ExtremeCloud IQ Controller User Guide

Version 10.06.01

9037871-00 Rev AA
June 2023

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/

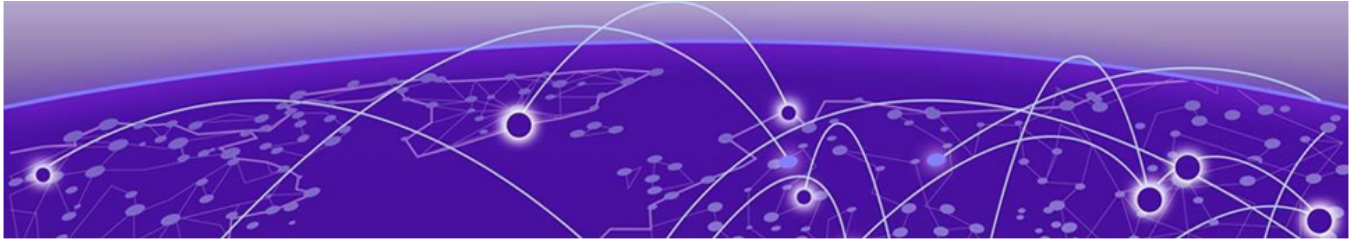


Table of Contents

Preface

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

Table 3: Command syntax

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

Table 3: Command syntax (continued)

Convention	Description
...	Repeat the previous element, for example, *member*[*member*...].
\	In command examples, the backslash indicates a “soft” line break. When a backslash separates two lines of a command input, enter the entire command at the prompt without the backslash.

Documentation and Training

Find Extreme Networks product information at the following locations:

Current Product Documentation
Release Notes
Hardware and software compatibility for Extreme Networks products
Extreme Optics Compatibility
Other resources such as 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

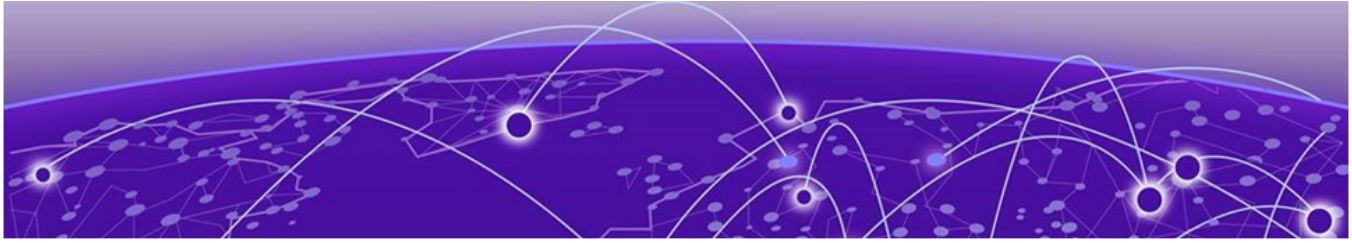
You can subscribe to email notifications for product and software release announcements, Field Notices, and Vulnerability Notices.

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 Controller supported access point models and appliances, refer to the appropriate *Installation Guide*.



Welcome to ExtremeCloud IQ Controller

Extreme Campus Controller has been branded ExtremeCloud IQ Controller. ExtremeCloud IQ Controller supports Campus/Centralized sites only.

ExtremeCloud IQ Controller offers a streamlined customer experience with a common platform and operating system across multiple Extreme Networks products. Get the power of ExtremeWireless and ExtremeCloud IQ - Site Engine in one easy-to-use platform. ExtremeCloud IQ Controller offers the following features:

- Integrated Access Control
- Integrated Maps
- Historical data charts
- Programmable REST API
- On-premise standalone deployment with integration into ExtremeCloud™ IQ, ExtremeCloud™ IQ - Site Engine, ExtremeCloud™ A3, and on-premise services.

Note
The SSH/CLI interface of ExtremeCloud IQ Controller is intended for diagnostics and internal use only. This interface is not supported for system configurations. All configuration is to be executed using the provided user interface or through the available and documented REST API. For more information about the REST API documentation, see *ExtremeCloud IQ Controller documentation*.

The Appliance

The appliance is a network device designed to integrate with an existing wired Local Area Network (LAN). The ExtremeCloud IQ Controller provides centralized management, network access, and routing to wireless devices that use Wireless APs to access the network.

The appliance provides the following functionality:

- Controls and configures wireless APs, providing centralized management.
- Authenticates wireless devices that contact a wireless AP.
- Assigns each wireless device to a network service when it connects.
- Routes traffic from wireless devices, using a network service, to the wired network.
- Applies filtering roles to the wireless device session.
- Provides session logging and accounting capability.
- Manages switches.

ExtremeCloud IQ Controller supports the use of both a virtual appliance and a physical appliance.

Related Topics

Appliance Product Family on page 13

Appliance Product Family

ExtremeCloud IQ Controller supports the following virtual appliances:

- VMWare:
  - VE6120
  - VE6125
- KVM
  - VE6120K
  - VE6125K
- Microsoft Hyper-V
  - VE6120H

And the following hardware appliances:

- E1120
- E2120
- E2122
- E3120
- E3125

  ExtremeCloud IQ Controller v10.06.01 introduces a new E3125 hardware platform, variation of the E3120 that offers 100G per second.

Wireless AP Overview

Extreme Networks APs use the 802.11 wireless standards (802.11a/b/g/n/ac/ax) for network communications, and bridge network traffic to an Ethernet LAN. In addition to the wireless APs that run proprietary software and communicate with an appliance only, Extreme Networks offers cloud-enabled APs.

The following ExtremeWireless™ access points are supported by ExtremeCloud IQ Controller. For more information about the Universal APs, see Universal AP Operational Modes on page 24.

Table 4: Supported Access Point Models

AP Class	Supported Access Points
Wi-Fi 6E Universal World-Wide APs ExtremeCloud IQ or on-premise operation	• AP3000/X • AP4000 • AP4000-1 • AP5010 • AP5050U/AP5050D
Wi-Fi 6 Universal APs ExtremeCloud IQ or on-premise operation	• AP302W • AP305C/CX • AP305C-1 • AP410C • AP410C-1 • AP460C/S6C/S12C
Wi-Fi 6 on-premise operation only	• AP460i/e • AP410i/e • AP410i-1 • AP505i • AP510i/e • AP510i-1 • AP560i/h/m/t/u
Wi-Fi 5 on-premise operation only **Note:** AP3900 series requires a minimum firmware revision of 10.41.01 (or later) for onboarding into ExtremeCloud IQ Controller. Customers migrating from ExtremeWireless installations or onboarding new AP3900 inventory to ExtremeCloud IQ Controller must ensure APs are running at least the minimum revision prior to onboarding. Depending on the age of the inventory, this may require a manual upgrade of the unit firmware outside of the management framework.	• AP3917i/e/k • AP3916ic • AP3915i/e • AP3912i • AP3935i/e • AP3965i/e

The Extreme Networks® Defender Adapter SA201 is supported.

A wireless AP physically connects to a LAN infrastructure and establishes an IP connection to ExtremeCloud IQ Controller, which manages the AP configuration through the Wireless Assistant. The appliance provides centralized management (verification and upgrade) of the AP firmware image.

A UDP-based protocol enables communication between an AP and ExtremeCloud IQ Controller. The UDP-based protocol encapsulates IP traffic from the AP and directs it to the appliance. The appliance decapsulates the packets and encrypts (IPsec)[Default AP and appliance communication] and routes them to the appropriate destinations, while managing sessions and applying roles.

Note
For higher transmission rates, by default, multicast is converted to unicast for all Wi-Fi 6 access points discovered by ExtremeCloud IQ Controller.
There is a maximum client threshold of 64 clients. Above 64 clients, the AP defaults to broadcasting on a DTIM interval.

Related Topics

Support for World-Wide Universal Access Points with Wi-Fi 6E Technology on page 15
Universal AP Operational Modes on page 24
Support for ExtremeWireless AP3xx Access Points on page 79
Support for ExtremeWireless AP4xx Access Points on page 80
Support for ExtremeWireless AP5xx Access Points on page 81

Support for World-Wide Universal Access Points with Wi-Fi 6E Technology

The World-Wide Universal Access Points are high-performance 802.11ax 6 GHz tri-band access points designed for high-density, indoor environments. They operate simultaneously across the 6 GHz, 5 GHz, and 2.4 GHz bands, offering full 6 GHz WLAN service and sensor capability. They can be deployed with ExtremeCloud IQ Controller or ExtremeCloud IQ:

- AP3000/X
- AP4000
- AP4000-1
- AP5010
- AP5050U/AP5050D

Related Topics

World-Wide Universal Access Points Compliance Regions on page 16
AP3000 Series Radios and 6 GHz Support on page 16
AP4000/AP4000-1 Radios and 6 GHz Support on page 18
AP5000 Series Radios and 6 GHz Support on page 19
6 GHz Channel Allocation and Notation on page 23
Universal AP Operational Modes on page 24
Understand Radio Mode on page 147

Radio as a Sensor on page 152
WLAN Service Settings on page 250

World-Wide Universal Access Points Compliance Regions

The compliance region for the World-Wide Universal Access Points is determined upon cloud discovery. Cloud discovery is required. When the AP discovers the cloud, it adopts the regulatory and compliance specifications of the domain region. When you manually add an AP to ExtremeCloud IQ Controller, the region is automatically determined in reference to the country of operation defined for the site. This is the defined region for on-premise adoption. If necessary, the region is automatically redefined upon cloud discovery.

In ExtremeCloud IQ Controller, the compliance region is defined at the site level. If the compliance region changes after cloud adoption, the AP automatically changes sites, joining a site defined for the new region. If there is no site definition for the new region, the AP has the status *In-Service Trouble*. The device has discovered ExtremeCloud IQ Controller but it is not a member of a device group.

Related Topics

AP4000/AP4000-1 Radios and 6 GHz Support on page 18
Support for World-Wide Universal Access Points with Wi-Fi 6E Technology on page 15
6 GHz Channel Allocation and Notation on page 23

NEW! AP3000 Series Radios and 6 GHz Support

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

- AP3000 — Indoor access point
- AP3000X — Indoor access point with optional external antenna.

The AP3000 series access points offer two radios in three modes:

Table 5: AP3000/X Operating Modes

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

- Radio 1:
  - sensor
  - b/g
  - g/n
  - b/g/n

  - g/n/ax (Default)
  - client-bridge
  - ax6
- Radio 2:
  - sensor
  - a/n/ac
  - a/n/ac/ax (Default)
  - client-bridge

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

Note
The World-Wide Universal Access Points 6 GHz radios support only the following 6E WFA Compliant network authentication methods:

- OWE (Opportunistic Wireless Encryption) for Open Networks
- WPA3-Personal (SAE/H2E)
- WPA3-Enterprise
- WPA3-Enterprise 192-bit mode
- WPA3-Compatibility

Note
WPA3-Compatibility is *not* WFA compliant. WPA3-Compatibility supports both WPA2 Personal and WPA3 Personal on the same network. If a WPA3-Compatibility network is assigned to 6 GHz radio, only WPA3 Personal is assigned, thus making the network compliant.

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

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

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

Related Topics

AP3000X Professional Install Settings on page 238

AP4000/AP4000-1 Radios and 6 GHz Support

The AP4000/AP4000-1 access points offer three radios:

- Radio 1 — 2x2 WLAN Service 2.4 GHz

  Radio modes:
  - b/g
  - g/n
  - b/g/n
  - g/n/ax
  - client-bridge
- Radio 2 — 2x2 WLAN Service 5.0 GHz

  Radio modes:
  - a/n/ac
  - a/n/ac/ax
  - client-bridge
- Radio 3 —
  - 2x2 WLAN Service 6.0 GHz, Or
  - 2x2 WLAN Tri-Band Sensor, 2.4 GHz, 5.0 GHz, 6.0 GHz

  Radio modes:
  - sensor
  - ax6
  - client-bridge

AP4000/AP4000-1 access points support the following:

- IEEE 802.11ax Orthogonal Frequency-Division Multiple Access (OFDMA) multi-user access.
- Out of Band discovery on the 6 GHz band. APs that provide WLAN service on the 6 GHz band include Reduced Neighbor Report IE in all 2.4 GHz and 5 GHz beacons and probe responses. Out of Band discovery helps clients find 6 GHz SSIDs and channel information that comes from 2.4 GHz and 5 GHz beacons of co-located access points.
- Supports AirDefense Services Platform (ADSP) on 2.4 GHz, 5 GHz, and 6 GHz radios.
- 6E WFA Compliant network authentication methods.

  The World-Wide Universal Access Points 6 GHz radios support only the following 6E WFA Compliant network authentication methods:
  - OWE (Opportunistic Wireless Encryption) for Open Networks
  - WPA3-Personal (SAE/H2E)
  - WPA3-Enterprise

- WPA3-Enterprise 192-bit mode
- WPA3-Compatibility

Note
WPA3-Compatibility is *not* WFA compliant. WPA3-Compatibility supports both WPA2 Personal and WPA3 Personal on the same network. If a WPA3-Compatibility network is assigned to 6 GHz radio, only WPA3 Personal is assigned, thus making the network compliant.

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

Note
AP*model*-1 access point models do not support IoT.

Related Topics

Support for World-Wide Universal Access Points with Wi-Fi 6E Technology on page 15
World-Wide Universal Access Points Compliance Regions on page 16
6 GHz Channel Allocation and Notation on page 23

AP5000 Series Radios and 6 GHz Support

The AP5000 series access points are Wi-Fi 6E tri-radio access points with support for multiple Extreme Networks operating systems. The AP5000 series access points include the following AP models:

- AP5010 — Indoor access point
- AP5050U — Indoor/Outdoor, underseat access point
- AP5050D — Indoor/Outdoor AP with selectable narrow and wide angle built in directional antennas.

The AP5050U/D has an Environment choice of **Indoor**, **Outdoor**, or **Outdoor — Under Seat**, depending on the installation location.

Support for 6 GHz (Wi-Fi 6E) radio (Indoor) operation is dependent on the compliance region. Support for 6 GHz (Wi-Fi 6E) radio (Outdoor) operation is currently not supported.

Table 6 outlines the current radio support per compliance region for the AP5050U/D. Support for 6 GHz (Wi-Fi 6E) (Outdoor) operation will be enabled in a future release.

Table 6: Radio support for AP5050U/D per compliance region

AP Model	Indoor 2.4GHz	Indoor 5GHz	Indoor 6GHz	Outdoor 2.4GHz	Outdoor 5GHz	Outdoor 6GHz
AP5050U-FCC	Yes	Yes	No	Yes	Yes	No
AP5050D-FCC	Yes	Yes	No	Yes	Yes	No

Table 6: Radio support for AP5050U/D per compliance region (continued)

AP Model	Indoor 2.4GHz	Indoor 5GHz	Indoor 6GHz	Outdoor 2.4GHz	Outdoor 5GHz	Outdoor 6GHz
AP5050U-CAN	Yes	Yes	No	Yes	Yes	No
AP5050D-CAN	Yes	Yes	No	Yes	Yes	No
AP5050U-WR	Yes	Yes	Yes	Yes	Yes	No
AP5050D-WR	Yes	Yes	Yes	Yes	Yes	No

The AP5000 Series access points offer three radios:

- Radio 1 —
  - 4x4 WLAN Service 2.4 GHz, Or
  - 2x2 WLAN Tri-Band Sensor, 2.4 GHz, 5.0 GHz, 6.0 GHz

  Radio modes:
  - sensor
  - b/g
  - g/n
  - b/g/n
  - g/n/ax
  - client-bridge
- Radio 2 — 4x4 WLAN Service 5.0 GHz

  Radio modes:
  - a/n/ac
  - a/n/ac/ax
  - client-bridge
- Radio 3 — 4x4 WLAN Service 6.0 GHz

  Radio modes:
  - ax6
  - client-bridge

AP5000 series access points support the following:

- IEEE 802.11ax Orthogonal Frequency-Division Multiple Access (OFDMA) multi-user access.
- Out of Band discovery on the 6 GHz band. APs that provide WLAN service on the 6 GHz band include Reduced Neighbor Report IE in all 2.4 GHz and 5 GHz beacons and probe responses. Out of Band discovery helps clients find 6 GHz SSIDs and channel information that comes from 2.4 GHz and 5 GHz beacons of co-located access points.

- Supports AirDefense Services Platform (ADSP) on radio 1 (3 bands) when 2x2 WLAN Tri-Band Sensor 2.4 GHz, 5.0 GHz, 6.0 GHz is selected on radio 1.
- 6E WFA Compliant network authentication methods.

Note
The World-Wide Universal Access Points 6 GHz radios support only the following 6E WFA Compliant network authentication methods:

- OWE (Opportunistic Wireless Encryption) for Open Networks
- WPA3-Personal (SAE/H2E)
- WPA3-Enterprise
- WPA3-Enterprise 192-bit mode
- WPA3-Compatibility

Note
WPA3-Compatibility is *not* WFA compliant. WPA3-Compatibility supports both WPA2 Personal and WPA3 Personal on the same network. If a WPA3-Compatibility network is assigned to 6 GHz radio, only WPA3 Personal is assigned, thus making the network compliant.

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

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

Related Topics

AP5000 Series Power Management on page 21
Privacy Settings WPA3 on page 255

AP5000 Series Power Management

AP5000 Series Power Consumption Widget

ExtremeCloud IQ Controller offers a power consumption widget for the AP5000 series access points. This widget offers a visual display of the power consumption for the AP over the display period.

To access the Power Consumption widget:

1. Go to **Monitor** > **Devices** > **Access Points**.
2. Select an AP5010 or AP5050 access point from the **Access Points List**.

3. To edit the AP dashboard, select .
4. Select **Widgets** > **Power** > **Power Consumption**.
5. Drag the Power Consumption widget icon onto the dashboard.

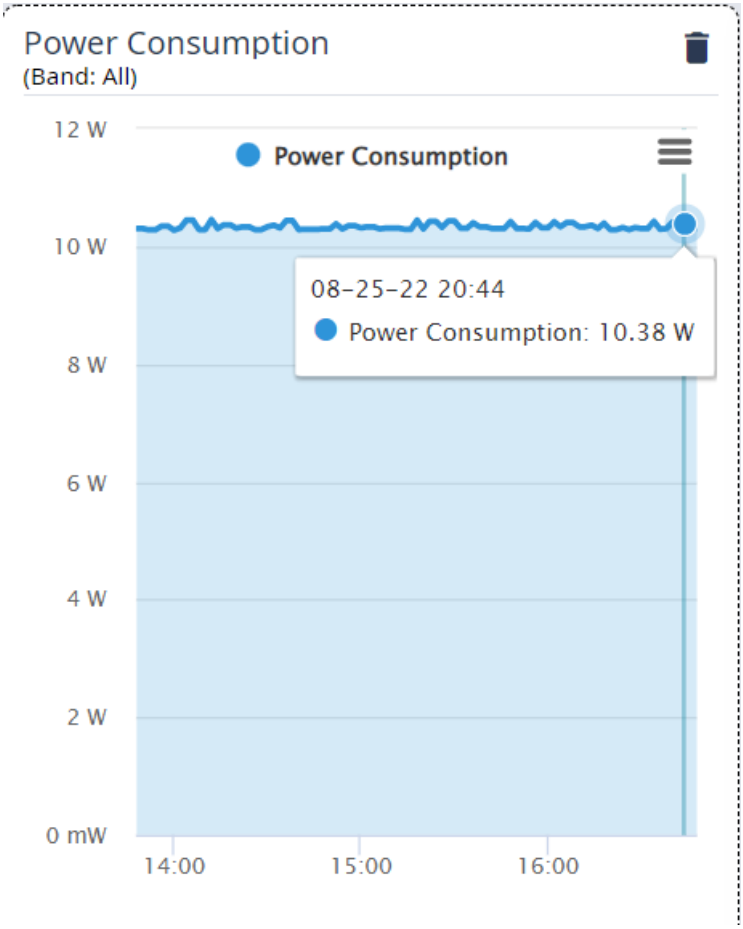


Figure 1: AP5010 Power Consumption Widget

AP5010 Power Source Feature Restrictions

Depending on the power source that is reported to ExtremeCloud IQ Controller, the AP5010 has the following restrictions.

Table 7: AP5010 feature restrictions related to the power source provided to the AP

Power Status	High	Normal	Low	Normal
Power Source	802.3BT	802.3AT	802.3AF	Power Supply
PSE= OFF	OFF	OFF	OFF All 3 Radios operate 2x2 Maximum Tx 10 dBm	OFF
PSE=Auto	ON	OFF	OFF	OFF

Table 7: AP5010 feature restrictions related to the power source provided to the AP (continued)

Power Status	High	Normal	Low	Normal
Power Source	802.3BT	802.3AT	802.3AF	Power Supply
USB=OFF	OFF	OFF	OFF	
USB=Auto	ON	ON All 3 Radios operate 3x3	OFF	ON All 3 Radios operate 4x4

AP5050 Power Source Information

The AP5050U and AP5050D access points do not include a USB port or an external power supply. These outdoor access points operate on standard power.

Table 8: AP5050 power source provided to the AP

Power Status	High	Normal
Power Source	802.3BT	802.3AT
PSE= OFF	OFF	OFF
PSE=Auto	ON	OFF

Related Topics

AP Feature Restrictions in Low Power Mode on page 218

6 GHz Channel Allocation and Notation

Because numerous channels are offered on the 6 GHz band, it is a best practice to configure the Preferred Scanning Channel (PSC) so that the amount of probing is kept to a minimum. Preferred channels function as primary channels at each channel width: 20, 40, 80, and 160 MHz.

Note
All channels on the 6 GHz band are supported when 20 MHz and 40 MHz are used. It is a best practice to configure Preferred Scanning Channels for faster scanning.

Example: 6 GHz channel notation `47e/160`

- 47 — Selected channel
- e — Represents 6E (6 GHz band). Differentiates 6 GHz overlapping channel numbers with bands 2.4 GHz and 5 GHz.
- /160 — Channel bonded to 160 MHz

Related Topics

Understanding Smart RF and Channel Width on page 183
Configuring a Channel Plan on page 184
Channel Select Dialog on page 216

Universal AP Operational Modes

The following Wi-Fi 6 access points can operate in either ExtremeCloud™ IQ or in an on-premise environment — one configured operating mode at a time:

- AP3000/X
- AP302W
- AP305C/CX
- AP305C-1
- AP4000
- AP4000-1
- AP410C
- AP410C-1
- AP460C/S6C/S12C
- AP5010
- AP5050U/AP5050D

Note
Ports on the Universal APs are labeled ETH0, ETH1. Other AP models label the ports GE1 and GE2.

From the factory, the Universal APs are configured for management by ExtremeCloud IQ and always engage with ExtremeCloud IQ for onboarding. You have the option to deploy your devices locally — on-premise from ExtremeCloud IQ Controller (or a WiNG controller) — or to deploy your devices from ExtremeCloud IQ. From an ExtremeCloud IQ account, onboard and register the Universal AP using either Local Management or Cloud Management. To manage these APs on-premise, you must specify **Local Management**.

When deploying the AP for Local Management, the AP will restart as a WiNG7 access point and discover the ExtremeCloud IQ Controller provided that you have configured the necessary DHCP and DNS options. If at any time, you want to manage the Universal AP from ExtremeCloud IQ, from the ExtremeCloud IQ Controller **Device List**, simply "Release to Cloud" The APs will restart and operate again in the ExtremeCloud IQ operating mode.

For more information, see the following topics in the *ExtremeCloud IQ Controller Deployment Guide*:

- Deploying Universal APs
- Configuring DHCP, NPS, and DNS Services

Related Topics

AP Actions on page 206

AP Client Bridge

AP Client Bridge topology extends a wired LAN using a wireless network. The Client Bridge can be used to tunnel network traffic to ExtremeCloud IQ Controller, enabling

connectivity for wired devices that are moved around a facility. For example, a medical device that is moved between rooms can maintain connectivity to ExtremeCloud IQ Controller through an AP radio configured as the uplink. The medical device moves with the Client Bridge AP, the two devices can be connected through the wired port (ETH1/GE2) or through a wireless connection. Client Bridge can be deployed for untagged traffic from an access port to a single VLAN on ExtremeCloud IQ Controller. (The wired port is associated with a single network.) Or, as a Transparent Bridge that supports a trunk port with tagged traffic to multiple VLANs.

For more information, see Transparent Bridge on page 263.

The Client Bridge deployment includes one or more infrastructure APs. After provisioning, the Client AP connects to normal infrastructure services. The infrastructure AP is essentially any AP deployed for standard service offering. The infrastructure APs communicate with the ExtremeCloud IQ Controller supporting the usual traffic flow. The Client Bridge AP roams like a wireless client, supporting background scanning to determine available infrastructure APs. The Client Bridge AP associates on the infrastructure AP SSID (using network credentials) establishing a Client Bridge link with the infrastructure.

Client Bridge AP is adopted by ExtremeCloud IQ Controller and is managed as any other AP:

- When the Client Bridge AP is in *Client* mode (i.e. the GE2 port is set to **Client**), the wired clients connected to Client Bridge AP are controlled by the same policies as the wireless clients that are connected to any other AP.
- When the Client Bridge AP is in *Transparent Bridge* mode (i.e. the GE2 port is set to **Bridge**), the Client Bridge AP is transparently forwarding all traffic without monitoring individual sessions.

To get started, configure the Client Bridge settings on ExtremeCloud IQ Controller. Configure the Client Bridge from the configuration Profile. The Client Bridge AP is a member of a device group that references a Profile configured for Client Bridge.

Define Client Bridge from the **Radios** tab within the configuration Profile. Only one radio can be configured as a Client Bridge. This can be either radio. Regardless of which radio is configured as the Client Bridge, both radios will continue to provide service.

Client Bridge and Transparent Bridge are supported on Wi-Fi 6 AP models:

- Wi-Fi 6E World-Wide Universal APs ExtremeCloud IQ or on-premise operation
- Wi-Fi 6 Universal APs ExtremeCloud IQ or on-premise operation
- Wi-Fi 6 on-premise operation only.

.

Note
The ETH1/GE2 Bridge port is *not* supported on access points with a single Ethernet port.

Note
For ExtremeCloud IQ Controller deployments with network policy assignment for proper end-system visibility, the Client Bridge AP must be in a Centralized Site (Campus mode) and must be managed by ExtremeCloud IQ Controller.

Wired and wireless clients can be managed by Client Bridge. Client traffic can be forwarded on any of the following supported topologies: Bridged@AP, Bridged@AC, Fabric Attach, and VxLAN. A wired client refers to a device that has direct wired connectivity to the client port (GE2) of the AP. This can be a direct connection into the AP port or connected through a layer 2 switch. The wired client port supports up to 128 simultaneous client sessions.

Note

- The following AP models with PSE provide downstream POE:
  - AP5010 — PSE controlled from the user interface, and it is available only when the AP is powered from BT.
  - AP302W and AP310i/e — PSE is switched on automatically when the AP is powered from AT.
- Ports on the Universal APs are labeled with the prefix ETH.
- When Client Bridge is configured on a single interface AP, the single interface is used as the client port, not as an uplink, and you will not see the **GE2 Port Function** field in the configuration Profile **Advanced Settings**.

Network policy is applied to both wired and wireless clients in the same way. The network policy is enforced on the Client Bridge AP before the network traffic is forwarded. All configuration updates are pushed to the Client Bridge AP before being applied to the infrastructure AP.

The role assignment for each AP is defined in its unique configuration Profile. When using Bridged@AP and Fabric Attach topologies, ensure that the Client Bridge role assignment is synchronized with the infrastructure AP role assignment.

Note
For a Client Bridge path, policy enforcement for clients is handled at the Client Bridged AP, including any adjustments to topology assignment (VLAN Tagging). The infrastructure AP operates purely as a transparent bridge for the traffic that is received from the Client Bridge AP. The same applies to management network access. If the infrastructure is configured to require management traffic on a specific VLAN, and is tagged by the infrastructure AP, the same configuration needs to be applied to each Client Bridge AP, ensuring that the VLAN tags match the infrastructure requirement. It behaves essentially as if the Client Bridge access point was directly connected to the same infrastructure switch port as the infrastructure AP that provides the path for wireless connectivity.

Related Topics

Configure Client Bridge on page 144
Transparent Bridge on page 263
Understand Radio Mode on page 147
Device Groups on page 32
Add or Edit a Configuration Profile on page 134

Managing Client Bridge in ExtremeCloud IQ Controller

You can view data from a Client Bridge AP on both the **Access Points List** and on the **Clients List**. Both lists are available from the **Monitoring** workbench on ExtremeCloud IQ Controller.

All columns on the list screens are not displayed by default. See Configuring Column Display on page 43 to customize your column layout.

From the **Access Points List**, display the Radio Mode columns to indicate that an AP is configured as a Client Bridge. The Radio Mode column value for a Client Bridge AP is **bridge**.

Note
A best practice is to indicate in the AP Name that the AP is a Client Bridge.

In the **Clients List**, use the Device Type column to indicate that this client is an AP Client Bridge.

Note
Client Bridge enables the access point to be used as a wireless service extender on one radio band while the other band is in Client Bridge mode. This function is optional. However, if the device is expected to be used in a roaming scenario throughout a facility, this operational mode is not recommended. For use cases requiring mobility, the mobility of the access point may cause undue interference to the infrastructure RF plan. That interference can manifest as excessive co-channel interference or even fluctuation in settings and stability of the RF infrastructure settings when using Dynamic RF management methods.

Related Topics

Configuring Column Display on page 43
AP Client Bridge on page 24
Configure Client Bridge on page 144

GRE Point-to-Point Tunnel

ExtremeCloud IQ Controller supports tunneling traffic between access points without traversing the controller. Generic Routing Encapsulation (GRE) offers direct, point-to-point communication between network nodes with support for one to three termination points. This option steers tunneled traffic to destination points other than the default controller and offers support where other tunneling options like VxLAN and Fabric Attach are not a consideration.

APs establish a GRE tunnel with the defined target termination point and directly bridge traffic to and from clients associated to the topology. The data path for wireless client traffic can now travel to a separate data center without involving a controller.

To configure a GRE point-to-point tunnel:

- Define the VPN Concentrator termination points
- Define the GRE VLAN topology as tagged or untagged and select up to three termination points.

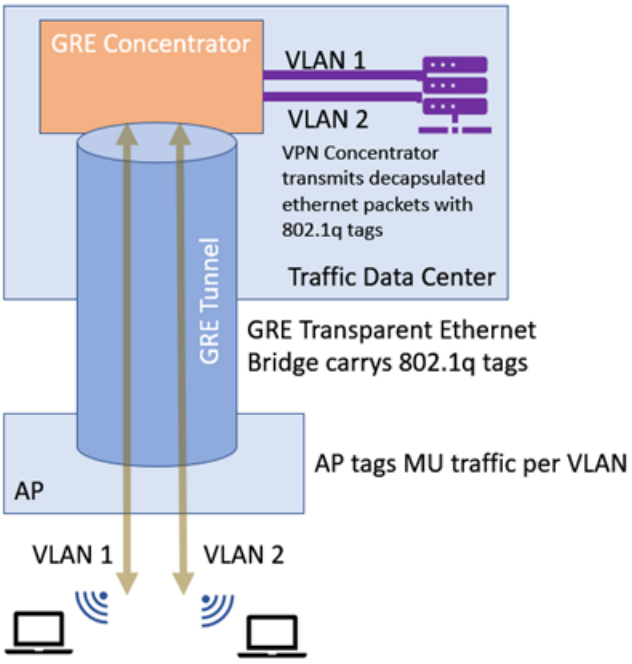


Figure 2: GRE Point-to-Point Tunneling

Related Topics

VPN Concentrators on page 248
GRE Topology on page 313

Cloud Visibility

You can view a stream of data coming from ExtremeCloud IQ Controller managed access points in ExtremeCloud™ IQ.

Cloud Visibility provides a data stream of information to ExtremeCloud IQ for consolidated reporting. The feature facilitates reporting of wired and wireless metrics, including client application metrics, into ExtremeCloud IQ. The reporting frequency is 5 minutes.

ExtremeCloud IQ Controller reports metrics on 32 application categories to ExtremeCloud™ IQ. Reported are the Rx and Tx bytes for each application category, and the number of mobile users in each category, per network.

Onboard the controller to your ExtremeCloud IQ account as easily as any other device. After onboarded, launch the ExtremeCloud IQ Controller user interface from ExtremeCloud IQ. This enables you to access and manage the controller and devices from your ExtremeCloud IQ account.

The following requirements must be met to view APs and clients in ExtremeCloud IQ:

- An ExtremeCloud™ IQ Navigator or Pilot account
- Onboard ExtremeCloud IQ Controller to ExtremeCloud IQ.

Cloud Connection

The cloud icon on the product banner indicates connectivity with ExtremeCloud IQ

- Green indicates that the controller has discovered the cloud URL and indicates connectivity to ExtremeCloud IQ.
- Gray indicates that the controller has not discovered the cloud URL.

Connection can take up to 15 minutes after the controller is onboarded. To refresh the browser and connect on demand, go to **Administration** > **License** > **License Details** and select **Synchronize Now**.

- Hover over to view the Cloud Virtual IQ address (VIQ) of the ExtremeCloud IQ connection.
- Select to open a new browser tab to ExtremeCloud IQ. The ExtremeCloud IQ log on page is displayed.

See the *ExtremeCloud IQ Controller Deployment Guide* for information on onboarding ExtremeCloud IQ Controller to ExtremeCloud IQ and accessing the controller user interface from ExtremeCloud IQ.

- ExtremeCloud IQ Controller requires internet connectivity and a Domain Name Server (DNS) configuration.

The following AP models support Cloud Visibility:

- Wi-Fi 6 AP models
- AP39xx
- SA201 Defender Adapter

Note
Reporting of metrics for managed switches is not supported.

Sites Overview

Use sites to define boundaries for fast roaming and session mobility without interruption. A site represents a physical, geographic area in your network, and defines a roaming domain. As the top-level element in the ExtremeCloud IQ Controller data model, the site runs Sessions Manager and RF Manager functions for all RF Domains in the site. Define the licensing domain for the site by selecting the **Country** option.

A site in ExtremeCloud IQ Controller is composed of one or more device groups. Each device group holds one or more APs. The APs in a device group must have the following in common:

- AP Model
- Configuration Profile
- RF Domain
- Regulatory domain and configuration type, which is defined at the site level.

A site can include multiple device groups all in a single RF domain, or multiple device groups, each group in a unique RF domain.

A site also includes the following:

- One or more floor plans. Floor plans are unique to each site.
- Site metadata used to place the site on a Google map.
- List of switches associated with the site.

Related Topics

Centralized Site on page 31
Add a Site on page 130
Site Default Dashboard on page 53
Modifying Site Configuration on page 131
Site Location on page 132
Configuring Column Display on page 43

Centralized Site

A Centralized configuration uses ExtremeWireless AP models:

- Wi-Fi 6 AP models
- AP39xx

Each Wireless AP opens an IPsec tunnel to ExtremeCloud IQ Controller, and the Session Manager and RF Management policy run on ExtremeCloud IQ Controller.

A Centralized site topology allows seamless roaming within one geographic location. A single site supports multiple device groups with a total of 200 to 4,000 APs (in appliance High Availability mode) for the site. With a Centralized site, ExtremeCloud IQ Controller performs as the management server and the session manager. The RF domain manager resides locally on ExtremeCloud IQ Controller.

Although session management is centralized at the appliance, users can select the best topology for network access.

The following AP models can be deployed in a Centralized site:

- AP3000/X
- AP302W
- AP305C/CX
- AP305C-1
- AP310i/e
- AP310i/e-1
- AP360i/e
- AP4000
- AP4000-1
- AP410i/e
- AP410i-1

- AP410C
- AP410C-1
- AP460i/e
- AP460C/S6C/S12C
- AP5010
- AP5050U/AP5050D
- AP505i
- AP510i/e
- AP510i-1
- AP560i/h
- AP3917i/e/k
- AP3916ic
- AP3915i/e
- AP3912i
- AP3935i/e
- AP3965i/e

Related Topics

Use Case: Large Centralized Site on page 32

Use Case: Large Centralized Site

Scenario: A large Centralized site is composed of two separate buildings. Each building supports a unique configuration with its own policy requirements. Clients need the ability to roam between buildings without session interruption.

Solution: Create a Centralized site, defining multiple device groups. Each device group will support a unique profile configuration.

Device Groups

The device group is composed of APs with the same model, configuration Profile, and RF Management profile. The device group is defined within a site, so device groups within a site also share the configuration type and licensing domain that is defined for the site.

If you have created a default device group for a specific AP model, upon discovery, the APs that match that AP model are available on the **Create Device Group** dialog. Manually select each AP to add it to the group. To automatically assign APs to a device group configure Adoption Rules before APs connect for the first time.

If the device group is not yet created upon AP discovery, the AP is listed in the **Access Points** List with a status of *in-service trouble*. After you create the device group and specify the configuration Profile for that AP model, APs that match the configuration Profile are available on the **Create Device Group** dialog. Manually select each AP to add it to the group.

Each device group contains the following elements:

- AP devices included in the group. An AP can only be a member of one device group at a time. You can manually move a device from one group to another.
- A configuration Profile.
- An RF Management policy.

Note
RF Management and configuration Profiles can be shared across device groups.

Note
Most AP radio properties depend on a regulatory domain; which is defined at the site level. Devices that are connected to ExtremeCloud IQ Controller but not assigned to a device group have the status of *In-Service Trouble*. Devices that have not discovered ExtremeCloud IQ Controller have the status of *Unknown*.

Related Topics

Adding Device Groups to a Site on page 132
Device Group Parameters on page 133
Add or Edit a Configuration Profile on page 134
Automatic Adoption on page 317
Floor Plans on page 35
Site Parameters on page 130

Profiles

Configuration Profiles in ExtremeCloud IQ Controller offer consistency and simplicity. Use a Profile to associate configuration parameters to a device group, and to apply configured network policy roles to the group. You can associate a single Profile to one or many device groups within a site, or device groups within one site can have separate Profiles.

Profiles are used to configure APs and individual radios. The available configuration options depend on the AP model. For a full list of configuration settings, see Table 33 on page 135.

Figure 3 illustrates multiple sites composed of one or more device groups, sharing a configuration Profile, and a separate device group using a different Profile. The Profile can be shared across sites and device groups or not. The device group is composed of APs with the same model, configuration Profile, and RF Management profile.

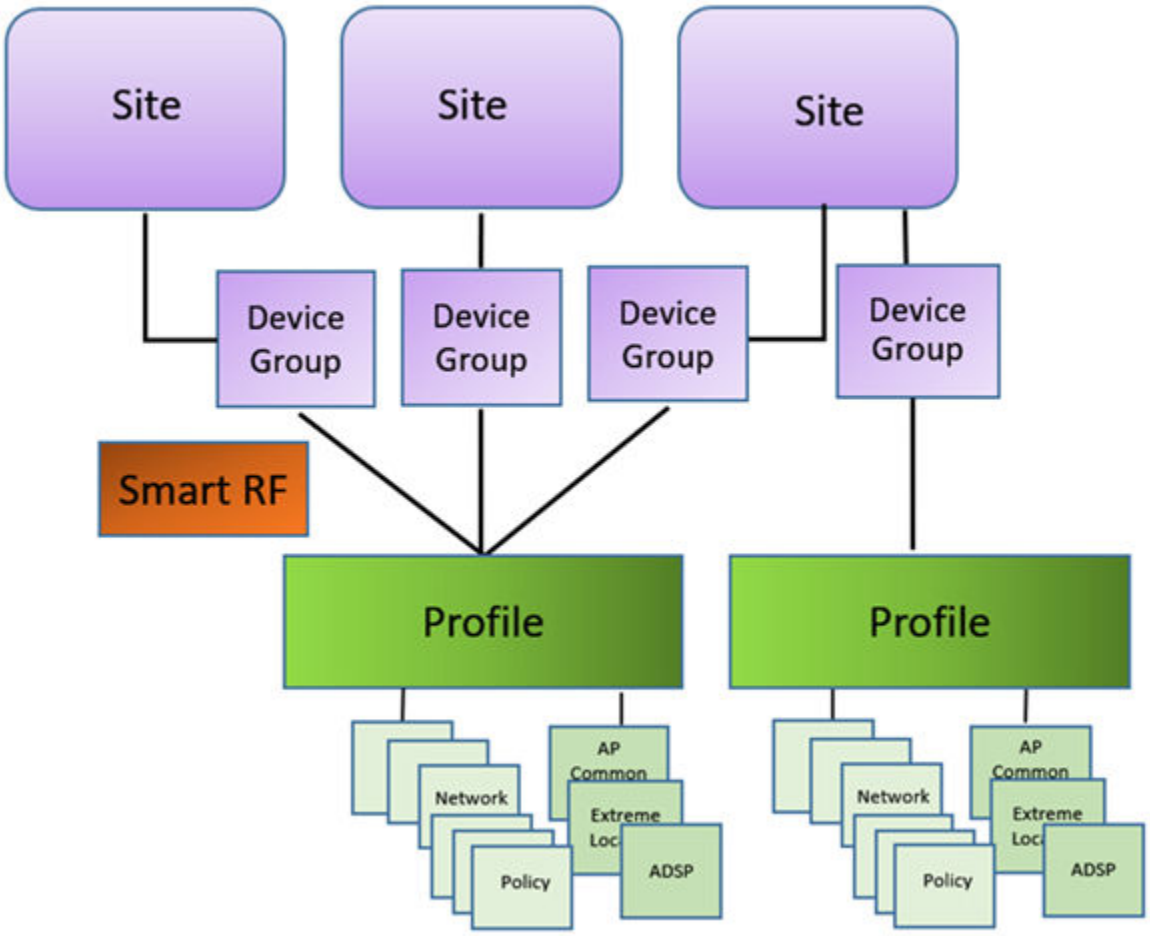


Figure 3: Site Data Model

Related Topics

Add or Edit a Configuration Profile on page 134
RF Management on page 34

RF Management

Self Monitoring At Run Time (SMART) RF Management is designed to simplify RF configurations for new deployments, while optimizing radio performance.

An RF policy can reduce deployment costs by scanning the RF environment to determine the best channel and transmit power configuration for each radio, allowing APs to respond dynamically to changing RF conditions. Apply RF Management policies to specific RF Domains.

After gathering information from the RF environment, RF Management makes intelligent configuration choices. It monitors the network for external interference, neighbor interference, non-Wi-Fi interference, and client connectivity. It then intelligently applies algorithms determining optimal channel and power selection for all APs in the network and constantly reacts to changes in the RF environment.

Real-time network monitoring allows RF Management to provide self-healing functions, providing automatic mitigation from potentially problematic events such as radio interference, non-Wi-Fi interference (noise), external Wi-Fi interference, coverage holes, and radio failures. Self-healing is used to enable a WLAN to better maintain wireless client performance and site coverage during dynamic RF environment changes, which would otherwise require manual reconfiguration to resolve.

This value depends on the RF Sensitivity setting on the **Basic** tab.

Related Topics

Configuring RF Management on page 180
Configuring ACS RF Policy on page 185
Configuring Smart RF Policy on page 187
Smart RF Widgets Per Device on page 101

Floor Plans

Use Floor Plans to visualize a wireless deployment, plan device placement, and troubleshoot network performance issues. The floor plan illustrates how the location of the AP affects network performance, and illustrates AP location within a floor plan. Floor plans retrieve a list of all APs and associated clients on the system with their current configurations. Use the floor plan to visualize AP performance based on signal strength and channel assignment, and to verify network readiness within a floor plan. Floor plan statistics are refreshed with a manual page refresh.

A floor plan is associated with the site. Work with floor plans under site configuration to import, export, or configure a floor plan. View a configured floor plan from the **Site** dashboard page. You can also view floor plans from the **Client** and **Devices** workbenches.

Toggle between floor plan **Configuration** and floor plan **View**:

- From the floor plan **View** page, click **Configure Site** > **Floor Plans** to open the floor plan **Configuration** page.
- From the floor plan **Configuration** page, click BACK to display the floor plan **View**.

Related Topics

Site Parameters on page 130
Configuring a Floor Plan on page 193
Floor Plan View on page 56
Positioning Profile Settings on page 169

Position Aware Services

Client location tracking is designed to manage a wireless environment and its resources. The Positioning Engine works in conjunction with the ExtremeCloud IQ Controller floor plans to define specific areas for Position Aware Services.

The Positioning Engine determines location based on measured Received Signal Strength (RSS) of the client stations at the AP. The location algorithm uses RF

fingerprinting based on a Path Loss model and determines location by triangulating RSS reported from one or more APs.

To improve efficiency of external location related applications, ExtremeCloud IQ Controller exposes a notification event conveying significant changes in the X/Y positioning of an associated device relative to the site floor plan. When you have a Positioning Profile configured, Location Update messages are available as a subscribe-able event. Programmers can leverage the ExtremeCloud IQ Controller Python SDK as a method to access and subscribe to such events. Each station event contains the following information:

- MULOG_TYPE_LOCATION
- AP MAC address
- Floor ID
- EID_LOCATOR_POINT_SET (This binary payload contains one set of X/Y coordinates and the probability as 32-bit integers.)

Python SDK is required to access the Location Update messages. For programmable access to ExtremeCloud IQ Controller Python SDK, see Python SDK. The messages are not visible in the ExtremeCloud IQ Controller user interface.

To suppress Location Update messages, access the Positioning Profile within the device group configuration Profile, and set the Collection setting to **Off**.

Client Location Tracking is supported on:

- AP39xx
- Wi-Fi 6 AP models

Estimating location using readings from multiple APs provides a more accurate location estimate. Estimating location using RSS from a single AP is sufficient to determine the location of client in terms of proximity to the associated AP. The client location is indicated on the map with an icon that is representative of the specific client type. The Positioning Engine tracks location of multiple clients simultaneously and returns position relative to the floor plan. The Positioning Engine can be configured to track associated users (active clients) or all users. When Positioning is configured for all clients, Location Update messages are sent for all tracked MAC addresses — both associated clients and non-associated clients.

- Associated User. An associated user is an authenticated client. An associated user joins the SSID provided by the AP by simply associating to the open or protected SSID. Positioning Engine can track location for every associated client up to the ExtremeCloud IQ Controller model limit of associated clients.
- Un-Associated User. An unassociated user is a client that is not authenticated but is in the designated area. Positioning Engine can track these clients.

Related Topics

Positioning Profile Settings on page 169
Position Aware Deployment on page 37

Position Aware Deployment

Deploying APs for location tracking requires additional consideration above the standard AP deployment guidelines for coverage and capacity. The following are best practices for AP deployment:

- Minimum Received RSS. No fewer than three APs should be detecting and reporting the RSS of any client station. Only RSS readings stronger than -75 dBm are used by the Location Engine.
- Use the same AP model for the entire floor plan.
- Design your floor plan with the APs installed at the corners of the floor plan, along the perimeter of the location area. (An area is considered a closed polygon.) Do not cluster APs in the center of the location area. The following illustration shows a recommended AP placement.

Figure 4: Recommended AP Placement

- The maximum distance between APs depends on environmental factors such as the presence of walls and structures, but as rule of thumb, in a location-aware deployment, place the APs 10 to 20 meters apart.
- Install APs at the same height on the wall, and do not install APs behind walls or ceilings.
- Install APs away from metal structures like poles or racks, because metal can affect the radiated pattern.

Related Topics

Position Aware Services on page 35
Positioning Heatmaps on page 67
Placing Devices on page 199

Floor Plan Limits

A floor plan can represent a facility size of up to 200,000 meters squared.

Table 9 outlines the floor plan limits for each type of ExtremeCloud IQ Controller.

Table 9: Floor Plan Limit per Appliance

Appliance	Maximum Number of Floor Plan Files	Maximum Number of APs Per Floor
E1120	50	500
E2120	400	1,000

Table 9: Floor Plan Limit per Appliance (continued)

Appliance	Maximum Number of Floor Plan Files	Maximum Number of APs Per Floor
E2122	400	1,000
E3120	1,000	1,000
E3125	1,000	1,000
VE6120	200	1,000
VE6120H	200	1,000
VE6125	400	1,000
VE6120K	200	1,000
VE6125K	400	1,000

Note
There is a file size limit for Ekahau model files:

- 46 MB uncompressed SVG files on appliances:
  - E2120
  - E2122
  - E3120
  - E3125
- 18 MB uncompressed SVG files on appliances:
  - E1120
  - VE6120
  - VE6125
  - VE6120H
  - VE6120K
  - VE6125K

Files larger than these limits will not import on the listed appliances. Consider converting large SVG files to PNG prior to import.

Related Topics

Floor Plans on page 35

Navigate the User Interface

Banner

The ExtremeCloud IQ Controller banner at the top of the page displays the following information:

- Select to display platform information:
  - Model
  - Hostname

- Version
- MAC address
- Serial Number [Locking ID]
- Up Time
- Availability details:
  - Mode – Paired vs Stand-Alone
  - Role Primary vs Backup
  - Peer IP address
  - Synchronization Status – Synchronized vs Out of sync
  - Link Status – Link Up vs Link Down

- indicates connectivity to ExtremeCloud IQ:
  - Hover over to view the Cloud Virtual IQ address (VIQ) of the ExtremeCloud IQ connection.
  - Select to open a new browser tab to ExtremeCloud IQ. The ExtremeCloud IQ log on page is displayed.
- Select to display Best Practice information.
- Select **admin** to display context-sensitive Online Help and Terms and Conditions.

Navigation Pane

The ExtremeCloud IQ Controller user interface is divided into workbenches that correspond to the network administration workflow. Monitor your network from the **Monitor** workbench and configure network settings from the **Configure** workbench.

- To expand the main navigation pane, select .
- To pin the navigation pane in place, select at the bottom of the pane.

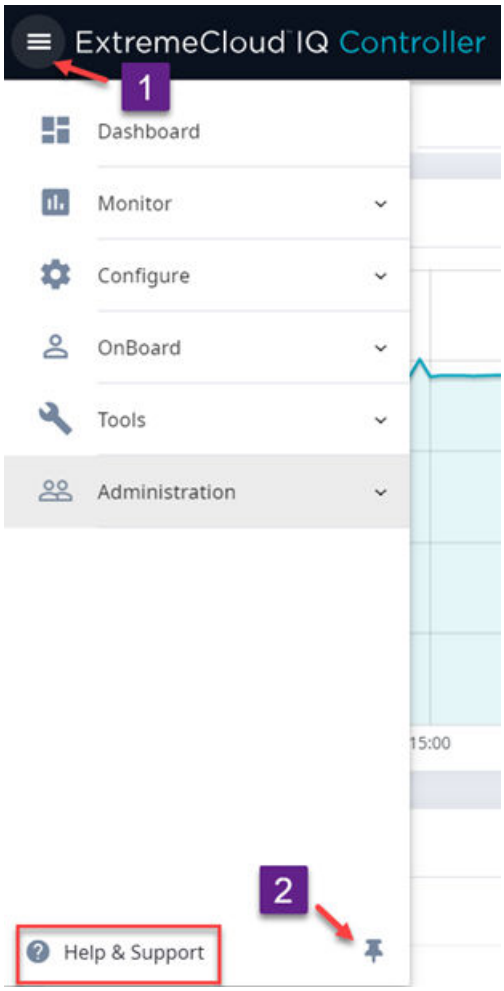


Figure 5: Main Navigation Pane

ExtremeCloud IQ Controller sites are the building blocks on which your network configuration is based. Start with **Configure** > **Sites** and work your way down the **Configure** workbench as you configure your network.

The **Dashboard** is the first workbench. After the network is up and running, use the **Dashboard** and **Monitor** workbenches to monitor your network activity and performance.

The ExtremeCloud IQ Controller user interface can be accessed using the HTTPS protocol on the TCP port 5825. For example, if your ExtremeCloud IQ Controller has the IP address, 192.168.10.10, you can manage it in a browser by typing `https://192.168.10.10:5825/` into the URL field.

The factory preset credentials are Username: "admin", Password: "abc123". These values are case-sensitive.

Workbenches

ExtremeCloud IQ Controller offers the following workbenches:

Dashboard

Monitor your network activity and performance on the **Overview** dashboard.

Monitor

Monitor the following network components:

- Sites
- Devices
- Networks
- Clients
- Policy

Configure

Set up the following network components:

- **Sites**. Network segmentation based on geographical location. Use sites to define boundaries for fast roaming and session mobility without interruption. Sites are comprised of Device Groups that organize network devices by platform, offering common configuration and RF Management.
- **Devices**. Configure access points, radio settings, switches, and adoption rules.
- **Networks**. Configure network services that bind a wireless LAN service (WLANS) to a default role.
- **Policy**. Define policy rules to specify network access settings for a specific user role.
- **Adoption**. Configure adoption rules. The AP adoption feature simplifies the deployment of a large number of APs. A set of rules defines the device group assignment for new APs, when they register for the first time. Without adoption rules defined, you must manually select each AP for inclusion in a device group.
- **ExtremeGuest**. Configure ExtremeGuest™ integration with ExtremeCloud IQ Controller.
- **AAA Policy**. Configure AAA Policy for external RADIUS, bypassing ExtremeCloud IQ Controller.

Onboard

Configure network access, including AAA configuration, captive portal configuration, access control groups, and a rules engine.

Tools

Use Workflow, Logs, Reports, and Diagnostics for network troubleshooting.

Administration

Configure system settings, work with utilities, manage upgrades, configure container applications, apply system licenses, and manage accounts.

Online Help

ExtremeCloud IQ Controller offers a context-sensitive Online Help system. To display the Online Help, from the navigation pane, select **Help & Support**. Also, to access the topic-based Help System:

1. From the logged in user name on any page, select the drop-down menu.
2. Select **Online Help**.

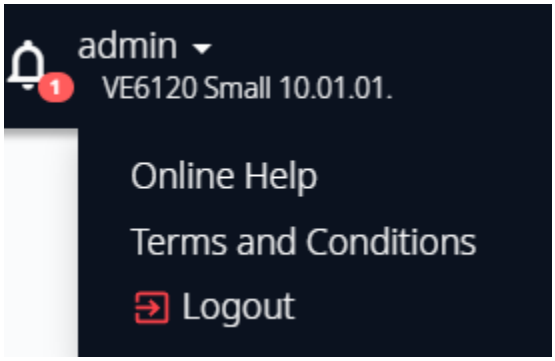


Figure 6: ExtremeCloud IQ Controller user name menu

Additionally, select on each dialog to display Help content for that dialog.

The Online Help file organization corresponds to the workbench structure of ExtremeCloud IQ Controller. The Online Help file offers a Table of Contents and Search Facility so you can find the information that you need.

Also on the User name menu, you will find the **Terms and Conditions** and **Logout** options.

Related Topics

Dashboard on page 44
Cloud Visibility on page 29
System Health Best Practice Widget on page 384

Search Facility

Each list page in ExtremeCloud IQ Controller offers a search facility so you can easily find what you are looking for based on specific criteria. Regular expression search, including wild cards is not supported.

Additionally, you can use tools on the **AP List** page and the **Client List** page to create customized queries and chart results in a pie chart format.

Related Topics

Query Builder on page 73

Configuring Column Display

Configure which columns display on a list screen. To configure the column display:

1. Select ☰ to display the list of columns.
2. Select a column to display. Or, clear the check mark to hide the column.

Note
To save space, some columns are hidden by default. To customize the list screen, select the columns to be displayed. Configure the AP and Client list screens to fit your needs. Use the horizontal scroll bar to view all your selected columns.

Some list screens support exporting data to .csv file. when exporting to .csv is supported, select **Export all Data to CSV** or **Export Visible Data to CSV**. A spreadsheet with data is created in your Downloads folder.

Understanding Date and Time

The dates and times that you see displayed in the user interface represent the local time zone of your browser. This can be different from the time zone of the appliance where ExtremeCloud IQ Controller is installed.

For example, if ExtremeCloud IQ Controller is installed on an appliance in EDT time zone, and your browser is installed on a machine in PDT time zone, the time represented in the detail views and logs will be in PDT, the time zone of the browser.

In this scenario, if you register a client with ExtremeCloud IQ Controller at 8:30 EDT, the Event Logs and Client Detail values show the time as 5:30.

Dashboard

Default Dashboard

The Overview dashboard displays widgets that can help you proactively monitor and troubleshoot your network. The dashboard provides a graphical representation of information related to devices, clients, and network traffic. Depending on the report, the widget represents historical data or a combination of historical and the latest data from shared memory.

Note
Historical data is persistent after system restarts and software upgrades, but not if the system is restored to the factory defaults or from a backup.

ExtremeCloud IQ Controller is installed with a Default dashboard. You can customize the Default dashboard and add additional dashboards with custom layouts and a unique set of widgets. The maximum number of supported dashboards is 10. The free-form dashboard can have a maximum of 10 widgets.

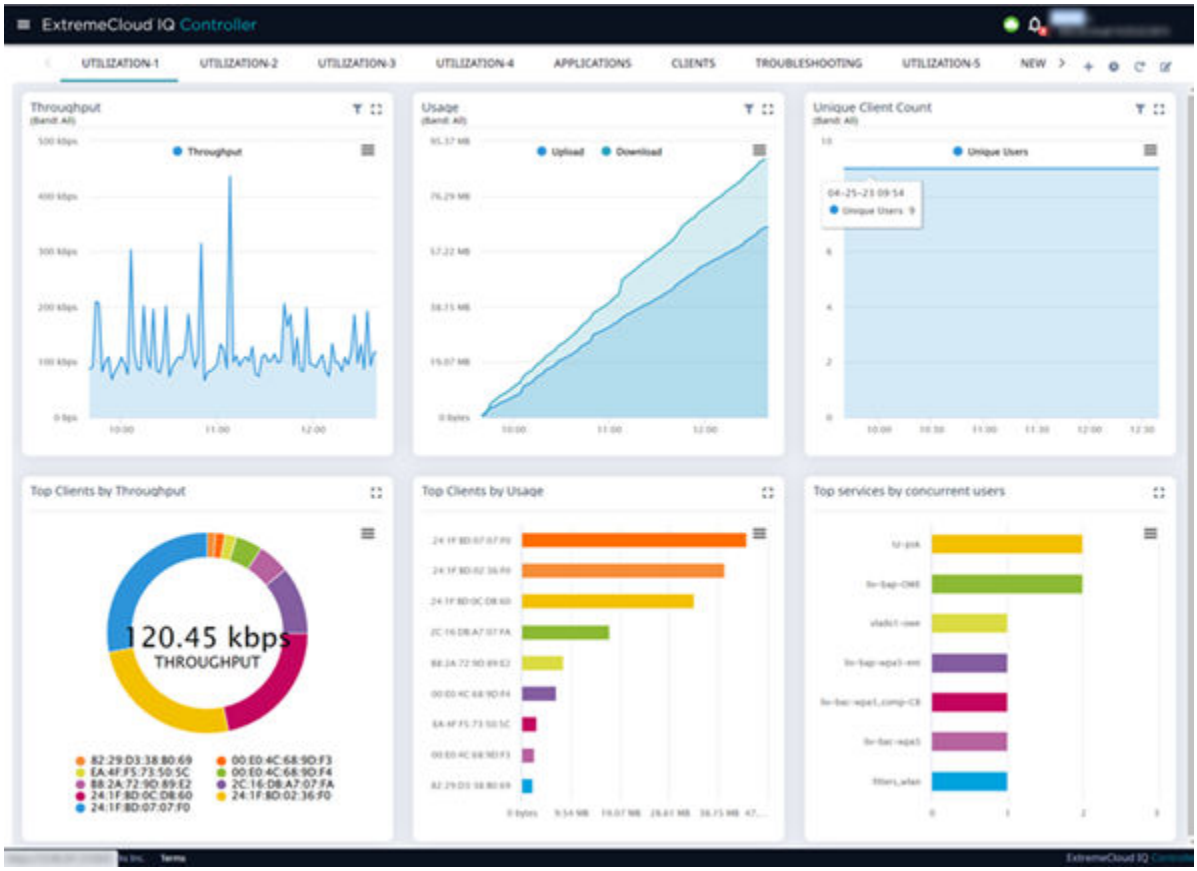


Figure 7: Default Overview Dashboard

Dashboard Widgets

The Overview dashboard widgets are classified according to the type of data they access:

- Network utilization metrics including top and bottom values for clients, APs, switches, and networks
- Radio Frequency metrics
- Switches with top and bottom throughput levels
- Client distribution and client count for the top and bottom manufacturer, network, and operating system
- Captive Portal metrics that include details on guests associated with the network and dwell time for each guest
- Application Visibility metrics categorize applications and application groups by throughput, client count, usage, and unique users
- System metrics that indicate network health.
- Troubleshooting that displays packet capture instances.

Combine widgets from any of the categories to create one or more unique dashboards.

Report Duration

From the top of the **Dashboard** page:

- Select to set the **Duration** value for the time period reported. Valid duration values are:
  - Last 3 hours
  - Last 3 days
  - Last 14 days
- Select to refresh the data on demand.
- Hover the mouse over a widget to display tool tip information.

Filter by Radio Band

Filter by radio band. Select to display data for a specific radio band.

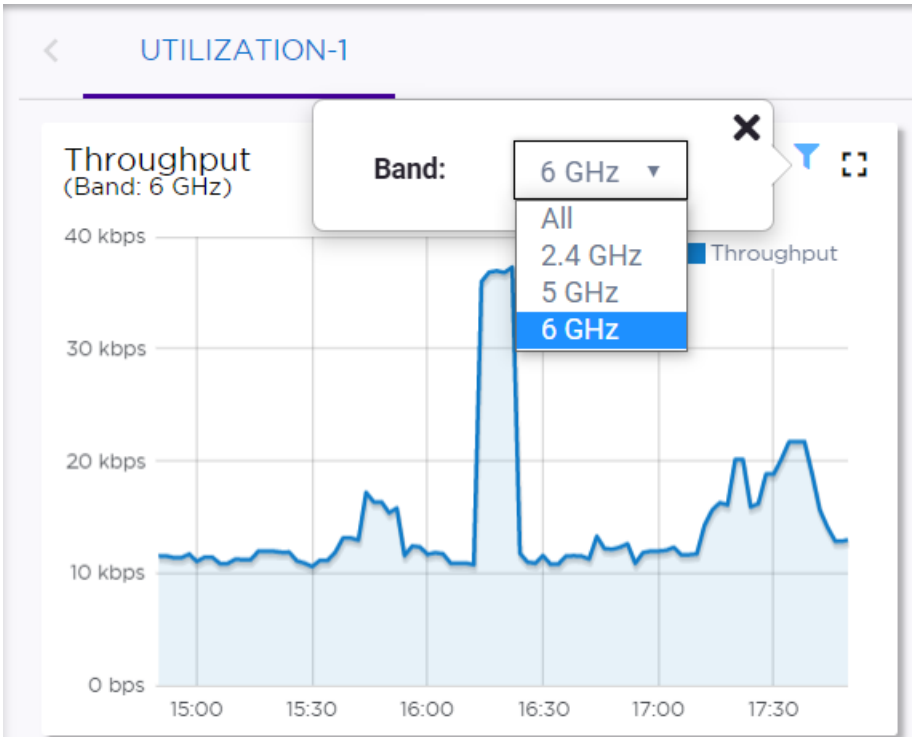


Figure 8: Select Radio Bands — Throughput Widget

Note
The datasets are sampled at different intervals. Therefore, it is possible that data from the 14-day dataset will not include data from the 3-day dataset or from the 3-hour dataset. It is possible that a new client will not appear in a dataset if the dataset has not been recently updated.

Related Topics

Add a New Dashboard on page 47
Modify a Dashboard on page 48
Understanding Date and Time on page 43

Availability Link Status on page 51
System Health Best Practice Widget on page 384
Network Health Widget on page 395
Smart Poll on page 396
Dashboard Widget — Packet Capture Instances on page 97
Diagnostics on page 384

Add a New Dashboard

Create additional dashboards to organize network data.

To add a new dashboard:

1. From the default dashboard, select the plus sign.
   The **Layout** tab displays.
2. In the **Name** field, enter a name for the dashboard.
3. Select a layout option for the dashboard.
   Each layout option has a set configuration. Choose the layout that matches the number of widgets you want to display. The last widget option enables you to display up to 10 widgets.

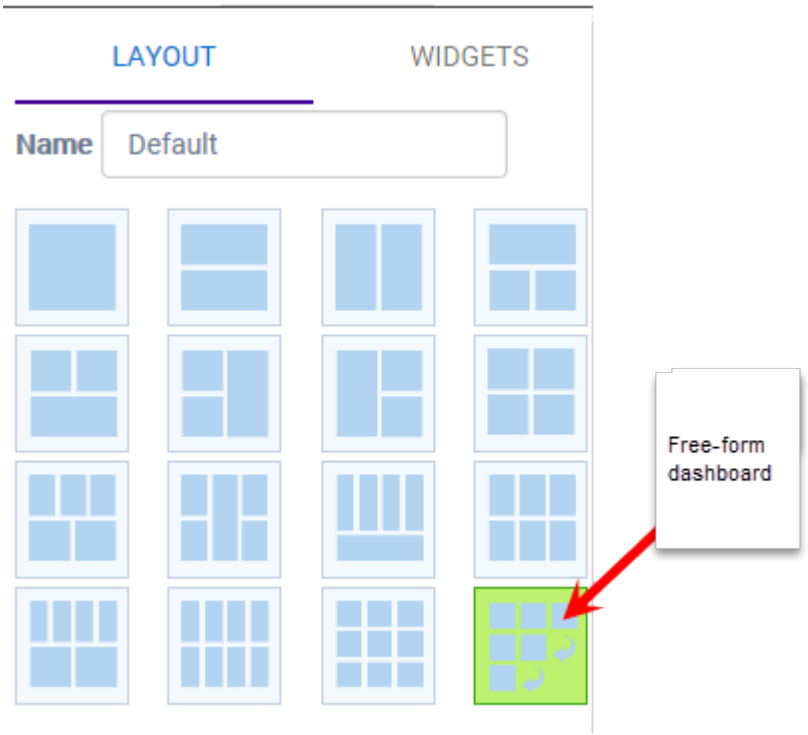


Figure 9: Widget Layout Options

4. Select the **Widgets** tab.
   The list of widgets by category is displayed.
5. Expand the list of widgets in each category.
6. Drag and drop a widget onto the dashboard, within the layout that you have selected.

7. Select **Save**.

Modify a Dashboard

You can customize the default dashboard views to fit your network's analytic requirements, such as monitoring the topology, component health, and device performance.

To modify a dashboard:

1. From the **Overview Dashboard** page or from the dashboard page of a specific entity, such as a device, select **Edit**.

   The **Layout** and **Widgets** tabs display on the far right.

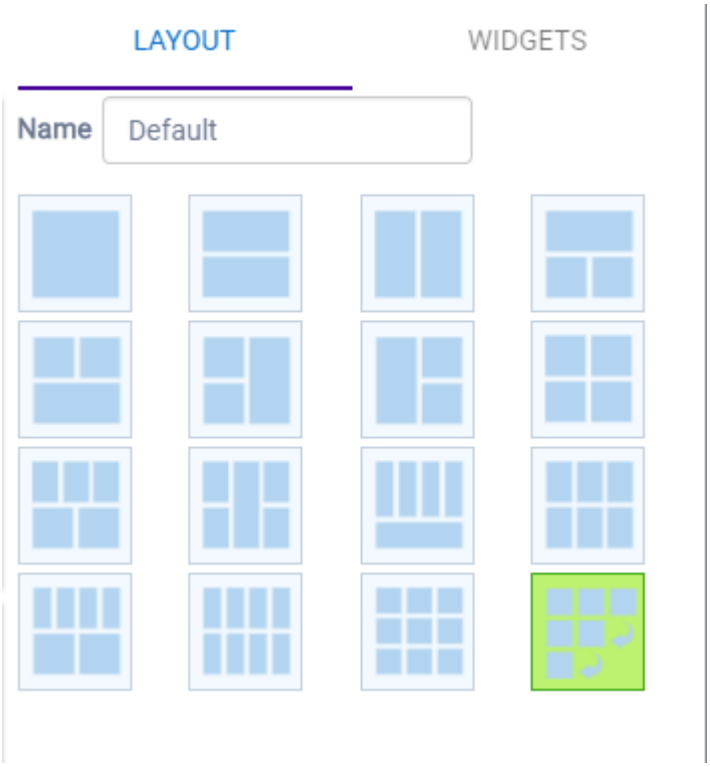


Figure 10: Dashboard - Edit Mode

2. From the **Layout** tab, select a layout.
3. From the **Widgets** tab, expand the categories that you want to use. Select the widgets that you want included in the layout. The following widget categories are available:

   Utilization

   Provides utilization metrics such as client count, and various top 10 and bottom 10 counts. Separate widgets display statistics for multiple networks, providing the ability to compare multiple SSIDs for client count, utilization, and throughput.

   RF

Provides Radio Frequency metrics such as RF quality, RF health, channel utilization, and various top 10 and bottom 10 metrics. This group also includes various Smart RF metrics.

Switch

Tracks top and bottom switches by throughput.

Clients

Tracks client distribution based on different parameters.

Captive Portal

Provides captive portal related information such as associated guests and dwell time.

Application Visibility

Provides application visibility metrics.

System

System metrics indicate network health.

Troubleshooting

Provides a packet capture list and Poll site statistics.

4. Select **Save**.

Utilization Stats by Network SSID

ExtremeCloud IQ Controller offers dashboard reports that you can use to compare network usage.

1. Go to **Dashboard** and select .
2. Select **Widgets** > **Utilization**.

The following Utilization widgets display data for multiple networks:

- Clients per Network
- Throughput per Network
- Utilization per Network

These widgets have the capability to check or clear the time series to be shown. By default, a minimized widget shows the first 10 time series with the legend displaying a checked mark. When the widget is expanded, all the checked time series are displayed with the full legend displayed. Users can select up to 10 SSIDs, clearing SSIDs as required. Select each line on the graph to display a tool tip that includes the network SSID for easy identification.

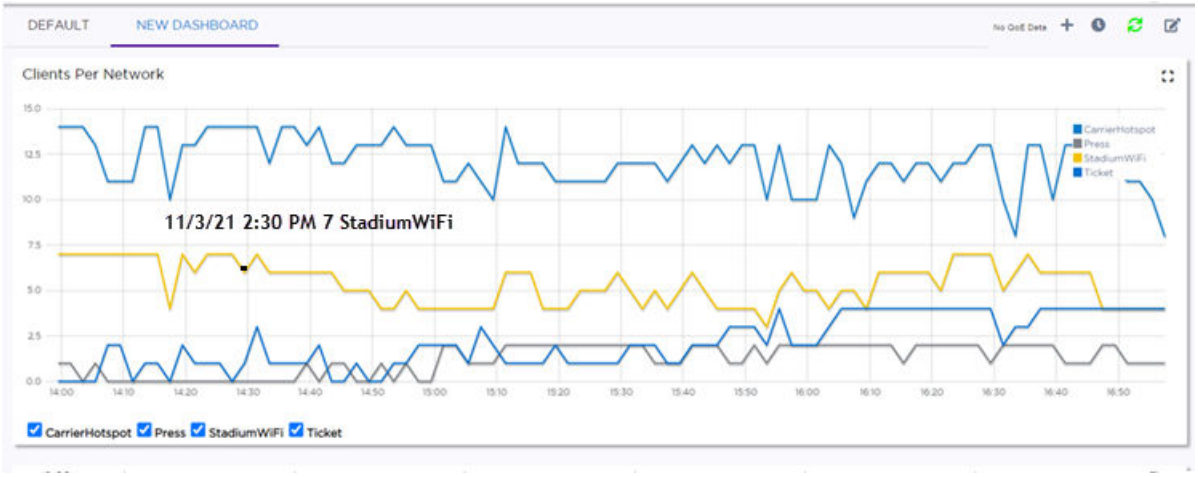


Figure 11: Clients per Network

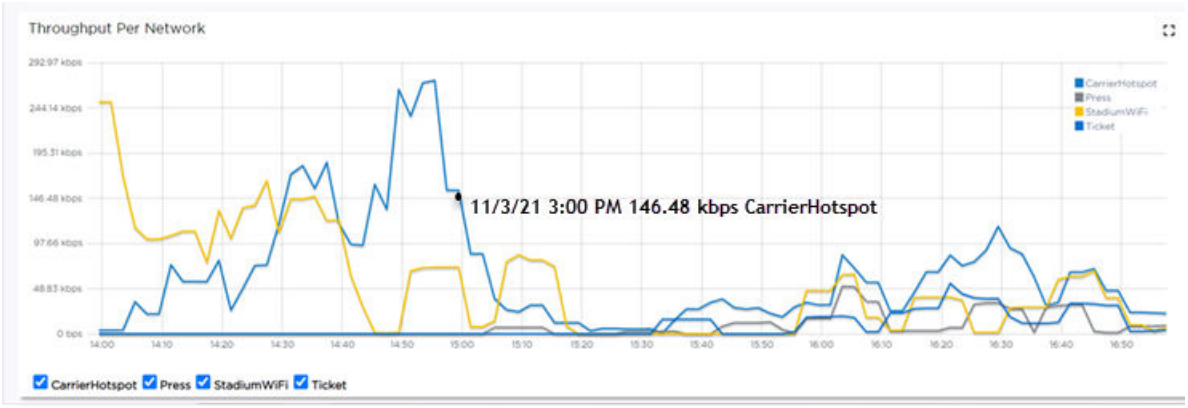


Figure 12: Throughput per Network

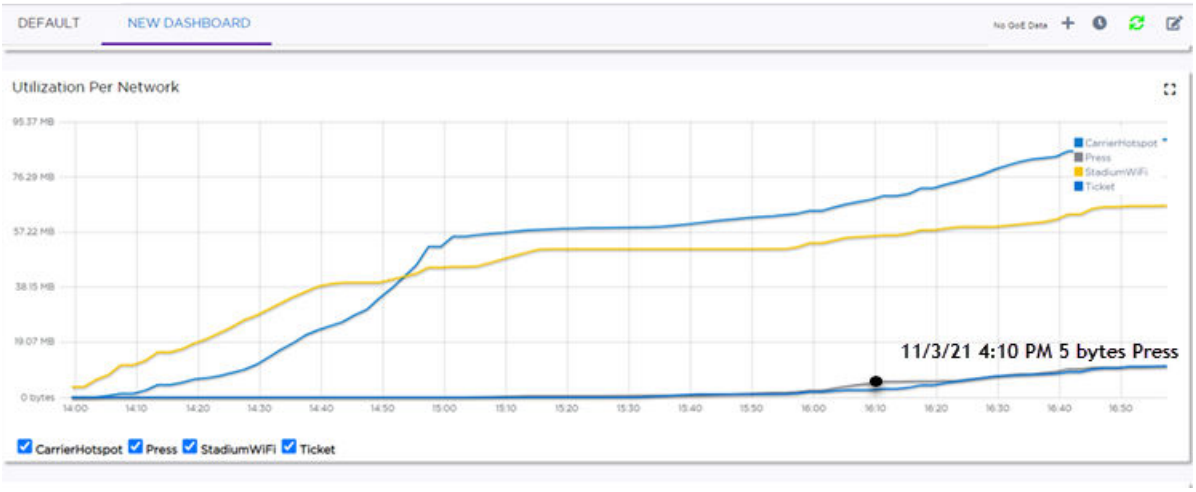


Figure 13: Utilization per Network

Related Topics

Modify a Dashboard on page 48
Reports on page 416

Availability Link Status

When an availability pair is configured, the synchronization status between the paired appliances is displayed on the Dashboard Network Health chart. Table 10 describes each possible link status.

