Authentication

Before You Begin

Create a standard wireless network policy. For more information, see [About SSIDs](#) on page 128.

About This Task

This option requires all users to authenticate themselves by entering the same pre-shared key. Select the required **Key Management**, **Encryption Method**, and **Key Type** entries from their respective drop-down menus or leave them at their default values, and enter a required value in the **Key Value** text box.

Procedure

1. Select **Personal** SSID Authentication.
 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. WPA2 supports PMK caching and pre-authentication, whereas WPA does not.
 - Select **WPA-(WPA or Auto)-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 support WPA (not WPA2), this option allows the Extreme Networks device to support them.
 - **Auto-(WPA or WPA2)-PSK** to negotiate the use of WPA2 or WPA with clients based on the version they support.
 3. For **Encryption Method** (WPA or WPA2 only): Choose **CCMP (AES)**.
CCMP (AES) (Counter Mode-Cipher Block Chaining Message Authentication Code Protocol) is a security protocol that 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).
-
- Note**
When the SSID is configured for WPA3 (SAE), the encryption method is always set to 128-bit encryption.

Configure WEP SSID Authentication

Before You Begin

Create a standard wireless network policy. For more information, see [About SSIDs](#) on page 128.

About This Task

Extreme Networks supports both WEP 802.1X and WEP. The difference is in how they manage keys. WEP 802.1X can refresh keys dynamically, whereas WEP requires keys to be changed manually. Because of the effort required to enter keys manually on

clients, WEP is only suitable for a relatively small number of clients. Use these steps to configure WEP SSID authentication options.

**Note**

Although WEP can deter casual eavesdropping, it cannot withstand more serious attacks. More secure replacements for WEP are WPA and WPA2, and Extreme Networks encourages the use of these stronger security mechanisms whenever possible.

Procedure

1. Select **WEP** for **Key Management**.

**Note**

If you select **WEP 802.1X**, you will only need to perform **Step 2**.

2. For **Encryption Method**, choose either **WEP 104** or **WEP 40**.

The difference is the length (104-bit or 40-bit) of the encryption keys. The shared secrets are derived from values you enter in the **Key Value** fields. Generally, a longer key is more secure than a shorter one.

3. For **Authentication Method**, choose either **Open** or **Shared**.

- **Open:** The Extreme Networks device accepts any client without challenging it.
- **Shared:** The Extreme Networks device sends a random plain text string to the client. The client encrypts the string and sends it back. The device decrypts it and compares the string with the one it sent. If they match, the client has authenticated itself by proving it possesses the same shared encryption key as the device.

4. Choose either **ASCII Key** or **Hex Key**.

- If you chose **WEP 104** and **ASCII Key**, enter a 13-character ASCII string in the **Key Type** fields. If you chose **WEP 104** and **Hex Key**, enter a 26-digit hexadecimal string.
- If you chose **WEP 40** and **ASCII Key**, enter a 5-character ASCII string in the **Key Type** fields. If you chose **WEP 40** and **Hex Key**, enter a 10-digit hexadecimal string.

5. Specify the **Default Key** the device uses to encrypt the data it sends.

You can change this to **Key Values 2, 3, or 4**. Use **Show Password** to display the strings as you enter them. When the Extreme Networks device encrypts data with its **Default Key**, it includes the key ID number that WEP adds to the 802.11 frame header. The recipient can locate the key with the same ID number. Similarly, when a client encrypts data with its **Default Key**, it includes the key so that the Extreme Networks device can locate a matching key. The client can use the same default key as the Extreme Networks device to encrypt data, or it can use one of the other three keys, and still decrypt it by using the key ID number to locate the matching key.

**Note**

When entering WEP keys on wireless clients, make sure those keys are in the same order as the matching keys on the Extreme Networks device. For clients that store keys numbered 1, 2, 3, 4 or keys numbered 0, 1, 2, 3, the keys in the first, second, third, and fourth positions, regardless of their numbers, must correspond with the keys at the same positions on Extreme Networks devices. For example, the key in the first position numbered either 1 or 0 on a client must match the key in the first position (**Key Value 1**) on an Extreme Networks device.

Add an Availability Schedule for User Profiles

Before You Begin

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.

About This Task

In the **Create User Profile** window, use these steps to configure an SSID availability schedule:

Procedure

1. Toggle **Availability Schedule** to **On**.
2. Select the add icon.
3. Enter a name for the schedule.
4. Enter a description for the schedule.
5. Select **One Time** or **Recurring**.

If you select **One Time**, the schedule can only be used one time. Select **Recurring** if you want this schedule to apply to this user profile on an ongoing basis.

6. Select **Save Schedule**.

To apply the availability schedule to an SSID, you must activate it on the **Standard Wireless Network Settings** panel, in **Additional Settings**.

Configure Switch Templates

Before You Begin

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 [Switch Deployment Guide](#).

About This Task

A switch template is a visual depiction of the physical ports on a switch. Configure how ports function by assigning port types and port usage settings to the template, and then applying the template to managed switches. The following steps describe how to create a switch template inside the network policy creation workflow.

Under **Device Configuration**, you can choose to override settings made under **Common Settings** in a network policy. The Switch Template Override feature allows you to create and manage switch templates based on common settings for 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 device configuration will be inherited by the network policy common settings.

To make changes to a switch template at the device level, from **Manage > Devices**, select a device name.

Procedure

1. Select **Add** and an existing template from the drop-down list.
Select the check boxes for multiple models and then **Select** to apply the same configuration to multiple device templates.
2. Enter a name.
3. Ensure that **Enable Override Policy Common Settings** is set to **ON** to make any changes to device configuration.
4. For STP Configuration, toggle to **On** and see [Configure Switch STP Settings](#) on page 145.
5. For **IGMP Settings**, 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.

- 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.

- For **Extreme Loop Recovery Protocol Settings**, select to configure ELRP client periodic packet transmission for VLAN(s) 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.

- 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.
- For **PSE Settings**, toggle to **On** to configure maximum power thresholds to generate alerts to ExtremeCloud IQ about exceeding maximum power levels.
- Select **Enable Flow Control** to manage the port data receive transmission rate.
- 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.
- For the **Port Configuration** section, see the following:
 - To **Configure Ports in Bulk** - [Create a New Port Type](#) on page 137
 - To **Configure Ports Individually** - [Configure Individual Ports](#) on page 140
- For **sFlow Control** see [Configure an sFlow Receiver](#) on page 216.
- For **Supplemental CLI**, see [Configure Supplemental CLI](#) on page 144.
- For **Advanced Settings**, see [Configure Switch Device Template Advanced Settings](#) on page 149.
- Select **Save**.

What to Do Next

Continue configuring the network policy. To create a switch stack template, see [Manually Create a Switch Stack](#) on page 147.

Configure Switch Common Settings

About This Task

This section contains configuration elements applicable to all Switch Engine, EXOS, Fabric Engine, and VOSS switches assigned to a specific network policy.

Procedure

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 **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.
4. 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.

5. For **Extreme Loop Recovery Protocol Settings**, select to configure ELRP client periodic packet transmission for VLAN(s) 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.

6. 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.
7. For **PSE Settings**, toggle to **On** to configure maximum power thresholds to generate alerts to ExtremeCloud IQ about exceeding maximum power levels.
8. 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 137 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.

Create a New Port Type

Before You Begin

Create or modify a Switch Template.

About This Task

Use this task to create ports in bulk.

Procedure

1. Either under **Create Ports in Bulk**, select one or more ports and select **Assign > Create New** or select the plus sign next to **Port Type** under **Configure Ports Individually**.
2. If this template applies to a 5570 or 5520 switch, you can define 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 a Classification Rules Network Policy](#) on page 66 for more information about classification rules.

- d. Select one or more of these VIM ports and continue to **Step 3**.

3. Enter a name.
4. Edit the associated description if necessary.
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.
 - **Mirror port:** Ports that mirror data from one or more other ports for diagnostic purposes. Configure one of the following settings for a new mirror port type:
 - **Ingress-and-Egress mirror:** Route all traffic.
 - **Anomaly mirror:** Route all anomalous traffic.
 - **Egress mirror:** Route outbound traffic only.
 - **Ingress mirror:** Route inbound traffic only.
 - **VLAN mirror:** Route traffic from all ports belonging to that VLAN.

Use the switch-specific CLI commands set to configure the switch.

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 170.
9. Select **Next**.
10. For **User Authentication**:
 - **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:** If you selected **MAC Authentication**, choose **PAP**, **CHAP**, or **MS CHAP V2** (for users on an Active Directory server) to determine how the port forwards authentication requests from users to an external RADIUS or Active Directory server. If you choose PAP, the port sends an unencrypted password to the RADIUS server. If you choose CHAP or MS CHAP V2, the port sends the RADIUS or Active Directory authentication server the result of an operation it performs on the password, instead of the password itself. The authentication server performs the same operation, and then compares the two results to check if they 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 External RADIUS Server Settings](#) on page 214.
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 185.

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 will 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 will disable itself upon reception of a BPDU. The port will enter the error-disabled state, and will be removed from the active topology.
 - **Filter** - Controls whether a port explicitly configured as Edge will transmit 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.
 - **Thersholds:** 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 MAC's, with the option to retain MAC's. We also have the option to take action when MAC's are aged out.
 22. For **ELRP**, toggle to **ON** to enable ELRP per port.
 23. For **PSE**, select an existing profile or select the plus sign to add a new one.
See [Configure PSE Parameters](#) on page 142.
 24. Review all the port settings in the **Summary** section and select **Save** when complete.

Configure Individual Ports

Before You Begin

Create or modify a Switch Template, then select the **Port Configuration** tab.



Note

In order to modify an existing port, use the drop-down menu to set the **Port Type** to **OFF**, and select the edit icon. You can then edit all port parameters from the **Summary** page.

About This Task

Use this task to configure or modify settings for individual ports.

Procedure

1. For **Port Details**, see [Configure Port Details](#) on page 140.
2. For **Port Settings**, see [Configure Port Settings Parameters](#) on page 141.
3. For **STP**, see [Configure STP Parameters](#) on page 143.
4. For **Storm Control**, see [Configure Storm Control](#) on page 143.
5. For **PSE**, see [Configure PSE Parameters](#) on page 142.

What to Do Next

Continue configuring the Switch Template.

Configure Port Details

Before You Begin

Create or modify a switch template.

About This Task

Use this task to configure the first portion of the **Configure Ports Individually** section.

Procedure

1. Configure the columns as follows:
 - **Interface:** The interfaces available for the switch, such as Eth1/0/1-Eth1/0/52.
 - **Port Type:** The current 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.

Use the drop-down to select a different port type or to turn this port off. Select the plus sign to create a new port type. See [Create a New Port Type](#) on page 137.

 - **Enabled:** Indicates whether the port is currently activated.
 - **LACP:** Activate to apply link aggregation control protocol to a member of a link aggregation port group . See [Aggregate LAG and LACP Ports](#) on page 144.
 - **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.
2. Continue to the next port configuration section.

Configure Port Settings Parameters

Before You Begin

Create or modify a switch template and select the **Port Configuration** tab.



Note

To modify an existing port, use the drop-down menu to set the **Port Type** to **Off**, and select the edit icon. You can then edit all port parameters from the **Summary** window.

About This Task

This task is part of **Port Configuration**.

Procedure

1. Enter a 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.

Configure PSE Parameters

Before You Begin

Create or modify a switch template.

About This Task

Use this task to configure PSE settings, which define how ports manage the power that they supply to devices.

Procedure

1. Select the add icon.
2. Enter 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. Enter an optional description.
7. Select **Save**.

Configure Storm Control

Before You Begin

Create or modify a switch template, then select the **Port Configuration** tab.



Note

To modify an existing port, use the drop-down menu to set the **Port Type** to **Off**, and select the edit icon. You can then edit all port parameters from the **Summary** page.

About This Task

Use this task to configure traffic storm mitigation by tracking the source and type of frames to determine whether they are legitimately required. The switch discards frames that it determines 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.

Procedure

1. Select **Broadcast** to include traffic that is forwarded to all destinations simultaneously.
2. Select **Unknown Unicast** to include traffic with a destination address does not appear in the forwarding database.
3. Select **Multicast** to include traffic with a multicast address as a destination.
4. Select **TCP-SYN** to include TCP-SYN flood traffic.
5. For **Rate Limit Type**, select **KBps** or **Percentage** if you selected **Byte Based**, and **PPS** if you selected **Packet Based**.
6. For **Value**, enter when the switch should discard traffic of the selected types.

Configure STP Parameters

Before You Begin

Create or modify a switch template, then select the **Port Configuration** tab.



Note

To modify an existing port, use the drop-down menu to set the **Port Type** to **Off**, and select the edit icon. You can then edit all port parameters from the **Summary** page.

About This Task

By default, STP is disabled. Use this task to toggle it on and configure settings. Extreme Networks and Dell EMC recommend you enable STP for Dell EMC switches.

Procedure

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 will disable itself upon reception of a BPDU. The port will enter the error-disabled state, and will be removed from the active topology.
 - **Filter:** Controls whether a port explicitly configured as Edge will transmit and receive BPDUs.
 - **Disabled:** Turns off BPDU Protection.
4. When 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.

Aggregate LAG and LACP Ports

Before You Begin

Create or modify a Switch Template.

About This Task

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.

Procedure

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.

What to Do Next

Continue configuring the Switch Template.

Configure Supplemental CLI

Before You Begin

To use the supplemental CLI tool, first navigate to **Global Settings > VIQ Management**, and enable **Supplemental CLI**.

About This Task

Use this task to update CLI commands to multiple devices simultaneously from ExtremeCloud IQ. You can save Supplemental CLI objects containing CLI commands,

and the commands can then be updated for devices automatically each time you update the network policy.

Procedure

1. Toggle **Supplemental CLI On**.
2. Select existing supplemental CLI objects using the drop-down list next to **Re-use Supplemental CLI Settings**.
3. To add a new supplemental CLI object:
 - a. Enter a name.
 - b. Enter an optional description.
 - c. Enter the CLI commands.
 - 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.

Configure Switch STP Settings

Before You Begin

Create or modify a switch template.

About This Task

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.

Procedure

1. Toggle the switch to **On** and then 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 an **STP Bridge Priority** from the drop-down list.

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 **STP Timers** parameters:

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.

About Switch Stacks

ExtremeCloud IQ can manage switch stacks. You can instantly create a Switch Engine switch stack or create a switch stack manually.

- To instantly create Switch Engine switch stacks, see [Instantly Create a Switch Engine Stack](#) on page 146.
- To manually create a switch stack, see [Manually Create a Switch Stack](#) on page 147.

Instantly Create a Switch Engine Stack

Before You Begin

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.

About This Task

Use this task to instantly configure a Switch Engine switch stack in ExtremeCloud IQ.

Procedure

1. Navigate to **Manage > Devices**
2. Find the new stack in the **Devices List** and select its checkbox.
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**.

Results

The assigned template now displays in the **Policy** column.

Manually Create a Switch Stack

Before You Begin

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 134 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).

About This Task

After you have onboarded the switches in your stack, you must create a stack template in ExtremeCloud IQ that exactly matches the physical stack.

Procedure

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**.

What to Do Next

Push a network policy to the stack. For more information, see [Manage Switch Stacks](#) on page 147.

Manage Switch Stacks

Before You Begin

Create a switch stack template. See [About Switch Stacks](#) on page 146.

About This Task

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.

Procedure

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 [Device List Views](#) on page 248 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, you must create a new stack template that matches the number of switches in the new physical stack.
 4. Add an existing switch to a stack:
Use the previous procedure to add an existing switch to a stack. You must cable the switch to the physical stack, and then create a stack template matching the new 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 [Device List Views](#) on page 248 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 [Device List Views](#) on page 248 for more information.

What to Do Next

If necessary, create a new switch stack template to reflect any of the above changes.

Configure Switch Device Template Advanced Settings

Before You Begin

Create or edit a switch template.

About This Task

ExtremeCloud IQ can update device firmware and reboot the device during onboarding.

Procedure

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 checkbox below.
4. To use **Supplemental CLI**, select **On**.

For more information, see [Configure Supplemental CLI](#) on page 144.

What to Do Next

Complete configuring the device template.

Configure URL Filtering Rules

Before You Begin

First create the user profiles to be associated with your URL filtering rules.

About This Task

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.

Procedure

1. Select the add icon.
2. Enter a name for the rule.
3. Enter an optional description.

4. 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.