Note
Both client and AP statistics remain available on both sides of an availability pair. However, cross-appliance statistical data can be affected if a mobile user is roaming across multiple APs when the availability pair connection between the appliances is down.

Table 10: Synchronization Status for an Availability Pair

Status	Description
Unknown	Link is down.
Synchronized	All changes are pushed to the peer appliance. **Note:** There may be a brief period when a change on the first appliance has not yet been pushed to the second appliance. During this time, you could see "Changed" on one appliance and "Synchronized" on the other appliance. This will be resolved as soon as the change has successfully been pushed to the second appliance.
Synchronizing	Changes are being pushed to the peer.
Changed	Not synchronized. There are pending changes that have not been pushed to the peer appliance.
Failed	Synchronization failed.

Related Topics

Availability on page 445
Network Health Widget on page 395

Monitor

Use the **Monitor** workbench to monitor network configuration and activity.

Sites List

Go to **Monitor** > **Sites** to view a list of sites configured in ExtremeCloud IQ Controller. Select a site to view the site dashboard and related components.

Highlights on the **Sites List**:

- **Status** indicates the site status:
  - the site is In-Service.
  - the site is in Critical trouble.
  - the site is unknown.
- **Name** identifies the site.
- **Country** indicates the licensing domain for the site.
- **Role** and **Network** indicate the number of configured roles and networks associated with the site through the Associated Profile. Networks and roles must be associated with a configuration Profile. Topology assignment to a site is inferred from the role and network assignment in the Profile. Each device group has a configuration Profile assignment. Therefore, APs within the device group are associated with the network definition (including VLAN assignment) and the role policy definition through the configuration Profile.
- **Switches** and **APs** indicate the number of devices of each type that are associated with the site. Furthermore, the following columns provide more information about AP association to the site:
  - **Adoption Primary** and **Adoption Backup** indicate the number of APs adopted to the Primary and Backup controller. In stand-alone mode, all APs are adopted to the Primary controller.
  - **Active APs** and **Non Active APs** indicate the number of active APs and inactive APs for the site.
- **Clients** indicates the number of active clients associated with the site.

Related Topics

Sites Overview on page 30
Centralized Site on page 31
Add a Site on page 130
Site Default Dashboard on page 53
Modifying Site Configuration on page 131
Site Location on page 132
Configuring Column Display on page 43
Associated Profiles on page 137

Site Default Dashboard

The Site Default Dashboard offers reports on the following topics:

- Site Utilization. Provides metrics on the amount of traffic passing through the site.
- RF Management. Provides metrics on radio frequency quality and channel utilization.
- Switches. Provides metrics on switch throughput.
- Clients. Provides metrics on client distribution by protocol and client count by manufacturer, operating system, and network.
- Captive Portal. Provides metrics on users who access the network through captive portal.
- Application Visibility. Provides metrics on application groups related to throughput, client count, and usage.
- Location. (Positioning) Provides metrics identifying visitor traffic by floor or area. (Supported on AP39xx only.)
- Filter by radio band. Select to display data for a specific radio band. For more information, see Filter by Radio Band on page 46.

Related Topics

Venue Dashboard on page 53
Add a New Dashboard on page 47
Modify a Dashboard on page 48

Venue Dashboard

The Venue Dashboard offers venue-specific reports that are based on customer-defined user groups. Use the Network Usage, Network Throughput, and Client Count widgets to create reports that are categorized by user-defined user groups. Define user groups that contain the Hotspot 2.0 NAI Realm of the service provider, or group users by SSID or client user group.

The following widget reports are provided on the **Venue Dashboard**. These dashboard widgets cannot be removed.

- **Usage by Type**. Usage for uplink and downlink.
- **Throughput by Type**. Throughput for uplink and downlink.

- **Throughput by Group**. Throughput per defined user group.
- **Upload Usage by Group**. Upload usage by defined user group.
- **Download Usage by Group**. Download usage by defined user group.
- **Unique Users by Group**. Number of unique users by defined user group.
- **Concurrent Users by Group**. Number of simultaneous connections by defined user group.

Note
Aggregate data crosses a High Availability Pair.

Use the ExtremeCloud IQ Controller Report Generator to generate the same Venue reports in PDF format. Generated reports can be downloaded and scheduled using Scheduler for ExtremeCloud IQ Controller.

To generate customer-defined reports, go to **Tools** > **Reports** > **Templates**.

Related Topics

Define Venue User Groups on page 418
Reports on page 416
Create Report Template on page 417
SP Identification on page 267
Scheduler for ExtremeCloud IQ Controller on page 471

Network Snapshot: Sites

To view network details from the **Sites** screen:

1. Go to **Monitor** > **Sites** and select a site.

   The **Site Dashboard** displays.
2. Select any of the tabs described in the following table.

Table 11: Tabs on the Sites Screen

Tab	Description
Dashboard	Customer-defined reports based on site statistics and venue-specific user groups: • **Default** tab displays network metrics for the site. • **Venue** tab displays customer-defined reports generated for venue-specific user groups.
Networks	Lists the network services associated with the site. Select a network to display network details.
Access Points	List of access points associated with the site. For more information, see: • AP Actions on page 206 • Radio Settings Button on page 55
Switches	List of switches associated with the site.

Table 11: Tabs on the Sites Screen (continued)

Tab	Description
Clients	List of clients associated with the site.
Troubleshooting	Offers packet capture at the AP, remote console access to the AP, and Smart Poll reporting.
Floor Plans	Floor plans associated with the site.
Smart RF	View widgets that show information about the following: • APs per Power level. • APs per Channel • Mitigation • Mitigation History

3. You can also:

   Select ⚙ to modify configuration settings.

   Select ☰ to go back to the list.

Related Topics

Site Default Dashboard on page 53
Venue Dashboard on page 53
WLAN Service Settings on page 250
Access Points List on page 69
Switches on page 239
Clients on page 115
Troubleshooting on page 93
Floor Plans on page 35
Smart RF Widgets Per Device on page 101

Radio Settings Button

Go to **Monitor** > **Sites** > **Access Points** to view a list of APs associated with the site. Select the check box next to the AP. Select the Radio Settings buttons at the bottom of the page to view settings for the selected AP.

The following radio settings are available:

Table 12: Radio Settings

Field	Description
Set Tx Power	
Channel Width	Set the channel width for the selected AP radio. See **Set Channel Width** below for more information.
Channel	Select from the list of available channels.

Table 12: Radio Settings (continued)

Field	Description
Max Tx Power (dBm)	Determines the maximum power level that can be used by the radio in dBm. The values are governed by compliance requirements based on the country, radio, and antenna selected, and will vary by AP.
Set Channel Width	
Channel Width	Set the default channel width for the selected radio. • 20 MHz • 40 MHz • 80 MHz (supported on 5GHz only 802.11ac and 802.11ax) • 160 MHz ◦ AP5xx – Radio 1 and Radio 2 support 160 MHz ◦ AP4xx / AP4xxC – Radio 2 only (5 GHz band) supports 160 MHz ◦ AP4000/ AP4000-1 – Radio 2 (5 GHz band) and Radio 3 (6 GHz band) support 160 MHz ◦ AP5010 – Radio 1 (5 GHz band) and Radio 3 (6 GHz band) support 160 MHz. ◦ AP5050 – Radio 1 (5 GHz band) and Radio 3 (6 GHz band) support 160 MHz. (Radio 3 is currently turned off for regulatory compliance.) ◦ AP3xx/AP3xxC — *Do not support* 160 MHz width on the 5 GHz radio. A best practice is to use a predetermined width configured as part of the design of the entire RF deployment. To learn about how Smart RF handles channel width settings, see Understanding Smart RF and Channel Width on page 183.
Auto Channel Select	ACS optimizes channel arrangement based on the current situation in the field if it is triggered on all APs in a deployment. ACS only relies on the information observed at the time it is triggered. After an AP has selected a channel, it remains operating on that channel until the user changes the channel or triggers ACS.

Floor Plan View

After the floor plan is configured, view the floor plan from **Monitor** > **Sites**. From the floor plan **View**. you can view and filter information related to the placed devices.

Go to **Monitor** > **Sites**. Select a site and select the **Floor Plans** tab.

- View the following map information across the top of the screen:
  - Map area, network coverage, environment, and scale.
  - Number of ceiling mounted APs.

  - Number of wall mounted APs.
  - Number of devices in each status.
- Control which device badges appear on the map based on the selected device group or statistical thresholds.
- View status, details, and statistics for each device.
- View clients associated with a selected device.
- View map zones for AP location.

Related Topics

Viewing a Floor Plan on page 57
Floor Plans on page 35
Configuring a Floor Plan on page 193

Viewing a Floor Plan

After the floor plan is configured, view it from a selected site's dashboard. The floor plan represents placed devices and associated badges that show configuration and performance data for the device. From the **Floor Plans** view, you can toggle between floors, filter data, and further fine-tune the map display.

To access **Floor Plans** view, go to **Monitor** > **Sites**, select a sight and select **Floor Plans**.

If one or more floor plans exist, available floor plans display in the right-side pane.

Here are a few things you can do with a floor plan:

- To search for devices:
  - Select the search icon .
  - Select on the search field and select device from the drop-down list.
- To zoom in and out, do one of the following:
  - Select to zoom in.
  - Select to zoom out.
  - Double-click on the map to zoom in. Use the mouse scroll wheel to zoom out.
  - Select the map and use the mouse scroll wheel to zoom in and out.
- Check device status:

Table 13: Device Status from the Floor Plans View

Status	Description
	AP is in-service, operating.
	In-service, trouble.
	Critical. Indicates that ExtremeCloud IQ Controller cannot communicate with the AP.

Table 13: Device Status from the Floor Plans View (continued)

Status	Description
	Unknown. AP is unknown to the displayed floor plan based on floor plan filter settings. Typically occurs when the device group for the AP is not selected.
	Unknown. The AP serial number is unknown to the floor plan. Typically occurs when you import a floor plan with AP place holders. For more information, see Use Case: Importing A Floor Plan with Unknown APs on page 195.
	Sensor device
	Switch
	Camera AP displayed as circular icon.
	Extreme Defender Adapter
	Ceiling-Mounted AP
	Wall-Mounted AP

Use **Auto Refresh** to automatically refresh the information presented. From the **Auto Refresh** drop-down field, select the refresh value. Valid values are:

- OFF
- 30 Seconds
- 1 Minute
- 3 Minutes
- 5 Minutes

You can also select  to manually refresh the page anytime.

Note

Save your page setting changes. **Auto Refresh** is implemented at the browser level and therefore will reset any selections or unsaved page setting changes. When using **Auto Refresh**, select a refresh interval that allows you to complete the operation within the defined interval. For best results, set **Auto Refresh** to OFF during configuration selections or selection of a large number of elements.

Both Associated and Unassociated clients are refreshed, provided they are marked as showing on the **Positioning** dialog. For more information, see Positioning Heatmaps on page 67.

Related Topics

Device Context Menu on page 62
Filtering Floor Plan By Badge Information on page 62
Understanding Readiness Maps on page 64

User Interface Controls

The **Floor Plan View** offers user interface controls in a pane to the right of the map display.

- Floors. Click to display the floor maps associated with the selected device group. Double-click a floor map in the right pane to display the full map.
- Maps. Click to display a list of possible maps:
  - Heatmap. Use heat maps to represent network connectivity based on one or more AP attributes.
  - Channels. Show APs by channel.
  - Link Speed. Device performance based on link speed.
  - RFQI. Device performance based on radio frequency performance.
  - BLE Coverage. Device performance based on BLE coverage. For a list of supported devices, see IoT Profile Settings on page 163.

  You can also select all APs or deselect all APs in one click.
- Positioning. Use heat maps to indicate Location Readiness and Foot traffic.
- Filters. Select to display filter options. Filter the floor map by AP attributes to focus on network attributes that need attention.
- Options. Select to display the following options:
  - Select Badges. Opens the **AP Badge Configuration** window.
  - Show/Hide Badges. Toggles the AP badge display on the active floor plan.
  - Show/Hide Grid. Toggles grid line display on the active floor plan.
  - Show/Hide Cameras. Display or hide camera APs. Camera APs are displayed with a circular icon.
  - Show Orientations. Show AP orientation on the active map. Wall-mounted APs display a black triangle on the map indicating their orientation.
  - Show/Hide Zones. Display or hide zones that are configured for Location Engine area change event support.

Related Topics

Placing Devices on page 199
Configuring AP Orientation on page 200
Configuring Floor Plan Zones on page 201
Configuring Camera AP Angle on page 200

Assigning Badges

Badges display real-time statistics that can be configured for each AP. If a metric is not assigned to a badge position, it is not shown on the user interface. By default, all the badges are assigned to an AP. The following metrics can be assigned to badges:

- RSS. Filter range: [-100, -10] dBm
- SNR. Filter range: [0, 50] dB
- TX Power. Filter range: [0, 30] dBm
- Radio Status
  - Green. Radio is on and providing service.
  - Red. Radio is on but *not* providing service.
  - Blue. Radio is off.
- Channel. Filter range: [1, 200]
- Clients. Filter range: [0, 200]
- Throughput.
  - Select min/max for the filter range. Available ranges:
    - [0, 1000] Kbps
    - [1, 50] Mbps
    - [50, 1000] Mbps
    - [1, 10] Gbps
  - Delta throughput since last statistics collection.
- Retries:
  - Filter range: [0, 100] %
  - Delta retries since last stats collection

To configure badges on APs manually:

1. From the right panel, select **(Options)** > **Select Badges**.

2. In the **Badge Configuration** dialog, drag and drop the badges from the left panel to the AP.

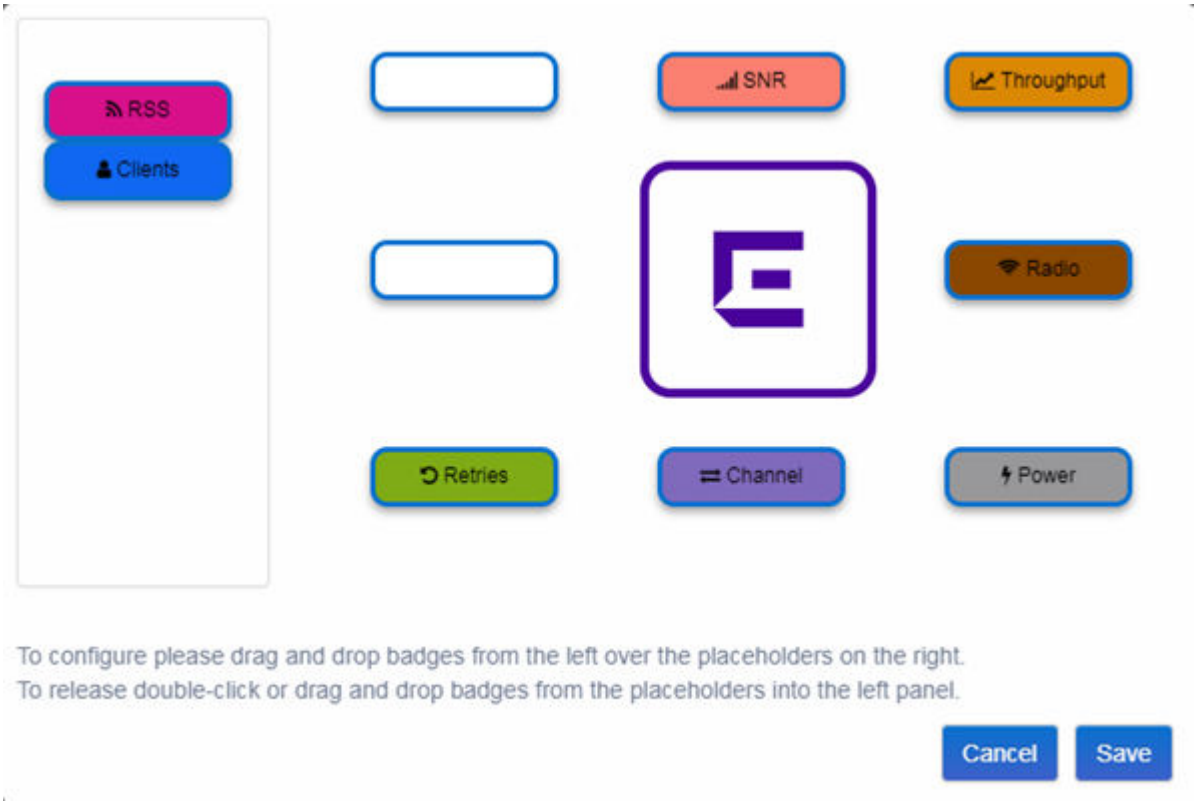
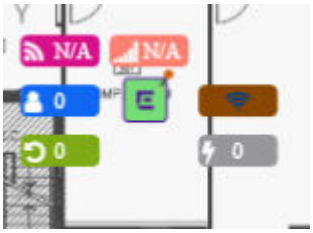


Figure 14: Badge Configuration Dialog

The badges display around the AP and are visible when you zoom in on the map.



Select  to display the badges legend that identifies the active badges.

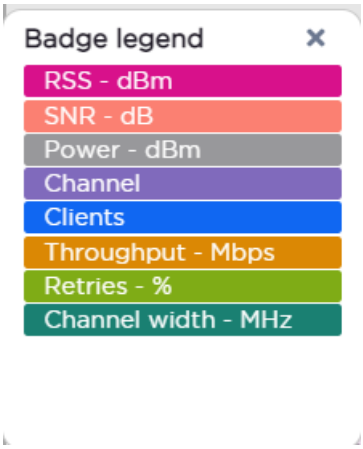


Figure 15: Badges Legend displays active badges

Related Topics

Filtering Floor Plan By Badge Information on page 62

Device Context Menu

Right-click a device icon to view the following information:

- A link to the device configuration page.
- A link to the device details page.
- A link to the list of clients associated to the AP.

Select the **Exclude** check box to exclude a device from simulations. If excluded, data from this device will not be considered when generating heat maps.

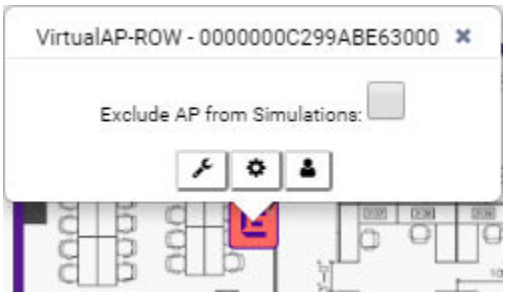


Figure 16: Device Context Menu

Related Topics

Network Snapshot: AP Details on page 84

Filtering Floor Plan By Badge Information

The floor plan can be filtered by the badge information that you configure for each device. Set the filter criteria from the **Filters** panel on the right side of the screen. A device badge displays on the floor plan when its value meets the selected filter criteria. Use map filtering to troubleshoot the network, displaying device badges that meet specific thresholds.

For example, when looking for APs with 20 clients, set the Client filter to 20 and look for APs with blue Client badges displayed.

To filter by AP statistics:

1. From the panel on the right side of the screen, select the Filters icon .

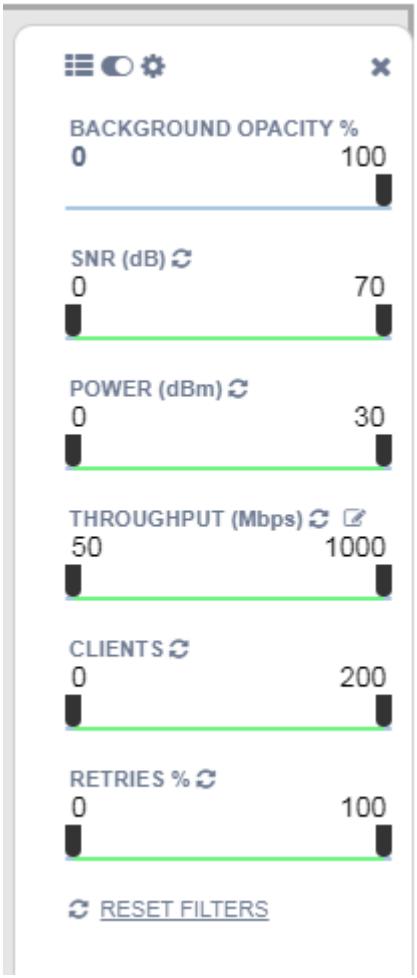


Figure 17: Map Filters Panel

2. Use the slide bar on each filter to set criteria for the map display.
   The AP badges that meet the filter criteria appear on the map.

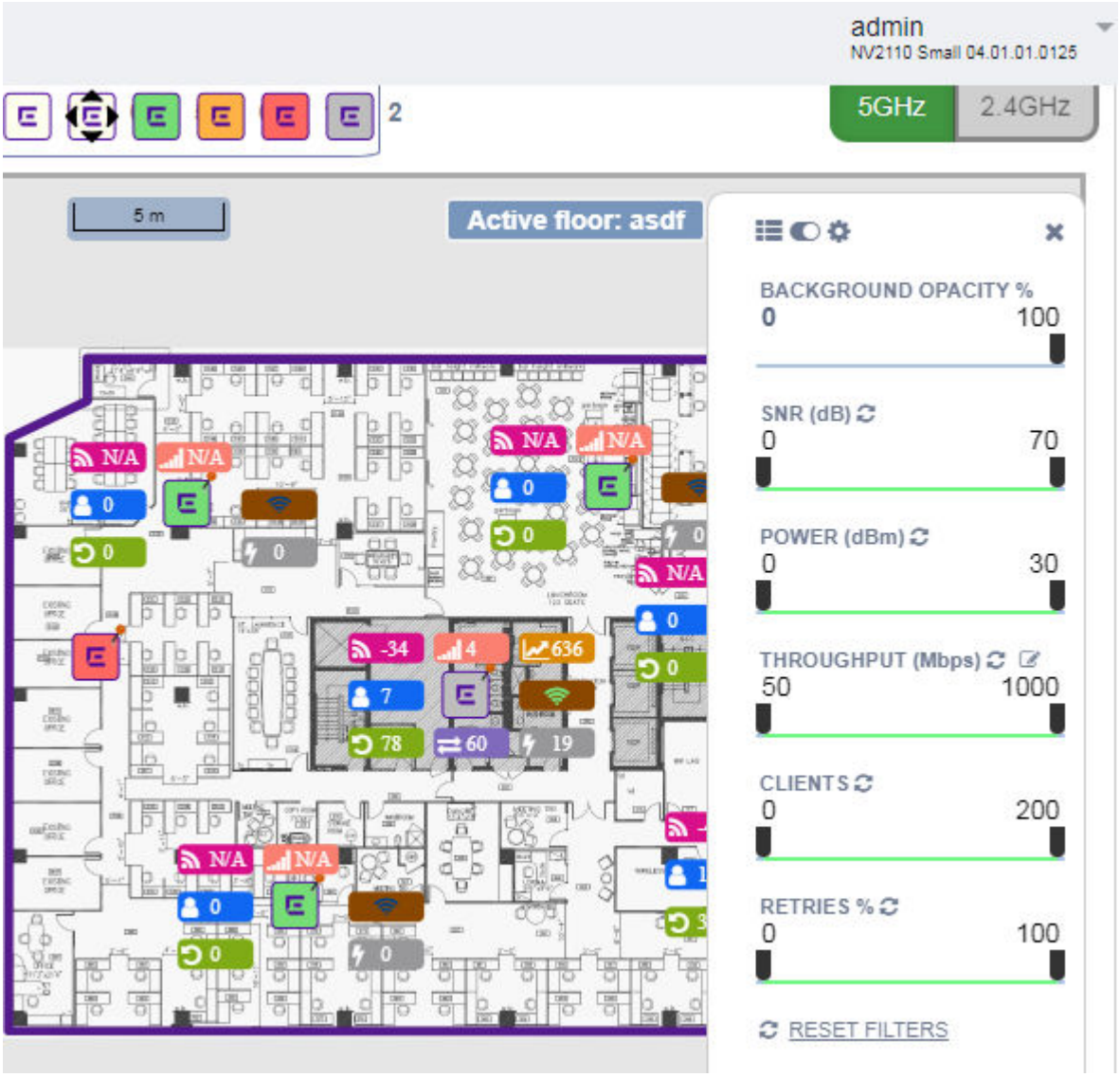


Figure 18: Badges that meet filter criteria appear on map

Understanding Readiness Maps

ExtremeCloud IQ Controller **Floor Plans** view offers heat maps to illustrate network readiness, performance, and optimum positioning. The following readiness maps are available:

- Heat map. RSS signal strength.
- Heat map: BLE. Indicates expected coverage of Bluetooth Low Energy. Supported on the 2.4 GHz band for APs with a BLE radio.
- Channels map. Indicates AP channel with the strongest RSS.

- Link Speed.
- RFQI (RF Quality Index) of the radios enables you to quickly identify APs with poor RF quality. The labels themselves are color coded to indicate overall RF quality of the AP based on the signal strength of the clients connected to them and the retry rates. If there are no clients, there is no measurement.

In addition, see Positioning for details about heat maps that indicate optimal positioning of an AP.

To access the maps:

1. From the right panel, select **Maps** to display a list of map types.
2. To activate a map, select the ball and drag to the right.

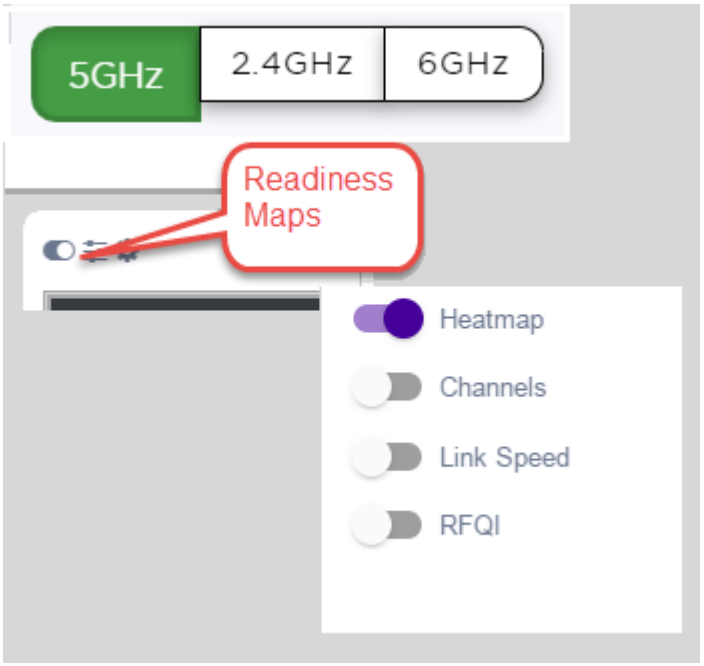


Figure 19: Network Readiness Maps

Right-click anywhere on a heatmap to view the numeric value at that location on the map.

Figure 20: Push-Pin Reading for Heatmap Values

You also have the option to **Select All APs** or **Deselect All APs**. Use these options in addition to individual AP selection to more easily control which APs are selected.

Use Cases: If you want all but one AP selected:

1. Select **Select All APs**.
2. Right-click on the AP that you *don't* want.
3. Select **Exclude AP from Simulations**.

If you only want one AP selected:

1. Select **Deselect All APs**.
2. Right-click the AP that you *do* want selected.
3. Clear the check box **Exclude AP from Simulations**.

Related Topics

Positioning Heatmaps on page 67

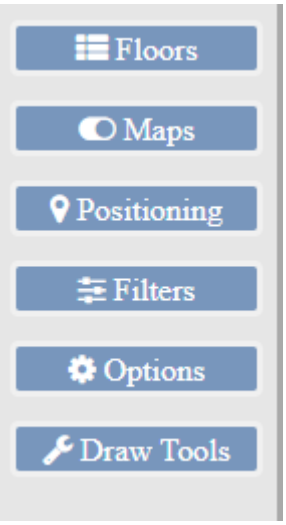
Positioning Heatmaps

ExtremeCloud IQ Controller **Floor Plans** view offers **Positioning** heat maps to illustrate optimal device location and client foot traffic. The following Positioning maps are available:

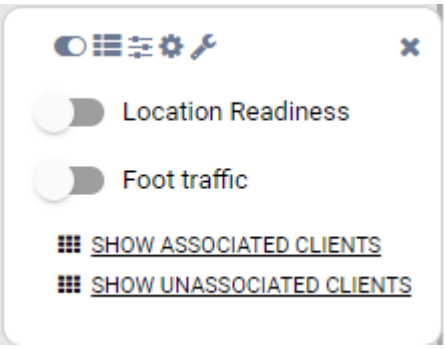
- Location Readiness. Predicted location quality.
- Foot Traffic (Supported on AP39xx only).

To access the Positioning maps from the floor plan view:

1. Display an available floor plan.
2. From the right panel, click **Positioning**.



3. To activate a map, click the ball and drag to the right.



4. To show clients, select either **Show Associated Clients** or **Show Unassociated Clients**.

Note
If your Positioning Profile is configured to track only active clients, you will not be able to see unassociated clients on the map.

Related Topics

Understanding Readiness Maps on page 64
Positioning Profile Settings on page 169

Position Aware Services on page 35

Smart RF Widgets Per Site

You can also get Smart RF information at the site level. To view Smart RF data for a site:

1. Go to **Monitor** > **Sites**.
2. Select a site.
3. Select **Smart RF**.

Figure 21 illustrates the following RF data for the selected site:

- Number of device groups with Smart RF Monitoring enabled.
- Number of device groups with Smart RF Monitoring disabled.
- Number of device groups using Automatic Channel Selection (ACS). AP39xx access points support ACS as the RF Management policy.
- Number of device groups using Static RF. Static RF represents APs not capable of Smart RF or ACS.

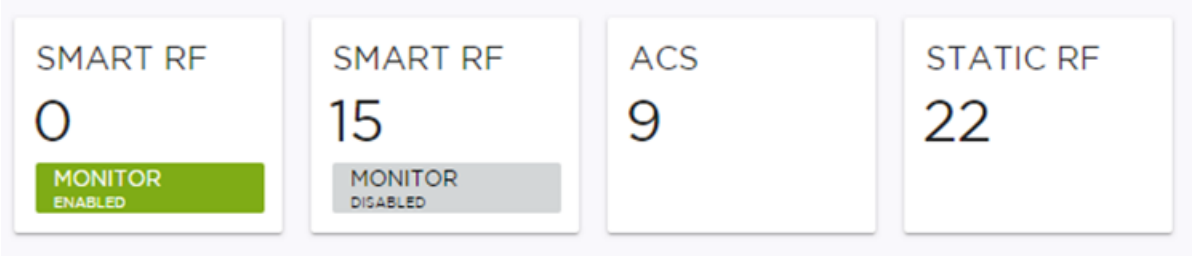


Figure 21: Smart RF data per site

The following data for a site is displayed in the site widgets:

- APs per Power level.
- APs per Channel
- Mitigation
- Mitigation History

Related Topics

Smart RF Widgets Per Device on page 101

Device List

View access points (APs) and switches from **Monitor** > **Devices**.

- See Access Points List on page 69 for a list of supported APs.
- See the ExtremeCloud IQ Controller Release Notes for a list of supported switches.
- ExtremeCloud IQ Controller supports Extreme Defender Adapter SA201 for the Defender for IoT solution. For more information on Extreme Defender for IoT, refer to documentation located in the Extreme Networks documentation portal.

Related Topics

Understanding Access Point States on page 72

Adoption Rules on page 318
Add APs on page 212
Add or Edit a Configuration Profile on page 134
Advanced AP Radio Settings on page 153
Network Snapshot: AP Details on page 84
Opening Live SSH Console to a Selected AP on page 98
Packet Capture on page 93
Switches on page 239

Access Points List

Go to **Monitor** > **Devices** > **Access Points** to see a list of APs in ExtremeCloud IQ Controller.

The model and licensing domain of the AP determine the site configuration type and site licensing domain. The configuration Profile and RF Management for a device group are specific to the AP platform.

The **Country** option on the site must support the AP licensing domain.

Highlights on the **Access Points List**:

- The **MAC Address** column displays the AP MAC Address of the primary port. Use this information to identify the AP and facilitate integration processes.
- The **Profile** column indicates which configuration Profile the AP is associated with. A configuration Profile is defined at the device group. It applies configuration settings to the group.
- The **Radio 1 Clients**, **Radio 2 Clients**, and **Radio 3 Clients** columns indicate the client count on each radio. This information enables you to monitor load balancing on the AP. The value Sensor, in this column, indicates that the radio is configured as a sensor. For more information, see Radio as a Sensor on page 152.
- The **Radio Mode** columns indicate the mode for each radio on the AP. Use the Radio Mode columns to indicate that an AP is configured as a Client Bridge. The Radio Mode column value for a Client Bridge AP is **bridge**.
- The **Adoption** column indicates if the AP is associated with the Primary or Backup ExtremeCloud IQ Controller in an availability pair. Use this information to understand an access point's home session. This value *does not* indicate where an AP may be currently connected in an availability pair.
- The **Tunnel** column on the Access Point List displays which controller the AP has an active tunnel to. Possible values are:
  - Primary — The AP has an active tunnel to the primary controller in an availability pair.
  - Backup — The AP has an active tunnel to the secondary controller in an availability pair.
  - N/A — Indicates that an active tunnel does not exist or that there is a configuration entry for the AP, but the AP is not currently connected.
- The **Overrides** column indicates that the AP has overrides. To view which override settings are enabled, select the AP and go to **Advanced** > **Overrides**.

- The **Ethernet Port Speed** and **Ethernet Port Mode** are available for each port on a selected device:
  - When the interface is connected, port speed and mode display.
  - When an available port is disconnected, the value is **NC** (Not Connected).
  - For single port AP models, the value for the second port is **NA** (Not Available).
- The two **Switch Port** columns display the MAC address of the switch to which the selected AP is connected. Use this information to quickly access a switch that may be associated with a service escalation. Port information also aides in validating configuration and diagnostic functions.
- The **CERT** column indicates that a Certificate Signing Request (CSR) certificate has been applied to the AP.
- The **Force Normal Power Operation** column indicates that the AP will draw normal power from the POE switch port for full-capacity operation regardless of the IEEE 802.3 ft/at/bt and or LLDP-MED power switch port negotiation. The defined power level for full-capacity power operation is unique for each AP model.

  Note
  Use this setting with caution. Improper use can result in an AP power source overload, resulting in an unstable AP operation.

- The **Pwr Source** column — Indicates if the AP is operating with BT (802.3BT), AT(802.3AT), AF, or DC. (Only AP5010 supports BT.)
- The **Power Status** column value depends on the AP model:
  - For AP5010, possible values are: High, Normal, or Low.
  - All other AP models, possible values are: Normal or Low.

Note
The **Power Source** column has been deprecated and will therefore display None.

Use **Auto Refresh** to automatically refresh the information presented. From the **Auto Refresh** drop-down field, select the refresh value. Valid values are:

- OFF
- 30 Seconds
- 1 Minute
- 3 Minutes
- 5 Minutes

You can also select to manually refresh the page anytime.

Note
Save your page setting changes. **Auto Refresh** is implemented at the browser level and therefore will reset any selections or unsaved page setting changes. When using **Auto Refresh**, select a refresh interval that allows you to complete the operation within the defined interval. For best results, set **Auto Refresh** to OFF during configuration selections or selection of a large number of elements.

Supported ExtremeWireless™ Access Points

The following ExtremeWireless™ access points are supported by ExtremeCloud IQ Controller:

ExtremeWireless Wi-Fi 6E World-Wide Universal Access Points

ExtremeCloud IQ or On-premise operation:

- AP3000/X
- AP4000
- AP4000-1
- AP5010
- AP5050U/AP5050D

ExtremeWireless Wi-Fi 6 Universal Access Points

ExtremeCloud IQ or On-premise operation:

- AP302W
- AP305C/CX
- AP305C-1
- AP410C
- AP410C-1
- AP460C/S6C/S12C

ExtremeWireless Wi-Fi 6 Access Points

On-premise operation only:

- AP310i/e
- AP310i/e-1
- AP410i/e
- AP410i-1
- AP460i/e
- AP505i
- AP510i/e
- AP510i-1
- AP560i/h

ExtremeWireless Wi-Fi 5 Access Points

On-premise operation only:

- AP3917i/e/k
- AP3916ic
- AP3915i/e
- AP3912i
- AP3935i/e
- AP3965i/e

The Extreme Networks Defender Adapter SA201 is supported.

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

For documentation on each AP model type:

1. Go to Extreme Networks documentation.
2. Scroll down to **Wireless & Mobility**.
3. Select the AP model type.

Note
Most AP radio properties depend on a regulatory domain; which is defined at the site level. Devices that are connected to ExtremeCloud IQ Controller but not assigned to a device group have the status of *In-Service Trouble*. Devices that have not discovered ExtremeCloud IQ Controller have the status of *Unknown*.

Related Topics

Understanding Access Point States on page 72
AP Actions on page 206
Radio Settings Button on page 55
Add APs on page 212
Add a Site on page 130
Device Groups on page 32
Configuring Column Display on page 43
Advanced Setting Overrides on page 221
AP Certificates on page 209
Universal AP Operational Modes on page 24
Support for World-Wide Universal Access Points with Wi-Fi 6E Technology on page 15

Understanding Access Point States

The following describes access point states on the **Access Points Device List**.

Table 14: AP State from the Device List

State	Description
	In-Service. Device has discovered ExtremeCloud IQ Controller and is providing service.
	Indicates which AP in a Distributed site acts as the domain manager (RFDM). The RFDM communicates directly with ExtremeCloud IQ Controller collecting statistics, access point upgrade information, and Smart-RF activities. Understanding which AP is the RFDM can help with troubleshooting.
	In-Service Trouble. Device has discovered ExtremeCloud IQ Controller but it is not a member of a device group.

Table 14: AP State from the Device List (continued)

State	Description
	Unknown. Device is added to ExtremeCloud IQ Controller but the device has never discovered ExtremeCloud IQ Controller.
	Critical. After being Active, Discovered, and Onboarded, associated device is no longer connected to ExtremeCloud IQ Controller.
	Indicates that the AP is in the process of upgrading.

Note
Most AP radio properties depend on a regulatory domain; which is defined at the site level. Devices that are connected to ExtremeCloud IQ Controller but not assigned to a device group have the status of *In-Service Trouble*. Devices that have not discovered ExtremeCloud IQ Controller have the status of *Unknown*.

Query Builder

Create custom filters with Query Builder, specifying criteria for each available column (regardless of whether it is selected for display) and view query results in pie chart format. For example, you can determine how many APs are on a given channel. Device results include all configured APs regardless of their current status.

Build customized queries to filter data from the following areas in ExtremeCloud IQ Controller:

- **Monitor** > **Devices** > **Access Points** > **AP List**
- **Monitor** > **Clients** > **Client List**
- **Tools** > **Logs**.

After you build and execute a query, the distribution for a selected column (and client duration) is rendered for visualization. The visualization is limited to elements returned by the query. The selected column for visualization is preserved after you log out. When you log in again, your selection is preserved.

Note
Query operations for all three pages are the same, but the **Logs** page does not support further visualization.

The queries for each grid can be named, edited, and deleted, up to 10 queries per grid.

Related Topics

Build a Query for Devices or Clients on page 73
Build a Query for Logs on page 377

Build a Query for Devices or Clients

This topic outlines how to build a query to filter data on the **AP List** and **Client List**. To build a query for Logs, see Build a Query for Logs on page 377.

Take the following steps to build a customized query, filtering data on the **AP List** and **Client List** pages, and viewing results in pie chart format:

1. To access the **AP List** page:

   Go to **Monitor** > **Devices** > **Access Points**. Or,

   Go to **Configure** > **Devices** > **Access Points**.
2. To access the **Clients List** page, go to **Monitor** > **Clients**.
3. To open Query Builder, select  .
4. Select a listed query or select  to open the **Query Builder** dialog.
5. To create a new query, select **Group**.

   Query Builder starts with a logical group of conditions. You can add more groups, joined with query conditions. Valid conditions between two or more groups:

   - AND
   - OR

   Note
   AND is the only supported condition within a group.
6. From **Source Field**, select a value that represents a column used in the query.
7. Select the **Comparison Operator**.

   The available operators depend on the data type. Number types offer comparisons such as greater or less than. Valid values are:

   - Equals
   - Not Equals
   - Contains
   - Greater Than
   - Less Than
   - Less or Equals
   - Greater or Equals
8. Under **Search Condition**, provide the value that you are searching for.

   Selecting the **Search Condition** field displays a drop-down of existing values. The list is filtered as you type. Wildcards are not supported. To match a portion of the search condition, use the operator **Contains**.

   - Select **+** to add more conditions.
   - Select **-** to remove conditions.
9. To add another condition row, select **+**.
10. **Group** — Each group has conditions joined by the selected operator. You can add additional groups or add conditions to the group.

11. To run the query, select **Execute**.

    The query is automatically saved. AP List queries are saved separately from Client List queries. The filter icon is highlighted to indicate that a query is in effect.

Note
Query Builder generates a Pandas query syntax. The syntax preview is displayed at the top of the **Query Builder** dialog. For saved queries:

- Select to view the Pandas query.
- Select to copy the Pandas query to the clipboard.

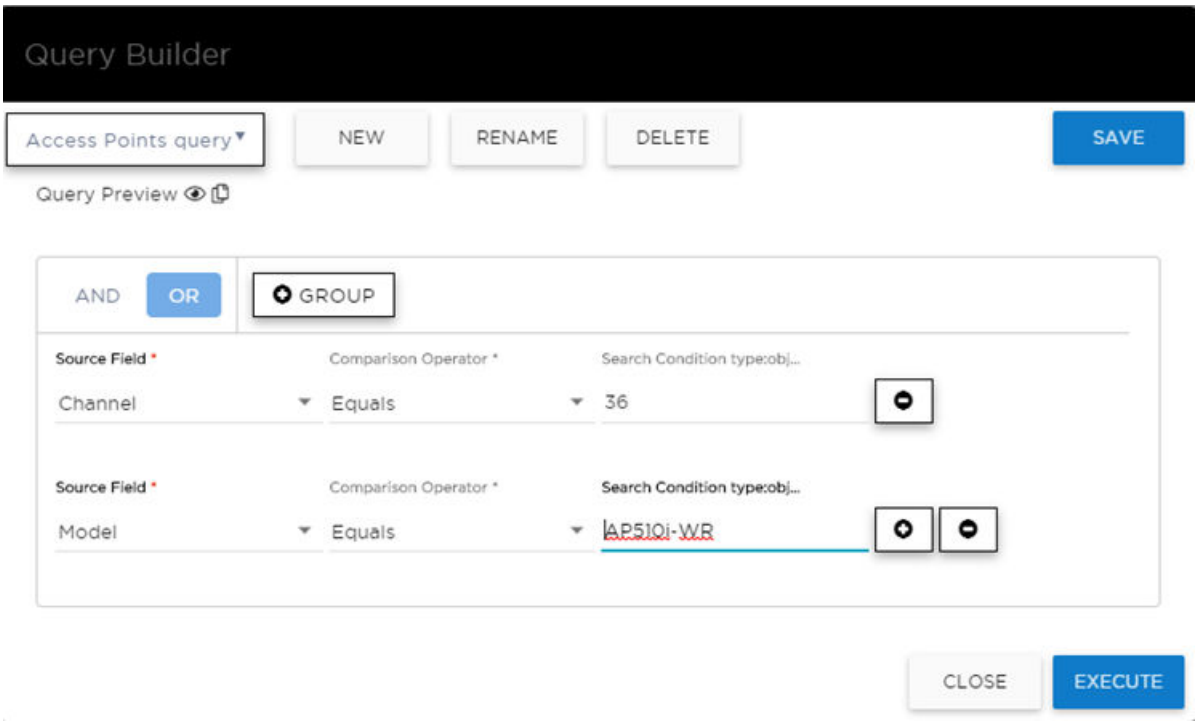


Figure 22: Query Builder: Channel distribution by AP model per site

Select from the list of saved queries or create a new query.

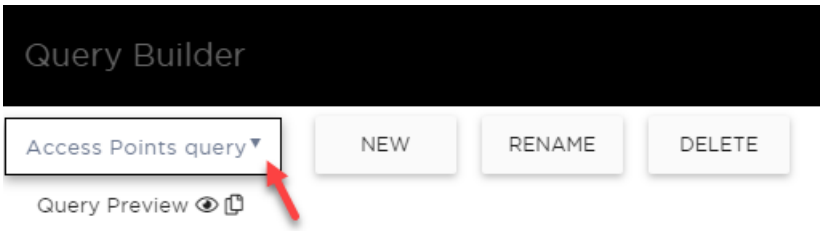


Figure 23: List of saved queries

Query Builder actions:

- **New**. To create a new query, provide a name and select **OK**. There is a limit of 10 saved queries per user, per grid. After the 10-query limit has been reached, the **New** button is unavailable.
- **Rename**. Rename an existing query.
- **Delete**. Delete the query that is currently displayed.
- **Close**. Close the Query Builder dialog. If you close Query Builder without running the query, your query details are deleted.
- **Reset**. Close the Query Builder dialog and save the current query. The next time you open Query Builder, this query will display. This option is available after you run a specific query.
- **Execute**. Run the query and save it.
- **Save**. Save changes without executing the query. Save is only visible when changes have been made.

Related Topics

Visualize a Query on page 76
Query Builder on page 73
Build a Query for Logs on page 377

Visualize a Query

Note
The **Logs** page does not support visualization.

To visualize your query:

1. Select .
2. Select the column with the data element you want displayed.
3. Select **Render**.

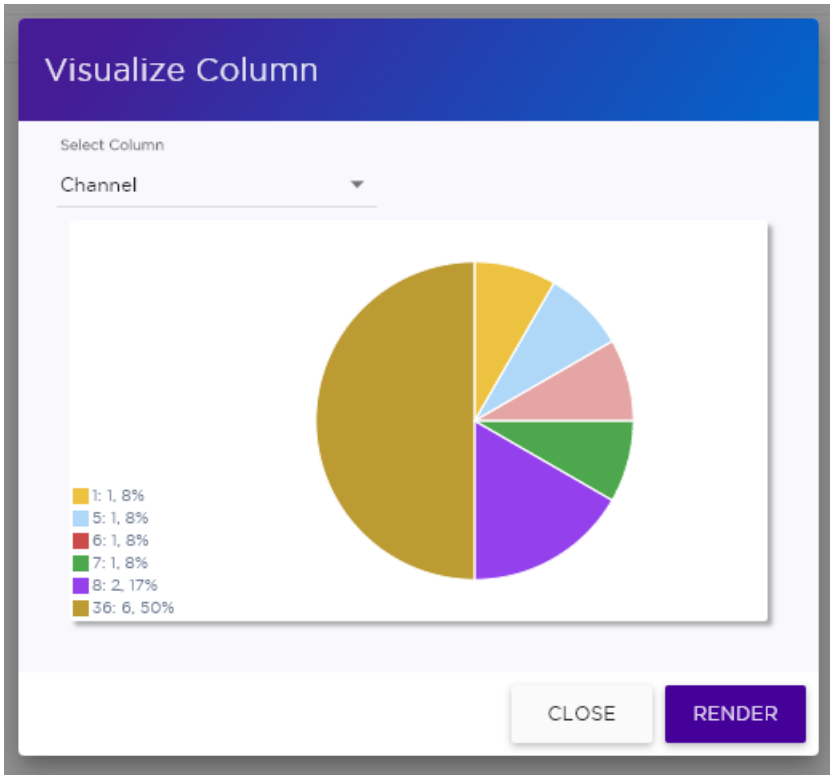


Figure 24: Channel Assignment for AP410i-CAN associated with Site Thornhill

The pie chart in Figure 24 shows selected APs by channel assignment. The query filters all AP410i-CAN access points that are associated with site Thornhill. This column selection is preserved after you log out. You can access this information again when you log in.

For results with more than 10 items, the chart includes pages, and the percentage calculation reflects the global total.

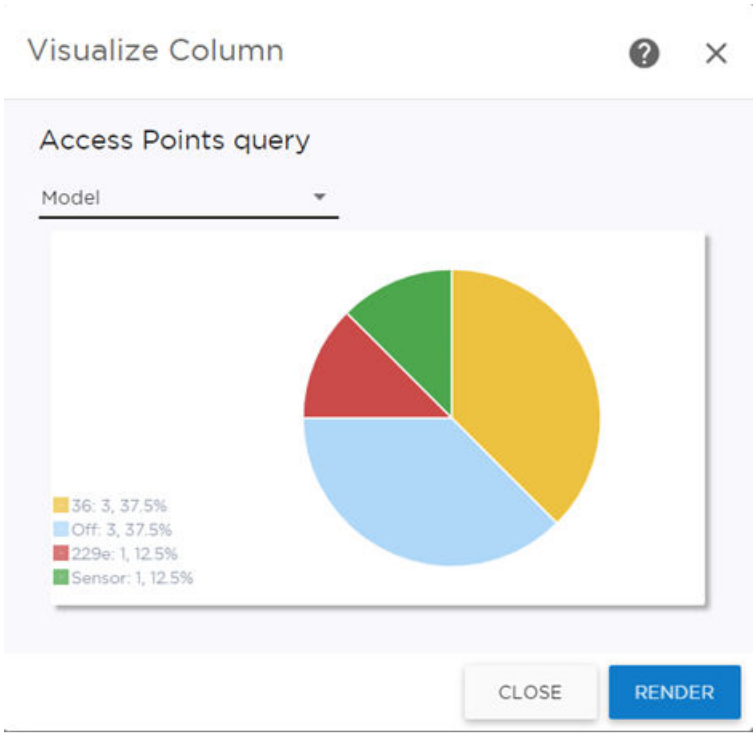


Figure 25: AP count by model number

Related Topics

Build a Query for Devices or Clients on page 73
Query Builder on page 73

Support for ExtremeWireless AP3xx Access Points

ExtremeCloud IQ Controller supports the ExtremeWireless™ AP302W, AP305C, AP310i/e, AP310i-1 indoor access points and the AP305CX and AP360i/e outdoor access points.

Table 15: Radio Configuration and support for AP3xx

AP Model	Radio Configuration
AP302W	• Universal AP with two operating modes: on premise and cloud-enabled. For more information, see Universal AP Operational Modes on page 24. • Radio Modes: ◦ Mode 1 — Dual-band concurrent operation ◦ Mode 2 — Radio 1 dual-band sensor, Radio 2 5GHz traffic forwarder ◦ Mode 3 — Radio 1 5GHz Low band, Radio 2 5GHz High band traffic forwarder • Ports on the Universal APs are labeled with the prefix ETH. ◦ ETH0 — 1GHz Uplink port (No LAG or Layer 2 backup function support.) ◦ ETH1, ETH2, ETH3 — Local network client wired ports. ◦ Pass-Through ports. Hardware wired ports, no software support needed. • PKI support, IPsec tunnel security • Client Bridge is supported. • Mesh Network is supported. • Internet of things (IoT) devices are supported.
• AP305C/CX • AP305C-1	• Universal AP with two operating modes: on premise and cloud-enabled. For more information, see Universal AP Operational Modes on page 24. • 2.4/5GHz dual-band Sensor. ◦ Mode 1 — 2.4GHz service radio and 5GHz service radio ◦ Mode 3 — 5GHz lower band service radio and 5GHz upper band service radio • AP305C/CX — IoT is supported. • AP305C-1 — IoT is not supported. • Client Bridge and Wired Mesh Network extension are supported: ◦ When Client Bridge is configured on a single interface AP, the single interface is used as the client port, not as an uplink, and you will not see the **GE2 Port Function** field in the configuration Profile **Advanced Settings**. ◦ When a single interface AP is configured as a Mesh non-root AP, the single interface is used as a client port, not as an uplink.

Table 15: Radio Configuration and support for AP3xx (continued)

AP Model	Radio Configuration
	◦ When a single interface AP is configured as a Mesh root, the single interface is used as an uplink, not as a client port.
• AP310i/e • AP310i/e-1 • AP360i/e	• One dual-band 2.4GHz/5GHz radio and one 5GHz radio. ◦ Mode 1 — 2.4GHz service radio and 5GHz service radio ◦ Mode 2 — 2.4/5GHz dual-band Sensor and 5GHz service radio ◦ Mode 3 — 5GHz lower band service radio and 5GHz upper band service radio • AP310i/e and AP360i/e — IoT is supported. • The AP310i/e-1 — IoT is not supported.

Related Topics

Understand Radio Mode on page 147
Radio as a Sensor on page 152
Professional Install Settings on page 231
Universal AP Operational Modes on page 24

Support for ExtremeWireless AP4xx Access Points

ExtremeCloud IQ Controller supports ExtremeWireless™ AP410i/e, AP410i-1, AP410C, AP410C-1, and AP460i/e, AP460C, AP460S6C, or AP460S12C access points.

The APxxxC models are Universal APs that support two operating modes: on premise and cloud-enabled. For more information, see Universal AP Operational Modes on page 24.

The access points feature built-in dual-band radios, two band-locked radios, up to eight Wi-Fi internal or external antennas, and one Bluetooth Low Energy (BLE) antenna. Internet of things (IoT) is supported on most AP410 and AP460 models.

Note
AP*model*-1 access point models do not support IoT.

The AP4xx series access points offer three radios:

- Radio 1 — WLAN Service
  - AP410i/e and AP460i/e (2.4 GHz)
  - AP4xxC — (2.4/5.0 GHz) supports (a/n/ac/ax) and (a/n/ac).
- Radio 2 (5.0 GHz) — WLAN Service (For all models).
- Radio 3 — Dedicated sensor

Related Topics

Understand Radio Mode on page 147

Radio as a Sensor on page 152
Professional Install Settings on page 231

Support for ExtremeWireless AP5xx Access Points

ExtremeCloud IQ Controller supports ExtremeWireless™ AP505i, AP510i/e, AP510i-1, AP560i/h/m/t/u access points. These access points support more users and internet of things (IoT) devices. In addition to both internal and external antennas, these APs support a Bluetooth Low Energy (BLE) antenna.

- AP510i/e indoor, one dual band 2.4GHz/5GHz radio and one 5GHz radio.
  - Mode 1 — 2.4GHz service radio and 5GHz service radio
  - Mode 2 — 2.4/5GHz Sensor and 5GHz service radio
  - Mode 3 — 5GHz lower band service radio and 5GHz upper band service radio
  - Radio Channels:
    - Radio 1 can operate as:
      - 2.4GHz with all 2.4GHz channels
      - 5GHz lower band with 5GHz lower band channels (channels 36-64)
      - 2.4/5GHz Sensor scanning and 2.4GHz and 5GHz channels
    - Radio 2 can operate as
      - 5GHz upper band with 5GHz upper band channels (channels above 100)
      - 5GHz Full with 5GHz full channel list

    Note
    The AP510i-1 does not support IoT and the 5GHz radio does not support 160MHz operation.
- AP505i indoor, one 2.4GHz radio and one 5GHz radio.
  - Mode 1 — 2.4GHz service radio and 5GHz service radio. Can be used as a dedicated sensor.
- AP560i/h outdoor. The AP560i/h will follow the AP510 mode of operation depending on the power source.
  - **Normal Mode**

    AP560 requires AT power (25W) to operate in normal mode with full performance. The AP must be powered from one of the following scenarios:
    - Ethernet port (GE1 PoE) connected to an AT switch port and Ethernet port (GE2) not connected
    - Ethernet port (GE2 PoE) connected to an AT switch port and Ethernet port (GE1) not connected
    - Both Ethernet port (GE1 PoE) and Ethernet port (GE2 PoE) connected to an AT switch port
    - External power supply.
  - **Low Power Mode**

    When power source is AF (14.5W), the AP operates in Low Power mode with limited performance. The AP560 operates in Low Power mode when GE1 or GE2

is connected to AF switch port and no external power is connected. The following are AP560 Low Power Mode limitations:

- MODE 1: dual band concurrent and MODE 2: sensor and 5GHz data forwarder:
  - Radio 1 will be limited to 2x2 and max power 16dBm
  - Radio 2 will be limited to 2x2 and max power 16dBm
- MODE 3
  - Radio 1 will be limited to 2x2 and max power 18dBm
  - Radio 2 will be limited to 2x2 and max power 0dBm (providing no service).

Note

When both ports on a dual-port AP are powered, the port with the lowest power determines the power result.

The AP Override setting **Force Normal Operation** can be enabled, indicating that the AP is configured to operate with the normal, full-power capacity regardless of a detected AP power restriction. This setting is intended for expert users. For more information, see Advanced Setting Overrides on page 221.

The AP560 is offered in a product bundle that targets the installation environment. Refer to Table 16 and Table 17 on page 83 for descriptions of each product bundle.

Table 16: AP560i portfolio

AP Model Number	Description
AP560m-FCC	The AP560m is a pole-mount bundle that includes the AP560i access point and the following brackets: ◦ KT-147407-02 bracket kit ◦ KT-150173-01-ExtArm Features include: ◦ Outdoor, one 2.4GHz radio and one 5GHz radio ◦ 4x4 on both radios ◦ Software Programmable ◦ Internal Antenna ◦ Mounting Brackets included. For more information, see the AP560m documentation.
AP560u-FCC	The AP560u is an under-seat solution bundle that includes the AP560i access point and the following items: ◦ EIO-03 under-seat housing kit ◦ WS-EIO-02 Silicone rubber kit (#30524) Features include: ◦ Outdoor, one 2.4GHz radio and one 5GHz radio ◦ 4x4 on both radios ◦ Software Programmable ◦ Software Selectable Internal Antenna For more information, see the AP560u documentation.

Table 17: AP560h portfolio

AP Model Number	Description
AP560h-FCC	The AP560h is a stadium optimized access point, supporting a high density of users and devices. The AP560h offers flexible deployment options and can be mounted to a pole, a wall, and to other access points. Requires the following mounting brackets: ◦ 30520 (WS-MBOPOLE01) Bracket ◦ WS-MBOART02; 10" 2-Axis extension arm Features include: ◦ Outdoor, one 2.4GHz radio and one 5GHz radio ◦ 4x4 on both radios ◦ Software Programmable

Table 17: AP560h portfolio (continued)

AP Model Number	Description
	◦ Software Selectable Internal Antenna ◦ Overhead solution For more information, see the AP560h documentation.
AP560t-FCC	The AP560t is an access point bundle that includes the AP560h access point and the following brackets: ◦ 30520 (WS-MBOPOLE01) Bracket ◦ WS-MBO-ART02 Extension Arm

Related Topics

Understand Radio Mode on page 147
Radio as a Sensor on page 152
Professional Install Settings on page 231
Advanced Setting Overrides on page 221

Network Snapshot: AP Details

To view network details from the AP screen:

1. From the left pane, select **Monitor** > **Devices** > **Access Points**.

   The **Access Points** list opens.
2. Select an AP.

   The network details for the selected AP display.

   If the AP is configured on a mapped floor plan, a map displays showing the AP location with all associated clients. Select the map to open the floor plan view.

   If there is no map, the Topology diagram displays.
3. You can also:

   Select ⚙ to modify configuration settings.

   Select ☰ to go back to the list.

AP Details

The following details are available for each AP. Details may differ based on the AP model.

- IP Address
- MAC Address
- Serial Number
- Model
- Software Version
- Country

- Eth Power Status
- Radios — Indicates the following information for each AP radio:
  - Radio Index
  - Mode
  - Channel — Indicates channel number and the channel selection mode:

    Green — Fixed Channel
    Purple — SmartRF
    Blue — Mesh ACS / Client Bridge
  - Channel Width
  - Power Level — Indicates power level per chain or total power level depending on the global Tx value setting.

Table 18: Tabs on the AP Details Screen

Tab	Description
Dashboard	Network charts provide client count and radio channel data. Use this information to determine network traffic associated with the AP and channel statistics.
Sites	Sites that include this AP. Click the site to show details.
Networks	List of network services associated with the device. Click a network to show network details.
VLANs	Details about AP Tunnel status for the selected AP and VXLAN information related to MTU packet size. For more information, see AP Tunnel Information on page 91. **Note:** Supported on Wi-Fi 6 AP models.
Roles	List of Roles associated with the device group, of which this device is a member.
Clients	List of clients associated with the AP. Add or remove clients from Allow and Deny lists.
Troubleshooting	Offers packet capture at the AP, remote console access to the AP, and Smart Poll reporting.
Smart RF	View widgets that show information about the following: • Mitigation • Occupancy and neighbor channels • Peer AP visibility.
Certificate	Current credentials in use by the AP.
AP Events	AP Event Report that offers various historical information about AP events.

Related Topics

AP Tunnel Information on page 91
AP Widgets on page 86
Smart RF Widgets Per Device on page 101
View AP Events — Single Access Point on page 104
Sites Overview on page 30
Opening Live SSH Console to a Selected AP on page 98
Packet Capture on page 93
Floor Plans on page 35
Global Client Access Lists on page 117

AP Widgets

The following widget reports are available from the AP dashboard:

- Topology/Map. Toggle between a topology diagram and a floor map. The Topology diagram represents the AP switch port connection information. The Map diagram indicates where the AP is installed on an associated floor plan.
- Device Utilization. Provides metrics on throughput and data usage for each AP and clients associated with the AP.
- RF Management. Provides metrics on radio frequency quality, channel utilization, channel noise, load, signal to noise ratio (SNR) levels, and client retry statistics.
- Clients. Provides metrics on client distribution by protocol, operating system, and manufacturer per AP.
- Expert: AP metrics for the expert user related to RFQI, RTT, RSS, and RX and TX Rates.
- Application Visibility. Provides details about applications the client is accessing and metrics on application groups related to throughput and usage per AP.

To view widgets for an individual AP:

1. Go to **Devices** > **Access Points**.
2. Select an AP from the list and review the widgets on the **Dashboard** page.

Filter by radio band. Select to display data for a specific radio band.

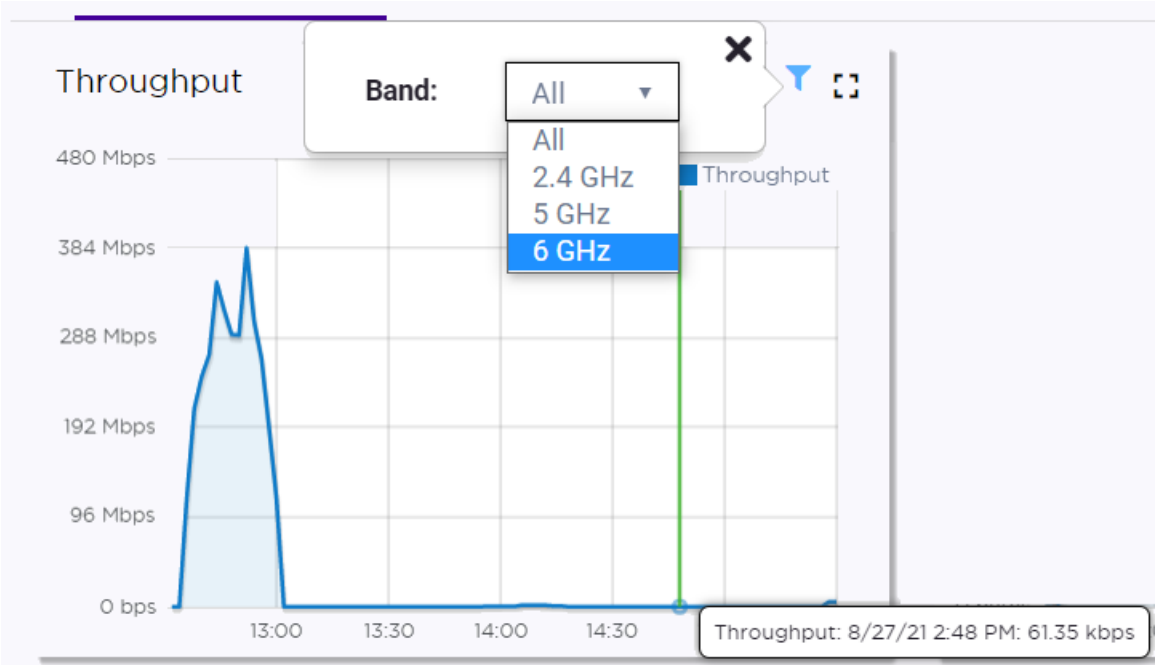


Figure 26: 6 GHz Band Throughput

Note
The datasets are sampled at different intervals. Therefore, it is possible that data from the 14-day dataset will not include data from the 3-day dataset or from the 3-hour dataset. It is possible that a new client will not appear in a dataset if the dataset has not been recently updated.

Related Topics

LLDP Switch Port Connectivity on page 87
Add a New Dashboard on page 47
Modify a Dashboard on page 48

LLDP Switch Port Connectivity

The Topology diagram displays the selected AP port connection to one or more switches, which are connected to ExtremeCloud IQ Controller. The diagram (shown in Figure 27) represents the relationship between an AP, a switch, and ExtremeCloud IQ Controller, displaying the link speed between the AP ports and the switch ports, and connection status with ExtremeCloud IQ Controller.

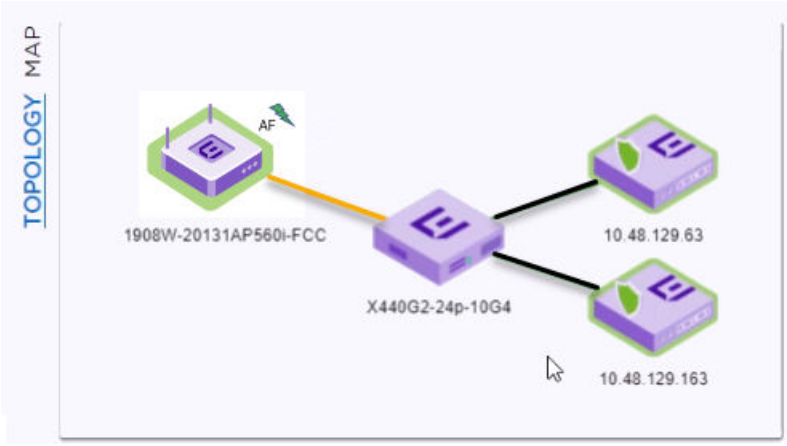


Figure 27: Topology Map representing LLDP Port Connectivity

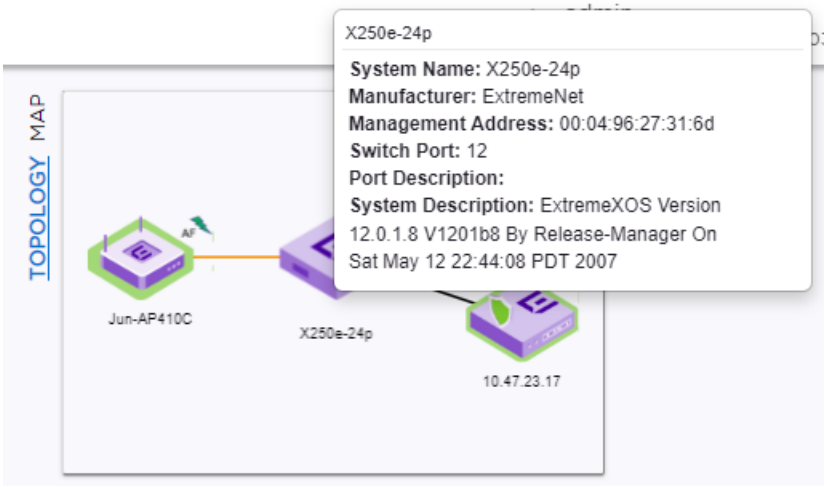


Figure 28: Extreme Switch data

Figure 29 describes each Topology Map icon with status.

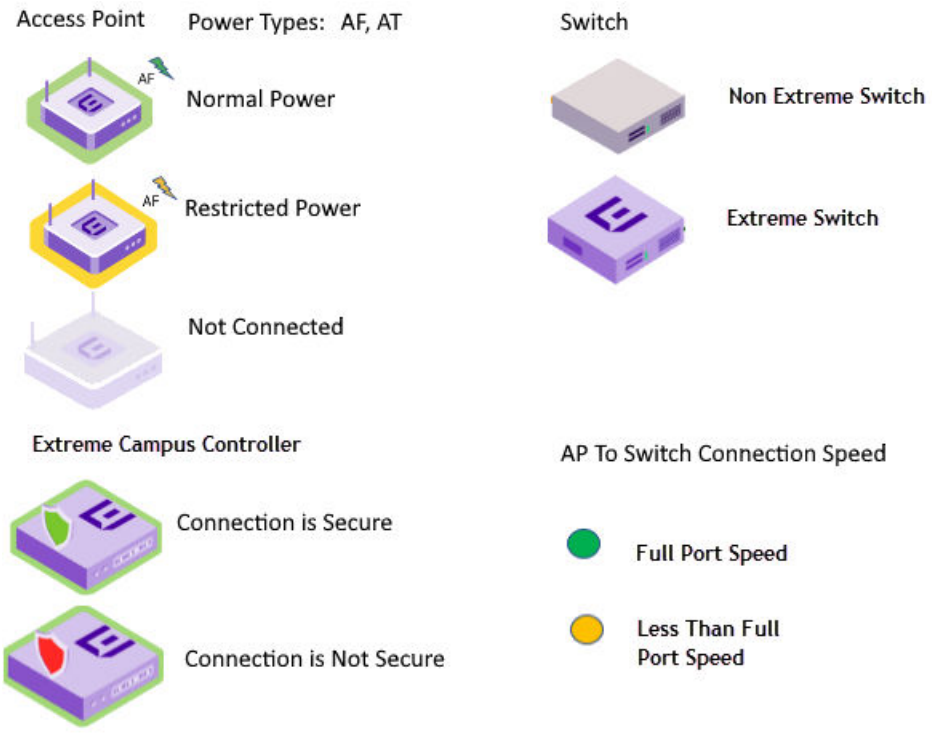


Figure 29: Topology Map Legend

Note
If the Link Layer Discovery Protocol (LLDP) is not enabled on the switch, LLDP data is not available.

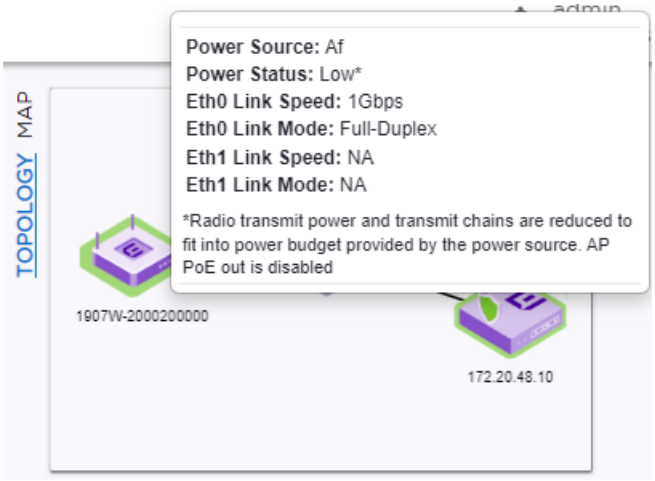


Figure 30: LLDP data not available

The AP reports switch port connection details to ExtremeCloud IQ Controller. Reported properties include the following:

AP

The AP reports the AP Name and Power Source. Power Source values include normal and restricted levels for the following:

- AF
- AT

Switch

When both LLDP (Link Layer Discovery Protocol) and TLV (Type Length Value) advertisement are enabled, the switch reports the Switch Port and System Name. If only the LLDP is enabled, the switch Port Number displays. If the LLDP is not enabled on the switch, the switch is a gray icon.

ExtremeCloud IQ Controller

ExtremeCloud IQ Controller reports the controller Connectivity Status and IP address.

The connection status is indicated as follows:

Green

- A green lightning icon with a green icon border indicates that the AP power level is normal.
- A green shield on the controller indicates that an AP secure tunnel is enabled for the AP connection to ExtremeCloud IQ Controller.
- A green line indicates that the port speed between the AP and switch is the maximum AP port speed. Refer to Table 19 on page 90.

Yellow

- A yellow lightning icon with a yellow icon border indicates that the AP power level is low.
- A yellow line indicates that the port speed between the AP and switch is less than the maximum AP port speed. Refer to Table 19 on page 90.

Red

- A red shield on the controller indicates that an AP secure tunnel is disabled for the AP connection to ExtremeCloud IQ Controller.

Table 19: Port Speeds per Access Point

AP Model	Port 1	Port 2
AP3xx	1Gb (PoE)	1Gb
AP4xx	2.5Gb (PoE)	1Gb
AP505	2.5Gb (PoE)	1Gb

Table 19: Port Speeds per Access Point (continued)

AP Model	Port 1	Port 2
AP510i/e, AP510-1i, AP560i/h	5Gb (PoE)	1Gb (PoE)
AP4000	2.5Gb (PoE)	1Gb

Note
The Topology map is not supported on AP39xx access points.

Note
If you have configured the selected AP on an associated floor plan, you can view the selected AP on the floor plan map from here. Select **Map** to view the selected AP on the floor plan. For more information, see Floor Plan View on page 56.

Related Topics

Access Points List on page 69
Network Snapshot: Switch Details on page 106
Floor Plan View on page 56

AP Tunnel Information

The **VLANS** tab for a selected device provides status information on the AP tunnel between the AP and the appliance, both for single deployments and for an availability pair. For devices configured with a VxLAN topology, it displays status information for the VxLAN tunnel.

Note
Supported on Wi-Fi 6 AP models.

To view tunnel status information:

1. Go to **Monitor** > **Devices** > **Access Points**.
2. Select an AP.
3. Select **VLANS**.

AP Tunnel

Note
This information *does not* pertain to the GRE Point-to-Point Tunnel feature, which supports tunneling traffic between access points without traversing the controller.

The following information displays for the AP tunnel between the selected AP and the appliance:

IP Address

The IP address of the appliance. In an availability pair, the primary appliance is listed first.

Status

Operational status of the AP Tunnel. Valid values are: Normal and Failed.

Type

Indicates the controller in an availability pair. Valid values are: Active or Backup, referring to the Primary Appliance or Backup Appliance, respectively.

Configured MTU

The Maximum Transmission Unit (MTU) setting for the AP. With Jumbo Frames, this can be up to 1800 bytes. AP MTU is configured in the device group configuration Profile or as an AP override.

Configured MTU Tunnel Status

The status of the MTU tunnel between the selected AP and the appliance. Valid values are Normal and Failed. When the **Configured MTU** value is set to 1800 and this tunnel fails, it indicates that a router in the chain between the AP and the appliance does not support the Jumbo Frames value of 1800 bytes. The MTU values for all devices in the path from AP to appliance must match.

Path MTU Learned by AP

When a router does not support the MTU setting of 1800 bytes, it sends a message back to the AP indicating the MTU value it can support. If necessary, reconfigure the **Configured MTU** value for this AP to match the router setting. The MTU values for all devices in the path from AP to appliance must match.

Internal Management Tunnel

The status of an internal tunnel within ExtremeCloud IQ Controller. Valid values are Normal, Failed, and MTU Failed. If this tunnel fails, contact Extreme Networks Support.

VLANS

The following information displays for configured VLANS:

Name

Topology Name

Mode

Topology type. Valid values are:

- Bridged@AP
- Bridged@AC
- Fabric Attach
- VxLAN

Tagged

A check mark indicates that VLAN is tagged. If you have more than one VLAN on a port, enable tagging to identify to which VLAN the traffic belongs. Ensure that the tagged vs. untagged state is consistent with the switch port configuration. Fabric Attach topologies are always tagged.

VLAN ID

Identifies the VLAN.

I-SID

For **Fabric Attach**. A unique VLAN identifier and a unique I-SID (service identifier). The I-SID range is (0-15999999).

Certificates

Indicates that a certificate has been applied to the AP.

Remote VTEP

For **VxLAN**. The IP address of the tunnel End-Point is referred to as a VxLAN Tunnel Endpoint (or VTEP). The VTEP is the IP address of the network switch. Network switches that act as a VTEP are referred to as VxLAN gateways. There can only be one VTEP per VxLAN topology.

VNI

For **VxLAN**. VxLAN Network Identifier. The VNI is a 24-bit identifier. It can be used in more than one VxLAN topology.

Tunnel Status

For **VxLAN**. Status of the VxLAN tunnel. Valid values are Normal, Failed, and MTU Failed. MTU Failed indicates that the VxLAN MTU setting of 1550 bytes is not supported on another device in the chain between the AP and the appliance. The MTU values for all devices in the path from AP to appliance must match.

Related Topics

Configuring VLANS on page 303
Advanced Configuration Profile Settings on page 172
Advanced Setting Overrides on page 221

Troubleshooting

ExtremeCloud IQ Controller offers tools for troubleshooting connectivity issues between the AP and the appliance. Access the Troubleshooting tools from the dashboard for a selected AP or a selected site.

To access the Troubleshooting tools go to:

- **Monitor** > **Devices** > **Access Points**. Select an AP and select **Troubleshooting**, or
- **Monitor** > **Sites**. Select a site and select **Troubleshooting**.

The following tools are available from the **Troubleshooting** tab:

- AP Packet Capture
- AP Remote Console
- Smart Poll

Related Topics

Packet Capture on page 93
Opening Live SSH Console to a Selected AP on page 98
Smart Poll on page 396

Packet Capture

Use Packet Capture to identify network inconsistencies by intercepting packets from the APs. Packets are captured based on the parameter configurations that you specify.

The **Overview** dashboard offers a packet capture instances widget that displays instances of packet captures to assist with network troubleshooting.

Capture packets from an individual AP or from a site. To capture packets from an individual AP, go to **Monitor** > **Devices** > **Access Points**. Select an access point, then select **Troubleshooting** > **Packet Capture**.

To capture packets associated with a site, go to **Monitor** > **Sites**. Select a site, then select **Troubleshooting** > **Packet Capture**.

Note
Use at least one IP address or MAC address filter when capturing packets from a site.

The packets are logged in a PCAP file. The PCAP file is temporarily stored on the ExtremeCloud IQ Controller that is associated with the AP or site. To view the PCAP file, export the file to a host running Wireshark.

Note
Live Packet Capture is available in addition to the saved file option. After starting Packet Capture, start Wireshark and add the remote interface using the ExtremeCloud IQ Controller management IP address. See the Wireshark documentation for details.

ExtremeCloud IQ Controller supports up to 10 simultaneous instances of packet capture. The maximum PCAP file size is 1GB, stored locally on appliances E1120, E2120, E2122, E3120, E3125 VE6125, and VE6125K. The virtual appliances VE6120, VE6120H, and VE6120K support a 200MB PCAP file. Files can also be stored on a remote SCP server.

Packets can be captured from APs associated with either ExtremeCloud IQ Controller in an availability pair. If the availability connection is disrupted, packet capture stops.

Continuous packet capture is supported. If an AP must restart after a capture has started, the capture will continue after the AP restart. If the appliance must restart, the capture parameters are not preserved.

After packet capture has started, you can change the capture parameters and refresh the capture, continuing to capture without interruption. This feature enables you to modify parameters as you monitor the capture process. There is one PCAP file for each packet capture instance.

- ExtremeWireless AP39xx, Wi-Fi 6 AP models):
  - Up to 4 IP filters can be applied
  - Up to 2 MAC filters can be applied
  - Capture wired and wireless packets simultaneously or independently
  - Capture packet refresh is supported
  - Live Packet Capture is supported.

Related Topics

Configure AP Packet Capture on page 95
Packet Capture Parameters on page 95
Dashboard Widget — Packet Capture Instances on page 97

Configure AP Packet Capture

To enable packet capture on an AP:

1. Go to **Monitor** > **Devices** > **Access Points**.
2. Select an access point (not the check box).
3. Select **Troubleshooting** > **AP Packet Capture**.
4. Configure the packet capture parameters.
5. Click **Start** to start the packet capture.
6. Click **Stop** to stop the packet capture.

   Packet capture stops when capture duration is reached or capture file size reaches 1GB.
7. Click **Active Packet Captures** to display a dashboard that shows the **Packet Capture Instances** widget. The widget lists recent packet capture instances. Active instances display in green and inactive instances display in red. Inactive instances are eventually removed from the widget.

   The file name is automatically generated. The name is based on the AP or site where the capture was initiated plus an internal capture ID.
8. Hover over the capture file and select **Download** to download the file.

Related Topics

Packet Capture Parameters on page 95
Packet Capture on page 93
Dashboard Widget — Packet Capture Instances on page 97

Packet Capture Parameters

Field Name	Field Description
In the **Capture Locations** pane, configure the following settings:	
Appliance Data Ports	Select this option to capture packets to and from the appliance. When capturing appliance data ports, you must configure at least one filter. From the **Add Filters** field, select either IP address or MAC address for the appliance. Only one capture task can apply to the Appliance Data Ports at a time. If more than one capture task is started using the Appliance Data Ports, the last requested task will be started.

Field Name	Field Description
Wired	Enables wired-packet capture on the selected AP. Filter packets on the basis of the direction of packet flow: • **In** — Capture packets received by the AP. • **Out** — Capture packets transmitted by the AP. • **Both** — Capture packets transmitted and received by the AP. This is the default value. Select **Includes Wired Clients** to include wired-packets received and transmitted to and from wired clients associated with the selected AP. This option is disabled by default.
Wireless	Enables wireless-packet capture on the selected AP. Filter packets on the basis of the direction of packet flow: • **In** — Capture packets received by the AP. • **Out** — Capture packets transmitted by the AP. • **Both** — Capture packets transmitted and received by the AP. This is the default value. Specify the radio interface on which to enable wireless-packet capture. • **Radio 1** — Enable packet capture on the AP's radio 1 interface. • **Radio 2** — Enable packet capture on the AP's radio 2 interface. • **Radio 3** — Enable packet capture on the AP4xx radio 3 (Sensor) interface. Available for AP4xx models only. You must configure an ADSP or Positioning profile to capture packets on the sensor radio. • **All Radios** — Enable packet capture on all radio interfaces for the selected AP. This option is selected by default. **Note:** AP39xx, Wi-Fi 6 AP models (Centralized site) support capturing wired and wireless packets simultaneously. The result is one PCAP file that includes both wired and wireless packets.
In the **Settings** pane, specify how you want to determine the length of the packet capture. Specify the duration or manually end packet capture by clicking **Stop**.	
Duration	Packet transfer window. Default value is 5 minutes.
Truncate Packet Size (Bytes)	Number of bytes for the truncated packet. When truncation is configured, the capture collects up to the configured size of the payload (including the IP/UDP/TCP headers). **Note:** TZSP header is always present. If the truncated packet size is zero, the TZSP header remains in the packet.
In the **Filter** pane, filter packets by MAC address, IP address, IP Protocol, or Port. The filters are mutually exclusive and are applied in the order in which they are listed. Enter at least one MAC address or IP address. **Note:** Excessive packet capture degrades network performance. If you are going to enable packet capture on all APs, specify at least one MAC address filter and one IP address filter to avoid performance degradation.	

Field Name	Field Description
Filter by MAC 1 and Filter by MAC 2	Specify one or two MAC addresses to filter packets for capture. When a MAC address is specified, only packets that move to and from the specified MAC addresses are captured. Support for multiple MAC addresses depends on the AP model.
Filter by IP 1 to Filter by IP 4	Specify one to four IP addresses to filter packets for capture. When an IP address is specified, only packets that move to and from the specified IP addresses are captured. Both IPv4 and IPv6 address formats are supported. Support for multiple IP addresses depends on the AP model. When using multiple IP address filters, packets matching any of the IP addresses are captured.
IP Protocol	Specify the protocol to filter for packet capture. Packets matching the specified protocol are captured. Valid values are: • **ICMP** — Captures only ICMP packets. This is the default value. • **TCP** — Captures only TCP packets. • **UDP** — Captures only UDP packets
Port	Specify a TCP or UDP port number. Packets with the matching port number are captured. Use **Port** as an additional filter, or if you wish to specify a protocol that is not included in the **IP Protocol** menu.
Packet Destination	Capture Destination. Valid values are: • File — Local PCAP file • scp — Provide the IP Address, the credentials, and the Destination Path for the remote server. **Note:** Each capture instance is assigned one local file. All active capture instances must use the same SCP server.
Export	**Note:** Hover over the PAC file to download. Certain APs support capturing wired and wireless packets simultaneously.
Active Packet Captures	Select **Active Packet Captures** to display the dashboard where you can view Packet Capture Instances. To add the Packet Capture Instances widget to your dashboard: 1. Go to **Dashboard**. 2. Select ✎. 3. Select **Widgets** > **Troubleshooting**. 4. Drag the packet capture widget to the Dashboard. 5. Save the Dashboard.

Related Topics

Dashboard Widget — Packet Capture Instances on page 97
Dashboard on page 44
Add or Edit a Configuration Profile on page 134

Dashboard Widget — Packet Capture Instances

ExtremeCloud IQ Controller offers a dashboard widget to help manage multiple packet captures. ExtremeCloud IQ Controller supports up to 10 packet capture instances. To start a packet capture, go to the **Troubleshooting** tab for each selected AP or site. A summary of all currently active packet capture instances is provided on the Default dashboard. The Dashboard Widget — Packet Capture Instances displays a line item for each packet capture instance.

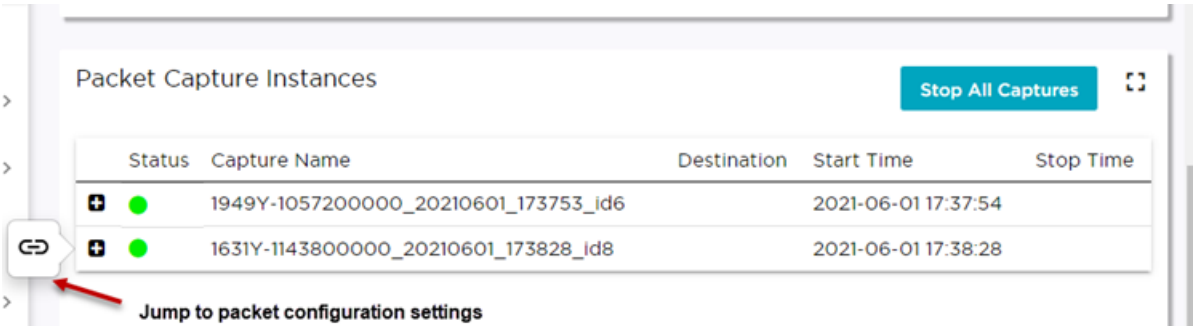


Figure 31: Default Dashboard -- Packet Capture Instances

Active instances display in green and inactive instances display in red. Inactive instances are eventually removed from the widget. The file name is automatically generated. The name is based on the AP or site where the capture was initiated plus an internal capture ID. Move easily between the dashboard widget and the packet capture configuration settings:

- From the dashboard, select the packet capture instance link to jump to the specific packet capture configuration instance.
- From each packet capture configuration page, select **Active Packet Captures** to jump to the dashboard widget.

You can stop individual packet capture instances from the corresponding configuration page, and you can stop all packet captures from the dashboard widget.

Related Topics

Packet Capture Parameters on page 95
Configure AP Packet Capture on page 95
Packet Capture on page 93

Opening Live SSH Console to a Selected AP

ExtremeCloud IQ Controller provides a remote console to enable diagnostic debugging of wired and wireless APs. Use the remote console to open a live SSH console session to an AP and troubleshoot using the built-in commands, such as ping and traceroute. You can initiate remote console on both local and remote APs configured behind a firewall.

To open a remote console to an AP from the Devices List:

1. Go to **Monitor** > **Devices** > **Access Points**.
2. Select an access point (not the check box).
3. Select **Troubleshooting** > **AP Remote Console** > **Connect**.

   The selected AP's SSH console opens.

4. To terminate the SSH console session, select **Disconnect**.

To open a remote console to an AP from the Sites List:

1. Go to **Monitor** > **Sites**.
2. Select a site.
3. Select **Troubleshooting** > **AP Remote Console**.
4. From the drop down field, select an access point.
5. Select **Connect**.

Channel Inspector Report — Fixed Channels

Use the Channel Inspector Report to gain insight into channel interference on fixed radio channels.

Note
This report does not support Smart RF. For information on Channel Inspection Report for Smart RF, see Channel Inspector Report — Smart RF on page 102

Configure radio channels from the device group configuration Profile or override the Profile configuration for an individual AP. Then, run this report against radio channels that are configured as Fixed Channel. Select ⚙ to jump to the AP radio configuration.

To access the Channel Inspector Report for Fixed Channels:

1. Go to **Monitor** > **Devices** > **Access Points**.
2. Select an AP.
3. Select **Troubleshooting** > **Channel Inspector**.
4. Configure the following:

   Duration

   Enter the number of minutes to run the report. Consider the OCS Interval configuration under the radio Advanced Settings.

   Radios 1-3

   For each radio that is configured for Fixed Channel, select the channel to inspect. Radios that are configured with Smart RF or MESH/ACS, are indicated and cannot be included in the report.
5. Select **Start**.

A report label indicates that channel inspection is running. The following information is available for each AP or beacon:

- AP Type
  - Managed — Indicates an AP or beacon that is adopted by ExtremeCloud IQ Controller.
  - External — Indicates an AP or beacon that is not adopted by ExtremeCloud IQ Controller.

  The Channel Inspector widget does not address radio frequency noise from non-Wi-Fi sources.
- BSSID. Basic Service Set Identifier. Identifies the AP.

- SSID. Service Set Identifier. Identifies the network to which the station is associated.

  While the BSSID identifies the AP interface that the station is using, the SSID identifies the overall service being used. The BSSID has the same structure as an AP MAC address, but you can have multiple BSSIDs coming off the same physical interface. The SSID is typically a human readable word, like “FreeWi-Fi”.
- AP Name. Name of the AP provided at network setup.
- Radio. Indicates the radio number.
- RSS. Received Signal Strength value.
- Last Seen in Minutes
- Channel:
  - Number
  - Width
  - Power
  - Attenuation

Additionally, information for each radio is presented that ranks available channels, presenting levels for each type of interference.

Table 20: Channel Inspector Interference Report

Field	Description
Frequency	Radio Frequency channels with the beacon channel (primary) denoted with brackets. The following is an 80 MHz channel example showing [5220] as the beacon channel. 44: (5180 5200 [5220] 5240).
Noise	Level of measured internet noise on the selected channel.
Ranking	Ranks selected channel against other available channels. Ranking is indicated by 1-5 stars. The higher the rank value, the more stars, and the more desirable the channel. The algorithm takes four input parameters: • Noise • Overlap Count • Co-Channel Count • Adjacent Count
Interference Types	Describes the channel interference in relation to the operating channel.
Overlap	Applicable for 40MGz and 80MGz channels only. The 20MGz channel is designated as the primary and the other channels are designated as secondary extension channels. If the primary channel of one AP is the same as the extension channel of another AP it is considered overlapping. Overlapping is the worst type of interference.

Table 20: Channel Inspector Interference Report (continued)

Field	Description
Co-Channel	All the APs on the same channel as the target AP are competing. Using Distributed Control Function (DCF) collisions are avoided because the APs know to avoid each other; however, the more traffic on the channel the greater the chance of collisions. Throughput slows but all packets get through. Example Notation, Co-Channel 20 44: (5220) indicates that there is co-channel interference on the beacon channel 5220.
Adjacent	APs on adjacent channels are close enough to interfere but not close enough to know they are interfering. They do not have the benefit of DCF.

Related Topics

Configure AP Details and Radio Settings on page 213
Advanced AP Radio Settings on page 153
Channel Inspector Report — Smart RF on page 102

Smart RF Widgets Per Device

The following widget reports for each radio are available from the AP **Smart RF** tab:

Note
The Smart RF tools reflect data available for channels that are selected in the Channel Plan when Smart RF is enabled on the radio. For more information, see Channel and Power Settings on page 182.

- **Mitigation**. Mitigation action taken by Smart RF to improve the network:
  - Channel Change — The channel of an AP radio was changed
  - Power Change — The power of an AP radio was changed
  - Select Shutdown — AP radio shutdown
  - Coverage Hole — AP reacts to holes in AP coverage
- **Channel Energy**. Displays the amount of interference detected by each radio on each channel and indicates the source of the interference:
  - Neighbor Wi-Fi for APs
  - External Wi-Fi for non-neighbor sources of Wi-Fi interference
  - Non Wi-Fi Energy for interference that is not generated by a Wi-Fi signal
- **Channel Ranking**. Provides a high level of visibility as to the occupancy of the RF spectrum around a particular AP. The following data is provided on the widget:
  - Frequency. Radio Frequency channels with the beacon channel (primary) denoted with brackets. The following is an 80MHz channel example showing [5220] as the beacon channel. 44: (5180 5200 [5220] 5240).
  - Noise. Channel noise measured in Decibel-milliwatts (dBm).

- Ranking. Indicates the best operating channel based on a 5-star ranking. This ranking is relative to the channels that are available. The higher the rank the more desirable the channel. The ranking algorithm considers the following parameters:
  - noise level
  - overlap count
  - co-channel count
  - adjacent AP count
- Overlap. Number of APs on overlapping channels. Applicable for 40MGz and 80MGz channels only. The 20MGz channel is designated as the primary and the other channels are designated as extension channels (secondary). If the primary channel of one AP is the same as the extension channel of another AP it is considered overlapping. Overlapping is the worst type of interference.
- Co-Channel. Number of co-channel APs. APs on the same channel as the target AP are competing. Using Distributed Control Function (DCF) collisions are avoided because the APs know to avoid each other; however, the more traffic on the channel the greater the chance of collisions. Throughput slows but all packets get through.
- Adjacent. Number of APs on adjacent channels. Adjacent APs are close enough to interfere, but not close enough to know they are interfering. They do not have the benefit of DCF.

To display more details for a specific channel, select a row in the widget. The Channel Inspector Interference Report displays.

- **Neighbor List**. Indicates channel occupancy and neighboring channels.
  - Neighbor APs are identified by both the SSID and BSSID.
  - The channel width for each neighbor AP is displayed, and it is an option to display the AP security setting.
  - APs that are managed by ExtremeCloud IQ Controller are reported separately from APs that are not managed by ExtremeCloud IQ Controller.
  - The Neighbor Report can be sorted by radio band — 2.4 GHz, 5 GHz, and 6 GHz respectively.

Related Topics

Smart RF Widgets Per Site on page 68
Channel and Power Settings on page 182
Channel Inspector Report — Smart RF on page 102
Configuring RF Management on page 180
Network Snapshot: Sites on page 54

Channel Inspector Report — Smart RF

The Channel Inspector Report enhances Smart RF on the controller by providing details about channel interference for each radio.

To access the Channel Inspector Report for Smart RF:

1. Go to **Monitor** > **Sites**.
2. Select a site. Then select the **Smart RF** tab.

3. From the **AP Smart RF** dashboard, select a row on the **Channel Ranking** widget.

The channel data generated from Smart RF populates the report. The report is generated from the last channel scan. The report lists visible BSSID and SSID data with RF measurements.

Note
For more information, see:

- Smart RF Widgets Per Device on page 101
- Basic RF Management Settings on page 180
- Scan Settings for Smart RF on page 187
- Channel and Power Settings on page 182

Table 21: Channel Inspector Interference Report

Field	Description
Interference Type	Describes the channel interference in relation to the operating channel. Possible values are: • Co-Channel. All the APs on the same channel as the target AP are competing. Using Distributed Control Function (DCF) collisions are avoided because the APs know to avoid each other; however, the more traffic on the channel the greater the chance of collisions. Throughput slows but all packets get through. Example Notation, Co-Channel 20 44: (5220) indicates that there is co-channel interference on the beacon channel 5220. • Adjacent. APs on adjacent channels are close enough to interfere but not close enough to know they are interfering. They do not have the benefit of DCF. • Overlapping. Applicable for 40MGz and 80MGz channels only. The 20MGz channel is designated as the primary and the other channels are designated as secondary extension channels. If the primary channel of one AP is the same as the extension channel of another AP it is considered overlapping. Overlapping is the worst type of interference.
Frequency	Radio Frequency channels with the beacon channel (primary) denoted with brackets. The following is an 80 MHz channel example showing [5220] as the beacon channel. 44: (5180 5200 [5220] 5240).
RSS	Received Signal Strength value.
BSSID	Basic Service Set Identifier. Identifies the AP.
SSID	Service Set Identifier. Identifies the network to which the station is associated.
AP Name	Name of the AP provided at network setup.

Related Topics

Smart RF Widgets Per Device on page 101

Basic RF Management Settings on page 180
Scan Settings for Smart RF on page 187
Channel and Power Settings on page 182

AP Events

To help monitor network health, ExtremeCloud IQ Controller collects and displays AP event data. The AP event log level is configured at the site device group level for all APs in the device group. Additionally, the AP event log level can be overridden for one or more individual APs. Valid log level values are: Critical, Major, Minor, and Info. Whether or not an event is displayed here depends on the configured AP event log level. The default log level value is *Major*.

A best practice is to configure AP event log level from the device group configuration Profile. However, log level overrides for individual APs can be useful when troubleshooting the network.

View AP Events for a Single AP

To view AP events for a single AP:

1. Go to **Monitor** > **Devices** > **Access Points**.
2. Select an AP.
3. Select the **Events** tab.

View all AP Events

To view all AP events:

Go to **Tools** > **Logs** > **AP Events**.

Note
In a High Availability Pair, the AP Events do not synchronize when the link between appliances is down, and no further synchronization is performed for the unsynchronized events after the connection is restored.

Related Topics

View AP Events — Single Access Point on page 104
View All AP Events on page 381
Advanced Configuration Profile Settings on page 172
Advanced Setting Overrides on page 221
Multiple APs Event Level Override on page 209

View AP Events — Single Access Point

Review AP events from the AP **Events** tab.

1. Go to **Monitor** > **Devices** > **Access Points**.
2. Select an access point.
3. Select the **Events** tab.

The following history reports are available:

- Reboot History — User requested restarts and AP initiated restarts
- Upgrade History — A count for successful upgrades and failed upgrades
- Radar Detection — The number of times radar is detected by the AP.

  When using a DFS Channel, the AP must listen for radar. When radar is detected, the AP stops transmission on that channel, marks the channel as unusable (for 30 minutes), and immediately switches to new channel based on the configured channel plan.

- Select to set the **Duration** value for the time period reported. Valid duration values are:
  - Last 3 hours
  - Last 3 days
  - Last 14 days
- Select to refresh the data on demand.
- Hover the mouse over a widget to display tool tip information.

Enable Debug Logging — This option sets the Event log level to *Informational*. The log is refreshed every 20 seconds. It can take up to 2 minutes for new log messages to display. This setting is disabled after you navigate away from the **Events** page, automatically reinstating the previous log level.

Related Topics

AP Actions on page 206
Upgrade AP Images on page 442
Smart Poll on page 396
View All AP Events on page 381

Switches List

ExtremeCloud IQ Controller can manage a maximum of 1000 switches. In ExtremeCloud IQ Controller, switches are primarily used for stats reporting. Switches operate independently of the connectivity state. For example, switch states do not change when the appliance is not reachable. You can configure authentication on the switch ports for MBA and 802.1x against an external/(site-local) authentication RADIUS server. Because the authenticated sites are directly reachable from the device, the connectivity status only affects the consistency of the statistics.

- To see a list of configured switches in ExtremeCloud IQ Controller , go to **Monitor** > **Devices** > **Switches**.
- To view a list of switches associated with a site, go to **Monitor** > **Sites**, select a site. Then, select the **Switches** tab.

Select a switch to display the switch dashboard and other associated components.

Select to refresh the data on demand.

Related Topics

Understanding Switch States on page 106
Network Snapshot: Switch Details on page 106
RADIUS Configuration for Switches Per Site on page 131
Switch Port Configuration on page 243

Understanding Switch States

The following describes switch states on the **Switches Device List**.

Table 22: Switch State from the Device List

State	Description
	In-service: • Switch acknowledges the sent configuration • Switch sends statistics every 5 minutes.
	In-Service Trouble: • Switch in process of connecting to ExtremeCloud IQ Controller • Configuration is pending acknowledgment from switch • Switch reset pending • Switch reboot pending • Switch upgrade pending
	Unknown. Switch has not discovered the ExtremeCloud IQ Controller.
	Critical: • Switch stops sending requests for 5 minutes or longer • Consistent with a loss of connectivity to ExtremeCloud IQ Controller

Network Snapshot: Switch Details

To view network details from the switch screen:

1. Go to **Monitor** > **Devices** > **Switches**.
2. Select a switch (not the check box).

   The network details for the selected switch display.

   Hardware details:

   - Power Supplies
   - Fans
   - PoE Budget. Select  to see AP capacity estimation based in the current PoE draw.

- Temperature
- VIM (Versatile Interface Module)

Table 23: Tabs on the Switch Details Screen

Tab	Description
Dashboard	Widgets display network details related to the selected switch.
Ports	A list of configured ports on the selected switch.
LAG Ports	Link Aggregation Group (LAG) Ports organized as a list of master ports and the LAG members that are associated with the master port. All ports assigned to a LAG must have the same port function. The configuration of the master port is shared with its LAG members. When a port is added to a LAG, its previous unique configuration is removed and the port inherits the group configuration. **Note:** A Link Aggregation Group whose function is to connect to an AP is limited to two ports in the group. Both ports must negotiate to the same speed (1 Gbps). LAG is supported on ExtremeWireless AP39xx and 11ax APs. LAG *is not* supported on AP305C, AP410C, and AP460C.
Traces	Trace information related to the selected switch.
VLANS	A list of VLANS associated with the switch, including the switch port number.
Troubleshooting	Provides a remote console to enable diagnostic debugging of ExtremeXOS switches.

3. You can also:

   Select ⚙ to modify configuration settings.

   Select ☰ to go back to the list.

Related Topics

PoE Budget AP Estimator on page 108
Switch Widgets on page 108
Ports List on page 108
LAG Ports on page 109
Traces on page 109
VLANS on page 110
Troubleshoot a Switch Using the CLI on page 109
Configure a Switch on page 242
Switch Port Configuration on page 243
Port Dashboard on page 108

Switch Widgets

To view widgets for an individual switch:

1. Go to **Monitor** > **Devices** > **Switches**.
2. Select a switch (not the check box) and review the widgets on the **Dashboard** page.

These widgets provide basic information for an individual switch, including:

- Utilization
- Top 5 busiest ports
- Port usage distribution showing the proportion of ports assigned to each of the possible port functions:
  - Serve an Access Point
  - Serve a Host (other than an access point)
  - Link to another bridge/switch
  - Other
- Port PoE states

PoE Budget AP Estimator

The PoE Budget AP Estimator outlines PoE budget data per AP model number for the selected switch model. Use this information to effectively plan your AP/Switch topology.

The following data is available for the selected switch:

- AP Model
- Max Draw (in Watts)
- Total AP Capacity
- AP Capacity Remaining

Related Topics

Network Snapshot: Switch Details on page 106

Ports List

A list of configured ports on the selected switch.

Related Topics

Port Dashboard on page 108
Switch Port Configuration on page 243

Port Dashboard

The **Port** screen displays information and details about a specific switch port. To access the **Ports** screen:

1. Go to **Monitor** > **Devices** > **Switches**.
2. Select on a switch.
3. Select the **Ports** tab.
4. Select on a port.

The following information is available on the **Ports** screen.

- Link State
- Admin Status
- Name
- Alias
- Function
- Authentication
- Port Speed
- Neighbor

Related Topics

Switch Port Configuration on page 243

LAG Ports

Link Aggregation Group (LAG) Ports organized as a list of master ports and the LAG members that are associated with the master port. All ports assigned to a LAG must have the same port function. The configuration of the master port is shared with its LAG members. When a port is added to a LAG, its previous unique configuration is removed and the port inherits the group configuration.

Related Topics

LAG Configuration on page 243

Traces

Trace information related to the selected switch.

Troubleshoot a Switch Using the CLI

ExtremeCloud IQ Controller provides a remote console to enable diagnostic debugging of ExtremeXOS® switches. To troubleshoot using the EXOS CLI commands, use the remote console to open a live console session to an EXOS switch.

Note
ExtremeCloud IQ Controller remote console to a switch *does not* support 200 Series switches.

You can initiate remote console to a switch from any ExtremeCloud IQ Controller in an availability pair. A switch deployed in a remote office behind a firewall or Network Address Translation (NAT) is reachable from the ExtremeCloud IQ Controller remote console.

To access the live console from the switch **Troubleshooting** tab, the ExtremeXOS switch must be in GUI-Mode. To set the switch mode, select the settings button ⚙ and then select **Advanced**. For more information on Switch mode, see Access the Switch CLI on page 246.

To access the remote console on the **Troubleshooting** tab:

1. Go to **Monitor** > **Devices** > **Switches**.

2. Select an EXOS switch (not the check box).
3. Select **Troubleshooting** > **Switch Remote Console** > **Connect**.

   The switch console opens. Log in with your ExtremeCloud IQ Controller credentials.
4. To terminate the console session, select **Disconnect**.

Consider the following about a remote console on the **Troubleshooting** tab:

- One console session is allowed to a switch at a time. Subsequent connection requests to the same switch are rejected.
- You can open up to 100 simultaneous remote consoles, each to a separate switch.
- It can take up to 60 seconds for the switch to connect.
- Avoid modifying the switch configuration from the **Troubleshooting** tab.
- Read-only users of ExtremeCloud IQ Controller cannot access the **Troubleshooting** tab.
- Modifications made during the CLI diagnostics session are not preserved on ExtremeCloud IQ Controller.
- After you leave the **Troubleshooting** tab, the remote session is terminated. There is no history or current status of a connection.

For information on ExtremeXOS CLI commands, see ExtremeXOS documentation.

Related Topics

Access the Switch CLI on page 246
Advanced Switch Settings on page 245
Switch Configuration Backup Files on page 247

VLANS

A list of VLANS associated with the switch, including the switch port number.

Related Topics

VLANS on page 302

Networks List

Go to **Monitor** > **Networks** to view a list of networks configured in ExtremeCloud IQ Controller. Select a network to view the network dashboard and related network components.

Related Topics

Network Snapshot: Network Dashboard on page 110
Network Widgets on page 111

Network Snapshot: Network Dashboard

To access the **Network Services** screen:

1. Go to **Monitor** > **Networks**.

2. Select a network service from the list.

   The network details for the selected service are displayed.

Table 24: Tabs on the Network Service Screen

Tab	Description
Dashboard	Network charts provide throughput and volume information for each network service. Use this information to understand network traffic and load.
Sites	List of sites associated with the network service.
Access Points	List of access points associated with the network service. Use the search facility to find a specific AP.
Switches	List of switches associated with the network service.
Clients	List of clients associated with the network service. Use the search facility to find a specific client. Add or remove clients from Allow list or Deny list directly from the client list.

3. You can also:

   Select ⚙ to modify configuration settings.

   Select ☰ to go back to the list.

Related Topics

Network Widgets on page 111

Network Widgets

The following widget reports are available from the Networks dashboard:

- Client Utilization. Provides metrics on client throughput and data usage.
- RF Management. Provides metrics on radio frequency quality.
- Clients. Provides metrics on Transmission Control Protocol (TCP) and Return Trip Time (RTT) per client.
- Expert: Client metrics for the expert user related to RFQI, RTT, RSS, and RX and TX Rates.
- Application Visibility. Provides details about applications the client is accessing and metrics on application groups related to throughput and usage.

To view widgets for an individual network:

1. Go to **Monitor** > **Networks**.
2. Select a network from the list and review the widgets on the **Dashboard** page.

Mesh Point Network Diagram

View a diagram of your mesh network from the **Monitor** workbench. Go to **Monitor** > **Networks** > **Mesh Points** and select a mesh point network.

- To display **Node Information**, select the AP node.

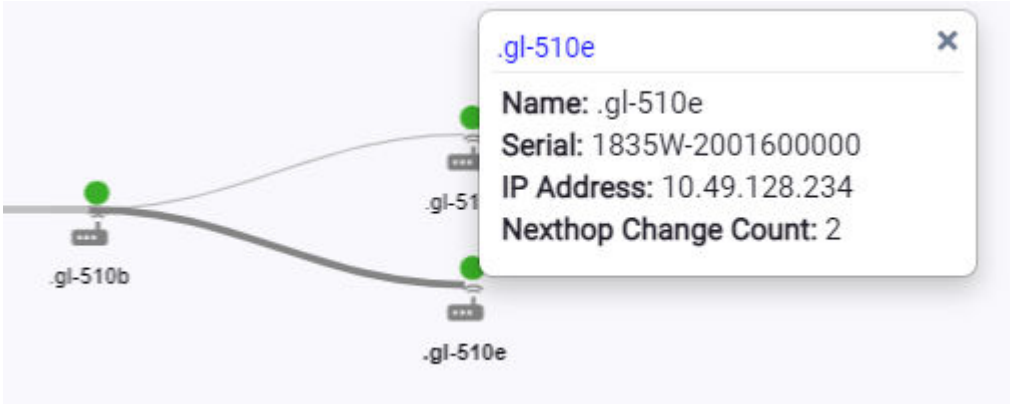


Figure 32: Mesh Node Information

Name
: AP Name

Serial Number
: AP Serial Number

IP Address
: IP Address of the AP

Nexthop Change Count
: (Displayed for non-root APs with an active link.) Indicates how often the uplink has changed. This value indicates link stability. A stable value that does not increment during the service period is preferred.

- To display **Link Information**, select the line connecting the nodes. Bi-directional link information is displayed.

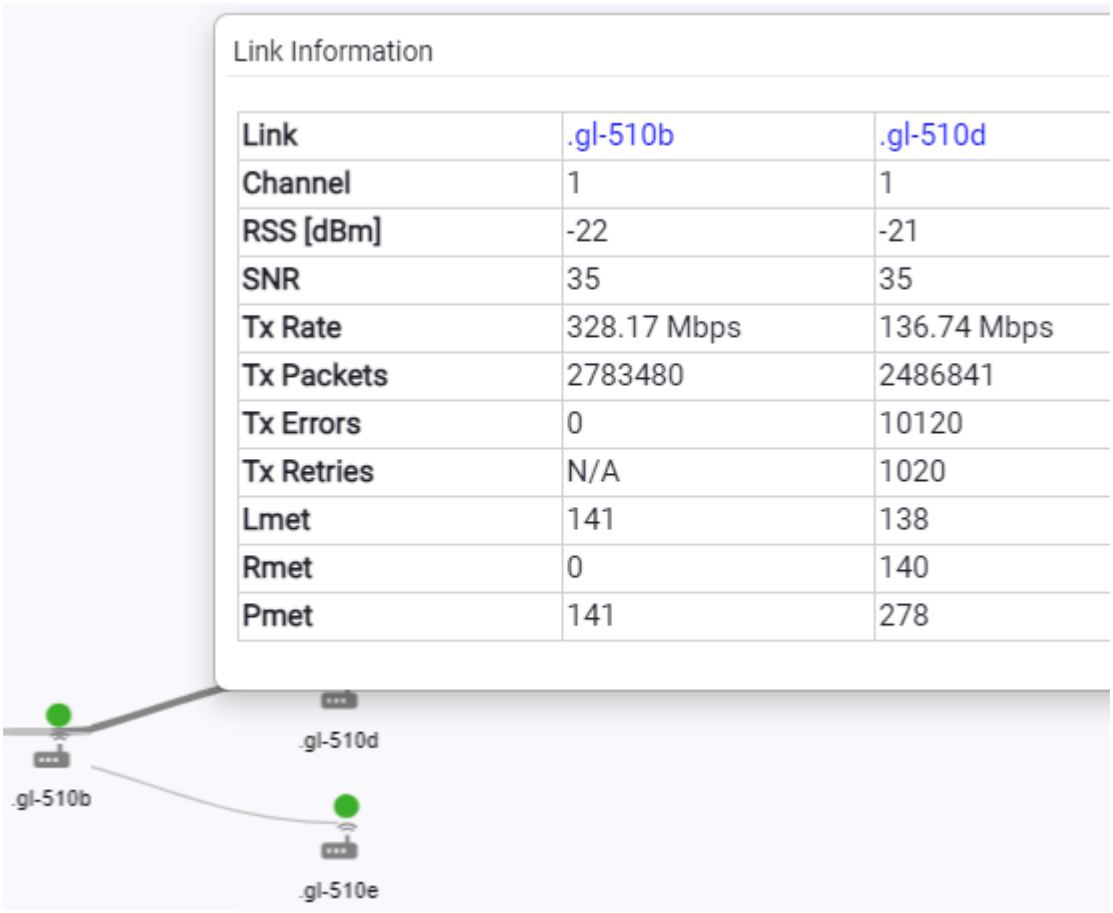


Figure 33: Mesh Link Information

Table 25: Mesh Link Information Fields

Field	Range	Description	Directional Notes	
			AP1	AP2
RSS (dBm)	-1 to -127 dBm	Received Signal Strength	Packets from AP1, detected at AP2	Packets from AP2, detected at AP1
SNR	0 to 127	Signal-to-Noise Ratio	Packets from AP1, detected at AP2	Packets from AP2, detected at AP1
Tx Rate (bps) (Bits per second)	0 to 4398 Gbps (Gigabits per second)	Moving Average of Tx PHY Rate	Tx Rate of packets from AP1, detected at AP2	Tx Rate of packets from AP2, detected at AP1
Tx Packets	0 to 4294967295	Count of Tx packets.	Number of Tx packets from AP1 to AP2	Number of Tx packets from AP2 to AP1

Table 25: Mesh Link Information Fields (continued)

Field	Range	Description	Directional Notes	
			AP1	AP2
Tx Errors	0 to 4294967295	Count of Tx error packets	Packet errors from AP1, detected at AP2	Packet errors from AP2, detected at AP1
Tx Retries	0 to 4294967295	Count of Tx retried packets	Number of Tx packet retries from AP1 to AP2	Number of Tx packet retries from AP2 to AP1
Lmet	0 to 8191	Cost Metric of Link to neighbor AP. Lower value is better.	Cost of Link derived from packets that are sent from AP1 and received at AP2	Cost of Link derived from packets that are sent from AP2 and received at AP1
Rmet	0 to 8191	Cost Metric of neighbor AP's path to Root AP. Lower value is better.	Cost Metric reported in MCX packets sent from AP1 to AP2	Cost Metric reported in MCX packets sent from AP2 to AP1
Pmet	0 to 16382	Cost of Path to Root AP when the AP uses a neighbor AP as a parent AP. A lower value is preferred. With an active link, the AP periodically checks the threshold. Mesh ACS is triggered when the value measures below the defined threshold, initiating a new nexthop. The default threshold is 1500. Use this value to determine link stability.	Pmet = Lmet + Rmet	Pmet = Lmet + Rmet

The **Neighbors** indicator button displays possible paths between APs.

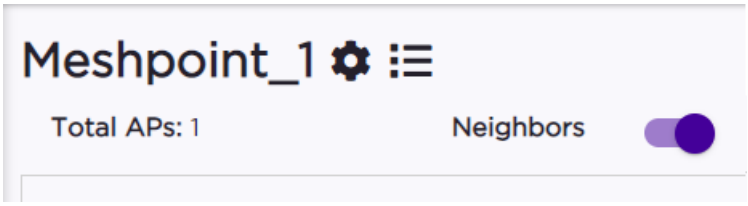


Figure 34: Neighbors Indicator on Mesh Point Diagram

Move around the diagram using the following tools:

- Navigate the network diagram using the arrow buttons.

Figure 35: Navigation Buttons

- Zoom in and out using the zoom buttons.

Figure 36: Zoom Buttons

- To center the diagram, select .
- To refresh the diagram, select .
- To jump to the **Mesh Point Network Configuration Settings**, select .

Related Topics

Mesh Point Network Settings on page 262
Mesh Point Network on page 260
Configure a Mesh Point Network on page 262
Advanced Configuration and Mesh Device Settings on page 139
Mesh Point Profile Configuration on page 138

Clients

The **Clients** tab displays a list of clients in your network. Use this information to understand client status, access roles, and associated APs. From the client list, you can add clients to and remove clients from access lists.

From the client **Actions** button, you can delete and disassociate clients, re-authenticate clients, and move clients into and out of groups.

Highlights on the **Clients List**:

- IP Address — The IP Address field displays the IPv4 address and indicates when there is up to three IPv6 addresses. Hover over the IP Address field to view the full IPv6 address. You also have the option to display the IPv6 addresses in a separate field.
- RSS (dBm) — Received Signal Strength Indicator is the estimated power level that a client device is receiving from the associated access point.
- Spatial Stream — Number of MIMO streams supported by each client. Use this information to inform your decisions about hardware purchases and decisions about network configuration.

- Capabilities — Client protocol capabilities. Indicates which protocol capabilities the client supports. Valid values are:
  - PMF (Protected Management Frame) — PIM (Protocol Independent Multicast) Flooding Mechanism.
  - RRM — Radio Resource Management
  - WPA1/WPA2/WPA3 — Wi-Fi Protected Access (versions 1-3)
- DL Lost Retries Packets — Indicates the number of packets lost between the AP and the client (downlink). This value indicates the health of the RF environment. Possible reasons for packet transmission failure are channel noise or co-channel interference.
- DL Lost Retries Bytes — Indicates the number of bytes lost in packet transmission between the AP and its clients (downlink). This value indicates the health of the RF environment. Possible reasons for packet transmission failure are channel noise or co-channel interference.
- Channel — Indicates the channel to which the client is connected. Possible values include a specific channel number or a channel number, plus offset, and channel width.

  For example, **44+1/40** represents channel 44, +1 offset of the primary channel, / 40 MHz channel width.

Use Query Builder to create reports using the available data points.

Select a client to see client details.

Related Topics

Understanding Date and Time on page 43
Understanding Client Status on page 116
Query Builder on page 73
Global Client Access Lists on page 117
Client Actions on page 118
Network Snapshot: Clients Dashboard on page 120
Configuring Column Display on page 43

Understanding Client Status

The **Client List** shows the status of each client in the network.

- Green — Clients with currently active sessions.
- Gray — Inactive. Inactive clients continue to be displayed as long as they were active within the Duration selected.
  - Last 3 hours
  - Last 3 days
  - Last 14 days

  Client data is removed from the system after 14 days of being inactive.

Use **Auto Refresh** to automatically refresh the information presented. From the **Auto Refresh** drop-down field, select the refresh value. Valid values are:

- OFF
- 30 Seconds
- 1 Minute
- 3 Minutes
- 5 Minutes

You can also select to manually refresh the page anytime.

Note
Save your page setting changes. **Auto Refresh** is implemented at the browser level and therefore will reset any selections or unsaved page setting changes. When using **Auto Refresh**, select a refresh interval that allows you to complete the operation within the defined interval. For best results, set **Auto Refresh** to OFF during configuration selections or selection of a large number of elements.

Related Topics

Dashboard on page 44

Client Access Lists

Clients on a Deny list are denied network access. Clients on an Allow list are granted network access. Use these lists to create a subcategory of users that are set apart from the larger group by their access privileges. The client MAC address is used to add the client to a specific list.

You have the option to configure access lists per site or for all networks being broadcast by any AP managed by ExtremeCloud IQ Controller or by an ExtremeCloud IQ Controller availability pair.

Note
Configure a Deny list or an Allow list, but not both. To filter specific users by MAC address, configure Access Control rules.

Related Topics

Global Client Access Lists on page 117
Site Client Access Lists on page 118
Managing Access Control Rules on page 364

Global Client Access Lists

To set up a global list for all ExtremeCloud IQ Controller networks:

1. Go to **Monitor** > **Clients** and select **Allow/Deny List**.
   This displays the list **Mode** for your network and a list of MAC addresses.
2. Select **Allow List** or **Deny List**.
   The Mode you select applies to the entire network.

3. To add MAC addresses to the list, select **Add** and enter a MAC address for the client.
4. To delete a MAC address from the list, select the MAC address from the list, then select **Delete**.

   To select the entire list, select the **MAC Address** check box.

Related Topics

Client Access Lists on page 117
Site Client Access Lists on page 118

Site Client Access Lists

The selected Access List Mode applies to all access points in the site. The access list is stored on the AP and shared across the site. A client MAC address on the site Deny List, cannot connect to a network broadcast by any AP associated with the site.

To set up an access list for clients associated with a site:

1. Go to **Configure** > **Sites** and select a site.
2. Select **Allow List/Deny List** tab.
3. Select **Enforce site level control over RF association**.
4. Select the Mode: **Allow List** or **Deny List**.
5. To add MAC addresses to the list, select **Add** and enter a MAC address for the client.
6. To delete a MAC address from the list, select the MAC address from the list, then select **Delete**.

   To select the entire list, select the **MAC Address** check box.

Related Topics

Client Access Lists on page 117
Global Client Access Lists on page 117

Client Actions

The following describes actions you can take on clients in the Clients list. From the Clients list, select one or more clients and select one of the following actions from the **Actions** drop-down.

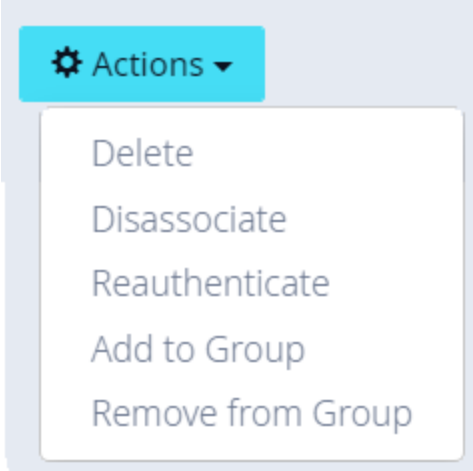


Figure 37: Client Actions Button

Table 26: Client Actions

Field	Description
Delete	Delete a client from the network. • The client is removed from groups of which it was a member. • The client *remains* on an Allow list or Deny list, if it was included on a list before deletion. • **Also Delete User Registrations** indicates whether or not the user registrations are being deleted along with the client/end-system.
Disassociate	Users are disassociated from the AP. Consequently, the users must log on again and be authenticated on ExtremeCloud IQ Controller before the wireless service is restored.
Reauthenticate	The authentication state is not preserved during fast failover. If a WLAN Service requires authentication, the client device must reauthenticate. The session availability is not guaranteed because authentication may require additional time during which the user session may be disrupted. Use this option to manually reauthenticate one or more clients.
Add to group	Adds selected clients to a group. Check **Force Reauthentication** to automatically reauthenticate the client to the network.
Remove from group	Removes selected clients from the group. Check **Force Reauthentication** to automatically reauthenticate the client to the network.

Related Topics

Network Snapshot: Clients Dashboard on page 120
Global Client Access Lists on page 117
Understanding Client Status on page 116

Network Snapshot: Clients Dashboard

The **Clients** screen displays information and details about a specific client, as well as the client location on a mapped floor plan.

To access the **Clients** screen:

Go to **Clients** and select a client from the list.

Information about the selected client is displayed.

Table 27: Client Information

Client MAC address and status	Associated Access Point
Client IP Address	Network SSID
IPv6 Address, if applicable	Associated AP Radio
Last device group	RSS Reading
Date and time last seen on the network	Protocol
Manufacturer	Tx Rate (Transmitted signal rate)
Role	Rx Rate. (Received signal rate.)
	Device Family
	Device Type
	Host Name

The **Client Details** displays a chart of client association with an AP.

Table 28: Tabs on the Client Screen

Tab	Description
Dashboard	Network charts provide throughput, volume, and speed information for each client. Use this information to understand network traffic and load.
Sites	Lists sites associated with the client.
Networks	Lists the network services associated with the client. Select a network to display network details. See WLAN Service Settings on page 250 .
Access Points	Lists access points associated with the client. Use the search facility to find a specific AP. The AP Name that you specify is displayed by default.
Station Events	Log of station events for the client. Use the search facility to locate a specific event. Search on any column heading. To enable station events, go to **Admin** > **System** > **Logs** and check **Send Station Events**.

Related Topics

Client Widgets on page 122

Station Events on page 121
Client Actions on page 118
Understanding Date and Time on page 43
Dashboard on page 44
Floor Plans on page 35
System Logging Configuration on page 457

Station Events

Use the following information to troubleshoot access and performance for a specific client. Review client details and events associated with a client. The event source can be the Access Control Engine or the Wireless Manager. The fields in Table 29 are documented in alphabetical order.

Table 29: End-System Event Fields

Field	Description
Access Control Engine	IP address of the NAC (Network Access Control) server.
Authentication Type	Indicates the type of 802.1x authentication or MAC authentication. For example, 802.1X (PEAP).
Device Type	Indicates device type for the client.
End System	Indicates MAC address of the client.
Extended State	Details about the action that triggered the event. Valid values are: • Authentication • State Change • De-registration • Registration • No Error
Location	MAC addresses and network identifiers that the client has been associated with. Indicates client position on the network.
RADIUS Response Attributes	Attributes from the RADIUS server that describe the form of access that is granted to the client.
RADIUS Server	IP address of the external RADIUS server, if any.
Reason	Indicates the specific rule from the Access Control Rule Engine that allowed client access to the network.
Registration Type	Indicates type of registration when Extended State equals Registration. Valid values are: • Guest • Secure Guest • Guest Web Access • Authenticated • Authenticated Guest

Table 29: End-System Event Fields (continued)

Field	Description
Role	Indicates the policy role that allowed client access to the network.
State	State of the action that initiated the event. Valid values are: • Accept • Disconnected • Reject • Pending
State Description	Additional details about the event state.
Source	Indicates where the event originates. Valid values are: • Access Control Engine • Wireless Manager
Timestamp	Indicates date and time of the event.
User Name	Logged in user associated with the client.

Related Topics

Configuring Roles on page 291
Access Control Rules on page 361

Client Widgets

The following widget reports are available from the Client dashboard:

- Client Utilization. Provides metrics on client throughput and data usage.
- RF Management. Provides metrics on radio frequency quality.
- Clients. Provides metrics on Transmission Control Protocol (TCP) and Return Trip Time (RTT) per client.
- Expert: Client metrics for the expert user related to RFQI, RTT, RSS, and RX and TX Rates.
- Application Visibility. Provides details about applications the client is accessing and metrics on application groups related to throughput and usage.

To view widgets for an individual client:

1. Go to **Clients**.
2. Select a client from the list and review the widgets on the **Dashboard** page.

Related Topics

Add a New Dashboard on page 47
Modify a Dashboard on page 48

Policy

You can define policy rules for a role to specify network access. Network policies are a set of rules, defined in a specific order, that determine how connections are authorized or denied. If you do not define policy rules for a role, the role's default action is applied to all traffic subject to that role. However, if you require user-specific filter definitions, then the filter ID configuration identifies the specific role that is applied to the user.

Related Topics

Roles List on page 123
Configuring Roles on page 291

Roles List

A role is a set of network access services that can be applied at various points in a policy-enabled network. Roles are usually named for a type of user such as Student or Engineering. Often, role names match the naming conventions that already exist in the organization. The role name should match filter ID values set up on the RADIUS servers.

The default non-authenticated role is used when the client is not authenticated but able to access the network. The default authenticated role is assigned to a client when it successfully authenticates but the authentication process did not explicitly assign a role to the client.

Note
To configure default roles, go to **Configure** > **Networks**.

When the default action is sufficient, a role does not need additional rules. Rules are used only to provide unique treatment of packet types when a single role is applied.

ExtremeCloud IQ Controller is shipped with a default policy configuration that includes the following default roles:

- Enterprise User
- Quarantine
- Unregistered
- Guest Access
- Deny Access
- Assessing
- Failsafe

The Enterprise User access policy is intended for admin users with full access.

The Quarantine access policy is used to restrict network access to end-systems that have failed assessment. The Quarantine policy role denies all traffic by default while permitting access to only required network resources such as basic network services (for example, ARP, DHCP, and DNS) and HTTP to redirect web traffic for assisted remediation.

Related Topics

Add Policy Roles on page 292
Role Widgets on page 126
Policy Role Settings on page 292

Preconfigured Policy Roles

ExtremeCloud IQ Controller is shipped a with the following default policy configurations listed in Table 30.

Policy roles define the authorization level that ExtremeCloud IQ Controller assigns to a connecting end-system based on the end-system's authentication and/or assessment results. The access policies define a set of network access services that determine exactly how an end-system's traffic is authorized on the network.

Table 30: Preconfigured Policy Roles

Role	Description
Enterprise User	Intended for admin users with full access
Quarantine	The Quarantine access policy is used to restrict network access to end-systems that have failed assessment. The Quarantine policy role denies all traffic by default while permitting access to only required network resources such as basic network services (e.g., ARP, DHCP, and DNS) and HTTP to redirect web traffic for assisted remediation.
Unregistered	The Unregistered access policy default action is to deny all unregistered traffic.
Guest Access	The Guest Access policy allows registered guest traffic.
Deny Access	The Deny Access policy default action is to deny all traffic.

Table 30: Preconfigured Policy Roles (continued)

Role	Description
Assessing	The Assessment access policy temporarily allocates a set of network resources to end-systems while they are being assessed. Typically, the Assessment access policy allows access to basic network services (e.g. ARP, DHCP, and DNS), permits all IP communication to the Assessment servers so the assessment can be successfully completed, and HTTP to redirect web traffic for Assisted Remediation. For RFC 3580-compliant switches, the Assessment access policy may be mapped to the Quarantine VLAN. It is not mandatory to assign the Assessment policy to a connecting end-system while it is being assessed. The policy role received from the RADIUS server or an accept policy can be applied to the end-system, allowing the end-system immediate network access while the end-system assessment is occurring in the background. In this case, the policy role or accept policy (or the associated VLAN for RFC 3580-compliant switches) must be configured to allow access to the appropriate network resources for communication with the Assessment servers. **Note:** The Assessment server sends an ICMP Echo Request (a "ping") to the end-system before the server begins to test IP connectivity to the end-system. Therefore, the Assessment policy role, the router ACLs, and the end-system's personal firewall must allow this type of communication between end-systems and Assessment servers in order for the assessment to take place. If the Assessment server cannot verify IP connectivity, the Failsafe policy is assigned to the end-system.
Failsafe	The Failsafe access policy is applied to an end-system when it is in an Error connection state. An Error state results if the end-system's IP address could not be determined from its MAC address, or if there was an assessment error and an assessment of the end-system could not take place. For RFC 3580-compliant switches, the Failsafe access policy may be mapped to the Production VLAN.
Pass Through External RADIUS	Use this policy when the AAA mode is RADIUS (using an external RADIUS server). When this policy is selected, end-systems that match the rule get the RADIUS attributes from the upstream server's ACCEPT response, including Filter-Id.
Use Default Auth Role	Use the Default Auth Role that is configured for the wireless network that the end-system is connected to.

Related Topics

Add Policy Roles on page 292

Role Widgets

Widgets for an individual role policy show the following information:

- Top applications (by throughput) per role
- Top applications (by throughput) by concurrent users per role

To view widgets for an individual role:

1. Go to **Monitor** > **Policy** > **Roles**.
2. Select a role from the list and review the widgets on the **Dashboard** page.

   The widgets on the Roles dashboard relate to Application Visibility. Possible widgets include:
   - Application Categories by Client Count
   - Top Rules by Hit Count
   - Rule Hit Count
   - Bottom Application Groups by Client Count.

Related Topics

Add a New Dashboard on page 47
Modify a Dashboard on page 48
Rule-Level Statistics on page 126

Rule-Level Statistics

ExtremeCloud IQ Controller offers rule-level statistics that track policy rule usage in managing packet traffic. Gather Hit Count statistics for specific roles and specific rules. Widgets indicating roles with Top and Bottom Hit Counts display on the **Overview** dashboard. Widgets indicating filter rules with Top and Bottom Hit Counts display on the **Roles** dashboard. Additionally, the **Rule Hit Count** widget, on the **Roles** dashboard, provides the actual hit counts for each configured rule per role. Use this information to understand which policies are most often used when managing your network traffic.

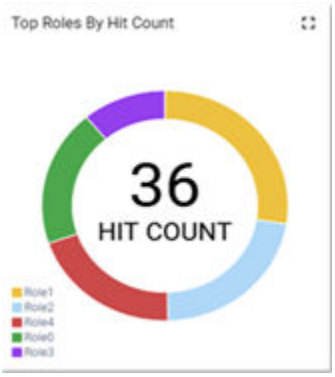


Figure 38: Hit Count Widget on the Overview Dashboard

To access the **Roles** dashboard, go to **Monitor** > **Policy** > **Roles** and select a role from the list.

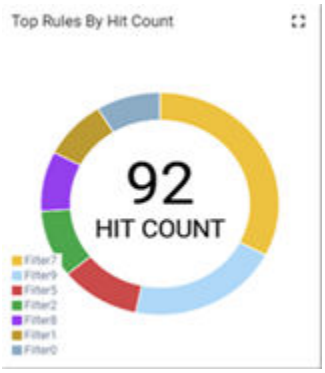


Figure 39: Top Rules by Hit Count on the Roles Dashboard

Figure 40: Rule Hit Count on the Roles Dashboard

Rule-level statistics are saved per role, per rule, as an aggregate of all mobile user clients. Hit count is collected separately for From User Traffic and To User Traffic, and hits to the default policy are included. When the policy configuration changes, only statistics for the latest configuration are displayed, but data is saved for up to 14 days.

Standard ExtremeCloud IQ Controller reporting duration is supported. Live reporting is not supported.

- Select to set the **Duration** value for the time period reported. Valid duration values are:
  - Last 3 hours
  - Last 3 days
  - Last 14 days
- Select to refresh the data on demand.
- Hover the mouse over a widget to display tool tip information.

Note
Hit Count reporting is synchronized within an availability pair.

Configure

Use the **Configure** workbench to set up the network components.

Network Configuration Steps

The following is the basic workflow for setting up your network using ExtremeCloud IQ Controller:

Note
To ensure the devices discover ExtremeCloud IQ Controller, configure DHCP, NPS, and DNS Services for ExtremeCloud IQ Controller discovery. For more information, see the *ExtremeCloud IQ Controller Deployment Guide*.

Note
Users with Read-Only access to ExtremeCloud IQ Controller do not have access to the ExtremeCloud IQ Controller configuration options.

1. Create one or more sites.

   Select a Country for the site. The Country option affects the licensing domain associated with the site.
2. Configure one or more device groups for each site.

   A device group is defined by the AP platform. It contains APs with the same model type. The configuration Profile and RF Management profiles are defined at the device group level. The available configuration options depend on the AP platform definition of the device group.
3. Configure one or more networks. When configuring a network, you will do the following:
   a. Define network authentication.
   b. Configure roles associated with the network.

c. Configure VLANs associated with the network.

4. Configure Adoption Rules so that new APs are automatically assigned to the appropriate device group based on factors such as AP platform, IP address, host name, or serial number.
5. (Optional) Configure additional roles.
6. Go back to each device group and associate the configured networks and the defined roles by editing the assigned configuration Profile. Alternatively, you can associate the Profile with the network or policy definition during the initial configuration of the network or role. For more information, see Associated Profiles on page 137.
7. Install and add devices.

   Access Points and switches are automatically added to an ExtremeCloud IQ Controller configuration via the cloud-connector when the DHCP and DNS prerequisites have been met. However, you can use the Add function to pre-provision any AP or switch before they connect, allowing them to be added to the correct site.

   AP discovery behavior depends on your site configuration and whether or not you are using adoption rules:

   - If you have a device group with a valid profile and a valid adoption rule, the APs are automatically added to the proper device group.
   - If you have a device group with a valid profile, but no adoption rules, the APs are listed in the device group where you can manually add them to the group.
   - If you do not have a valid device group for the AP, the AP is listed on the **Devices** list with an *In-Service Trouble* status. After a valid device group is created, the AP is automatically listed within the device group, where you can manually add it to the group.
8. (Optional) Add one or more floor plans for each site.
9. Set up access control and captive portal.

Related Topics

Sites Overview on page 30
Adding Device Groups to a Site on page 132
WLAN Service Settings on page 250
Policy on page 290
Floor Plans on page 35
AAA RADIUS Authentication on page 326
Onboard AAA Authentication on page 334
Associated Profiles on page 137

Sites

Use sites to define boundaries for fast roaming and session mobility without interruption. Manage sites from **Configure** > **Sites**. For more information about sites, see Sites List on page 52.

Related Topics

Sites Overview on page 30
Centralized Site on page 31
Add a Site on page 130
Site Default Dashboard on page 53
Modifying Site Configuration on page 131
Site Location on page 132
Adding Device Groups to a Site on page 132
Add or Edit a Configuration Profile on page 134
Configuring RF Management on page 180
Configuring Column Display on page 43
Configuring a Floor Plan on page 193
Site Client Access Lists on page 118

Add a Site

To add a site to ExtremeCloud IQ Controller, take the following steps:

1. Go to **Configure** > **Sites** > **Add**.
2. Configure the site parameters.

Related Topics

Site Parameters on page 130

Site Parameters

Configure the following parameters for site configuration.

Table 31: Site Configuration Parameters

Field	Description
Name	Determines the name of the site.
Country	Define the regulatory country for the site. The regulatory domain of the AP must match the Country setting for the site. This field provides automatic search capabilities. Begin typing in the field to display the country.
Time Zone	Indicates the time zone for the selected country. This field provides automatic search capabilities. Begin typing in the field to display the time zone.

Related Topics

Floor Plans on page 35
Site Location on page 132
Device Groups on page 32
Switches on page 239
Site Client Access Lists on page 118

SNMP Configuration on page 451
Centralized Site on page 31

Modifying Site Configuration

After a site is created, you can modify the configuration settings, clone the site, or delete the site. To get started:

1. Go to **Configure** > **Sites**.
2. Select a site from the list.
3. To clone a site, select **Clone** and provide a name for the new site.

   A message indicates if the site was successfully cloned. To open the new site, click **OK**.
4. To delete a site, select **Delete**.

   A delete confirmation message displays. Select **OK**.

Related Topics

Site Parameters on page 130
Floor Plans on page 35
Site Location on page 132
Device Groups on page 32
RADIUS Configuration for Switches Per Site on page 131
Advanced Tab on page 203

RADIUS Configuration for Switches Per Site

ExtremeCloud IQ Controller supports direct access from a switch to an external RADIUS server within the site configuration. You can associate up to two RADIUS servers for accounting and two RADIUS servers for authentication.

Note
When using 200 Series switches, only one accounting server is supported.

You must first configure the RADIUS servers before you can associate them to switches in a site configuration.

1. Configure each RADIUS server.

   Go to **Onboard** > **AAA** > **RADIUS Servers**.
2. Associate the RADIUS servers to the switches within the site configuration.

   a. Go to **Configure** > **Sites** and select a site.
   b. Select the **Switches** tab.
   c. Configure the following parameters:

   MSTP

   Enable the MSTP (Multiple Spanning Tree Protocol) to optimize load balancing.

   AAA Policy

Refer to external RADIUS servers directly without proxy by NAC. For configuration steps, see Configure AAA Policy on page 327.

Switches

Check the switches that are associated with the site.

Related Topics

AAA RADIUS Authentication on page 326
Configure AAA Policy on page 327
Switch Port Configuration on page 243

Site Location

To display your site location on a physical map from the Site workbench, provide site metadata including map coordinates. To access Site metadata:

1. Go to **Configure** > **Sites**.
2. Select a site and select the **Location** tab.
3. Provide the following optional information:
   - Site Manager Name
   - Site Manager Email
   - Site Manager Contact
     - Region
     - City
     - Postal Code
     - Campus
   - Map Coordinates. Your site location is automatically displayed based on data in the geodatabase served from your browser. You can also select a location on the map to populate the Map Coordinates field, or type specific coordinates in this field.

     Note
     Depending on where your sites are located, the global map on the **Sites** list page will zoom into that area. Site location is determined by the coordinates specified. The zoom factor depends on the location of the sites.
4. Select **Save**.

Related Topics

Site Parameters on page 130

Adding Device Groups to a Site

Create the site, then add device groups to the site. To understand the relationship between sites, device groups, and access points, see Device Groups on page 32.

To add a device group to an existing site:

1. Go to **Configure** > **Sites** and select a site from the list.
2. Select **Device Groups**, then select **Add**.
3. Configure the device group settings.
4. After the device group is added, select **Save** on the **Site** page.

Related Topics

Device Groups on page 32
Device Group Parameters on page 133
Profiles on page 33
RF Management on page 34
Adoption Rules on page 318

Device Group Parameters

Configure the following parameters:

Table 32: Device Group Settings

Field	Description
Name	Device Group name.
Profile	The configuration profile associated with the device group. Each AP platform has a default configuration profile. Select the default profile from the list or take one of the following actions: • To add a new profile, select . Then, provide a name and platform. • To edit a profile, select . • To copy or clone a profile, select . Then, provide a name. • To delete a profile, select

Table 32: Device Group Settings (continued)

Field	Description
RF Management	The RF Management profile associated with the device group. ExtremeCloud IQ Controller includes a default RF policy. • AP 39xx access points support Default ACS. • Wi-Fi 6 AP models access points support Default Smart RF. Select the default profile from the list or select to create a unique RF policy.
APs	List of APs that match the configuration Profile and Site regulatory domain. In order for an AP to be included in a device group: • The regulatory domain of the AP must correspond with the site Country value. • The configuration Profile of the device group must match the AP model number. Select each AP to include in the device group. Then, select **OK**. To organize your AP deployment automatically, create Adoption Rules. **Note:** You may need to create more than one configuration Profile per AP model, depending on the configuration settings you enable.

Related Topics

Add or Edit a Configuration Profile on page 134
Advanced Configuration Profile Settings on page 172
Configuring Smart RF Policy on page 187
Adoption Rules on page 318

Add or Edit a Configuration Profile

ExtremeCloud IQ Controller is installed with a default configuration Profile for each AP platform. You can modify the default Profile or create a new Profile, but default Profiles cannot be deleted.

New Profiles display the configuration settings that were delivered with your initial ExtremeCloud IQ Controller installation. After making changes, if you need to return to a base ExtremeCloud IQ Controller configuration, create a new Profile for the AP platform. The new Profile will consist of the initial settings. Before configuring a unique configuration Profile, configure the networks and roles associated with the new Profile.

1. Go to **Configure** > **Sites** and select a site.
2. Select the **Device Groups** tab.
3. To add a new device group, select **Add**. Or, select a device group from the list.