5. Select the **Whitelist** subtab.

- a. Manually enter up to 32 allowed URLs.
- b. You can also import a `.cvs` file containing up to 32 URLs by dragging the file into the field or searching for an existing `.cvs` 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
```

6. Select the **Blacklist** subtab.

- a. Manually enter up to 32 allowed URLs.

You can also import a `.cvs` file containing up to 32 URLs by dragging the file into the field or searching for an existing `.cvs` file.

7. Select the **Categories** subtab.

8. Choose the categories this rule blocks.

9. 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**.

10. Select **Save Detail**.

11. Continue adding filters if needed.

12. Select **Save URL Rule**.

13. 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 152.

What to Do Next

Add this **URL Filtering Rule** to a network policy **Router Settings**.

Add a User Profile

About This Task

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. You can define the following user traffic settings:

- **Security:** Apply IP or MAC firewall rules. For more information, see [Configure User Profile Security Settings](#) on page 152.
- **Traffic Tunneling:** Enable three types of generic routing encapsulation (GRE) traffic tunneling for a user profile: Layer 3 roaming, identity-based, or standard GRE tunneling. For more information, see [Configure User Profile Traffic Tunneling Settings](#) on page 155.
- **QoS:** Set rate limits and traffic forwarding rules for each traffic class. For more information, see [Configure User Profile QoS Settings](#) on page 156.
- **Availability Schedule:** Define user profile availability for specific dates, days, and times. For more information, see [Configure Availability Schedule Settings](#) on page 153.
- **Client SLA:** Enable devices to monitor client throughput and take action if the actual throughput is below the targeted minimum level. For more information, see [Configure User Profile Client SLA Settings](#) on page 154.
- **Date/Time Limit:** Configure access restrictions for users based on the user's assigned profile. For more information, see [Configure User Profile Access Restrictions](#) on page 154.

Procedure

1. Select the add icon.
2. Enter a name for the profile.
3. Select a VLAN or VLAN group for the profile.
To add a new VLAN or VLAN group, select the add icon. See [Configure VLAN Settings](#) on page 170 for more information.
4. Complete the required settings sections as detailed above.
5. Select **Save User Profile**.

Configure User Profile Security Settings

Before You Begin

Begin the process of creating a User Profile.

About This Task

Use this task to apply IP or MAC firewall rules.

Procedure

1. 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 the add icon.
 - b. Enter 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 Policy Rules](#) on page 172).
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 Policy Rules](#) on page 174).

Configure Availability Schedule Settings

Before You Begin

You need to create a user profile or SSID to which you apply a schedule. For User Profiles, you must first turn **Availability Schedule On**.

About This Task

You can create an availability schedule for network SSIDs to determine when they are available for access and for User Profiles to make the user profile available for specific dates, days, and times.

Procedure

1. Select the add icon.
2. Enter a name for the schedule.
3. Enter an optional description.
4. Select **One Time** to apply this schedule one time only.
5. Select the active time period for the schedule.
6. Select **Recurring** if you want this schedule to apply on an ongoing basis.
7. Choose every day or specific days of the week, and time ranges during this time period.

8. Select **Save**.

**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 56.

Configure User Profile Client SLA Settings

Before You Begin

Service-level agreements (SLAs) are contracts that specify the performance parameters within which a network service is provided.

About This Task

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.

Procedure

1. Turn on turn **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.

Configure User Profile Access Restrictions

Before You Begin

Create a user profile that requires access restrictions.

About This Task

You can configure access restrictions (date and time limits) for users based on their assigned user profiles. This is particularly helpful when you are managing non-employee guest users, such as visitors, VIPs, and contractors. Use this task to create these access restrictions.

Procedure

1. 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. Select **Save**.

Configure User Profile Traffic Tunneling Settings

Before You Begin

Create a user profile.

About This Task

You can enable three types of GRE traffic tunneling for a user profile: Layer 3 Roaming, Identity-based, or Standard GRE tunneling.

- Layer 3 Roaming allows you to adjust roaming thresholds so that a device will disassociate with a wireless client that has roamed to it from another subnet and has either been idle for a period of time, or whose traffic has dropped 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.

Procedure

1. Turn on **Traffic Tunneling (GRE)**.
2. For **Layer 3 Roaming**:
 - a. Enter a time period between 10 and 600 seconds.
 - b. Enter a threshold number between 0 and 2147483647 packets per minute.
3. For **Identity-Based Traffic Tunneling**:
 - a. For the **Tunnel Source**, select a subnet from the drop-down list, or add a new subnet.

To add a new IP address or host name, see [Add IP Objects and Host Names](#) on page 168.

- b. For **Tunnel Destination**, choose an IP address or host name from the drop-down list or add a new address or host name.
To add a new IP Address or Host Name, see [Add IP Objects and Host Names](#) on page 168.
 - c. For **Tunnel Authentication**, enter the password the AP uses to authenticate to the GRE termination point.
4. For **Standard GRE Tunneling**:
 - a. For **Tunnel Destination**, choose an IP address or host name from the drop-down list or add a new address or host name.
To add a new IP address or host name, see [Add IP Objects and Host Names](#) on page 168.
 - b. If you select **Tunnel Mode dot1q**, enter, select, edit, or add the 802.1Q native VLAN ID.
To add a VLAN ID, see [Configure VLAN Settings](#) on page 170.
 - c. If you select **Tunnel Mode Access Mode**, enter, select, edit, or add the VLAN ID.
To add a VLAN ID, see [Configure VLAN Settings](#) on page 170.
5. Select **Save**.

Configure User Profile QoS Settings

Before You Begin

Create a User Profile.

About This Task

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.

Procedure

1. Turn **Quality of Service (QoS)** on.
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. Enter 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. For **Mark outgoing traffic using**, Extreme Networks devices can apply priority and class mappings to outgoing traffic based on either of these standard QoS classification systems.
6. To add a marker map, see [Configure Marker Maps](#) on page 185.
7. Select **Save**.

Add Application Sets

About This Task

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.

Procedure

1. Select **Add**.
2. Enter a name for the new application.
3. Select **Application** or **Category**.
4. Enter a character string for the application or category name you want to add.
Search results are displayed in the **Application Name and Category table**.
5. In the **Application Name and Category table**, select applications for your application set.
These are automatically added to the **Selected Applications** box.
6. Select **Save**.

About Client Mode Profiles

You can set a radio on some APs 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 best-practice recommendation is to use a wired interface to configure client mode APs because the configuration process can be much faster than it is with a wireless backhaul.

There are four ways to configure APs for client mode:

- Using a wired connection and a device template (recommended). For instructions, see [Configure a Client Mode AP Profile using a Wired Connection and a Device Template](#) on page 158.
- Using a wireless connection and device template. For instructions, see [Configure a Client Mode AP using a Wireless Connection and a Device Template](#) on page 158.
- Using a wired connection and AP auto-provisioning. For instructions, see [Configure a Client Mode AP using a Wired Connection and Auto Provisioning](#) on page 160.
- Using a wireless connection and AP auto-provisioning. For instructions, see [Configure a Client Mode AP using a Wireless Connection and Auto Provisioning](#) on page 161.

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

Before You Begin

You must configure at least one network policy before you can create client mode profiles. For more information, see [About Client Mode Profiles](#) on page 157.

About This Task

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.

Procedure

1. In a network policy, configure a wireless network (SSID).
2. Add an Open, or PSK SSID without a captive web portal.
3. Configure a client mode AP device template.
4. Select **Add** and an AP model to use as the client mode AP.
5. In the template panel, name the template.
6. Configure the WAN-side backhaul (WiFi0 or WiFi1) radio for **Backhaul Mesh Link**.
7. Select **Client Mode Profile** for the LAN-side client mode radio (WiFi0 or WiFi1).
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 162.
8. Select the LAN-side client mode radio icon for WiFi0 or WiFi1.
9. From the drop-down list, select an existing client mode profile.
10. Select **Save**.

Configure a Client Mode AP using a Wireless Connection and a Device Template

About This Task

Use the following steps to configure a client mode AP using a wireless connection and a device template. For more information, see [About Client Mode Profiles](#) on page 157.

Procedure

1. Select **Wireless Auto-Provisioning Global Setting**.

Configure this setting to enable auto-provisioning of the client mode AP over a wireless mesh connection, regardless of the AP model that is configured for client mode. Navigate to *admin_name* > Global Settings > Administration > VHM Management. In the VHM Management window, enable **AP Out-of-the-Box Wireless Onboarding**.

2. Configure a network policy (see [Add a Network Policy](#) on page 51).

3. Configure a wireless network (SSID).

Add an Open or PSK wireless network (SSID) without a captive web portal (CWP) to your network policy.

Use the **Add > Quick Add Devices** option to add the client mode AP serial numbers.

4. Configure a **Portal AP Device Template**.

You must configure at least one portal AP (an AP that uses a wired backhaul) to enable auto-provisioning of the client mode AP over a wireless mesh connection, regardless of which AP model is used in client mode.



Note

A portal AP must have a wired backhaul or it cannot be configured as a portal. One or more APs must be configured as portal APs to support mesh operation.

When you are configuring the portal AP, consider using a static-channel link for the mesh AP backhaul link, which, although not required, can improve connectivity.



Note

Some APs can have the WiFi 0 radio configured to use the 5 GHz band. For the mesh backhaul link, make sure to use the same band, not the same radio, on the portal APs and the mesh client mode APs.

5. Select the **Device Templates** tab.

6. Select **Add**.

7. Select an AP model to use as a portal AP.

8. Enter a name for the template.

9. Select the radio to be used for the client mode AP mesh backhaul.

Select the WiFi1 icon if the 5 GHz radio will be used for backhaul. Select the WiFi0 icon if the 2.4 GHz radio will be used for backhaul.

10. Select **Assign**.

11. Select **Radio Usage > Backhaul Mesh Link**.

12. Select **Save**.

13. Configure a device template for the client mode AP.

For some APs, you can configure the WiFi0 radio to use the 5 GHz band. For the mesh backhaul link, make sure to use the same band, not the same radio, on portal APs and mesh client mode APs.

14. Select Add and an AP model to use as a client mode AP.

15. Enter a name for the template.
16. Select the WIFI1 icon if the 5 GHz radio will be used for backhaul.
17. Select the WIFI0 icon if the 2.4 GHz radio will be used for backhaul.
18. Select **Assign**.
19. Select **Radio Usage > Backhaul Mesh Link**.
20. Select **Save**.
21. On the **Additional Settings** tab, configure other necessary settings such as DNS Server and Device Time Zone.
22. Select **Save**.
23. Select **Next** to deploy the policy.
24. Use the **Add > Advanced Onboarding** option to add the portal and client mode AP serial numbers.
Make sure you also assign the location and the network policy created earlier.
25. Select **Finish**.

Configure a Client Mode AP using a Wired Connection and Auto Provisioning

Before You Begin

When you are creating a network policy to be used with auto-provisioning, select **Express Policy Setup** and create a wireless network policy with an Open or PSK wireless network (SSID), without a captive web portal. Client mode APs only work with Open and PSK SSIDs. For more information, see [About Client Mode Profiles](#) on page 157.

About This Task

Procedure

1. Select **Express Policy Setup**.
2. Select either **Open** or **PSK**.
Client-mode APs only work with open and PSK SSIDs.
3. Onboard serial numbers for the client mode APs.
To use auto-provisioning to configure your portal APs, continue with this procedure. If you are going to use device templates to configure your portal APs, complete the required settings and then complete this procedure.

Use the **Add > Quick Add Devices** option to add the client mode AP serial numbers.
4. Create auto-provisioning rules for client mode APs (see [Configure Auto-Provisioning](#) on page 111).
5. Plug the AP into a power outlet.

6. Plug the AP into the network using a twisted-pair Ethernet cable.

When you power on a client mode AP, it searches for a portal AP, connects through the backhaul as a mesh AP, discovers ExtremeCloud IQ, downloads its predefined configuration, and automatically extends wireless coverage to its surrounding area.

The AP automatically establishes a mesh connection and obtains an IP address. The discovery and provisioning process normally takes 3 to 10 minutes.

The status light changes to white when a CAPWAP protocol connection is established with ExtremeCloud IQ.

The AP automatically downloads its configuration file and begins broadcasting its assigned SSID.

Configure a Client Mode AP using a Wireless Connection and Auto Provisioning

About This Task

Use the following procedures to use auto-provisioning to configure client mode APs over a wireless connection. For more information, see [About Client Mode Profiles](#) on page 157.

Procedure

1. Enable **Wireless Auto-Provisioning**.

You must enable wireless auto provisioning of the client mode AP over a wireless mesh connection, regardless of which AP model you are configuring for client mode.

Navigate to **admin_name > Global Settings > Administration > VHM Management**.

Enable **AP Out-of-the-Box Wireless Onboarding**.

2. Select **Express Policy Setup**.
3. Create a wireless network policy.

Create a wireless network policy with an Open or PSK wireless network (SSID), without a captive web portal. Client mode APs only work with Open and PSK SSIDs.

4. Configure the Portal AP.

You must configure at least one portal AP (an AP that uses a wired backhaul) to enable auto-provisioning of the client mode AP over a wireless mesh connection, regardless of this which AP model you auto-provision for client mode.



Note

Each AP must have a wired backhaul or it cannot be configured as a portal AP. One or more APs must be configured as portal APs to support mesh operation.

When you configure the portal AP, consider using a static-channel link for the mesh AP backhaul link, which, although not required, can improve connectivity.



Note

For some APs, you can configure can have the WIFI 0 to use the 5 GHz band. For the mesh backhaul link, make sure to use the same band, not the same radio, on the portal APs and the mesh client mode APs.

5. Assign a network policy to the AP.
For the portal AP backhaul wireless mesh link radio, select the **Radio Usage Backhaul Mesh Link** mode.
To select a static channel for the backhaul mesh link radio (optional), enable **Exclude Channels** and select the required static channel.
6. Select **Save**.
7. To update your device directly from this window, select **Update Now**.
8. Onboard client mode AP serial numbers.
If you are going to use auto-provisioning to configure your portal APs, continue with this procedure. If you are going to use device templates to configure your portal APs, complete the required device template settings and then complete this procedure. Use **Add > Quick Add Devices** to add the client mode AP serial numbers, which then appear in the devices list.
9. Create an auto-provisioning rule for client mode APs.
10. Enter a name for the rule.
11. Select the device model of the client mode APs.
12. Enable serial numbers.
13. Choose **Select Serial Numbers**.
14. In the **Identify Devices for Provisioning** dialog box, move the client mode AP serial numbers into the **Selected** column of the table.
15. Select **Save**.
16. In **New Auto-Provisioning Rule**, select the network policy.
17. Select the country code.
18. Select **WiFi0 for a 2.4 GHz mesh backhaul**.
19. Select **WiFi1 for a 5 GHz mesh backhaul**.
Make sure to use the same client mode AP band, not the same radio, as you configured on the portal AP or APs.
20. For the backhaul radio, in the WiFi0 or WiFi1 tab, clear the **Client Access** check box and select the **Backhaul Mesh Link** check box.
Do not make a wired connection of any type when wirelessly provisioning a client mode AP, as wired connections take precedence over wireless connections.
21. Select **Save**.

NEW! Configure a Client Mode Profile

Before You Begin

Navigate to either of the following UIs:

- **Configure > Common Objects > Policy > AP Template > Client Mode > Client Mode Profile**
- **Configure > Common Objects > Basic > Client Mode Profiles**

About This Task

Use this procedure to configure a Client Mode Profile.

Procedure

1. Enter a **Client Mode Profile Name**.
2. Enter a **Description** (optional).
3. 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 WiFi network. Clear this check box to configure other options for this profile.
4. Choose one of the following three 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.
5. Set the **Enable Port Forwarding** slider button to **On**, 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.
6. When you are finished configuring the Client Mode Profile settings, select **Save**.

Related Topics

[Configure DHCP Servers and DHCP Relay Agents](#) on page 164

[Configure Wireless Interfaces for an AP Template](#) on page 104

[Configure a Client Mode AP Profile using a Wired Connection and a Device Template](#) on page 158

[Configure a Client Mode AP using a Wireless Connection and a Device Template](#) on page 158

[Configure a Client Mode AP using a Wired Connection and Auto Provisioning](#) on page 160

[Configure a Client Mode AP using a Wireless Connection and Auto Provisioning](#) on page 161

Configure DHCP Servers and DHCP Relay Agents

About This Task

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 is applied. Hover over the number in this column to see a list.

Use the following procedure to add a new DHCP Server and Relay object.

Procedure

1. Select the plus sign.
2. Enter a name for this object.
3. Enter a description for this object.

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

4. Select the management interface on which the DHCP Server or Relay agent is set.
5. Select the type of service.

6. 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
7. If you select **DHCP relay agent**, designate a Primary DHP Server and a Secondary DHCP Server (optional).
 8. Select **Save**.
 9. To update the device immediately, select **Update Now**.
 10. In the **Device Update** dialog box, select the type of update, and then select **Save as Defaults**.
 11. Select **Perform Update**.

Add a DNS Service

Before You Begin

Add or modify a subnetwork space. See [Add a Subnetwork Space](#) on page 217. It will also be helpful to have configured your DNS Servers. See [Configure a DNS Server](#) on page 187.

About This Task

Extreme Networks routers use DNS services in their subnetwork configurations (see [Configure Subnetwork Space Advanced Settings](#) on page 219). 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 a DNS service for use at the network policy level, or at the device level for routers and VPN Gateway Virtual Appliances.

Procedure

1. Enter a name.
2. Enter an optional description.
3. Select **Enable DNS Snooping for static DNS clients** to enable access data collection.
4. 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.
5. If you select, **Set the router as the DNS server in DHCP offers**, options display:
 - **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.
6. Select **Save**.

What to Do Next

Return to [Configure Subnetwork Space Advanced Settings](#) on page 219.

Add IP Objects and Host Names

About This Task

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 External RADIUS Server Settings](#) on page 214. Use this task to add a new IP object and Host name.

Procedure

1. Select the plus sign.
2. Enter a name for the new object.
3. Select the object type from the drop-down menu.
4. Fill in the required information.
5. Select **Save**.

Add a MAC Object and Host Name

About This Task

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 Policy Rules](#) on page 174. In QoS traffic classification and marking policies, you can prioritize traffic based on its OUI.

Procedure

1. Select the plus sign.
2. Select **MAC Address**.
3. Enter the new name.
4. Enter the new address.
5. Select **Save**.
6. Select the plus sign.
7. Select MAC **OUI**.
8. Enter the new name.
9. Enter the new OUI.
10. Select **Save**.

Add a Notification Template

About This Task

There are two default notification templates available in ExtremeCloud IQ; an SMS template and an Email template. You can also configure customized notification templates with this task for non-employees who need to obtain network access (for example, guests, contractors, and VIPs).

Procedure

1. Select the plus sign.
2. Enter the new name.
3. Select the template type from the drop-down list.
4. For **SMS**, enter the following information:
 - **Security Type:** Select **PPSK** (private pre-shared key) or **RADIUS**.
 - **Template Content:** Enter the text that you want the SMS message to contain. Insert any of the variables (**Login Name**, **Password**, **SSID**, or **Expiration**) by selecting a variable button below the text box and filling in that information.
5. For **Email**, enter the following information:
 - **Security Type:** Select **PPSK** or **RADIUS**.
 - **Icon URL:** Enter the URL path.
 - **Logo URL:** Enter the path to upload a logo image.
 - **Description Text:** Enter the text that you want to appear in the email message. You can insert an **SSID** variable and a **Link** variable using the variable buttons. To see how your message will display, select **Preview**.
6. Select **Save**.

Configure OS Objects

About This Task

You can add, modify, and delete OS objects. Extreme Networks devices can reassign users to different user profiles based on several characteristics of their clients. The operating system of a client is one way to categorize a device (the other two are MAC address or 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 these steps to configure a new DHCP or HTTP OS object:

Procedure

1. Select the add icon.
2. Enter a name for the object.
3. Enter a description for the object.

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

4. Select either **DHCP Option** or **HTTP Agent**.
5. For either choice, select the add icon above the table.
6. Select an OS type from the drop-down menu.
If you do not see the OS you need, you can enter a new one in the field. For **DHCP Option**, if you select a default OS types, the Parameter Request List field is automatically filled in with the default DHCP option 55 string. If you add a new OS type, you can then enter 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.
If you selected **HTTP Agent**, enter a description.

**Note**

Because devices use HTTP snooping to learn clients' operating systems, the OS version string that you enter 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.

7. Select **Add**.

Configure VLAN Settings

Before You Begin

Create a user profile that will use these VLAN settings.

About This Task

Although you can manage VLANs from Common Objects, it is recommended that you configure them inside a network policy workflow.

Use these steps to configure VLAN settings:

Procedure

1. Select the add icon.
2. Enter the name of the new VLAN or VLAN group.
3. Enter the default VLAN for this VLAN profile.
Typically, the default VLAN is 1. If you are assigning a VLAN group to this profile, select an existing group from the drop-down list, or select the plus sign to create a new VLAN group. For more information about adding a new VLAN Group, see [Add a VLAN Group](#) on page 171.
4. Select the **Apply VLAN to devices for classification** check box to create VLANs that you can apply to specific devices based on their location.
5. Select the plus sign.
6. Enter the new VLAN ID.
7. Select **Add** to add the it to the VLAN table.
8. Under **Classification Rules** in the VLAN table, select an existing classification rule, or select the add icon to add a new rule.
See [Configure a Classification Rules Network Policy](#) on page 66 for more information.

9. Select **Link**.
10. Enter a name for the classification rule.
For easier tracking, you might want to add the locations and device models using this VLAN classification rule (for example, VLAN-AP230-Sunnyvale).
11. Enter an optional description.
12. Select the plus sign to choose the device location.
13. Assign your VLAN profile based on the location of managed devices.

**Note**

When selecting a location, drill down to the level where the devices are located. For example, if the devices are located on the floor of a building, select that specific floor.

14. Choose **Select**.
15. Select **Save VLAN**.

What to Do Next

Complete the user profile configuration.

Add a VLAN Group

Before You Begin

Create the VLANs that you will assign to this group and the user profile to be associated with this group.

About This Task

VLAN groups combine multiple VLANs as a single common object. Use the following steps to create a VLAN group, and then bind the group to a user profile.

Procedure

1. Select the add icon.
2. Enter a name for the VLAN group.
3. Enter an individual VLAN or a range of VLANs.
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**.

What to Do Next

Bind this group to a user profile.

Configure Supplemental CLI

Before You Begin

To use the supplemental CLI tool, first navigate to **Global Settings > VIQ Management**, and enable **Supplemental CLI**.

About This Task

Use this task to update CLI commands to multiple devices simultaneously from ExtremeCloud IQ. You can save Supplemental CLI objects containing CLI commands, and the commands can then be updated for devices automatically each time you update the network policy.

Procedure

1. Toggle **Supplemental CLI On**.
2. Select existing supplemental CLI objects using the drop-down list next to **Re-use Supplemental CLI Settings**.
3. To add a new supplemental CLI object:
 - a. Enter a name.
 - b. Enter an optional description.
 - c. Enter the CLI commands.
 - 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.

Add IP Firewall Policy Rules

About This Task

Use this task to create IP firewall policy rules that determine how the device manages traffic based on network or application services, and source and destination IP addresses.

Procedure

1. Select the add icon.
2. 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 [Add a Network Service Object](#) on page 173.

- a. Choose either **Network Services** or **Application Services**.
You cannot select both.
 - b. Select up to 100 items.
 - c. Select **Add Service**.
3. 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.
 4. 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.
 5. 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.
 6. 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.
 7. Select **Save**.

What to Do Next

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.

Add a Network Service Object

About This Task

Network service objects identify Layer 4 traffic by protocol and port number. Use this task to create custom network services to use when defining firewall policies.

Procedure

1. Select the add icon.
2. Enter a name for the new object.
3. Enter an optional description.
4. Set how long the device waits before it terminates an inactive session.
5. Choose the protocol that you want the service to use:
 - **TCP** (Transmission Control Protocol) – 6
 - **UDP** (User Datagram Protocol) – 17
 - **SVP** (SpectraLink Voice Priority) – 119
 - **Custom** – For this custom option, the Protocol Number field replaces the Port Number field. Enter the protocol ID number (1 to 255).



Note

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. For services that use TCP or UDP, set the destination port number used by the receiving device to map the service to a specific processor.
7. If this service needs to make use of an application layer gateway (ALG), select **DNS**, **FTP**, **HTTP**, **SIP**, or **TFTP**, from the drop-down list, otherwise, leave this empty.
8. Select **Save Network Service**.

Add MAC Firewall Policy Rules

Before You Begin

About This Task

MAC firewall policy rules 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.

Procedure

1. Select the add icon.
2. 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**.

3. 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**.
4. 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.
5. 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.
6. Select **Save**.

What to Do Next

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.

Traffic Filters

About This Task

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 add, clone or modify, and delete traffic filters using the icons above the table. From either the network policy workflow, or **Common Objects > Security > Traffic Filters**, complete the following steps to configure a traffic filter.

Procedure

1. Select the add icon above the table.
2. Enter a name for the filter.
3. Enter a description.

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

4. Select or clear check boxes to permit or deny specific types of management and diagnostic access to the mgt0 interface and permit traffic between connected clients.

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 (for APs only): Permit inter-station traffic between APs.

5. Select **Save**.

Configure MGT IP Filters

About This Task

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.

Procedure

1. Select **ON** from the **Network Policy Settings** page.
2. To use an existing filter, select the **Re-use MGT IP Filter** icon.
3. To create a new filter, enter the name that you want to use to identify this filter when you apply it to a network policy.
4. Enter an optional description.
5. In the **Permitted Management Traffic From** section, select an IP address in the **Available IP Address** column from which you want to permit administrators to access the devices, and then select the single arrow (>) to move it to the **Selected IP Address** column.
6. Select **Add Another IP Object** to repeat the process.
7. Select **Save MGT IP Filter**.

Add a WIPS Policy

About This Task

The Extreme Networks Wireless Intrusion Prevention System (WIPS) uses a variety of techniques for detecting unauthorized APs by checking for those that do not conform to specified criteria and ad hoc networks.



Note

You can configure either AP-based WIPS services or advanced Extreme AirDefense WIPS services. The second option requires that you first install an AirDefense on-premise service.

Procedure

1. Select the add icon
2. Enter a name for the new policy.
3. Enter an optional description.
4. If you accept the default **AirDefense Essentials** setting, select **Save**.
5. If you enable **Rogue Access Point Detection** to detect unauthorized access points in the area, for more information, see: [Configure Rogue AP Detection](#) on page 177.

Configure Rogue AP Detection

Before You Begin

Create a new WIPS policy and select **Enable Rogue Access Point Detection**.

About This Task

This legacy WIPS configuration enables you to detect unauthorized access points in the area.

Procedure

1. 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 assumes that both MAC addresses belong to the same device. Because one of its addresses is in the MAC learning table, the rogue is considered to be in the same backhaul network as the detecting AP, and **In Net** displays in the **In Network** column for that rogue in the list of rogue APs. You can then take appropriate steps to mitigate the rogue.
2. Select **Detect rogue access points based on their MAC OUI** to detect rogue access points by MAC OUI.
 - a. Choose **Select MAC OUIs of wireless devices that are permitted in the WLAN** to create a list of MAC OUIs with network access enabled.

- b. Select an OUI from the drop-down list.
Select the add icon to add a new OUI if you don't want to use the ones in the drop-down list.
- c. Select **Add**.
3. Select **Detect rogue access points based on hosted SSIDs and encryption type** to detect rogue access points for SSID names that other access points advertise, along with the type of encryption they use.
For example, if you have a network security policy that requires all SSIDs to use Enterprise 802.1x, then any valid SSID using Enterprise 802.1x makes the access point hosting it valid. On the other hand, an access point is categorized as a rogue if it hosts an SSID using WEP or no encryption at all.
4. Select **Detect rogue access points based on hosted SSIDs and encryption type** to include SSID checks in the WIPS policy.
5. Select the add icon.
6. Select **Add**.
7. Select an SSID from the drop-down list.
8. If the SSID does not appear in the drop-down list, you can enter the name in the field.
9. Select **Check the type of encryption used by this SSID** and choose one of the following to restrict access to this WLAN based on the encryption that the client device uses within the chosen SSID:
 - **Open:** Enable only devices in the chosen SSID using no encryption to access the WLAN.
 - **WEP:** Enable only devices in the chosen SSID using WEP encryption to access the WLAN.
 - **Enterprise 802.1x:** Enable only devices in the chosen SSID using a valid WPA encryption to access the WLAN.

**Note**

You can add up to 1024 SSIDs to a WIPS policy. If you enable SSID detection but do not add any SSIDs to the list, the AP will consider all SSIDs to be rogue because no SSID is indicated as being valid.

10. **Detect clients in an ad hoc network** (default).

**Note**

When stations in an ad hoc network, or IBSS (independent basic service set), transmit 802.11 beacons and probe responses, the ESS (extended service set) bit is set to 0 and the IBSS bit is set to 1, indicating IBSS capability. When APs detect these types of management frames, they categorize those stations transmitting them as members of an ad hoc network and as rogue.

11. Select **Enable rogue client reporting** to report rogue clients.

**Note**

You can change the duration that elapses before disconnected rogue clients are deleted from the reports.

12. Configure the following information to control how you want to mitigate rogue APs and their clients:

- **Mitigation Mode 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.

- **Mitigation Mode 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.

- **Automatically mitigate rogue APs if they are connected to your wired (backhaul) network:** This ensures that APs only mitigate rogue APs that are in their backhaul network, not APs in external networks that happen to be within radio range.
- **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 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).
- **Repeat mitigation for detected rogue clients:** Specifies how many consecutive periods to spend attacking a rogue AP and its clients before allowing client inactivity to cause a ceasefire 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 will last for 60 seconds before entering

a cease-fire period due to client inactivity. The range is from 0 to 2,592,000 seconds (30 days). A value of 0 means that mitigator APs send deauthentication frames for the entire amount of time that a mitigation effort is in effect (as defined in the next setting).

- **Limit mitigation efforts per rogue AP to:** The maximum amount 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 will stop it when 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 process will continue indefinitely unless the client inactivity period elapses.
- **Stop mitigation if no client activity is detected in:** Set a 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 to automatic mode only.) 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 mitigator APs. Set the number of mitigator 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.

13. Select **Save**.

About QoS

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.

About Classifier Maps

Quality of Service (QoS) prioritizes and optimizes the forwarding of different types of traffic through a network. You can use classifier maps to map traffic to Extreme Networks QoS classes by service type, specific MAC OUIs, individual SSIDs, and priority numbers in various standard QoS classification system (802.1p/DiffServ/802.11e). The device prioritizes, processes, and forwards the incoming traffic as determined by the QoS level to which it is mapped. For outgoing traffic, devices use marker maps.

For more information about QoS in general, see [About QoS](#) on page 180

When a device applies a classifier map, it checks to see if an incoming packet matches a setting in the map by checking for matches in the following order. It then uses the first match it finds.

1. Services
2. MAC OUIs
3. SSIDs
4. 802.1p/DiffServ/802.11e

To map a traffic category to a QoS class, select the specified map and then define the traffic settings as described in [Configure Classifier Map Services](#) on page 183.

Configure Classifier Map Services

About This Task

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.

Procedure

1. 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.

2. Select one or more services (up to a maximum of 100) that you want to map to a class.
3. Select **Save**.
4. Choose **Select...** and filter services by typing part or all of a service name in the Filter field.

As an alternative, you can select services individually.

5. Select **Save**.
6. Select a QoS class to which you want to map the selected services or applications.
7. 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.

8. 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.

9. Select the add icon to configure additional QoS class definitions.

To **modify** any classifier map, select the name of the map and modify everything except the map name, then select **Save**. To **remove** one or more classifier maps, select the check box for the map or maps you want to remove and then select the trash icon.

**Note**

You cannot remove a classifier map if one or more network policies currently reference it. You must first edit the network policies so that they no longer reference the map you want to remove.

Configure Classifier Maps Based on MAC OUIs

About This Task

Devices can map traffic to classes based on either the source or destination MAC OUI in a packet. To configure this, follow these steps:

Procedure

1. 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.

2. For the 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.

3. 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.

4. To add additional MAC-OUI-to-Extreme Networks QoS class definitions, select the add icon.

Configure Classifier Maps Based on SSIDs

About This Task

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:

Procedure

1. Select the name of an SSID.
2. Choose a QoS class to which you want to map traffic using this SSID.
3. Select the add icon to configure additional SSID-to-QoS class definitions.

Configure Classifier Maps Based on 802.1p/DiffServ/802.11e

About This Task

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.

Procedure

1. Select **802.1p/DiffServ/802.11e**.
2. Select a classification system.
You can use the default mappings or modify them if necessary.
3. Select **Save**.
4. Select **Next**.
5. Select **Upload** to deploy your network policy.

Configure Marker Maps

About This Task

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 the following procedures to configure marker maps for outgoing traffic. When you configure marker maps at the network policy level, you can reuse existing maps. Select the list, and in the dialog box, select the check box of a map and choose Select. All fields are automatically populated with the information for the selected map.



Note

Deleting a marker map from the Location Server dialog box also deletes it from the Common Objects list. You can only delete a marker map if no other configuration object is using it. To see a list of configuration objects that reference a marker map, hover over the number in the Used By column for that map in the Marker Maps window in the Common Objects section.

Procedure

1. Toggle **Marker Maps** to **On** or **Off** to enable or disable this feature.
2. Enter a name for the marker map.
3. Enter an optional description about this map.

The QoS marking tables show 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), and the DiffServ codepoint marking system (marked in the L3 packet header) on outgoing packets. 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.

Configure Rate Limiting and Queuing

About This Task

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.

Procedure

1. Select the add icon.
2. Enter a name for the rate limiting profile.

Use the **Rate Limit per User Profile** slider to set rate limits and the traffic forwarding mechanisms for each class of traffic originating from members of this user profile. This is the maximum amount of bandwidth in that all users belonging to this profile can use.



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.

3. The **Class Number/Name** is a read-only list of the eight classes.
4. Select from one of two types of scheduling methods, **Strict** or **WRR (weighted round robin)**.

Strict forces devices to immediately forward traffic with strict scheduling. This type of traffic is not queued.

Devices forward **WRR** traffic based on class and weight of the traffic. Traffic with a higher class and greater weight is forwarded more quickly.

5. 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

6. 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.

7. 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/x.
- 4 - Controlled: 54,000 Kbps for 802.11a/b/g, 1,000,000 for 802.11n, 2,000,000 for 802.11ac/x.
- 3 - Excellent Effort: 54,000 Kbps for 802.11a/b/g, 1,000,000 for 802.11n, 2,000,000 for 802.11ac/x.
- 2 - Best Effort 1: 54,000 Kbps for 802.11a/b/g, 1,000,000 for 802.11n, 2,000,000 for 802.11ac/x.
- 1 - Best Effort 2: 54,000 Kbps for 802.11a/b/g, 1,000,000 for 802.11n, 2,000,000 for 802.11ac/x.
- 0 - Background: 54,000 Kbps for 802.11a/b/g, 1,000,000 for 802.11n, 2,000,000 for 802.11ac/x.

Configure a DNS Server

Before You Begin

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.

About This Task

Perform the following steps to configure a DNS server.

Procedure

1. Select the add icon to add a new DNS server.
2. Enter a name for the server.
3. From the drop-down list, choose the IP address of the device that is being configured as a DNS server.
If you do not see the IP address or host name that you need, you can add it using the add icon.
4. Enter an optional description.
You can add up to three servers. The first entry becomes the primary server. The secondary entry becomes the secondary server, and so forth. Change their order using the Order arrows.
5. Select the plus icon again to enter another IP address.
6. Select **Add**.
7. Select **Save**.
8. Select **Next**.
9. To deploy your network policy, select **Upload**.

Configure an NTP Server

About This Task

Extreme Networks devices typically obtain the time and date for their internal clocks from an NTP server. Create NTP server profiles in the Common Objects area first, before creating Network Policies and the VGVA's that will reference them.

Procedure

1. Select the add icon.
2. Enter a new NTP Server name.
3. Enter an optional description.
4. For **HiveOS Device Sync Interval**, set a polling interval for devices to use for internal clock synchronization.
5. For **New & Dell Switch Sync Interval**, choose a polling interval to apply to Dell switches.
6. To add an NTP server, select the plus sign.
7. Select an existing NTP server host name or IP address with the **Select** icon or use the plus sign to create a new host name or IP address.
8. Select **Add**.
9. Repeat the procedure to add more NTP servers to the profile
The second entry becomes the secondary NTP server, and so forth. Because NTP servers are accessed in order from the top according to their position in the profile, you can use the up and down arrows to rearrange them if necessary.
10. Select **Save**.

Configure an SNMP Server

About This Task

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.

Complete the following steps to configure an SNMP server profile.

Procedure

1. Select the add icon.
2. Enter a name for the server.
3. Enter a brief description for the server.
4. Enter the contact information of the SNMP server admin so they can be contacted if necessary.

This can be an email address, telephone number, physical location, or a combination.

5. 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 their CAPWAP connection, or leave the box checked to disable this action.
6. To add the SNMP server to the table, select the add icon.
7. 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 be able to 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.

8. Select the version of SNMP that is running on the management station you intend to use from the drop-down list.

9. From the **Operation** drop-down list, 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.

10. 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.

11. Select **Save**.

Repeat this procedure to add up to three SNMP servers to the profile.

Configure a Syslog Server

About This Task

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, all syslog clients should use the same NTP time server. See [Configure an NTP Server](#) on page 188.

Procedure

1. Enter a name for the server.
2. Enter an optional description.

3. For **IQ Engine Syslog Facility**, select a 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, and so on, 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.
4. For **Non-IQ Syslog Facility**, select a syslog facility to categorize messages sent to syslog from non-IQ Engine devices.
5. Select the expand arrow to expand the **Syslog Group**.
Syslog groups organize messages by category and limit the number of messages sent based on severity level.
6. Assign a minimum severity level to each group from the drop-down lists.
Messages below the assigned level will not be sent from the AP to the syslog server.
7. If you must make PCI DSS compliance reports, leave that check box selected or clear the check box if the servers are on an external network outside the firewall.
8. Select the plus sign to add a syslog server.
9. Select an existing syslog IP Address or host name, or use the plus sign to create a new IP Address or host name.
10. From the drop-down list, choose the minimum severity level of messages that devices will send to the syslog server.
Devices send syslog messages for the severity level you choose, plus messages for all of the more severe levels above it.
11. To add another syslog server, select the plus sign, and repeat the previous steps.
12. Select **Save**.

**Note**

Use the up or down arrows to reorder the list of syslog servers in the table.

Configure an Access Console

About This Task

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 will not take affect on other devices.

Procedure

1. Enter the Access Console's name.
2. Enter an optional description.
3. Set the console's **Mode**.

Indicates whether the access console is set to be enabled automatically (**Auto**), manually enabled (**Enable**), or manually disabled (**Disable**).

4. Select one of the following **Access Security** options:

WPA-(WPA or Auto)-PSK: Choose to use WPA for key management on devices introduced before CloudIQ 6.1r5; and for Extreme Networks devices introduced in CloudIQ 6.1r5 or later, to negotiate the use of WPA2 or WPA with their associated clients.

WPA2 -(WPA2 Personal)-PSK: Choose to force clients to use the WPA2 key management scheme. WPA supports PMK caching and preauthentication where WPA does not.

Auto-(WPA or WPA2)-PSK: Choose to 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**.

5. Select an **Encryption Method** based on your chosen Access Security option.
6. When using one of the preshared key options, enter the **ASCII Key**.
7. Set the maximum number of wireless clients that can concurrently connect to the access console.
8. 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.
9. Select **Enable Telnet Access** to enable Telnet connectivity to the device through the access console.
10. To add a MAC Filter, select the plus sign.
11. 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.
12. Select the plus sign.
13. Either select an existing MAC Filter or select the plus sign to create a new **MAC Address** or **OUI**.
14. If you create a new address or OUI, enter the information and select **Save**.
15. 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.
16. Select **Add**.
17. Select **SAVE**.

Configure ALG Services

About This Task

You can configure ALG services from inside the network policy or as common objects.

Complete the following steps to configure ALG services.

Procedure

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 a Router Firewall Policy

Before You Begin

If you intend to use a User Profile as a source, create one first. See [Add a User Profile](#) on page 152.

About This Task

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.

Procedure

1. Enter a name.
2. Enter an optional description.
3. Select the plus sign to begin adding rules.
4. 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.

5. 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.
6. Select **Any** or an existing **Network Service** from the drop-down list, or create a new network service.
7. Choose **Permit** to pass traffic through the firewall or **Deny** to block it.
8. Turn logging **ON** or **OFF** for instances when the rule is enforced.
9. 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.

10. Select **SAVE FIREWALL**.

Configure an IP Tracking Group

About This Task

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 track group can be used to disable specific SSIDs when an IP is unavailable. Use this task to enable or disable IP tracking groups and view a list of available and selected groups for a network policy.

Procedure

1. Select the add icon.
2. Enter a name for the group.
3. Enter a description for the group.
4. Select either **Backhaul Connectivity Tracking for APs** or **WAN Interface Connectivity Tracking for APs**.
5. Select the check box to activate this IP tracking group, or clear it to disable the group.
6. Enter up to four IP addresses, separated by commas for tracked devices.
If you are tracking the default gateway, enter up to three IP addresses.
7. Leave the **Default Gateway** check box selected if the IP addresses use the default gateway.
8. Select either **All targets become unresponsive** or **A single target becomes unresponsive** as the directive for when to take action.

9. Enter the tracking interval for this group.
10. Enter the number of retries before reacting to an IP address failure.
11. Select one or more of the actions to take when a target becomes unresponsive.
12. Select **Save**.

Configure Layer 2 VPN Services

About This Task

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. To configure a Layer 3 IPsec VPN service, see [Configure Layer 3 VPN Services](#) on page 82.

Procedure

1. Select the add icon.
2. Enter a name for the service.
3. Enter an optional description.
4. Select either **Single Device VPN Server** or **Redundant Device VPN Server**.
If you selected **Single Device VPN Server**, continue with the next step. If you selected **Redundant Device VPN Server**, proceed to Step 13.
5. If you selected **Single Device VPN Server**, select an AP with Layer 2 IPsec VPN services enabled from the drop-down list.
6. **Server Public IP Address** is auto-filled based on the selected VPN server settings, but to change it, enter the IP address of the VPN server that VPN clients can reach across the network.
 - a. If the VPN server is behind a NAT device, enter the address of the MIP address on the NAT device.
 - b. If there is no NAT device in front of the VPN server, enter the server's mgt0 address, which is the same address as that in the next field.
7. **Server MGT0 IP Address** is auto-populated and is read-only.
8. **Server MGT0 Default Gateway** is auto-populated and is read-only.
9. Enter the first IP address of a range of addresses that the VPN server assigns to tunnel interfaces on VPN clients during the Xauth phase of tunnel setup.
Best practice suggests putting 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.
10. Enter the IP address at the end of the range of IP addresses in the address pool.
11. Enter the netmask that defines the subnet to which the tunnel interfaces belong.
12. Select the DNS server IP address or host name that VPN clients use to resolve domain names on the VPN server network.