4. From the **Profile** field:
   - To add a new profile, select  . Then, provide a name and platform.
   - To edit a profile, select  .
   - To copy or clone a profile, select  . Then, provide a name.
5. Configure the following parameters:

Table 33: Profile Configuration Parameters

Field	Description
Name	Name of the configuration Profile.
AP Platform	Select the AP Platform on which to base the new configuration Profile. Then, select **Save**. The Profile settings display.
Advanced	Select **Advanced** to view or modify Advanced Configuration Profile Settings.
Networks	Lists configured networks. Select a radio band and port (if applicable) for a configured network. Enable Band Steering per SSID for Wi-Fi 6 APs.
Mesh Points	Define mesh points for a wireless mesh network. ExtremeCloud IQ Controller allows one mesh point per AP, configured on one or more radios. For more information, see Advanced Configuration and Mesh Device Settings on page 139. Transparent Bridge is supported in a mesh network. A Transparent Bridge provides a mesh link between two sites without requiring policy enforcement per device. For more information, see Transparent Bridge on page 263. **Note:** Mesh and Client Bridge cannot be configured on the same radio.
Roles	List of configured policy roles. Select a policy role. You can also add a new policy role, edit a policy role, or delete a policy role. For more information, see: • Preconfigured Policy Roles on page 124 • Add Policy Roles on page 292

Table 33: Profile Configuration Parameters (continued)

Field	Description
Radios	Configure radio mode and advanced radio settings: • **Admin Mode** - Determines the radio mode. Select **On** to enable the radio. Select **Off** to disable the radio. • **Mode** - Radio mode. Values depend on the AP model and radio band: For more information, see Understand Radio Mode on page 147. • **Client Bridge Network** - Network associated with the Client Bridge. This field displays when Radio Mode is **Client Bridge**. For more information, see Configure Client Bridge on page 144. **Note:** Client Bridge and Mesh cannot be configured on the same AP. For each radio band, select **Advanced** to configure Advanced AP Radio Settings.
Wired Ports	If the AP supports wired ports, configure port speed for each port. Valid values are: • Auto • 100M • 10M
VLANS	Topologies associated with the configuration Profile. Associate a topology to a specific device group. This enables you to define a topology that is common to a set of devices and specify a specific attached VLAN. Topologies referenced by attached networks or roles are automatically added to the Profile VLANS list. You can also add topologies manually to the list. When creating a new topology, select the Profiles to associate with the new topology. For more information, see Configuring VLANS on page 303.
AirDefense	Select a configured air defense Profile. Or, Select ⊕ to add a new Profile. Select ✎ to edit the selected Profile.
IoT	Select a configured IoT Profile. Or, Select ⊕ to add a new Profile. Select ✎ to edit the selected Profile. **Note:** Supported on AP391x, Wi-Fi 6 AP models. Not supported on AP3935 and AP3965, and not supported on the APxx-1 models.
Positioning	Select a configured Positioning Profile. Or, Select ⊕ to add a new Profile. Select ✎ to edit the selected Profile. **Note:** Supported on Wi-Fi 6 AP models.

Table 33: Profile Configuration Parameters (continued)

Field	Description
Analytics	Select a configured ExtremeAnalytics Profile. Or, Select to add a new Profile. Select to edit the selected Profile. **Note:** Supported on Wi-Fi 6 AP models.
RTLS	Select a configured RTLS Profile. Or, Select to add a new Profile. Select to edit the selected Profile.

Related Topics

Advanced Configuration Profile Settings on page 172
Understand Radio Mode on page 147
Configure Client Bridge on page 144
Advanced AP Radio Settings on page 153
VLAN Profile Settings on page 161
AirDefense Profile Settings on page 161
Analytics Profile Settings on page 170
IoT Profile Settings on page 163
Advanced Configuration and Mesh Device Settings on page 139
Positioning Profile Settings on page 169
RTLS Settings on page 171
Associated Profiles on page 137

Associated Profiles

A list of configuration Profiles that the role, network, or VLAN can be associated with. Select a Profile to make the association. Clear a check box to disassociate the Profile.

Networks and roles must be associated with a configuration Profile. Topology assignment to a site is inferred from the role and network assignment in the Profile. Each device group has a configuration Profile assignment. Therefore, APs within the device group are associated with the network definition (including VLAN assignment) and the role policy definition through the configuration Profile.

After you have configured the network and the policy, it is necessary to open each device group and associate the configured network and the defined roles by editing the assigned configuration Profile.

ExtremeCloud IQ Controller simplifies this procedure. After saving a network configuration or policy definition, ExtremeCloud IQ Controller prompts you to select the configuration Profile for association. The defined VLAN is automatically associated with the network or role.

To associate a different VLAN to a specific Profile, select from the Profile **VLANS** tab or from the **Add VLAN** dialog, select **Associated Profiles**.

Note
The association that you define applies to all device groups that use the selected configuration Profile.

If necessary, you can modify a configuration Profile from the device group. The **Associated Profiles** dialog simply makes the profile association process easier.

Related Topics

Profiles on page 33
Add or Edit a Configuration Profile on page 134
VLAN Profile Settings on page 161

Associated Networks

The **Networks** tab lists configured networks that are available to each radio and port for the selected AP model. Select a network association for each radio and wired port as necessary.

Note
When configuring Network assignment for 6GHz radios, 6E WFA Compliant networks are required. Non-compliant networks are unavailable. For more information, see Auth Type under WLAN Service Settings on page 250.

Related Topics

Networks on page 249
WLAN Service Settings on page 250
Mesh Point Network on page 260
Mesh Point Network Settings on page 262
Hotspot on page 265
Captive Portal Settings on page 276
Advanced Network Settings on page 285
Managing a Network Service on page 290
Band Steering on page 290
Associated Profiles on page 137
Configure Client Bridge on page 144

Mesh Point Profile Configuration

Configure AP Mesh Point settings from the AP configuration Profile, which is assigned at the device group level. The Root behavior setting for the AP is determined in the configuration Profile that is assigned to the device group, but this setting can be overridden from the AP Override settings for each AP. Differentiate the AP Root behavior setting one of two ways:

- **(Best Practice)** Configure two device groups: One device group for the root AP, one device group for the non-root APs. Configure separate Profiles with the appropriate

Root behavior setting for each device group. For ease of configuration, you can copy configuration Profiles and make the necessary Root behavior changes.

- Configure one device group: From the configuration Profile, configure the Root behavior as non-root. Non-root is the correct configuration for all APs in the device group except for the one root AP. Then, override the Root behavior setting on that one root AP, configuring the designated AP as the root.

Before you configure Mesh Point configuration Profile settings, verify Advanced configuration Profile settings or individual AP Override settings:

- A single mesh point is supported on multiple radios for a single AP. You can use different channels for each hop of a multiple hop mesh network. This can improve air time utilization and possibly increase throughput. However, multiple hops do not improve latency, so a best practice is to keep the number of hops less than two.
- Radio settings for the root-AP and non-root APs must match.
- When you add or remove a mesh point from a radio, the AP will reboot.
- Dual-band support is available with Mesh Point. When one radio is configured for Mesh Point, both radios can provide service.
- The recommended Poll Timeout setting for non-root APs is 60 seconds.
- Transparent Bridge — To configure a Transparent Bridge, from the GE2 Port Function field select **Bridge**.

Note
Configuration parameters you set from the configuration Profile apply to all APs in a device group. To override settings for specific AP, go to the AP radio properties. For more information, see Advanced Setting Overrides on page 221.

Note
When a single interface AP is configured as a Mesh non-root AP, the single interface is used as a client port, not as an uplink. When a single interface AP is configured as a Mesh root, the single interface is used as an uplink, not as a client port.

Related Topics

Advanced Configuration and Mesh Device Settings on page 139
Configure a Mesh Point Network on page 262
Mesh Point Network on page 260

Advanced Configuration and Mesh Device Settings

Mesh networks are comprised of mesh points that are associated with radio channels on both root and non-root APs. When the radio channel is changed on a root AP, the non-root APs can find the root through Automatic Channel Selection (ACS). A non-root mesh AP is capable of scanning multiple channels to find the best root AP, and therefore providing the best path for network traffic.

A single mesh point can be configured on one or more AP radios.

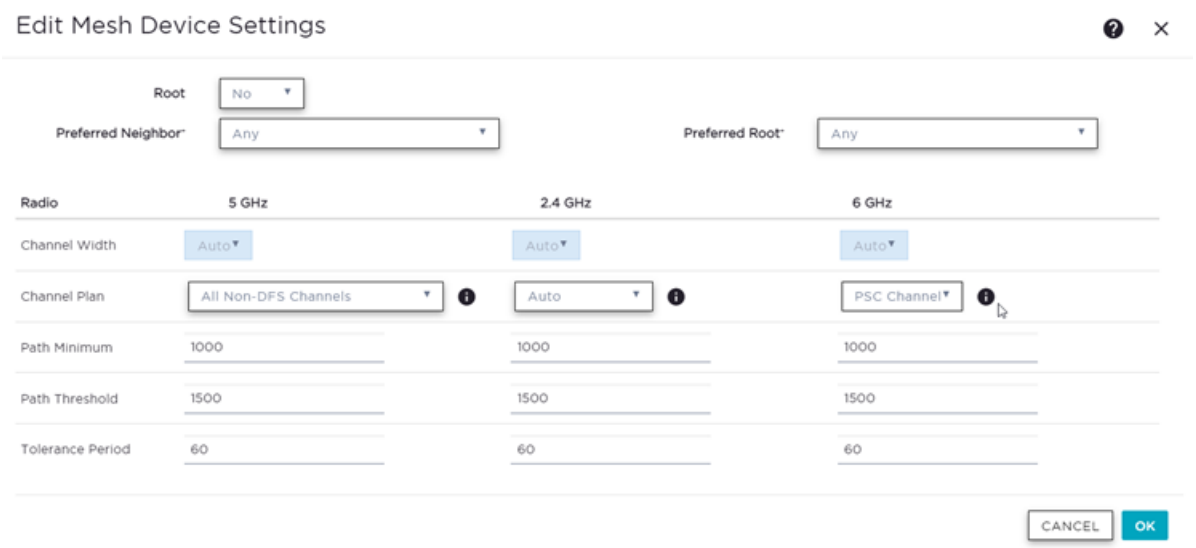


Figure 41: Mesh Point Profile Configuration, Multiple Radios

Non-root APs are configured with Mesh ACS (Automatic Channel Selection). This allows the non-root AP to follow the channel and width of the uplink AP. The non-root AP scans channels to find the best path to a root AP. Preferred Root and Preferred Neighbor settings influence the path to the root AP.

Note
Upon upgrade from earlier revisions, non-root APs in a mesh network are converted to Mesh ACS to determine the best channel.

The root AP can be configured for Auto or Fixed Channel. Mesh ACS and Smart RF offer different channel plans. The AP makes use of each plan, respectively. When using Fixed Channel, configure a channel that is part of the Mesh ACS channel plan because non-root APs use Mesh ACS. The root-AP uses the Smart RF channel plan for Auto configuration while performing as a root AP:

- When **Monitor Primary Port Link** is enabled and the backhaul connection is lost, the AP serves as a non-root AP and uses Mesh ACS to find a new root-AP.
- When **Monitor Primary Port Link** is not enabled and the backhaul connection is lost, the AP is lost.

To configure **Mesh Device Settings** in a configuration Profile:

1. On the Profile **Mesh Points** tab, select a single mesh network from one or more AP radio drop-down field.
2. Select **Advanced**.

3. Configure the following parameters:

Note
Most of the configuration settings apply to non-root APs only.

Table 34: Mesh Device Settings

AP Model	Option	AP Behavior
Wi-Fi 6 AP models	Root **Note:** Wi-Fi 6 access points can be part of the same mesh network, but they cannot participate in a mesh network with AP39xx. AP39xx access points must be a separate mesh network from the Wi-Fi 6 APs.	A root mesh point is defined as a mesh point that is connected to the WAN and provides a wired backhaul to the network. Select the root behavior of this mesh point. • **Yes** — Mesh point is root node for this mesh network. • **No** — Mesh point is not a root node for this mesh network. (Additional settings display.)
Wi-Fi 6 AP models	Monitor Primary Port Link	(Available for root APs) With Monitor Primary Port Link enabled, if a root AP loses connection to the backhaul, the non-root APs scan for a new root AP and the original root performs service as a non-root AP. When the original root AP restores connectivity, it resumes the role of root AP. Through the use of Automatic Channel Selection (ACS), the optimum path is restored.
Wi-Fi 6 AP models	Preferred Neighbor	(Available for non-root APs) Select the preferred Neighbor (AP name and radio) from a list of APs with a root or non-root mesh radio. When a non-root AP can see mesh beacons from more than one neighbor, this setting configures the AP to prefer one beacon over all others when choosing a path back to the root.
Wi-Fi 6 AP models	Preferred Root	(Available for non-root APs) Select the preferred root AP from a list of APs with a root mesh radio. Use this setting to balance the number of mesh points reporting to a specific root AP.
Radio Settings **Note:** Dual-band support is available with Mesh Point. When one radio is configured for Mesh Point, both radios can provide service.		Radio settings for the root-AP and non-root APs must match.

Table 34: Mesh Device Settings (continued)

AP Model	Option	AP Behavior
Wi-Fi 6 AP models	Channel Width	Represents the desired channel width. The channel width is set for all APs in a device group. Available options include: • Auto – Channel width is calculated automatically by the AP. It is displayed in the user interface for informational purposes only.
Wi-Fi 6 AP models	Channel Plan	Non-root APs are configured with Mesh ACS (Automatic Channel Selection). This allows the non-root AP to follow the channel and width of the uplink AP. The non-root AP scans channels to find the best path to a root AP. Preferred Root and Preferred Neighbor settings influence the path to the root AP. For APs that support 6 GHz, **PSC Channel** is an option. Because numerous channels are offered on the 6 GHz band, it is a best practice to configure the Preferred Scanning Channel (PSC) so that the amount of probing is kept to a minimum. Preferred channels function as primary channels at each channel width: 20, 40, 80, and 160 MHz. **Note:** Upon upgrade from earlier revisions, non-root APs in a mesh network are converted to Mesh ACS to determine the best channel.
Note: Path Minimum and Path Threshold are settings that refer to values in the Mesh Route Table. They are metric values determined by an algorithm that indicate when ACS scans for a better mesh point radio channel. The best route path algorithm includes elements such as hop count, data rates, RSSI, and loss rate. A perfect score is 1179.		
Wi-Fi 6 AP models	Path Minimum	The minimum root path metric value is used to evaluate the channel during the Mesh ACS scan process. Only the mesh point with a root path metric less than the minimum root path is considered a candidate mesh point that can hop to the mesh point root. Valid values are 100-20000. Default value is 1000. The lower metric value indicates a better quality mesh link to the root.

Table 34: Mesh Device Settings (continued)

AP Model	Option	AP Behavior
Wi-Fi 6 AP models	Path Threshold	The maximum root path metric value that determines when to evaluate the mesh point radio channel for a better path to the gateway. When the current path metric value exceeds this threshold, an ACS scan is triggered on the mesh point. Valid values are 800-65535. Default value is 1500. Setting this value below 1500 will result in more frequent channel scans.
Wi-Fi 6 AP models	Tolerance Period	This is a buffer period (in seconds) between when the metric value exceeds the Path Threshold and the scan begins. Set the number of seconds to allow the root path metric to recover before a scan begins. Valid values are 10-600. Default value is 60.
AP39xx	Root	• **Yes** - Mesh point is root node for this mesh network. • **No** - Mesh point is not a root node for this mesh network.
AP39xx Only	Path Selection Method	Select the method used for path selection in a mesh network. Available options include: • Uniform – The path selection method is uniform (two paths are considered equivalent if the average value is the same for these paths). Use this method for regular infrastructure meshing. • SNR-Leaf – Use this method in special infrastructure cases when it is more desirable to make path decisions based on SNR than on metric values.
AP39xx Only	Hysteresis Minimum Threshold	This is the minimum SNR value to consider a candidate for the next hop in a dynamic mesh network. For the AP39xx, this value maps to the Roaming Threshold value. • 100dB to 85dB maps to Low • 84dB to 70dB maps to Medium • 69dB to 0dB maps to High

Note
Do not rename an AP after it is added to a mesh network. Renaming the device affects the display of the reported statistics.

Related Topics

Mesh Point Network on page 260

Configure a Mesh Point Network on page 262
Add or Edit a Configuration Profile on page 134

Configure Client Bridge

Use a Client Bridge to extend a wired LAN using a wireless infrastructure. To configure a Client Bridge to work with ExtremeCloud IQ Controller take the following steps:

1. From ExtremeCloud IQ Controller, create a device group for your Client Bridge AP.
2. For RF Management, select **Default Smart RF**.
3. Edit the default configuration Profile for the AP model, specifying the client bridge settings.

   To edit the configuration Profile, select .
4. From the **Radios** tab, select **Client Bridge** as the Radio Mode value for either radio.

   Note
   Consider the following when configuring a radio as a Client Bridge:
   - Only one radio can be configured as a Client Bridge. This can be either radio. Regardless of which radio is configured as the Client Bridge, both radios will continue to provide service.
     - Radio 1 enables Client Bridge on the 2.4GHz band only.
     - Radio 2 enables Client Bridge on the 5GHz band only.
   - The Client Bridge radio will connect on the radio channel that is determined by the infrastructure AP.
   - When Client Bridge is configured on a single interface AP, the single interface is used as the client port, not as an uplink, and you will not see the **GE2 Port Function** field in the configuration Profile **Advanced Settings**.
   - Eight networks can be configured per radio. If one network is configured as a Client Bridge, seven additional networks can be configured for service on that radio.

5. Select the **Client Bridge Network**.

   The following WLAN parameters are passed to the Client Bridge AP to configure station mode on the radio:
   - Network SSID
   - Encryption or Authentication type
   - Pre-shared key

   The selected network must be configured with one of the following supported authentication types:
   - Open
   - WPA2-Personal (PSK)
   - WPA2-Enterprise 802.1x/EAP
   - WPA3-Enterprise 802.1x/EAP
   - MAC-base Authentication (MBA)

When using authentication types **WPA2-Enterprise 802.1x/EAP** and **WPA3-Enterprise 802.1x/EAP**, select the icon to configure the user ID and password.

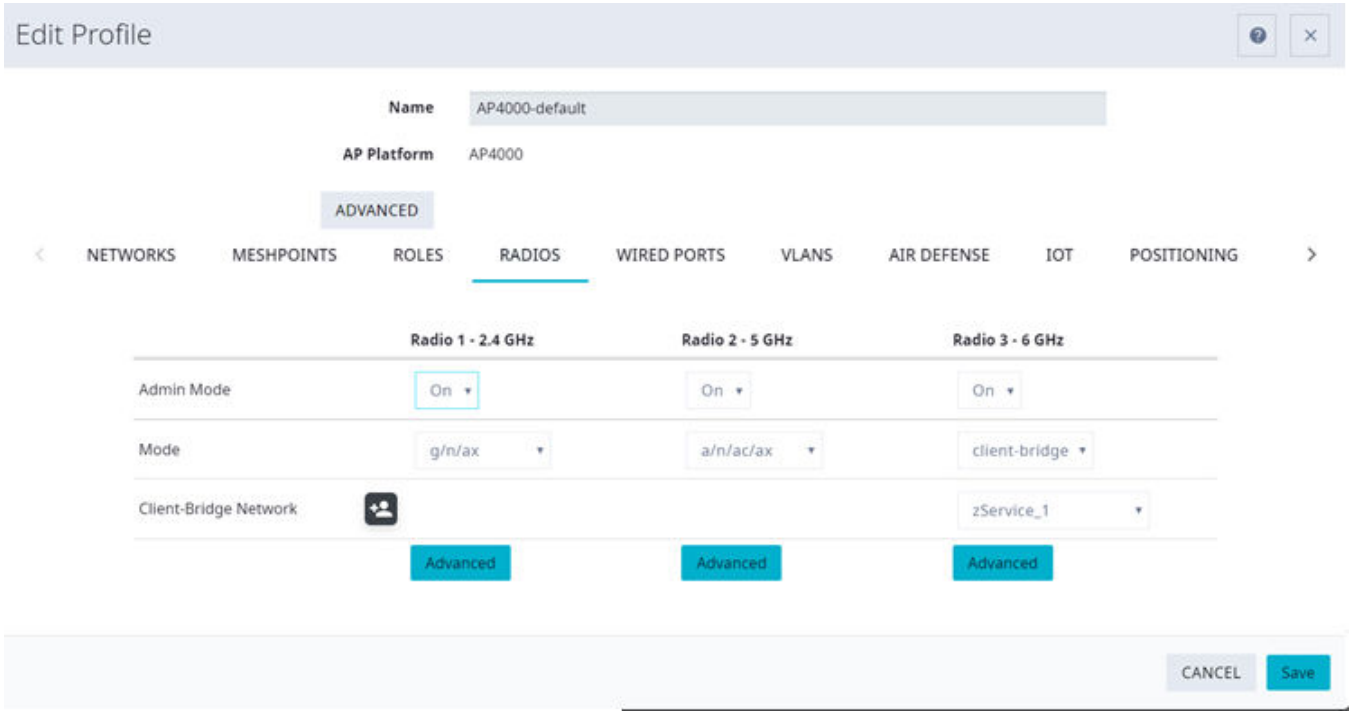


Figure 42: Configuration Profile with Client Bridge Configuration

Note
A Client Bridge AP will *not* associate to the infrastructure network with authentication types Open or WPA2-Personal (PSK) in combination with captive portal. These scenarios require user interaction.

Note
The Client Bridge network and the infrastructure AP network must match on the same radio. On the Client Bridge AP, if the 2.4 GHz radio is configured as Client Bridge, the infrastructure AP must broadcast that network on a 2.4GHz radio.

6. From the configuration Profile **Advanced** settings, the **GE2 Port Function** is automatically set to **Client** after configuring the Client Bridge radio.

   To configure a transparent point-to-point bridge that supports tagged traffic, set the **GE2 Port Function** to **Bridge**.

   Note
   - The ETH1/GE2 Bridge port is *not* supported on access points with a single Ethernet port.
   - Ports on the Universal APs are labeled with the prefix ETH.
   - When Client Bridge is configured on a single interface AP, the single interface is used as the client port, not as an uplink, and you will not see the **GE2 Port Function** field in the configuration Profile **Advanced Settings**.

7. Save the configuration Profile.
8. If you are planning to connect the end-system to the Client Bridge AP through the GE2 port, edit the configuration Profile again.
9. On the **Networks** tab, the Client Bridge network is indicated with a black highlight.

   Note
   The Client Bridge is always assigned the primary BSSID (Basic Service Set Identifier). If you change the Client Bridge network assignment, the radio is reset, resulting in a service interruption.

10. On the **Networks** tab, select **GE2** port.

    Only allow one network assignment to Client Bridge and GE2 interfaces respectively.

Figure 43: Configuration Profile Network Configuration – Client Bridge

11. Connect the Client Bridge AP to ExtremeCloud IQ Controller using the GE1 Port, which is designated as the primary port.
12. Assign the Client Bridge AP to the device group and assign the device group to the site.
13. After the Client Bridge link is established, disconnect the Client Bridge AP from the GE1 Port and ExtremeCloud IQ Controller.

    After the bridge is established, you can find the Client Bridge AP on the **Clients List**.

The end-system device traffic is connected through GE2 port (or ETH/POE port for the single interface). The Client Bridge AP communicates with the infrastructure AP on the wireless network.

When Client Bridge is configured on a single interface AP, the single interface is used as the client port, not as an uplink, and you will not see the **GE2 Port Function** field in the configuration Profile **Advanced Settings**.

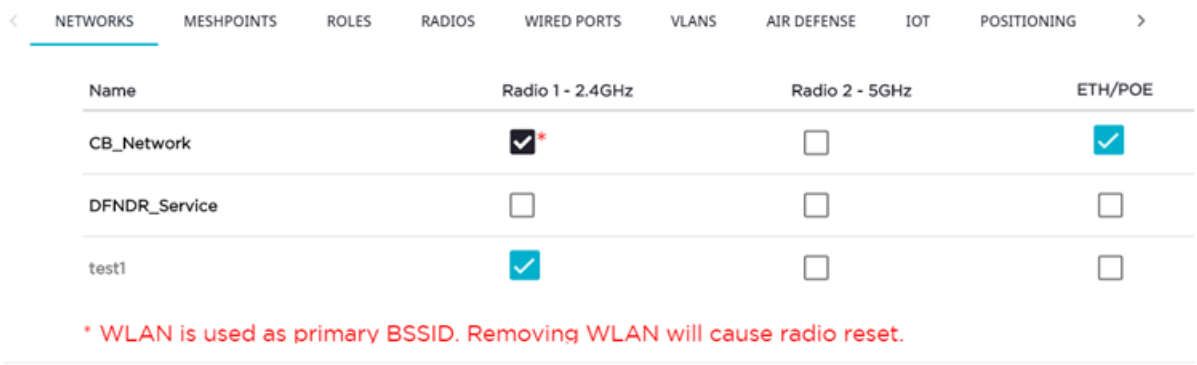


Figure 44: Configuration Profile Network Configuration – Client Bridge on a single interface AP

The wired port speed is configured on the **Wired Ports** tab.

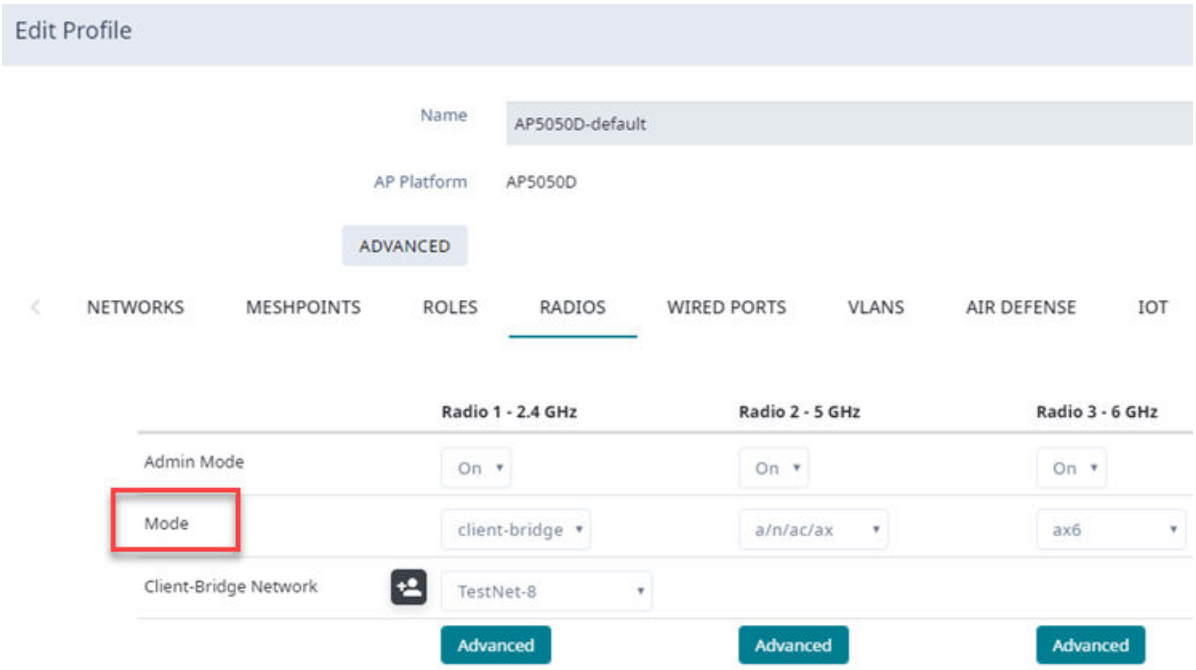
Related Topics

Transparent Bridge on page 263
Adding Device Groups to a Site on page 132
Advanced Configuration Profile Settings on page 172
AP Client Bridge on page 24
Managing Client Bridge in ExtremeCloud IQ Controller on page 27

Understand Radio Mode

Configure radio **Mode** from the device group configuration Profile **Radios** tab.

1. Go to **Sites** and select a site.
2. Select **Device Groups** and select a device group.
3. Next to the **Profile** field, select to edit the profile.
4. Select the **Radios** tab.



ExtremeCloud IQ Controller presents valid values for Radio Mode based on the AP capability.

Note

Sensor mode converts the radio to a sensor for ADSP and Positioning. The AP4xx access point models offer a third radio that is a separate sensor radio. For more information, see Radio as a Sensor on page 152.

Note
Only one radio can be configured for Client Bridge. All traffic received by the client bridge AP over wired port or by the remaining radios is forwarded to the infrastructure network via the client bridge radio.

Table 35: Radio Modes

AP Model	Radio 1	Radio 2	Radio 3
AP3000/X	2.4GHz /6GHz (dual band) • sensor • b/g • g/n • b/g/n • g/n/ax (Default) • client-bridge • ax6	5GHz • sensor • a/n/ac • a/n/ac/ax (Default) • client-bridge	
AP302W	2.4GHz /5GHz (dual band) • sensor • b/g • g/n • b/g/n • a/n/ac • g/n/ax • a/n/ac/ax • client-bridge	5GHz • a/n/ac • a/n/ac/ax • client-bridge **Note:** 160 MHz channel width not supported.	
AP305C/CX	2.4GHz /5GHz (dual band) • sensor • b/g • g/n • b/g/n • a/n/ac • g/n/ax • a/n/ac/ax • client-bridge	5GHz • sensor • a/n/ac • a/n/ac/ax • client-bridge **Note:** 160 MHz channel width not supported. AP305C must configure sensor for both radios together.	
Note: AP305C/CX offers a single port. When Client Bridge is configured on a single interface AP, the single interface is used as the client port, not as an uplink, and you will not see the **GE2 Port Function** field in the configuration Profile **Advanced Settings**. The ETH1/GE2 Bridge port is *not* supported on access points with a single Ethernet port.			

Table 35: Radio Modes (continued)

AP Model	Radio 1	Radio 2	Radio 3
• AP310i/e • AP310i/e-1	2.4GHz /5GHz (dual band) • sensor • b/g • g/n • b/g/n • a/n/ac • g/n/ax • a/n/ac/ax • client-bridge	5GHz • sensor • a/n/ac • a/n/ac/ax • client-bridge **Note:** 160 MHz channel width not supported.	
AP360i/e	2.4GHz /5GHz (dual band) • sensor • b/g • g/n • b/g/n • a/n/ac • g/n/ax • a/n/ac/ax • client-bridge	5GHz • sensor • a/n/ac • a/n/ac/ax • client-bridge **Note:** 160 MHz channel width not supported.	
• AP4000 • AP4000-1	2.4GHz • b/g • g/n • b/g/n • g/n/ax • client-bridge	5GHz • a/n/ac • a/n/ac/ax • client-bridge	6GHz/Sensor • sensor • ax6 • client-bridge
• AP410i/e • AP410i-1	2.4GHz • b/g • g/n • b/g/n • g/n/ax • client-bridge	5GHz • a/n/ac • a/n/ac/ax • client-bridge	Sensor • sensor (non-configurable)
• AP410C • AP410C-1	2.4GHz /5GHz • b/g • g/n • b/g/n • a/n/ac • g/n/ax • a/n/ac/ax • client-bridge	5GHz • a/n/ac • a/n/ac/ax • client-bridge	Sensor • sensor wireless capture limited to one stream of data (1x1) • sensor (non-configurable)

Table 35: Radio Modes (continued)

AP Model	Radio 1	Radio 2	Radio 3
AP460e	2.4GHz • b/g • g/n • b/g/n • g/n/ax • client-bridge	5GHz • a/n/ac • a/n/ac/ax • client-bridge	Sensor • sensor (non-configurable)
AP460C/S6C/S12C	2.4GHz/ 5GHz • b/g • g/n • b/g/n • a/n/ac • g/n/ax • a/n/ac/ax • client-bridge	5GHz • a/n/ac • a/n/ac/ax • client-bridge	Sensor • sensor (non-configurable)
AP5010	2.4GHz/ Tri-band Sensor, supports 2.4GHz wireless service, or a tri-band sensor • sensor • b/g • g/n • b/g/n • g/n/ax • client-bridge	5GHz • a/n/ac • a/n/ac/ax • client-bridge	6GHz • ax6 • client-bridge
AP5050U AP5050D	2.4GHz/ Tri-band Sensor, supports 2.4GHz wireless service, or a tri-band sensor • sensor • b/g • g/n • b/g/n • g/n/ax • client-bridge	5GHz • a/n/ac • a/n/ac/ax • client-bridge	6GHz (Not currently supported for regulatory compliance) • ax6 • client-bridge
AP505i	2.4GHz • sensor • b/g • g/n • b/g/n • g/n/ax • client-bridge	5GHz • sensor • a/n/ac • a/n/ac/ax • client-bridge	

Table 35: Radio Modes (continued)

AP Model	Radio 1	Radio 2	Radio 3
• AP510i/e • AP510i-1	2.4GHz /5GHz (dual band) • sensor • b/g • g/n • b/g/n • a/n/ac • g/n/ax • a/n/ac/ax • client-bridge	5GHz • sensor • a/n/ac • a/n/ac/ax • client-bridge	
AP560i/h	2.4GHz /5GHz (dual band) • sensor • b/g • g/n • b/g/n • a/n/ac • g/n/ax • a/n/ac/ax • client-bridge	5GHz • sensor • a/n/ac • a/n/ac/ax • client-bridge	
AP39xx	5GHz • sensor • a/n/ac • ac-strict	2.4GHz • sensor • b/g • g/n • b/g/n • g/n-strict	

Related Topics

AP Client Bridge on page 24
Transparent Bridge on page 263
Advanced AP Radio Settings on page 153

Radio as a Sensor

From the configuration Profile screen, set the AP radio mode to **Sensor** for supported APs. In Sensor mode, the radio does not service clients. The radio changes channels and functions as a sensor for ADSP and Positioning. Positioning can co-exist with any radio mode. The AP scans all channels that are allowed by the selected country. When the configuration Profile includes an ADSP profile, the ADSP server controls the channels, and Positioning reports the MAC addresses and RSS values that the radio receives.

ADSP is supported on all ExtremeWireless access points:

- The AP3000 and AP5000 series offer a dedicated tri-band sensor mode where both radios are set to **Sensor** at the same time.
- The AP4000 offers a 6 GHz radio band and sensor on the third radio.
- The AP4xx offers a separate sensor radio. On the AP410 and AP460, a white LED indicates sensor activity.
- On the AP3xx and AP5xx, the sensor can be set per radio — one radio can be configured as a sensor, and the other one can be configured to pass wireless traffic. The AP310 and AP510 are dual-band APs. A white LED indicates sensor selection.
- On AP39xx, both radios must be configured as sensors at the same time.

After the radio mode is set to Sensor on the configuration Profile, define the scan list under Advanced Profile settings.

Related Topics

Advanced Configuration Profile Settings on page 172
Add or Edit a Configuration Profile on page 134

Advanced AP Radio Settings

The purpose of advanced radio settings for an AP is to improve data packet throughput. Frame aggregation is a feature of the IEEE 802.11e, 802.11n, 802.11ac, and 802.11ax wireless LAN standards that increases throughput by sending multiple data frames in a single transmission. Frame transmission by an 802.11 device includes significant overhead. In fact, the overhead can consume more bandwidth than the payload itself. To address the overhead issue, the 802.11n standard offers MAC Service Data Unit (MSDU) aggregation and MAC Protocol Data Unit (MPDU) aggregation. Both types of aggregation result in a single frame. Management information is specified only once per frame; therefore, the ratio of payload data to the total volume of data is higher, resulting in greater throughput.

Note
You can configure radio settings for all APs in a device group from the device group **Radio** tab and **Advanced Radio** dialog. And you can override radio settings for one or more individual APs from the AP **Advance Settings** > **Override** dialog.

Radio settings are dependent on the access point model.

Table 36: Advanced Radio Settings

Field	Description
(Off Channel Scan) OCS Channels	**Note:** Supported on Wi-Fi 6 AP models. Define custom channel list: • Channels for Radio 1 are all 2.4 GHz or both 2.4 and 5 GHz lower band channels. Channel width is selectable. • Channels for Radio 2 are 5 GHz channels or 5 GHz upper band channels. Channel width is selectable. • Channels for Radio 3 (supported on the AP4000) are 6 GHz channels. See 6 GHz Channel Allocation and Notation on page 23 for more information.
OCS Interval (DTIMs)	Delivery Traffic Indication Message (DTIM) interval must be between 2-100. • R1 5G-L — 5.15-5.35 GHz • R2 5G-H — 5.5-5.925 GHz • R2 5G-F — 5.15-5.925 GHz • R1 2G-F —Channel 1 to 13 (Channel 14 for Japan) Supported on the following 802.11ax APs: • AP3000/X • AP310i/e • AP310i/e-1 • AP360i/e • AP4000 • AP4000-1 • AP410i/e • AP410i-1 • AP460i/e • AP505i • AP510i/e • AP510i-1 • AP560i/h • AP5010 • AP5050U/AP5050D
LDPC	Increases the reliability of the transmission resulting in a 2dB increased performance compared to traditional 11n coding.
STBC	Space Time Block Coding. A simple open loop transmit diversity scheme. When enabled, STBC configuration is 2x1 (two spatial streams combined into one spatial stream). TXBF overrides STBC if both are enabled for single stream rates. Enable this setting when you anticipate single stream clients with lower RSS power.

Table 36: Advanced Radio Settings (continued)

Field	Description
Guard Interval Mode	The guard interval is the space between characters being transmitted (not the space between packets). The default value is **Auto**, which is sufficient for most indoor deployments. Consider **Long** or **Quadruple** for outdoor deployments where devices are installed more than 100 meters away. Setting the Guard Interval to Long or Quadruple, gives each AP more time to detect the received signal, improving signal quality, but sometimes reducing signal throughput. Valid values are: • Auto • Long • Short • Quadruple Quadruple is the longest setting. It is applicable in 802.11ax mode only. **Note:** Supported on Wi-Fi 6 AP models.
Airtime Fairness Mode	Enabling Airtime Fairness organizes radio traffic allocating bandwidth to faster devices. If you have older devices on your network that are hogging bandwidth, consider enabling Airtime Fairness to give priority to faster devices.
Maximum Distance	Increasing the Maximum Distance can give APs in an outdoor deployment more time to receive acknowledgment messages. For outdoor deployments, where APs are installed more than 100 meters apart, consider increasing the Maximum Distance setting up to 15000 meters.
Tx Beam Forming	Tx Beam Forming is a technique of re-aligning the transmitter multipath spatial streams phases in order to get better signal-to-noise ratio on the receiver side. Support is based on AP model number: • AP 39xx — Available on the 5 GHz radio only. The valid values are: (multi-user) MU_MIMO and Disabled. • Wi-Fi 6 AP models — Available on the 5 GHz radio only. Valid values are (single-user) SU_MIMO, (multi-user) MU_MIMO, and Disabled. • AP4000 — Available on the 5 GHz and 6 GHz radios. Valid values are (single-user) SU_MIMO, (multi-user) MU_MIMO, and Disabled. SU-MIMO is limited to one pair of wireless devices simultaneously sending or receiving multiple data streams. MU-MIMO allows multiple wireless devices to simultaneously receive multiple data streams.

Table 36: Advanced Radio Settings (continued)

Field	Description
Radio Share Mode	Radio operates as a sensor and a traffic forwarder. Valid values are: • Off. When the radio mode is set to **Off**, the Radio Share capability is disabled. • Inline. AP reports to the ADSP server only multicast / broadcast traffic such as beacons and probe requests. Inline mode has minimal impact on AP performance, because the AP reports to the ADSP server only traffic that it processes. • Promiscuous. AP receives all packets seen on its operating channel and forwards them to the ADSP server. Promiscuous mode loads the AP resources, because AP has to process all traffic in the channel. In high-density, wireless deployments, use dedicated sensors instead of Radio Share in Promiscuous mode. Note: Set AP to Promiscuous mode when AP is required to perform Termination.
In-Band Discovery	In-band discovery mechanisms decrease the time for channel scanning the 6 GHz frequency band. This is advantageous due to the many channel options on the 6 GHz band. FILS (Fast Initial Link Setup) — Designed for dense environments, FILS provides fast roaming without 802.11r. An FILS frame is analogous to a condensed beacon. Only critical information such as SSID, BSSID, and channel can be found in an FILS frame. The AP4000 sends this broadcast action frame out every 20 time units (TUs), approximately 20 milliseconds. Supported on the 6 GHz radio band (AP4000). In-Band Discovery is disabled by default.
ADDBA Support	Block acknowledgment. Provides acknowledgment of a group of frames instead of a single frame. ADDBA Support must be enabled if Aggregate MPDU is enable.
Aggregate MSDU	Determines MAC Service Data Unit (MSDU) aggregation. Enable to increase the maximum frame transmission size.

Table 36: Advanced Radio Settings (continued)

Field	Description
802.11g protection mode	Enable this rate limit to prioritize 802.11g (ERP-OFDM) transmission allowing the 802.11g device to transmit unhindered. Protection is used when the packet rate is greater than the configured protection limit rate. For example, if the protection rate is set to 11Mbps, protection will be used when sending at rates greater than 11Mbps, which means 802.11g rates. To maintain compatibility between the older (802.11b (HR-DSSS) and the newer 802.11g (ERP-OFDM)) technologies, a mechanism was devised to allow the older 802.11b device to understand the newer 802.11g device without significantly lowering the data rate of the 802.11g client. The 802.11g device sends an RTS/CTS frame sequence (Request To Send/Clear To Send) that should be heard by all stations, it may also use only "CTS-to-self." This sequence is understood by the 802.11b station that reads the duration field from the frame and sets its NAV timer to hold off the medium until this timer expires. This allows the 802.11g to transmit unhindered. An AP notifies all clients within its service area that there are 802.11b devices present via a bit set in its beacons. Note: It is the newer protocol (802.11g) being protected from the older (802.11b) protocol. The protection rate limit threshold determines when to use protection.
Minimum Basic Rate	Defines the minimum data rate that must be supported by all stations in a BSS (Base Station Subsystem): • Select 6, 9, 12, 18, 24, 36, 48, and 54. The default value is 6.
Aggregate MPDUs	Determines MAC Protocol Data Unit (MPDU) aggregation. Enable to increase the maximum frame transmission size, providing a significant improvement in throughput.
Aggregate MPDU Max # of Sub-frames	Maximum number of sub-frames of the MAC Protocol Data Unit (MPDU) aggregation. The value range is 2-64.
DTIM	When any single wireless client associated with an access point has 802.11 power-save mode enabled, the access point buffers all multicast frames and sends them only after the next DTIM (Delivery Traffic Indication Message) beacon, which may be every one, two, or three beacons (referred to as the “DTIM interval”).

Table 36: Advanced Radio Settings (continued)

Field	Description
OFDMA	Specify the direction to use Orthogonal Frequency-Division Multiple Access (OFDMA). Valid values are: • Off • DL— downlink • UL— uplink • Both 802.11ax APs use OFDMA technology to partition a channel into resource units, allowing users with varying bandwidth needs to be served simultaneously. OFDMA is ideal for low bandwidth applications. Its benefits include: better frequency reuse, reduced latency, and increased efficiency. When OFDMA is enabled, the AP mandates the resource unit allocation for multiple clients for downlink and uplink OFDMA. A series of trigger frames are exchanged to allow multiple-user transmission in the downlink and uplink directions. To avoid overlapping of OFDMA symbols, specify a guard-interval. OFDMA is disabled by default. Supported on the following 802.11ax APs: • AP3000/X • AP310i/e • AP310i/e-1 • AP360i/e • AP4000 • AP4000-1 • AP410i/e • AP410i-1 • AP460i/e • AP505i • AP510i/e • AP510i-1 • AP560i/h • AP5010 • AP5050U/AP5050D

Table 36: Advanced Radio Settings (continued)

Field	Description
BSS Color	Configures support for 802.11ax BSS coloring and assigns the BSS color associated with the radio. BSS coloring is a means by which 802.11ax radios differentiate between overlapping Basic Service Sets (BSSs) in multi-path channels. A BSS represents a set of communicating devices consisting of one AP radio and one or more client stations. In an 802.11ax-enabled wireless network, each BSS is identified by a numerical identifier (the BSS color) added to the header of the PHY frame. BSS coloring impacts channel access behavior and spatial reuse operations. Based on the BSS color detected, APs can assign a new channel access behavior. Spatial reuse is another advantage of enabling BSS color. It applies adaptive Clear Channel Assessment (CCA) thresholds for detected Overlapping BSS (OBSS) frame transmissions, which enables APs to ignore transmissions from an OBSS and transmit at the same time. BSS color support is disabled by default. Supported on the following 802.11ax APs: • AP3000/X • AP310i/e • AP310i/e-1 • AP360i/e • AP4000 • AP4000-1 • AP410i/e • AP410i-1 • AP460i/e • AP505i • AP510i/e • AP510i-1 • AP560i/h • AP5010 • AP5050U/AP5050D

Table 36: Advanced Radio Settings (continued)

Field	Description
Target Wake Time	Enables 11ax Target Wake Time (TWT) support on the radio. The IEEE 802.11ax standard defines power-saving enhancements and improved resource scheduling features, such as scheduled sleep and wake times. TWT allows devices (APs and stations) to negotiate when and how frequently they will wake up to send or receive data. TWT increases device sleep time, thereby substantially improving the battery life of the client device. TWT is enabled by default. Supported on the following 802.11ax APs: • AP3000/X • AP310i/e • AP310i/e-1 • AP360i/e • AP4000 • AP4000-1 • AP410i/e • AP410i-1 • AP460i/e • AP505i • AP510i/e • AP510i-1 • AP560i/h • AP5010 • AP5050U/AP5050D
Cell Size Control	
Probe Suppression on Low RSS	Reduces the number of probe responses by preventing clients with low RSS from associating with an AP radio. This setting is configured per radio. Clients with RSS measured below the Probe Suppression RSS Threshold will not associate with the AP. This setting is disabled by default.
Probe Suppression RSS Threshold (dBm)	This setting is available when **Probe Suppression on Low RSS** is enabled. This setting determines the RSS threshold for forced disassociation and probe suppression. The default threshold is -90 dBm. Valid value range is -50dBm to -100dBm. **Best Practice:** Probe Suppression Threshold should not be greater than -70dB. The Probe Suppression Threshold defines the signal strength value that is deemed too low to be acknowledged by the AP. Setting the threshold above -70dB can result in an AP not acknowledging clients in close proximity, leading to poor connectivity or a sub-optimal roaming experience. The best practice is to follow the Site Survey methodology to determine the best value for the AP installation.

Table 36: Advanced Radio Settings (continued)

Field	Description
Disassociate on Low RSS	This setting is supported on AP39xx, AP3xx, AP4xx, or AP5xx. It is always disabled by default. This setting forces clients with low RSS to disassociate from an AP radio. This setting is configured per radio. A client is forced off an AP radio when RSS is measured at 5dBm below the Probe Suppression RSS Threshold. Enabling this option forces a client to roam to a better AP for improved network performance.
Probe Response Retry Limit	The default Probe Response Retry Limit is 4. If devices are having a problem connecting to the network, due to congestion or due to the quality of the device, consider increasing the retry limit. Maximum value is 10.
Rx Sensitivity Reduction (dB)	New APs are very sensitive and can pick up unwanted channel interference. If this is an issue, add an offset of 5-10 dB, which will reduce signal sensitivity and improve signal quality.
Multicast to Unicast Delivery	Converts multicast transmission to unicast for backward compatibility. Valid values are: • Disable — Transmission is not converted. • Auto — Multicast transmission is converted to unicast for the selected AP radio.

Related Topics

Advanced Setting Overrides on page 221
Add or Edit a Configuration Profile on page 134
6 GHz Channel Allocation and Notation on page 23

VLAN Profile Settings

Associate a topology to a specific device group. This enables you to define a topology that is common to a set of devices and specify a specific attached VLAN.

Topologies referenced by attached networks or roles are automatically added to the Profile VLANS list. You can also add topologies manually to the list. When creating a new topology, select the Profiles to associate with the new topology.

Related Topics

Configuring VLANS on page 303

AirDefense Profile Settings

The AP integrates with the Extreme AirDefense (AirDefense), offering an additional profile option that allows the AP to function as an AirDefense sensor or to act as a sensor and retain the ability to forward traffic.

When the AP is configured with an AirDefense dedicated sensor profile, the functionality of the AP is controlled by the AirDefense server. When the AP is

configured as a AirDefense Radio Share profile, it continues to forward traffic while sending packets to an AirDefense server. To ensure rate performance, an AP configured with a Radio Share profile does not forward its own Tx/Rx data to the ADSP server.

The AP3xx, AP4xx, and AP5xx support Radio Share and OCS. You have the option to scan neighboring channels in addition to the operating channel. AP4xx also offers a separate sensor radio.

1. Configure the following settings:

Table 37: AirDefense Profile Settings

Field	Description
Name	Name of AirDefense profile.
Add Server Address	The IP address of the AirDefense servers. Provide the FQDN or IPv4 string, maximum 255 characters. Enter the IP address, then click . The IP address is added to the **Servers** list. **Note:** When using the AirDefense Base (add-on container application), provide the IP address of the ExtremeCloud IQ Controller data port that is reachable by the APs and sensors.
Port	Specify a port for the AirDefense server. The default port is 443 (used with a dedicated external AirDefense Server). **Note:** When using the AirDefense Base (add-on container application), configure port number to **32032**.
Servers	List of IP addresses for servers. Click to remove an IP address from the list.

2. Select **Save**.

Related Topics

Radio as a Sensor on page 152
Advanced AP Radio Settings on page 153
Add or Edit a Configuration Profile on page 134
ADSP Support on .11ax APs on page 162
AirDefense Base Application on page 472

ADSP Support on .11ax APs

The following ADSP features are supported on the Wi-Fi 6 AP models:

- LiveView under Sensor Mode
- LiveView under Radio Share Mode
- Scan Pattern Support from the ADSP Server for Sensor.
- Termination under Sensor and Radio Share Modes.

- Rogue AP on the Wired interface.
- Threat detection and alarms are supported.

Note
AP Test *is not* supported on ExtremeWireless AP39xx.

Related Topics

AirDefense Profile Settings on page 161

IoT Profile Settings

The Internet of Things (IoT) refers to the myriad of devices that include beacons and the sensors that scan for and collect beacon data.

ExtremeCloud IQ Controller supports IoT beacon and scanning technology for a specific brand and generic BLE scanning. Both iBeacon and Eddystone-url offer both beacon and scan functions. In addition, ExtremeCloud IQ Controller supports generic scanning.

Configure a separate IoT profile for each IoT function and application or for a generic BLE scan:

1. Specify a profile name.
2. Specify a profile function — BLE Beacon or BLE Scan.
3. Select the IoT application or generic scan function.

Table 38: Supported IoT Options by Function

BLE Beacon Options	BLE Scan Options
• iBeacon • Eddystone-url Beacon	• iBeacon Scan • Eddystone-url Beacon Scan • Generic Scan

The resulting parameters depend on the function and application you select.

The following AP models support IoT regardless of the IoT application that is configured:

- AP3000/X
- AP302W
- AP305C/CX
- AP310i/e
- AP360i/e
- AP4000
- AP410i/e
- AP410C
- AP460i/e
- AP460C/S6C/S12C
- AP505i

- AP510i/e
- AP560i/h
- AP5010
- AP5050U/AP5050D
- AP391x

The following AP models *do not* support IoT:

- AP3935
- AP3965
- AP305C-1
- AP310i/e-1
- AP410i-1
- AP410C-1
- AP510i-1
- AP4000-1

Related Topics

Generic BLE Scan Settings on page 164
iBeacon Settings on page 165
iBeacon Scan Settings on page 167
Eddystone-url Beacon Settings on page 168
Eddystone-url Scan Settings on page 169
Add or Edit a Configuration Profile on page 134

Generic BLE Scan Settings

Generic BLE Scan extends the BLE Beacon function to a generic beacon format. The generic option enables the AP to detect and forward beacon messages for specified vendors.

Note
Generic BLE Scan is not supported on the AP3900 series access points.

Table 39: Generic BLE Scan Settings

Field	Description
Name	Unique profile name.
Function	Determines the purpose of the IoT profile. Select **BLE Scan**.
Application	Determines application type based on the previously selected function **BLE Scan**. Select **Generic**.
Scan	
Interval (ms)	Determines how long to wait between scans. Valid values are: Min (100ms) and Max (10240ms). The default value is Min (100ms).

Table 39: Generic BLE Scan Settings (continued)

Field	Description
Window (ms)	Determines how long to scan per channel. Valid values are Min (100ms) and Max (10240ms).Value must be less than Scan Interval value. Default value is 100ms.
Filter	
Unique Company Identifier	Identifier used to differentiate a large group of related beacons. A company can have a network of beacons with the same Company ID. Used for filtering data. If specified, the APs only forward beacons with matching values in the 2-byte field (bytes 6-7). A value of **Any** indicates that no filtering is applied. Look up Company IDs at https://www.bluetooth.com/specifications/assigned-numbers/company-identifiers/.
Min RSSI [dBm]	This is the signal strength required to include the packet in the BLE report. Valid values: -10 to -100. Default value is -100. Data from beacons with an RSSI that is less than the Min RSSI configured value is filtered out.
Destination	
IP Address	IP address of the customer Application Server that receives the beacon report.
Port	Destination Port on the customer Application Server that presents the beacon report. **Best Practice:** Verify that the server IP address and Port number specified in the Profile are open.

Related Topics

iBeacon Settings on page 165
iBeacon Scan Settings on page 167
Eddystone-url Beacon Settings on page 168
Eddystone-url Scan Settings on page 169
Advanced Setting Overrides on page 221

iBeacon Settings

Table 40: iBeacon IoT Settings

Parameter	Description
Name	Unique profile name.
Function	Determines the purpose of the IoT profile. Select **BLE Beacon**.
Application	Determines application type based on the previously selected function **BLE Beacon**. Select **iBeacon**.
Advertising Interval	The advertising interval for the beacon application. Valid values are: Min (100ms) and Max (10240ms). The default value is Min (100ms).

Table 40: iBeacon IoT Settings (continued)

Parameter	Description
UUID	Identifier used to differentiate a large group of related beacons. A company can have a network of beacons with the same UUID.
Major	Identifies *a subset of beacons* within the larger set. This value could represent a venue specific attribute, such as a specific store or wing in a building. Valid values are 0 to 65535. This setting can be defined for a specific AP. For more information, see Advanced Setting Overrides on page 221.
Minor	Identifies *an individual beacon*. Used to more precisely pinpoint beacon location. This value complements the UUID and Major values to provide more granular identification of a specific location, such as a particular shelf, door-way, or item. Valid values are 0 to 65635. Specify 0 for **Random Minor**. ExtremeCloud IQ Controller generates the Minor value. This ensures that each AP receives a unique value. This setting can be defined for a specific AP. For more information, see Advanced Setting Overrides on page 221.
Measured RSSI	The calibrated (or measured) RSSI, in dBm for the beacon. The transmitted beacon includes this value in the tag. Default values are: iBeacon -47dBm, Eddystone beacon -5dBm. The default precision value is acceptable in most cases. To calibrate your own precise value: Using Eddystone Beacon, measure the actual transmitter output from 1 meter away and add 41dBm. (41dBm is the signal loss that occurs over 1 meter.) If you are using Apple iBeacon, refer to: "Calibrating iBeacon" at https://developer.apple.com/ibeacon/Getting-Started-with-iBeacon.pdf This setting can be defined for a specific AP. For more information, see Advanced Setting Overrides on page 221.

Related Topics

iBeacon Scan Settings on page 167
Eddystone-url Beacon Settings on page 168
Eddystone-url Scan Settings on page 169
Generic BLE Scan Settings on page 164
Advanced Setting Overrides on page 221

iBeacon Scan Settings

Table 41: iBeacon Scan Settings

Field	Description
Name	Unique profile name.
Function	Determines the purpose of the IoT profile. Select **BLE Scan**.
Application	Determines application type based on the previously selected function **BLE Scan**. Select **iBeacon Scan**.
Scan	
Interval	Determines how long to wait between scans. Valid values are: Min (100ms) and Max (10240ms). The default value is Min (100ms).
Window	Determines how long to scan per channel. Valid values are Min (100ms) and Max (10240ms).Value must be less than Scan Interval value. Default value is 100ms.
Filter	
UUID	Identifier used to differentiate a large group of related beacons. A company can have a network of beacons with the same UUID. Used for filtering data. ExtremeCloud IQ Controller forwards data with matching UUID to the Application Server and filters out all other UUID data. If UUID configured value is all zeros, no filtering occurs.
Min RSSI [dBm]	This is the signal strength required to include the packet in the BLE report. Valid values: -10 to -100. Default value is -100. Data from beacons with an RSSI that is less than the Min RSSI configured value is filtered out.
Destination	
IP Address	IP address of the customer Application Server that receives the beacon report.
Port	Destination Port on the customer Application Server that presents the beacon report. **Best Practice:** Verify that the server IP address and Port number specified in the Profile are open.

Related Topics

iBeacon Settings on page 165
Eddystone-url Beacon Settings on page 168
Eddystone-url Scan Settings on page 169
Generic BLE Scan Settings on page 164

Eddystone-url Beacon Settings

Table 42: Eddystone-url Beacon Settings

Field	Description
Name	Unique profile name.
Function	Determines the purpose of the IoT profile. Select **BLE Beacon**.
Application	Determines application type based on the previously selected function **BLE Beacon**. Select **Eddystone-url Beacon**.
URL	The URL that is included with the Eddystone-url beacon. The URL is limited to 17 characters. The 17 characters does not include the protocol, but it does include the domain name. A secure protocol (HTTPS address) is required. The URL is compressed, effectively allowing more than a 17-character input. See https://github.com/google/eddystone/tree/master/eddystone-url for the Eddystone-url compression rules to more accurately judge the length of your URL. If necessary, also find third-party URL Shortening Services available on the internet. This setting can be defined for a specific AP. For more information, see Advanced Setting Overrides on page 221.
Advertise Interval	The advertising interval for the beacon application. Valid values are: Min (100ms) and Max (10240ms). The default value is Min (100ms).
Measured RSSI	The calibrated (or measured) RSSI, in dBm for the beacon. The transmitted beacon includes this value in the tag. Default values are: iBeacon -47dBm, Eddystone beacon -5dBm. The default precision value is acceptable in most cases. To calibrate your own precise value: Using Eddystone Beacon, measure the actual transmitter output from 1 meter away and add 41dBm. (41dBm is the signal loss that occurs over 1 meter.) If you are using Apple iBeacon, refer to: "Calibrating iBeacon" at https://developer.apple.com/ibeacon/Getting-Started-with-iBeacon.pdf This setting can be defined for a specific AP. For more information, see Advanced Setting Overrides on page 221.

Related Topics

iBeacon Settings on page 165
iBeacon Scan Settings on page 167
Eddystone-url Scan Settings on page 169
Generic BLE Scan Settings on page 164

Eddystone-url Scan Settings

Table 43: Eddystone-url Scan Settings

Parameter	Description
Name	Unique profile name.
Function	Determines the purpose of the IoT profile. Select **BLE Scan**.
Application	Determines application type based on the previously selected function **BLE Scan**. Select **Eddystone URL Scan**.
Scan	
Scan Interval	Determines how long to wait between scans. Valid values are: Min (100ms) and Max (10240ms). The default value is Min (100ms).
Scan Window	Determines how long to scan per channel. Valid values are Min (100ms) and Max (10240ms).Value must be less than Scan Interval value. Default value is 100ms.
Filter	
Min RSSI [dBm]	This is the signal strength required to include the packet in the BLE report. Valid values: -10 to -100. Default value is -100. Data from beacons with an RSSI that is less than the Min RSSI configured value is filtered out.
Destination	
IP Address	IP address of the customer Application Server that receives the beacon report.
Port	Destination Port on the customer Application Server that presents the beacon report. **Best Practice:** Verify that the server IP address and Port number specified in the Profile are open.

Related Topics

iBeacon Settings on page 165
iBeacon Scan Settings on page 167
Eddystone-url Beacon Settings on page 168
Generic BLE Scan Settings on page 164

Positioning Profile Settings

A Positioning profile is part of the larger device configuration profile. The Positioning profile enables position-aware services for the APs. You can configure tracking for all clients or only clients that are actively associated with the AP.

As part of the device group's configuration profile, the Positioning profile applies to all devices in the specific device group.

Note
Supported on Wi-Fi 6 AP models.

1. Configure the following parameters:

   Name

   Name for the Positioning Profile.

   Collection

   Determines the level of client data collection. Valid values are:

   - Off. Disable Positioning Services.

     Setting to Off stops all RSS collection from the APs, including Location Events.
   - Active Clients. Track associated clients to the selected AP. When you select this option, you will not be able to view un-associated clients on a floor plan.
   - All Clients. Track both associated and unassociated clients.
2. Select **Save**.

Related Topics

Add or Edit a Configuration Profile on page 134
Position Aware Services on page 35
Positioning Heatmaps on page 67

Analytics Profile Settings

Configure the AP to integrate with the Extreme Networks premier analytics solution ExtremeAnalytics™.

Note
Supported on Wi-Fi 6 AP models.

IPFIX reporting is directed through ExtremeCloud IQ Controller.

1. Configure the following settings:

Table 44: Analytics Profile Settings

Field	Description
Name	Name of Analytics profile.
Netflow Collector Address	The IP address of the ExtremeAnalytics server.
Netflow Export Interval	Report update in seconds.

2. Select **Save**.

Each AP platform can support up to 10 ExtremeAnalytics profiles.

Related Topics

Add or Edit a Configuration Profile on page 134

RTLS Settings

A Real-Time Location System (RTLS) profile must be configured and enabled within ExtremeCloud IQ Controller before ExtremeCloud IQ Controller will communicate with the location-based server and before the APs will perform location-based functionality. ExtremeCloud IQ Controller supports the following location-based solutions:

- AeroScout
- Ekahau
- Centrak.
- Sonitor

Configure the AP to integrate with a Real-Time Location System (RTLS).

1. Select the plus sign to create a new profile ( ).
2. Configure the following parameters:

Table 45: RTLS Parameters

Field	Description
Name	Provide a name for the RTLS profile.
Application	Select a supported RTLS application. Valid values are: • AeroScout • Ekahau • Centrak. Supported on AP39xx only. • Sonitor
Server IP Address	The IP address of the RTLS application server.
Server Port	Server port of the RTLS application server.
Multicast MAC	Multicast MAC address for the RTLS application server.
Note: Centrak and Ekahau configuration offer a default port number and multicast address. You can modify the default values if necessary.	

3. Select **Save**.

Consider the following information related to Real-Time Location System (RTLS):

- Ensure that your location-based service tags are configured to transmit on all non-overlapping channels 1, 6 and 11 (and on channels above 11 where allowed). For information about proper deployment of the location-based solution, refer to the third-party documentation (AeroScout/Ekahau/Centrak).
- Within an availability pair, tag report transmission pauses on fail-over APs until the APs are configured and notified by the location-based server. With an availability pair, it is good practice to configure each ExtremeCloud IQ Controller with the same location-based service.
- An RTLS profile cannot be deleted when it is part of an active configuration profile.

Related Topics

Add or Edit a Configuration Profile on page 134

Advanced Configuration Profile Settings

To access a configuration profile for a device group:

1. Go to **Configure** > **Sites**.
2. Select a site, then select **Device Groups**.
3. Next to **Profile**, select  to edit the device group profile.

To edit Advanced settings, from the **Edit Profile** page, select **Advanced** and configure the following parameters:

Table 46: Advanced Configuration Profile Settings

Field	Description
Client Balancing	Enable Client Balancing to distribute client traffic evenly between APs in the same device group. In an availability pair, create a device group on each appliance. The APs within each group will manage the user traffic within that group.
Secure Tunnel	Provides encryption, authentication, and key management between the APs and/or the appliance. Valid values are: • Off — Secure Tunnel is turned off and no traffic is encrypted. All SFTP/SSH/HTTP traffic works normally. • Control & Data — This mode only benefits Bridged@AC VLAN topologies. An IPsec tunnel is established from the AP to the appliance and all SFTP/SSH/HTTP/WASSP control and data traffic is encrypted. The AP skips the registration and authentication phases, and when selected, the Secure Tunnel feature can be configured. This is the default setting. • Debug — An IPsec tunnel is established from the AP to the appliance, no traffic is encrypted, and all SFTP/SSH/HTTP/WASSP traffic works normally. The AP skips the registration and authentication phases and when selected, the Secure Tunnel feature can be configured.

Table 46: Advanced Configuration Profile Settings (continued)

Field	Description
Enforce Manufacturing Certificate	Enforce usage of Extreme PKI (Public Key Infrastructure) when establishing an IKE (Internet Key Exchange) tunnel. Both APs and controllers have Extreme CA certificates installed. When this setting is enabled, the controller accepts only APs that provide Extreme PKI. **Note:** Supported on the Defender Adapter SA201 and on the ExtremeWireless access point models: AP39xx, Wi-Fi 6 AP models. This setting *is not* supported on the AP305C, AP410C, and AP460C access point models. There must be successful mutual authentication between the AP and the controller. If either side of the authentication fails, the tunnel is rejected. When this setting is enabled, APs that are not PKI capable (self-signed certificates) *are not* able to connect to the controller. The default is to clear this option. When this setting is cleared, the controller accepts the AP with a self-signed certificate. With either type of certificate, the certificate type must match in both directions before the authenticated tunnel is established. Authentication failure messages are logged in the ExtremeCloud IQ Controller Events Log. You can override the configuration Profile setting for individual APs from the **Advanced** > **Overrides** dialog for the selected AP.
Enable SSH	Determines if the Secure Shell (SSH) protocol is enabled. Enable SSH for direct access to an AP. When enabling SSH, configure a password. To configure an SSH password, go to **Admin** > **System** > **Maintenance**. You can enable SSH for each AP profile. By default, this setting is disabled.
Session Persistence	Determines if session persistence is enabled. A persistent session directs a client's requests to the same backend server for the duration of a session or the time it takes to complete a task or transaction. Enable this option to improve request response times. For more information, see Session Persistence on page 180.
Mgmt VLAN ID	Separating management traffic from user data traffic is a recommended practice. The Management VLAN ID is 1 by default. AP will accept wireless client even without active connection to ExtremeCloud IQ Controller on WLANs where ExtremeCloud IQ Controller is not required. You can override the configuration Profile setting for individual APs from the **Advanced** > **Overrides** dialog for the selected AP.

Table 46: Advanced Configuration Profile Settings (continued)

Field	Description
Tagged	Check this option to tag the VLAN. Tagged VLAN packets include header information that identifies which VLAN the packet is coming from. You can configure Tagged VLANs for all APs in a device group from the device group **Advanced Settings** dialog. You can override the configuration Profile setting for individual APs from the **Advanced** > **Overrides** dialog for the selected AP.
MTU	Maximum Transmission Unit in bytes. Determines the maximum size of each packet in transmission. Standard size is 1500 bytes. ExtremeCloud IQ Controller now supports up to 1800 bytes. This enhancement facilitates the transport of MU-DATA specifically between the AP and the appliance (or between the AP and a switch for VxLAN deployments) without incurring fragmentation. You can override the configuration Profile setting for individual APs from the **Advanced** > **Overrides** dialog for the selected AP.
Scan Mode	**Note:** Supported on Wi-Fi 6 AP models. Determines which channels are scanned. Valid values are: • Default Scan. — Scans all supported channels. Optimized to scan widest possible channel. • Channel Lock — Scans on single channel. • Custom Scan — Scan is based on a selected custom list. Define a custom channel list including channel width. ◦ Radio 1 channels are 2.4 GHz (AP510i/e includes 5 GHz channels). ◦ Radio 2 channels are 5GHz. ◦ Radio 3 channels (supported on the AP4000) are 6 GHz.
Scan Channels	Select channels for a custom channel list used for **Custom Scan** Scan Mode.

Table 46: Advanced Configuration Profile Settings (continued)

Field	Description
GE2 Port Function	**Note:** Ports on the Universal APs are labeled with the prefix ETH. Specify the function of the second AP Ethernet port: • Client. Indicates that the client port is enabled on the AP. The client option is used in the following scenarios: ◦ When an AP radio is configured as a Client Bridge. ExtremeCloud IQ Controller automatically sets the GE2 port to **Client**. ◦ To leverage the second port of the access point as a Client port, allowing pass-through access to attached clients. Client access is subject to policy. This capability is also utilized in support of work group meshing. A GE2 Client port is supported on the following access points: ▪ Wi-Fi 6 AP models ▪ AP3965 When the GE2 Port is set to **Client**, the WLAN assignment dialog displays an option to specify the GE2 assignment, and the **Wired Ports** tab is available from the AP Profile. • When the GE2 Port is set to **Bridge**, the port provides a transparent bridge that transports tagged and untagged traffic between two sides of a wireless connection, while preserving VLAN mappings over the wireless link. Packet tagging and policy is configured through services outside the wireless network configuration. A GE2 Bridge port is supported on the following access points that have more than one Ethernet port: Wi-Fi 6 AP models. **Note:** The ETH1/GE2 Bridge port is *not* supported on access points with a single Ethernet port. For more information, see Transparent Bridge on page 263. • AP Ethernet port traffic backup (failover) between GE1 and GE2 • LAG (Link Aggregation Group) Link aggregation combines network connections to increase throughput and to provide redundancy in case of link failure. Requires that both ports negotiate to the same speed (1 Gbps). **Note:** LAG is supported on ExtremeWireless AP39xx and 11ax APs. LAG *is not* supported on AP305C, AP410C, and AP460C.

Table 46: Advanced Configuration Profile Settings (continued)

Field	Description
	You can override the configuration Profile setting for individual APs from the **Advanced** > **Overrides** dialog for the selected AP.
USB Power	**AP models AP5010 only**. Provides 2.5W of power to the USB port to power external USB devices. Valid values are: • Off. USB power is turned off. • Auto. USB power turns on when the AP is powered by 802.3at (radios reduced to 3x3), 802.3bt, or external power supply. USB functions in the configuration Profile are disabled by default. You can override the configuration Profile setting for individual APs from the **Advanced** > **Overrides** dialog for the selected AP. **Note:** For more information, see AP5000 Series Power Management on page 21.
PSE Power	Supports power to the PSE port for supported APs: AP310i/-1, AP310e, AP302W, and AP5010. Functions in the AP3xx configuration Profile are set to Auto by default. Valid values are: • Off. PSE power is turned off. • Auto. Ports provide power when the AP receives enough power to support the feature. APs can run on Low power, but for PSE power, the minimum power required is dependent on the AP model (AT power for AP310i/e and AP302W; BT power for AP5010). **AP models AP5010 only**. Provides 802.3af/15.4W of PSE power to the ETH1 port. Auto indicates that PSE power is turned on when the AP is powered by 802.3bt. For more information, see AP5000 Series Power Management on page 21. You can override the configuration Profile setting for individual APs from the **Advanced** > **Overrides** dialog for the selected AP. **Note:** Configuration override is supported for APs running AP firmware version 10.02.01 or later.

Table 46: Advanced Configuration Profile Settings (continued)

Field	Description
AP Event Level	Specify the message level you want included in the AP Events Log. Valid values are: • Critical • Major • Minor • Info You can override the configuration Profile setting for individual APs from the **Advanced** > **Overrides** dialog for the selected AP. For more information, see Advanced Setting Overrides on page 221. Additionally, you can override the configuration Profile setting for multiple APs from the Device List Actions menu.
Poll Timeout (Seconds)	Specifies the amount of time, in seconds, to wait for a response from the appliance before rebooting. The value range is from 3 to 600 unless the controller is in an availability pair without fast failover enabled. The default value is 3. **Note:** When configuring a Mesh network, we recommend a value of at least 60 for the non-root AP configuration. Also, it is a best practice to wait at least 60 seconds before applying configuration changes that are applicable to non-root (node) access points. This ensures that possible interruptions due to configuration changes are resolved. You can override the configuration Profile setting for individual APs from the **Advanced** > **Overrides** dialog for the selected AP.
FA Auth Key	Configure custom Fabric Attach Authentication Keys up to 32 characters in length. Extreme Networks products offer a default FA AUTHENTICATION-KEY built-in. You can also configure a custom key here. When a custom key is not configured, the default key is used. The following special characters are *not* supported: {? <tab> \ “ `} You can override the configuration Profile setting for individual APs from the **Advanced** > **Overrides** dialog for the selected AP. **Note:** Supported on AP39xx, Wi-Fi 6 AP models access points.

Table 46: Advanced Configuration Profile Settings (continued)

Field	Description
LED Status	The LED Status pattern can indicate that the configuration profile has been pushed to the destination appliance. Select an LED Status. Valid values are: **Off** LEDs do not light. **Locate** LEDs blink so you can locate the AP. **Normal** Default mode for all APs. Identifies the AP status during the following processes: • registration • power on • boot **Note:** The value **Solid** has been deprecated in ExtremeCloud IQ Controller version 5.26.02. If Solid was previously configured, this value is mapped to **Normal** with the ExtremeCloud IQ Controller version 5.26.02 upgrade. You can override the configuration Profile setting for individual APs from the **Advanced** > **Overrides** dialog for the selected AP.
PEAP User Name and Password	Ability to configure the PEAP (Protected Extensible Authentication Protocol) user name and password for all devices in a device group or for a specific device override. Used to pre-provision devices for authorization to connect to the network. Credential and Certificate installation procedures are supported for AP39xx, SA201 Adapter, and Wi-Fi 6 AP models. You can override the configuration Profile setting for individual APs from the **Advanced** > **Overrides** dialog for the selected AP.