If you do not see the object you want, select the add icon and add a new one.

13. If you selected **Redundant Device VPN Server** in Step 4, enter the following information for **Device VPN Server 1** and **Device VPN Server 2**:
- **Device VPN Server:** Select an AP with Layer 2 IPsec VPN services enabled from the drop-down list.
 - **Server Public IP Address:** Auto-filled from the selected VPN server settings; editable.
 - **Server MGT0 IP Address:** Auto-filled from the selected VPN server settings; read-only.
 - **Server MGT0 Default Gateway:** Auto-filled from the selected VPN server settings; read-only.
 - **Client Tunnel IP Address Pool Start:** Enter the first IP address for the client pool.
 - **Client Tunnel IP Address Pool End:** Enter the last IP address for the client pool.
 - **Client Tunnel IP Address Pool Netmask:** Enter the netmask for the client pool of IP addresses.

**Note**

The VPN client IP address pools for redundant VPN servers can be in the same subnet or different subnets. However, the address pools must not overlap. If there is overlap, VPN clients can receive duplicate IP address assignments.

14. For **Device VPN Client DNS Server**, choose the DNS server IP address or host name object that VPN clients use to resolve domain names, or select the add icon to define a new one.
15. For **User Profiles for Traffic Management**, select **Enabled** in the VPN Tunnel Mode column to enable VPN clients to tunnel traffic for specific user profiles. ExtremeCloud IQ displays a list of user profiles whose traffic can be forwarded through the Layer 2 IPsec VPN tunnel or forwarded without tunneling.
- a. After enabled, to tunnel all client traffic, select **Tunnel All Traffic**.
 - b. To enable split mode tunneling, select **Split Tunnel**.
16. For IPsec VPN Authority Settings, see [Configure IPsec VPN Authority Settings](#) on page 83.
17. For Server-Client Credentials, see [About Server-Client Credentials](#) on page 84.
18. For Advanced Server Options, see [Configure Advanced Server Options](#) on page 85.
19. For Advanced Client Options, see [Configure Advanced Client Options](#) on page 86.

Configure IPsec VPN Authority Settings

Before You Begin

Create a Layer 2 IPsec VPN service. For more information, see [About Server-Client Credentials](#) on page 84.

About This Task

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 their format from DER to PEM.

**Note**

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.

Procedure

1. If you do not have a certificate or key that you want to use, select **Import**.
2. 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.
3. 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 to each other.

About Server-Client Credentials

As soon as you save the Layer 2 IPsec VPN service configuration, ExtremeCloud IQ populates this 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 a device is configured as a VPN client, ExtremeCloud IQ allocates one of the credentials to it. The name of the VPN client displays 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.

Configure Advanced Server Options

Before You Begin

Create a Layer 2 IPsec VPN service. For more information, see [About Server-Client Credentials](#) on page 84.

About This Task

Use this task to change the IKE Phase 1 and Phase 2 options.

Procedure

1. For **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 are automatically refreshed 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).
2. For **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.

3. 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.

Configure Advanced Client Options

Before You Begin

Create a Layer 2 IPsec VPN service.

For more information, see [About Server-Client Credentials](#) on page 84.

About This Task

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. Use this task to specify which type of management traffic you want VPN clients to send through the tunnel and which to forward locally.

Procedure

1. 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.
2. Select **Enable NAT Traversal** to enable VPN traffic to traverse NAT devices encountered along its data path.
 3. For **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.
 4. 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.

Configure LLDP and CDP Settings

Before You Begin

To enable LLDP/CDP for a port, ensure that LLDP/CDP is enabled under both the policy level and port level configuration.

About This Task

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 the following procedure to enable devices to receive and cache LLDP advertisements, and to advertise their own data through LLDP.

Procedure

1. Navigate to **Configure > Common Objects > Network > LLDP/CDP**.

2. Select the plus sign.
Alternately, you can edit an existing profile.
3. Enter a name for the profile.
4. Enter an optional description.
5. Select whether to enable LLDP on access ports.

**Note**

LLDP is enabled on other port types by default.

6. Select whether to receive, cache, and display LLDP advertisements from other network devices but to not advertise data.
7. Define the maximum number of LLDP entries from neighboring network devices that a device can store in its cache.
8. Set the length of time that the device instructs neighboring devices to retain the LLDP advertisements it sends them.

You might want to increase this setting while engaged in troubleshooting a network issue and decrease it if there is a need to reduce overall network traffic.
9. Set the interval for sending LLDP advertisements to neighboring network devices.
10. Set a maximum power level that devices can request in LLDP advertisements to avoid requests for more power than the switch can provide.
11. Enter the amount of time you want the interface to wait before initializing LLDP.
12. Enter the number of advertisement LLDP frames to send when the connected device (such as an IP phone) starts up or is discovered.
13. Select whether to enable devices to receive and cache CDP advertisements.

**Note**

You can enable devices to support both LLDP and CDP concurrently.

14. Select whether to enable CDP on access ports.
15. Define the maximum number of CDP entries that a device can store in its cache from neighboring network devices.
16. Select **SAVE**.

Configure Location Servers

Before You Begin

Create a network policy for these settings.

About This Task

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.

Procedure

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 203.

AeroScout Location Server: See [Configure Track Client Location Using an AeroScout Location Server](#) on page 202.

Tazmen Sniffer Protocol (Ekahau, etc...): See [Configure Track Client Location Using the Tazmen Protocol](#) on page 204.

What to Do Next

Continue configuring the network policy.

Configure Track Client Location Using an AeroScout Location Server

Before You Begin

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**.

About This Task

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.

Procedure

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 [Add IP Objects and Host Names](#) on page 168.

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.

What to Do Next

Continue configuring a network policy.

Configure Track Client Location Using an Extreme Location Server

Before You Begin

Configure a Location Server.

About This Task

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.

Procedure

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.

What to Do Next

Continue configuring a network policy.

Configure Track Client Location Using the Tazmen Protocol

Before You Begin

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.

About This Task

Use this task to configure Extreme Networks devices to work with a TZSP-based location service.

Procedure

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 [Add IP Objects and Host Names](#) on page 168.
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.

What to Do Next

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.

Add Management Options

About This Task

Read detailed information about Management Options [here](#).

Use these settings to control how administrators are authenticated and how they access the devices they manage.

Procedure

1. Select the plus sign.
2. Enter a name.
3. Enter an optional description.
4. If you are creating management options for APs, proceed to [Configure Forwarding Engine Control Management Options](#) on page 210.
5. After completing the previous step, proceed to [Configure System Settings Management Options](#) on page 211.
6. As a final step, proceed to [Configure Authentication Settings Management Options](#) on page 213.
7. After you have completed all the relevant sections, select **SAVE**.

About Management Options

Toggle the switch to **On** to enable Management Options and configure management settings. Use these settings to control how administrators are authenticated 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 proxying ARP requests and replies, allow 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.

For the steps to create management settings, see <insert cross reference to Add Management Options.>

Forwarding Engine Control

The forwarding engine controls the type of traffic being forwarded between interfaces, between GRE tunnels, and sets logging features.

GRE Tunneling Selective Multicast Forwarding

ExtremeCloud IQ devices can selectively block or allow 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 allowed list that allows all broadcast and multicast traffic through GRE tunnels (or allows all except to a few destinations). For the steps to configure multicast forwarding, see <insert cross reference to Configure Forwarding Engine Control Management>

Service Control

You can set the maximum number of **MAC sessions** (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. 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. Because the additional headers expand packet size, the device will be 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 allow room for the additional headers. Select the check box to enable 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. 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 MTU (maximum transmission unit) 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.)

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 may only be enabled only on access points running IQ Engine 6.8r1 and above. Enabling ARP Shield will not be enforced on access points running IQ Engine 6.5, switches, routers, or Virtual Gateway appliances.

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 6.8r1 and above. Disabling DHCP Shield will result in no changes to access points running IQ Engine 6.5, switches, routers, or Virtual Gateway appliances.

Proxy ARP requests enable learning MAC addresses and proxy replies to ARP requests. By default, this option is enabled and a device proxies all ARP requests and replies that traverse it. However, there might be occasions, such as when you need to diagnose a network issue, when you want to allow the ARP requests and replies between wireless clients and network devices such as the default gateway to flow directly across the device without proxying them..

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 so on before sending the traffic back across the device to reach the clients in the destination SSID.

The **Disable WebUI Without Disabling CWP** option disables the local web user interface on a device to improve system security without disabling the associated captive web portal.

System Settings allow you 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.

Device-level Settings include LED brightness adjustments, temperature alarm thresholds, fan thresholds, VoIP monitoring,

Airtime per Second controls the amount of airtime reserved for VoIP traffic. 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. Decreasing the amount of reserved airtime for VoIP traffic frees more airtime for different types of traffic other than VoIP. This can be useful if there are only a few VoIP users on the WLAN. Conversely, for a high number of VoIP users, increase the amount of reserved airtime for VoIP calls to better support these users.

Guaranteed Airtime for Roaming Clients sets the percentage of airtime that a device reserves on the access interface for receiving VoIP calls from roaming clients. 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 then deducts available airtime from the relevant user profile.

OS Detection allows devices to detect the OS of client devices based on a combination of DHCP option 55 contents and what is contained in HTTP headers. The following detection methods are available:

- Use the DHCP option 55 parameter list to identify the operating system of the connected client.

- Use HTTP user agent IDs to use the contents of the HTTP user agent ID within the HTTP headers to identify the operating system of the connected client.
- Use both detection methods (DHCP=primary method, HTTP=secondary method) 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 a device finds no match, it examines the HTTP header for the HTTP user agent ID to determine the operating system. If no match is found in either pass, ExtremeCloud IQ displays “unknown” as the client OS.

If a device is physically accessible to people other than administrators, you can disable the ability of the reset button on the front panel of the chassis to reset the device to its default settings or to a bootstrap configuration.

You can disable the functionality of the console port on a device and block all administrative access through that port. 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, you will not be able to log in to the device.

Using **Smart PoE**, an AP can detect if there are power injectors connected to one or both of its Ethernet ports, how many watts are available for each PoE channel, and if the power adapter is connected or not. It 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: In the event that 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.

PCI Wireless Control Data Collection provides data about MAC DoS, IP DoS, and MAC filter violations in PCI compliance.

The **Accept ICMP Redirect Messages** feature enables devices to accept ICMP redirect messages from routers on their subnet, or clear it so that devices reject ICMP redirect messages. 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, if you feel 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, then enable this option.

Activate iBeacon for APs that have internal iBeacon transmitters and that belong to a network policy.

The **Report client information gathered from captive web portals** option instructs devices to forward client information (such as name and email address) to ExtremeCloud IQ, where the information is logged as an event.

Authentication Settings

Use authentication settings to configure a database location for storing administrator accounts, set the **PPSK (Private PSK) save** list, and the MAC address format. You can specify the location of the database storing administrator accounts with which the AP authenticates administrators when they log in. You can store admin accounts locally on APs, remotely on RADIUS authentication servers, or both. 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, then the administrators will not be able to log in to the device.

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 its local database second.

Use **Private PSK Server Auto Save Interval** to set 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).

Some servers only accept MAC addresses in a particular format. To accommodate these requirements, you can specify the types of delimiters using MAC Address Format Delimiter between groups of digits, the number of groups to use, and whether to use lower case or upper case. How you set these parameters controls how MAC authentication for local users on an RADIUS server is affected. For example, if you set case sensitivity as lower case (default) 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: 0016CF8D55BCColon, two-delimiter, upper case: 0016:CF8D:55BCColon, five-delimiter, upper case: 00:16:CF:8D:55:BCDash, five-delimiter, upper case: 00-16-CF-8D-55-BCDot, five-delimiter, upper case: 00.16.CF.8D.55.BC

Configure Forwarding Engine Control Management Options

Before You Begin

Create or open an existing Management Option. See [Add Management Options](#) on page 205 for more information.

About This Task

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 only applies to APs.

Procedure

1. Select **Block All** to prohibit forwarding multicast and broadcast traffic through tunnels.
2. Select **Allow All** to enable forwarding multicast and broadcast traffic through tunnels.
3. To specify exceptions to the blacklist (**Block All**) or whitelist (**Allow All**), select the plus sign. In the dialog box, enter the destination IP address and netmask, and then select **Add**. You can also enter an IPv6 address.
4. For **Service Control**, select the fields as follows:
 - **Limit MAC sessions per station:** Select and set the maximum number of MAC sessions (Layer 2 sessions) that can be created to or from a station.
 - **Limit IP sessions per station:** Select and set the maximum number of IP sessions (Layer 3 sessions) that can be created to or from a station.
 - **Enable TCP Maximum Segment Size:** Select to enable a device to monitor the TCP MSS option in TCP SYN and SYN-ACK messages for traffic that passes through GRE tunnels (for Layer 3 roaming and static identity-based tunnels) and GRE-over-IPsec tunnels (for IPsec VPN tunnels). The device notifies the sender to adjust the TCP MSS value if it exceeds a maximum threshold.



Note

For 0 (auto), the device automatically readjusts the TCP MSS thresholds.

- **Enable 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 may only be enabled only on access points running IQ Engine 6.8r1 and above. Enabling ARP Shield will not be enforced on access points running IQ Engine 6.5, switches, routers, or Virtual Gateway appliances.

- **Disable 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 will be able to respond to DHCP discovery or IP lease requests. DHCP Shield is enabled by default on access points running IQ Engine 6.8r1 and above. Disabling DHCP Shield will result in no changes to access points running IQ Engine 6.5, switches, routers, or Virtual Gateway appliances.
- **Disable Proxy-ARP:** Clear this box to enable learning MAC addresses and proxy replies to ARP requests. Helpful for troubleshooting.
- **Disable Inter-SSID Flooding:** Select to disable multicast and broadcast traffic forwarding between access interfaces bound to different SSIDs. The multicast/broadcast traffic is instead moved to the backhaul interface, which can filter/pass on from there.

**Note**

Applies only to traffic on one AP, between client devices connected to two different SSIDs on one AP, on the same radio.

- **Disable WebUI Without Disabling CWP:** Select to improve system security without disabling the associated captive web portal.
5. Configure **Global Logging Options and Firewall Policies** as follows:
 - a. Select the **Log** check boxes to log dropped packets that are denied by MAC or IP firewall policies, and for the first packets of sessions destined for the IP address of the device itself.
 - b. Select the **Drop** check boxes to drop all fragmented IP packets, and all non-management traffic destined for the device.

What to Do Next

Continue to [Configure System Settings Management Options](#) on page 211.

Configure System Settings Management Options

Before You Begin

Create or open an existing Management Option. See [Add Management Options](#) on page 205 for more information.

Read detailed information about Management Options [here](#).

About This Task

System Settings enable you to adjust various device-level functions, including device health alarm thresholds, VoIP features, and client OS detection types.

Procedure

1. Adjust **Device-level Settings** as follows:

- **LED Brightness:** Use the drop-down menu to set device status LED brightness levels.
- **Temperature Alarm Threshold:** Set when a device's ambient temperature generates a warning.
- **Fans Underspeed Alarm Threshold:** Set when the fan's operating speed generates a warning.
- **Call Admission Control:** Indicates if 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.
 - **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. Consider lowering the percent if VoIP users rarely roam, and raising the setting if roaming occurs often.
- **OS Detection:** Enable devices to detect client device OS based on a combination of DHCP option 55 contents and what is contained in HTTP headers. After you select this option, choose from the following detection methods:
 - **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.

2. Adjust **Miscellaneous Settings** as follows:

- **Disable Reset Button:** Select to disable the ability of the reset button on the front panel of the chassis to reset the device to its default settings or—if set—to a bootstrap configuration.
- **Disable Console Port:** Select to disable the functionality of the console port on a device and block all administrative access to the device through that port.



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.

- **Enable Smart PoE:** 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.
- **Enable PCI Wireless Control Data Collection:** Select to include data about MAC DoS, IP DoS, and MAC filter violations in PCI compliance reports.
- **Accept ICMP Redirect Messages:** Select to enable devices to accept ICMP redirect messages from routers on their subnet, or clear it so that devices reject ICMP redirect messages.
- **Report client information gathered from captive web portals:** Select to instruct devices to forward client information (such as name and email address) to ExtremeCloud IQ, where the information is logged as an event.
- **Hostname in Beacon:** 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.

What to Do Next

Continue to [Configure Authentication Settings Management Options](#) on page 213.

Configure Authentication Settings Management Options

Before You Begin

Create or open an existing Management Option. See [Add Management Options](#) on page 205 for more information.

About This Task

In this section, configure a database location for storing administrator accounts, set the PPSK (Private PSK) save list, and the MAC address format.

Procedure

1. Specify the administrator accounts database that stores log-in credentials.

You can store administrator accounts locally on APs, remotely on RADIUS authentication servers, or in both places. If you select **BOTH**, the device authenticates administrators by first checking accounts on the external RADIUS servers specified in the RADIUS profile, and then checking accounts stored on its local database.



Note

If all the AP admin accounts are on a RADIUS server and the device cannot connect to it, the administrators will not be able to log into the device.

2. Set 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.

3. To accommodate MAC Address format requirements, specify the types of delimiters between groups of digits, the number of groups to use, and whether to use lower case or upper case.

How you set these parameters controls how MAC authentication for local users on an Extreme Networks RADIUS server is affected. For example, if you set case sensitivity as lower case and store local users with upper case MAC addresses for their user names and passwords, MAC authentication checks fail.

4. Select **SAVE**.

What to Do Next

Save the Management Option, [Add Management Options](#) on page 205.

Configure External RADIUS Server Settings

Before You Begin

You must create a wireless network SSID with **Enterprise 802.1X** access security. This option requires users to authenticate by entering a user name and password, which are checked against a RADIUS authentication server.

About This Task

If in the process of configuring RADIUS server settings, you discover you need to add an external RADIUS server, use this task. You will need the IP address, authentication port number, and the shared secret for the RADIUS server.

Use the following steps to configure a RADIUS server from the **Configure RADIUS Servers** window:

Procedure

1. Select the plus sign to add a new server.
2. Enter a name for the server.
3. Enter an optional description.
4. Select the IP address or host name for the RADIUS server.

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

If the address object is a host name, make sure that the devices are able to 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.

5. 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.
6. Set the shared secret for authenticating communications with the RADIUS server.
7. Select **Save External RADIUS**.

What to Do Next

Complete the network policy configuration.

Configure Network Services

About This Task

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 Router Firewall Policy](#) on page 193) and QoS traffic classification and marking policies (see [About Classifier Maps](#) on page 182 and [Configure Marker Maps](#) on page 185).

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:

Procedure

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.

Configure an sFlow Receiver

About This Task

Use sFlow receivers to provide visibility into your switch traffic patterns. You can configure sFlow receivers as common objects which you later assign to specific devices. Use the following procedures to configure an sFlow receiver as a common object:

Procedure

1. Select the add icon and then select Switch from the drop-down field.
2. Enter a name.
3. Enter an optional description.
4. Enter the IP address of the receiver where the accumulated data will be sent.
5. 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).

6. 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.

7. 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.

8. 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.

9. 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.

10. Select an interval for the sFlow receiver.

11. Select **Save**.

You can delete a single sFlow receiver or multiple receivers. To delete a single receiver, select the check box for that receiver, or select the check boxes for multiple 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. Enter the new name and then select **Clone**.

Add a Subnetwork Space

About This Task

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.

Procedure

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 219.

Configure Subnetwork Space Advanced Settings

Before You Begin

Create or modify a subnetwork space. For more information, see [Add a Subnetwork Space](#) on page 217.

About This Task

This task contains the next set of optional steps for creation of a new subnetwork space.

Procedure

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 [Add a DNS Service](#) on page 166.



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 Tunnel Policies

About This Task

A tunnel policy sets parameters for Layer 3 roaming or identity-based tunnels. 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.

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.

Use the following steps to add a new tunnel policy to support Layer 3 roaming or for a static identify-based tunnel from here (Common Objects) or from inside the network policy configuration workflow.

Procedure

1. Select the plus sign.

2. Enter a name for this policy.
3. Enter an optional description for the policy.
Although optional, descriptions can be helpful when you are troubleshooting your network.
4. Select one of the available options.
Select **Layer 3 Roaming** to adjust Layer 3 roaming thresholds. Make adjustments in the fields that are displayed.
Select **Identity-based Traffic Tunneling** to configure the tunnel source and destination, and to create a password or tunnel authentication.
Select **Standard GRE Tunneling** to configure non-Extreme Networks tunnel endpoints.
5. Select **Save**.

Configure an AAA Server Profile

Before You Begin

Before you can perform this task, you must create a network policy with an SSID with Enterprise (WPA/WPA2 802.1X) access security, and a default RADIUS server group.

About This Task

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. Use the following steps to configure an AAA server profile.

Procedure

1. Enter a profile name.
2. Enter an optional description.
3. 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.
4. In the **Additional Settings** section, enter the number of seconds for each response scenario.
5. Select **Enable Caching of Credentials** to improve performance across WAN links.
6. Select the number of seconds to retain this credential cache.
7. For Active Directory, select an existing Active Directory user database, or select the plus sign to add a new one.
See [Add an Active Directory Server](#) on page 75 for more information.

8. For LDAP Server, select an existing LDAP server, or select the plus sign to add a new one.
See [Configure an LDAP Server](#) on page 230 for more information.
9. For the **Approved RADIUS Clients** section, see [Add Approved RADIUS Clients](#) on page 74.
10. For Security Options, see [Configure AAA Server Security Options](#) on page 223.

What to Do Next

Continue configuring the server.

Configure AAA Server Security Options

Before You Begin

Configure an Extreme Networks device as a RADIUS Server.

About This Task

Use this task to add increased security to the AAA Server Profile. For more information, see [Configure an AAA Server Profile](#) on page 222.

Procedure

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.
 - **MDS** 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.

What to Do Next

Continue configuring the server.

About Captive Web Portals

Extreme Networks provides two types of captive web portals (CWPs): those that individual APs host on built-in web servers and those that ExtremeCloud IQ hosts on web servers in the cloud. The former supports 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. The latter supports 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 device-hosted CWPs, you must upload the configuration, web page files, and, for secure communications using HTTPS, certificates to your devices.
- For cloud-hosted CWPs, you must upload the configuration to your devices. ExtremeCloud IQ automatically stores the web page files and certificates in the cloud.

ExtremeCloud IQ can include multiple CWPs.

Customize and Preview Cloud-based Captive Portal Settings

Before You Begin

To configure a cloud-based CWP (captive web portal), you must first create a wireless network SSID with **Open** access security, enable the use of a captive web portal, and then select **Cloud Captive Web Portal** on the **Add a Wireless Network** screen. For more information, see [About Captive Web Portals](#) on page 224.

About This Task

This task is part of creating or editing a network policy. Use this task to configure a cloud-based CWP. Extreme Networks provides two types of cloud-hosted CWPs. One controls network access by leveraging user credentials in social media services like Google, Facebook, 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.

Procedure

1. To use social media services, select **Social Login**.
2. To require a PIN for logging in, select **Request a PIN**.

ExtremeCloud IQ sends a randomly generated PIN to authenticate the user.

3. Select an existing CWP or select **Add**.

- a. If you selected **Add**, enter the new CWP's name.
- 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.

The time is expressed in UTC and the report contains events for the previous 24 hours from that time.

- 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 as 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. As long as the customized files have the same names as the default ones, they will immediately take their place after they are imported to ExtremeCloud IQ.

4. Select **Use a different captive web portal for various clients** to use other CWPs for different clients based on device classification and classification rules.
5. Choose **Select a Classification Rule** to select 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 a Classification Rules Network Policy](#) on page 66.

What to Do Next

Complete the network policy configuration.

Customize and Preview Device-based Captive Web Portal Settings

Before You Begin

To configure a device-based captive web portal, you must create a wireless network SSID with **Enterprise 802.1X** access security, enable the use of a captive web portal, and then select **Captive Web Portal** on the **Add a Wireless Network** screen.

About This Task

This task is part of creating or editing a network policy. Use this task to configure a device-based captive web portal (CWP). 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 is displayed and includes a Use Policy Acceptance (UPA) page. When 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.

Procedure

1. Enter a CWP name.
2. Select **Customize and Preview** to see a preview of the captive web portal profile.
 - a. Select **Customize** to modify the landing page colors, logo, language, and message text.
 - b. Select **SAVE CONFIGURATION**.
3. Enable or disable the **Success Page**.
4. Select **Customization and Preview** to view the enabled Success Page.
 - a. Select **Customize** to modify the landing page colors, logo, language, and message text.
 - b. Select **SAVE CONFIGURATION**.
5. Enable or disable **Success Page > Redirect clients after a successful login attempt**.

When enabled, successful clients are sent to either the initial page or to a specified URL.
6. Enter the **Default Language**.
7. Select any additional languages you intend to support.
8. Select the check box for **Display session timer alert before session expires** to display the session timer in the client's browser.

The timer shows the registered client's login status, time remaining in the session, and elapsed time. You can choose to display the timer alert 5, 15, or 30 minutes before the session expires.
9. Enable **Network Settings 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.
 - a. Select **Customize** to enter an IP address and netmask for each of the interfaces.

You can use IPv4 or IPv6 addresses.

10. Enable **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.

- a. 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.
 - b. You can also select the plus sign to add a new VLAN ID.
 - c. Enter the name and VLAN ID.
 - d. Select **SAVE VLAN**.
11. 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. The client's network access is limited to only the AP with which it associated and the client browser is redirected to a registration page. After the guest registers, the AP stores the client's MAC address as a registered client and allows the guest to access external servers.

- a. Set the length of the DHCP lease assigned to the quarantined client of an unregistered guest.

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 very soon after registering.

- b. From the drop-down list, 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.

12. For **Web Servers Registration Period**, set the length of time that a registered client with an active session remains registered.

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.

13. For **Web Servers Domain Name**, enter 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 `cwp.aerohive.com` in the Web Server Domain Name field, and the clients' browsers will not show a security warning when they make an HTTPS connection to the captive web portal.

14. Select **Enable HTTP** to enable HTTPS on the CWP

15. 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.

16. For **Client Redirection**, 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.

17. Select **Introduce a delay before redirecting after a successful login attempt** to determine how long the CWP displays the Success page before initiating the redirection.

18. Select **Introduce a delay before redirecting after a failed login attempt** to determine how long the CWP displays the failure page before initiating the redirection.



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.

19. 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 the plus sign.
 - a. In the **Service Type** box, select one of the following:
 - **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.
 - b. If you selected **Web** or **All**, then paste IP addresses or host names separated by commas into the **Service Type** text box.
 - c. If you selected **Advanced**, then enter or select the following:
 - **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 drop-down list, enter a new IP address or domain name, or select the plus sign and define a new one.
 - **Service**: Choose **Web** to permit HTTP and HTTPS traffic from unregistered clients to the external web server, choose **All** to permit all types of traffic, or choose **Protocol**, enter a protocol number (from 0 to 255), and a port number to define the type of service you want to permit.
 - d. Select **Add**.

Your changes appear in the Walled Garden table.
 - e. To remove a rule, select the check box next to the rule ID and select **Remove**.
21. Select **Save CWP**.

What to Do Next

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

Import Captive Web Portal HTML Files

About This Task

This task is part of creating or editing a network policy. Use this task to import an HTML file for your CWP (captive web portal) configuration.



Note

Import HTML overrides the settings you configured in **Customize and Preview**.

Procedure

1. On the **New Captive Web Portal** page, select **Import HTML** under **Captive Web Portal Settings**.
2. Select **Upload/Remove**, navigate to the files on your system and upload them.
3. Select **Done**.

4. Select the files you want to use as 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. 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. As long as the customized files have the same names as the default ones, they will immediately take their place after they are imported to ExtremeCloud IQ.

What to Do Next

Complete the network policy configuration.

Configure an Extreme Networks A3 Server

Before You Begin

You must have existing A3 RADIUS server services.

About This Task

RADIUS servers offer two types of services:

- Authentication for user credentials (usually on port 1812)
- Accounting (logging) (usually on port 1813)

Security on RADIUS servers is handled with simple passwords. One is configured on the server and the other on each of the clients.

Use the following steps to configure an A3 server:

Procedure

1. Select the plus sign.
2. Enter a name for the server.
3. Enter an optional description.
4. Enter the **IP/Hostname** of the server.
5. Accept the defaults or enter specific **Server Type** ports.
6. Enter an optional password.
7. Select **Save Extreme Networks A3**.

Configure an LDAP Server

About This Task

Use this task to create an LDAP server with AAA Server profiles for devices configured as RADIUS servers. LDAP servers must first be created in the network policy workflow,

and will then appear in the table in this window. You can clone an existing LDAP server profile and customize it using the following procedures.

Procedure

1. 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.

2. Select the clone icon.
3. Enter a name for the cloned server.
4. Enter an **IP Address** or **Host Name**.
5. Enter an optional description.
6. Enter 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.

7. Enter 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`.
8. Enter the LDAP client distinguished name password used during the authentication part of an LDAP session.
9. Select **LDAP** or **LAPDS** for the required communication protocol.
10. Enter any required **Filter Attribute** for searching for elements below the baseObject.
11. Enable or disable removing the realm, which is commonly appended to a user name and delimited with an @ sign, from the filter.
12. Enter the LDAP server **Destination Port**.
13. Enable or disable **Transport Layer Security authentication and encryption**.

If you enabled it, fill in these fields:

CA Certificate File: Select the default certification authority digital certificate type.

LDAP Client Certificate: Select the default LDAP client digital certificate type.

Client Key File: Select the default client key digital certificate type.

Key File Password: Enter the client key file 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**, or **Demand** (as required, on demand).

14. Select **Save**.

Create a Certificate and Key

Before You Begin

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.

About This Task

To support secure wireless client traffic and captive web portal configurations using HTTPS, ExtremeCloud IQ provides features that enable you to create Certificate Management objects.

Procedure

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 232.
 - **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's public key. The third part consists of the same fields hashed with the server's message digest, or public key, and then encrypted with the issuing CA digital signature (the ExtremeCloud IQ CA, for example) private key. See [Create a Server CSR](#) on page 233.
 - **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 235.
 - **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 236.
3. Select **Save**.
4. You can also import a certificate or key.
See [Import a Certificate or Key](#) on page 236.

Create an ExtremeCloud IQ Certificate of Authority

Before You Begin

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.

About This Task

Use this task to generate your own Certificate Authority (CA).

Procedure

1. Select the add icon.
2. Enter a descriptive name or the domain name of the ExtremeCloud IQ appliance or Virtual IQ that you are going to 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.
3. Enter the name of the ExtremeCloud IQ organization.
Examples: Sophia University, Hilton Hotel, Extreme Networks.
4. Enter the name of the ExtremeCloud IQ division.
Examples: Marketing, Engineering, Sales.
5. Enter the ExtremeCloud IQ location.
6. Enter the ExtremeCloud IQ State or Province.
7. Enter the ExtremeCloud IQ two-character country code.
8. Enter an optional contact email address.
9. 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.
10. 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.
11. Enter the corresponding password for encrypting and decrypting the private key linked to the public key in the CA.
12. 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 Server CSR

Before You Begin

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.

About This Task

Use this task to create a server CSR.

Procedure

1. Enter a descriptive name or the domain name of the ExtremeCloud IQ appliance or Virtual IQ that you are going to use to sign server certificates.

These will later be used to verify those server certificates when used to authenticate participants in AAA exchanges. Examples: SophiaCA, HiltonCA, Extreme NetworksCA.

2. Enter the ExtremeCloud IQ organization's name.
Examples: Sophia University, Hilton Hotel, Extreme Networks.
3. Enter the ExtremeCloud IQ division's name.
Examples: Marketing, Engineering, Sales.
4. Enter the ExtremeCloud IQ location.
5. Enter ExtremeCloud IQ State or Province.
6. Enter ExtremeCloud IQ two-character country code.
7. Enter an optional contact email address.
8. Enter 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 SN (subject alternative names) in that certificate to perform two validity checks for the server: The VPN client checks that the SAN the VPN server presents as its IKE ID matches the SAN in the certificate the server supplies, and, the VPN client checks 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:** Enter 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:** Enter a text string in the form of a fully-qualified domain name, such as `portal.extremenetworks.com`.
- **IP Address:** Enter an IP address in dotted decimal notation, for example, `10.1.1.1`.

9. 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.

10. Enter the corresponding password for encrypting and decrypting the private key linked to the public key in the CA.
11. Enter a name to distinguish the CSR file.
12. Select **Save**.

ExtremeCloud IQ saves the CA certificate with the file name `Default_CA.pem` and the accompanying private key as `Default_key.pem`.

13. 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.

Concatenate an Existing Certificate and Private Key

Before You Begin

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.

About This Task

Use this task to create a new file containing a concatenation of a server certificate and an unencrypted private key.

Procedure

1. Enter a name for the concatenated certificate/private key file.
2. Enter an optional note about the certificate for later reference.
3. 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 236.

4. 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 236.

5. Enter the corresponding password for encrypting and decrypting the private key linked to the public key in the CA.

6. 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 You Begin

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.

About This Task

Use this task to create a self-signed certificate.

Procedure

1. Enter a name.
2. Enter the ExtremeCloud IQ organization name.
Examples: Sophia University, Hilton Hotel, Extreme Networks.
3. Enter the ExtremeCloud IQ division name.
Examples: Marketing, Engineering, Sales.
4. Enter ExtremeCloud IQ location.
5. Enter ExtremeCloud IQ State or Province.
6. Enter ExtremeCloud IQ two-character country code.
7. Enter an optional contact email address.
8. 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.
9. 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.
10. Select **Save**.

Import a Certificate or Key

About This Task

If you use a third-party CA to sign certificates, generate and export a CSR, send it to the CA, and when the CA returns the signed certificate and private key file, import the

certificate into ExtremeCloud IQ. Extreme Networks devices support PEM-formatted certificates.

Use the following procedure to import a CSR:

Procedure

1. Select the import icon.
2. Use **Select** to navigate to the location of the certificate file.
3. Select **Open**.
4. Select **Import**.
5. Select whether this file is a certificate or key.

To import certificates in PFX or DER formats, you must first use the conversion tool to reformat them as PEM files.

6. To import a PFX-formatted file, which contains a certificate and private key combined, first convert its format from PFX to PEM:
 - a. Select **Convert the certificate format from PFX to PEM**.
 - b. 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.

7. 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**.
8. Select **Save**.



Manage

- [Use the Filter Sidebar](#) on page 239
- [An Overview of Your Network](#) on page 239
- [Plan your Network](#) on page 240
- [Device List Views](#) on page 248
- [Device Details Overview](#) on page 267
- [Reports](#) on page 288
- [Manage Users](#) on page 292
- [Manage Events](#) on page 293
- [Alerts Management](#) on page 294
- [Manage Active Alarms](#) on page 295
- [Rogue APs](#) on page 295
- [Rogue Clients](#) on page 297
- [Manage Network Applications and Application Groups](#) on page 298
- [About Client Monitor](#) on page 298
- [About Diagnosis](#) on page 302
- [VPN Management](#) on page 304
- [Set the Time Frame for Captured Data Displays and Reports](#) on page 304

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:** 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.

Use the Filter Sidebar

About This Task

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.

The 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.

You can save individual filters or a list of filters. Saved filters are displayed in the saved filters section.

An Overview of Your Network

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. Generate and distribute customized reports in HTML format from the **Create Reports** tab. Download report data in **.csv** format. The Dashboard contains eight data widgets.

- **Network Summary:** This widget 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. The data updates hourly.
- **Top Application Groups:** This widget presents top usage in **Application Groups** 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:** This widget presents 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 (clients or users):** This widget presents top data usage. The data for client or user 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:** This widget presents a listing of Wi-Fi clients by OS type. The information displayed is customizable to show the frequency band distribution (2.4 GHz, 5 GHz, or both). You can download the data details in a spreadsheet.
- **Top Wired:** This widget presents 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):** This widget presents 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:** This widget is a bar graph showing the simultaneous client types within the selected period. You can download the data details in a spreadsheet.

Related Topics

[Set the Time Frame for Captured Data Displays and Reports](#) on page 304

Plan your Network

Use the **Planning** page under **Manage** to 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.



Note

Due to the complex factors that can 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 location name here to see a list of locations. The more characters you enter, the more precise the search results will be.
- **Global View** gives you an overall view all your network in the map. Beneath Global View, you will see the names of all locations, buildings, and floors. You can add multiple buildings to a location, and multiple floors to a building by importing floor plans or by drawing your own floor plan. For information about how to add locations, see [Add a Location](#) on page 241. For information about how to add buildings, see

[Add a Building](#) on page 242. For information about how to add floors, see [Add Floors](#) on page 243.

- **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:** Buildings maps display when you select a building in the hierarchy. A building map contains a floor plan of the building. Building maps contains **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. Select any blue text in the expanded Details panel to drill down for more specific network information. If there are multiple floors in a building, you can toggle between them to see floor plans and device deployment.
- **Floor Maps:** Floor maps display when you select the floor name in the hierarchy. 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 Heatmaps](#) on page 247.
 - **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.

Add a Location

About This Task

Use this task to add a location to your network map.

Procedure

1. From **Manage > Planning > Global View**, select **Add Location**.
2. Enter the location name.
3. Enter the location address.
4. Enter the associated network.
5. For an outdoor location:
 - a. Choose an environment type that most closely matches your installation.
 - b. Enter the most common installation height for APs.

- c. Enter a map size.
 - d. Enter a background image floor plan from your library.
For more information about floor plans, see [Add Floors](#) on page 243.
6. Select **Save**.

Add a Building

Before You Begin

Your network hierarchy must contain at least one location before you can add buildings and floors.

About This Task

Use this task to upload building perimeters and floor plan images which you can store in the image library for future use.

Procedure

1. Highlight a location from your network hierarchy.
2. Select **Add Building**.
3. Enter a name for the building.
4. Enter the building address.
5. Enter the associated network.
6. Select **Save**.

Draw a Building Perimeter

Before You Begin

You must have a network location that includes at least one building before you can draw a building perimeter.

About This Task

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.

Procedure

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**.

What to Do Next

The next step is to add internal walls and obstructions to the floors in your building. See [Add Interior Walls and Obstructions](#) on page 243

Add Interior Walls and Obstructions

About This Task

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.

Procedure

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 Floors

About This Task

Perform the following steps to add a floor to a building.

Procedure

1. In the **Hierarchy** panel, double-click the name of a building, or select **Add Floor** above the building map.
2. Enter a name for the floor.
3. Associate the floor with a building.
4. Choose an environment.
5. Enter the noise level (**Floor Attenuation**) of the floor.

6. Enter the installation height (distance from floor to ceiling) of the APs on the floor.
If the height varies from AP to AP, enter the average height. This setting has a minimal effect on location estimates except for sites such as warehouses where the height of ceilings or high crossbeams is substantial.
7. Enter the dimensions of the floor plan.
8. Upload a background image of a floor plan from the drop-down list, or use the drawing tools to draw a floor plan.
9. To scale the map for imported images, select the gear icon, and then select **Rescale Plan**.
10. Enter dimensions, or size the image manually by moving the red cross hairs to the end points of a known distance, such as a standard doorway.
11. Enter the known distance and select **Apply**.
12. Select **Save**.

Related Topics

[Draw a Floor Plan](#) on page 244

[Size a Floor Plan](#) on page 245

Draw a Floor Plan

About This Task

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.

Procedure

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

About This Task

When you import a floor plan with a background image, you need to scale the floorplan. Use the following steps.

Procedure

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

Before You Begin

Create a network hierarchy with at least one location, building, and floor.

About This Task

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 246.

Procedure