Table 46: Advanced Configuration Profile Settings (continued)

Field	Description
Client Bridge Roaming RSS threshold [dBm]	Determines when the client bridge AP scans to find a better infrastructure AP. Valid range: from -128 to -40. Default value is -70. A scan is triggered when one or more of the following criteria is met: • When the infrastructure AP RSS value is less than the configured RSS Threshold. • When the poll of the infrastructure AP is lost for one second. **Note:** When a WLAN is configured on the client bridge AP, a scan is triggered whenever the poll of the infrastructure AP is lost, regardless of the RSS Threshold. You can override the configuration Profile setting for individual APs from the **Advanced** > **Overrides** dialog for the selected AP.
Smart Poll	Reports link stability between the AP and a selected target (typically the appliance). Select **Enable** to enable the report feature and configure the following settings: • Smart Poll — Disable/Enable. The default value is Disable. • Smart Poll Interval in seconds. Valid values are: ◦ 5 ◦ 30 ◦ 60 ◦ 300 (5 minutes) Default value • Smart Poll Target — Identifies the target. Select ⊞ to add a target address. Enter up to 10 IP addresses or Fully-Qualified Domain Names (FQDN). ExtremeCloud IQ Controller validates the address. • Smart Poll Deadline — Deadline for the poll response in seconds. If the response is not received within the specified deadline, the poll status is failed. You can override the configuration Profile setting for individual APs from the **Advanced** > **Overrides** dialog for the selected AP.

Related Topics

Advanced AP Settings on page 221
Advanced Setting Overrides on page 221
View All AP Events on page 381

Session Persistence

Session Persistence applies to the session state on the AP. RADIUS authentication is always handled through the appliance — this can be the local ExtremeCloud IQ Controller or a third-party appliance. Associated clients remain unaffected by a lack of connectivity to the appliance.

When using MBA or 802.1x, the authenticating appliance must be visible. When enabling MBA, the selected 'MBA Timeout Role' provides the default role to which users are automatically assigned. The role can be permissive or restricted, depending on the administrative configuration. See WLAN Service Settings on page 250. When using 802.1x, if none of the appliances are available, then likely there is no path-to-authentication and new clients will be unable to authenticate on the wireless network. If the network association is set to OPEN or PSK SSIDs, no authentication is required and the AP will associate the device based on the 'Default Non-Auth' Role setting configured for the network.

Configuring RF Management

RF Management profiles are AP model dependent and reusable. Default profiles are intended to make RF Management easy, getting you up and running without having to configure an RF policy. However, you can always create additional profiles based off of default RF Management profiles. The RF Management support is dependent on the AP model.

The following AP models are supported:

- AP39xx supporting ACS Policy for RF Management
- Wi-Fi 6 AP models supporting Smart RF Policy for RF Management

Related Topics

Configuring ACS RF Policy on page 185
Configuring Smart RF Policy on page 187

Basic RF Management Settings

From the **Basic** tab, set the RF Management policy for both ACS and Smart RF. Select **Smart Monitoring Enabled** to display the Smart RF settings.

Table 47: Basic RF Management Settings

Field	Description
Name	Name of the RF Management policy.
Smart Monitoring Enabled	When enabled, detector radios monitor their coverage areas for potential failed peers or coverage area holes requiring transmission adjustments for coverage compensation. Smart Monitoring is enabled by default. When Smart Monitoring is disabled, the following RF Management tabs are not displayed: **Scanning**, **Recovery**, and **Select Shutdown**. And the following settings are not displayed on the **Basic Settings** page: Sensitivity and Recovery options.

Table 47: Basic RF Management Settings (continued)

Field	Description
Sensitivity **Note:** Available for Smart RF policy only.	Determines pre-defined thresholds for Smart RF. Valid values are: • Low — Interference recovery 30 dBm. Coverage Hole Recovery 20 dBm • Medium — Interference recovery 20 dBm. Coverage Hole Recovery 20 dBm • High — Interference recovery 5 dBm. Coverage Hole Recovery 20 dBm • Custom. Select **Custom** to modify Smart RF settings. **Note:** If the sensitivity setting is too low, you may be tolerating channel congestion, impacting network performance. If the sensitivity setting is too high, you may have difficulty finding an optimal channel. The default Smart RF policy that is delivered with ExtremeCloud IQ Controller is configured with **Medium** sensitivity.
Interference Recovery	Determines optimum channel due to noise thresholds, client count and other factors that influence channel switching algorithms. To avoid channel flapping, a defined hold-timer disables interference avoidance for a specific period of time upon detection. Interference Recovery is enabled for the default Smart RF policy.
Coverage Hole Recovery **Note:** Available for Smart RF policy only.	Determines radio power adjustments to react to holes in RF coverage in an AP deployment area. Smart RF determines the radio power adjustments required based on a reporting client's signal to noise (SNR) ratio. If a client's SNR is above the administrator threshold, the connected AP's transmit power increases until the noise rate falls below the threshold. Coverage Hole Recovery is enabled for the default Smart RF policy.
Neighbor Recovery	Determines coverage behavior when a radio failure is detected within the coverage area. RF Management provides automatic recovery by instructing neighboring APs to increase their transmit power to compensate for the coverage loss. Neighbor recovery is enabled for the default Smart RF policy.

Select the **Channel and Power** tab to modify radio channel and power settings.

Related Topics

Channel and Power Settings on page 182
Scan Settings for Smart RF on page 187
Neighbor Recovery Settings for Smart RF on page 189
Interference Recovery Settings for Smart RF on page 190

Channel and Power Settings

Modify **Channel and Power** settings to fine-tune channel selection within an RF Management policy. **Channel and Power** settings are available on all APs that are supported by ExtremeCloud IQ Controller.

Note
APs retain the last known channel and power settings after a connection loss or reboot.

Table 48: Channel and Power Settings

Field	Description
Channel Width	Represents the desired channel width. The channel width is set for all APs in a device group. Available options include: • 20 MHz • 40 MHz • 80 MHz (supported on 5GHz only 802.11ac and 802.11ax) • 160 MHz ◦ AP5xx – Radio 1 and Radio 2 support 160 MHz ◦ AP4xx / AP4xxC – Radio 2 only (5 GHz band) supports 160 MHz ◦ AP4000/ AP4000-1 – Radio 2 (5 GHz band) and Radio 3 (6 GHz band) support 160 MHz ◦ AP5010 – Radio 1 (5 GHz band) and Radio 3 (6 GHz band) support 160 MHz. ◦ AP5050 – Radio 1 (5 GHz band) and Radio 3 (6 GHz band) support 160 MHz. (Radio 3 is currently turned off for regulatory compliance.) ◦ AP3xx/AP3xxC — *Do not support* 160 MHz width on the 5 GHz radio. A best practice is to use a predetermined width configured as part of the design of the entire RF deployment. To learn about how Smart RF handles channel width settings, see Understanding Smart RF and Channel Width on page 183. **Best Practice:** Operating a 40 MHz channel in a 2.4 GHz band can cause co-channel inference with access points in the vicinity. The 2.4 GHz band has limited available channels. Therefore, for proper channel isolation, a 2.4 GHz band allows 3-4 (region dependent) 20 MHz channels. Best practice is to configure a 40 MHz channel on a 5 GHz radio.
Min TX Power dBm	Determines the minimum power level for the radio. Use the lowest supported value in order to not limit the potential Tx power level range that can be used for the radio. The Min Tx Power setting cannot be set higher than the Max Tx Power setting.

Table 48: Channel and Power Settings (continued)

Field	Description
Max TX Power dBm	Determines the maximum power level that can be used by the radio in dBm. The values are governed by compliance requirements based on the country, radio, and antenna selected, and will vary by AP.
Channel Plan	Select a Channel Plan option. See Configuring a Channel Plan on page 184.

Related Topics

Configuring a Channel Plan on page 184
Understanding Smart RF and Channel Width on page 183
Basic RF Management Settings on page 180
Scan Settings for Smart RF on page 187
Neighbor Recovery Settings for Smart RF on page 189
Interference Recovery Settings for Smart RF on page 190

Understanding Smart RF and Channel Width

ExtremeCloud IQ Controller Smart RF can ensure that the operating channel width does not conflict with radio band compliance limitations. Your channel width selection is considered when determining the optimum channel width, but it is not guaranteed. ExtremeCloud IQ Controller Smart RF uses data from the Neighbor Report to determine the best channel width. If your selected channel width is restricted by radio band compliance, Smart RF selects the next lower channel width. The minimum width is 20 MHz.

Important
If the channel plan does not include a channel width that meets compliance restrictions, the radio channel is disabled.

Smart RF runs the assessment for best channel while considering your desired channel width. The highest channel width (160 MHz) is selected by default for 5 GHz and 6 GHz radios. To allow Smart RF to determine the best possible channel width without you providing a desired width, select 160 MHz and Smart RF will automatically reduce the width as appropriate to configure the optimum width, provided that the AP model supports 160 MHz.

Note
Imported configurations previously set to Auto automatically convert to 160 MHz and are reduced appropriately.

Related Topics

Channel and Power Settings on page 182
Configure AP Details and Radio Settings on page 213
6 GHz Channel Allocation and Notation on page 23

Configuring a Channel Plan

If ACS or Smart RF is enabled you can define a channel plan for the AP. Defining a channel plan enables you to control which channels are available for use during an ACS or Smart RF scan. For example, you may want to avoid using specific channels because of low power, regulatory domain, or radar interference.

- For 2.4 GHz Radio nodes, select one of the following:
  - 3 Channel Plan — ACS scans the following channels: 1, 6, and 11 in North America, and 1, 7, and 13 in the rest of the world.
  - 4 Channel Plan — ACS scans the following channels: 1, 4, 7, and 11 in North America, and 1, 5, 9, and 13 in the rest of the world.
  - Auto — ACS scans the default channel plan channels: 1, 6, and 11 in North America, and 1, 5, 9, and 13 in the rest of the world.
  - Custom — If you want to configure individual channels from which the ACS or Smart RF selects an operating channel, select **Configure**. The **Add Channels** dialog is displayed. Select the individual channels you want to add to the channel plan while pressing the CTRL key, and then select **OK**.
- For 5 GHz Radio nodes, select one of the following:
  - All channels — ACS or Smart RF scans all channels for an operating channel and, when ACS or Smart RF is triggered, the optimal channel is selected from all available channels.

    This plan includes the following channels: 36, 40, 44, 48, 52, 56, 60, 64, 100, 104, 108, 112, 116, 132, 136, 140, 144, 149, 153, 157, 161, 165.
  - All Non-DFS Channels — ACS or Smart RF scans all non-DFS channels for an operating channel. The AP selects the best non-DFS channel.

    This plan includes the following channels: 36, 40, 44, 48, 149, 153, 157, 161, 165.
  - Custom — To configure individual channels from which to select an operating channel, select **Configure**. The **Custom Channel Plan** dialog displays. Select the individual channels you want to include in the channel plan. To select contiguous channels, use the Shift key. To select multiple, non-contiguous channels in the list, use the CTRL key. Select **OK** to save the configuration.
  - Extended Channel with Weather— ACS or Smart RF selects the best channel from the available channels list. Selected channel may be DFS, weather-radar DFS or non-DFS. Weather-radar channels are approved for selected AP models in selected countries. Consult the compliance information for the selected AP.
    - This plan includes the following channels: 36, 40, 44, 48, 52, 56, 60, 64, 100, 104, 108, 112, 116, 120, 124, 128, 132, 136, 140, 144, 149, 153, 157, 161, 165.
    - The weather channel includes 5600-5650MHz sub-bands and requires a listening period before the AP can provide wireless service. During the listening period, the Current Channel field for DFS channels displays the value *DFS Timeout*, and the weather channel fields display *DFS Timeout* . In Europe, the listening period can be up to 10 minutes. In the U.S., this period is 1 minute.
- For 6 GHz Radio nodes, select one of the following:
  - All channels — ACS or Smart RF scans all channels for an operating channel and, when ACS or Smart RF is triggered, the optimal channel is selected from all available channels.

- Custom — To configure individual channels from which to select an operating channel, select **Configure**. The **Custom Channel Plan** dialog displays. Select the individual channels you want to include in the channel plan. To select contiguous channels, use the Shift key. To select multiple, non-contiguous channels in the list, use the CTRL key. Select **OK** to save the configuration.
- **PSC Channels**. Because numerous channels are offered on the 6 GHz band, it is a best practice to configure the Preferred Scanning Channel (PSC) so that the amount of probing is kept to a minimum. Preferred channels function as primary channels at each channel width: 20, 40, 80, and 160 MHz.

  This plan includes the following channels: 1, 5, 9, 13, 17, 21, 25, 29, 33, 37, 41, 45, 49, 53, 57, 61, 65, 69, 73, 77, 81, 85, 89, 93, 97, 101, 105, 109, 113, 117, 121 125, 129, 133, 137, 141, 145, 149, 153, 157, 161, 165, 169, 173, 177, 181, 185, 189, 193, 197, 201, 205, 209, 213, 217, 221, 225, 229, 233.

Note

For a list of channels that are included in the selected channel plan, select on the user interface.

Related Topics

Channel and Power Settings on page 182
6 GHz Channel Allocation and Notation on page 23

Configuring ACS RF Policy

The ExtremeCloud IQ Controller RF Management policy depends on your AP model. AP39xx access points support Automatic Channel Selection (ACS) as the RF Management policy. ExtremeCloud IQ Controller is installed with a default ACS policy.

A Centralized site can support multiple ACS RF policies. Different AP device groups can use different ACS RF policies. You can modify the default policy or create a new policy. Policies that are being used by a device group cannot be deleted, but if the policy is not being used, you can delete it.

To configure ACS:

1. Go to **Configure** > **Sites** and select a Centralized site.
2. Click **Device Groups** tab.
3. Select a device group or click **Add**.

   The **RF Management** value is ACS for AP39xx.
4. Select next to RF Management, to edit the ACS policy.

Note

After modifying the default ACS policy settings, if you need to return to the initial settings, create a new ACS policy. New policies are comprised of the ACS settings that are delivered with the initial installation. Click to create a new policy.

Note
Interference Recovery and Neighbor Recovery should be enabled to allow ACS RF Policy to adjust/change channels automatically. You can use Interference Recovery only, or Neighbor Recovery only.

Related Topics

Basic RF Management Settings on page 180
Channel and Power Settings on page 182
Configuring a Channel Plan on page 184
Interference Recovery Settings for ACS on page 186

Interference Recovery Settings for ACS

The following settings define thresholds for the ACS policy Interference Recovery plan supported on AP39xx in a Centralized site. The default ACS policy enables Interference Recovery.

Select **Interference Recovery** and configure the following parameters.

Table 49: ACS Interference Recovery Settings

Field	Description
Channel Occupancy Threshold %	Defines the channel utilization level, measured as a percentage. If the threshold is exceeded, ACS scans for a new operating channel for the AP.
Noise Threshold (dBm)	Defines the noise interference limit, measured in dBm. If the noise interface exceeds this threshold, ACS scans for a new operating channel for the AP.
Update Period (Minutes)	Defines a period of time, in minutes, where the average values for DCS Noise and Channel Occupancy are measured. If the average value for either setting exceeds the defined threshold for that setting, then the AP triggers Automatic Channel Scan (ACS).
Wait Time (Seconds)	Length of the delay (in seconds) before logging an alarm. Default setting is 10 seconds.
Detect Bluetooth	Enable this setting to detect Bluetooth interference on the operating channel.
Detect Constant Wave	Enable this setting to detect Constant Wave interference on the operating channel.
Detect Cordless Phones	Enable this setting to detect cordless phone interference on the operating channel.
Detect Microwaves	Enable this setting to detect microwave interference on the operating channel.
Detect Video Bridges	Enable this setting to detect video bridge interference on the operating channel.

Configuring Smart RF Policy

The ExtremeCloud IQ Controller RF Management policy depends on your AP model. AP4xx and AP5xx support Smart RF as the RF Management policy. ExtremeCloud IQ Controller is installed with a default Smart RF policy.

You can modify the default policy or create a new policy. Policies that are being used by a device group cannot be deleted, but if the policy is not being used, you can delete it.

Note
Wi-Fi 6 AP models support Smart RF. Only one Smart RF Policy can be used per site.

To configure Smart RF:

1. Go to **Configure** > **Sites**.
2. Select a site, then select **Device Groups** tab.
3. Select a device group or select **Add**.

   The **RF Management** value is Smart RF for Wi-Fi 6 AP models.
4. Select next to RF Management, to edit the Smart RF policy.

ExtremeCloud IQ Controller is installed with a default Smart RF policy. You can modify the default policy or create a new policy, but you cannot delete a Smart RF policy.

Note
After modifying the default RF policy settings, if you need to return to the ExtremeCloud IQ Controller initial settings, create a new Smart RF policy. New policies are comprised of the Smart RF settings that are delivered with the initial ExtremeCloud IQ Controller installation. Select to create a new policy.

Related Topics

Basic RF Management Settings on page 180
Channel and Power Settings on page 182
Scan Settings for Smart RF on page 187
Neighbor Recovery Settings for Smart RF on page 189
Interference Recovery Settings for Smart RF on page 190

Scan Settings for Smart RF

A Smart RF policy can reduce deployment costs by scanning the RF environment to determine the best channel and transmit power configuration for each radio. Scan settings define the quality and duration of the RF scan. Scanning and recovery parameters have a defined sensitivity: Low, Medium, or High. AP models AP4xx and AP5xx support custom sensitivity settings.

To set custom sensitivity:

1. Go to **Configure** > **Sites**.
2. Select a site. Then select **Device Groups**.
3. Next to RF Management, select .

4. Go to **Basic Settings** > **Sensitivity** and select **Custom**.
5. From the **Scanning** tab configure the following parameters:

Table 50: AP Scan Settings

Field	Description
OCS Monitoring Awareness Override	Overrides OCS scanning. Smart RF relies on Off-Channel Scanning (OCS) to monitor the RF environment in real-time, allowing managed radios to adapt to changes in the RF environment. OCS can negatively impact some devices. When enabled, OCS checks for sensitive clients (for example, Voice and Power Save clients). If sensitive clients are found, OCS is skipped, and the **Number of Threshold Awareness Hits** counter is incremented.
Number of Threshold Awareness Hits	Enabled after you enable **OCS Monitoring Awareness Override**. When OCS is skipped, the OCS Awareness Hits counter is incremented. When it reaches the **Number of Threshold Awareness Hits**, OCS starts, even if sensitive clients may be negatively affected. This is because information about other channels is vital. This setting indicates when channel jumping for OCS will begin regardless of the **OCS Monitoring Awareness Override** setting. If you increase this value, channel jumping will wait, resulting in better service to sensitive clients but presenting limited information about other channels. The default value is 10.
Scan Duration [Milliseconds]	The length of time the scan occurs in milliseconds. Valid values are 20-150.
Scan Period [Seconds]	The scan frequency interval in seconds. Valid values are 1-120. The default value is 6 seconds.
Extended Scan Frequency	The frequency that radios scan on channels other than their peer radios. Valid values are 0 — 50. The default setting is 5 for all radio bands.
Scan Sample Count	The number of samples that each Smart RF managed radio takes before reporting to ExtremeCloud IQ Controller. The default is 5 samples from a 5GHz radio and 10 samples from the 2.4 GHz and 6 GHz radios when Medium sensitivity is selected.
Client Aware Scanning	A client awareness count (number of clients 1 — 255) for Off Channel Scans for the selected radio band. Channel scanning is avoided when the number of clients associated with the AP radio is greater than or equal to the value configured here.

Table 50: AP Scan Settings (continued)

Field	Description
Power Save Aware Scanning	Defines scanning for power save clients. Valid values are: • Dynamic. Disables smart monitoring when buffered data exists at the radio for a power save client. The default setting is Dynamic for all radio bands. • Strict. Disables smart monitoring when a power save capable client is associated to a radio. • Disable. Do not use the Power Save Aware Scan option.
Voice Aware Scanning	Defines how voice aware recognition is configured for Smart RF. Valid values are: • Dynamic. Disables smart monitoring when buffered data exists at the radio for a voice client. The default setting is Dynamic for all radio bands. • Strict. Disables smart monitoring when a voice client is associated to a radio. • Disable. Do not use the Voice Aware Scanning option.
Transmit Load Aware Scanning [%]	Defines the threshold for channel load. Channel scanning is avoided when channel load is greater than or equal to this value.

Related Topics

Basic RF Management Settings on page 180
Channel and Power Settings on page 182
Neighbor Recovery Settings for Smart RF on page 189
Interference Recovery Settings for Smart RF on page 190

Neighbor Recovery Settings for Smart RF

Neighbor recovery involves automatic recovery for failed or faulty access points or faulty antennas by instructing neighboring APs to increase their transmit power to compensate for the coverage loss. The default Smart RF policy enables Neighbor Recovery for AP4xx and AP5xx. It requires a minimum of four APs to function.

Note
Before you can edit these parameters, select **Custom** Sensitivity from the **Basic** Smart RF configuration tab.

Select **Recovery** > **Neighbor Recovery** and configure the following parameters.

Table 51: Neighbor Recovery Settings

Field	Description
Power Hold Time (seconds)	The number of seconds Smart RF waits before changing radio channels in response to channel noise. This hold timer definition avoids channel flapping. Range is 0 to 3600 seconds.
Neighbor Recovery	
2.4 GHz Neighbor Power Threshold (dBm)	Defines the maximum power the 2.4 GHz radio will emit to compensate for a failed neighbor radio. Valid values are -85 to -55 dBm. Default value is -65 dBm.
5 GHz Neighbor Power Threshold (dBm)	Defines the maximum power the 5GHz radio will emit to compensate for a failed neighbor radio. Valid values are -85 to -55 dBm. Default value is -65 dBm.
6 GHz Neighbor Power Threshold (dBm)	Defines the maximum power the 6 GHz radio will emit to compensate for a failed neighbor radio. Valid values are -85 to -55 dBm. Default value is -65 dBm.
Dynamic Sample Recovery	
Dynamic Sample Enabled	Enables an administrator to define how Smart RF adjustments are triggered by locking retry and threshold values.
Dynamic Sample Retries (1-10)	Define the number of Dynamic Sample Retries.
Dynamic Sample Threshold (1-30)	Define the Dynamic Sample Threshold.

Related Topics

Basic RF Management Settings on page 180
Channel and Power Settings on page 182
Scan Settings for Smart RF on page 187
Interference Recovery Settings for Smart RF on page 190

Interference Recovery Settings for Smart RF

The following settings define thresholds for the Smart RF policy Interference Recovery plan supported on AP4xx and AP5xx. The default Smart RF policy enables Interference Recovery.

Note
Before you can edit these parameters, select **Custom** Sensitivity from the **Basic** Smart RF configuration tab.

Select **Recovery** > **Interference Recovery** and configure the following parameters.

Table 52: Smart RF Interference Recovery Settings

Field	Description
Noise	When enabled, Smart RF policy scans for excess noise from wireless devices. When noise is detected, Smart RF-supported devices can move to a cleaner channel. Decision to move is based on Noise Factor setting. This feature is enabled in the default Smart RF policy.
Noise Factor	Define the level of network interference the Smart RF policy considers when calculating interference recovery. The default setting is 1.50. The range is 1.0 to 3.0.
Channel Hold Time	Defines the minimum time between channel changes during neighbor recovery. Set the time in seconds (1- 86,400). This setting prevents rapid channel changes.
Client Threshold	Defines the number of clients that must be associated with a radio channel to initiate an interference recovery override. When the client threshold is met, the associated channel remains fixed regardless of the interference level on the channel. Valid values are 1 - 255. This value depends on the RF Sensitivity setting on the **Basic** tab.
2.4 GHz Channel Switch Delta (dBm)	Defines the threshold for initiating a channel switch on the 2.4 GHz radio. Smart RF compares the difference between interference levels on the current channel and a prospective channel. If the difference is below the configured threshold, the channel does not change. Valid values are 5 - 35 dBm. This value depends on the RF Sensitivity setting on the **Basic** tab.
5 GHz Channel Switch Delta (dBm)	Defines the threshold for initiating a channel switch on the 5GHz radio. Smart RF compares the difference between interference levels on the current channel and a prospective channel. If the difference is below the configured threshold, the channel does not change. Valid values are 5 - 35 dBm. This value depends on the RF Sensitivity setting on the **Basic** tab.
6 GHz Channel Switch Delta (dBm)	Defines the threshold for initiating a channel switch on the 6GHz radio. Smart RF compares the difference between interference levels on the current channel and a prospective channel. If the difference is below the configured threshold, the channel does not change. Valid values are 5 — 35 dBm. This value depends on the RF Sensitivity setting on the **Basic** tab.

Related Topics

Basic RF Management Settings on page 180

Channel and Power Settings on page 182
Scan Settings for Smart RF on page 187
Neighbor Recovery Settings for Smart RF on page 189

Select Shutdown Settings

Select Shutdown is intended for high-density deployment designs focused on 5GHz coverage. It identifies and hides redundant 2.4GHz radios, thus reducing the overall CCI (Co-Channel Interference). Hidden radios are still on and will send Neighbor Reports. Select Shutdown is disabled by default.

From **Select Shutdown** configure parameters that will maintain CCI levels within specified limits. Configure the following parameters:

Table 53: Select Shutdown Settings

Field	Description
Enable	Select to enable auto-shutdown of radios causing interference within the Smart RF monitored network. Auto-shutdown of select 2.4 GHz radios, in dual-band networks, maintains CCI levels within specified limits. When enabled, Smart-RF monitors CCI levels to ensure that the deployment average CCI remains within specified minimum and maximum limits. If the deployment average CCI is found to exceed the maximum threshold, 2.4 GHz radios, causing neighbor interference, are shut down one-by-one until the deployment average CCI falls below the specified maximum threshold. The reverse process occurs when the deployment average CCI falls below the minimum threshold. In this scenario, previously disabled radios are enabled until the deployment average CCI reaches acceptable levels.
CCI High Threshold	Determines the maximum CCI threshold from -85 to -55 dBm. The default value is -80 dBm. This value indicates the upper limit for the deployment average CCI range.
CCI Low Threshold	Determines the minimum CCI threshold from -85 to -55 dBm. The default value is -100 dBm. This value indicates the lower limit for the deployment average CCI range.
Frequency	Determines the Shutdown interval in minutes. When the deployment average CCI exceeds the specified maximum threshold, Smart RF shuts down 2.4 GHz radios until the CCI reaches acceptable levels. Use this option, to configure the interval between successive radio shutdowns. Valid values are 0 - 3600 minutes. The default is 60.
Frequency Limiter	Indicates the value by which to multiply the OCS scan period to determine the minimum Frequency setting.

Related Topics

Scan Settings for Smart RF on page 187

Configuring a Floor Plan

Use the floor plan tool to visualize a wireless deployment, plan device placement for APs and switches, and troubleshoot network performance issues. The floor plan illustrates the location of the devices and how the devices affect network performance. You can visualize device performance based on signal strength and channel assignment, and verify network readiness within a floor plan.

A site can have multiple floor plans, usually a plan for each floor of a building. The devices represented in the map must come from the same site.

Note
Floor plan limits depend on the appliance. See Table 9 on page 37.

Badges provide real-time statistics for APs. (APs can also be excluded from a simulation.)

To use the floor plan feature for the first time, follow this process:

1. Select the plus sign to add a new floor plan.
2. Upload a background image.
3. Set the environment and scale.
4. Draw the boundary walls.
5. Draw the inner walls.
6. Place the devices.
7. Assign badges, and view the heat maps and device coverage.

Related Topics

Floor Plan Limits on page 37
Add a New Floor Plan on page 195
Setting a Background Image on page 197
Setting Floor Plan Scale on page 197
Drawing Boundary Walls on page 198
Drawing Inner Walls on page 199
Placing Devices on page 199
Assigning Badges on page 60
Floor Plans on page 35
Floor Plan View on page 56

Displaying an Existing Floor Plan

To display an existing floor plan in configuration mode:

1. Go to **Configure** > **Sites**. Add a new site or select a site and select **Floor Plans** tab.

   Note
   You can view existing floor plans without accessing Configure Site. Simply, select a site and click the **Floor Plans** tab.

2. Click the first field to display a list of available device groups within the site.

3. Select one or more device groups.
4. Select a floor from the list of floors to the right of the map panel.

   See Use Case: Device Group Filtering on page 194 for a use case scenario.

   The floor plan displays.
5. Use the **Draw Tools** to modify the floor plan.

Related Topics

Use Case: Device Group Filtering on page 194
Setting Floor Plan Scale on page 197
Drawing Boundary Walls on page 198
Drawing Inner Walls on page 199
Placing Devices on page 199
Assigning Badges on page 60
Floor Plans on page 35
Floor Plan View on page 56

Use Case: Device Group Filtering

View your devices on a floor plan to gain information about network readiness. Floor plans are associated with the site. Each site can have one or more floor plans — typically, one plan per floor. Devices that are displayed on the floor plan belong to a selected device group. All devices in a device group must share the same platform (as well as profile configuration and RF Management).

The example site has four device groups and three floor plans:

- The site has two floors and an outdoor courtyard.
- Each floor and courtyard has a separate floor plan:
  - First floor map
  - Second floor map
  - Outdoor courtyard map
- The site includes a device group for each AP platform:
  - DG-3915
  - DG-3935
  - DG-3917
  - DG-3965
- Floors 1 and 2 have a combination of AP models AP3935 and AP3915.
- The courtyard has AP Models AP3965 and AP3917.

To show all APs on the first floor, select device groups DG-AP3935 and DG-AP3915. Then, select the First floor map.

To show all APs on the second floor, select device groups DG-AP3935 and DG-AP3915. Then, select the Second floor map.

To show all APs in the outdoor courtyard, select device groups AP3965 and AP3917. Then, select Outdoor courtyard map.

When working in the **Floor Plan View** you can toggle floor plan maps from the map panel.

Displaying Floors with Non-Assigned APs and Empty Floors

Before you can display a floor plan, you must select one or more device groups that include the devices that are associated with the floor plan. If you have imported or created a floor plan that is not yet associated with devices or if you are using a floor plan for an empty floor, you can still display the floor plan:

- To display a floor plan with place-holder icons, select the device group **Non-Assigned APs**.
- To display a floor plan for an empty floor, select the device group **Empty Floor**.

Use Case: Importing A Floor Plan with Unknown APs

You have the option to create a floor plan map with a third-party tool and import the map to ExtremeCloud IQ Controller. Upon import, the AP place holder icon displays ( ).

You may want to create a floor plan before you have the APs installed. Or you may be reusing a floor plan that incorporated different APs from those that you are using now. In either case, the APs are unknown to ExtremeCloud IQ Controller.

To import an existing floor plan and update the associated APs:

1. From the floor plan **Configure** page, select **Import** and select the floor plan file to import.

   The map is displayed with unknown AP icons .
2. From the map, right-click each icon and select the serial number for the AP that will be installed in that location.

   Note
   The list of available APs is populated from the selected device groups.

3. To edit the AP placement, select the AP selector next to the **Place APs** field, then select the AP icon and drag it to a new location.

Related Topics

Add a New Floor Plan on page 195
Placing Devices on page 199

Add a New Floor Plan

A floor plan map begins with a new floor. You can draw a new floor or import a complete floor plan. Additionally, you can export floors or delete floors. Add floor plans when adding a new site or add a floor plan to an existing site

Note
Floor plan limits depend on the appliance. See Table 9 on page 37.

.

To add a new floor plan:

1. Go to **Configure** > **Sites**. Add a new site or select a site and select **Floor Plans** tab.
2. In the **Manage Floor Plans** pane, select + to add a new floor plan.
3. Enter a unique name for the new floor plan and the height of the floor ceiling. Then, select **OK**.
4. Draw a floor plan or import an existing plan.
   a. To import an existing plan, click **Import**.
   b. Navigate to the floor plan file and click **Open**.
5. Before you can save a floor plan, at a minimum, draw a boundary or set a background image.

The floor plan displays.

Next, go to Setting a Background Image on page 197.

Related Topics

Floor Plan Settings on page 196
Importing or Exporting a Floor Plan on page 196

Floor Plan Settings

1. Configure the following parameters for a floor plan.

Table 54: New Floor Plan Settings

Field	Description
Floor Name	Unique name for the floor plan.
Floor Height	Floor height in meters.

2. Select **OK**.

Related Topics

Add a New Floor Plan on page 195
Importing or Exporting a Floor Plan on page 196

Importing or Exporting a Floor Plan

ExtremeCloud IQ Controller supports the following floor plan file formats:

- Zip
- ExtremeCloud IQ Controller
- Ekahau

To import or export a floor plan file, take the following steps:

1. Go to **Configure** > **Sites**. Add a new site or select a site and select **Floor Plans** tab.
2. From the **Manage Floor Plans** pane, do the following:

To import a file:

1. Select **Import**.
2. Select the file format and navigate to the floor plan file.

3. Select **Open**. Then, click **Save**.

To export a file:

1. Select **Export**.
2. Select the floor plan file.

   The floor plan file is downloaded to your local machine.

Setting a Background Image

When creating a new floor plan, the first step is to set the background image.

To set the background image:

1. Go to **Configure** > **Sites**. Add a new site or select a site and select **Floor Plans** tab.
2. Select **Draw Tools** to display floor plan tools.
3. Under **Floor Image**, click to upload an image.
4. Navigate to the background image file.

   ExtremeCloud IQ Controller supports the following:

   - File formats: .jpg, .png. svg.

     Note
     .svg is not supported with Internet Explorer version 11.

   - Image resolution up to 2592x1456 pixels.
5. Click **Open**.

   The background image is displayed.
6. Click **Save** to save the floor plan.

   To remove the image: display the image on the map and click the **Floor Image** delete icon . Then, click **OK**.

Next, go to Setting Floor Plan Scale on page 197

Setting Floor Plan Scale

Scale the floor plan based on actual floor plan measurements. You can scale a floor plan using a doorway measurement, or by representing any known distance in the room.

Note
The following procedure corresponds to the callout numbers in Figure 45 on page 198

To scale a floor plan:

1. Display the floor plan.

   Go to **Configure** > **Sites**. Add a new site or select a site and select **Floor Plans** tab.
2. Select a floor plan to edit from the drop-down list.

3. Under **Scale / Measures**:
   - Click ⟷ to enter a known length in the Length field that displays.
     a. Draw the physical line on the map.
     b. In the field, enter a numeric value that represents the physical distance and that corresponds to the line drawing. The pixel value for the line drawing displays.
     c. Select the units of measure and click **Apply**.

     In the following figure, the floor plan scale is set (65px = 20 Meters).

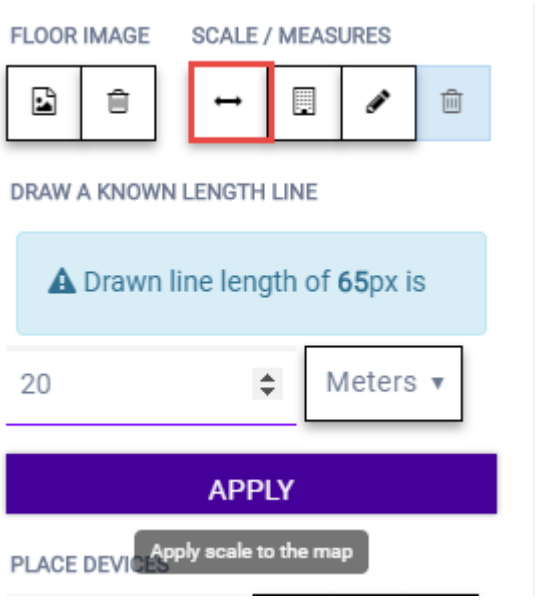


Figure 45: Setting Floor Plan Scale

   - Click to draw a doorway.
     a. Draw a line to represent a doorway.
     b. Click **Apply**.
   - Click ✎ to draw the floor length. Draw a line on the map that represents an actual physical distance. On the map, double-click the beginning and ending points of the line. The length of the wall (based on the set scale) is displayed on the map.

Drawing Boundary Walls

Draw the outside boundary of the building. The area within the boundary is used to determine device location and coverage. The area outside the boundary is ignored.

To draw boundary lines:

1. Go to **Configure** > **Sites**. Add a new site or select a site and select **Floor Plans** tab.
2. Select **Draw Tools** to display floor plan tools.
3. To anchor the beginning of the boundary line, click a corner of the outside boundary.

4. Click each corner to anchor the line. The drawing line zigzags across the image as you anchor each corner.

   Note
   If you make a mistake, you can click to edit the boundary or click to delete the boundary and start over.

5. When you finish the boundary, double-click the last corner to disable the pen tool.

Next, go to Drawing Inner Walls on page 199.

Drawing Inner Walls

Wall materials affect the propagation of the signal and estimation models. An accurate representation of the walls is essential to the accuracy of the model.

We recommend that you draw inner walls for a custom environment and choose material types, such as concrete around stairwells. It is important that you draw inner walls that are made of concrete or brick because these materials have a strong effect on the propagation. If installation requires that an AP be placed within a walled area, then define both walls on either side of the AP.

Note
If you do not want to create a custom environment and draw the inner walls, you can select basic inner wall types from the **Environment** drop-down list instead, such as office drywalls or cubicle walls. Office drywall has minimal impact on the RF signal propagation.

To draw inner walls for a custom environment:

1. Go to **Configure** > **Sites**. Add a new site or select a site and select **Floor Plans** tab.
2. Select **Draw Tools** to display floor plan tools.
3. Select **Custom** from the **Environment** drop-down.
4. Under **Draw Walls** field, select a wall type.

   The pen icon is enabled.
5. To anchor the line drawing, select a corner of the inner wall.
6. Select each corner of the inner wall to anchor the line, and progress to the next corner.
7. When you reach the end of your inner wall boundary, double-click the last corner to anchor the final line and disable the pen tool.

   Note
   Right-click on a wall to change its type or to delete it. You can also select to modify a wall or click to delete it.

Next, go to Placing Devices on page 199.

Placing Devices

As long as an AP is a member of a device group within the site, it can be placed on any map that is associated with that site. From the floor plan **Configuration**, you must first

select the device groups to work with, then select a floor plan that includes APs from the selected device groups.

Switches associated with the site can be placed on a floor plan.

To place a device on a floor plan:

1. Go to **Configure** > **Sites**. Add a new site or select a site and select **Floor Plans** tab.
2. Select **Draw Tools** to display floor plan tools.
3. Select the **Place Devices** field, and select an AP or switch from the drop-down list. The **Place Devices** field is populated with APs that are part of a selected device group and switches that are part of the site.

   This field supports auto-complete. You can type one or more characters in the *Select a device* to find devices.
4. Select the device from the list.

   The cursor changes to a device icon .
5. Select on the floor plan to place the device.
6. If you need to move the device on the floor plan, first select the selector tool, then select the device icon and move it on the map.
7. To save the floor map, select **Save**.
8. Select BACK to display the floor plan **View** page.

Next, go to Assigning Badges on page 60.

Configuring AP Orientation

APs can be mounted on a wall or ceiling. When mounted on a wall, the AP direction can be adjusted. Configure the AP orientation from the floor plan **Configuration** page, then view the orientation displayed on the floor plan **View** page.

To set AP orientation:

1. From the floor plan **Configuration** page, right-click the AP icon on the map and select .
2. Select the **Ceiling** or **Wall** picture to set orientation.

   If you select **Wall**, set the AP height in meters. Height is the distance from the AP to the floor.

   From the floor plan **View**, a black arrow displays on the map, indicating the AP orientation. Select the black arrow and drag to a new orientation.

Configuring Camera AP Angle

Set the camera angle for an AP3916ic directly from the floor plan map:

1. Go to **Configure** > **Sites**. Add a new site or select a site and select **Floor Plans** tab.
2. Select **Draw Tools** to display floor plan tools.
3. Place the AP3916ic on the floor plan map.
4. Right-click the camera icon and select to adjust the camera viewing angle.

   A large purple arrow displays.

5. Drag the large purple arrow around until it is pointing in the direction that you need.

Related Topics

User Interface Controls on page 59

Configuring Floor Plan Zones

Configure zones on a floor plan to support Location Engine generation of area change events.

Define up to 16 specific zones per floor to determine whether a client position is inside or outside of each zone. Additionally, you can create areas located inside of other areas. A client can only be located in one area at a time.

Note
You must have a floor plan displayed to enable the Draw Zones feature.

To draw a zone on the floor plan map:

1. Go to **Configure** > **Sites**. Add a new site or select a site and select **Floor Plans** tab.
2. Select **Draw Tools** to display floor plan tools.
3. Under **Draw Zones**, select , then click the map and draw the first line.
4. Click again to draw a second line and so forth.
5. When you are finished drawing the zone, double-click to release your cursor.
6. Right-click the zone to configure Zone Name and Zone ID.
7. To edit an existing zone, select and click one of the lines of the zone.
8. Drag your cursor to change the zone area.
9. Double-click to release your cursor.
10. Click **Save** to save the floor plan.

Related Topics

User Interface Controls on page 59

Deleting APs from the Map

To delete an AP from a floor map:

1. Go to **Configure** > **Sites**. Add a new site or select a site and select **Floor Plans** tab.
2. Right-click on an AP icon on the map.
3. Select **Delete**.

   The selected AP is removed from the map.

4. To delete all APs from the map at once, next to the **Place APs** field, select .

Site Allow List/Deny List

Enforce Site-Level Control Over RF Association

Configure Client Access Lists for clients at the site level. For more information, see Site Client Access Lists on page 118.

Enforce IP Address Protection

Protect critical network resources from MU clients by creating a list of Address Resolution Protocol (ARP) IPv4 addresses for network routers, gateway servers, and other critical servers. ExtremeCloud IQ Controller assigns the Quarantine Role to clients that use a reserved IPv4 address from this configured list and logs an entry indicating that the restricted IP address was hit.

The Critical IP Address List is configured per site. The list applies to all clients in the site. When a client uses a protected IP address, the following takes place:

- All Address Resolution Protocol (ARP) traffic from that client is blocked.
- The client is assigned to the Quarantine Role, and it remains on Quarantine until the client is disassociated from the network.
- The following event log is generated:

```
Usage of reserved IP address detected. Client [], IP address [].
Client will be assigned role Quarantine.
```

To view event logs, go to **Tools** > **Logs** > **Events**.

Note
Enforce IP Address Protection configuration changes only apply to new client registrations. Adding and removing IP addresses from the Critical IP Address List does not affect the state of the connected clients. In order to enforce or remove enforcement of a pre-existing client session, the session needs to be removed from the system – disassociate the client. Client re-association is processed according to the latest state of the Critical IP Address List.

Related Topics

Configure IP Address Protection List on page 202
Site Client Access Lists on page 118

Configure IP Address Protection List

Configure a list of protected IPv4 addresses to protect critical gateway IP addresses. The maximum number of addresses in a list is 32.

1. Go to **Configure** > **Sites**, and select a site.
2. Select the **Allow List/ Deny List** tab.
3. Select **Enforce IP Address Protection**.
4. Select **Add** and enter a valid IPv4 address.

5. From the top of the **Sites** page, select **Save**.

   To save the list, each row in the list must include a valid IP address, with no empty rows.

   Note
   The Critical IP Address List is emptied when you uncheck the **Enforce IP Address Protection** option and save your changes. When you enable this option again, you will have to create a new list.

   Select ☰ to export the list data to .csv.

Remove an IP Address

To remove an IP address from the list:

1. Select the check box next to the IP address and select **Delete**.
2. From the top of the **Sites** page, select **Save**.

Advanced Tab

On the **Advanced** tab, you can configure the following advanced settings for a site:

- **SNMP**. Simple Network Management Protocol configuration for switches associated with a specific site. For more information, see SNMP Configuration on page 451.
- **Adoption Preference**. Control the distribution of APs in a particular site between appliances in a High Availability Pair.

Related Topics

SNMP Configuration on page 451
Adoption Preference on page 203
Availability Pair Settings on page 449
Advanced Setting Overrides on page 221
AP Actions on page 206

Adoption Preference

ExtremeCloud IQ Controller supports the ability to specify an appliance adoption preference and to support a High-Availability pair of appliances located in separate data centers. APs assigned to a site will discover the appliance specified in the **Adoption Preference**. The load assignment for the preferred appliance persists. However, you can re-map the AP-to-site preference at any time, to adjust for experience, business needs, or network conditions.

For **Adoption Preference**, select the preferred connection point for APs that are assigned to this site. Possible values are:

Use Global Settings

The global settings are dependent on the Availability setting **Auto AP Balancing** (which is located under **Administration** > **System** > **Availability**).

- When **Auto AP Balancing** is Active - Active, which spreads the load across the availability pair, the **Use Global Settings** field displays **Load Balance**.

- When the **Auto AP Balancing** is Active - Passive, which uses the secondary appliance for failover only, the **Use Global Settings** field displays **Primary Appliance**.

For more information about the load balancing configuration for an availability pair, see Availability Pair Settings on page 449.

Primary Appliance

APs for this site will be homed on the primary appliance.

Backup Appliance

APs for this site will be homed on the secondary appliance. The secondary appliance is used for load balancing or failover support.

Adoption Preference is also an override configuration setting for one or more APs:

- To configure the **Adoption Preference** for a single AP, refer to Advanced Setting Overrides on page 221.
- To configure the **Adoption Preference** for multiple APs, refer to AP Actions on page 206.

Note
The **Tunnel** column on the Access Point List displays which controller the AP has an active tunnel to. Possible values are:

- Primary — The AP has an active tunnel to the primary controller in an availability pair.
- Backup — The AP has an active tunnel to the secondary controller in an availability pair.
- N/A — Indicates that an active tunnel does not exist or that there is a configuration entry for the AP, but the AP is not currently connected.

Devices

Manage access points (APs) and switches from **Configure** > **Devices**. See the ExtremeCloud IQ Controller Release Notes for a list of supported APs and switches.

Note
ExtremeCloud IQ Controller supports Extreme Defender Adapter SA201 for the Defender for IoT solution. For more information on Extreme Defender for IoT, refer to documentation located in the Extreme Networks documentation portal.

Related Topics

Understanding Access Point States on page 72
Adoption Rules on page 318
Add APs on page 212
Add or Edit a Configuration Profile on page 134
Advanced AP Radio Settings on page 153
Network Snapshot: AP Details on page 84

Opening Live SSH Console to a Selected AP on page 98
Packet Capture on page 93
Switches on page 239

Access Points

Go to **Configure** > **Devices** > **Access Points** to add and configure APs in ExtremeCloud IQ Controller.

The model and licensing domain of the AP determines the site configuration type and site licensing domain. The configuration Profile and RF Management for a device group are specific to the AP platform.

Use **Auto Refresh** to automatically refresh the information presented. From the **Auto Refresh** drop-down field, select the refresh value. Valid values are:

- OFF
- 30 Seconds
- 1 Minute
- 3 Minutes
- 5 Minutes

You can also select to manually refresh the page anytime.

Note
Save your page setting changes. **Auto Refresh** is implemented at the browser level and therefore will reset any selections or unsaved page setting changes. When using **Auto Refresh**, select a refresh interval that allows you to complete the operation within the defined interval. For best results, set **Auto Refresh** to OFF during configuration selections or selection of a large number of elements.

For more information about supported access points, see Access Points List on page 69.

Related Topics

Understanding Access Point States on page 72
Access Points List on page 69
Query Builder on page 73
AP Actions on page 206
Add APs on page 212
Add a Site on page 130
Device Groups on page 32
Configuring Column Display on page 43

AP Actions

You can take action on multiple access points at one time from the **Access Points** list.

Note
Save your page setting changes. **Auto Refresh** is implemented at the browser level and therefore will reset any selections or unsaved page setting changes. When using **Auto Refresh**, select a refresh interval that allows you to complete the operation within the defined interval. For best results, set **Auto Refresh** to OFF during configuration selections or selection of a large number of elements.

1. Go to **Configure** > **Devices** > **Access Points** and select one or more APs.
2. Take the following actions from the AP **Actions** button.

Table 55: AP Actions

Field	Description
Manage Certificates	Manage certificates for selected APs. Possible values are: • **Generate CSR** — Enter the attributes for a Certificate Signing Request that is downloaded after the form is complete. See Generate CSR on page 210. Then, send the .csr file to the certificate authority to be signed and returned as a .cer file. • **Apply Signed Certificate** — Apply a signed certificate to the selected APs. See Apply Signed Certificate on page 211. • **Reset to Default** — Remove applied certificates from the selected APs.
Assign to Site	Assign selected APs to a specific site. The **Assign to Site** dialog displays with available sites and device groups. Select a site and device group; then select **OK**. Selected APs must share the same model type. Based on the AP model type, device groups and sites are displayed in the "assign to" lists. Use this feature to easily move APs to different supported sites. **Note:** When working with 802.11ax access points that offer dual-mode support, make sure that the correct discovery options are configured for device adoption into the destination site. For more information, see the *ExtremeCloud IQ Controller Deployment Guide*. To add a new site or device group, select ⊙ and configure the parameters. For more information, see Assign Devices to Site on page 248.

Table 55: AP Actions (continued)

Field	Description
Adoption Preference	Select the preferred controller for adoption of the selected APs. The **Adoption Preference** dialog displays the following controller options: • Use global availability settings. This option refers to the Auto AP Balancing configuration described in Availability Pair Settings on page 449. To configure Auto AP Balancing, go to **Administration** > **System** > **Availability**. • Primary Appliance • Backup Appliance
AP Event Level	Override the log level for selected APs. Valid log level values are: Critical, Major, Minor, and Info. For more information, see Multiple APs Event Level Override on page 209.
Image Upgrade	Select from the list of AP version images and apply to selected APs. If more than one AP is selected, the upgrade image must be common between the selected APs. If not, a message displays indicating that there is no common image. Download appropriate image or select different APs. For information on downloading an upgrade image, see Software Upgrade on page 434. **Minimize service impact**. Check this box to upgrade APs without impacting AP service to clients. When this option is enabled, APs upgrade in batches allowing clients to roam to other APs during an AP upgrade. **Note: Minimize service impact** is enabled by default. The order for AP upgrade is as follows: 1. APs without clients. 2. APs with < 1kB per second traffic via the APs wired port. 3. APs grouped by channel. APs serving the same channel are upgraded together. 4. APs serving DFS and Weather channels. There is a delay of 180 seconds between upgrading each set of APs. APs serving DFS and Weather channels are upgraded within a 9-minute interval.
Delete	Delete the selected APs.

Table 55: AP Actions (continued)

Field	Description
Release To Cloud	Restarts selected Universal APs in the Cloud operating mode to be managed in ExtremeCloud IQ. The following APs support this feature: • AP3000/X • AP302W • AP305C/CX • AP305C-1 • AP4000 • AP4000-1 • AP410C • AP410C-1 • AP460C/S6C/S12C • AP5010 • AP5050U/AP5050D For more information, see Universal AP Operational Modes on page 24.
Reboot	Restart the selected APs.

Related Topics

Generate CSR on page 210
Apply Signed Certificate on page 211
AP Certificates on page 209
Multiple APs Event Level Override on page 209
Access Points List on page 69
Radio Settings Button on page 55
Assign Devices to Site on page 248
Adoption Preference Override on page 208
Universal AP Operational Modes on page 24

Adoption Preference Override

Select the preferred controller for adoption of the selected APs.

1. Go to **Configure** > **Devices** > **Access Points**.
2. Select one or more devices from the **Access Points List**.
3. Select **Actions** > **Adoption Preference**.
4. Select **Enable** to enable the Select Adoption field.
5. Select one of the controller options for preferred adoption.
   - Use global availability settings. This option refers to the Auto AP Balancing configuration described in Availability Pair Settings on page 449. To configure Auto AP Balancing, go to **Administration** > **System** > **Availability**.
   - Primary Appliance
   - Backup Appliance

Related Topics

AP Actions on page 206
Advanced Setting Overrides on page 221

Multiple APs Event Level Override

Event Level is configured in the configuration Profile for the device group. Additionally, configure the Event Level override for individual APs from the Advanced Settings Overrides tab, or override the Event Level for multiple APs from the **Device List** Actions menu. Overriding the Event Log Level for one or more specific APs can be helpful when troubleshooting.

To override the Event Level on multiple APs:

1. Go to **Configure** > **Devices** > **Access Points**.
2. Select one or more devices from the **Access Points List**.
3. Select **Actions** > **AP Event Level**.
4. Select **Enable** to enable the Select AP Event Level field.
5. Select the event level.
   - Critical
   - Major
   - Minor
   - Info
6. Select **OK**.

   All APs that were selected from the Device List are updated with the selected event level.

Related Topics

AP Actions on page 206
Advanced Setting Overrides on page 221
Advanced Configuration Profile Settings on page 172

AP Certificates

Access points can be authenticated to the network using a self-signed certificate. The uploaded certificates are used for 802.1x authentication with the infrastructure.

Note
Tunneling between an AP and a controller is also certificate based, but tunneling supports the ExtremeCloud IQ Controller pre-installed Manufacturer certificate, which is different than a certificate used for AP 802.x authentication to the network. Uploading certificates to the AP (or enabling PEAP on the profile), is used for 802.1x authentication function.

On ExtremeCloud IQ Controller you can generate a unique .csr file for each AP. Then, send the .csr file to the certificate authority to be signed and returned as a unique .cer signed certificate. Another option is to apply a generic certificate (.pfx file) that you export from the certificate authority. Generic .pfx certificates can be applied to more than one AP.

Zip files can contain more than one unique .cer certificate. ExtremeCloud IQ Controller applies each certificate to the appropriate AP based on the identifying property: serial number, AP name, or MAC address. The zip file can also contain one generic .pfx file that can be applied to multiple APs. However, uploading a single zipped .cer certificate to multiple APs is not supported. Consider this when selecting more than one AP for certificate management.

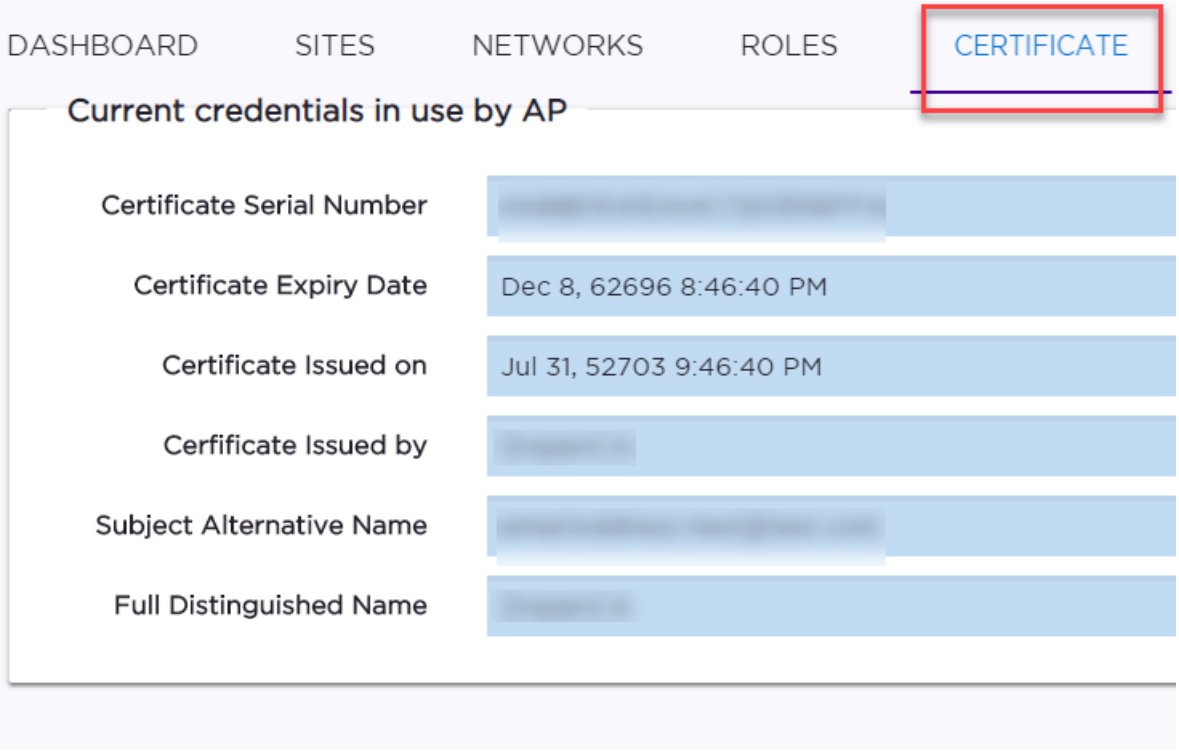
To manage certificates, go to **Configure** > **Devices** > **Access Points**. Select one or more access points and select **AP Actions** > **Manage Certificates**.

From the **Access Point List**, you can verify that a certificate has been applied. Select the **CERT** column for display.

To view certificate details for a selected AP:

1. Go to **Monitor** > **Devices** > **Access Points**.
2. Select an AP, then select the **Certificate** tab.

   Certificate details display.



Related Topics

AP Actions on page 206
Generate CSR on page 210
Apply Signed Certificate on page 211
Access Points List on page 69

Generate CSR

Complete the following attribute fields to generate a Certificate Signing Request (CSR).

Country Name

Two-letter ISO abbreviation for country name.

State or Province Name

Name of the state or province.

Locality Name

Name of the city or locality.

Organization Name

Name of the organization.

Organizational Unit

Name of unit within the organization.

Common Name

Possible values: AP Name, Serial Number, or MAC address.

Email Address

Email address for notification purposes.

Key Size

The number of bits in the key. This indicates encryption level. Valid values are 1024 or 2048.

Select **Generate CSR**. The certificate file is downloaded to your local machine.

Note
Send the .csr file to the certificate authority to be signed and returned as a .cer file.

Related Topics

Apply Signed Certificate on page 211
AP Certificates on page 209
AP Actions on page 206
Access Points List on page 69

Apply Signed Certificate

Before you apply a signed certificate, do one of the following:

- Generate a .csr file and send it to the certificate authority to be signed, returning a .cer file.
- Export a generic .pfx certificate from the certificate authority.

To apply a Signed Certificate:

1. (.PFX Only) Provide the password that was used when exporting a .pfx signed certificate from the certificate authority.
2. From the **Upload Signed Certificate** field, drop the certificate file. Or, select the field to navigate to the certificate file. Valid file types are:
   - .pfx

- .cer (DER Format)
- .zip

Note
Uploading a single zipped certificate to multiple APs is not supported.

Related Topics

Generate CSR on page 210
AP Certificates on page 209
AP Actions on page 206
Access Points List on page 69

Add APs

Access points and switches are automatically added to ExtremeCloud IQ Controller via the cloud-connector when the DHCP and DNS prerequisites have been met. For full instructions on configuring DHCP, NPS, and DNS services, refer to the *ExtremeCloud IQ Controller Deployment Guide*. You can use the Add functionality to pre-provision any AP or switch before they connect.

Using the Add functionality, you can clone an existing AP or add a unique AP configuration.

If you create device groups first, then add APs, a list of discovered APs that match the site and device group configuration settings will display on the **Edit Device Group** page. You can then select each AP from the **Edit Device Group** page to add it to the device group.

Tip
If your APs are not displaying within the **Edit Device Group** page, verify the following:

- AP licensing domain matches the site Country value.
- AP model number matches the site Type and the device group Profile configuration.

Note
You can add several APs and then register them at one time. An AP that is discovered by ExtremeCloud IQ Controller, but is not yet a member of a device group, has a status of *In-Service Trouble*.

1. Go to **Configure** > **Devices** > **Access Points**.
2. To add a new AP, select **Add**.
3. To add a clone, select the check box next to an AP in the list and select **Clone**.
4. Configure the following parameters:

   Model

   Select an AP model number from the drop-down list. The model number is on the AP.

   Serial Number

Unique number that identifies the AP. Provide this number for new and cloned APs. The serial number format is determined by the AP model. Some AP models require the user to pad the serial number with five trailing zeros.

Note
Serial numbers for AP models AP39xx and the 11ax standard WiNG AP models (AP3xx, AP4xx, and AP5xx), pad the registration serial number with five trailing zeros. For example, the serial number format for these AP models is *<SN>*00000, and must be entered as `2120W-2123400000` (16 digits).

Universal AP models: AP302W, AP305C/X, AP305C-1, AP410C/S6/S12, AP410C-1 and AP4000 do not include trailing zeros. The serial number format for these AP models is `64002103260092` (14 digits).

AP5010 does not include trailing zeros, the serial number format for this AP model is `640021032-60092` (15 digits).

The ExtremeCloud IQ Controller user interface prompts you for the proper format based on the AP model number.

Region

For all ExtremeWireless Wi-Fi 6E World-Wide Universal Access Points. For example, select the operational region for the AP5010 model.

Name

Unique name for the AP. Provide a unique name for new and cloned APs.

Description

Text description to help identify the AP.

5. Select **OK**.

Note
Most AP radio properties depend on a regulatory domain; which is defined at the site level. Devices that are connected to ExtremeCloud IQ Controller but not assigned to a device group have the status of *In-Service Trouble*. Devices that have not discovered ExtremeCloud IQ Controller have the status of *Unknown*.

Related Topics

Adoption Rules on page 318
Access Points List on page 69

Configure AP Details and Radio Settings

To modify settings for an access point (AP) and its radio properties:

1. Go to **Configure** > **Devices** > **Access Points**.
2. Select an AP from the list.

Name

Text field used to identify the AP.

Hostname

The Hostname for the AP. The Hostname value can be the same as or different from the AP Name. Both the AP Name and AP Hostname are displayed on the AP List and on the AP Details dialog. See Include Hostname in the Advanced Network Settings, to include the AP Hostname in the beacon signal.

Description

Optional description.

Environment

The operational environment of the AP.

Profile

Select the profile link to jump to the configuration Profile associated with the selected AP. All Profile changes affect all APs associated with the Profile. To override configuration settings for a specific AP, select **Advanced** > **Overrides** for the selected AP.

3. Configure the following radio properties:

Note
The AP must be part of a device group before the radio settings and the **Professional Install** button are displayed. To add an AP to a device group, see Add APs on page 212.

Table 56: Radio Properties

Field	Description
Radio Band Title	The title indicates the radio band and if the radio is configured for Mesh or Client Bridge. **Note:** Mesh and Client Bridge cannot be configured on the same AP.
Use RF Management Policy	Indicates if settings from the RF Management policy that is associated with the device group are used. Valid values: • **Yes**. Indicates that the Smart RF policy is used. Links to the RF Management Policy and the site are present. • **Fixed Channel**. Indicates that a manually configured channel plan is in use. The radio settings are displayed. You can modify Fixed Channel radio setting here. To modify an RF Management Policy, go to **Advanced** > **Overrides**. **Mesh:** Mesh Radio configuration supports **Fixed Channel** for root APs and **Mesh ACS** for non-root APs. See Configure a Mesh Point Network on page 262 for more information about configuring a Mesh Network.

Table 56: Radio Properties (continued)

Field	Description
Channel Width	Determines the channel width for the radio. Valid values are: • 20 MHz • 40 MHz • 80 MHz (supported on 5GHz only 802.11ac and 802.11ax) • 160 MHz ◦ AP5xx – Radio 1 and Radio 2 support 160 MHz ◦ AP4xx / AP4xxC – Radio 2 only (5 GHz band) supports 160 MHz ◦ AP4000/ AP4000-1 – Radio 2 (5 GHz band) and Radio 3 (6 GHz band) support 160 MHz ◦ AP5010 – Radio 1 (5 GHz band) and Radio 3 (6 GHz band) support 160 MHz. ◦ AP5050 – Radio 1 (5 GHz band) and Radio 3 (6 GHz band) support 160 MHz. (Radio 3 is currently turned off for regulatory compliance.) ◦ AP3xx/AP3xxC — *Do not support* 160 MHz width on the 5 GHz radio. A best practice is to use a predetermined width configured as part of the design of the entire RF deployment. To learn about how Smart RF handles channel width settings, see Understanding Smart RF and Channel Width on page 183. Select ⇶ to select a channel.
Request New Channel	Specifies the primary channel of the wireless AP. Depending on the licensed regulatory domain, channels may be restricted. ACS in the 2.4 GHz radio band with 40 MHz channels is not recommended due to severe co-channel interference.

Table 56: Radio Properties (continued)

Field	Description
Max Tx Power	Determines the maximum power level that can be used by the radio in dBm. The values are governed by compliance requirements based on the country, radio, and antenna selected, and will vary by AP.
DFS Fallback Channels	Specify a 5GHz channel that the radio will adopt if DFS (Dynamic Frequency Selection) fails. ExtremeWireless APs support up to 9 channels. The following setting is supported on ExtremeWireless access point models Wi-Fi 6 AP models that are configured for a Centralized site. **Note:** DFS is not recommended on a radio configured for Mesh. • **Return to configured channel after failed event**. When selected, the device returns to the configured radio channel after a DFS failed event. When this option is enabled, the following options display: ◦ **DFS Revert Hold Time**. The amount of time that a device will stay on a fallback channel before returning to the selected DFS channel. Valid values are 30 to 3600 minutes. The default value is 90 minutes. ◦ **DFS Revert Client Aware**. A threshold that determines if the radio will revert back to the DFS channel after moving to the configured channel. In addition to **DFS Revert Hold Time**, the radio client count also has to drop below the configured threshold. If the number of clients using the radio channel is less than the configured threshold, the radio will revert to the DFS channel. Valid values are 1 – 255. The default value is 0. Zero indicates that the conditioning based on number of clients is ignored.

4. Select **Save**.

Related Topics

Advanced AP Settings on page 221
Advanced Setting Overrides on page 221
Professional Install Settings on page 231
Understanding Smart RF and Channel Width on page 183
Channel Select Dialog on page 216

Channel Select Dialog

Use the **Channel Select** dialog to select radio channels for a selected AP radio.

1. Go to **Configure** > **Devices** > **Access Points**.
2. Select an AP.
3. To display the **Channel Select** dialog, next to Channel Width, select .

   The **Channel Select** dialog displays.

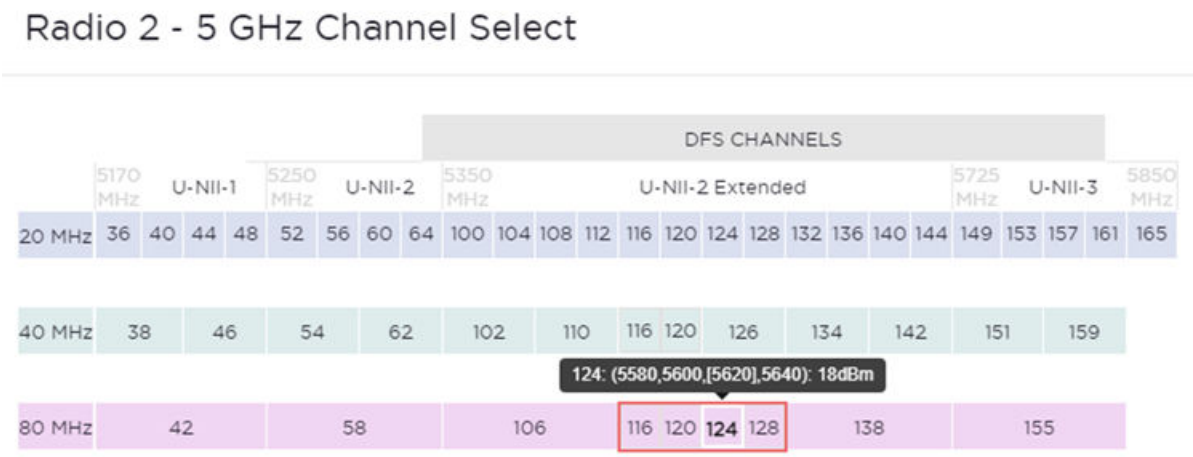


Figure 46: Channel Select dialog displaying 5 GHz band available channels

Note
The **Channel Select** dialog displays only channels that match the compliance for the selected AP.

The following details describe the **Channel Select** dialog:

- The selected channel number is displayed in a bold font with a lighter background.
- Select a different channel cell to change the channel selection. When you select a cell in a different radio band, the channel width will correspond to the new radio band selection.
- When the selected channels represent a combination of channels, the selected channels include a red border.
- Hover over the selected channels to display detailed frequency and power information.

For 6 GHz radios — When selecting the 20MHz and 40MHz channel widths, all channels are available. When selecting 80 MHz and 160 MHz channel widths, only the Preferred Scanning Channels (PSC) can be configured. The other channels are disabled and are displayed in a gray font with a lighter background. Frequency and power information is not available for disabled channels. PSC channels are: 5, 21, 37, 53, 69, 85, 101, 117, 133, 149, 165, 181, 197, 213, 229.

Figure 47: Channel Select dialog displaying 6 GHz band available channels

Related Topics

6 GHz Channel Allocation and Notation on page 23

Configuring RF Management

RF Management profiles are AP model dependent and reusable. Default profiles are intended to make RF Management easy, getting you up and running without having to configure an RF policy. However, you can always create additional profiles based off of default RF Management profiles. The RF Management support is dependent on the AP model.

The following AP models are supported:

- AP39xx supporting ACS Policy for RF Management
- Wi-Fi 6 AP models supporting Smart RF Policy for RF Management

Related Topics

Configuring ACS RF Policy on page 185
Configuring Smart RF Policy on page 187

AP Feature Restrictions in Low Power Mode

The following tables describe the AP feature restrictions when the access point is operating in 802.3af (Low Power Mode). The information is organized by AP model number:

- AP5xx models
- AP4xx models
- AP3xx models
- AP4xxC models
- AP3000/X models
- AP4000
- AP5010

Consider the following labels to determine if a feature is supported in Low Power Mode:

- **Yes**. Supported in Low Power Mode
- **No**. Not Supported in Low Power Mode
- **N/A**. Not applicable for the AP model.

Table 57: Low Power Mode Feature Restrictions for AP5xx models

AP Model	Power Profile	2.4 GHz Radio	5 GHz Radio	Dual 5GHz	USB	PSE
AP510i	802.3af	16 (2x2)	16 (2x2)	No	No	N/A
AP510e	802.3af	14 (2x2)	14 (2x2)	No	No	N/A
AP505i	802.3af	18 (2x2)	18 (2x2)	N/A	No	N/A
AP560i/h	802.3af	16 (2x2)	16 (2x2)	No	N/A	N/A

Table 58: Low Power Mode Feature Restrictions for AP4xx models

AP Model	Power Profile	Sensor	2.4 GHz Radio	5 GHz Radio	Dual 5GHz	USB	PSE
AP410i	802.3af	• 20 for 2.4GHz • 20 for 5GHz	20	20 (2x2)	N/A	No	N/A
AP410e	802.3af	• 19 for 2.4GHz • 18 for 5GHz	19	18 (2x2)	N/A	No	N/A
AP460i	802.3af	• 20 for 2.4GHz • 22 for 5GHz	23	22 (2x2)	N/A	No	N/A
AP460e	802.3af	• 19 for 2.4GHz • 20 for 5GHz	22	20 (2x2)	N/A	No	N/A

Table 59: Low Power Mode Feature Restrictions for AP3xx models

AP Model	Power Profile	Radio 1 2.4/5GHz	5 GHz Radio	Dual 5GHz	USB	PSE
AP310i	802.3af	• 20 for 2.4GHz • 19 for 5GHz	20	Yes	No	No
AP310e	802.3af	• 19 for 2.4GHz • 17 for 5GHz	18	Yes	No	No

Table 59: Low Power Mode Feature Restrictions for AP3xx models (continued)

AP Model	Power Profile	Radio 1 2.4/5GHz	5 GHz Radio	Dual 5GHz	USB	PSE
AP360i	802.3af	• 23 for 2.4GHz • 21 for 5GHz	21	Yes	No	No
AP360e	802.3af	• 22 for 2.4GHz • 19 for 5GHz	19	Yes	No	No
AP305C/X	802.3af	• 18 for 2.4GHz • 18 for 5GHz	18	Yes	no	na
AP302W	802.3af	• 18 for 2.4GHz • 18 for 5GHz	18	Yes	Yes	no

Table 60: Low Power Mode Feature Restrictions for AP4xxC models

AP Model	Power Profile	Sensor	2.4 GHz Radio	5 GHz Radio	Dual 5GHz	USB	PSE
AP410C	802.3af	15	14 (2.4GHz)	17 (5GHz 3x3)	No	No	N/A
AP460C	802.3af	15	14 (2.4GHz)	17 (5GHz 2x2)	No	No	N/A
AP460S12C	802.3af	15	14 (2.4GHz)	17 (5GHz 2x2)	No	No	N/A
AP460S6C	802.3af	15	14 (2.4GHz)	17 (5GHz 2x2)	No	No	N/A

Table 61: Low Power Mode Feature Restrictions for AP3000/X

AP Model	Power Profile	2.4 GHz Radio	5 GHz Radio	6 GHz Radio	Dual 5GHz	USB	PSE
AP3000/X	802.3af	16	16	16	N/A	No	N/A

Table 62: Low Power Mode Feature Restrictions for AP4000

AP Model	Power Profile	2.4 GHz Radio	5 GHz Radio	6 GHz Radio	Dual 5GHz	USB	PSE
AP4000	802.3af	16	16	16	N/A	No	N/A

Table 63: Low Power Mode Feature Restrictions for AP5010

AP Model	Power Profile	2.4 GHz Radio	5 GHz Radio	6 GHz Radio	Dual 5GHz	USB	PSE
AP5010	802.3af	10 2x2	10 2x2	10 2x2	N/A	OFF	OFF

Related Topics

AP5000 Series Power Management on page 21

Advanced AP Settings

Table 64: Advanced AP Setting Actions

Actions	Description
Reboot	Restart the AP.
Retrieve Trace	ExtremeCloud IQ Controller collects information from the AP, including logs and crash reports if applicable.
Download Trace	Download the trace report.