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.

Results

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

Before You Begin

Create a network hierarchy with at least one location, building, and floor.

About This Task

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 245.

Procedure

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.

Results

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 243), and view heat maps ([View Heatmaps](#) on page 247) to calculate the best deployment sites.

View Heatmaps

Before You Begin

Populate your maps with real devices, simulated devices, or a combination.

About This Task

Use this task to view device heat maps to see data about your wireless network coverage, including RSSI, SNR, channels, data rates, and interference.

Procedure

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.

Results

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.

Device List Views

Manage > Devices

Use the Device List to view, [add](#), and [update](#) managed and unmanaged devices, and perform other management actions. Select the check box for a device to see the [Utilities](#) and [Actions](#) available for that device. Select the host name of a device to see and configure additional details.

For more information about the default view of the Device List, see [Device List Views](#) on page 250.

Filters

Use the [filter sidebar](#) 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 looks normal. When one or more filters are applied, the icon contains a colored dot. You can save and name multiple filters.

Default Table Columns

The Device list includes several default columns, but you can customize your view using the column picker. For more information about the default table columns, see [Default Device Columns](#) on page 250.

Status Indicators

The Status Indicators above the table shows network connection status, total apps, clients, users, alarms, and security. This data automatically updates whenever you open the Devices window. Hover over or select any non-zero value in an indicator to see more. Select the refresh icon to refresh the status indicator and device data. Hover over or select any number to see more information.

The Status column in the table can contain multiple icons indicating the status of the device. Hover over any icon for more information.

Digital Twin

See [About Digital Twin](#) on page 250.

Device List Views

View and configure your managed devices from any of the main views. The default view shows you all of the devices in your network. For more information, see [Device Details Overview](#) on page 267.



Note

Switch Stack Display: Switch stacks appear in the device list by the hostname of the primary switch. Select the stack icon next to the switch host name to see stack details.

- **Default View:** Select **Default View** to see a drop-down list of the other view options, which are described [Device List Views](#) on page 250. From any of these views, you can add, delete, and update your network devices, and customize your view using the filter tool.
- **Default Device Columns:** The default columns that are displayed in the device list are described [Default Device Columns](#) on page 250. Use the column picker to customize the table columns. Scroll horizontally if the columns do not fit the width of the window. Select and drag the right edge of any column to change the column width. Your customized display is maintained even when you go to another window, log out and then log in again.
- **Device List Functions:** Several features help you understand how your devices are functioning. These features are described [Device List Functions](#) on page 252.

See [Manage](#) on page 238 for more information about the **Manage** tab.

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 display 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.

Device List Views

Select **Default View** to see a drop-down list of the other view options, which are described below. From any of these views, you can add, delete, and update your network devices, and customize your view using the filter tool. The available device views are:

- **Default View:** Displays information about all of the devices in your network, including controllers and their controller-managed devices.
- **Wireless View:** Displays information about only the wireless devices on your network.
- **LAN View:** Shows data for LAN devices in a specific location. LAN view table columns can be arranged independently of the other views using the LAN column picker.
- **WAN View:** Shows data for only WAN routers and is set to L3 mode. WAN view table columns can be arranged independently of the other views using the WAN column picker.
- **Locally Managed View:** Displays devices that are managed locally, such as those managed by IQ Virtual Appliance or by a controller.
- **Controller View:** Displays all onboarded controllers.

Default Device Columns

The default columns that are displayed in the device list are described below. Use the column picker to customize the table columns. Scroll horizontally if the columns do not fit the width of the window. Select and drag the right edge of any column to change

the column width. Your customized display is maintained even when you go to another window, log out, and then log in again.

By default, the table contains the following columns:

- **Status:** The connection status of the device, indicated by icon colors. Hover over an icon to see what it identifies. Select [here](#) to display the complete status icon table.



Note

For switches, an icon indicates that the switch uses device-level configuration settings instead of the device template (network policy) configuration. Select this icon to revert to the device template configuration.

- **Host Name** (sortable): The host name of the device. Select the host name to see an overlay window with detailed information and configuration options for this device.
- **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**.
- **Managed By:** Whether the device is managed by ExtremeCloud IQ or ExtremeCloud IQ Site Engine. Site Engine manages devices not produced by Extreme Networks.
- **Uptime:** The amount of time since the device last rebooted and re-connected.
- **MGT IP Address:** The IP address of the device.
- **Clients:** The number of clients connected to this device.
- **MAC:** The MAC address of the device.
- **Location:** The location of the device in your network. To assign or change the location, either select the location name, then select the Actions>Assign Location link, or select the name in the location column. In the dialog box, highlight the device, move it to the correct 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.

- **Serial #:** The serial number of the device.
- **Feature License and Device License:** Identifies the type of license the device is using. None or a blank in these columns indicates that no license exists. Licenses are not required for simulated, unmanaged, or free-license devices.
- **Model:** The hardware model of the device. The hardware model and serial number appear on a label on the underside of the chassis.
- **OS Version:** The version that is currently running on the device.
- **Updated:** The last time the configuration on this device was updated. If an update was not successful, 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 automatic provisioning. Hover over the error message to see details. To view error message descriptions listed by device and timestamp, select the error message link.
- **MGT VLAN:** The management VLAN for this device.

- **MAKE:** Extreme Networks: For example, Fabric Engine, Switch Engine, EXOS, VOSS, WiNG. External: For example CISCO.
- **MANAGED:** Whether or not the device is currently managed.
- **COUNTRY:** The device country location code.
- **OS:** The operating system currently running on the device. For example, FABRIC, WiNG, CLOUD-IQ ENGINE, CISCO.

Some other column display options are as follows:

- **IQ Agent:** For switches, the IQ Agent version. IQ Agent enables communication between switches and ExtremeCloud IQ.
- **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.
- **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 WiFi0 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 WiFi0 radio is operating.
- **WiFi2 Power:** The power level of the WiFi2 radio.
- **WiFi0 Power:** The power level of the WiFi0 radio.
- **NTP State:** Shows whether NTP is enabled, disabled, or is not applicable.
- **Stack Unit:** The unit number of a switch in a stack.
- **Stack Role:** The role (primary, secondary, or member) of a switch in a stack.

Device List Functions

Several features help you understand how your devices are functioning. These features are described below:

Status icons: [Status icons](#) appear in the table for each device. Hover over any icon to see the icon name.

Download device data: Select the download icon to download data in .csv format.

Search for devices: Enter all or part of a device name, MAC address, or serial number in the search field to see a display of all matches.

Edit devices: Select the check box or device host name, then select the edit icon. You can also select multiple check boxes for devices that you want to edit simultaneously.

Delete devices: Select the check box for each device or devices, select the delete icon, and confirm the deletion.

To select devices: Select the host name or check box. The number of devices you select is displayed in **Showing <devices selected> of <total filtered devices> Selected**. There are multiple ways to select devices:

- Select each device check box individually.
- Select all of the devices in the current window by selecting the header row check box at the top of the list (bulk select). Then clear the check boxes for devices for which you do not want to perform an action.
- When you have multiple windows of devices, to select all of devices in all windows, choose **All Pages** above the table.

View Configuration Audit Matches and Mismatches: Select the configuration audit icon to see the following information on the Audit, Delta, and Complete tabs in the dialog box:

- The **Audit** tab lists any modifications made since the previous configuration update.
- The **Delta** tab shows CLI commands that have changed since the previous update.
- The **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.

Device Status Icons

Table 4: Device Status Icons





Icon	Icon Name	Full Description
	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.
	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.

Table 4: Device Status Icons (continued)











Icon	Icon Name	Full Description
	Unknown State	Device is in an unknown state. Cause: This condition can arise when the indicators are ambiguous, indeterminate, 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.
	Configuration Audit Match	The network policy configuration matches the current running configuration.
	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.
	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.
	Device Update Unsuccessful	Device did not accept the OS or configuration upload. Cause: There are many reason 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.
	Monitoring Unassociated Clients	Device is using presence analytics to monitor client devices that are not associated to the network, such as passers by.
	Switch Stack (Closed)	Device is a switch stack, but the stack is collapsed visually and displays as a single device.
	Switch Stack (Open)	Device is a switch stack, and the stack is expanded visually to reveal stack members.

Table 4: Device Status Icons (continued)











Icon	Icon Name	Full Description
	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.
	Swap for Real Device	Device is a simulated device that you can exchange for a real device.
	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.
	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.

Table 4: Device Status Icons (continued)











Icon	Icon Name	Full Description
	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 (ExtremeCloud IQ)	Device is managed by a platform that is visible in ExtremeCloud IQ.
	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.
	Extreme Cloud Appliance Cluster (Closed)	Device is a logical cluster of appliances, but the cluster is collapsed visually to appear as a single device.
	Extreme Cloud 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.

Table 4: Device Status Icons (continued)

Icon	Icon Name	Full Description
	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.

Utilities

About This Task

The **Utilities** drop-down list in the **Manage** section offers a variety of useful troubleshooting tools.



Note

Utilities are only available for devices managed by ExtremeCloud IQ (XIQ), not devices managed by ExtremeCloud IQ Site Engine (XIQ-SE). 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 the cross-references below:

- For more information about device diagnostics utilities, see [Device Diagnostics](#) on page 258.
- For more information about Spectrum Analysis, see [Spectrum Intelligence Details](#) on page 260.
- For more information about PSE, see [Restart PSE](#) on page 261.
- For more information, see [Restart Device to Default](#) on page 259.

Status options include:

- Advanced Channel Selection Protocol
- Interface
- Wi-Fi Status Summary

Tools options include:

- Client Info
- Get Tech Data. See [Get Tech Data](#) on page 262

- Locate Device. See the locate device steps below, and [Locate Device](#) on page 262.
- L2 Neighbor Info, see [Neighbor Information](#) on page 262.
- Packet Capture, see [Perform a Remote Packet Capture](#) on page 263.
- VLAN Probe, see [VLAN Probe](#) on page 263.

Use the following steps to locate a device:

Procedure

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

About This Task

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.

Procedure

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.
- **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.

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

About This Task

(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**

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.

Procedure

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 260.

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 complete understanding of the affected frequencies and channels.

Neighboring APs

A table displays a list of neighbor APs.

Restart PSE

About This Task

(Applies to switches only.) You can restart the PSE function on PoE switches.

Procedure

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.

Client Information

Client Information presents an aggregated view of unique historical client connections within the last 30 days.

Get Tech Data

About This Task

This utility collects technical data about devices to assist in troubleshooting.

Procedure

1. Select one or more devices.
2. Select **Get Tech Data**.
3. Confirm the number of devices you selected.

What to Do Next

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

About This Task

Use the Locate Device utility to alter the status LED on an AP 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.

Procedure

1. Select the device that you want to locate.
2. Select **Locate Device**.
3. Select the color and blink mode for the status LED.
4. Select **Submit**.
5. To return the LED to normal operation, select **Return to normal mode**.

Neighbor Information

About This Task

This utility lets you see information about the backhaul link between a device and its neighbors.

Procedure

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.

Perform a Remote Packet Capture

Before You Begin

This function requires you to use a trial or paid CloudShark account, which you can create at <https://www.cloudshark.org/>.

About This Task

Use this task to perform packet captures on a target network AP.

Procedure

1. To initiate a packet capture and direct the results to CloudShark, set the capture parameters and select the **CloudShark Download Location**.
When completed, you can view the capture via use of the CloudShark website application.
2. To initiate a packet capture and direct the resulting capture to you local drive, set the capture parameters and select the **Local Download Location**.
These files are available on ExtremeCloud IQ for an hour.

VLAN Probe

About This Task

A VLAN probe helps you locate available VLANs for devices in a complex network with multiple VLANs.

Procedure

1. Select the device for which you want to locate available VLANs.
2. Select **VLAN Probe**.
3. Enter the start and end of a range of VLAN IDs to probe.

You can enter up to five ranges, however, range numbers cannot overlap.

4. Define how many probes to send (up to 10) on each VLAN.
5. Specify how long to wait for a reply from each probe.
You can set a timeout from 1 to 60 seconds.
6. Select **Stop** to stop a probe before it is complete.
7. Select **Clear** to clear entries for a probe.

Results

When the VLAN probe is complete, a display shows whether the probed VLANs are available for use, and if so, their subnet.

SSH Availability

About This Task

You can use the SSH Availability utility to temporarily enable SSH availability on a device.

Procedure

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.

About Actions

Actions let you perform a number of functions for a device. Depending on the device type selected, the **Actions** drop-down list presents multiple options; for example, you can reboot, assign a country code or location, assign a network policy, create a bootstrap configuration, clone a device, or issue CLI commands to devices through ExtremeCloud IQ. Select the check boxes for the device or devices on which you want to perform actions, and then select **Actions**.



Note

Not all actions are available for all device types.

- **Assign Network Policy:** Assign an existing network policy to the device or devices.
- **Assign Location:** Assign a location from your network maps to the 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.

- **Reboot:** Reboot devices after uploading a configuration. Rebooting momentarily disconnects any associated clients from the SSID, which could be disruptive.

- **Assign Country Code:** Select a country code for a managed device from the drop-down list. The country code determines which radio channels and power limitations devices will support to comply with the wireless regulations for the country in which they will operate. For devices intended for use in the United States, the region code is preset as **FCC** and the country code is preset as **United States**. Select **Save** to reboot the selected devices.
- **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 116.
- **Change Device Mode:** Change the device mode from AP to Router.
- **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.
- **Advanced:** This option offers three functions: **CLI Access**, **Bootstrap Configuration**, and **Update Netdump Settings**. Select the check boxes for the devices you want to update, and select one of these options from the **Advanced** menu:
 - **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 265 for more information.
 - **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. See [Update Netdump Settings](#) on page 266 for more information.
- **Assign Deployment Mode:** Assign Pre-provisioned or production deployment modes.
- **Change Management Status:** Choose managed or unmanaged.
- **Clear Audit Mismatch:** There can occasionally be a mismatch between the configuration database and the device configuration database. If this occurs, perform this action.
- **Clone Device:** Apply the existing device-level configuration from one device to a new device with the same model. For example, if a 5520-24T switch malfunctions and you need to replace it with a new 5520-24T switch, this option allows you to apply the existing device-level configurations used by the previous 5520-24T. For more information, see [Clone A Device](#) on page 267.

Bootstrap Configuration

About This Task

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.

Procedure

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

About This Task

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.

Procedure

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**.

What to Do Next



Note

This feature becomes active after you perform a full configuration update for the selected devices.

Clone A Device

About This Task

Use this task to apply the existing device-level configuration from one switch to a new switch with the same model. For example, if a switch malfunctions and you need to replace it with a new switch, this task enables you to do so and then apply the existing device-level configurations used by the previous switch.



Note

Licensing is not cloned.

Procedure

1. Select the check box for the device in the **Device List**.
2. Select **Actions**.
3. Select **Clone Device**.
4. Under **Replacement Device**, if the device is not yet **Onboarded**, select **Quick Onboard**, enter its serial number and proceed to **Step 6**.
 - a. 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.

Device Details Overview

Select the host name of a device in the Device list to see a details panel for that device. At the top of this panel you will see a graphic showing how this device is connected.

Hover over the icon to see node type, IP address, host name, and VLAN assignments for this device.

The left column of this panel displays an image of the device location, an icon and model number of the device, optional uploaded images of the actual device installation, the connection state, active alarms, the number of connected clients, and real time CPU and memory usage data.

Below this information are two tabs:

- **Monitor:** Select to display details about the status of this device. Refer to [Device Details Monitor Functions](#) on page 268.
- **Configure:** Select to perform device-level configuration tasks and update your devices directly. Refer to [Device Details Configuration Tasks](#) on page 271.



Note

The options that appear under the Monitor and Configure tabs vary depending upon your selected device.

Device Details Monitor Functions

The **Overview** page provides an overview of the device status.

Depending on the device, you can further monitor the status of the device as follows:

- **Clients:** Provides details of the [Clients](#) on page 268 connected to the device.
- **Diagnostics:** Provides a [Diagnostics](#) on page 269 details timeline for the device, such as port transmit and receive traffic.
- **Events:** Displays changes to the network, including configuration changes, for which [Events](#) on page 269 notifications exist.
- **Alarms:** Indicates network issues for which [Alarms](#) on page 270 exist and require administrator attention.

Clients

Under **Manage > Devices > Monitor > Clients**, a graph displays a blue timeline representing 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 change the time frame using the **Time Range** controls.

Details about the clients that are connected during the specified time range are listed in the table. These details include:

- Type of client (wired, wireless, undetermined)
- OS type
- Connection status
- Host name
- Client MAC address
- Connected port name
- User name

- VLAN to which client is connected
- Client IP address
- SSID

You can select any point along the timeline in the graphic to display details only for connected clients at that precise time.

Use the filter to specify what details to display. You can also use the **Search** field to filter your view.

Related Topics

[Set the Time Frame for Captured Data Displays and Reports](#) on page 304

Diagnostics

Under **Manage > Devices > Monitor > Diagnostics**, a graph displays diagnostics statistical data captured for ports for the specified time frame. By default, the data capture time frame is 24 hours. You can change the time frame using the **Time Range** controls.

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 utilisation
- Transmit and receive errors
- Transmit and receive data usage types (unicast, multicast, broadcast)

After you select one or more ports on the diagram, select **Port Details** for in-depth information about each port. After you select one or more port checkboxes, you can use the **Action** dropdown to bounce those ports or bounce their PoE.

Related Topics

[Set the Time Frame for Captured Data Displays and Reports](#) on page 304

Events

A graphic at the top of this window shows the device and its network connections. Events that occur in the network for the selected device are recorded and displayed in this window. Table data is updated hourly. Select whether you want to display events from the current day or up to seven days. There is an **Events** tab and a **Configuration Events** tab above the table. Configuration events show only changes to the device configuration, either from inside a network policy, or at the device level.

Use the key-ahead 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**. You can download table data as a **.csv** file.

Sort the table by the event category using the drop-down list. To control how the information is presented, select any of the column headings. For example, if you want to organize the content by host name, select the **Host Name** heading.

Each alarm or event log entry consists of the following elements:

- **Type:** Indicates if the row represents an alarm or an event.
- **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. The following can be displayed: Major, Info, and Clear.
- **Category:** Indicates how ExtremeCloud IQ was notified of the alarm or event. Available categories are CAPWAP, channel power, state change, client connection down, and client connection change.
- **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.

Alarms

Under **Manage > Devices > Monitor > Alarms**, a table lists active alarms for network issues that require administrator attention. There are two views available here: **Alarm Details** (default view) and **Timeline**.

The Alarms **Timeline** view displays a graph with colored timelines representing when and how many active alarms have occurred and were cleared. By default, the graph displays data captured for a 24-hour time frame. You can change the time frame using the **Time Range** controls.

For either view, use the **Update** button to update your devices to reflect changes you make here. Use the refresh icon to refresh the data. Use the column picker to select which columns are displayed. Your column selections are maintained even if you go to another window and return, and when you log out and log in again. Horizontal scrolling is available for this table when there are too many columns to fit in your display window.

Alarm Details default table 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.

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 and are displayed in the Event 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 Topics

[Set the Time Frame for Captured Data Displays and Reports](#) on page 304

Device Details Configuration Tasks