Related Topics

Advanced Setting Overrides on page 221
IP Address Assignment on page 230

Advanced Setting Overrides

Many AP properties are configured from the device group configuration Profile, where they apply to all APs in the device group. Override the following settings for a specific AP from the **Advanced** > **Overrides** tab.

Best Practice: For a consistent configuration, a best practice is to configure the APs through the configuration Profile. Overrides are available for unique configuration. However, variances from the configuration Profile can result in APs not receiving general policy changes. Consider configuration Overrides carefully. To determine which APs are configured with overrides, from the **AP List**, display the **Overrides** column. See Access Points List on page 69.

To access the **Overrides** dialog:

1. Go to **Configure** > **Devices** > **Access Points**.
2. Select an AP.
3. Select **Advanced** > **Overrides**.

Table 65: Advanced AP Setting Overrides

Field	Description
Management VLAN ID Override	Virtual Local Area Network Identifier. Enable VLAN tagging to insert a VLAN ID into a packet header identifying which VLAN the packet belongs to. You can configure this setting for all APs in a device group from the device group **Advanced Settings** dialog. And, you can override the device group setting for an individual AP from here.
Static MTU	A static Maximum Transmission Unit (MTU). When this option is enabled, the MTU is fixed at the value you specify. Otherwise, the default value of 1500 is used.

Table 65: Advanced AP Setting Overrides (continued)

Field	Description
GE2 Port Function	Specify the function of the second AP Ethernet port: • Client. Indicates that the client port is enabled on the AP. The client option is used in the following scenarios: ◦ When an AP radio is configured as a Client Bridge. ExtremeCloud IQ Controller automatically sets the GE2 port to **Client**. ◦ To leverage the second port of the access point as a Client port, allowing pass-through access to attached clients. Client access is subject to policy. This capability is also utilized in support of work group meshing. A GE2 Client port is supported on the following access points: ▪ Wi-Fi 6 AP models ▪ AP3965 When the GE2 Port is set to **Client**, the WLAN assignment dialog displays an option to specify the GE2 assignment, and the **Wired Ports** tab is available from the AP Profile. • When the GE2 Port is set to **Bridge**, the port provides a transparent bridge that transports tagged and untagged traffic between two sides of a wireless connection, while preserving VLAN mappings over the wireless link. Packet tagging and policy is configured through services outside the wireless network configuration. A GE2 Bridge port is supported on the following access points that have more than one Ethernet port: Wi-Fi 6 AP models. **Note:** The ETH1/GE2 Bridge port is *not* supported on access points with a single Ethernet port. For more information, see Transparent Bridge on page 263. • AP Ethernet port traffic backup (failover) between GE1 and GE2 • LAG (Link Aggregation Group) Link aggregation combines network connections to increase throughput and to provide redundancy in case of link failure. Requires that both ports negotiate to the same speed (1 Gbps). **Note:** LAG is supported on ExtremeWireless AP39xx and 11ax APs. LAG *is not* supported on AP305C, AP410C, and AP460C.

Table 65: Advanced AP Setting Overrides (continued)

Field	Description
AP Event Level	Enable to override the AP Event Level for a specific AP. Valid log level values are: Critical, Major, Minor, and Info. You can also override the AP Event Level for multiple APs from the AP Actions menu on the Device List.
Force Normal Power Operation	Instructs the AP to draw normal power from the POE switch port for full-capacity operation regardless of the IEEE 802.3 ft/at/bt and or LLDP-MED power switch port negotiation. The defined power level for full-capacity power operation is unique for each AP model. Refer to the hardware documentation for each AP model. **Note:** Use this setting with caution. Improper use can result in an AP power source overload, resulting in an unstable AP operation.
Poll Timeout	Specifies the amount of time, in seconds, to wait for a response from the appliance before rebooting. The value range is from 3 to 600 unless the controller is in an availability pair without fast failover enabled. The default value is 3. You can configure this setting for all APs in a device group from the device group **Advanced Settings** dialog. And, you can override the device group setting for an individual AP from here.
FA Auth Key	Configure custom Fabric Attach Authentication Keys up to 32 characters in length. Extreme Networks products offer a default FA AUTHENTICATION-KEY built-in. You can also configure a custom key here. When a custom key is not configured, the default key is used. The following special characters are *not* supported: {? <tab> \ “ `} **Note:** Supported on Wi-Fi 6 AP models. You can configure this setting for all APs in a device group from the device group **Advanced Settings** dialog. And, you can override the device group setting for an individual AP from here.

Table 65: Advanced AP Setting Overrides (continued)

Field	Description
LED Status	You can configure LED Status for all APs in a device group from the device group Profile Advanced settings. You can also override LED Status for an individual AP from here. Valid values are: **Off** LEDs do not light. **Locate** LEDs blink so you can locate the AP. **Normal** Default mode for all APs. Identifies the AP status during the following processes: • registration • power on • boot **Note:** The value **Solid** has been deprecated in ExtremeCloud IQ Controller version 5.26.02. If Solid was previously configured, this value is mapped to **Normal** with the ExtremeCloud IQ Controller version 5.26.02 upgrade.
Adoption Preference	Indicates the preferred controller for device adoption. Use this setting to control the number of APs adopted by each controller in an availability pair. Define AP-Controller mappings for system efficiency and control over roaming domains. Valid values are: • Use global availability settings. This option refers to the Auto AP Balancing configuration described in Availability Pair Settings on page 449. To configure Auto AP Balancing, go to **Administration** > **System** > **Availability**. • Primary Appliance • Backup Appliance
WLAN	You can override the radio WLAN assignments for a specific AP. The result is that the AP has a unique radio WLAN assignment, plus port and IOT assignments, and policy definitions that are defined in the configuration Profile. The AP must be part of a device group, but you can override the WLAN per AP in order to enable or disable a selected network. This can be useful for testing and troubleshooting purposes. See WLAN Override on page 227.

Table 65: Advanced AP Setting Overrides (continued)

Field	Description
PEAP User Name and Password	Ability to configure the PEAP (Protected Extensible Authentication Protocol) user name and password for all devices in a device group or for a specific device override. Used to pre-provision devices for authorization to connect to the network. Credential and Certificate installation procedures are supported for AP39xx, SA201 Adapter, and Wi-Fi 6 AP models.
Enforce Manufacturing Certificate	Enforce usage of Extreme PKI (Public Key Infrastructure) when establishing an IKE (Internet Key Exchange) tunnel. Both APs and controllers have Extreme CA certificates installed. When this setting is enabled, the controller accepts only APs that provide Extreme PKI. Note: Supported on the Defender Adapter SA201 and on the ExtremeWireless access point models: AP39xx, Wi-Fi 6 AP models. This setting *is not* supported on the AP305C, AP410C, and AP460C access point models. There must be successful mutual authentication between the AP and the controller. If either side of the authentication fails, the tunnel is rejected. When this setting is enabled, APs that are not PKI capable (self-signed certificates) *are not* able to connect to the controller. The default is to clear this option. When this setting is cleared, the controller accepts the AP with a self-signed certificate. With either type of certificate, the certificate type must match in both directions before the authenticated tunnel is established. Authentication failure messages are logged in the ExtremeCloud IQ Controller Events Log. You can configure this setting for all APs in a device group from the device group **Advanced Settings** dialog. And, you can override the device group setting for an individual AP from here.

Table 65: Advanced AP Setting Overrides (continued)

Field	Description
Client Bridge	**Client Bridge Override** — Select to enable override settings. **Roaming RSS Threshold** — Determines when the client bridge AP scans to find a better infrastructure AP. Valid range: from -128 to -40. Default value is -70. A scan is triggered when one or more of the following criteria is met: • When the infrastructure AP RSS value is less than the configured RSS Threshold. • When the poll of the infrastructure AP is lost for one second. **Note:** When a WLAN is configured on the client bridge AP, a scan is triggered whenever the poll of the infrastructure AP is lost, regardless of the RSS Threshold. You can configure this setting for all APs in a device group from the device group **Advanced Settings** dialog. And, you can override the device group setting for an individual AP from here.
IOT Settings	IoT is supported on the following access point models: AP391x, Wi-Fi 6 AP models. The following AP models *do not* support IoT: AP3935, AP3965, AP305C-1, AP310i/e-1, AP410i-1, AP410C-1, AP510i-1, and AP4000-1 You can configure beacon settings for all APs in a device group from the device group Profile **IoT** tab. And you can override some beacon application settings for an individual AP from here. The following applications support AP overrides: • iBeacon application. Overrides are supported for the following settings: ◦ IoT iBeacon Major ◦ IoT iBeacon Minor ◦ Measured RSSI • Eddystone-url Beacon application. Overrides are supported for the following settings: ◦ Eddystone URL ◦ Measured RSSI **Note:** If a beacon application is not configured in the device group Profile, the IOT pane is empty.

Table 65: Advanced AP Setting Overrides (continued)

Field	Description
Mesh Points	The mesh point settings on an AP radio can be overwritten here. Mesh point configuration is handled from the device group configuration Profile. If you want to modify configuration for a mesh point, check the mesh point check box to display the edit button (✎). Select ✎ to display the **Edit Mesh Device Settings** dialog. To override a setting, select the check box and provide an override value. **Note:** Mesh Device Setting overrides are available when the AP is part of a Mesh Network. **Important:** It is not a best practice to override the Root setting for a specific AP. Configure the Root setting from the device group.
Smart Poll	Smart Poll configuration is handled from the device group configuration Profile. The Smart Poll settings for an AP can be overwritten here. To modify configuration for an individual AP, select **Smart Poll Override** and configure the Smart Poll parameters.
Radio Setting Overrides	You can configure radio settings for all APs in a device group from the device group Profile **Radio** tab and **Advanced Radio** dialog. And you can override radio settings for an individual AP from here.

Related Topics

WLAN Override on page 227
Cell Size Control Settings on page 229
Advanced AP Settings on page 221
IP Address Assignment on page 230
Advanced Configuration Profile Settings on page 172
iBeacon Settings on page 165
Eddystone-url Beacon Settings on page 168
Advanced AP Radio Settings on page 153
Advanced Configuration and Mesh Device Settings on page 139

WLAN Override

A configuration Profile is specified at the device group. All access points that are part of the device group are associated with the same configuration Profile. The network policies are created based on default policies defined for the WLAN, and policies added directly to the configuration Profile. The AP has all WLAN and policy assignments based on the corresponding Profile.

You can override the radio WLAN assignments for a specific AP. The result is that the AP has a unique radio WLAN assignment, plus port and IOT assignments, and policy definitions that are defined in the configuration Profile. The AP must be part of a device group, but you can override the WLAN per AP in order to enable or disable a selected network. This can be useful for testing and troubleshooting purposes.

Note
ExtremeCloud IQ Controller will display a warning if the network reassignment affects the primary BSSID on the radios, resulting in a radio reset. You will have the opportunity to consider the impact of network reassignment before overriding a WLAN.

ExtremeCloud IQ Controller automatically determines the related role assignments that are referred by the new WLAN service, and it adjusts the role listing per AP. Roles assigned to the Profile and roles referenced by the new WLAN Service are merged. The larger role set is visible per AP for diagnostic purposes.

To override the WLAN assignment:

1. On the **Overrides** tab, select **WLAN**, and then select **Configure**.

   ExtremeCloud IQ Controller displays a list of configured networks. The settings that display are those that are inherited from the associated configuration Profile.
2. Select the WLAN assignment per radio.

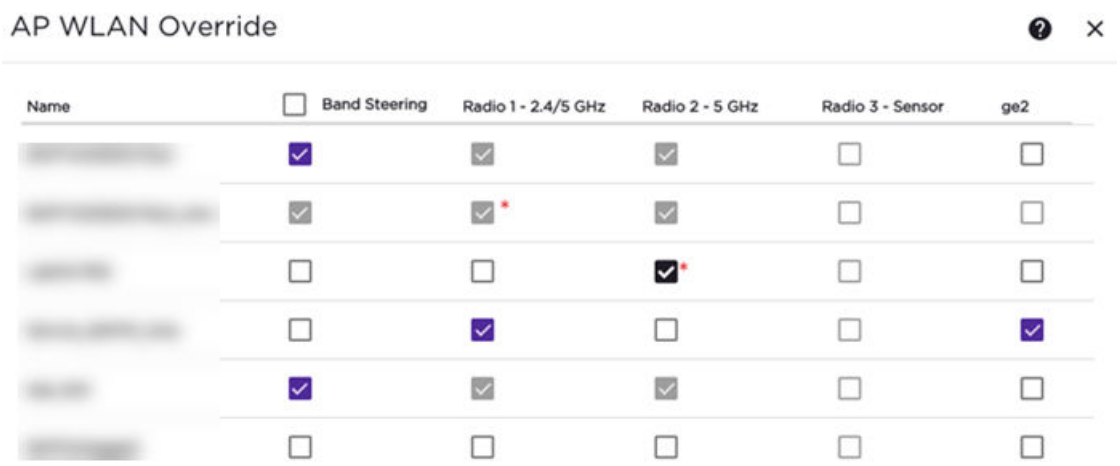


Figure 48: AP WLAN Override

3. (Optional) Enable **Band Steering** for the selected AP.

   Band Steering is intended to relieve congestion by encouraging dual-band client devices to use the higher capacity 5 GHz band. To make use of Band Steering, ensure that networks are assigned to both radios.

   For Band Steering to work effectively, configure similar coverage areas for the 2.4 GHz and 5 GHz bands. Design the network for both 5 GHz and 2.4 GHz coverage. For networks where coverage quality differs between bands, disable Band Steering.

Band Steering requires that the same SSID be present on both 2.4 GHz and 5 GHz radios. ExtremeCloud IQ Controller automatically collapses radio assignments to a single selection when Band Steering is enabled, and a single, dual-band radio is represented for WLAN service override assignment. Adding a WLAN service automatically creates an assignment to both radios (2.4 GHz and 5 GHz). You can disable Band Steering at either the AP override or on the **Networks** tab of the configuration Profile, to regain control over the WLAN assignment per radio band.

Note
The Band Steering feature steers 5 GHz clients toward the 5 GHz band. 6E clients can self steer into the 6 GHz band for service.

On the AP List, a check mark in the **Override** column indicates that the AP is associated with an Override.

Related Topics

Advanced Setting Overrides on page 221
Add or Edit a Configuration Profile on page 134

Cell Size Control Settings

These AP settings help improve network connectivity. They can be set at the device group level or as an AP Override setting.

Table 66: Cell Size Control Settings

Field	Description
Probe Suppression on Low RSS	Reduces the number of probe responses by preventing clients with low RSS from associating with an AP radio. This setting is configured per radio. Clients with RSS measured below the Probe Suppression RSS Threshold will not associate with the AP. This setting is disabled by default.
Disassociate on Low RSS	This setting is supported on AP39xx, AP3xx, AP4xx, or AP5xx. It is always disabled by default. This setting forces clients with low RSS to disassociate from an AP radio. This setting is configured per radio. A client is forced off an AP radio when RSS is measured at 5dBm below the Probe Suppression RSS Threshold. Enabling this option forces a client to roam to a better AP for improved network performance.

Table 66: Cell Size Control Settings (continued)

Field	Description
Probe Suppression RSS Threshold (dBm)	This setting is available when **Probe Suppression on Low RSS** is enabled. This setting determines the RSS threshold for forced disassociation and probe suppression. The default threshold is -90 dBm. Valid value range is -50dBm to -100dBm. **Best Practice:** Probe Suppression Threshold should not be greater than -70dB. The Probe Suppression Threshold defines the signal strength value that is deemed too low to be acknowledged by the AP. Setting the threshold above -70dB can result in an AP not acknowledging clients in close proximity, leading to poor connectivity or a sub-optimal roaming experience. The best practice is to follow the Site Survey methodology to determine the best value for the AP installation.
Probe Response Retry Limit	The default Probe Response Retry Limit is 4. If devices are having a problem connecting to the network, due to congestion or due to the quality of the device, consider increasing the retry limit. Maximum value is 10.
Rx Sensitivity Reduction (dB)	New APs are very sensitive and can pick up unwanted channel interference. If this is an issue, add an offset of 5-10 dB, which will reduce signal sensitivity and improve signal quality.

Related Topics

Advanced Setting Overrides on page 221

IP Address Assignment

Table 67: IP Address Assignment Settings

Field	Description
DHCP	Indicates if a DHCP Server is used to assign the AP IP address. The server relies on the standard protocol known as Dynamic Host Configuration Protocol (DHCP) to respond to broadcast queries by clients. When you select **DHCP**, the IP address fields display the server-assigned address information. For more information about configuring a DHCP server, see the *ExtremeCloud IQ Controller Deployment Guide*.
Static	Indicates if a permanent IP address is assigned for this AP. After selecting **Static**, provide the information for the following address fields: • IP Address • Mask — Subnet Mask • Default Gateway

Related Topics

Advanced AP Settings on page 221
Advanced Setting Overrides on page 221

Professional Install Settings

To configure external antennas on an AP, add the AP to a valid device group. Then configure the antennas:

1. Go to **Configure** > **Devices** > **Access Points**.
2. Select an AP model that offers configurable antennas.

   Note
   Professional Install is offered on AP models with external antennas and on AP models that have internal selectable antennas. The AP must be a member of a valid device group.

3. Select **Professional Install**.

The fields and corresponding antenna value options on the **Professional Install** dialog depend on the selected AP and the antenna models that are available. Select an antenna for each available port. By default, the two antennas must be identical. However, you have the option to select **No Antenna** for the second antenna port. Select the antenna model from the drop-down field. Choose the desired attenuation for each radio from the drop-down list. Selectable range is from 0 to 30 dBI. Additionally, the AP3915e, AP3917e, and AP510e access point models offer an external IoT antenna.

Note
Single-band antennas limit the AP operation to the radio that is associated with the antenna and reduce the sensor functionality of the IoT sensor radio.

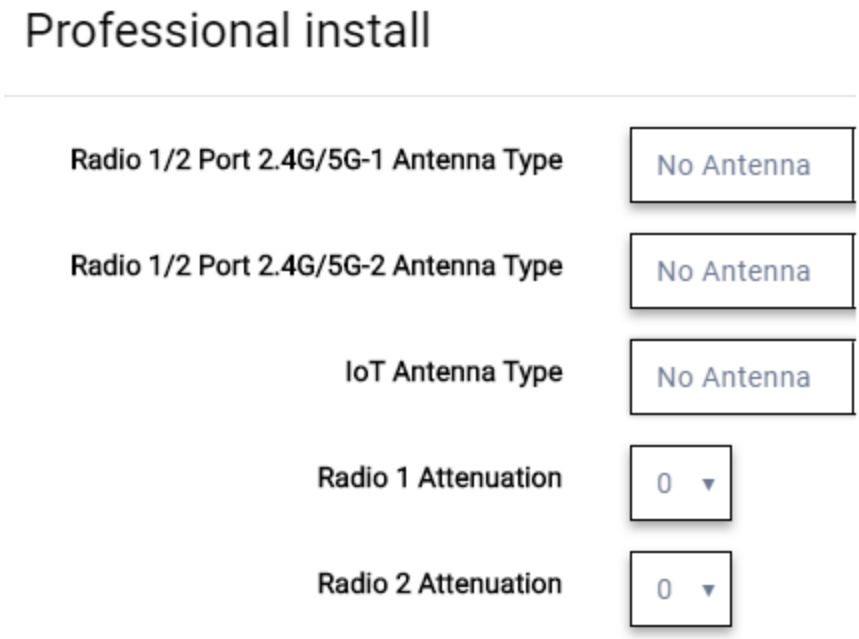


Figure 49: Professional Install Settings (Two port AP)

Related Topics

AP305CX Professional Install on page 232
AP310e/AP360e Professional Install Settings on page 233
AP410e Professional Install Settings on page 234
AP460e Professional Install Settings on page 235
AP510e Professional Install Settings on page 236
AP560h Professional Install on page 238
AP3000X Professional Install Settings on page 238
AP5050D Professional Install Settings on page 239
Advanced AP Settings on page 221
Configure AP Details and Radio Settings on page 213
Add APs on page 212

AP305CX Professional Install

The antenna ports for the AP305CX are defined as follows:

- Radio 1 Port 2.4/5G-1
- Radio 1 Port 2.4/5G-2
- Radio 2 Port 5G-3
- Radio 2 Port 5G/IoT-4

The antenna list is dependent on your regulatory domain. The default antenna is the antenna with the highest gain.

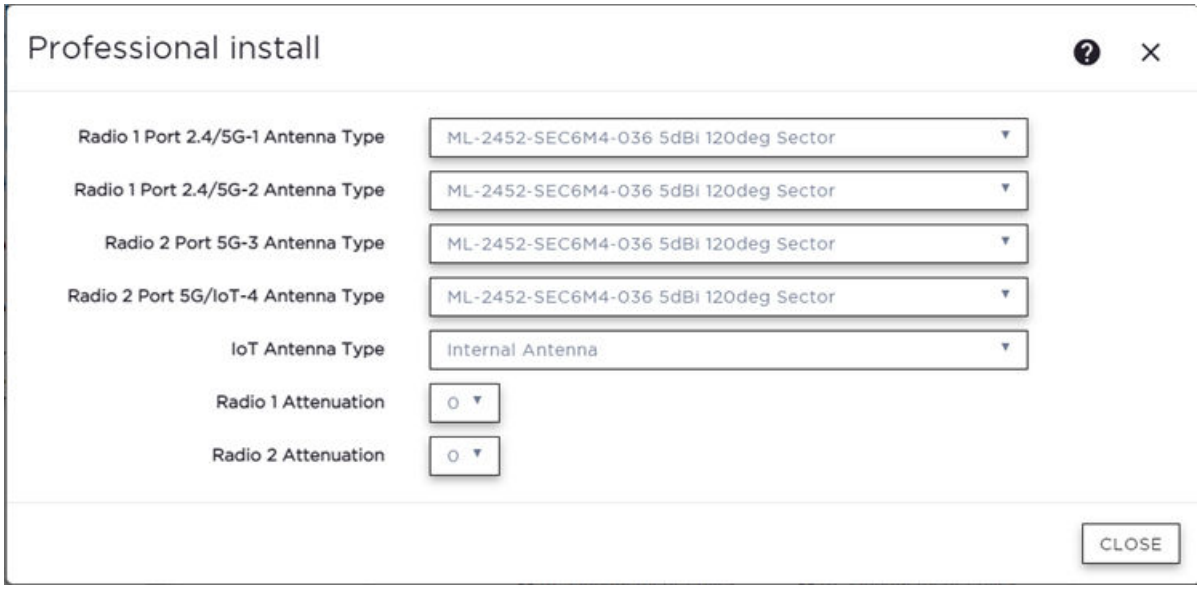


Figure 50: AP305CX External Antenna Configuration

AP310e/AP360e Professional Install Settings

The following rules apply to AP310e and AP360e antenna installation:

- Group 1 (2.4 GHz/5 GHz) accepts identical dual-band antennas.
- Group 2 (5 GHz) accepts identical 5 GHz or dual-band antennas.
- Antennas must be configured consecutively for each group. Group 1 starts with Port 1/Group 1 and Group 2 starts with Port 3/Group 2. An equal number of antennas must be configured for both groups. For example, to support a 2x2 deployment, install Group 1 and Group 2 — 2 antennas each.
- Mode 1. Radios 1 and 2 are enabled when:
  - Both groups of antennas must be configured. Radio 1 is enabled only if one or more antennas are configured in Group 1. Radio 2 is enabled only if one or more antennas are configured in Group 2.
- Mode 2. Radio 1 is a 2.4/5 GHz sensor and Radio 2 forwards traffic.
  - Radio 1 dual-band sensor is enabled only if one or more antennas are configured in Group 1.
  - Radio 2 5 GHz WLAN service is enabled only if one or more antennas are configured in Group 2.
- Mode 3. Radios are configured Dual 5 GHz mode.
  - Radio 1 is enabled only if one or more antennas are configured in Group 1.
  - Radio 2 is enabled only if one or more antennas are configured in Group 2.

Table 68: Radio Modes AP310e/AP360e

Mode	Radio 1	Radio 2
1	2.4 GHz traffic forwarder	5 GHz traffic forwarder
2	2.4 GHz/5 GHz sensor	5 GHz traffic forwarder

Table 68: Radio Modes AP310e/AP360e (continued)

Mode	Radio 1	Radio 2
3	5 GHz traffic forwarder (channels 36-64)	5 GHz traffic forwarder (channels 100-165)
Sensor	2.4 GHz sensor	5 GHz sensor

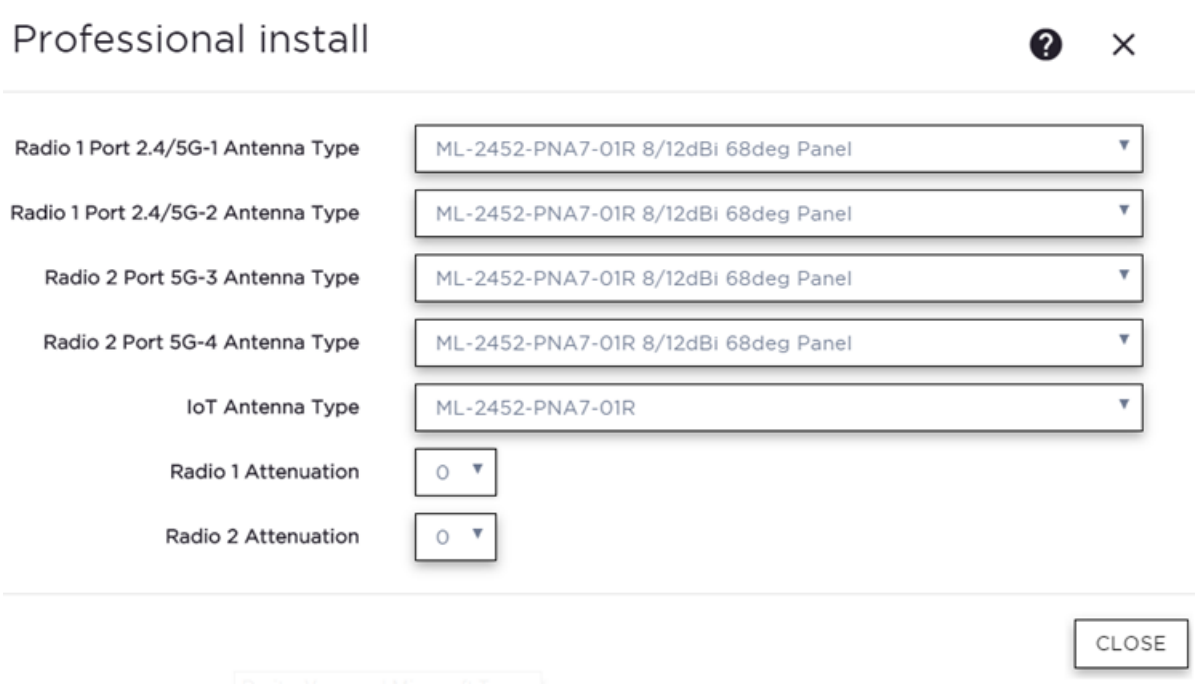


Figure 51: AP310e/AP360e Antenna Professional Install

Related Topics

Add APs on page 212

AP410e Professional Install Settings

The AP410e is an indoor AP with external antennas. The AP410e has the following antenna layout:

- Radio 1 and Radio 2 share ports 1 and 2
- Radio 2 uses ports 3 and 4
- Radio 3 uses ports 5 and 6
- IoT radio uses port 7 (not configurable)

The default value for Radios 1-3 is “No Antenna”, and the default value for the IoT radio is “Internal."

The ports are grouped as follows. Each port in the group must be configured with the same antenna model:

- Group 1 — Ports 1 through 4

- Group 2 — Ports 5 and 6

Note
To display the **Professional Install** dialog, the AP must be part of an AP410e device group.

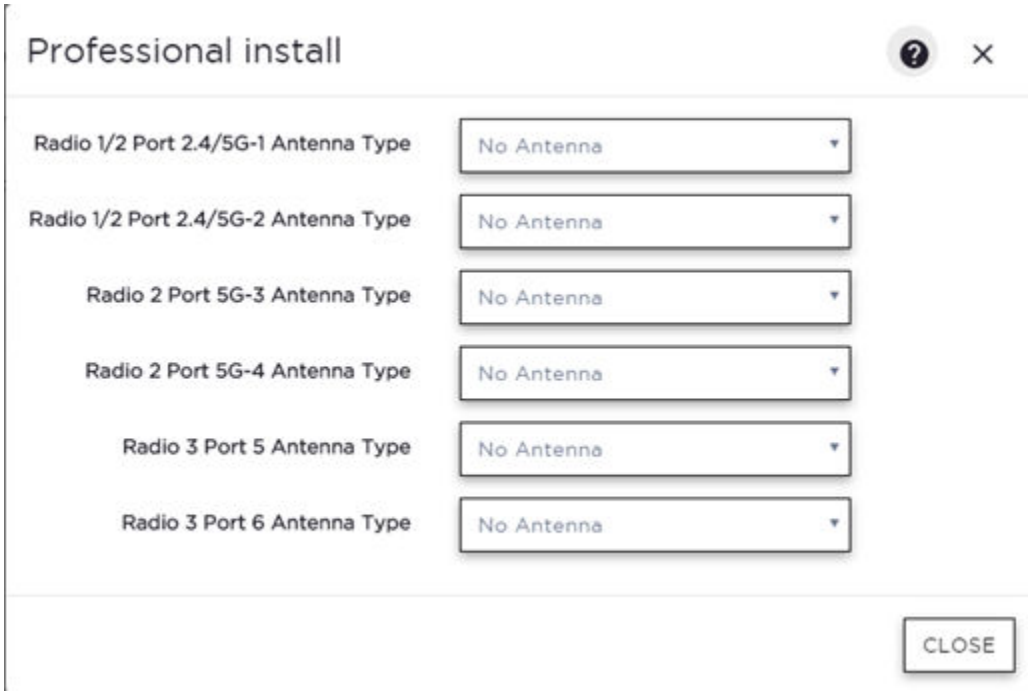


Figure 52: AP410e Professional Install Settings

Related Topics

Add APs on page 212

AP460e Professional Install Settings

The AP460e is an outdoor AP with external antennas. The AP460e has the following antenna layout:

- Radio 1 uses ports 5 and 6
- Radio 2 uses ports 1 through 4
- Radio 3 uses ports 7 and 8
- IoT radio uses port 9 (not configurable)

The default value for Radios 1-3 is “No Antenna”, and the default value for the IoT radio is “Internal."

The ports are grouped as follows. Each port in the group must be configured with the same antenna model:

- Group 1 — Ports 1 through 4 (Radio 2)
- Group 2 — Ports 5 and 6 (Radio 1)

- Group 3 — Ports 7 and 8 (Radio 3)

Note
To display the **Professional Install** dialog, the AP must be part of an AP460e device group.

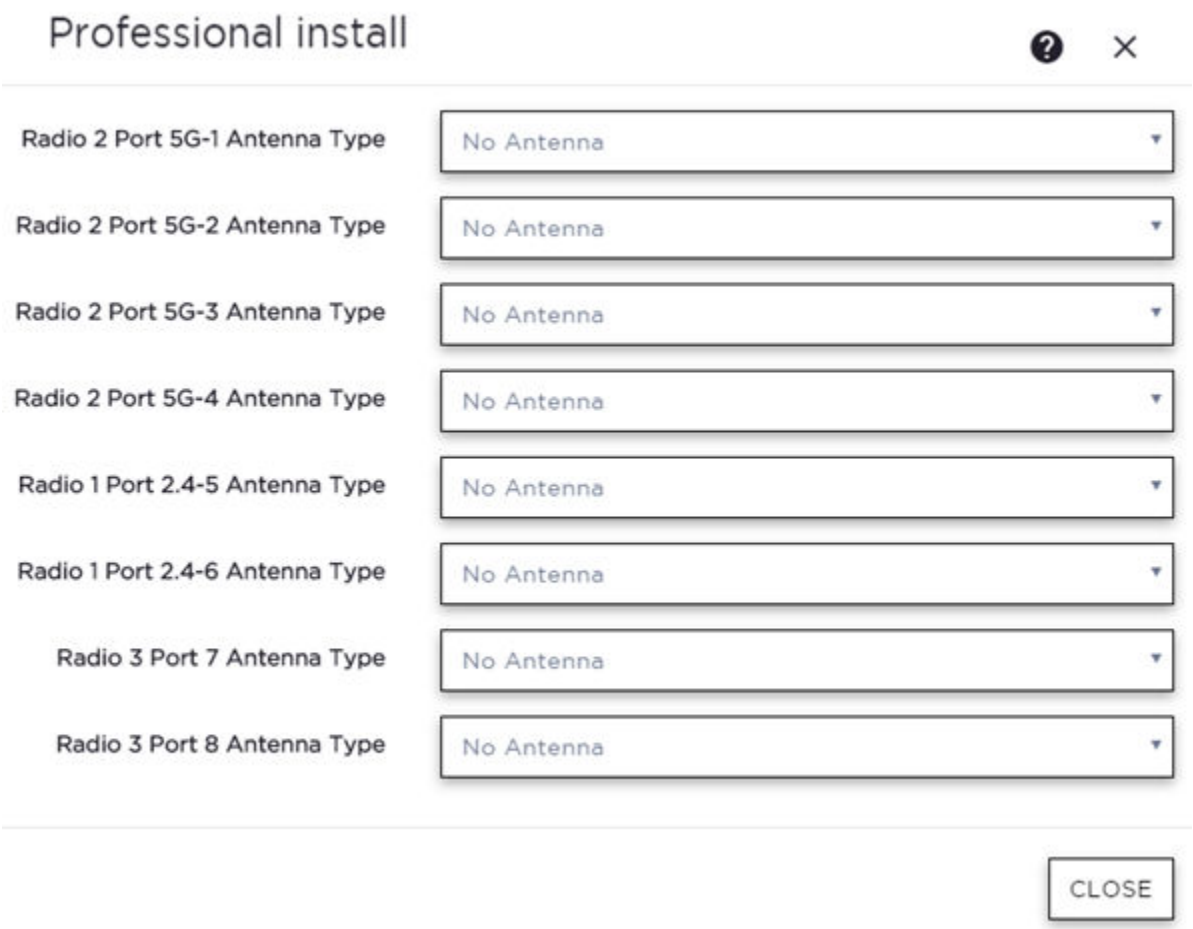


Figure 53: AP460e Professional Install Settings

Related Topics

Add APs on page 212

AP510e Professional Install Settings

The following rules apply to AP510e antenna installation:

- Group 1 (2.4GHz/5GHz) accepts identical dual band antennas.
- Group 2 (5GHz) accepts identical 5G or dual band antennas.
- Antennas must be configured consecutively for each group. Group 1 starts with Port 1/Group 1 and Group 2 starts with Port 5/Group 2. An equal number of antennas must be configured for both groups. For example, to support a 4x4 deployment, install Group 1 & Group 2 — 4 antennas each. To support a 2x2 deployment, install Group 1 & Group 2 — 2 antennas each.

- Mode 1. Radios 1 and 2 are enabled when:
  - One or more antennas are configured in Group 1.
- Mode 2. Radio 1 is a 2.4/5 GHz sensor and Radio 2 forwards traffic.
  - Radio 2 WLAN Service.
    - Radio 2 5GHz WLAN service needs Group 1 antenna.
  - Radio 1 – Sensor.
    - Radio 1 2.4GHz sensor needs Group 1 antenna.
    - 5GHz sensor need Group 2 antenna.
    - Or, Dual-band sensor needs one or more antennas configured in both Group 1 and Group 2.
- Mode 3. Radios are configured Dual 5GHz mode.
  - Radio 1 is enabled only if one or more antennas are configured in Group 2.
  - Radio 2 is enabled only if one or more antennas are configured in Group 1.

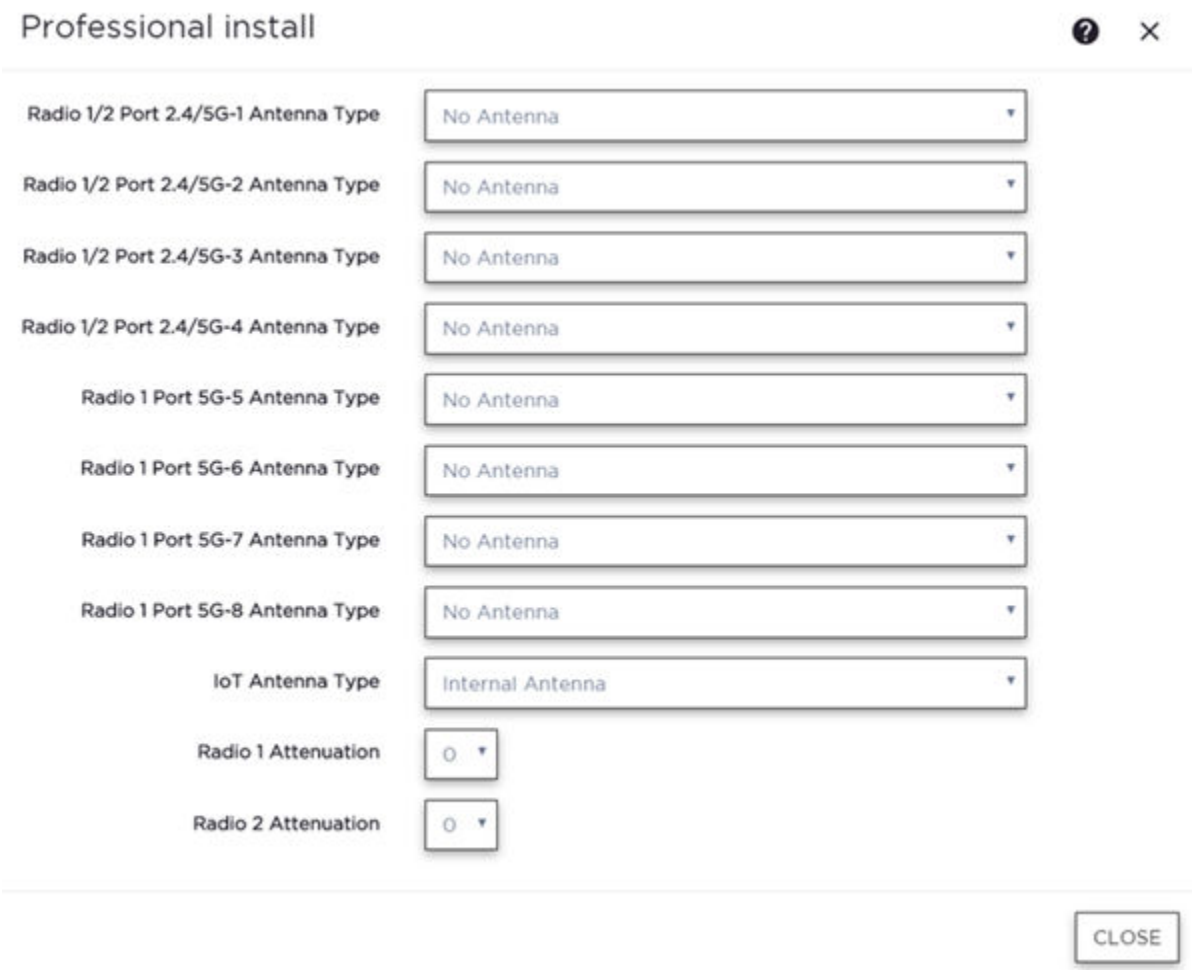


Figure 54: AP510e Antenna Professional Install

Related Topics

Add APs on page 212

AP560h Professional Install

The AP560h is an outdoor AP that has two types of selectable, internal antenna. Select one of the following antennas:

- INTERNAL-560H-30, dual band, 8feed, 30 degree sector. This is the default antenna.
- INTERNAL-560H-70, dual band, 8feed, 70 degree sector

Note
The AP must be part of an AP560 device group to display the **Professional Install** dialog.

Figure 55: AP560h Professional Install Settings

Related Topics

Add APs on page 212

NEW!

AP3000X Professional Install Settings

The AP3000X supports two configurable external antenna. The same antenna can be used for both the 2.4 GHz radio and the 5 GHz radio, when the AP is in 2.4 GH / 5 GHz mode. When the AP is in 6 GHz / 5GHz mode, only the 5 GHz radio is supported. The 25-85392-01R adapter is required.

Note
The AP must be part of an AP3000X device group to display the **Professional Install** dialog.

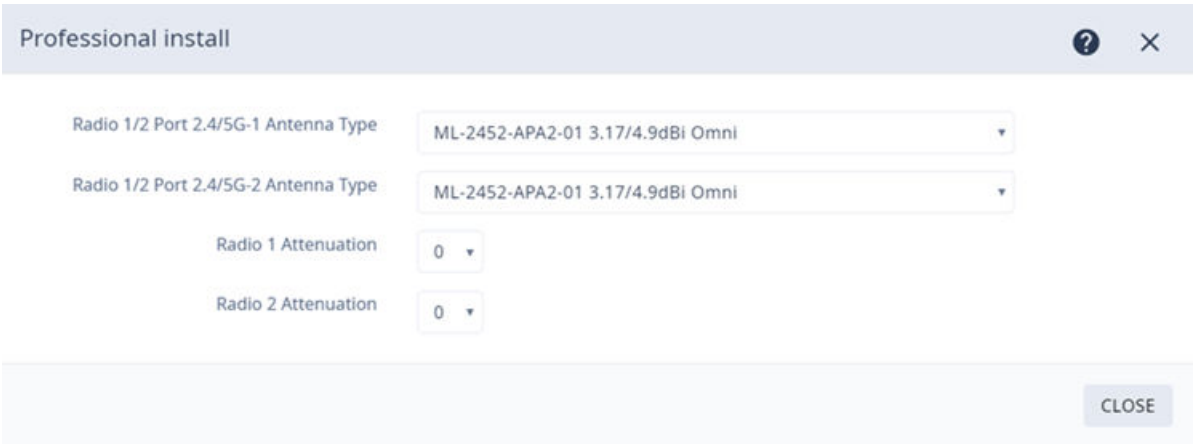


Figure 56: AP3000X Professional Install Settings

Related Topics

Add APs on page 212

AP5050D Professional Install Settings

The AP5050D is an outdoor AP that has two types of selectable, internal antenna. Select one of the following antennas:

- INTERNAL_5050D 30 degree sector
- INTERNAL_5050D 70 degree sector

Note
The AP must be part of an AP5050D device group to display the **Professional Install** dialog.

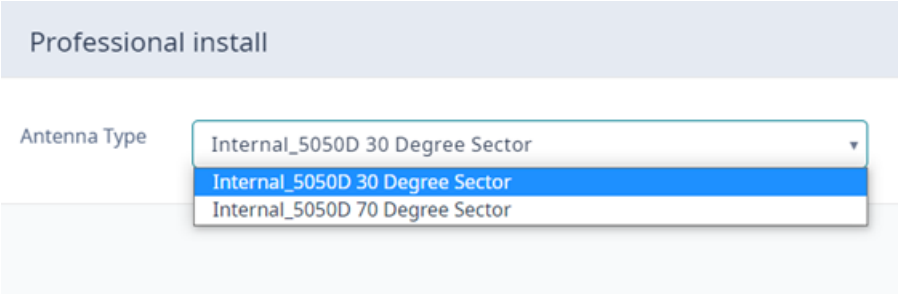


Figure 57: AP5050D Professional Install Settings

Related Topics

Add APs on page 212

Switches

ExtremeCloud IQ Controller can manage a maximum of 1000 switches.

- To configure a switch, go to **Configure** > **Devices** > **Switches**.
- For a list of supported switches, see the Release Notes.

Related Topics

Adding a Switch on page 241
Configure a Switch on page 242
Switch Actions on page 240
Switches List on page 105
RADIUS Configuration for Switches Per Site on page 131

Switch Actions

Take the following actions from the switch **Actions** button.

Table 69: Switch Actions

Field	Description
Delete	Delete the selected switch.
Reboot	Restart the selected switch.
Reset	Issues a configuration reset and reboot to the switch, resets the configuration to the initial settings.
Upgrade	Upgrade switch software. You must be an Administrator to upload the per-packaged software.
Retrieve Traces	Initiates a traces routine creating a zip file that includes switch configuration, state information, and log files. ExtremeCloud IQ Controller receives the Traces zip file and presents a download-able zip file in the Traces tab on the Monitor page for the switch. ExtremeCloud IQ Controller keeps one file and overwrites that file as subsequent files are received.
Assigned to Site	Assign selected switches to a site. **Assign to Site** dialog displays with available sites. Check one site and click **Ok**.

Related Topics

Assign Devices to Site on page 248

Understanding Switch States

The following describes switch states on the **Switches Device List**.

Table 70: Switch State from the Device List

State	Description
	In-service: • Switch acknowledges the sent configuration • Switch sends statistics every 5 minutes.
	In-Service Trouble: • Switch in process of connecting to ExtremeCloud IQ Controller • Configuration is pending acknowledgment from switch • Switch reset pending • Switch reboot pending • Switch upgrade pending

Table 70: Switch State from the Device List (continued)

State	Description
	Unknown. Switch has not discovered the ExtremeCloud IQ Controller.
	Critical: • Switch stops sending requests for 5 minutes or longer • Consistent with a loss of connectivity to ExtremeCloud IQ Controller

Adding a Switch

Access Points and Switches are automatically added to via the cloud-connector when the DHCP and DNS prerequisites have been met. You can use the Add functionality to pre-provision any AP or switch before they connect.

To add a switch to your network:

1. Per-configure your external DHCP and DNS servers on your network for discovery of the new switch. In order for the to communicate to the ExtremeCloud IQ Controller:
   - The DHCP Server (that will be serving an IP to the switch) needs to return a DNS Server and Domain Name to the switch.
   - The DNS Server needs to map the name `extremecontrol.<domain-name>` to the IP address of the ExtremeCloud IQ Controller that you plan to add the switch.
   - Confirm that the DHCP server is serving the correct DNS and domain name information.

   Note
   For full instructions on configuring DHCP, NPS, and DNS services, refer to the ExtremeCloud IQ Controller Deployment Guide

2. Go to **Configure** > **Devices** > **Switches**.
3. Select **Add** and configure the parameters.

   Note
   You can clone a switch from within a site, see Switches on page 239.

4. Configure the following parameters.

   Serial Number

   Unique number that identifies the switch. Provide this number for new and cloned switches. This number is on the switch.

   Model

   Select model number from the drop-down list. The model number is on the switch.

   Name

   Unique name for the switch. Provide a unique name.

   Description

Text description to help identify the switch.

5. Select **OK**.
6. Connect your switch to the network and power it on.

Note
The switch must be reset to factory default configuration. Refer to the switch documentation to reset your switch to factory defaults.

Related Topics

Switch Actions on page 240
Configure a Switch on page 242
Switches on page 239

Configure a Switch

The information that displays on the **Switch Configuration** page depends on the Switch Mode. By default, switches are in GUI-Mode. To configure an ExtremeXOS switch through the CLI, you can place the switch in CLI-Mode. For more information, see CLI - Mode Advanced Settings on page 247.

Note
CLI-Mode support is limited to ExtremeXOS switches.

To access the switch configuration page:

1. Go to **Configure** > **Devices** > **Switches** and select a switch (not the check box).

   For switches that are *not* in CLI-Mode, ExtremeCloud IQ Controller displays a list of ports on the **Switch Configuration** page. From the configuration page, create LAG groups and select the Admin state, Port Function, and PoE of each port.

   For each port, the following information is displayed:

   - Admin State
   - Name
   - Alias Function
   - Speed
   - Neighbor
   - LAG Members
   - PoE
2. Select one or more ports from the list. Then, set the Admin State, Port Function, and PoE options to **On** or **Off**. Select **Apply** after each selection.

Switch in CLI-Mode:

After placing an ExtremeXOS switch in CLI-Mode, the **Switch Configuration** page display is limited to the following buttons:

- **Activate Console**. Opens a remote console for a live SSH console session.
- **Backups**. Displays a list of switch configuration backup files. From this list you can view a file or restore a configuration from a backup file.

- **Create Backup**. Create a backup file of the switch configuration.
- **Advanced**. In CLI-Mode, switch advanced settings are limited to changing the switch mode. From here you can select **Change to GUI-Mode**.

Related Topics

LAG Configuration on page 243
Switch Port Configuration on page 243
Advanced Switch Settings on page 245
CLI - Mode Advanced Settings on page 247
Access the Switch CLI on page 246

LAG Configuration

To configure a Link Aggregation Group (LAG):

1. To set a Master Port, select **New LAG**.
2. Select the Master Port number from the drop-down field.

   Note
   Dialog options display for the master port after you select a port number.

3. Select a Member Port number under **Ports Eligible for LAG membership**. Then, drag the port to the **Master Port** pane.
4. Select **Save Master**.

Related Topics

Configure a Switch on page 242
Advanced Switch Settings on page 245

Switch Port Configuration

To access port configuration:

1. Go to **Configure** > **Devices** > **Switches**.
2. Select a switch.
3. Select a port in the **Name** column.

Configure the following parameters for individual switch ports:

Name

Port name.

Alias

(Optional) A user-friendly name used as an alias for the port.

Admin State

Indicates if the port is an Admin Port. Valid values are On or Off.

Function

Port function refers to the type of device the port serves. Valid values include:

- Access Point. Connects an access point. This port is part of all VLANs that are defined for all VLANs on the site.
- Interswitch. Serves as a point to point link to another switch. This port is part of all VLANs that are defined for all VLANs on the site.
- Host. Connects to a host, such as a workstation, phone, or printer.
- Other. Any other type of switch connection.

For Host and Other ports, specify the following:

- VLAN ID and PVID (port VLAN ID)
- Tagged status
- Authentication mode
- MAC-based Authentication (MBA)

Note
Configure only one untagged VLAN ID /PVID per port.

PoE Enabled

Indicates if the port is enabled for Power over Ethernet. PoE must be supported on the port.

VLANs

Select one or more configured VLANs. Click the plus sign to add the VLAN to the list.

Authentication Mode

Authentication Mode. 802.1x can be configured on individual ports. When Authentication is enabled on the switch port, this switch gets the RADIUS Authentication definition and the RADIUS servers specified under the site configuration are used.

- 802.1x
- Disabled

MAC-based Authentication (MBA)

MAC-based Authentication (MBA) option displays and is automatically enabled when Authentication mode above is **Disabled**.

When Authentication mode is disabled, MBA can be configured on individual ports. When MBA is enabled on the switch port, the switch gets the RADIUS Authentication definition and the RADIUS servers that are specified under the site configuration are used.

Related Topics

RADIUS Configuration for Switches Per Site on page 131

Advanced Switch Settings

Table 71: Advanced Switch Settings

Field	Description
Bridge Priority	Indicates the priority of the switch in a Spanning Tree network configuration to determine the Root Bridge Switch. All switches are assigned a Bridge Priority. The Bridge Priority plus the Mac Address determine the Switch ID. The lower the numerical value of the Switch ID, the more likely the switch is the Root Bridge (switch). All switches in your network can be assigned the same default Bridge Priority. If this is the case, the switch Mac Address decides which switch is the Root Bridge Switch.
IGMP Snooping	Enable snooping of Internet Group Management Protocol (IGMP) network traffic to provide a method for intelligently forwarding multicast packets within a Layer 2 broadcast domain. By snooping the IGMP registration information, the device forms a distribution list that determines which end stations receive packets with a specific multicast address. Layer 2 switches listen for IGMP messages and build mapping tables and associated forwarding filters. IGMP snooping also reduces IGMP protocol traffic. Default: Disabled
MSTP Configuration	Enable or disable MSTP configuration for the site from the Site **Switch** tab. Port MSTP configuration is set based on port function (AP, Host, Inter-switch and Other).
VLAN Configuration	VLAN configuration is based on Switch port function: • AP — All the tagged and untagged VLANS are configured for the AP's device group. • Host — Administrator configurable. The Administrator can configure any of the VLANs that are configured in the system. • Other — Default setting. Typically configures port to VLAN 1, but this is configurable for all VLAN(s) that are configured on ExtremeCloud IQ Controller. • Interswitch — All tagged and untagged VLANS are configured for all AP device groups that are serviced by the switch, along with all of the VLANS used by the host and other port types.

Table 71: Advanced Switch Settings (continued)

Field	Description
SNMP Configuration	You can configure SNMP for the individual switch or for the full ExtremeCloud IQ Controller. For more information, see SNMP Configuration on page 451.
Switch Mode	Toggle between Switch CLI-Mode and Switch GUI-Mode. • Select **Change to GUI-Mode** to provide CLI access under switch Monitoring for troubleshooting purposes. For more information, see Troubleshoot a Switch Using the CLI on page 109. • Select **Change to CLI-Mode** to provide CLI access under switch Configuration to modify the switch configuration. **Note:** The **Troubleshooting** tab and CLI access is not available under switch Monitoring when the switch is in CLI-Mode.

Related Topics

Advanced Setting Overrides on page 221
IP Address Assignment on page 230

Access the Switch CLI

ExtremeCloud IQ Controller allows access to an ExtremeXOS switch CLI for troubleshooting and manual configuration. Switch CLI access is available in two modes:

- GUI-Mode. Provided for troubleshooting using CLI Show commands.

  This is the default mode for the switch. For more information on troubleshooting an ExtremeXOS switch, see Troubleshoot a Switch Using the CLI on page 109.
- CLI-Mode. Provided for switch configuration from the command line interface.

  Access CLI-Mode from the Switch **Advanced Settings** page.

Important
Switching Between GUI and CLI Mode

- Switching to CLI-Mode *is not* service disrupting:
  - CLI script runs against the switch.
  - Cloud connector client saves switch configuration to a file.
  - ExtremeCloud IQ Controller uploads and stores the configuration file in Redis.
- Switching to GUI-Mode *is* service disrupting:
  - GUI-Mode is the default mode for a switch. When you change to CLI-Mode, and then back to GUI-Mode, the switch is reset to factory settings and configured based on the defaults for the switch model and the site configuration.

To access the switch CLI-Mode:

1. Go to **Configure** > **Devices** > **Switches** and select an ExtremeXOS switch.
2. Select **Advanced**.
3. Select **Change to CLI-Mode**.
4. Select **Activate Console**.

   A console window opens. It can take up to 60 seconds for the switch to connect.
5. When the login prompt displays, log in with your ExtremeCloud IQ Controller credentials.

Related Topics

Troubleshoot a Switch Using the CLI on page 109
Advanced Switch Settings on page 245
CLI - Mode Advanced Settings on page 247
Switch Configuration Backup Files on page 247

Switch Configuration Backup Files

When a switch is changed to CLI-mode, ExtremeCloud IQ Controller automatically creates a backup file of the switch configuration. It also provides an option to create additional configuration backup files. You can create the file, view the file within the user interface, and restore the switch configuration from a backup file.

To access the switch configuration backup files:

1. Activate CLI-Mode on an ExtremeXOS switch. For more information, see Access the Switch CLI on page 246.
2. Go to **Configure** > **Devices** > **Switches**.
3. Select an ExtremeXOS switch, then:
   - To create a backup file, select **Create Backup**.
   - To view the backup file, select **Backups** > **View**.
   - To restore a configuration from a backup file, select **Backups** > **Restore**.

Related Topics

Access the Switch CLI on page 246
Configure a Switch on page 242

CLI - Mode Advanced Settings

In CLI-Mode, switch advanced settings are limited to changing the switch mode. From here you can select **Change to GUI-Mode**.

Related Topics

Configure a Switch on page 242
Access the Switch CLI on page 246

VPN Concentrators

A VPN Concentrator is a configured connection point for use with the Generic Routing Encapsulation (GRE) point-to-point tunnel. Configure the name and IP address for each VPN Concentrator, then specify one to three concentrators in the GRE topology definition. The VPN Concentrator IP address (tunnel termination point) is specified in the VLAN definition. The VLAN specification in the configuration Profile (that is associated with the device group) determines the connection between the VPN Concentrator IPv4 address and the AP.

Related Topics

Configure VPN Concentrators on page 248
GRE Point-to-Point Tunnel on page 28

Configure VPN Concentrators

The VPN Concentrator is effectively the IPv4 address of the tunnel termination point. VPN Concentrators are used with Generic Routing Encapsulation (GRE) tunnels to offer direct point-to-point traffic flow without involving the controller. The VPN Concentrator must first be configured as a device type in ExtremeCloud IQ Controller before it can be used to define a GRE tunneled topology.

Note
In future releases, the IPv4 address will be coupled with IPSEC security options.

Take the following steps to configure a VPN Concentrator:

1. Go to **Configure** > **Devices** > **VPN Concentrators** and select **Add**.
2. Configure the following parameters:

   Name

   The VPN Concentrator name

   Description

   Optional description of the VPN Concentrator

   IP Address

   The IPv4 address of the tunnel termination point. Although each AP can support many GRE topologies, a single assigned topology supports three concentrators. IPv6 is not supported.

Related Topics

GRE Point-to-Point Tunnel on page 28
GRE Topology on page 313

Assign Devices to Site

You can assign access points, switches, and Defender adapters directly from the respective device list, which simplifies the manual onboarding process.

To add a device to a site from a device list:

1. Go to **Configure** > **Devices**.
   - To assign APs or adapters, select **Access Points**.
   - To assign switches, select **Switches**.

   ExtremeCloud IQ Controller displays a list of devices.
2. Select one or more devices, and then select **Actions** > **Assign to Site**.

   Note
   Selected APs and adapters must be the same model type.

   The **Assign to Site** dialog opens.
3. Select a site. To create a new site, select .
4. Select a device group. To create a new device group, select .

Refer to the related information for rules associated with creating sites and device groups.

Note
When working with 802.11ax access points that offer dual-mode support, make sure that the correct discovery options are configured for device adoption into the destination site. For more information, see the ExtremeCloud IQ Controller Deployment Guide.

Related Topics

Site Parameters on page 130
Device Group Parameters on page 133
Centralized Site on page 31

Networks

Roles are typically bound to topologies. Applying roles assigns user traffic to the corresponding network point of attachment, and the WLANS handles authentication and QoS for the network. Network configuration involves the following tasks:

- Defining SSID and privacy settings for the wireless link.
- Configuring the method of credential authentication for wireless users. See **AuthType** under WLAN Service Settings on page 250.

To add a network, go to **Configure** > **Networks** > **Add**.

Related Topics

WLAN Service Settings on page 250
Mesh Point Network on page 260
Mesh Point Network Settings on page 262
Hotspot on page 265
Captive Portal Settings on page 276
Associated Profiles on page 137
Advanced Network Settings on page 285

Managing a Network Service on page 290
Band Steering on page 290

WLAN Service Settings

Table 72: WLAN Service Configuration Settings

Field	Description
Network Name	Enter a unique, user-friendly value that makes sense for your business. Example: Staff
SSID	Enter a character string to identify the wireless network. Maximum 32 characters. Upper and lowercase allowed. Example: PermanentStaff
Hotspot	The following values are valid for hotspot configuration: • **Disabled**. Hotspot functionality is not enabled. Default value. • **Enabled**. Hotspots are enabled for this WLAN. ◦ Privacy is set by default to WPA. ◦ You must configure Protected Management Frame (PMF). ◦ The authentication method is set to AAA with External RADIUS Server. You can configure MBA, if required. ◦ Auth Type is WPA2-Enterprise (802.1x/EAP) ◦ You must disable the Advanced network setting **Client-Client Communication**. • **OSU**. Allows the definition of Online Sign Up or OSEN WLAN. When configuring Online Signup for the hotspot, you must configure a separate OSU WLAN. Then, specify that WLAN on the Online Signup tab. Configure the policy and topology assigned to the OSU WLAN to allow access only to the OSU server. No access to the internet. Valid Auth Type values for OSU Hotspot are: ◦ Open ◦ WPA2-Enterprise (802.1x/EAP) **Note:** You must specify a AAA policy when configuring OSU for Hotspot. **Note:** After you have defined a WLAN service with a hotspot, you cannot disable the hotspot. You can only delete the WLAN service and recreate it. For more information, see Hotspot on page 265.
Status	Enable or disable the network service. Disabling the network service shuts off the service but does not delete it.

Table 72: WLAN Service Configuration Settings (continued)

Field	Description
AuthType	Define the authorization type. Valid values are: • Open —Anyone is authorized to use the network. This authorization type has no encryption. The Default Auth role is the only supported policy role. • OWE — Opportunistic Wireless Encryption (OWE) offers security to open networks, ensuring that traffic between an AP and a client is encrypted. Other clients can sniff and record traffic, but cannot decrypt it. • WEP — Static Wired Equivalent Privacy (WEP) offers keys for a selected network, that match the WEP mechanism used on the rest of the network. Each AP can participate in up to 50 networks. Specify one WEP key per network. This option is offered to support legacy APs. See Privacy Settings for WEP on page 259. • WPA2 with PSK — Network access is allowed to any client that knows the pre-shared key (PSK). All data between the client and the AP is AES encrypted using the shared secret. Privacy is based on the IEEE standard, and privacy settings are editable. If MAC-based authentication (MBA) is enabled, you can assign different roles to different devices with a PSK because MBA distinguishes between different devices. If MBA is not enabled, then devices with a PSK use the Default Auth role only. See Privacy Settings for WPA2 with PSK on page 258. • WPA2 Enterprise w/ RADIUS — Supports 802.1X authentication with a RADIUS server, using AES encryption. This method can be used with client certificate-based authentication (EAP-TLS). All 802.1X protocols are supported. Two-stage authentication is supported offering a combination of MAC-Based (MBA) authentication and WPA2-Enterprise (802.1x/EAP). The wireless client is first authenticated using MBA and then, in stage 2, the client authenticates with WPA2-Enterprise (802.1x/EAP). **Note:** Captive Portal is not supported when using WPA2 Enterprise w/ RADIUS. An exception is *Centralized Web Authentication (CWA)*. CWA captive portal supports WPA2 Enterprise w/ RADIUS. See Privacy Settings for WPA2 Enterprise with RADIUS on page 258. • WPA3 - Personal with SAE/H2E — 128-bit encryption.WPA3 uses a pre-shared key (PSK) and Simultaneous Authentication of Equals

Table 72: WLAN Service Configuration Settings (continued)

Field	Description
	(SAE) or Hash-to-Element (H2E). WPA3 offers an augmented handshake and protection against future password compromises. See Settings for WPA3 Personal with SAE and H2E on page 256. • WPA3-Compatibility — Option for mixed deployments of 802.11ax APs and older AP models. For use when WPA2 and WPA3 are configured on the same network. Clients that support either WPA3 Personal or WPA2 Personal can connect to this network at the same time and on the same SSID. If you are unsure which method your device supports, use WPA3-Compatability. Note: When a device is assigned to 6 GHz radio, only WPA3 Personal is assigned. See Settings for WPA3 Personal with SAE and H2E on page 256. • WPA3-Enterprise — WPA2-Enterprise with Protected Management Frames (PMF). This option requires and enforces PMF enablement. The TKIP-CCMP option is disabled. For more information see, Settings for WPA3 Enterprise on page 257. • WPA3-Enterprise (192-bits) — WPA3-Enterprise with 192-bit security protocols (at a minimum) and cryptographic tools to better protect sensitive data. For more information, see WPA3-Enterprise with 192-bit mode on page 257. **Note:** The World-Wide Universal Access Points 6 GHz radios support only the following 6E WFA Compliant network authentication methods: • OWE (Opportunistic Wireless Encryption) for Open Networks • WPA3-Personal (SAE/H2E) • WPA3-Enterprise • WPA3-Enterprise 192-bit mode • WPA3-Compatibility **Note:** WPA3-Compatibility is *not* WFA compliant. WPA3-Compatibility supports both WPA2 Personal and WPA3 Personal on the same network. If a WPA3-Compatibility network is assigned to 6 GHz radio, only WPA3 Personal is assigned, thus making the network compliant. ExtremeCloud IQ Controller requires that your 6 GHz radio network assignment be 6E WFA compliant. It rejects network configuration changes that result in 6 GHz radio network assignments that are not compliant. It might be necessary to redefine your

Table 72: WLAN Service Configuration Settings (continued)

Field	Description
	networks when configuring the 6 GHz radio on the Universal Access Points. A green icon displays on the user interface when the Auth Type is 6E WFA Compliant. 
Enable Captive Portal	Check this option to enable captive portal support on the network service.
Captive Portal Type	See Captive Portal Settings on page 276.
MAC-based Authentication	The following parameter displays when MAC-based Authentication is enabled: • **MBA Timeout Role**. Select the role that will be assigned to a wireless client during MAC-based authentication (MBA) if the RADIUS server access request times out. If no MBA Timeout Role is selected, then a RADIUS server timeout is treated like an Access-Reject, which prevents the client from accessing the network. Other options: ◦ — create a new role ◦ — edit role ◦ — delete role • Two-stage authentication is supported offering a combination of MAC-Based (MBA) authentication and WPA2-Enterprise (802.1x/EAP). The wireless client is first authenticated using MBA and then, in stage 2, the client authenticates with WPA2-Enterprise (802.1x/EAP).
Authentication Method	Displayed after **Captive Portal** or **MBA** is selected. Select from the following authentication values: • Default. Select **Configure Default AAA**. • Proxy RADIUS (Failover). Configure up to 4 RADIUS servers for redundancy. • Proxy RADIUS (Load Balance). Configure up to 4 RADIUS servers for load balancing. • Local. Look up in the local password repository. • LDAP. Look up on a remote LDAP server. This option enables LDAP Configuration.

Table 72: WLAN Service Configuration Settings (continued)

Field	Description
AAA Policy	Select a AAA policy or select to add a new policy. Alternatively, you can select to edit an existing policy. To see the list of configured AAA policies, go to **Configure** > **AAA Policy**. This option is not displayed for WLAN Networks that do not require authentication or authorization. The value **Local Onboarding** refers to RADIUS requests that are directed through the ExtremeCloud IQ Controller. Local Onboarding is the default value for WLAN Networks configured for Internal Captive Portal. AAA Policy can only be configured for WLAN Networks requiring MACAUTH, External Captive Portal, or EAP. **Note:** Specify a AAA policy when configuring OSU for Hotspot.
Default AAA Authentication Method	Indicates the default authentication method that is configured when you select **Configure Default AAA**.
Primary RADIUS	IP address of primary RADIUS server.
Backup RADIUS	IP address of backup RADIUS server.
LDAP Configuration	Lightweight Directory Access Protocol. Select a configuration or select the plus sign to add a new configuration.
Authenticate Locally for MAC	Authenticate the MAC address on ExtremeCloud IQ Controller. Do not authenticate MAC address on the RADIUS server. This setting is not available when you have selected **Default** as the Authentication Method.
Default UnAuth Role	The default network policy roles for an unauthenticated client. Select a role from the list. Other options: • — create a new role • — edit selected role • — delete selected role
Default Auth Role	The default network policy roles for an authenticated client. Select a role from the list. Other options: • — create a new role • — edit selected role • — delete selected role Select the policy role as the default authentication policy role. Typically, **Enterprise User** is the Default Auth Role. You can select any of the configured roles. To configure a new role: 1. Go to **Configure** > **Policy** > **Roles**. 2. Go to **Onboard** > **Rules** and edit a policy rule, specifying **Default Auth Role** in the Accept Policy field.

Table 72: WLAN Service Configuration Settings (continued)

Field	Description
Default VLAN	The default network topology. A topology can be thought of as a VLAN (Virtual LAN) with at least one egress port, and optionally include: sets of services, exception filters, and multicast filters. Examples of supported topology modes are Bridged at AP and Bridged at AC. Select a VLAN from the list. Other options: • — create a new VLAN • — edit selected VLAN • — delete selected VLAN
Scheduling	**Note:** Scheduling is unavailable until you install and run Scheduler for ExtremeCloud IQ Controller. Select **Scheduling** to open the Scheduler application. This is a Docker application that resides on ExtremeCloud IQ Controller. Download Scheduler for ExtremeCloud IQ Controller from the Extreme Networks support portal, and install the application.

Related Topics

Advanced Network Settings on page 285
Scheduler for ExtremeCloud IQ Controller on page 471
REST API Access for Docker Container Applications on page 473
Captive Portal Settings on page 276
LDAP Configurations on page 338
Add Policy Roles on page 292
Configure AAA Policy on page 327
Configuring VLANS on page 303
Hotspot on page 265
Mesh Point Network Settings on page 262
Associated Profiles on page 137

Privacy Settings WPA3

WPA3™ is an increased level of network security certified by the Wi-Fi Alliance®. WPA3 provides security protocols that enhance and simplify Wi-Fi security. All WPA3 networks:

- Use the latest security methods
- Bar outdated legacy protocols
- Require use of Protected Management Frames (PMF).

WPA3 offers different versions and levels of security:

WPA3-Personal with SAE and H2E

Intended for individual users providing robust, password-based authentication that is enabled through Simultaneous Authentication of Equals (SAE) or Hash-to-Element (H2E). Delivering better protection, it allows users to choose passwords that are easy to remember, and it can protect data after a password is compromised and data is sent.

Note
ExtremeCloud IQ Controller supports both SAE and H2E on 2.4 GHz and 5 GHz radios. For 6 GHz radios, we only support H2E.

WPA3-Enterprise

WPA3-Enterprise extends WPA2-Enterprise adding Protected Management Frames on all WPA3 connections.

WPA3-Enterprise with 192-bit mode

WPA3-Enterprise with 192-bit security protocols (at a minimum) and cryptographic tools to better protect sensitive data.

Related Topics

Settings for WPA3 Personal with SAE and H2E on page 256
Settings for WPA3 Enterprise on page 257
WPA3-Enterprise with 192-bit mode on page 257
Privacy Settings for WPA2 Enterprise with RADIUS on page 258
WLAN Service Settings on page 250

Settings for WPA3 Personal with SAE and H2E

WPA3 Personal with SAE and H2E— Network access is allowed to any client that knows the pre-shared key (PSK).

Note
ExtremeCloud IQ Controller supports both SAE and H2E on 2.4 GHz and 5 GHz radios. For 6 GHz radios, we only support H2E.

Configure the following privacy settings:

- Protected Management Frames — Management Frames are the signaling packets used in the 802.11 wireless standard to allow a device to negotiate with an AP. PMF adds an integrity check to control packets being sent between the client and the access point. Valid values are:
  - WPA3 - Personal (SAE and H2E). Setting is **Required**. Requires that all devices use PMF format. This could result in older devices not connecting.
  - WPA3 - Compatibility:
    - **Enabled**. Supports PMF format but does not require it.
    - **Required**. Requires PMF format.
- Input Method. Enter the PSK in String or HEX:
  - String value — Supports a PSK of 1-63 characters
  - HEX value — Supports a PSK of exactly 64 characters and must contain HEX digits only.

- WPA3 Key. The password to access this wireless network. Select **Mask** to prevent the password characters from displaying.

Related Topics

Privacy Settings WPA3 on page 255
WLAN Service Settings on page 250

Settings for WPA3 Enterprise

WPA3 Enterprise 802.1x/EAP — Requires Protected Management Frames (PMF) enabled. For a network with WPA3-Enterprise authentication, PMF cannot be disabled. Network access is allowed to any client that knows the pre-shared key (PSK).

Note
6E WPA Compliance (WPA3)

Configure the following privacy settings:

- Fast Transition — Provides faster roaming by authenticating the device before roaming occurs. This setting is enabled by default.
- Mobility Domain ID — Used by 802.11r, this setting defines a network scope that supports 11r fast roaming. Master keys are shared within the Mobility Domain, allowing clients to support fast roaming.

ExtremeCloud IQ Controller also supports WPA3-Enterprise with 192-bit mode.

Related Topics

Privacy Settings WPA3 on page 255
WPA3-Enterprise with 192-bit mode on page 257
Settings for WPA3 Personal with SAE and H2E on page 256
WLAN Service Settings on page 250

WPA3-Enterprise with 192-bit mode

WPA3-Enterprise with 192-bit security protocols offers better protection for sensitive data. ExtremeCloud IQ Controller treats 192-bit mode configuration like WPA3-Enterprise (802.1X/EAP), offering the same configuration options with the following added restrictions. WPA3-Enterprise with 192-bit security:

- Is supported on AP5010 only. Network assignment is restricted to profiles of supporting devices.

  Note
  Future AP model releases will also support 192-bit security.

- Is supported for External RADIUS implementations only. Local onboarding is not supported.
- Does not support Client Bridge. Client bridge configuration will be supported in a future release.
- Does not support Hotspot 2.0.
- Does not support configuration of Fast Transition and Mobility Domain ID.

Related Topics

Privacy Settings WPA3 on page 255
Settings for WPA3 Enterprise on page 257
Settings for WPA3 Personal with SAE and H2E on page 256
WLAN Service Settings on page 250

Privacy Settings WPA2

ExtremeCloud IQ Controller supports WPA2 security protocols.

Related Topics

Privacy Settings for WPA2 with PSK on page 258
Privacy Settings for WPA2 Enterprise with RADIUS on page 258

Privacy Settings for WPA2 with PSK

WPA2 with PSK — Network access is allowed to any client that knows the pre-shared key (PSK).

Configure the following privacy settings:

- TKIP-CCMP — Select this option to use Temporal Key Integrity Protocol (TKIP) and Counter Mode with Cipher Block Chaining Message Authentication Code Protocol (CCMP). **Best Practice:** TKIP encryption is considered to be a less secure means of communication. An industry best practice is to use a more secure option for network privacy.
- Protected Management Frames — Management Frames are the signaling packets used in the 802.11 wireless standard to allow a device to negotiate with an AP. PMF adds an integrity check to control packets being sent between the client and the access point. Valid values are:
  - Enabled. Supports PMF format but does not require it.
  - Disabled. Does not address PMF format. Clients connect regardless of format.
  - Required. Requires all devices use PMF format. This could result in older devices not connecting.

  PMF is enabled by default.
- Input Method. Enter the PSK in String or HEX:
  - String value — Supports a PSK of 1-63 characters
  - HEX value — Supports a PSK of exactly 64 characters and must contain HEX digits only.
- WPA2Key. The password to access this wireless network.

Related Topics

WLAN Service Settings on page 250

Privacy Settings for WPA2 Enterprise with RADIUS

WPA2 Enterprise w/ RADIUS — Supports 802.1X authentication with a RADIUS server, using AES encryption. This level of network security can be used in conjunction with client certificate-based authentication (EAP-TLS). All 802.1X protocols are supported.

Two-stage authentication is supported offering a combination of MAC-Based (MBA) authentication and WPA2-Enterprise (802.1x/EAP). The wireless client is first authenticated using MBA and then, in stage 2, the client authenticates with WPA2-Enterprise (802.1x/EAP).The wireless client is first authenticated using MBA and then, in stage 2, the client authenticates with WPA2-Enterprise (802.1x/EAP). Wireless devices must pass both MBA and WPA2-Enterprise before they are allowed access to the network. After passing 2-staged authentication, the wireless client is fully authenticated and assigned a policy role as provisioned by the administrator. If either part of the two-staged authentication process fails, the client is disconnected from the network, and the client must attempt MBA authentication again.

Note
Captive Portal is not supported when using WPA2 Enterprise w/ RADIUS. An exception is *Centralized Web Authentication (CWA)*. CWA captive portal supports WPA2 Enterprise w/ RADIUS.

Configure the following privacy settings:

- TKIP-CCMP — Select this option to use Temporal Key Integrity Protocol (TKIP) and Counter Mode with Cipher Block Chaining Message Authentication Code Protocol (CCMP). **Best Practice:** TKIP encryption is considered to be a less secure means of communication. An industry best practice is to use a more secure option for network privacy.
- Protected Management Frames — Management Frames are the signaling packets used in the 802.11 wireless standard to allow a device to negotiate with an AP. PMF adds an integrity check to control packets being sent between the client and the access point. Valid values are:
  - Enabled. Supports PMF format but does not require it.
  - Disabled. Does not address PMF format. Clients connect regardless of format.
  - Required. Requires all devices use PMF format. This could result in older devices not connecting.

  PMF is enabled by default.
- Fast Transition — Provides faster roaming by authenticating the device before roaming occurs. This setting is enabled by default.
- Mobility Domain ID — Used by 802.11r, this setting defines a network scope that supports 11r fast roaming. Master keys are shared within the Mobility Domain, allowing clients to support fast roaming.

Related Topics

WLAN Service Settings on page 250

Privacy Settings for WEP

Important
Always use a restrictive policy to the associated VLAN to reduce your exposure after a breach.

Static WEP (Wired Equivalent Privacy) uses keys for a selected network, that match the WEP mechanism used on the rest of the network. Each AP can participate in up to 50 networks. Specify one WEP key per network.

Note
This option is offered to support legacy APs.

Configure the following privacy settings for a WLAN network:

- WEP Key Length — Select the WEP encryption key length. Valid values are: 64-bit and 128- bit.
- Input Methods — Select one of the following input methods:
  - Input Hex — If you select **Hex**, type the WEP key input in the WEP Key box. The key is generated automatically, based on the input.
  - Input String — If you select **String**, type the secret WEP Key string used for encrypting and decrypting in the WEP Key box.
- Key Index — Select the WEP encryption key index. Valid values are 1 to 4.
- WEP Key — Type the WEP key using the **Input Method** chosen above.

Related Topics

WLAN Service Settings on page 250
Mesh Point Network Settings on page 262

Mesh Point Network

An access point can be configured to be a part of a mesh network. In a mesh network, nodes in the network can communicate with each other, and each node can maintain more than one path to its peers. Mesh networking enables users to access broadband applications anywhere by providing robust, reliable, and redundant connectivity to all the members of the network. When one of the nodes in a mesh network becomes unavailable, the other nodes in the network can still communicate with each other directly or through intermediate nodes.

Mesh provides efficient routing and path changes in infrastructure and mobility modes by proactively maintaining a table of alternative paths to mesh point root APs. Alternative paths allow root APs the flexibility to change paths immediately when a better path becomes available. This proactive approach allows a mesh AP to make intelligent path decisions in a dynamically changing RF environment.

Consider the following about a mesh network:

- The Mesh APs use wireless beacons to advertise their capabilities. Mesh APs connect to each other using the information in the beacons. A single mesh point is supported on multiple radios for a single AP.
- Mesh points forward all traffic into the wired network through mesh point root APs. A root AP is an AP connected to the wired network. Mesh points find the optimum path to a mesh point root AP.
- With Monitor Primary Port Link enabled, if a root AP loses connection to the backhaul, the non-root APs scan for a new root AP and the original root performs service as a non-root AP. When the original root AP restores connectivity, it resumes

the role of root AP. Through the use of Automatic Channel Selection (ACS), the optimum path is restored.

- The path between any two APs is one hop. The path to a mesh point root can consist of multiple hops. In a mesh point network, APs automatically determine the best path to each mesh point root AP. A single hop path is not necessarily better than a path with multiple hops.
- A mesh network is self-healing. The network reforms when an AP fails, preventing a single point of failure.
- Both bridged WLAN services and tunneled WLAN services are supported.

Note
Do not rename an AP after it is added to a mesh network. Renaming the device affects the display of the reported statistics.

To create a mesh network:

1. Configure a Mesh Point Network.
2. Create a device group and configuration Profile for the root AP and a second device group and configuration Profile for the non-root APs.
3. From the device group configuration Profile:
   - Specify the Mesh Point Network.
   - Specify Advanced configuration Profile settings.
   - Specify the Mesh Device Settings.

Note
The access points are limited to one mesh point. Multiple radios can be configured for a single mesh point.

Note
Mesh Point is supported on ExtremeWireless AP39xx, Wi-Fi 6 AP models. The mesh network must contain only AP39xx access points or only Wi-Fi 6 access points. You cannot combine the AP39xx platform with the Wi-Fi 6 access point platforms in a single mesh network.

Initially, configure non-root APs over wired Ethernet, connected to the Management Port. After adding an AP to a non-root mesh device group, the AP will reboot and then it will be a member of the group without the Ethernet network. (It is highly recommended to disconnect the Management Ethernet port at this time.) If you need to modify the configuration of a non-root AP after deploying in a mesh network, reconnect the AP through the Management Ethernet port and verify mesh point configuration. When a non-root AP is incorrectly configured in a mesh network, it can become stranded. To recover a stranded AP, reconnect to the Management Port through the wired Ethernet.

Note
Mesh device settings are supported at the Profile level or configured as an override for a specific AP.

Related Topics

Configure a Mesh Point Network on page 262
Mesh Point Network Settings on page 262
Advanced Configuration and Mesh Device Settings on page 139
Mesh Point Network Diagram on page 111
Advanced Setting Overrides on page 221

Configure a Mesh Point Network

1. Configure the mesh point.
   Go to **Configure** > **Networks** > **Mesh Points** > **Add** and configure the Mesh Point Network Settings.
2. Associate the mesh point network with the device group configuration Profile.
   a. Go to **Sites**, and select a site.
   b. Select the **Device Groups** tab, and select a specific device group.
   c. Next to the **Profile** field, select .
   d. Select the **Mesh Points** tab, and select the mesh point network for a single radio.

   Note
   The access points are limited to one mesh point. Multiple radios can be configured for a single mesh point.

3. Select **Advanced** and configure the **Mesh Device Settings** in the configuration Profile. See Advanced Configuration and Mesh Device Settings on page 139.

Note
Mesh device settings are supported at the Profile level or configured as an override for a specific AP.

Related Topics

Mesh Point Network on page 260
Mesh Point Network Settings on page 262
Mesh Point Network Diagram on page 111
Mesh Point Profile Configuration on page 138
Advanced Configuration and Mesh Device Settings on page 139
Advanced Setting Overrides on page 221

Mesh Point Network Settings

To configure a mesh point network, do the following:

1. Go to **Configure** > **Networks** > **Mesh Points** > **Add**.
2. Configure the following parameters:

Mesh Point Name

Name that identifies the mesh point.

Mesh ID

Identifies the mesh network. APs must have the same Mesh ID in order to form mesh links. APs with configured mesh points exchange beacons and the Mesh

ID is checked. If a Mesh ID does not match that of the network, the beacon is dropped. If the Mesh ID does match that of the network, the AP adds an entry in the Mesh Point Neighbor Table.

The SSID is used as the Mesh ID for networks that support AP39xx access points.

Auth Type

A pre-shared key (PSK) is used to AES encrypt traffic traveling between Mesh Point APs. Modifying the key after a non-root AP is deployed may cause it to become stranded. Connect the non-root AP through the Ethernet port before changing the PSK.

Select **Edit Privacy** to enter the WPA2 key.

Related Topics

Mesh Point Network on page 260
Configure a Mesh Point Network on page 262
Advanced Configuration and Mesh Device Settings on page 139
Mesh Point Network Diagram on page 111

Transparent Bridge

A Transparent Bridge enables you to expand the wireless network by interconnecting the wireless APs through wireless links in addition to the traditional method of interconnecting APs via a wired network. A Transparent Bridge deployment is ideally suited for locations where installing Ethernet cabling is too expensive or physically impossible. Transparent Bridge:

- Enables connectivity over a mesh network without requiring policy enforcement.
- Carries VLAN tagged traffic between two areas of connection: trunk ingress-trunk egress.
- Typically used for point-to-point links.

To configure Transparent Bridge:

1. Configure a Mesh Point Network.
2. Configure two device groups: One device group for the Root AP and one device group for non-root APs.
3. From the non-root AP device group, configure the GE2 Port Function:
   a. Select **Advanced** to view Advanced Profile settings.
   b. From the GE2 Port Function field, select **Bridge**.

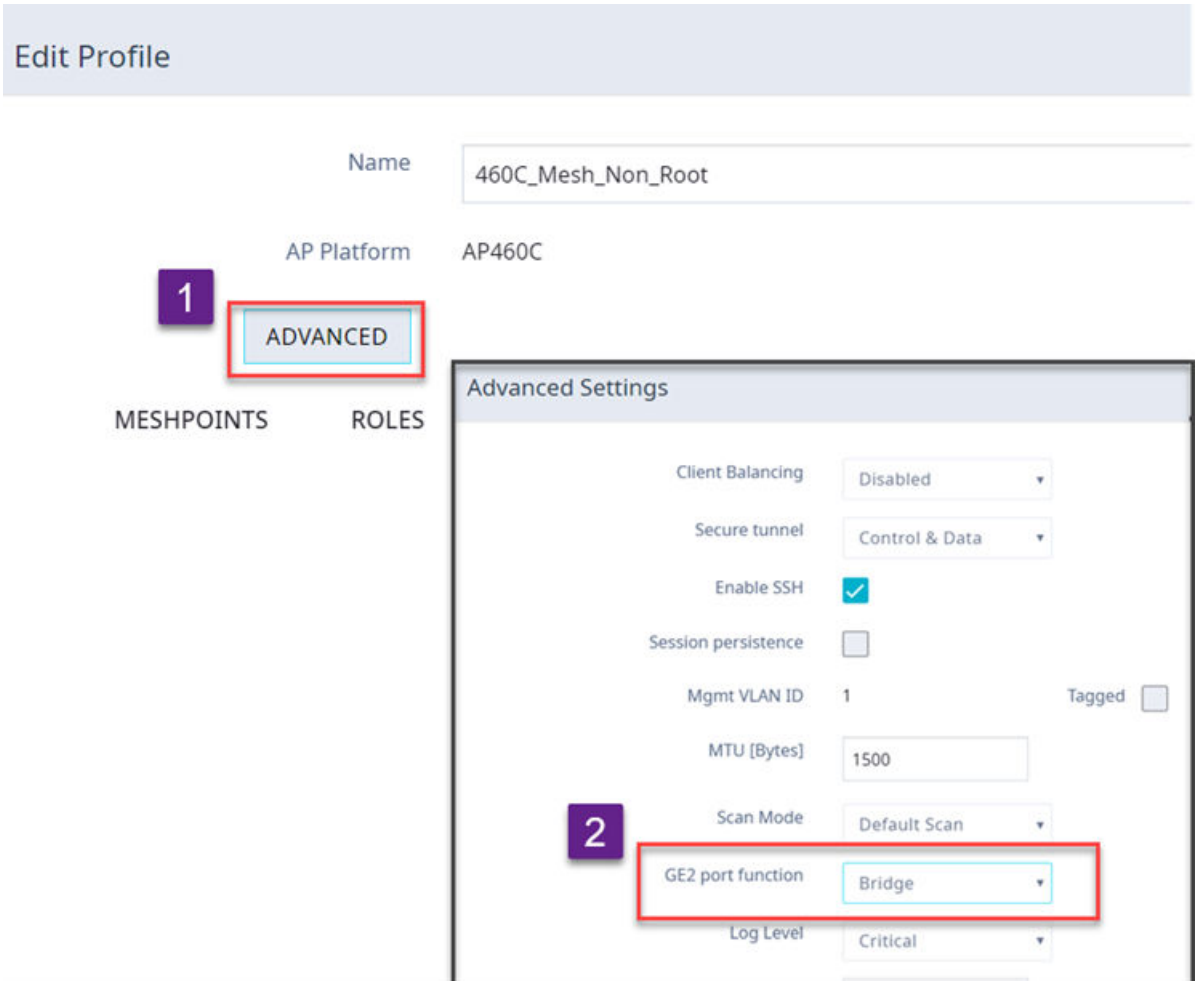


Figure 58: Configure Transparent Bridge from Device Group Configuration Profile

Note

Transparent Bridge provides a mesh link between two sites without requiring policy enforcement per device. Network policy and VLAN are not configured, and the **GE2 Port** field on the device group configuration Profile Networks tab is not displayed.

The ETH1/GE2 Bridge port is *not* supported on access points with a single Ethernet port.

You can configure Transparent Bridge for all APs in a device group and you can override settings for one or more individual APs from the AP **Advance Settings** > **Override** dialog.

Related Topics

Configure a Mesh Point Network on page 262
Mesh Point Network Settings on page 262

Hotspot

ExtremeCloud IQ Controller supports the definition of Hotspot 2.0 service for AP39xx and Wi-Fi 6 access points deployed in a Centralized site.

Traditionally, using a hotspot presents end users with several challenges, including initial connection issues, security concerns, and connectivity while roaming. Hotspot 2.0 offers the following features to improve the hotspot end-user experience:

- Pre-association network discovery and selection using the dot11u ANQP protocol, resulting in a seamless initial connection.
- Simplified account registration. Network administrators create accounts easily, and provisioning is achieved without user input.
- Enhanced security, using over the air transmission secured by WPA2.

Each hotspot WLAN has its own Access Network Query Protocol (ANQP) configuration. The HESSID and ANQP Domain ID are specific to the hotspot WLAN.

With pre-association, a mobile device uses ANQP to perform network discovery. The mobile device's connection manager uses hotspot information, such as the service provider policy and user preferences, to automatically select a hotspot network. A mobile device queries the hotspot for key service provider identification and authentication information and selects a network. The ANQP response is generated using parameters configured by the hotspot operator.

Only one hotspot WLAN can be assigned to an AP and to a specific Profile configuration. The hotspot WLAN can refer to a single Online Signup (OSU) WLAN, which can be open or encrypted. Network operators define the filter policy during hotspot configuration.

Related Topics

Configure Hotspot on page 265

Configure Hotspot

To configure a hotspot:

1. Go to **Configure** > **Network** > **WLAN Services** > **Add**.
2. From the Hotspot field, select **Enable**.
   The **Configure** button displays.
3. Select **Configure**.
4. Configure the following settings:

   HESSID

   One SSID can be used across multiple WLANs (BSS), so the HESSID helps a client identify when the BSSID belongs to a homogenous BSS with identical configuration. Beacon with same {HESSID, SSID} pair belong to same WLAN. The {HESSID, SSID} pair must be unique for each WLAN. By default, the HESSID is set to the MAC address of the controller Ethernet port. Hotspots can have the same HESSID as long as the SSID is unique. If opting to configure the HESSID manually, we recommend using an AP BSSID as the HESSID. In a mobility domain, manually configure the HESSID to a unique value, differentiating it from the value used in the controller's WLAN.

Access Network

Identifies the type of network. Valid values are:

- Private network. An enterprise network with user accounts.
- Private network with guest access. An enterprise network providing guest access.
- Chargeable public network. (Default) Open to anyone but access requires payment.
- Free public network. Open network, free of charge but may still require acceptance of terms of use (and may involve OSU servers with captive portal).

DGAF Disabled

Downstream Group-Address Forwarding Disabled. By default this option is checked. When checked, the AP is not forwarding downstream group-addressed frames.

Select each tab to complete the hotspot configuration.

Note
All required fields on the selected tab must be filled out before you can select **OK** to save the configuration.

Related Topics

Hotspot Identification on page 266
SP Identification on page 267
Network Characteristics on page 271
Online Signup on page 272

Hotspot Identification

From the **Hotspot Identification** tab, configure the following parameters:

Domain

FQDN specified by the user. Default value is empty string. This is a list of one or more domain names of the entity operating the hotspot network. Domain names in the domain name list may contain sub-domains. If the service provider's FQDN is not in the domain name list but is in the realm list, then a mobile device that chooses that service provider is considered to be roaming.

Venue Info

Describes the venue. Select from a list of predefined values:

1. In the first field, select a description of the venue group.
2. In the second field, select a value. The second field is not populated with values until after you select a value from the first field. The default value is **Unspecified**.
3. Select **New** to configure:
   - Operator Name
   - Venue Name

- Language

Note
Configure up to four languages for each venue.

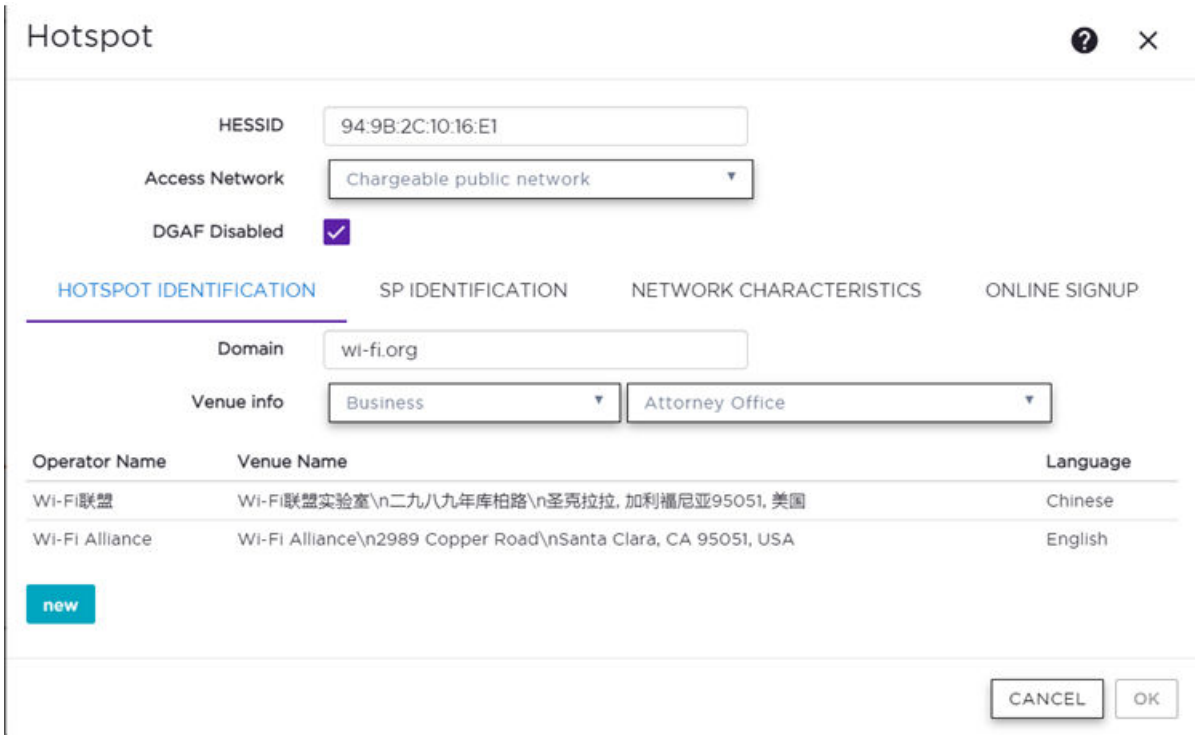


Figure 59: Hotspot Identification Tab

Related Topics

Configure Hotspot on page 265
SP Identification on page 267
Network Characteristics on page 271
Online Signup on page 272

SP Identification

The hotspot SP Identification tab displays hotspot properties for service provider identification and authentication.

To configure SP Identification for the hotspot:

1. Configure a WLAN Services Hotspot. For more information, see Configure Hotspot on page 265.

2. Select the **SP Identification** tab.

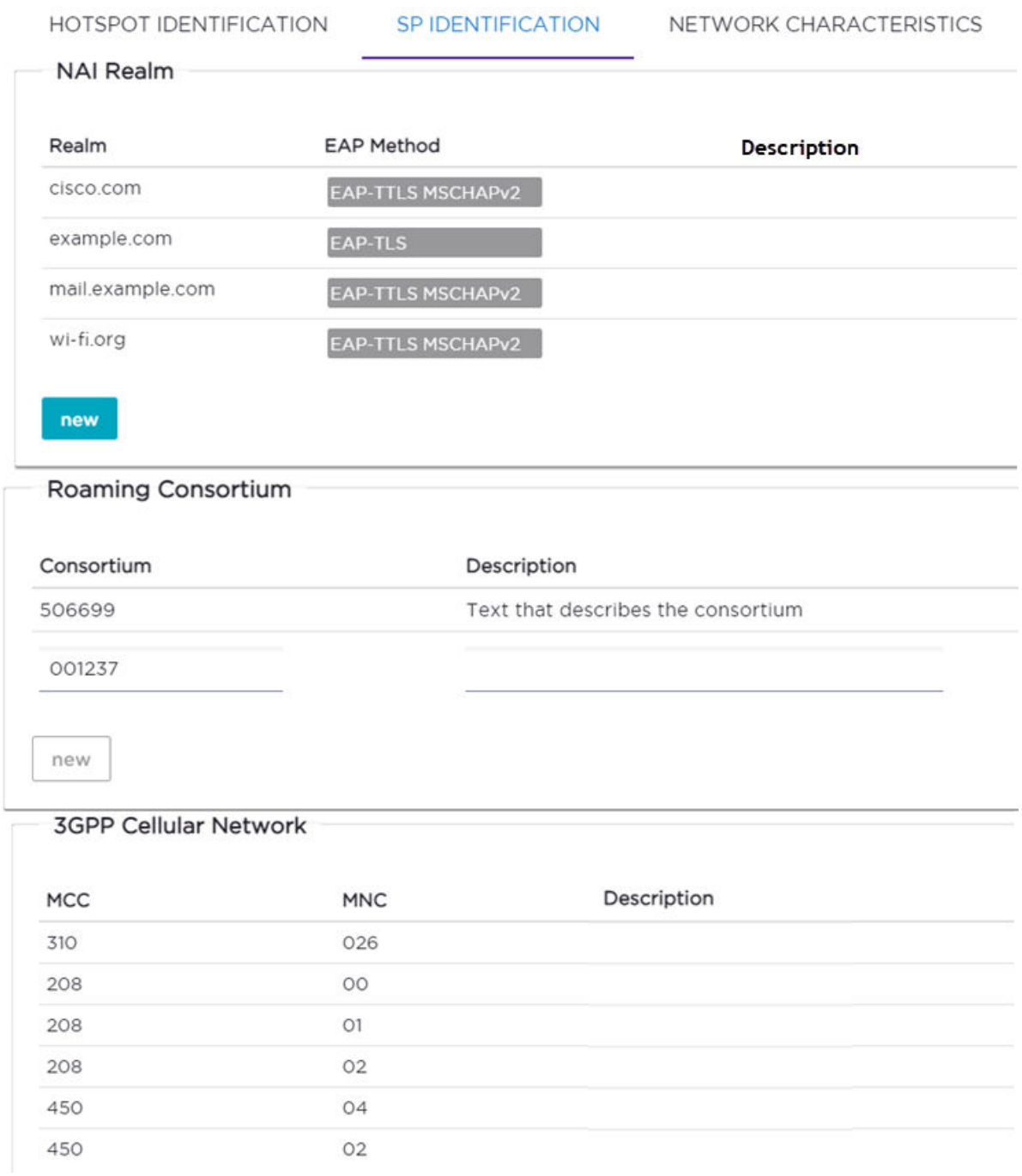


Figure 60: Service Provider Identification

3. Configure the following parameters:

   Realm. The NAI (Network Access Identification) Realms list is a FQDN (Fully-Qualified Domain Name) of the service provider. This is a list of realms that can be successfully authenticated. Each realm may have up to four supported EAP methods.

   Note
   Wildcards are supported. For example, for realm, you can enter `*.extreme.area120.com`, instead of entering specific realms.

   To add realms:

   a. Select **New**.
   b. Enter a value in the **Realm** field. The NAI Realm is a FQDN of the service provider.
   c. Select the EAP Method.

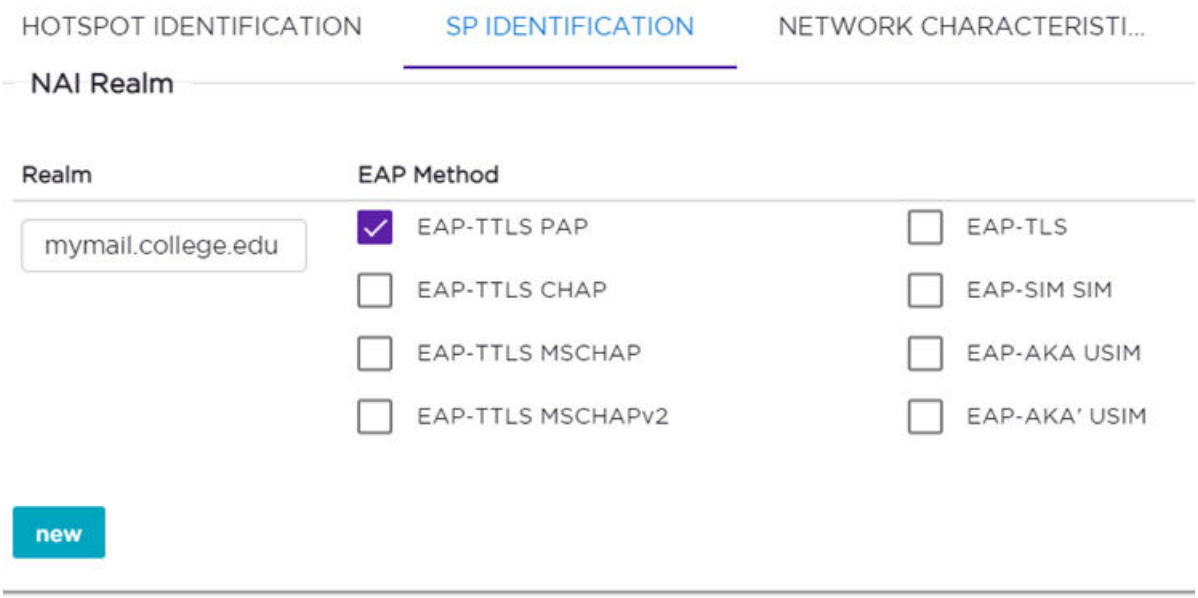


Figure 61: Realm Configuration

Configure an NAI Realm list for each hotspot as follows:

- Add all realms that can authenticate the logon credentials or certificate credentials of a mobile device, including the realms of all roaming partners that are accessible from the hotspot AP. Include the realm of the home SP.
- Add a realm for the PLMN ID. This is the cellular network identity based on public land mobile network (PLMN) information.
- You can configure the EAP method list to support devices that do not know the EAP methods that are being used by a given service provider.

If the device has been provisioned with the home service provider, the device does not need to use the EAP methods in the NAI Realm List. The mobile device knows

the EAP method required to authenticate against its home service provider and automatically uses it.

Note
Keep your DNS server records up to date so that mobile devices can resolve the server domain names (FQDN).

Mobile devices with a SIM or USIM credential, can obtain a realm from the hotspot NAI Realm list. While 3GPP credentials are usually used to access a hotspot, a targeted NAI home query is an efficient alternative approach. The device's connection manager compares the realm information in the list to the information that is stored on the device. The connection manager uses the mobile device's pre-configured user preferences and policy to make a decision between a hotspot AP or a non-hotspot AP, if both are available.

Roaming Consortium. Configure authentication of mobile devices to the members of a roaming consortium, or for a particular service provider that has a roaming consortium. Add the appropriate **IEEE-assigned Organizational Identifier (OI)**. Specify up to eight identifiers unique to the organization that are part of the MAC address.

Note
The order of the roaming consortium definition is important and it is preserved during configuration changes and system upgrade. The AP39xx access points continue to support only two identifiers. The AP39xx receives the first two identifiers in the list.

Use roaming consortium authentication when you do not know all the authenticated realms. Using identifiers unique to the organization in the beacon is a battery efficient roaming method because there are no ANQP queries needed.

3GPP Cellular Network. This is a list of cellular network IDs in the form of mobile country code (MCC), mobile network code (MNC). This list establishes whether an AP has a roaming arrangement with the 3GPP service providers.

a. Select **New** to expand the **3GPP Cellular Network** pane.
b. Enter the MCC and MNC values.
c. Provide an optional description. The **Description** field supports up to 32 bytes and UTF-8 format.

Note
The **New** button remains unavailable until valid values are entered in both fields.

d. Select **New** to accept the entered values and open a new row.

4. After you have finished configuring the **SP Identification** tab, select **OK** to save the configuration.

Related Topics

Configure Hotspot on page 265
Hotspot Identification on page 266

Network Characteristics

The hotspot Network Characteristics tab displays network parameters for the hotspot.

To configure Network Characteristics for the hotspot:

1. Configure a WLAN Services Hotspot. For more information, see Configure Hotspot on page 265.
2. Select the **Network Characteristics** tab.

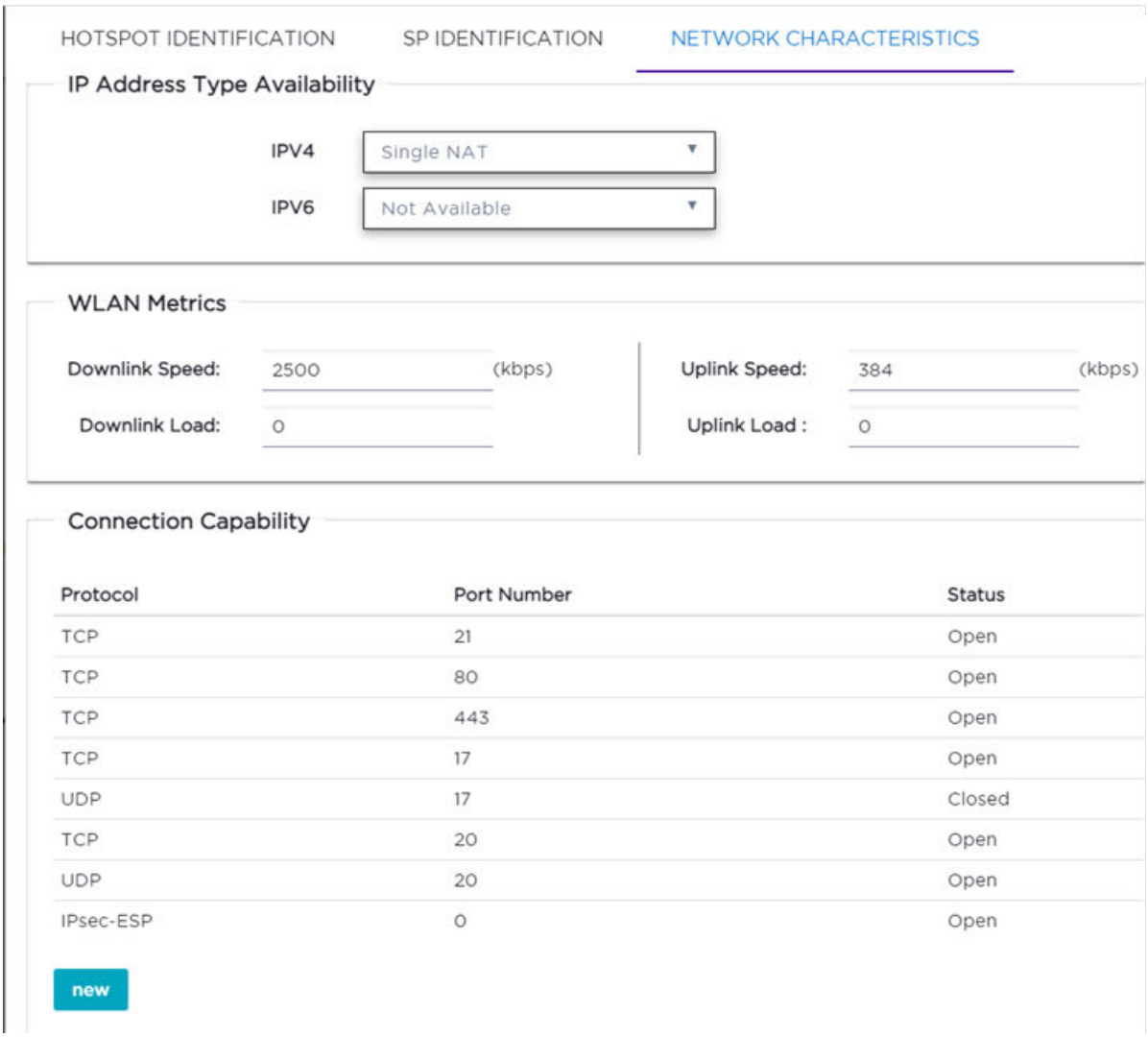


Figure 62: Configuring Network Characteristics

3. Configure the following parameters:

   IP Address Type Availability. The mobile device uses the IP Address Type Availability information to make network selection decisions. Select the level of restriction for each network type.

IPV4 valid values are:

- Not Available
- Public
- Port Restricted
- Single NAT
- Double NAT
- Port Restricted Single NAT
- Port Restricted Double NAT
- Unknown

IPV6 valid values are:

- Not Available
- Available
- Unknown

WLAN Metrics. Enter the values for maximum Uplink and Downlink speed and load parameters for the WLAN service.

The mobile device uses information from the WAN Metrics configured here to make network selection decisions. The mobile device can determine if necessary throughput is available from the hotspot before connecting. If the mobile device receives indication that the basic service set (BSS) is at capacity, the device will not associate with that AP.

Connection Capability. The mobile device uses connection capability information to make network selection decisions by determining which services are blocked or supported at the hotspot. Configure up to 16 ports.

- To add a protocol, select **New**. Select the protocol, the port number, and the status associated with the protocol. Valid status values include: Closed, Open, or Unknown.

  Note
  Make an effort to configure all ports and do not rely on the Unknown value.

4. After you have finished configuring the **Network Characteristics** tab, select **OK** to save the configuration.

Related Topics

Configure Hotspot on page 265
Hotspot Identification on page 266
SP Identification on page 267
Online Signup on page 272

Online Signup

The hotspot **Online Signup** tab displays hotspot properties for Online Signup (OSU) users. Online Signup allows users who are not part of the provider network to manually

connect to the hotspot. It also allows for added security for users who want to connect anonymously. To configure Online Signup, you must configure a separate WLAN for OSU with Open Authentication or WPA2-Enterprise (802.1x/EAP). Encryption is specific to the service provider. Credentials in the mobile device SIM Card authenticate the user.

To configure the OSU WLAN that you will specify on the **Online Signup** tab:

1. Go to **Configure** > **Network** > **WLAN Settings**.
2. From the Hotspot field, select **OSU**.
3. From the Auth Type field, select **Open** or **WPA2-Enterprise (802.1x/EAP)**.

Note
You must specify a AAA policy when configuring OSU for Hotspot.

Note
You will specify this OSU WLAN in the Online Signup configuration.

To configure Online Signup for the hotspot:

1. Configure a WLAN Services Hotspot. For more information, see Configure Hotspot on page 265.
2. Select the **Online Signup** tab.

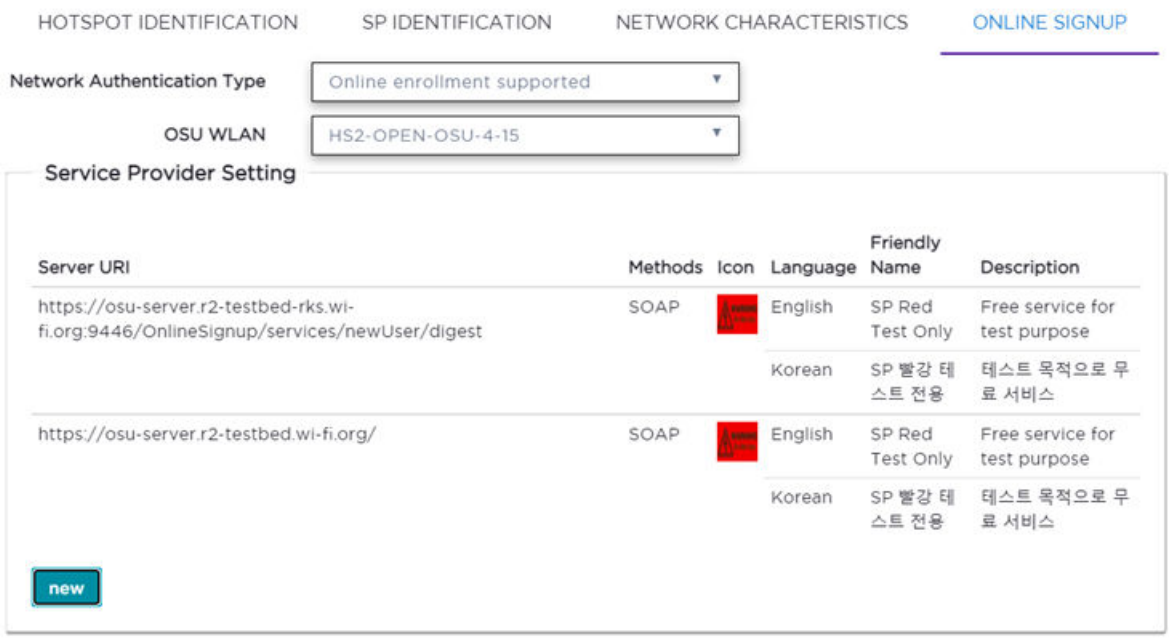


Figure 63: Configuring Online Signup

3. Configure the following parameters:

   Network Authentication Type. Possible values for network authentication are:

   - Acceptance of terms and conditions. Redirection is accomplished after user accepts Terms and Conditions.
   - Http/Https redirection. Redirect Http or Https automatically. Provide the Redirection URL.
   - Online enrollment supported. Authentication supports online enrollment. Service Provider configuration pane displays.
   - DNS redirection. DNS redirection serves a web page other than what the end user had requested.

   OSU WLAN. This is the address of the Online Signup WLAN. Create this WLAN separately. The Auth Type for the OSU WLAN can be either Open or WPA2 Enterprise. Encrypted Authentication is specific to the Service Provider. Network Authentication is available in the SIM Card of the mobile device.

   Server Provider Setting. This is service provider configuration settings.

   - To add a provider to the list, select **New** and configure the provider settings. For more information, see Configuring the OSU Service Provider on page 274.
   - To remove a provider from the list, select the list row, then select  .
   - To edit provider information, select the list row, then select  . For more information, see Configuring the OSU Service Provider on page 274.
4. Select **OK** to save the Online Signup configuration.

Related Topics

Configuring the OSU Service Provider on page 274
Configure Hotspot on page 265

Configuring the OSU Service Provider

Hotspot configuration supports Online Signup. This task outlines how to create a list of service providers that support Online Signup.

Take the following steps to configure an Online Signup service provider:

1. Configure a WLAN Services Hotspot. For more information, see Configure Hotspot on page 265.
2. From the WLAN Services Hotspot tab, select the **Online Signup** tab.

3. In the Service Provider Setting pane, select **New**.
   The **OSU SP Configuration** dialog opens.

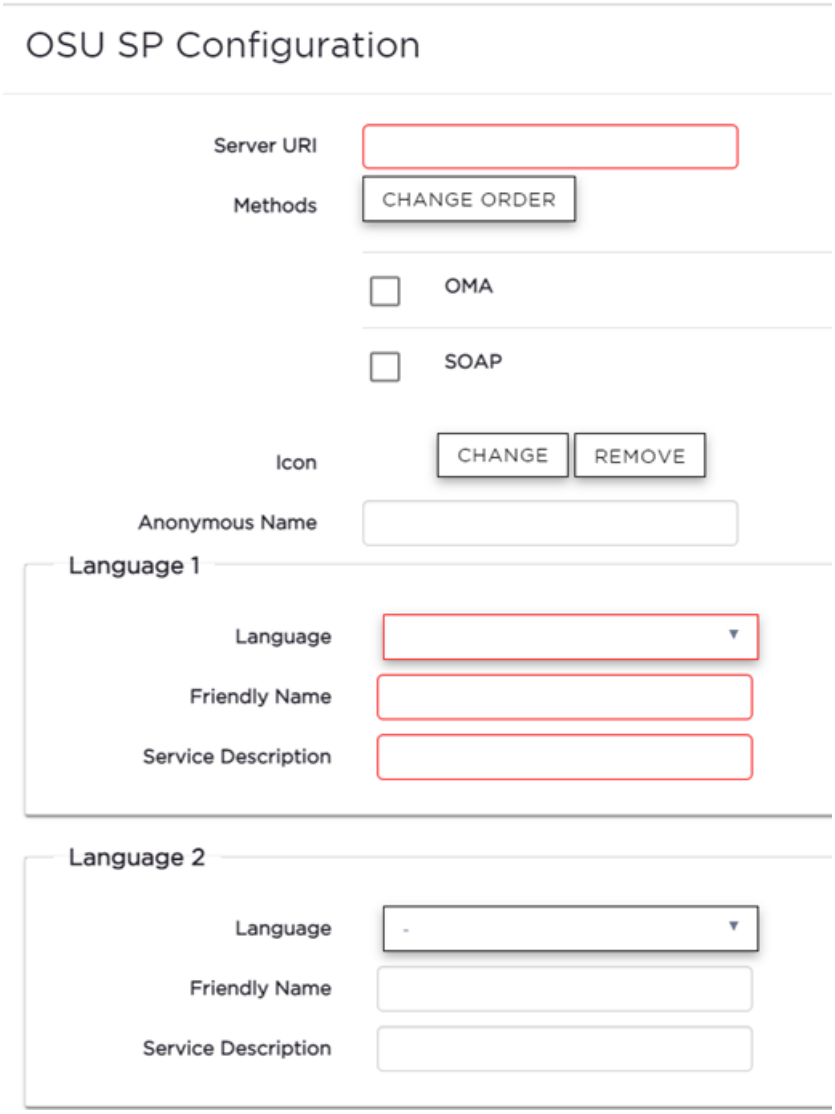


Figure 64: Configuring the OSU Service Provider

4. Configure the following parameters:

   Server URI

   The OSU server URI.

   Methods

   OSU Method is the preferred list of encoding methods that the OSU server supports in order of priority. Select the connection method used by the provider. Select **Change Order** to reorder the method priority.

   Icon

   Add an icon that is associated with Online Signup:

   - To add or change the icon, select **Change**. Then, navigate to a .png file.

- To remove the icon, select **Remove**.

Anonymous Name

Configure a name that anonymous users can use to access the network.

Language

Configure the Language, Friendly Name, and Service Description for the Online Signup user interface.

5. Select **OK** to save the OSU SP configuration.

Related Topics

Online Signup on page 272

Captive Portal Settings

Go to **Networks** > **WLANS** to enable captive portal. Select the portal type: Internal, External, or CWA (Centralized Web Authentication). The configuration settings depend on the portal type.

Note
By default, when captive portal is enabled, HTTP, DNS, and DHCP access is provided to ExtremeCloud IQ Controller for redirection.

Related Topics

Internal Captive Portal Settings on page 276
External Captive Portal Settings on page 277
Centralized Web Authentication on page 278
ExtremeGuest Captive Portal Settings on page 283
Captive Portal Redirect Port List on page 285

Internal Captive Portal Settings

An internal captive portal resides on ExtremeCloud IQ Controller. Configure the following parameters for an internal captive portal.

Table 73: Internal Captive Portal Settings

Field	Description
Portal name	Select an icon to add, edit, or delete a captive portal. When you add or edit a captive portal, the portal configuration dialog displays.
Portal Connection	Indicates the Interface/Topology that is used for the portal communication.
Use FQDN for connection	Use the Fully-Qualified Domain Name (FQDN) of the VLAN instead of its IP address when redirecting clients to the captive portal. This is required for OpenID Connect.
Walled Garden Rules	Click **Walled Garden Rules** to configure policy rules for the internal captive portal.

Table 73: Internal Captive Portal Settings (continued)

Field	Description
Use HTTPS for connection	(Optional) Indicates that the connection will be secure with HTTPS.
Authentication method	Select the local authentication method for the Internal Captive Portal. The following authentication methods are supported for Internal Captive Portal: • Local. Look up in the local password repository. • LDAP. Look up on a remote LDAP server. This option enables LDAP Configuration. • Default AAA Server. This value must be configured for Local or LDAP. **Note:** Default AAA provides validation of client acceptance status based on provided credentials. Indication of a specific role for policy assignment change is not supported.
LDAP Configuration	Lightweight Directory Access Protocol. Select a configuration or select the plus sign to add a new configuration.

Related Topics

Portal Website Configuration on page 345
Portal Network Configuration on page 355
Portal Administration Configuration on page 357
Default Rules for Captive Portal on page 365
Interfaces on page 425

External Captive Portal Settings

An external captive portal resides on a separate server. Configure the following settings for an external captive portal.

Table 74: External Captive Portal Settings

Field	Description
ECP URL	URL address for the external captive portal. When integrating with ExtremeCloud™ A3, the URL format is: `https://<VIP of A3>/Extreme::XCC`
Walled Garden Rules	Select **Walled Garden Rules** to configure policy rules for the external captive portal.
Identity	(Optional) Determines the name common to both the ExtremeCloud IQ Controller and the external Web server if you want to encrypt the information passed between the ExtremeCloud IQ Controller and the external Web server. Required for signing the redirected URL. If you do not configure the Identity, the redirector on the AP drops the traffic.

Table 74: External Captive Portal Settings (continued)

Field	Description
Shared Secret	(Optional) The password that is used to validate the connection between the client and the RADIUS server.
Use HTTPS for connection	Indicates that the connection will be secure with HTTPS.
Send Successful Login To	Indicates destination of authenticated user. Valid values are: • Original Destination. The destination of the original request. • Custom URL. Provide the URL address.

Related Topics

Configuring L2 Rules on page 294
Configuring L7 Application Rules on page 297
Walled Garden Rules on page 283

Centralized Web Authentication

Typically, when an external captive portal is employed, a web server hosts a single site that allows users to authenticate to the network. Centralized Web Authentication (CWA) offers the ability to serve a web page based on a set of conditions that are defined on the RADIUS server. The user is redirected to the appropriate web page after successful authentication using the 802.1x protocol.

With a CWA captive portal, the URL for the captive portal is provided dynamically through RADIUS attributes. The redirection can occur either at the AP (for Bridged@AP topologies) or at ExtremeCloud IQ Controller (for Bridged@AC topologies). Examples of conditions that determine the destination web page include: the expiration date for a user password or the due date of a bill that must be paid before a user can gain access to the network.

CWA supports an ExtremeControl captive portal server and a Cisco® ISE captive portal server. The configuration procedure for captive portal on ExtremeCloud IQ Controller is the same regardless of the captive portal server. CWA is supported on both Bridged@AC and Bridged@AP topologies.

From ExtremeCloud IQ Controller, configure the following:

- AAA Policy defining the RADIUS server, then specify that AAA Policy on the CWA captive portal network configuration.
- Policy role that includes a redirect rule. The redirect rule must use the TCP protocol and redirect the client based on the domain name or IP address that is specified in the URL message that is sent from the RADIUS server.

For information on the captive portal server configuration, see the ExtremeCloud IQ Controller Deployment Guide.

Note
Extreme Networks AP39xx and the Wi-Fi 6 AP models all support Centralized Web Authentication (CWA) captive portal.

Related Topics

CWA Network Settings on page 279
CWA Policy Redirection Role on page 281
Configure AAA Policy on page 327

CWA Network Settings

To configure a Centralized Web Authentication (CWA) captive portal:

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

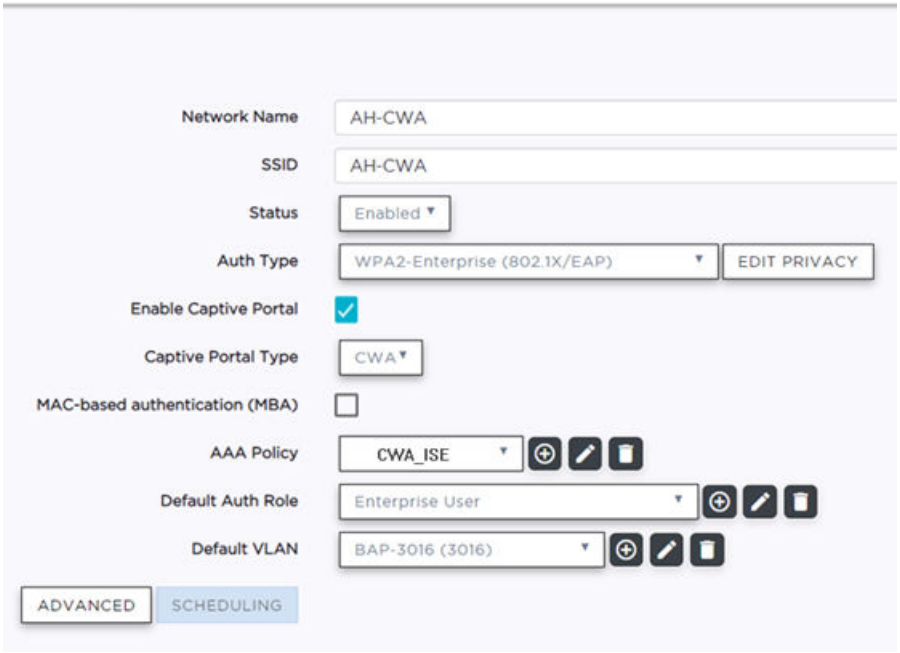


Figure 65: CWA Network on ExtremeCloud IQ Controller

2. Configure the following settings:

Table 75: Centralized Web Authentication Network Settings

Field	Description
Network Name	Enter a unique, user-friendly value that makes sense for your business. Example: Staff
SSID	Enter a character string to identify the wireless network. Maximum 32 characters. Upper and lowercase allowed. Example: PermanentStaff

Table 75: Centralized Web Authentication Network Settings (continued)

Field	Description
Status	Enable or disable the network service. Disabling the network service shuts off the service but does not delete it.
Auth Type	The Authorization Type for a CWA captive portal must be **WPA2 Enterprise (802.1x EAP)**
Enable Captive Portal	Select this option to configure a captive portal network.
MAC-Based Authentication	(Optional) Select this option to enable MBA. When selected, multi-factor authentication is enabled. The following parameter displays when MAC-based Authentication is enabled: • **MBA Timeout Role**. Select the role that will be assigned to a wireless client during MAC-based authentication (MBA) if the RADIUS server access request times out. If no MBA Timeout Role is selected, then a RADIUS server timeout is treated like an Access-Reject, which prevents the client from accessing the network. Other options: ◦ — create a new role ◦ — edit role ◦ — delete role
Captive Portal Type	**CWA**
AAA Policy	Specify the AAA Policy associated with the captive portal. Define the RADIUS server used for authentication in the AAA Policy. This is the IP address of the captive portal. See Figure 66 on page 281.
Default Auth Role	Specify the default authorization role that is configured on ExtremeCloud IQ Controller.
Default VLAN	Specify the default VLAN that is configured on ExtremeCloud IQ Controller.

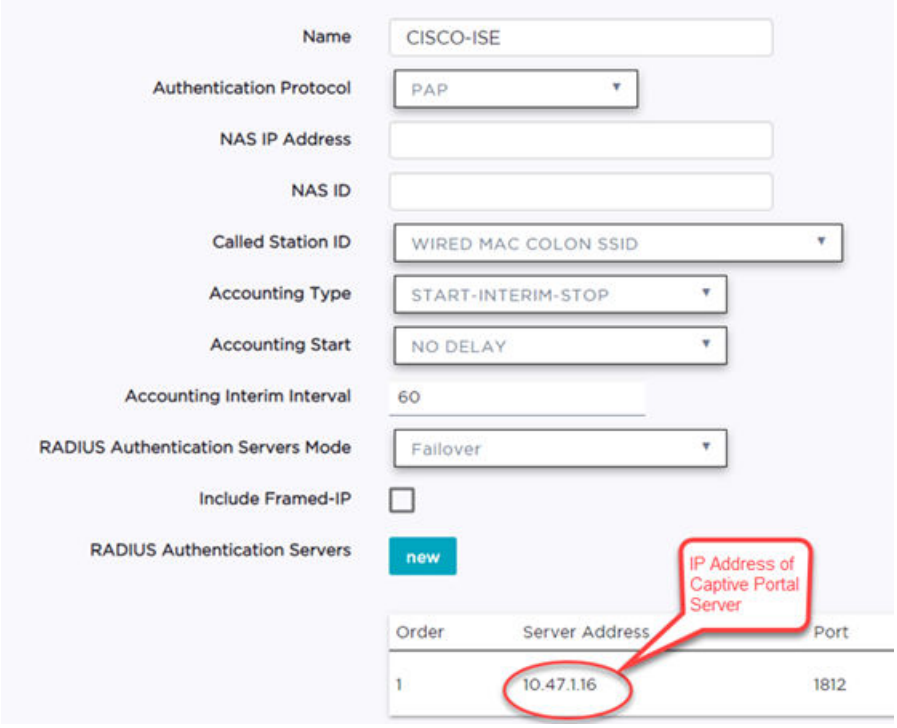


Figure 66: AAA Policy for CWA — RADIUS Server definition

Related Topics

Configure AAA Policy on page 327
CWA Policy Redirection Role on page 281
Add Policy Roles on page 292
Configuring VLANS on page 303

CWA Policy Redirection Role

To configure a policy role with at least one redirection rule:

1. Go to **Configure** > **Policy** > **Role** > **Add**.
2. Create a new role.
3. Select **Layer 3/Layer4** and configure the parameters for a redirect rule that works with CWA captive portal. See Table 76 on page 282.

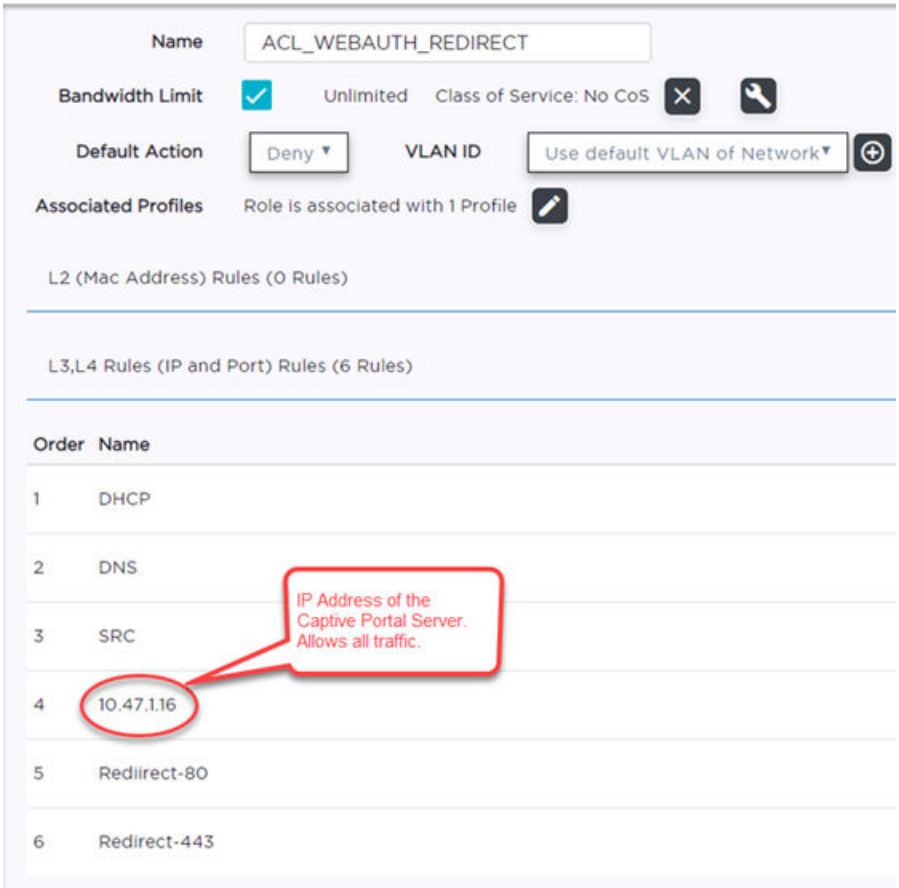


Figure 67: Example Redirection Role on ExtremeCloud IQ Controller that includes six L3/L4 rules

Figure 68: Redirect-80 rule redirects HTTP traffic from Port 80

Table 76: Rule Configuration for Layer3/Layer4 Redirection Rules

Field	Description
Name	Provide a name for the rule. Example: **Redirect-80** that redirects traffic on HTTP port 80.
Action	**Redirect**
Protocol	**TCP**
IP/Subnet	**User-Defined**. Then specify the IP address of the captive portal.
Port	Include at least one rule for HTTP port 80 or HTTPS port 443

Related Topics

Add Policy Roles on page 292

ExtremeGuest Captive Portal Settings

An ExtremeGuest captive portal resides on an ExtremeGuest server. Configure the following settings.

Table 77: ExtremeGuest Captive Portal Settings

Field	Description
Captive Portal Type	**EGuest**
Walled Garden Rules	Select **Walled Garden Rules** to configure policy rules for the external captive portal.
ExtremeGuest Servers	• Select the ExtremeGuest server from the drop-down list of configured servers. The number of server fields depends on the number of configured servers. Configure one portal server and up to two backup servers. ◦ Select an icon (, , or) to manage your servers from here. Select the appropriate check box to indicate that the server handles authentication, accounting, or both. At least one selection is required for each server. ◦ Select **Portal** to configure one server as the portal server. If your portal server goes down, you must manually select a backup server as the portal server.

Related Topics

ExtremeGuest Server Settings on page 325
Walled Garden Rules on page 283

Walled Garden Rules

When authenticating with third-party credentials such as Facebook or Google, the ExtremeCloud IQ Controller unregistered access policy must allow access to the third-party site (either allow all SSL or make allowances for third-party servers). The Portal Configuration must have the specific site registration enabled and include the Application ID and Secret for the third-party site.

Third-party registration for networks redirecting HTTP traffic to the captive portal using DNS Proxy requires additional configuration.

Create a unique application to the third-party software. Refer to the following developer sites:

- Facebook Developers page at https://developers.facebook.com/apps/
- Google Developers page at https://console.developers.google.com/projectselector/apis/library
- Microsoft Developers page at https://apps.dev.microsoft.com/#/appList.
- Yahoo Developers page at https://developer.yahoo.com/
- Salesforce Developers page at https://developer.salesforce.com/

The Application ID and Application Secret assigned during the creation of the third-party application must be provided in the Portal Configuration page.

Note
With an availability pair, when configuring authentication in the portal, specify the URI (*Uniform Resource Identifier*) for both the Primary and Secondary appliance.

Related Topics

Adding Walled Garden Rules on page 284
Configuring L2 Rules on page 294
Configuring L3, L4 Rules on page 295
Authentication with Third-party Credentials on page 349
Third-party Registration Requirements on page 349

Adding Walled Garden Rules

Take the following steps to configure Walled Garden rules:

1. Go to **Configure** > **Networks** and select a network.
2. Enable **Captive Portal**.
3. Select **Walled Garden Rules**.
4. Select a drop-down to display settings for each OSI layer:
   - L2 (Mac Address) Rules
   - L3, L4 (IP and Port) Rules
5. Configure the rule parameters.

   The following is an example of a DNS-based Layer 3 rule that allows access through Facebook.

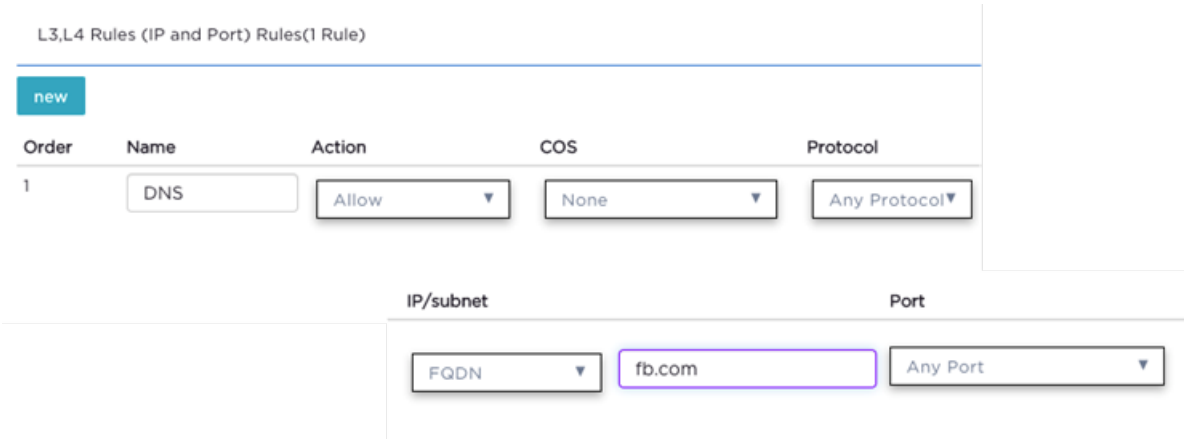


Figure 69: Layer 3 Rule

Each application site requires specific rules to access their site domains. Table 78 lists the rule configuration parameters needed for each application site.

Note
The domain information for each application site is subject to change. Refer to specific application site documentation if necessary.

Table 78: FQDN Rules Required for Social Logins

Application Site	Rule Parameters
Facebook	• Allow FQDN to facebook.com, port HTTPS • Allow FQDN to fbcdn.net, port HTTPS
Google	• Allow FQDN to accounts.google.com, port HTTPS
Microsoft	• Allow FQDN to login.live.com, port HTTPS • Allow FQDN to gfx.ms, port HTTPS • Allow FQDN to akadns6.net, port HTTPS
Salesforce	• Allow FQDN to login.salesforce.com • Allow FQDN to sfdcstatic.com
Yahoo	• Allow FQDN to login.yahoo.com, port HTTPS • Allow FQDN to yimg.com, port HTTPS

Related Topics

Walled Garden Rules on page 283
Configuring L2 Rules on page 294
Configuring L3, L4 Rules on page 295

Captive Portal Redirect Port List

Configure a port on the ExtremeCloud IQ Controller interface to which the client is redirected after the ECP response. If ECP support is configured for HTTP then the port is typically **80**, otherwise it is typically **443**. It is possible to configure a different port. The hw_port attribute appears in the redirection response from ExtremeCloud IQ Controller.

1. Go to **Configure** > **Networks** > **WLANS**.
2. Select **Enable Captive Portal**.
3. Select **CP Redirect Port List**.
4. Select to add a port to the list.
5. To delete a port, select the port, and then select .

Advanced Network Settings

To configure advanced network settings:

1. Go to **Configure** > **Networks** > **WLANS** > **Add**.
2. Select **Advanced**.

3. Configure the following parameters:

OWE Transition Auto Provisioning

Enable this option to generate an Opportunistic Wireless Encryption (OWE) network automatically when the network authentication is set to Open. OWE offers security to open networks, ensuring that traffic between an AP and a client is encrypted. Other clients can sniff and record traffic, but cannot decrypt it.

Agile Multiband

Enables wireless devices to better respond to changing wireless network conditions. Improved resource utilization helps balance wireless network load, increase capacity, and provide end users the best possible wireless experience.

This feature is enabled by default. It is supported on ExtremeWireless access points AP3xx, AP4xx, and AP5xx.

RADIUS Accounting

Indicates that the RADIUS server will also handle RADIUS accounting requests.

ExtremeCloud IQ Controller provides Vendor Specific Attributes (VSAs) in the message to the RADIUS server. For more information, see Vendor Specific Attributes on page 289.

Hide SSID

Prevents the SSID from going in a beacon message but sends out the SSID when a device probes the APs.

Include Hostname

Includes the AP Hostname in the beacon signal. Enable this setting to easily identify the access point that is the originator of a particular signal without having to resort to BSSID conversion tables. This feature can be useful during site surveys.

The Hostname value is limited to 32 characters, no spaces. It can be the same as or different from the AP Name. Both the AP Name and AP Hostname are displayed on the **AP List** and on the **AP Details** dialog in ExtremeCloud IQ Controller.

Radio Management (11k) Support

Enabling this option helps improve the distribution of traffic in a wireless network by allowing a client to select an AP based on its active subscribers and overall traffic. (This feature is dependent on the client's ability to support this option.) APs serving WLANs with 11k support enabled perform a background scan to collect neighbor AP information and determine alternatives to recommend to the client.

Quiet IE

When Quiet IE is enabled, the AP temporarily silences the clients by including a Quiet IE countdown (from 200 to 1) in the Beacons and Probe Responses. When Quiet Count reaches 1, all the clients have to be quiet for the Quiet Duration given in the Quiet IE.

U-APSD (WMM-PS)

Power Save mode. Between transmitting packets the client device sleeps and saves power while the access point buffers downlink frames. The application decides when to receive packets.

Note
U-APSD can interfere with device functionality.

Admission Control

Enable one or more of these options to prioritize traffic and provide enhanced multimedia support. When a client connects, it receives a reserved amount of time, which improves the reliability of applications by preventing over-subscription of bandwidth. If Admission Control is enabled, the clients must use it. If a client does not support it, that client's traffic will be downgraded.

Note
It is not recommended to enable Admission Control if all clients do not support it.

Admission Control for Voice (VO)

Forces clients to request admission to use the highest priority access categories in both inbound and outbound directions.

Admission Control for Video (VI)

Provides distinct thresholds for VI (video).

Admission Support for Best Effort (BE)

If the client does not support admission control for the access category that requires admission control, the traffic category will be downgraded to lower access category that does not have Mandatory Admission control.

Global Admission Control for Background (BK)

Provides global admission control for background bandwidth.

Client to Client Communication

Control blocking traffic between wireless clients on the same SSID. Select this setting to enable blocking of client-to-client traffic per network. This setting is disabled by default. Blocked client traffic is supported.

Enable this setting on your network configuration and assign the network to a configuration Profile. Assign the configuration Profile to a device group. All APs, in that device group will block traffic between wireless clients on the SSID.

Note
Blocking client-to-client traffic on Bridged at AP and Fabric Attach topologies is not supported.

Clear on Disconnect

Purge client session after client is disconnected. This option is enabled by default.

Pre-Authenticated idle timeout (seconds)

The amount of time (in seconds) that a mobile user can have a session on the controller in *pre-authenticated* state during which no active traffic is passed. The session is terminated if no active traffic is passed within this time.

Post-Authenticated idle timeout (seconds)

The amount of time (in seconds) that a mobile user can have a session on the controller in *authenticated* state during which no active traffic is passed. The session will be terminated if no active traffic is passed within this time.

Maximum session duration (seconds)

The maximum user session length in seconds.

Related Topics

WLAN Service Settings on page 250
Configuring DSCP Classification on page 288

Configuring DSCP Classification

A Differentiated Services Code Point (DSCP) is a packet header value that indicates Quality of Service (QoS) priority level for traffic delivery. All 64 DSCP code-points are supported.

To define a class of service for each DSCP code:

1. Go to **Configure** > **Networks** > **WLAN Services**.
2. Select a network or select **Add**.
3. Select **Advanced**.
4. Scroll to the bottom of the **Advanced Settings** page and select **QoS/DSCP**
5. Select a Service Class value for each DSCP code.

   Valid priority values in descending order:

   - Network Control (7)
   - Premium (Voice) (6)
   - Platinum (5)
   - Gold (4)
   - Silver (3)
   - Bronze (2)
   - Best Effort (1)
   - Background (0)

Related Topics

Advanced Network Settings on page 285

Vendor Specific Attributes

ExtremeCloud IQ Controller provides the following Vendor Specific Attributes (VSAs) in the message to the RADIUS server:

Table 79: Vendor Specific Attributes

Attribute Name	ID	Type	Messages	Description
AP-Name	2	string	Sent to RADIUS server	The name of the AP the client is associating to. It can be used to assign role based on AP name or location.
AP-Serial	3	string	Sent to RADIUS server	The AP serial number. It can be used instead of (or in addition to) the AP name.
AP Ethernet MAC		string	Sent to RADIUS server	The MAC address of the AP used by the ECP to determine client location.
AP Location		string	Sent to RADIUS server	The physical location of the AP. Provided by the network administrator.
VNS-Name	4	string	Sent to RADIUS server	The name of the Virtual Network the client has been assigned to. It is used in assigning role and billing options, based on service selection.
SSID	5	string	Sent to RADIUS server	The name of the SSID the client is associating to. It is used in assigning role and billing options, based on service selection.
BSS-MAC	6	string	Sent to RADIUS server	The name of the BSS-ID the client is associating to. It is used in assigning role and billing options, based on service selection and location.
Role-Name	7	string	Sent to RADIUS server	The name of the role applied to the station's session.
Topology-Name	8	string	Sent to RADIUS server	The name of the topology applied to the station's session.
Ingress-RC-Name	9	string	Sent to RADIUS server	The name of the rate limit applied to the station's session's outbound traffic.
Egress-RC-Name	10	string	Sent to RADIUS server	The name of the rate limit applied to the station's session's inbound traffic.
RSS	11	integer	Sent to RADIUS server	Received Signal Strength. RSS value in the RADIUS Accounting logs can identify areas that have a weak Wi-Fi signal. Use this information to increase coverage in problem areas.

Managing a Network Service

After a network service is created, you can modify the configuration settings or delete the network. To get started:

1. Go to **Configure** > **Networks**.
2. Select **WLANs** or **Mesh Points**.
3. Select a network service from the list.

   The network settings display.
4. Modify configuration settings as needed and select **Save**.
5. To delete a network, select **Delete**.

   A delete confirmation message displays.
6. Select **OK**.

Related Topics

WLAN Service Settings on page 250
Mesh Point Network Settings on page 262
Networks List on page 110

Band Steering

Band Steering is intended to relieve congestion by encouraging dual-band client devices to use the higher capacity 5 GHz band. To make use of Band Steering, ensure that networks are assigned to both radios.

For Band Steering to work effectively, configure similar coverage areas for the 2.4 GHz and 5 GHz bands. Design the network for both 5 GHz and 2.4 GHz coverage. For networks where coverage quality differs between bands, disable Band Steering.

Enable or disable Band Steering per SSID from the **Networks** tab within the device group or for a specific AP WLAN override. Band Steering per SSID is supported on all Wi-Fi 6 access points.

Note
The Band Steering feature steers 5 GHz clients toward the 5 GHz band. 6E clients can self steer into the 6 GHz band for service.