ExtremeCloud IQ enables you to perform device-level configuration tasks and update your devices at the device level. Settings made at this level (**Manage > Devices > device_name > Configure**) 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.

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.
- **Port Configuration:** Edit port types, STP, Storm, and PSE settings.
- **Device Credentials:** Assign or change network administrator credentials and administrator assignments.
- **SSH:** Temporarily enable SSH in order 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 select an AP 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.
- **Interface Settings:** View the default template settings and control actions for the **Wireless** (WiFi) and **Wired** (Ethernet) ports. You can edit any field that is not grayed out.
- **Device Credentials:** Assign or change network administrator credentials and administrator assignments, and configure CAPWAP and Shared Key settings.
- **Configure Netdump:** Enable an unresponsive AP to automatically save a core dump file to a TFTP server on the network the next time it boots.
- **DHCP Server and Relay:** For a small network, configure and enable a DHCP server on a device to provide network settings dynamically to clients.
- **Neighboring Devices:** Define a list of neighbor access points that will collaborate in the Layer 3 roam process.

- **Bonjour Gateway Settings:** Choose the AP you want to act as your Bonjour Gateway Designated Device (BDD) at the device level.
- **Troubleshoot:** Enable Client Monitor so devices can detect client issues, and report client connection activities and problems to ExtremeCloud IQ.
- **SSH:** Temporarily enable SSH in order to troubleshoot the device.

After you make changes to the configuration, you need to [push the configuration changes to the device](#).

AP Device Configuration

About This Task

Device configuration is handled at the device template level. It is a best practice to configure devices using a device template. However, it is possible to override the device template settings for a specific device. To configure settings for a specific AP, take the following steps:

Procedure

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. The following **Device Details** display:
 - **Host Name:** Enter 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:** Enter a location name, for example `headquarters, building 1`.
4. For **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.
5. For **Management Interface:**
 - **Static Address:** Select this option to enter a static address for this interface.
 - **IPv4 Address:** Enter the IPv4 address you want the device to use for the mgt0 interface.
 - **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.
 - **Dynamic Address Configuration (DHCP):** Select this option to have an address automatically assigned by DHCP.
 - **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 IP Address 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.
 - **Automatically Generate Subnet Mask:** Enter the netmask for the subnet to which the mgt0 interface connects.
 - **Static Fallback 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.
 - **Static Fallback Subnet Mask:** Enter the appropriate netmask for the subnet to which the mgt0 interface connects.
 - **Static Fallback Default Gateway:** The address through which the device (and its connected hosts) can reach the Internet.
 - **Management VLAN:** Enter the management VLAN for this interface.
 - **Native VLAN:** Enter the native VLAN for this interface.
6. For information about **Supplemental CLI**, see [Device Details Configure Supplemental CLI](#) on page 276.
 7. Use **Disable WebUI on Device** 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** to view the corresponding override table.
 10. For **Antenna Location Type**, select a location from the drop-down list.
 11. To update the device immediately, select **Update Now** 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 288.

Related Topics

[Configure Device Templates](#) on page 92

Switch Device Configuration

About This Task

Use this task to make device configuration changes at the switch device level, which overrides any equivalent settings in the network policy assigned to this device after you push the updated configuration to the device.

Procedure

1. To configure or modify existing settings for a specific switch, select the host name of the switch in the **Devices** list, then select the **Configure** tab in the **Device Details** panel, under the **Configure** tab, and select **Device Configuration**.
2. For **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`.
3. For **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.
4. **Enable or Disable Management Settings**.

When enabled, Switch Engine management interface settings will be applied and override template-level management interface settings. If disabled, template settings can be applied or the device will use manually configured management interface settings. Leave disabled when using **Out-Of-Band Management**.
5. Configure **Supplemental CLI**.

For more information, see [Device Details Configure Supplemental CLI](#) on page 276.
6. To update the device immediately, select **Update Now** in the upper-right corner of the page.

For more information about how to push updated configuration to the device, see [Push the Device-Level Configuration to the Device](#) on page 288.

Device Management Servers

Before You Begin

The **Device Management Servers** page does not appear until you apply a network policy to the device.

About This Task

Use this task to override a network policy and make device-level changes to management server settings for a device. The changes only affect 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 management servers page does not display until you apply the network policy to both single switches and stacks.

Procedure

1. Select **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.

*Configure Device Ports***About This Task**

You can configure port configuration details and settings at the device level. Device 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 in order to change the device-specific port configuration. You can also return to the original template configuration with the **Revert** option.

**Note**

Only options available to the specific switch display. For details about each option, see [Create a New Port Type](#) on page 137.

Procedure

1. If not already there, navigate to **Manage > Devices**.
2. Select a device hostname to see a details panel for that device.
3. Select the **Configuration** tab.
4. Select **Port Configuration**.
5. Select **Unlock** to enable device-level configuration changes.
6. Select **Port Details**.
7. Edit any field that is not grayed-out.

8. Select **Port Settings**.
9. Edit any field that is not grayed-out.
10. Select **STP**.
11. Edit any field that is not grayed-out.
12. Select **Storm Control**.
13. Edit any field that is not grayed-out.
14. Select **PSE**.
15. Edit any field that is not grayed-out.
16. Select **Save Configuration**.
17. To revert back to the network policy, from the **Devices** list, select the check box for this device, and from the **Actions** drop-down, use the **Revert Device Template to Device Defaults** option.

Configure Port Router Forwarding

About This Task

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.

Procedure

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

Before You Begin

To use the supplemental CLI tool, first navigate to **Global Settings > VIQ Management**, and enable **Supplemental CLI**.

About This Task

Use this task to update CLI commands to multiple devices simultaneously from ExtremeCloud IQ. You can save supplemental CLI objects containing CLI commands, and the commands can then be automatically updated for devices each time you update the network policy. On the **Device** page, you have the option to keep the Supplemental CLI object in the network policy and append another Supplemental CLI object to the end of the running configuration list.

Customers who use CLI to manage features that are not configured in the UI can choose to override the UI (or to override the CLI). This can benefit deployments that rely on overly complex CLI objects.

Procedure

1. Select the Supplemental CLI object from the list of previously saved Supplemental CLI objects, or select the plus sign to add a new Supplemental CLI object (see [Add a Supplemental CLI Object](#) on page 277 for more configuration information).
2. 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.
3. When you are finished, select **Save**.
4. To update the device immediately, select **Update Now** at the top right.
5. In the Device Update dialog box, select the type of update, and then select **Save as Defaults**.
6. To update the device immediately, select **Perform Update**.

Add a Supplemental CLI Object

Before You Begin

To use the supplemental CLI tool, first navigate to **Global Settings > VIQ Management**, and enable **Supplemental CLI**.

About This Task

Use this task to update CLI commands to multiple devices simultaneously from ExtremeCloud IQ. You can save supplemental CLI objects containing CLI commands,

and the commands can then be automatically updated 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 will result 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 startup. Re-running some commands after already applied can cause future **Device Update Failed** errors.

Procedure

1. To add a new supplemental CLI object:
 - a. Enter a name.
 - b. Enter an optional description.
 - c. Enter 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}`.
2. Select **Save** and perform a complete configuration update each time you append commands to device configurations.

About Digital Twin

Digital Twin allows you to create simulated devices for Universal Hardware switch models to help you prepare your network for real devices. Digital Twin devices display in the device list and are identified with an icon with two masks. From the device list, you have several options:

- Select the hostname of a twin to see 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.

To learn about Digital Twin device configuration, see [Device Details Configure a Digital Twin Device](#) on page 278.

Device Details Configure a Digital Twin Device

About This Task

Digital Twin allows you to create simulated devices for Universal Hardware switch models to help you prepare your network for real devices. You can create up to 20

Digital Twin devices, each with a lifespan of 4 hours. 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. Use this task to configure a Digital Twin device.

Procedure

1. From **Manage > Devices**, select the plus sign above the device list.
2. Select **Quick Add Devices > Deploy Your Devices Directly to the Cloud**.
3. Under **Device Type**, select **Digital Twin**.
4. Select an **OS Persona**.
5. Select a device model from the drop-down list.
6. Select the **OS version**.
7. Assign a network policy from the drop-down list.



Note

You can do this at a later time if you have not yet configured a network policy.

8. Select **Launch Digital Twin** or **Relaunch Digital Twin**.

Results

The Digital Twin devices now appears in the Device List.

Related Topics

[About Digital Twin](#) on page 278

Configure Device Credentials

About This Task

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 device. Device-level credentials offer access to devices through Telnet, SSH, or console connections.



Note

At this level, you are making changes to the selected device only. These changes always override the network policy configurations. To revert to the settings in the network policy, from the **Device List**, select the device host name, and use the **Actions** button.

A root admin has complete privileges, which include the ability to add, modify, and delete other administrators, and to reset the configuration. A read-only admin can view settings but cannot add, modify, or delete them. You can require that an admin be prompted for a password before accessing high-level privileged CLI commands. To configure a root admin with full capability, follow these steps:

Procedure

1. Select the add icon.

2. Enter the name of the admin.
3. Create a password for this admin.
Passwords should contain at least 8 characters, including at least one number, one special character, and one uppercase character.
4. Configure the primary and secondary CAPWAP connections.
You can select an existing CAPWAP server from the drop-down list, or select the add icon to define a new server.
5. Configure a shared key passphrase for authentication.

Results

These changes have been made at the device level and override any configuration in the network policy device template. To revert back to the network policy, from the **Devices** list, select the check box for this device, and from the **Actions** drop-down, use the **Revert Device Template to Device Defaults** option.

Configure Netdump

Before You Begin

You must perform a full configuration update for each device on which you want to enable netdump.

About This Task

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:

Procedure

1. Select the check box to enable Netdump.
2. Enter the IP address of the TFTP server to where you want the device to send the core file.
3. Name the netdump file.
4. Enter the VLAN of the interface the device will use to send the netdump file to the TFTP server.
5. Enter the native VLAN of the device.
6. Select the check box to have the device bootloader use DHCP to obtain an IP address at startup.
7. Select the check box to expand this section.
8. Enter the required network settings that the bootloader must use to connect to the network.
9. Enter the IP address of the reporting device.
10. Enter the netmask for the reporting device.
11. Enter the IP address of the TFTP server.
12. Select **Save**.
13. To update the device immediately, select **Update Now**.

14. Select the type of update.
15. Select **Save as Defaults**.
16. Select **Perform Update**.

Results

The device will send a core dump file to the TFTP server the next time it reboots.

Assign an sFlow Receiver

Before You Begin

Before you can assign an sFlow receiver to a switch, you must first configure sFlow receivers as common objects. sFlow is not available for all Extreme switch models. See [Configure an sFlow Receiver](#) on page 216.

About This Task

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.

Procedure

1. Select the add icon.
2. Enable **sFlow Receiver**.
3. Enable **Interface Packet Sampling**.
4. Move interfaces you want to sample from the **Available** column to the **Selected Interfaces** column using the arrows.
5. Enable **Counter Polling**.
6. Move interfaces you want polled from the **Available** column to the **Selected Interfaces** column.
7. Select **Save**.
8. Select **Save sFlow Receivers**.

Device Level WAN Stateful Firewall

About This Task

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:

Procedure

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 be processed.
7. Select **Save**.
8. To delete firewall rules, select the check box next to the rule.
9. Select the delete icon.

Configure VRRP

Before You Begin

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

About This Task

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.

Procedure

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.

Configure SSH

Before You Begin

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.

About This Task

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 the following steps to enable SSH on a device from the device details panel, under **Configuration > Additional Settings > SSH**.

Procedure

1. 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.
2. 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.
3. 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.

Configure DHCP Server and Relay Settings

About This Task

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.

Procedure

1. Select the add icon.
2. Enter a name.
3. Enter an optional description.
4. Select the name of the DHCP server or relay agent interface from the drop-down list.
5. 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.

6. Enable or disable **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.
7. 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.
8. Select **Enable NAT Support** if this DHCP server uses NAT.
9. For **IP Pool**, define the IP address pool from which the DHCP server draws IP addresses when making assignments.
 - a. Select the add icon to add a new IP pool.
 - b. Enter the start and end IP addresses.
 - c. Select **Add**.
10. To configure each of the required parameters that the DHCP server will return to clients along with an IP address, see [Configure DHCP Server Options](#) on page 285.
11. To define custom DHCP options to provide additional network settings to connected clients, see [Configure Custom DHCP Options](#) on page 284.
12. Select **Save**.

Configure Custom DHCP Options

Before You Begin

Create or modify **DHCP server and Relay settings**.

About This Task

Use this task to define custom DHCP options to provide additional network settings to connected clients.

Procedure

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 will provide:
 - **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**.

What to Do Next

Update the device from the **Manage > Device** page.

Configure DHCP Server Options

Before You Begin

Create basic **DHCP Server and Relay settings**.

About This Task

Use this task to configure each of the required parameters that the DHCP server will return to clients, along with an IP address.

Procedure

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.
15. Enter the secondary **NTP server** IP address for DHCP client clock synchronization.
16. Enter the **Log Server** IP address for DHCP clients.

What to Do Next

Save the configuration or continue to **Custom** settings.

Configure Bonjour Gateway Settings

Before You Begin

Define Bonjour Gateway settings in the network policy.

About This Task

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.

Procedure

1. Select the **Hostname** of the device.
2. Select **Configure**.
3. 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.
4. Optionally, rename the **Realm**, or leave blank to use the existing name.
5. Select **Save**.

What to Do Next

Push a complete configuration to the BDD, followed by a **Delta** update to all other APs.

Device Details Neighbor Devices

About This Task

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.

Procedure

1. 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.

2. Select the plus sign to manually add a Layer 3 roaming or Bonjour gateway neighboring Extreme Networks device.
3. Select an available neighbor device from the drop-down menu 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.

4. Select **Save**.
5. To update the device immediately, select **Update Now**.
6. Select the type of update, and then select **Save as Defaults** to save this option as the default action.
7. To update the device immediately, select **Perform Update**.

Router URL Filtering

Before You Begin

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.

About This Task

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,

Procedure

1. Navigate 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

Before You Begin

Perform any necessary configuration changes at the device level. After you save these changes, an exclamation mark displays in the device Status column, indicating the device configuration is now out of sync with the network policy.

About This Task

Use this task to push any configuration changes made at the device level to the specific device, which will replace the exclamation mark with a green check. ExtremeCloud IQ also allows you to upgrade the device in two ways:

- Via **Manage > Devices > Update Devices** on the Devices List page
- Via **Manage > Devices > host_name > Update** on the Configure page.

Procedure

1. Select the device(s) to update in the Devices List.
2. Select **Update Devices**.
3. If on the **Configure** page, select **Update**.
4. Select **Delta Configuration Update**.
5. Select **Perform Update**.

The status icon changes from an exclamation mark to a green check.

6. 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 and Fabric Engine 8.9 installed on the Universal switches.

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.

ExtremeCloud IQ currently 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 gives you 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.

Create a Network Summary Report

About This Task

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 the following procedure to configure and generate a network summary report.

Procedure

1. Navigate to **Manage > Reports**.
2. Select the **Network Summary** tab (selected by default).
3. Select the time range options for this report.
4. Name the report.
5. To customize which data widgets appear in this report, select the checkbox to the left of a widget to include it.

You can choose to display all of them, or display them selectively. Many of them are interactive, meaning that you can hover over data to see more information. There are two views: **Access** (the default view) and the **WAN** view.

6. Select the format for this report.
7. Choose recurrence options for this report.
8. Share this report with others by entering valid email addresses in the **Share With** field.
9. Select **Generate**.

Results

ExtremeCloud IQ automatically generates this report according to your instructions and you can view it on the **My Reports** page.

Generate a PCI DSS 3.2 Report

About This Task

The 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.

Procedure

1. Select the **PCI DSS** tab.
2. Name the report.
3. Select the time range options for this report.
4. Widgets are automatically displayed in the report, but you can customize whether or not they appear.

To delete any of these widgets, select the **x** to the right of the widget name. The **x** turns into a **+**.

5. To share this report with others, enter valid email addresses in the **Share With** field.
6. Select **Generate Report**.

Results

ExtremeCloud IQ automatically generates this report according to your instructions and you can view it on the **My Reports** page.

Generate a WIPS History Report

About This Task

A WIPS history report shows you 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.

Procedure

1. Select the **WIPS History** tab.
2. Select time range options for this report.
3. Name the report.
4. Three widgets are automatically displayed in the report, but you can customize whether or not they appear.

To delete any of these widgets, select the **x** to the right of the widget name. The **x** turns into a **+**.

5. Select recurrence options for the report.

6. Share this report with others by entering valid email addresses in the **Share With** field.
7. Select **Generate**.

Results

ExtremeCloud IQ automatically generates this report according to your instructions and you can view it on the **My Reports** page.

Generate a WiFi Statistics Summary

About This Task

The WiFi Statistics Summary provides information about your wireless clients and their connections, availability through your APs, and other wireless details.

Procedure

1. Select the **WiFi Statistics Summary** tab.
2. Name the report.
3. Select the time range options for this report.
4. Share this report with others by entering valid email addresses in the **Share With** field.
5. Select **Generate**.

Results

ExtremeCloud IQ automatically generates this report according to your instructions and you can view it on the **My Reports** page.

Generate a Client Tracking Report

About This Task

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 the following procedure to configure a client tracking report.

Procedure

1. Select the **Client Tracking** tab.
2. Select the time range options for this report.
3. Name the report.
4. Select an identifier for the client.
After selected, enter a MAC address, a user name, or a host name.
5. Choose a file format for the data.
6. To share this report with others, enter valid email addresses in the **Share With** field.
7. Select **Generate**.

Results

ExtremeCloud IQ automatically generates this report according to your instructions and you can view it on **My Reports**.

Manage Users

Under **Manage > Users**, you can view details about connected users in real time or within a specified time frame.

The following sections describe the type of data related to connected users that is captured and displayed, and the actions you can take to customize your view.

View Connected Users

The Connected Users list displays these details about the 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 has been assigned, if any. You can configure user groups in the SSID portion of a network policy workflow or in **Configure > Users > 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, N/A or Never Expire is displayed.

You can take the following actions:

- Use the **Source** dropdown menu to filter information by **All** users, or by authentication type: **RADIUS**, **PPSK**, or **Others**.
- View data in **Real Time**.
- View **Historical** data, which 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.
- Select the refresh icon to refresh the data at any time.
- To see detailed information about a specific user, select the user name. For more information about the details displayed, see [View User Details](#) on page 293.
- 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 download icon to save user data as a **.csv** file named **monitoring.activeUsers**.

Related Topics

[Set the Time Frame for Captured Data Displays and Reports](#) on page 304

View User Details

Select a user name from the **Users** table to see a **Summary View** for the user, which displays 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 at any time, select the refresh icon.

Manage 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 is displayed in the table. Your 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. 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 Management

This page provides a graphical representation of event and metric alerts for a specified time range. Use **Alert Policy** to view currently configured policies and enable them, view unconfigured policies and configure them, and create brand new alert policies. For more information, see [Configure an Alert Policy](#) on page 31.

Configure an Alert Policy

About This Task

Use this task to define and configure an alert policy for reporting events and metrics.

For information about how to manage alerts, see [Alerts Management](#) on page 30.

Procedure

1. Select **Alert Policy** from the **Alert Dashboard** page.

You can now view **Configured Polices** and **Unconfigured Polices**.

- a. For **Configured Polices**, use the check boxes to enable and disable alerts in bulk or individually.
- b. Select whether you want alerts sent to an email or SMS.



Note

Before you can select SMS, you need to define a valid phone number to receive alerts. You can do so from **Global Settings**. For more information, see [Manage Account Details](#) on page 21.

- c. Use the filter option to customize the alerts displayed.
 - d. For **Unconfigured Policies**, highlight a policy, select the plus sign in the **Action** column, and proceed to **Step 2**.
2. Choose the type of alert this policy will report: **Event** or **Metric**.
 - For a **Device** event: Select **Device** events or **Security** events. For a Device event, select the type of device event to report an alert.
 - For a **Metric** event: Use the dropdown menus to define the metric.
 3. Select the **Trigger Type** for the frequency of alerts.
Specify dates and times for **Deferred** and **Repeated**.
 4. Select the type of alert to report: **Information only**, **Warning** or **Critical**.
 5. Enter an optional description.
 6. Select **Save**.
 7. The saved alert then displays in the **Configured Policies** list.
 8. Select whether to report this alert via email or SMS.

9. Enable the alert.
10. To define a brand new alert policy, select **Add New Policy** and follow **Steps 2-9**.

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 Topics

[Set the Time Frame for Captured Data Displays and Reports](#) on page 304

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 the WIPS is displayed here, but 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. 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.
- For information about how to filter the data that this table displays, see [Use the Filter Sidebar](#) on page 239. 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 [Configure Rogue AP Detection](#) on page 177.

Rogue Clients

Under **Manage > Security > Rogue Clients**, details are displayed for devices that are enabled with a wireless intrusion prevention system (WIPS) configuration that includes ad hoc network settings, and 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 is using 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. 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. You can show in-net rogues, 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.
- For information about how to filter the data in this table, see [Use the Filter Sidebar](#) on page 239. 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 and Last Time Reported:** Self explanatory.

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 Topics

[Set the Time Frame for Captured Data Displays and Reports](#) on page 304

Manage Network Applications and Application Groups

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 40.

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

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 Topics

[Search for Clients](#) on page 299

Search for Clients

[About the Issue List Table](#) on page 300

[Troubleshoot an Issue](#) on page 300

[Take Action for a Client Issue](#) on page 301

[Download Issue Lists](#) on page 301

[Set the Time Frame for Captured Data Displays and Reports](#) on page 304

Search for Clients

Before You Begin

Open a **Client Monitor** window.

About This Task

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**.

Procedure

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

Before You Begin

Open a **Client Monitor** window.

About This Task

Use this task to troubleshoot issues listed on the **Client Monitor** screen.

Procedure

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

Before You Begin

Open a **Client Monitor** window.

About This Task

You can act on client issues by escalating them, resolving them, commenting on them, and notifying other administrators about them through email.

Procedure

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

Before You Begin

Open a **Client Monitor** window.

About This Task

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.

Procedure

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.
- **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 301.

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 303.

Perform a Change Status Email Notification

Before You Begin

Run **Diagnosis** under **Manage > Tools**.

About This Task

Use this task to send an email notification when the status of an issue changes.

Procedure

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.

VPN Management

About This Task

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.

Procedure

1. Select a VPN from the list.
2. Select an option from the **Manage Keys** drop-down list.

NEW! Set the Time Frame for Captured Data Displays and Reports

Before You Begin

Navigate to any of the following UIs:


- **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**

About This Task

Use this procedure to set the time frame for displaying, or generating a report of, captured data for various network operations and events. By default, data captured is presented for a 24 hr time frame, with hourly updates. In most cases, the data captured is presented along a colored timeline in a graph. The color key for timelines and the type of data captured on a timeline is shown above the right-hand side of a graph's time frame. In some cases, data is presented in other formats, for example, in reports or in other types of graphical representation.

Procedure

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, 30, or 90 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. You can narrow the time frame using one of the following methods. The specific method available depends on the UI.
 - Click 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 and dragging it wherever you want.
3. Where the captured data is displayed in a graph along a timeline, you can view data as follows:
 - Click on a timeline to view data for a 30 minute period along the timeline. The adjusted time frame appears grey in the graph.
 - Click on a 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 Topics

[An Overview of Your Network](#) on page 239

[Device Details Monitor Functions](#) on page 268

[Create a Network Summary Report](#) on page 289

[Generate a Client Tracking Report](#) on page 291

[View Connected Users](#) on page 292

[Manage Active Alarms](#) on page 295

[Rogue APs](#) on page 295

[Rogue Clients](#) on page 297

[About Client Monitor](#) on page 298

[About Diagnosis](#) on page 302

[Network 360 Monitor Overview](#) on page 307

[About Client 360](#) on page 310



ML Insights

[Network 360 Monitor Overview](#) on page 307

[Network Scorecard](#) on page 309

[About Client 360](#) on page 310

Use **ML Insights** 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.

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 [Plan your Network](#) on page 240). 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.

- Because data is collected on an hourly basis, this window might be empty for up to one hour. Select **Where's My Data?** for more information.
- For large networks with multiple locations, enter the first few characters of the location name in the type-ahead **Search Maps** field to automatically bring up matching items. As you enter more characters, the search results become more precise.
- Use the **Filter** section to manage the data that is displayed. When a filter is applied, the filter icon contains a circle in the lower right corner.

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:** 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 carat icon at the bottom of a widget, you can expand it for more information.
- **Client:** Displays overall and wireless health scores, bandwidth usage, issues, channel distribution, supported spatial streams, maximum client capability in the 2.4 and 5 GHz bands, association and probe requests, 802.1x technology, transmit power, and more.
- **WiFi Health:** Displays usage, clients, and the overall WiFi 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.
- **Applications 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 60.

Related Topics

[Set the Time Frame for Captured Data Displays and Reports](#) on page 304

Network 360 Monitor - Device View

The **Network 360 Monitor Device** view displays your network hierarchy, shown in outline form in the left nav 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.
- **Device Trail over Time:** Create a device trail to track Bluetooth devices roaming on a floor over a period of time. Select a Bluetooth device, a time period, and a speed from the drop-down lists.
- **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.

Network 360 Monitor - 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.
- **Device Trail over Time:** To create a device trail to track Bluetooth devices roaming on a floor between zones over a period of time, select a device, a time period, and a speed from the drop-down lists.
- **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.

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. The scorecards are described below. Scores display for a selected location if you use the locations filter.

- **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.

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 that is displayed in this window. 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.

Select the **Refresh** icon to refresh table data, the **Download** icon to download data in multiple formats, and the **Column Picker** 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.

Alias for active clients. 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.

For inactive clients (the Inactive tab), a timeline enables you to change the time range for which captured client data is displayed.

By default, ten clients are displayed per window. Change the number of clients displayed at the bottom left corner of the table. The clients list allows you to display and select many entries at a time, which can be useful for large-batch operations.

Related Topics

[Client Alias](#) on page 310


[Set the Time Frame for Captured Data Displays and Reports](#) on page 304

NEW 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.



Essentials

[ExtremelOT Essentials in ExtremeCloud IQ](#) on page 312

[Extreme AirDefense Essentials in ExtremeCloud IQ](#) on page 313

[ExtremeGuest Essentials in ExtremeCloud IQ](#) on page 314

[ExtremeLocation Essentials in ExtremeCloud IQ](#) on page 315

Use **Essentials** to access the following Essentials Applications in ExtremeCloud™ IQ:

- ExtremelOT Essentials
- Extreme AirDefense Essentials
- ExtremeGuest Essentials
- ExtremeLocation Essentials

NEW! [ExtremelOT Essentials in ExtremeCloud IQ](#)


ExtremelOT™ Essentials provides security management with a simplified configuration workflow, plus traffic and application visibility of connected end devices. ExtremelOT Essentials also enables 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. However, 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 ExtremIoT Essentials functionality is dependent on your ExtremeCloud IQ user access level.

**Note**

ExtremIoT Essentials functionality also requires an ExtremeCloud™ IQ Pilot license.

The following options are available from the **ExtremIoT 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 ExtremIoT 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.

NEW! [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.

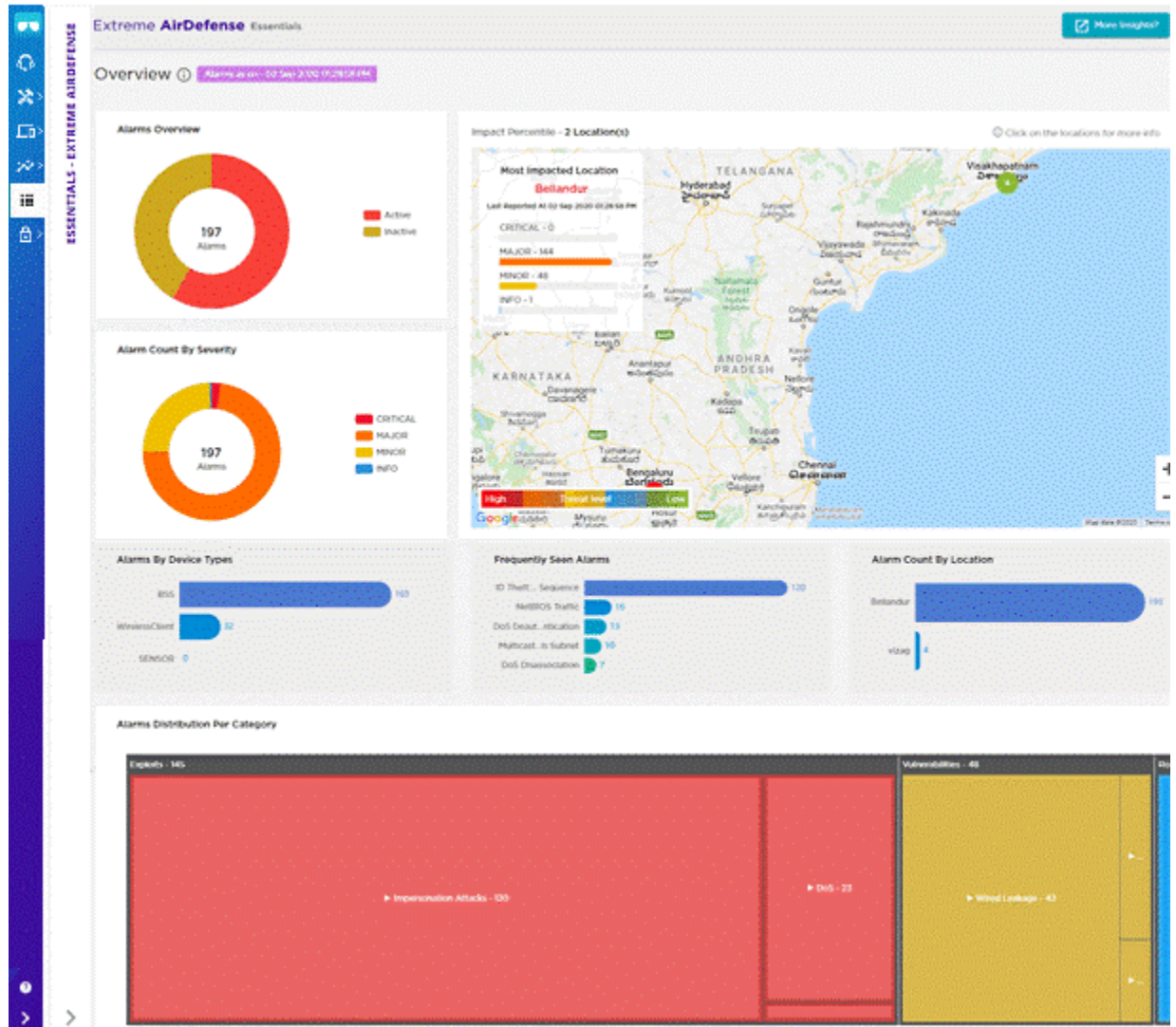


Figure 1: Extreme AirDefense Essentials Overview View in ExtremeCloud IQ

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.


NEW! 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.

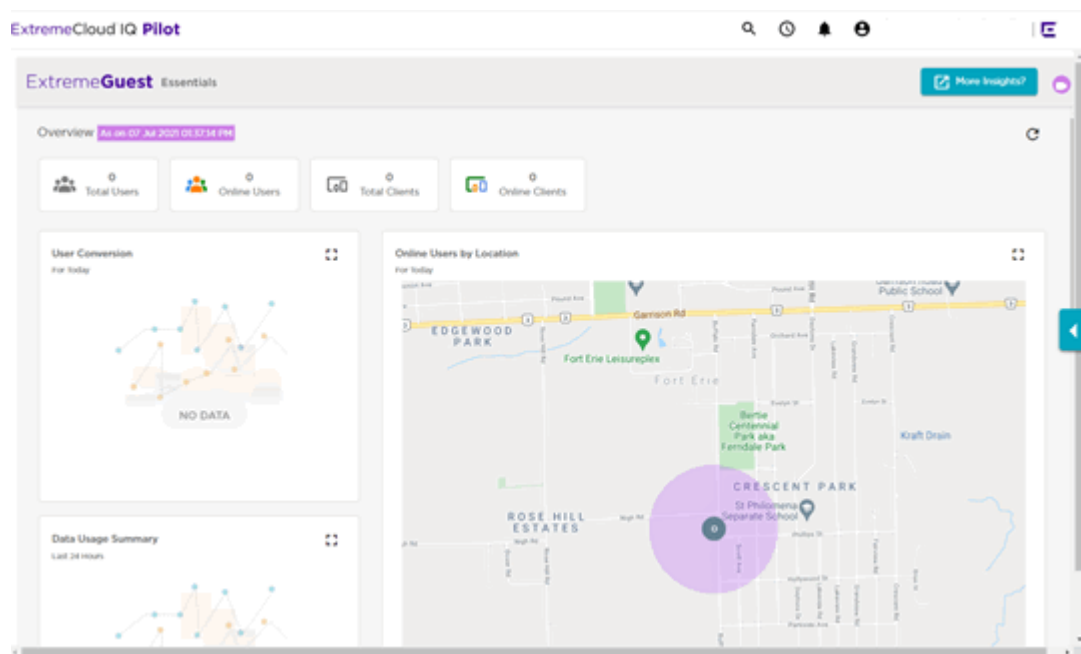


Figure 2: ExtremeGuest Essentials Overview View in ExtremeCloud IQ

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.


NEW! 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 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:

- real-time and historical location analysis
- new and repeat visitor tracking
- engagement time monitoring
- site or zone specific intelligence
- assets and employee tracking

You can use the ExtremeCloud IQ Dashboard Essentials  > icon to list the Essentials applications and choose ExtremeLocation Essentials. The ExtremeLocation Essentials Overview launches in ExtremeCloud IQ.

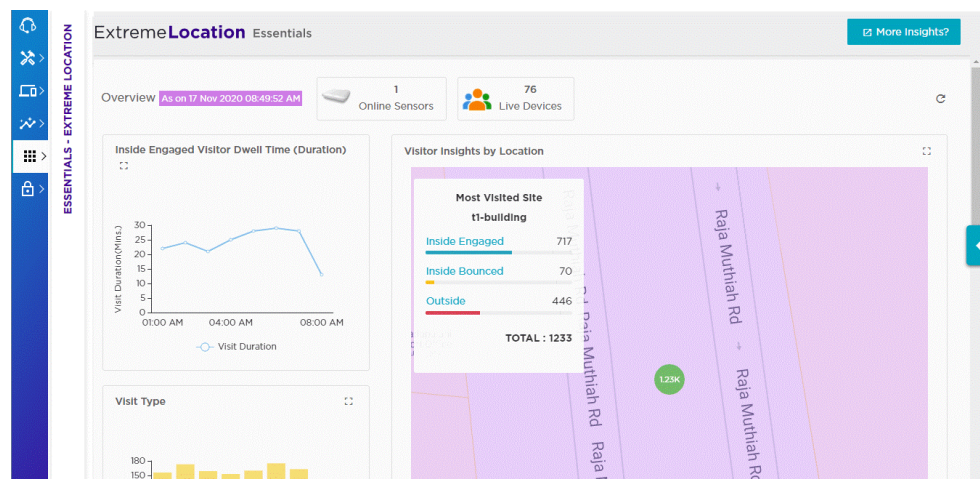


Figure 3: ExtremeLocation Essentials Overview View in ExtremeCloud IQ

You can select the **More Insights** button at the top right corner of the Overview to access all the features of ExtremeLocation Essentials and open the application in a separate browser tab.



CoPilot Dashboard

- [CoPilot Widget Tools](#) on page 318
- [CoPilot Adverse Traffic Patterns Widget](#) on page 319
- [The CoPilot DFS Recurrence Widget](#) on page 319
- [CoPilot PoE Stability Widget](#) on page 320
- [CoPilot Port Efficiency Widget](#) on page 321
- [CoPilot Wi-Fi Capacity Widget](#) on page 321
- [Submit a Support Ticket](#) on page 321
- [Wireless Connectivity Experience Widget](#) on page 322
- [Wired Connectivity Experience](#) on page 323

Your ExtremeCloud IQ CoPilot subscription provides visibility and insight through a dashboard that is available via a separate tab in the left navigation panel of ExtremeCloud IQ. This dashboard displays a number of data widgets that contain in-depth information about alerts and anomalies that are present in your network. Use this information to troubleshoot and address issues, and enhance network performance.

Many of the dashboard widgets are interactive. Hover over or select numbers, graph lines, icons, and buttons for more details, use drop-down lists to sort or refine data, edit the dashboard display to add or delete widgets, or refresh the data at any time. The various widgets are described below.

- **Widget Tools:** Each widget contains multiple tools that help you address issues. See more information [here](#).
- **Account Summary:** Provides details specific to this account, such as date initiated, location, primary admin, and VIQ name and ID.
- **Adverse Traffic Patterns:** Displays anomalies caused by TX and RX traffic loads that result in high resource use of multicast and broadcast communications. See more information [here](#).
- **Assurance Scans:** Shows a timeline of when ExtremeCloud IQ Pilot analyzed data coming from a managed device, and identifies when and how many anomalies were discovered. Hover over any bar in the timeline to see more details.
- **Device Uptime:** Shows a timeline of how many of all managed devices were connected (online) or disconnected (offline) to ExtremeCloud IQ.
- **Device by OS:** Displays an inventory of devices by operating system.
- **Devices by Type:** Displays an inventory of devices by type.
- **DFS Recurrence:** Displays anomalies related to radar-influenced channel changes. See more information [here](#).

- **ExtremeCloud IQ Applications:** Shows the **ExtremeCloud IQ Essentials** and other applications that are enabled for this account.
- **Licenses:** Displays the number of used and available licenses for **ExtremeCloud IQ CoPilot**, **ExtremeCloud IQ Pilot**, (for APs and switches), and **Navigator** (for WiNG devices). Select **Manage** to see more details. To return to the dashboard from the **Licensing** window, select the headphones icon.
- **PoE Stability:** Displays anomalies related to PoE flapping and sudden changes in power draw. See more information [here](#).
- **Port Efficiency:** Identifies wired and wireless device interfaces that are not making efficient use of their uplink backhaul connection. See more information [here](#).
- **Usage:** Shows a timeline of client data usage. Hover over any portion of the timeline to see more details.
- **WiFi Capacity:** Displays anomalies related to AP capacity and airtime usage. See more information [here](#).
- **Submit a Support Ticket:** Triggers an ExtremeCloud IQ support ticket. See more information [here](#).
- **Wireless Connectivity Experience:** Displays information in the form of a data quality index. See more information [here](#).
- **Wired Connectivity Experience:** Displays information about connectivity for wired devices, such as switches. See more information [here](#).

CoPilot Widget Tools

The following tools are available in the information box for each anomaly.

Tool Tips: Hover over any black circle with a white "i" for an explanatory tool tip.

Sort: Widget data can be sorted by location, anomaly severity, and most recent occurrence.

Learn More: Select the camera icon to watch videos that explain more about the widget.

Pin: Select the pushpin icon to pin an anomaly to the top of the anomalies list.

Mute or Delete: Select ... to mute or delete an anomaly. This can be helpful by letting you delete recurring anomalies for which there is no action, or about which you are not concerned.

Hide Muted Anomalies: Select **Hide Muted** at the bottom of the widget to hide all recurring muted anomalies.

Anomaly details: Select anywhere inside a widget anomaly pane to see more details about that anomaly, including recommended remedial actions. You can make the following selections from inside the details panel:

- Select the down arrow to see more information about a specific anomaly, including recommended remedial actions.
- Select the pushpin icon to pin this anomaly to the top of the list of anomalies.

- Select the thumbs-up icon if this information was helpful and the thumbs-down icon if it was not. Your responses here will be analyzed and used to improve this information in future product releases.

Select the **Need Help** button if the suggested remedies do not correct an anomaly. Follow the instructions to have ExtremeCloud IQ generate a support ticket.

CoPilot Adverse Traffic Patterns Widget

This widget displays anomalies caused by TX and RX traffic loads that result in high resource use of multicast and broadcast communications. 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 overtake the available CPU capacity, which can increase latency and packet loss and might even bring a device down. The CPU threshold for APs is 90%. The CPU threshold for switches is 50%. The following data is displayed for active devices:

- Maximum and average CPU usage over time for wired and wireless devices.
- TX and RX unicast, multicast, and broadcast byte counts over time for backhaul interfaces on wired and wireless devices.



Note

Multicast information is not available for wireless devices, since they use unicast or broadcast only.

The CoPilot DFS Recurrence Widget

DFS Recurrence This widget displays anomalies related to radar-influenced channel changes. When an access point switches channels, the quality of service for connected clients can decrease temporarily, while repeated channel changes can 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. This allows the AP to continue to use DFS channels that are not affected by radar. If ExtremeCloud IQ determines that the entire range of DFS channels is affected, it is recommended that users completely disable DFS for the affected AP. The severity of a DFS anomaly is classified as: 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.

DFS Recurrence This widget displays anomalies related to radar-influenced channel changes. When an access point switches channels, the quality of service for connected clients can decrease temporarily, while repeated channel changes can 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. This allows the AP to continue to use DFS channels that are not affected by radar. If ExtremeCloud IQ determines that the entire range of DFS channels is affected, it is recommended that users completely disable DFS for the affected AP.

The severity of a DFS anomaly is classified as:

- 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.

CoPilot PoE Stability Widget

This widget displays anomalies related to PoE flapping and sudden changes in power draw. Data is presented over a period of 24 hours, and includes date and time details.

APs commonly receive power through an Ethernet backhaul cable connection to an upstream switch. This is known as Power over Ethernet or PoE. When an AP first boots, it selects a power mode based on the available PoE protocols (it can start with PoE and move to PoE+ after a brief interval) and uses this power mode until it reboots.

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 can all cause APs to cycle through power modes, while never reaching a steady state. The PoE Stability widget displays information about this situation using the following models:

- **Normal:** Normal: Indicates a small number of flips, with the vast majority of time spent in a single PoE mode.
- **Anomalous:** Abnormally large number of flips, normal amount (i.e. vast majority) of time spent in a single PoE mode is the least client-impacting form of anomaly: while there are many flips, the AP spends the vast majority of time in one state (i.e. there is stable behavior over time).
- **Anomalous:** A normal (i.e. small) number of flips, but an abnormally large amount of time spent in both PoE modes during the flips. This can have an impact because while the AP flips between modes relatively rarely, it is capable of PoE+ but instead spends significant amounts of time operating at the lower-rated PoE.
- **Anomalous:** An abnormally large number of flips, abnormally large amount of time spent in both PoE modes. The AP regularly flips between modes while also spending a significant amount of time in the suboptimal mode. Spending a significant amount of time in the suboptimal mode alone is not an anomaly: if the AP operates on the lower spec PoE mode most of time but is stable in terms of flips, this is normal behavior.

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.

CoPilot Port Efficiency Widget

This widget identifies wired and wireless device interfaces that are not making efficient use of their uplink backhaul connection. This can happen in a number of ways:

- An interface might only use half-duplex communication, that is, just 50% of the available throughput capacity.
- An interface can 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, and 2500 Mbps. Data rates of 10 Mbps or 100 Mbps are considered inefficient. 1000 Mbps and 2500 Mbps usage 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.

CoPilot Wi-Fi Capacity Widget

This widget displays anomalies related to 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 devices (APs). Information reported in this widget includes:

- Total time that a channel was in use.
- Total time that 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 RDC from which the data was obtained.

Submit a Support Ticket

Configure ExtremeCloud IQ to 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 show tech output 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.

Wireless Connectivity Experience Widget

This widget displays information in the form of a data quality index. You can display data for a specified number of locations, (the Show drop-down) for SSIDs, or client types (the View-by drop-down). Many parts of the widget contents are interactive. Hover to see more details.

The quality index scores client connectivity experiences from 1 (worst) to 10 (best). In an ideal scenario, the quality index should be 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 following tools are available in the quality index:

- Select the = or down arrow symbols next to the rating to see a comparison to the rating 24 hours previous. The = symbol means the rating is the same, and the up and down arrows indicate that the rating has dropped or climbed compared to 24 hours previously. In the timeline, the data displayed at the left edge of the timeline are from the previous 24 hours. The data displayed at the right edge of the timeline is the most current.
- Select inside the widget, either over the location, SSID, or client type, or directly inside the timeline chart to see a Connectivity Details panel. In this panel, drop-down lists let you view different locations. Use the type-ahead search field to search for locations. You can change the time view from one hour up to the last 90 days. Hover over the timeline for even more information about connections, including time to associate, time to authenticate, total number of unique clients, and the number of clients above the threshold, if you are viewing for the last seven days or less.
- Select the timestamp to drill down for details about specific events and clients. In the details panel, use the time window button on the left to display data for a 10 minute or one hour period for anything you select on the timeline. The details table has a search field, and any table header with an arrow can be sorted. Select the client MAC address to see the Client 360 view.
- In the Connectivity Experience panel, if you view by location, there are no other filter options. If you view by SSID or client type, you can filter by location using the filter icon in the right top corner.
- The Aggregated Quality Index in this panel displays data for the times and filters selected. The Time to Connect section displays the quality index by time to associate and time to authenticate. All timelines in this panel are synchronized. To zoom in to details on a timeline, drag and select across the timeline. Select again, or deselect to return to the normal view.

Thresholds: The global threshold is dynamically calculated base on information from all clients in the Regional Data Center. The local threshold is dynamically calculated per location and SSID type (PSK vs Open vs Enterprise), and the lower threshold is used.

Wired Connectivity Experience

This widget displays information about connectivity for wired devices, such as switches. Data is reported for each unit of hardware, even for stacked switches. The actions and options are similar to the Wireless Connectivity widget. For wired deices, you can only view by location. In this widget, the details panel is labeled Hardware and displays port errors.

Assurance Scans: This timeline shows when ExtremeCloud IQ analyzed data coming from a managed device, and identifies when and how many anomalies were discovered. Hover over any bar in the timeline to see more details.

Licenses: Displays the number of used and available licenses for ExtremeCloud IQ CoPilot, ExtremeCloud IQ Pilot (for APs and switches) and Navigator (WiNG devices). Select Manage to go the licensing window. Select the headphones icon to return to the ExtremeCloud IQ CoPilot dashboard from the Licensing window.: Displays the number of used and available licenses for ExtremeCloud IQ, (for APs and switches) and Navigator (WiNG devices). Select **Manage** to go the licensing window. Select the headphones icon to return to the dashboard from the Licensing window.

Wi-Fi Efficiency:Displays anomalies related to wireless communication between clients and APs. You can sort the data by location, severity, and most recent occurrence. This widget presents packet data anomalies and information about them.

Wi-Fi Capacity: Displays anomalies related to 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's connection duration and the channel utilization information related to wireless devices (APs). Information reported in this widget includes:

- Total time that a channel was in use.
- Total time that peak usage for the channel was 80% or higher.
- The total number of peak intervals and non-peak intervals (80% and 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 RDC from which the data was obtained.