Related Topics

Add or Edit a Configuration Profile on page 134
WLAN Override on page 227

Policy

You can define policy rules for a role to specify network access. Network policies are a set of rules, defined in a specific order, that determine how connections are authorized or denied. If you do not define policy rules for a role, the role's default action is applied to all traffic subject to that role. However, if you require user-specific filter definitions, then the filter ID configuration identifies the specific role that is applied to the user.

Related Topics

Roles List on page 123
Configuring Roles on page 291
Class of Service on page 299
VLANS on page 302
Configuring Rates on page 317

Configuring Roles

A role is a set of network access services that can be applied at various points in a policy-enabled network. Roles are usually named for a type of user such as Student or Engineering. Often, role names match the naming conventions that already exist in the organization. The role name should match filter ID values set up on the RADIUS servers.

The default non-authenticated role is used when the client is not authenticated but able to access the network. The default authenticated role is assigned to a client when it successfully authenticates but the authentication process did not explicitly assign a role to the client.

Note
To configure default roles, go to **Configure** > **Networks**.

When the default action is sufficient, a role does not need additional rules. Rules are used only to provide unique treatment of packet types when a single role is applied.

ExtremeCloud IQ Controller is shipped with a default policy configuration that includes the following default roles:

- Enterprise User
- Quarantine
- Unregistered
- Guest Access
- Deny Access
- Assessing
- Failsafe

The Enterprise User access policy is intended for admin users with full access.

The Quarantine access policy is used to restrict network access to end-systems that have failed assessment. The Quarantine policy role denies all traffic by default while permitting access to only required network resources such as basic network services (for example, ARP, DHCP, and DNS) and HTTP to redirect web traffic for assisted remediation.

Related Topics

Add Policy Roles on page 292
Role Widgets on page 126
Policy Role Settings on page 292

Add Policy Roles

Define policy roles to provide unique treatment of packet types when a single role is applied.

Note
Associate each role with a configuration Profile of a device group for each AP in the group to make use of the policy role.

1. Go to **Configure** > **Policy** > **Roles** > **Add**.
2. Configure the parameters for the role. For more information, see Policy Role Settings on page 292.
3. Select the drop-down arrow to open the appropriate OSI layer.

   Add rules associated with the appropriate OSI layer. Each OSI layer has one default rule that is provided by ExtremeCloud IQ Controller. Policy rules are applied from top to bottom.
4. To add new rules, select **New**.

   Note
   ExtremeWireless Wi-Fi 6 access points support rule sets that contain up to 256 rules. AP39xx series access points support rule sets with no more than 64 rules.

5. To edit a rule, click on the rule to open the rule parameters. Configure the rule parameters and select **Save**.

   Note
   If you create a Deny All rule for any subnet as the top rule, the policy will drop all traffic.

Related Topics

Policy Role Settings on page 292
Policy Rules for OSI L2 to L4 on page 293
Application (Layer 7) Rules on page 296
Associated Profiles on page 137

Policy Role Settings

Table 80: Role Parameter Settings

Field	Description
Name	Name of the role.
Bandwidth Limit	Select this option to allow unlimited bandwidth. Select to set the Class of Service value.

Table 80: Role Parameter Settings (continued)

Field	Description
Default Action	Determines the access control default action. If you do not define policy rules for a role, the role's default action is applied to all traffic subject to that role. However, if you require user-specific filter definitions, then the filter ID configuration identifies the specific role that is applied to the user. Valid values are: • Allow. Allow packets using the specified VLAN option. Specify either the Default Network VLAN or a configured VLAN. • Deny. Deny packets that do not match a filter rule or deny packets when a filter rule does not exist. When a packet *does* match the filter rule action Allow, allow packet using the specified VLAN option. Specify either the Default Network VLAN or a configured VLAN.
VLAN ID	Policy roles default to the VLAN specified during network configuration. You can specify a unique VLAN here. Click to add a new VLAN option.
Associated Profile	Indicates profiles that this role is associated with. Click to modify profile association. **Note:** Associate a role with a configuration Profile. The configuration Profile is associated with the device group. Each AP in the device group makes use of the policy role.
Rules	Policy rules are organized by Open Systems Interconnection (OSI) layer classification. Select the drop-down arrow to display rules that pertain to each OSI layer.

Related Topics

Policy Rules for OSI L2 to L4 on page 293
Application (Layer 7) Rules on page 296

Policy Rules for OSI L2 to L4

You can define policy rules for a role to specify network access settings for a specific user role. Network policies are a set of rules, defined in a specific order, that determine how connections are authorized or denied. If you do not define policy rules for a role, the role's default action is applied to all traffic subject to that role. However, if you require user-specific filter definitions, then the filter ID configuration identifies the specific role that is applied to the user.

A role can have no rules if the default action is sufficient. Rules are used only to provide different treatments for different packet types to which a single role is applied.

Specify the OSI layer to which the rule pertains. The rule defines one or more actions to take on a packet matching criteria specified by the rule. The criteria could be the MAC address (L2) or the IP address or port number (L3 and L4).

The default action for all rules is **Contain to VLAN**, indicating that the rule applies to all traffic associated with the VLAN defined at the Role. This can be the Network default VLAN or a unique VLAN ID specified at the Role. The ability to specify the VLAN ID at the Role makes configuring network policy easier.

If the traffic is allowed, it can also be assigned a Class of Service (CoS) that can affect the priority and latency of that traffic. Only the rules in the policy assigned to a client are applied to a client's traffic.

Note
Rules in the Application Layer (L7) apply to application access and use different matching criteria.

For additional information about Policy Rules Direction, see Understanding the Policy Rules Direction in the GTAC Knowledge Center.

Related Topics

Configuring L2 Rules on page 294
Configuring L3, L4 Rules on page 295

Configuring L2 Rules

Configure policy rules that are associated with a role from the **Role Configuration** page. To configure an OSI Layer 2 rule, which filters on MAC Address:

1. Select the L2 drop-down and select **New** or select the rule to edit and existing rule.
2. Configure the following parameters:

Name

Name the rule.

Action

Determines access control action for the rule. Valid values are:

- None - No role defined
- Allow - Packets contained to role's default action's VLAN/topology
- Deny - Any packet not matching a rule in the policy is dropped.
- Containment VLAN - A topology to use when a network is created using a role that does not specify a topology. (Not applicable for L7 Application Rules.)

COS

Determines the importance of a frame while it is forwarded through the network relative to other packets. The CoS defines actions to be taken when rate limits are exceeded.

MAC Address Type

Indicates if the MAC Address is user defined or any MAC Address. **User Defined** enables the **MAC Address** field for user input.

MAC Address

Media access control address. Sometimes known as the hardware address, is the unique physical address of each network interface card on each device. Specify the MAC address of the wireless client.

3. Select **Save**.

   All rule types are applied to the policy in top to bottom order. The policy is installed on the enforced APs.

Related Topics

Configuring L3, L4 Rules on page 295
Policy Rules for OSI L2 to L4 on page 293

Configuring L3, L4 Rules

Configure policy rules that are associated with a role from the **Role Configuration** page. To configure an OSI Layer 3 and 4 rule, which filters on IP Address and Port number:

1. Select the L3, L4 drop-down and select **New** or select the rule to edit and existing rule.
2. Configure the following parameters:

   Name

   Name the rule.

   Action

   Determines access control action for the rule. Valid values are:

   - None - No role defined
   - Allow - Packets contained to role's default action's VLAN/topology
   - Deny - Any packet not matching a rule in the policy is dropped.
   - Containment VLAN - A topology to use when a network is created using a role that does not specify a topology. (Not applicable for L7 Application Rules.)

   COS

   Determines the importance of a frame while it is forwarded through the network relative to other packets. The CoS defines actions to be taken when rate limits are exceeded.

   Protocol

   The user defined protocol or protocol type associated with the defined rule. Traffic from this protocol is subject to the defined rule. Valid values are:

   - User Defined, then specify a protocol that is not already in the list. Use this option to explicitly specify a protocol that is not listed.
   - A specific protocol from the list.

   IP Subnet

Specify the IP address or subnet address associated with the defined rule. Traffic from this address will be subject to the defined rule. Valid values are:

- User Defined. Specify the destination IP address and mask. Use this option to explicitly define the IP/subnet aspect of the rule.
- Any IP - Maps the rule to the associated Topology IP address.
- Select a specific subnet value - Select to map the rule to the associated topology segment definition (IP address/mask).
- FQDN - Allows for filtering on fully qualified domain names.
- Other subnet options include:
  - Sepectralink Mcst
  - Vocera Mcst
  - mDNS/Bonjour

Port

The port or port type associated with the defined rule. Traffic from this port is subject to the defined rule. Valid values are:

- User Defined, then type the port number. Use this option to explicitly specify the port number.
- A specific port type. The appropriate port number or numbers are added to the Port text field.

3. Select **Save**.

   All rule types are applied to the policy in top to bottom order. The policy is installed on the enforced APs.

Application (Layer 7) Rules

An *application rule* leverages the AP's deep packet inspection (DPI) engine to detect the underlying application to which a frame or flow belongs. The rule then applies access control and quality of service actions to all the traffic associated with the application, not just traffic destined for specific IP addresses or ports. The control actions regulate both access control and traffic engineering (rate limit, marking, and prioritization) for applications and groups.

Use case examples include:

- Identifying critical applications and assigning a higher priority and CoS value.
- Blocking restricted web content.
- Blocking or limiting peer-to-peer protocols to preserve bandwidth and flows for other applications.
- Limiting bandwidth usage by non-business related traffic.

ExtremeCloud IQ Controller installs application policies with rules on the supported APs where enforcement occurs.

Note
Application policies are supported by ExtremeCloud IQ Controller-enabled APs only, not switches.

Rules

Application policies consist of rules with matching criteria, coupled with one or more actions to take when a packet matches the rule's criteria. The matching criteria for an application is usually just the name of the application. The ExtremeCloud IQ Controller user interface lets you first select a category of applications, resulting in a subset of applications to choose from. Additionally, you can create a single rule that applies to all traffic in the application category by selecting a category and then selecting 'Wild Card' as the specific application.

Custom application rules are rules that you create to recognize (match) applications that are not in the pre-defined set of application matches provided by ExtremeCloud IQ Controller. You create a custom application rule by defining a regular expression to match against host names. The rule's match criteria will be available as a match criteria for policy rules that you create in the future.

Actions and Limitations

When the Action filter for the application rule is set to Deny, the first few packets of a flow must be allowed to pass through so that the deep-packet inspection (DPI) engine can examine the contents and classify the packets. After the packets are classified as Deny and the flow is blocked, the first few packets have already passed through the system. For typical web traffic, the leak is minimal for a long duration flow. However, for short duration flows, the Deny filter may not be effective.

Any flows that are not matched through classification are handled by the Default Action.

The Redirect action is only available for IPv4 traffic, not IPv6. The Allow, Deny, and Contain actions are available for IPv6.

Related Topics

Adding Custom Apps to the Application List on page 298

Configuring L7 Application Rules

Create application rules when you need application-level (Layer 7) enforcement, for example, to limit or block access to non-business related traffic.

You can create a new application rule anywhere in the list of policy rules and create any number of application rules in one role.

To configure application rules:

1. Go to **Policy** > **Roles** > **Add**.
2. For application policy rules, select the **L7 Application Rules** drop-down.
3. Select ✎ in that row.

   The **Rules** dialog displays.

   #### From User

   A packet header includes both a destination IPv4 address and a source IPv4 address. Determine how to filter traffic that flows from the station to the network

by defining the destination or the source address as the filter. Options include: Destination (dest), Source (src), and None.

To User

A packet header includes both a destination IPv4 address and a source IPv4 address. Determine how to filter traffic that flows from the network to the station by defining the destination or the source address as the filter. Options include: Destination (dest), Source (src), and None.

Search

Type the application to search for. The Group and Application Name fields are automatically populated when you select an application from the Search field.

Group

Internet applications are organized in groups based on the type or purpose of the application. After you select an Application Group, the Application Name drop-down is populated with application names that are part of the specified group.

Application Name

Names of applications that are a member of the specified group.

Access Control

Determines access control action for the rule. Valid values are:

- None - No role defined
- Allow - Packets contained to role's default action's VLAN/topology
- Deny - Any packet not matching a rule in the policy is dropped.
- Containment VLAN - A topology to use when a network is created using a role that does not specify a topology. (Not applicable for L7 Application Rules.)

Class of Service

Determines the importance of a frame while it is forwarded through the network relative to other packets. The CoS defines actions to be taken when rate limits are exceeded.

Click the plus sign to configure CoS. For more information, see .Configuring CoS on page 300

4. Select **Close** > **Save**.

   All rule types are applied to the policy in top-to-bottom order. The policy is installed on the enforced APs.

Adding Custom Apps to the Application List

When creating Application Rules, you can add custom applications to the list of possible applications. Take the following steps to configure a custom app for the Application Rule that is associated with a role:

1. Go to **Configure** > **Policy** > **Roles** > **Add**.
2. Select the drop-down arrow for L7 (Application) Rules and click **New** or select a rule in the list.

3. Select ✎ in that row.

   The **Rules** dialog displays.
4. Select ✎ next to the **Application** field.
5. Select **Create New Application**.
6. Configure the custom application settings.
7. The custom application is added to the list of available applications for the specified application group.

Related Topics

Custom Application Settings on page 299
Configuring L7 Application Rules on page 297

Custom Application Settings

Configure the following parameters to add custom applications to the L7 Apps list.

Table 81: Custom Application Settings

Field	Description
Group	Internet applications are organized in groups based on the type or purpose of the application. After you select an Application Group, the Application Name drop-down is populated with application names that are part of the specified group. The group names are pre-defined standard Extreme Application Analytics™ signature groups. The group names are case-sensitive.
Name	The name of the custom application.
Pattern	The Matching Pattern is the URL pattern that is associated with the application (case-sensitive, up to 64 characters).

Class of Service

In general, COS refers to a set of attributes that define the importance of a frame while it is forwarded through the network relative to other packets, and to the maximum throughput per time unit that a client or port assigned to the role is permitted. The CoS defines actions to be taken when rate limits are exceeded.

A role can contain default access control (VLAN) and/or Class of Service (priority) characteristics that will be applied to traffic when the rule either allows traffic, or does not specifically disallow traffic and the last rule is ALLOW ALL.

Class of Service is a 3-bit field that is present in an Ethernet frame header when 802.1Q VLAN tagging is present. The field specifies a priority value between 0 and 7, more commonly known as CS0 through CS7. These values can be used by QoS disciplines to differentiate and shape or police network traffic.

CoS operates only on 802.1Q VLAN Ethernet at the data link layer (Layer 2), which other QoS mechanisms (such as DiffServ, also known as DSCP) operate at the IP network layer (Layer 3).

After packets are classified, they are assigned a final User Priority (UP) value, which consists of the Priority and ToS/DSCP. Marking bits to be applied to the packet is taken from the CoS, and if the value is not set, then the received value (ToS/DSCP) is used. ToS/DSCP Marking rewrites the Layer 3 Type of Service (ToS) byte.

Related Topics

Configuring CoS on page 300
Configuring ToS/DSCP on page 301

Configuring CoS

The set of rules included in a role, along with any access or CoS defaults, determine how all network traffic of any client assigned to the role will be handled. For example, a Doctor role can be assigned a higher priority CoS and default access control due to the sensitivity and urgency of services that a doctor provides to patients.

1. Go to **Configure** > **Policy** > **Class of Service**.
2. Select **Add**, or select an existing Class of Service from the list.
3. Configure the following parameters:

   Name

   Naming should reflect the priority for your organization and be easily recognized by your IT team, such as Bulk Data or Critical Data.

   Priority

   Define how the Layer 2 priority of the packet will be marked. Priority 0 is the highest priority.
4. For **ToS/DSCP**, define how the Layer 3 ToS/DSCP will be marked. Enter a hexadecimal value in the **0x (DSCP:)** field, or select **Configure** to open the **ToS/DSCP** dialog box.
5. In the **CoS** dialog box, set the **Mask** value.

   Mask

   Select a hexadecimal value to use for the ToS/DSCP value. For example, if the mask is 0xF0, then only the four most significant bits of the ToS of the received packets are marked. So, if the received ToS is 0x33 and the ToS marking is set to 0x2A, then the resulting ToS is 0x23.
6. Specify the inbound and outbound rate limits, and select **OK**.
7. Click  to add a new bandwidth rate.
8. Select **Save**.

Related Topics

Configuring ToS/DSCP on page 301
Bandwidth Rate on page 301

Configuring ToS/DSCP

You can configure ToS/DSCP from the network rules page or the Class of Service page. Define how the Layer 3 ToS/DSCP will be marked:

1. Go to **Configure** > **Policy** > **Roles** > **Add**.

   Or, **Class of Service** > **Add** > **Configure** ToS/DSCP and skip to step 5.
2. Select Bandwidth Limit and click  .
3. Click **Edit** next to Advanced Settings.
4. Click **Configure** ToS/DSCP.
5. In the **ToS/DSCP** dialog box, select either **Type of Service (ToS)** or **Diffserv Codepoint (DSCP)**. Set the related options, and click **OK**.

   Type of Service (ToS)

   Precedence

   Assign a priority to the packet. Packets with lower priority numbers are more likely to be discarded by congested routers than packets with higher priority numbers.

   Delay Sensitive

   Specifies that the high priority packets will be routed with minimal delay. It can be useful to enable this option for voice protocols.

   High Throughput

   Specifies that high priority packets will be routed with high throughput.

   High Reliability

   Specifies that high priority packets will be routed with low drop probability.

   Explicit Congestion Notification (ECN)

   Permits end-to-end notification of network congestion while preventing dropped packets. ECN can be used only with two ECN-enabled endpoints.

   Diffserv Codepoint (DSCP)

   Well-Known Value

   These values are explicitly defined in the DSCP related RFCs and implemented on many vendors' switches and routers.

   Raw Binary Value

   Specify a binary value if you want finer definition of priority.

Bandwidth Rate

Inbound Rate: Inbound traffic is sent from the client to the network. Rate limits are enforced on a per-client basis whether the rate limit is assigned to a rule or role. Each client has its own set of counters that are used to monitor its wireless network utilization. Traffic from other clients never count against a client's rate limits. Maximum Number of Limiters per Group: 8 inbound.

Outbound Rate: Outbound traffic is sent from the network towards the client. Maximum Number of Limiters per Group: 8 outbound.

Configure the following parameters to configure a new Bandwidth Limit:

Name

The name for the rate limit.

Average Rate (CIR)

The rate at which the network supports data transfer under normal operations. It is measured in kilobits per second (Kbps).

The supported rate for ExtremeCloud IQ Controller is 500,000 Kbps.

Related Topics

Configuring CoS on page 300

VLANS

VLANs are logical subnets that isolate traffic to a single group. Many VLANs can coexist on a single Ethernet cable (typically referred to as a 'VLAN Trunk'). The AP can place traffic on any VLAN to which it is exposed and tunnel traffic between two APs with a GRE tunnel. Other options are bridging locally at the controller, VxLAN, and Fabric Attach. Fabric Attach enables the AP to connect to a Fabric Network.

It is not necessary to include a VLAN tag in a packet that is being transmitted over a VLAN. A packet transmitted without a VLAN tag is said to be untagged. Since there is no way to identify the VLAN to which an untagged packet belongs, there can be only one untagged VLAN on a VLAN trunk.

It is common practice to place all AP management traffic on an untagged VLAN and place user traffic on tagged VLANs. ExtremeCloud IQ Controller preconfigures switches with a single untagged VLAN that is used for managing access points and the switches themselves.

Another common option is to place all traffic on a single untagged VLAN. This is a simpler option to use when a network's applications do not benefit from VLAN deployment.

ExtremeCloud IQ Controller fully supports mixing tagged and untagged traffic. An AP wired interface can be an untagged member of one VLAN and a tagged member of several other VLANs simultaneously.

With switches, all administrator-created VLANs in ExtremeCloud IQ Controller are classified as tagged VLANs. When a tagged VLAN is assigned to a port, the port is configured to expect all traffic received from the VLAN or sent to the VLAN to be tagged. You can override the tagging on a per-port basis for the ports types Host and Other.

Associate a topology to a specific device group. This enables you to define a topology that is common to a set of devices and specify a specific attached VLAN. Topologies referenced by attached networks or roles are automatically added to the Profile VLANS list. You can also add topologies manually to the list. When creating a new topology, select the Profiles to associate with the new topology.

Related Topics

Configuring VLANS on page 303

Configuring VLANS

A VLAN defines how the user traffic is presented through the network interface.

To configure a VLAN:

1. Select **Configure** > **Policy** > **VLANS**.
2. Select **Add**, or select an existing VLAN from the list.

3. Configure the following parameters:

Table 82: VLAN Configuration Settings

Field	Description
Name	Provide a unique name for the VLAN.
Mode	Bridged@AC — The ExtremeCloud IQ Controller bridges traffic for the station through its interfaces, rather than routing the traffic. For B@AC, topology the station's "point of presence" on the wired network is the data plane port assigned to the topology. Bridged@AP — Assigned to APs, the AP bridges traffic between its wired and wireless interfaces without involving the ExtremeCloud IQ Controller. The station's "point of presence" on the wired network for a bridged at AP topology is the AP's wired port. GRE — A Generic Routing Encapsulation (GRE) topology traverses wireless client traffic from a campus AP to a locally managed Extreme Networks VPN Concentrator or 3rd party GRE terminating device. GRE tunneling supports traversing client traffic through positioned access points at a location separated from ExtremeCloud IQ Controller. Fabric Attach — The Fabric Attach topology type allows an AP to attach to a Shortest Path Bridging (Fabric Connect) Network. The client component on the AP communicates directly with the server on an edge switch (or it can communicate with the server through a proxy) to allow the AP to request VLAN to I-SID (backbone Service Identifier [IEEE 802.1 ah] mappings). The Fabric Attach topology type is similar to B@AP with the added I-SID parameter. Fabric Attach can be configured on the ExtremeCloud IQ Controller anywhere a B@AP topology can be configured. VxLAN — VxLAN is a network virtualization technology that leverages existing Layer 3 infrastructures to create tenant overlay networks. VxLAN addresses the requirements of a multi-tenant data center network infrastructure by: • Increasing virtual network scalability to 16 million instances. This allows for tenant VLAN (Virtual LAN) isolation whereby multiple tenants can manage their own VLAN/VMAN and MAC address spaces. • Adding an encapsulation that effectively hides VM MAC addresses from the physical network that results in physical networking devices to have smaller MAC and IP table sizes. • Allowing for Layer 2 adjacency across IP networks by which DC network operators protect their investment in their current infrastructure. Additionally operators can distribute traffic loads across links efficiently using Layer 3 ECMP (Equal-Cost Multi-Path routing).

Table 82: VLAN Configuration Settings (continued)

Field	Description
VLAN ID	Specify the VLAN ID. **Note:** It is possible to configure a unique VLAN ID when configuring a role. This provides more flexibility in the Contain to VLAN default Action. A unique VLAN ID is also required for a GRE topology. The VLAN ID range is (1 - 4094). 4094 is reserved for Internal VLAN ID.
VNI	For **VxLAN**. VxLAN Network Identifier. The VNI is a 24-bit identifier. It can be used in more than one VxLAN topology.
Remote VTEP	For **VxLAN**. The IP address of the tunnel End-Point is referred to as a VxLAN Tunnel Endpoint (or VTEP). The VTEP is the IP address of the network switch. Network switches that act as a VTEP are referred to as VxLAN gateways. There can only be one VTEP per VxLAN topology.
I-SID	For **Fabric Attach**. A unique VLAN identifier and a unique I-SID (service identifier). The I-SID range is (0-15999999). Use **I-SID = 0** to support Fabric Attach Standalone Proxy mode on Extreme Networks Ethernet Routing Switches. Standalone Proxy mode indicates that the network does not include a Fabric Attach Server switch (and therefore does not include a Shortest Path Bridging Fabric Core).
Tagged Traffic	If you have more than one VLAN on a port, enable tagging to identify to which VLAN the traffic belongs. Ensure that the tagged vs. untagged state is consistent with the switch port configuration. Fabric Attach topologies are always tagged.
Port	The port for network traffic bridged at controller (for example, physical ports: Port0, Port1, Port3, Port4). LAG ports are supported on physical appliances only (LAG1, LAG2). When the VLAN uses a Port that is then added to a LAG, use the LAG as the VLAN.
Layer 3	Check this box when configuring parameters for the network layer (B@AC). **Note:** The **Certificates** button displays to configure browser certificates for captive portal security.
Layer 3 Parameters	
Remote Settings: IP Address	The IP Address of a remote server on which the VLAN resides.

Table 82: VLAN Configuration Settings (continued)

Field	Description
IP Address	IP address of the VLAN. Wireless clients can access ExtremeCloud IQ Controller via this IP address. **Note:** The following subnets are reserved for internal communications and Docker operations: • 172.17.0.0/24 • 172.31.0.16/28 The ExtremeCloud IQ Controller user interface logic prevents adding addresses in these address ranges for VLAN interface references.
FQDN	Fully-Qualified Domain Name
CIDR	CIDR field is used along with IP address field to find the IP address range.
DHCP	Dynamic Host Configuration Protocol allows network administrators to centrally manage and automate the assignment of IP addresses on the corporate network. DHCP sends a new IP address when a computer is plugged into a different place in the network. The protocol supports static or dynamic IP addresses and can dynamically reconfigure networks in which there are more computers than there are available IP addresses. Valid values are: • Local Server. Indicates that the ExtremeCloud IQ Controller is used for managing IP addresses. • Use Relay. Indicates that the ExtremeCloud IQ Controller forwards DHCP requests to an external DHCP server on the enterprise network. DHCP relay bypasses the local DHCP server for the ExtremeCloud IQ Controller and allows the enterprise to manage IP address allocation to a site from its existing infrastructure.
Enable Device Registration	Indicates that the wireless AP or switch can use this port for discovery and registration.
Mgmt Traffic	Indicates that this port will be used to manage traffic. Enable **Mgmt Traffic** to access the ExtremeCloud IQ Controller user interface through this port.
Associated Profiles	Select to display a list of configured Profiles. You can associate a VLAN to a specific set of devices through the assigned configuration Profile for the device group.

4. To configure advanced parameters, select **Advanced**.
5. Select **Save**.

Related Topics

VLAN Advanced Setting on page 307
VLAN Profile Settings on page 161
Associated Profiles on page 137
VLANS on page 302

Fabric Attach Topology on page 309
VxLAN Topology on page 310
GRE Topology on page 313
Generate Browser Certificates on page 343
Associated Profiles on page 137

VLAN Advanced Setting

Configure the following parameters to optimize your network connectivity. Modifying the following settings is optional. Consider changes thoughtfully.

Note
For higher transmission rates, by default, multicast is converted to unicast for all Wi-Fi 6 access points discovered by ExtremeCloud IQ Controller.
There is a maximum client threshold of 64 clients. Above 64 clients, the AP defaults to broadcasting on a DTIM interval.

Multicast Bridging

Select this option to enable forwarding of multicast traffic (point-to-multipoint) between the wired and wireless sides of the AP. Because multicasts consume a lot of 802.11 air time, when you enable this option you must also specifically identify the types of multicast traffic that you want forwarded by adding one or more rules.

Multicast Rules

Add one or more multicast rules if you enabled **Multicast Bridging**. Multicast rules (point-to-multipoint) permit traffic that matches the rule. A multicast rule is defined as the multicast IP address of the traffic destination and a mask that allows a range of addresses to be matched by a single rule. ExtremeCloud IQ Controller offers a predefined set of multicast rules. Select a preset multicast rule or define a new rule.

Block Non-Essential Broadcast

When enabled, block non-essential broadcast traffic on a bridged at controller (B@AC) topology.

This setting overrides user-level policy role definitions:

- When the network policy is Allow All, all broadcast traffic except ARP and DHCP on a topology is blocked in both directions. ARP and DHCP broadcast traffic is considered essential.
- When the network policy is Deny All, all inbound traffic is blocked. Outbound ARP and DHCP traffic is forwarded. All other outbound traffic is blocked.

Related Topics

Pre-defined Multicast Rules on page 307
Configuring a Multicast Rule on page 308
Configuring VLANS on page 303

Pre-defined Multicast Rules

1. Go to **Policy** > **VLANS** > **Add**, or select a VLAN.
2. Select **Advanced**.

3. Select **Add Pre-Defined Rule**.
4. Select a value from the **Multicast Group** field and click **Add**.

Related Topics

Configuring a Multicast Rule on page 308
Configuring VLANS on page 303

Configuring a Multicast Rule

1. Go to **Policy** > **VLANS** > **Add**, or select a VLAN.
2. Select **Add New Rule**.
3. Configure the following parameters:

IP address

Enter the multicast IP address for the traffic destination.

CIDR

Classless Inter-Domain Routing. An address aggregation scheme that uses supernet addresses to represent multiple IP destinations.

Wireless Replication

Enables the forwarding of multicast traffic from a wireless client to other wireless clients. If disabled, multicast traffic from wireless clients is forwarded to wired clients only. Wireless clients will not receive it.

Group

Indicates the multicast group associated with the rule. Multicast is a communication pattern in which a source host sends a message to a group of destination hosts.

Local DHCP Management Settings

Configure the following Local DHCP settings:

Domain Name

The name of the domain that is allocated for the IP address range.

Lease (Seconds)

The DHCP Lease represents the time period between when a device obtains the IP address and the time the IP address expires. When the **Lease** expires, the device releases the IP address and ExtremeCloud IQ Controller issues a new one. Default Lease is 36000 seconds, Default Max Value is 2592000 seconds. Devices can request a lease value.

DNS Servers

Primary IP address for the DNS (Domain Name Server).

WINS Servers

IP address of the WINS (Windows Internet Name Service) server.

Gateway

Gateway IP address.

Address Range

IP address range. Value is prompted by the subnet IP address that you configured.

Exclusions

(Available from the VLAN configuration) A range or single IP address that is excluded from the greater Address Range. Save your VLAN configuration before selecting **Exclusions** to configure IP address exclusions.

Related Topics

Configure IP Address Exclusions on page 309
Add an Interface on page 427
Configuring VLANS on page 303

Configure IP Address Exclusions

Exclude specific IP addresses or a range of IP addresses when configuring the IP Address Range for the Local DHCP server.

Note
Save your VLAN ID configuration before configuring IP Address Range Exclusions for a Local DHCP.

1. From the **Local DHCP Settings** dialog, select **Exclusions**.
2. Configure an IP Address Range or a Single IP Address that will be excluded from the larger IP Address Range configured under **Local DHCP Settings**.
3. Add an optional comment indicating why these addresses are excluded.
4. To add a new comment, select **New**.
5. To save the excluded IP addresses, select **Save**.
6. After you save, you can edit or delete the saved exclusions:
   - To edit the saved exclusions, select .
   - To delete the saved exclusions, select .

Related Topics

Local DHCP Management Settings on page 308

Fabric Attach Topology

The Fabric Attach topology type allows an AP to attach to a Shortest Path Bridging (Fabric Connect) Network. The client component on the AP communicates directly with the server on an edge switch (or it can communicate with the server through a proxy) to allow the AP to request VLAN to I-SID (backbone Service Identifier [IEEE 802.1 ah] mappings). The Fabric Attach topology type is similar to B@AP with the added I-SID parameter. Fabric Attach can be configured on the ExtremeCloud IQ Controller anywhere a B@AP topology can be configured.

Note
When Fabric Attach is configured, LLDP (Link Layer Discovery Protocol) is automatically enabled on all APs associated with the topology. The setting cannot be disabled by users.

The switch requires that the VLAN/I-SID mapping is unique per port per switch, therefore only one AP per switch port is allowed.

ExtremeWireless APs connected to a Fabric-enabled switch automatically use the default management VLAN that is configured on the switch. Moving an AP from a Fabric-enabled switch to a non Fabric-enabled switch requires a factory default reset to connect to the new management VLAN.

Note
In a mobility scenario that includes a local and foreign ExtremeCloud IQ Controller, make sure the Fabric Attach topology configuration is the same on each ExtremeCloud IQ Controller, ensuring that an AP that moves between appliances has the same set of topologies.

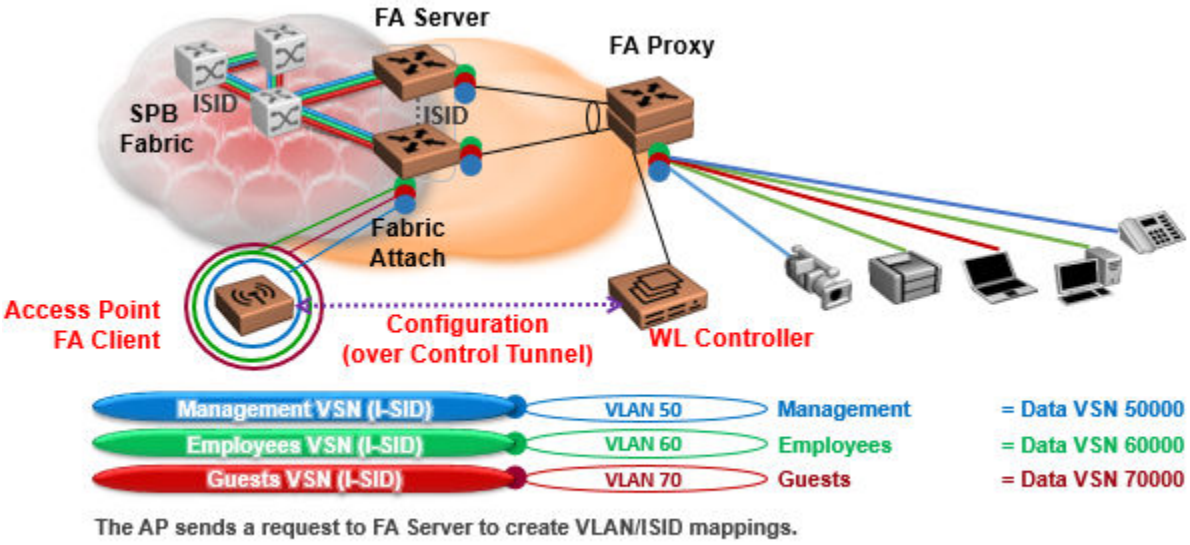


Figure 70: Fabric Attach for FA Clients — Automated Network Services

VxLAN Topology

ExtremeCloud IQ Controller leverage VxLAN capabilities of ExtremeXOS switches to establish different head-ends for tunneling traffic in an enterprise. Support includes:

- Tunnel in VxLAN from AP directly to a target switch
- Bypass ExtremeCloud IQ Controller
- Abstracts interconnections.

VxLAN is a Layer 2 overlay scheme over a Layer 3 network. Overlays are called VxLAN segments and only a VM and a physical machine (tenant) within the same segment have Layer 2 connectivity. VxLAN segments are uniquely identified using an identifier called the VxLAN Network Identifier (VNI). The VNI is a 24-bit identifier; therefore, an administrative domain can support up to 16 million overlay networks.

Because the scope of the MAC, originated by tenants, is restricted by the VNI, overlapping MAC addresses across segments can be supported without traffic leaking

between tenant segments. When a tenant frame traverses a VxLAN overlay network, it is encapsulated by a VxLAN header that contains the VNI. This frame is further encapsulated in a UDP header and L2/L3 headers.

VxLAN can add up to a 50-byte header to the tenant VM frame. For VxLAN to work correctly, this requires that the IP MTU be set to at least 1550 bytes on the network-side interfaces. IP MTU of 1550 should also be set on all transit nodes which carry VxLAN traffic. The point at which a tenant frame is encapsulated (or decapsulated) is referred to as a VxLAN Tunnel Endpoint (or VTEP). VTEPs are typically located on hypervisors but may also be located on physical network switches. Network switches that act as a VTEP are referred to as VxLAN gateways.

The role to encapsulate/decapsulate a frame is performed by a VxLAN Tunnel Endpoint (VTEP), also referred to as a VxLAN gateway. A VxLAN gateway can be a Layer 2 gateway or Layer 3 gateway depending on its capacity. A Layer 2 gateway acts as a bridge connecting VxLAN segments to VLAN segments. A Layer 3 gateway performs much like a Layer 2 gateway, but it is also capable of routing traffic between tenant VLANs.

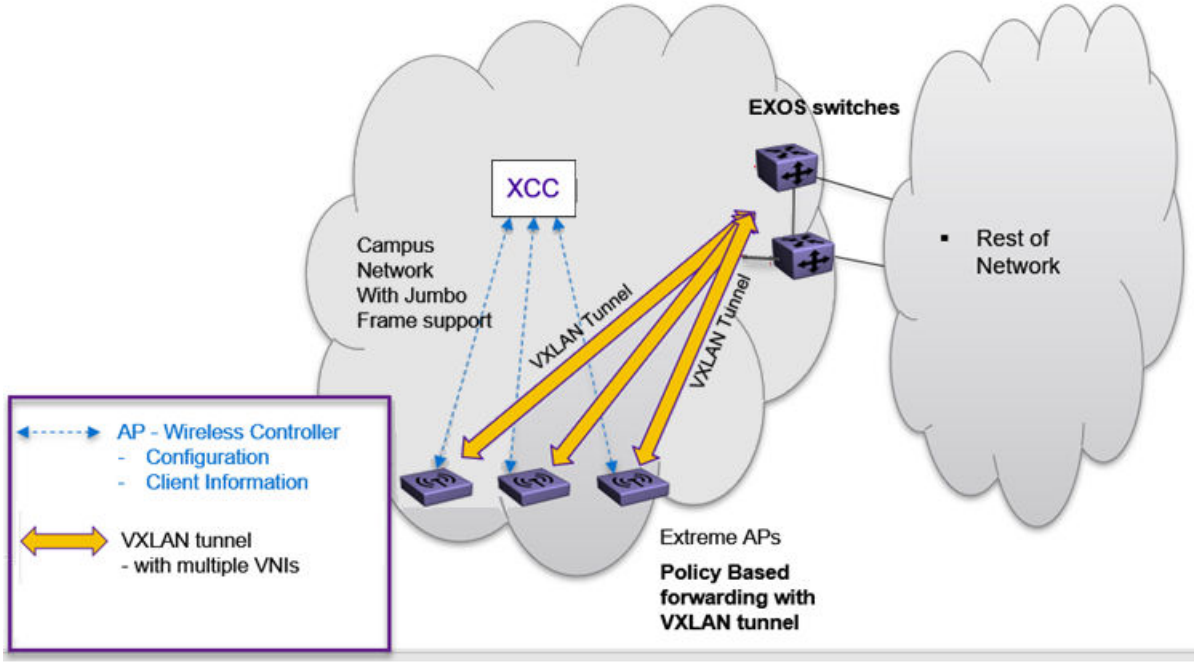


Figure 71: VxLAN Topology

Related Topics

Configuring a VxLAN in ExtremeCloud IQ Controller on page 311
Configuring VLANS on page 303
VxLAN ExtremeXOS Considerations on page 313

Configuring a VxLAN in ExtremeCloud IQ Controller

A VxLAN topology in ExtremeCloud IQ Controller can be supported in the following configurations:

- A default VLAN for policy roles

- Contain to VLAN action for policy rules
- A default VLAN for network configuration

VxLAN is supported on a Centralized network with Jumbo-Frame support. You are not required to explicitly enable Jumbo Support on the AP. The network path that the tunnel will traverse, from AP to VTEP switch must be provisioned for Jumbo Frame support for at least 1550 byte packets. The AP does not require a special setting for handling larger frames towards the clients. The AP and switches must be at least one hop away, and all devices between the AP and the ExtremeXOS switch must allow Jumbo-Frame of IP 1550 bytes.

The following ExtremeXOS switches and APs support a VxLAN topology:

- **ExtremeXOS Switches:**
  - X465
  - X590
  - X690
  - X695
  - X870
  - X670-G2
- **ExtremeWireless access points:** Wi-Fi 6 AP models with firmware version WiNG 7.4.0 or later.

When configuring a VxLAN topology, configure only one VNI and one VTEP (switch IP address). If you have a VNI that associates with more than one VTEP (switch IP address), you must configure a separate VxLAN topology. You can use the same VNI, but associate it to a different VTEP (switch IP address).

Due to a hardware limitation of 512 access points per switch, configure more than one VxLAN topology in a deployment that manages more than 512 access points. Each topology configuration can use the same VNI with a different VTEP.

Note
The VLAN ID in the VxLAN topology is shared within the Bridge@AP VLAN ID pool. The VLAN ID cannot be duplicated among the Bridge@AP, Fabric Attach, and VxLAN topologies for the same AP. ExtremeCloud IQ Controller does not allow a duplicate VLAN ID per site.

To configure a VxLAN topology in ExtremeCloud IQ Controller:

- Go to **Configure** > **Policy** > **VLANs**.
- Select **Add** and configure the VLAN parameters.

Related Topics

Configuring VLANS on page 303
VxLAN ExtremeXOS Considerations on page 313

VxLAN ExtremeXOS Considerations

Consider the following items before configuring a VxLAN topology with ExtremeXOS switches:

- The physical interface that handles the ExtremeXOS local endpoint IP address must be different than the attached physical port for the Tenant VLAN for VxLAN VNI. You must have at least two trunk ports to separate local endpoint traffic and tenant VLAN traffic.

  Example:

  ```
  configure vlan VLAN_3000 add ports 48 tagged
  configure vlan VLAN_3000 ipaddress 10.47.1.104 255.255.254.0
  configure virtual-network local-endpoint ipaddress 10.47.1.104 vr "VR-Default"

  configure vlan VLAN_3105 add ports 47 tagged
  configure virtual-network "IDAP" vxlan vni 8192
  configure virtual-network "IDAP" add vlan VLAN_3105
  configure virtual-network IDAP add remote-endpoint vxlan ipaddress 10.47.100.100 vr
  VR-Default
  configure virtual-network IDAP add remote-endpoint vxlan ipaddress 10.47.100.108 vr
  VR-Default
  configure virtual-network IDAP add remote-endpoint vxlan ipaddress 10.47.100.109 vr
  VR-Default
  ```

- A remote endpoint (AP) must be at least one hop away from the ExtremeXOS local endpoint.

  The configuration must include at least one gateway router between the AP and the switch. The gateway must enable IP MTU (Maximum Transmission Units) of 1550 bytes.

  Example:

  ```
  configure vlan VLAN_3000 add ports 48 tagged
  configure vlan VLAN_3000 ipaddress 10.47.1.104 255.255.254.0
  configure virtual-network local-endpoint ipaddress 10.47.1.104 vr "VR-Default"

  configure vlan VLAN_3105 add ports 47 tagged
  configure virtual-network "IDAP" vxlan vni 8192
  configure virtual-network "IDAP" add vlan VLAN_3105
  configure virtual-network IDAP add remote-endpoint vxlan ipaddress 10.47.100.100 vr
  VR-Default
  configure virtual-network IDAP add remote-endpoint vxlan ipaddress 10.47.100.108 vr
  VR-Default
  configure virtual-network IDAP add remote-endpoint vxlan ipaddress 10.47.100.109 vr
  VR-Default
  ```

GRE Topology

A Generic Routing Encapsulation (GRE) topology traverses wireless client traffic from a campus AP to a locally managed Extreme Networks VPN Concentrator or 3rd party GRE terminating device. GRE tunneling supports traversing client traffic through positioned access points at a location separated from ExtremeCloud IQ Controller.

The GRE Point-to-Point tunneling feature makes use of the Internet Control Message Protocol (ICMP). This is a network level protocol that communicates network connectivity issues back to the source of the compromised transmission. When more than one GRE concentrator is configured on a topology, access points use ICMP ping

to check connectivity between the access point and the GRE concentrator. When the ICMP ping to concentrator fails, the access point selects the next configured concentrator as a destination for the GRE tunnel. The communication ports on each device must be open to allow ICMP communication between the access points and GRE concentrators.

Supported APs

The following Universal Access Points support GRE Point-to-Point Tunneling:

- AP3000/X
- AP302W
- AP305C/CX
- AP305C-1
- AP4000
- AP4000-1
- AP410C
- AP410C-1
- AP460C/S6C/S12C
- AP5010
- AP5050U/AP5050D

Note
Performance can vary depending on the AP model.

APs communicate through the GRE tunnel. Although each AP can support many GRE topologies, a single assigned topology supports three concentrators. IPv6 is not supported.

Each AP issues a ping to the GRE concentrator to determine reachability. If there is no response within 30 seconds, the AP fails over to a backup concentrator.

AP Events

The following AP events address tunnel status:

- Connection is Up (Info) — An event is generated when the connection to any VPN Concentrator is established.
- Connection is Down (Major) — An event is generated when the connection is lost to a particular concentrator.

Note
It is a best practice to configure more than one VPN Concentrator per VLAN topology for failover. A topology that uses a single generic (non-encrypted) GRE tunnel, without configured backups, is not using the available mechanisms to detect if a VPN Concentrator is down. Therefore, no AP alarms, related to the tunnel connectivity, are generated for such a topology.

Related Topics

Configure a GRE Topology on page 315

Configure VPN Concentrators on page 248
GRE Point-to-Point Tunnel on page 28
View All AP Events on page 381

Configure a GRE Topology

Configure a Generic Routing Encapsulation (GRE) topology on ExtremeCloud IQ Controller. The VPN Concentrator must be configured in ExtremeCloud IQ Controller before it can be used to define a GRE tunneled topology.

To configure the GRE VLAN topology:

1. Go to **Configure** > **Policy** > **VLAN**.
2. Configure the following parameters:

   VLAN Name

   Name of the GRE VLAN

   Mode

   Select **GRE** for a Generic Routing Encapsulation (GRE) tunnel.

   VLAN ID

   The ID of the VLAN. This value must be unique.

   Tagged

   Specify if the egress port traffic is tagged or untagged. Most GRE VLAN topologies must be tagged. Each concentrator can support only one *untagged* topology. Select **Tagged** to tag the topology.

   Concentrators

   List of VPN Concentrators.

   Select a concentrator from the list, then select **Add**. You can add up to three concentrators to a single topology. When more than one termination point is added to the list, failover is supported.

   The order of the termination points is significant. The primary concentrator must be the first termination point in the list. The AP issues a ping request to the first termination point. If that request fails, it pings the second point, and then the third point. With this organization, you can use the same three concentrators for multiple VLANs, and by varying the termination point order for each VLAN, you can balance the traffic load.

   Note
   It is a best practice to configure more than one VPN Concentrator per VLAN topology for failover. A topology that uses a single generic (non-encrypted) GRE tunnel, without configured backups, is not using the available mechanisms to detect if a VPN Concentrator is down. Therefore, no AP alarms, related to the tunnel connectivity, are generated for such a topology.

Related Topics

GRE Point-to-Point Tunnel on page 28

VLAN Groups

A VLAN group can be associated with a single wireless network. In a large venue, a VLAN group can support many wireless clients on a single WLAN. The wireless client can associate with any VLAN in the group. The association is determined by a MAC address hashing algorithm.

Note
Bridged@AC topologies using AP39xx access points are supported.

To access VLAN Groups, go to **Configure** > **Policy** > **VLAN Groups**.

- Select a group to view or edit.
- Select **Add** to add a new group.

Consider the following with VLAN Groups:

- Bridged@AP and Fabric Attach topologies are not supported.
- In the case of a VLAN ID conflict, the member VLAN ID takes precedence over the group VLAN ID.

Related Topics

VLAN Group Settings on page 316

VLAN Group Settings

To create a VLAN Group:

1. Go to **Configure** > **Policy** > **VLAN Groups**.
2. Click **Add**.
3. Configure the following parameters:

   Name

   Group name.

   Mode

   - **Bridged@AC** topologies using AP39xx access points are supported.

     Note
     You cannot modify the group mode after the group is created.

   VLAN ID

   ID for the VLAN Group

   VLANs

   List of configured VLANs that can be added to the group. Select a VLAN from the list and click the plus sign to add the VLAN to the group.
4. Click **Save**.

Related Topics

VLAN Groups on page 316

Configuring Rates

You can set a data transfer rate for a policy.

To configure rates:

1. Go to **Configure** > **Policy** > **Rates**.
2. Select **Add** or select an existing rate from the list.
3. Configure the following parameters:

   Average Rate (CIR)

   The rate at which the network supports data transfer under normal operations. It is measured in kilobits per second (Kbps).

   The supported rate for ExtremeCloud IQ Controller is 500,000 Kbps.
4. Select **Save**.

Automatic Adoption

The adoption feature simplifies the deployment of a large number of access points and switches. A set of rules defines the device group assignment for new devices, when they register for the first time. Without adoption rules defined, you must manually select each device for inclusion in a device group.

Note
Without adoption rules, when a device group configuration matches the device license domain and model number, ExtremeCloud IQ Controller prompts you to add the devices, but you must manually select each device for inclusion in the device group.

Adoption rules support the following:

- Automatic adoption of access points and switches based on matching criteria
- Site and device group assignment based on matching criteria
- Device adoption denial based on matching criteria
- Device redirection to a different ExtremeCloud IQ Controller
- Site and a device group assignment based on a partial match of the FQDN or DNS suffix
- Event Logging of the device adoption process

Related Topics

Configure AP Adoption Rule on page 319
Configure Switch Adoption Rule on page 319
Pattern-Based Matching on page 320
Configure Adoption Based on FQDN or DNS Suffix on page 321
Configure Device Redirection on page 322

Adoption Rules

To avoid a manual process, create adoption rules before you register devices. Adoption rules organize access points and switches based on preset conditions or rules.

When you are ready to register one or more devices:

1. Create the logical device groups for the access points within a site.
2. Configure the adoption rules that populate the groups.
3. Register the devices.

The APs are organized into the logical sites and device groups automatically, based on the adoption rule definitions. Switches are associated with the logical sites, but not assigned to device groups. Rules are evaluated from the top down. Use the up and down arrows to put adoption rules in a specific order. If the device does not match the criteria of the first adoption rule, then the next rule is evaluated.

Note
For AP adoption only — In addition to matching rule criteria, the site and device group configuration must match the AP for the adoption rule to take effect. The AP license domain must match the site Country, and the AP model number must match the site Type and device group Profile configuration.

Related Topics

Adding or Editing Adoption Rules on page 318
Deleting Adoption Rules on page 324

Adding or Editing Adoption Rules

Adoption rules filter on one or more of the following network attributes:

- Model — Matching criteria is a sub-string. For example, if filter criteria is FCC, all APs with FCC in the model number will match.
- Host Name — Matching criteria is a sub-string.
- IP Address / CIDR — Enter a single IP address for each rule. The range for CIDR is 0 to 32. If the CIDR is 0, the IP address will not be used as a matching criteria.
- Serial Number — Matching criteria must be an exact string. Enter a single serial number for each rule.

Note
To successfully match an adoption rule, all specified parameters must match.

To add or edit an adoption rule:

1. Go to **Configure** > **Adoption**.
2. To add a new rule, select **Add**.
3. To edit an existing rule, select an adoption rule in the list, and then select ✎.

Related Topics

Configure AP Adoption Rule on page 319

Configure AP Adoption Rule

Specify a site and device group when creating an AP adoption rule.

1. Go to **Configure** > **Adoption** > **Add**.

   The **New Rule** dialog displays.
2. To create a rule for access points, select **AP**.
3. For **Action**, select one of the following values:
   - Allow
   - Deny
   - Redirect
4. Select the site associated with the adoption rule.

   The site holds the device group. The device group includes the APs that meet the filter criteria.

   Pattern-Based refers to adopting access points based on their domain. For more information, see Pattern-Based Matching on page 320.
5. Select a device group that will contain the APs that meet the filter criteria.
6. Select a filter parameter, and then select .

Note
Each filter value can only be applied once to a single rule.

Related Topics

Configure Switch Adoption Rule

Specify a site when creating a switch adoption rule. The device group does not apply to switches.

1. Go to **Configure** > **Adoption** > **Add**.

   The **New Rule** dialog displays.
2. To create a rule for switches, select **Switch**.
3. For **Action**, select one of the following values:
   - Allow
   - Deny
   - Redirect
4. Select a site.

5. Select a filter parameter, and then select .

Related Topics

Adoption Rule Filters on page 323
Configure Device Redirection on page 322

Pattern-Based Matching

In standard adoption rules, a site and device group are explicitly specified. In Pattern-Based matching, site and device group assignment is defined based on variables that represent the FQDN and DNS-Suffix of the device. The device reports to ExtremeCloud IQ Controller. The assignment is based on the matching criteria for the $FQDN or $DNS-SUFFIX variables.

Note
Before you define a Pattern-Based adoption rule, you must create a site and device group using a name that will match the name defined by the variables. Coordinate your variable definitions with the names of your existing sites and device groups. Then, create the adoption rules configuring variables with specific index definitions that will result in a match to the site name or device group name that you created.

An adoption rule is comprised of a filter definition and a site and device group definition. First, the rule matches the device attributes to the defined filter criteria. Then the rule assigns those devices to a site or device group based on the $FQDN or $DNS-SUFFIX variable values that match existing sites and device groups.

The FQDN and DNS suffix must follow a consistent format for Pattern-Based matching to be successful. One Pattern-Based rule definition can assign devices to any number of configured sites and device groups based on successful variable matches. When the defined pattern *does not* match an existing site or device group, an error is logged and ExtremeCloud IQ Controller continues evaluating the next adoption rule.

Examples: Variable Definitions

`$FQDN[x:y]`

Uses the sub-string of the Fully-Qualified Domain Name reported by the device, from character at position x to character at position y. The first character is position 1 (not 0). The value of y must be greater than or equal to the value of x.

Site example — Use this variable `$FQDN[x:y]` to specify a site. My existing site is named SITE_RDU. I define my site variable pattern as SITE_$FQDN[6:8]. The AP reports the FQDN as “ap510RDU.cath.extremenetworks.com”. Based on the variable definition index [6:8], the AP is assigned to site named SITE_RDU. Because I have a site named SITE_RDU, this AP will be placed in a device group within that site. For Pattern-Based matching to work in this example, you must have a site previously configured that is named "SITE_RDU". If that site does not exist, an error is logged and the rules engine continues evaluating adoption rules.

Device Group example — Specify a device group pattern “AP510-$FQDN[6:8]”. The AP reports a FQDN as “ap510RDU.cath.extremenetworks.com”. Based on the variable definition index [6:8], the AP is assigned to the device group named AP510-

RDU. For Pattern-Based matching to work, in this example, you must have a device group previously configured that is named AP510-RDU. If that device group does not exist, an error is logged and the rules engine continues evaluating adoption rules.

$DNS-SUFFIX[x:y]

Uses the sub-string of the Domain Name Server suffix reported by the device, from character at position x to character at position y. The first character is position 1 (not 0). The value of y must be greater than or equal to the value of x. The DNS suffix is the FQDN with the hostname removed. When the AP reports the FQDN “ap510i.RDU.extremenetworks.com”, then the DNS suffix is “RDU.extremenetworks.com”.

My existing site is named Site_RDU. My variable is defined as Site_$DNS-SUFFIX[1:3]. Variable index [1:3] results in a site named Site_RDU. Characters 1 to 3 in the DNS suffix results in RDU.

If you are consistent with the naming convention for sites, device groups, and FQDNs, you will be able to use one rule to assign any AP regardless of the specific AP model or domain name.

Related Topics

Configure Adoption Based on FQDN or DNS Suffix on page 321

Configure Adoption Based on FQDN or DNS Suffix

Adoption rules are simplified using a Pattern-Based site. The Pattern-Based adoption rule enables you to adopt devices based on their domain. Using a Pattern-Based site, the number of `Allow` rules can be reduced significantly.

Note
Before you can create adoption rules, you must create the sites and device groups to which your adoption rules will apply. You must use consistent naming conventions that match your variable definitions for Pattern-Based matching to be successful.

1. Create a site and device group that will hold your access points or switches.

   Consider the full name of the site and device group when configuring the Pattern-Based matching variables.
2. Go to **Configure** > **Adoption** > **Add**.

   The **New Rule** dialog displays.
3. Select the device type:
   - To create a rule for access point adoption, select **AP**.
   - To create a rule for switch adoption, select **Switch**.
4. From the **Action** field, select a rule action. Valid values are:
   - Allow
   - Deny
   - Redirect

5. In the **Site** field, select **Pattern-Based**.

   An additional field displays.
6. Configure a site name using FQDN or DNS-Suffix variables (for example, `Site_$FQDN[x:y] or Site_$DNS-SUFFIX[x:y]`).
7. For AP adoption rules only — specify a device group.

   When using a Pattern-Based site, manually enter the device group name. Configure a device group name using Pattern-Based variables: FQDN or DNS-Suffix. For example, `AP510_$FQDN[x:y] or AP510_$DNS-SUFFIX[x:y]`, or provide an explicit device group name. You can use an explicit device group name with a Pattern-Based site.

   Note
   It is important that you configure the Pattern-Based matching variables using a consistent naming convention that matches the names of your existing sites and device groups. For more information and examples, see Pattern-Based Matching on page 320.
8. Select a filter parameter, and then select .

First the devices must match the filter definition, then they are placed in a site and device group that matches the defined pattern.

Pattern-based adoption rule

Where variable definition is:

```
SITE-$FQDN[1:7]
```

When the destination site is defined using the FQDN, the site name is composed of the prefix SITE and positions 1-7 of the FQDN.

```
SITE-$DNS-SUFFIX[4:7]
```

When destination site is defined using the DNS suffix, the site name is composed of the prefix SITE and positions 4-7 of the DNS Suffix.

Related Topics

Adoption Rule Filters on page 323
Pattern-Based Matching on page 320

Configure Device Redirection

You can configure an adoption rule that redirects devices to another appliance when matching criteria are met.

Note
AP39xx access points do not support adoption rule redirection where the redirected destination is defined as an FQDN. AP39xx only supports a redirected destination that is defined as an IPv4 address.

1. Go to **Configure** > **Adoption** > **Add**.

   The **New Rule** dialog displays.

2. Select the device type:
   - To create a rule for access point adoption, select **AP**.
   - To create a rule for switch adoption, select **Switch**.
3. From the **Action** field, select **Redirect**.

   The **IP Address** field is displayed.
4. Provide the IP address of the destination ExtremeCloud IQ Controller.
5. Select a filter parameter, and then select .

Note
Devices that match filter criteria on a redirect action do not connect to ExtremeCloud IQ Controller initially. They are redirected to another ExtremeCloud IQ Controller. If the destination ExtremeCloud IQ Controller contains adoption rules with filter criteria that match the redirected devices, the devices are adopted by the destination ExtremeCloud IQ Controller. You must configure adoption rules on the second appliance as a separate action from the redirection. Adoption to the second appliance is not included in the redirect action.

Related Topics

Adoption Rule Filters on page 323

Adoption Rule Filters

The filter parameters for an adoption rule depend on the type of device associated with the rule and the defined action. Rules can be configured for device adoption, denial, and redirection to a different ExtremeCloud IQ Controller.

IP Address/CIDR

Filter the APs or switches by IP address, adopting APs into the specified device group based on their IP address. CIDR field is used along with IP address field to find the IP address range.

For switch adoption rules, specify the management IP address.

Host Name

Filter the APs by host name, adopting APs into the specified device group based on their host name. This field matches on sub strings.

For switch adoption rules, use the system name. The full host or system name is not required for a match.

Model

Model number on the device. This field matches on sub strings. The full model number is not required for a match.

Serial Number

Serial number on the device. Serial number requires an *exact* string match.

Note
Each filter value can only be applied once to a single rule.

Related Topics

Adding or Editing Adoption Rules on page 318
Adoption Rules on page 318
Deleting Adoption Rules on page 324

Deleting Adoption Rules

Adoption rules can be deleted.

Note
When a device group is deleted, all the AP adoption rules that reference that device group are deleted from ExtremeCloud IQ Controller.

To delete an adoption rule:

1. Go to **Configure** > **Adoption** and select on an adoption rule in the list.
2. Select .

   A confirmation dialog displays.
3. Select **OK**.

Related Topics

Adoption Rules on page 318

ExtremeGuest Integration

Use ExtremeGuest™ as an External Captive Portal Server to create and monitor External Captive Portals.

Note
The ExtremeCloud IQ Controller Network Access Control (NAC) Rules Engine is not invoked for clients on a WLAN Network that is configured to use the ExtremeGuest Server.

The Network Access Server (RADIUS client) on ExtremeCloud IQ Controller handles the RADIUS transactions. RADIUS transactions are not relayed by NAC on ExtremeCloud IQ Controller.

ExtremeGuest integration within ExtremeCloud IQ Controller:

- To configure the ExtremeGuest server, select **Add**.
- To configure the ExtremeGuest captive portal settings, go to **Configure** > **Networks** > **Add**. Then, select **Enable Captive Portal**.

Related Topics

ExtremeGuest Server Settings on page 325
ExtremeGuest Captive Portal Settings on page 283

ExtremeGuest Server Settings

To configure the ExtremeGuest server, take the following steps:

1. Go to **Configure** > **ExtremeGuest** and select **Add**.
2. Configure the following parameters:

IP Address

IP address of the ExtremeGuest server.

Name

Name of the ExtremeGuest server.

FQDN

Fully-qualified domain name of the ExtremeGuest server.

Authentication Timeout Duration (Seconds)

Determines a timeout value, in seconds, for the RADIUS server connection.

Authentication Retry Count

Determines the number of times ExtremeCloud IQ Controller will attempt to authenticate an end user.

Authentication Client UDP Port

User Datagram Protocol (UDP) port number used for client authentication. UDP needs only one port for full-duplex, bidirectional traffic.

Shared Secret

The password that is used to validate the connection between ExtremeCloud IQ Controller and the ExtremeGuest server.

Mask — Determines if the Shared Secret or password value is displayed on the user interface. Enable Mask to display dots in place of the Shared Secret or password value. To display the password characters, clear the **Mask** check box.

Callback User Name

User ID that Callback Manager uses to access the ExtremeGuest server.

Callback Password

The password that Callback Manager uses to access the ExtremeGuest server. The minimum password length is 6 characters.

Mask — Determines if the Shared Secret or password value is displayed on the user interface. Enable Mask to display dots in place of the Shared Secret or password value. To display the password characters, clear the **Mask** check box.

Related Topics

ExtremeGuest Captive Portal Settings on page 283
ExtremeGuest Integration on page 324

Callback Manager

Callback Manager is an ExtremeCloud IQ Controller component that supports the integration of ExtremeCloud IQ Controller and ExtremeGuest. Callback Manager

supports a Centralized site deployment only. It can report the following configuration changes to an ExtremeGuest server:

- Centralized site configuration changes
- AP configuration changes for APs associated with a Centralized site
- Network configuration changes for networks that are associated with a Centralized site.

Note
The ExtremeGuest user configures the report requests for each ExtremeGuest server.

Multiple servers are supported, and each server can request a different report.

To report configuration changes:

1. Callback Manager logs into the registered ExtremeGuest server over a secure http server (https):
2. Callback Manager receives the ExtremeGuest server request.
3. Callback Manager posts the requested configuration changes.
4. ExtremeGuest saves the changes.

Configure the User ID and password that Callback Manager uses to access the ExtremeGuest server on the **ExtremeGuest Server Settings** page.

If an ExtremeGuest server is unreachable, Callback Manager retries connection every few minutes. After the server is reached, Callback Manager sends the latest configuration changes. In this scenario, changes can be missed while the server is unreachable, but upon connection, the server receives the latest configuration information.

The reporting process is persistent after an ExtremeCloud IQ Controller restart. After the appliance is restarted, Callback Manager continues to report changes that it had yet to report.

Related Topics

ExtremeGuest Server Settings on page 325

AAA RADIUS Authentication

You have options when configuring AAA Authentication:

- Use the local Network Access Control (NAC) to terminate or proxy a RADIUS authorization and accounting request.
- Use the local Network Access Server (NAS) to distribute RADIUS requests.

If you are going to authenticate with the Local Named Repository, opt for configuring authentication through the local NAC. If you are going to use an external RADIUS server, you have the option to configure the RADIUS server through the local

NAC, through the local NAS, or connect directly to the RADIUS server, bypassing ExtremeCloud IQ Controller.

- To configure AAA Policy for external RADIUS, bypassing ExtremeCloud IQ Controller, go to **Configure** > **AAA Policy**.
- To configure AAA RADIUS servers within the local NAC, go to **Onboard** > **AAA**.

The RADIUS Authorization and Accounting transactions occur between the Network Access Server (NAS) on ExtremeCloud IQ Controller and the RADIUS server without involving NAC.

However, you have the option to configure Access Control Rules within the local NAC, making use of automated policy management. Access Control Rules enable you to apply network access permissions and restrictions based on defined rules. The rules can address network resources, a user's role or purpose in the organization, or the device type that is used to access the network. Network access control is dynamic. End-user network access can change as group associations change without a network administrator getting involved.

Regardless of the RADIUS configuration method you choose, you can easily configure RADIUS attributes and find support for RADIUS Change of Authorization (CoA).

Related Topics

Configure AAA Policy on page 327
Onboard AAA Authentication on page 334
Access Control Rules on page 361

Configure AAA Policy

You can create a AAA Policy that can be referenced through a WLAN Service, bypassing the local Network Access Control on ExtremeCloud IQ Controller.

Note
AAA Policy can only be configured for WLAN networks requiring MACAUTH, External Captive Portal, or EAP.

To configure a AAA network policy:

1. Go to **Configure** > **Networks** > **WLANs** and select a network.
   AAA Policy is displayed for WLAN Networks that require authentication or authorization. The value **Local Onboarding** refers to RADIUS requests that are directed through the ExtremeCloud IQ Controller. Local Onboarding is the default value for WLAN Networks configured for Internal Captive Portal.
2. Select an **Auth Type**.
   The AAA Policy field displays.
3. From the AAA Policy field, select to add a new policy, or select to edit a policy.
4. Configure the following parameters:
   Name
   Policy name.
   Authentication Protocol

Authentication protocol type for the RADIUS server (PAP, CHAP, MS-CHAP, or MSCHAP2).

NAS IP Address

IP address of the Network Access Server (NAS).

NAS ID

A RADIUS attribute that identifies the client to a RADIUS server. The NAS-Identifier can be used instead of an IP address to identify the client.

Call Station ID

Identifies a group of access points. The Call Station ID is often configured in a large network using an external NAC or RADIUS server. Possible values are:

- Wired MAC: SSID
- BSSID (APs supported on a Centralized site only)
- Site Name
- Site Name: Device Group Name
- AP Serial Number

Note
Call Station ID allows for Zone authentication with a Centralized site.

- Site Campus
- Site Region
- Site City

Accounting Type

Determines when the appliance generates the accounting request. Valid values are:

- Start-Interim-Stop — Start record after successful login by the wireless device, interim record, and an accounting stop record based on session termination.
- Start-Stop — Start record after successful login by the wireless device user and an accounting stop record based on session termination.

The appliance sends the accounting requests to a remote RADIUS server.

Wait for client IP before starting accounting procedure

By default, the Accounting Start record is generated when the client is authenticated. Enable this setting to generate the Accounting Start record when the client acquires a non local IP address. Use this option for captive portals, which use RADIUS Accounting to learn of the client IP address before providing the landing page.

Accounting Interim Interval

The number of seconds (60-3600) between each interim update for a specific session. Default value is 60.

RADIUS Authentication Servers Mode

Select the availability behavior for RADIUS servers. Valid values are: **Failover** or **Load Balance**.

AAA Policy supports the ability to load balance RADIUS requests across target servers in a load-balancing pool. (A minimum of two servers is required.) Each client authentication session begins and ends on a single RADIUS server. The ExtremeCloud IQ Controller validates that each server can be reached and logs an alert when a server in the pool is unreachable. The server pool is readjusted based on the status of each server in the pool.

Note
Configure one server for both Accounting and Authentication purposes.

When this setting is set to **Failover**, a RADIUS request is sent to one server at a time:

- The RADIUS request is sent to the Primary server (based on the RADIUS server order in the AAA policy).
- When the Primary server is not accessible, the request is sent to the second server (the Failover server).
- When the Primary server is accessible, the request is automatically sent to the Primary server instead of the Failover server.

Note
The RADIUS Status message (RFC 5997) indicates if the RADIUS server is accessible.

When this setting is set to **Load Balance**, a RADIUS request is sent in round robin fashion:

- When a RADIUS server is not accessible, ExtremeCloud IQ Controller stops sending requests to that server.
- When a server is accessible, the server is added to the pool of servers.

Note
The RADIUS Status message (RFC 5997) indicates if the RADIUS server is accessible.

Note
There is no correlation between the RADIUS server that is used for authentication and the RADIUS server that is used for accounting.

RADIUS Accounting Servers Mode

Determines the server selection mode when accounting packets are sent to a single server. When the selected accounting server does not respond to the accounting requests, the accounting packets are sent to the next configured

accounting server. The selection applies to all Services and to all sites on ExtremeCloud IQ Controller.

- **Round-Robin** — The server is selected on a round-robin basis starting at the top of the list of approved servers. The first server is used until it fails, and that pattern continues down the list. When the last server fails, then the first server is used again.
- **Broadcast** — RADIUS accounting packets are sent to all configured accounting servers in the AAA Policy.

  For controllers in an availability pair, the primary and backup servers must be synchronized when the WLAN Services are synchronized. (For more information, see Availability Pair Settings on page 449. If the primary server has failed resulting in a backup server being used for authentication, the controller periodically sends a "Health Check" to the primary server to see if it has recovered. If the primary server has recovered, the controller starts using the primary server for all new authentications. All authentications in progress continue to use the backup server.

Note
There is no correlation between the RADIUS server that is used for authentication and the RADIUS server that is used for accounting.

Include Framed IP

Select this option to include the FRAMED-IP attribute value pair in the RADIUS ACCESS-REQ message. You can include the user IP address in the RADIUS ACCESS-REQ through the FRAMED-IP attribute. This can extend user access reporting capabilities. Framed IP is supported by External Captive Portal only. Centralized Web Authentication does not support Framed IP.

Report NAS Location

Sends Network Access Server (NAS) Location per the RFC5580 Out of Band agreement. After a NAS Location change, the new NAS Location is reported in the next RADIUS Request or RADIUS Accounting message.

Note
Mid-session requests and the Initial Server Request for Location as described in RFC5580 are not supported.

The following additional attribute value pairs (AVP) used by RFC5580 are supported:

- LOCATION-INFO
- LOCATION-DATA

Note
Site Location details are reported in LOCATION-DATA. For more information on Site Location information, see Site Location on page 132.

- BASIC-LOCATION-POLICY-RULES
- OPERATOR-NAME (Described below)

Override Reauthentication Timeout

Enable this setting to override the reauthentication period that is returned by the RADIUS server. When reauthentication is enabled, the timeout value that is returned by the RADIUS sever is overwritten with the value that is specified here. Valid values for the Override Reauthentication Timeout are 60-300 seconds.

Block repeated failed Authentications

Enable this setting to minimize the RADIUS server load that is created by repeated authentication requests and failures. Authentication requests from a client are blocked for a configurable period of time. While blocked, RADIUS requests from the client are ignored. This setting applies to a specific WLAN. The client can continue to send authentication requests on a different WLAN.

Consecutive failed Authentications must be received at the ExtremeCloud IQ Controller in the **Elapsed time for failed Authentications (Seconds)** for the **Quiet Timeout (Seconds)** to start. After the quiet timeout expires, the client's RADIUS requests are forwarded to the RADIUS server again.

When enabled, the following settings display:

Consecutive failed Authentications

The number of failed authentication attempts. Valid values are 1 to 10. Default value is 5.

Elapsed time for failed Authentications (Seconds)

The threshold in seconds that determines if the client authentication requests are blocked. This is the window of time in which the failed authentication attempts occur. Valid values are 1 to 10 seconds. The default value is 3 seconds.

Quiet Timeout (Seconds)

The amount of time that authentication requests from the client are blocked before its RADIUS requests are forwarded to the RADIUS server again. Valid values are 1 to 300 seconds. The default value is 300 seconds (5 minutes).

By default, if 5 attempts are made within 3 seconds, the client authentication requests are blocked for 300 seconds (5 minutes), and RADIUS requests from that client are ignored. After 5 minutes, client RADIUS requests are forwarded to the RADIUS server again.

Note
In Failover mode, the Deny list is published to the peer ExtremeCloud IQ Controller.

Operator Name

RADIUS attribute composed of the operator namespace identifier and the operator name. The combination of operator name and namespace identifier

uniquely identifies the owner of an access network. The Operator Name cannot exceed 253 bytes. Valid values are:

- Tadig — Three-character Country Code followed by a two- character alphanumeric operator ID
- Realm — Registered Domain Name of Operator
- E212 — Mobile Country Code or Mobile Network Code
- OneCC — Three-character Country Code followed by 1-6 uppercase ITU Carrier Codes
- None

RADIUS Authentication Servers

To add RADIUS servers for authentication, select **Add**. You can configure up to four RADIUS servers for authentication.

RADIUS Accounting Servers

To add RADIUS servers for accounting, select **Add**. You can configure up to four RADIUS servers for accounting.

Related Topics

RADIUS Settings on page 332

RADIUS Settings

Configure the following parameters, and then select **Save**.

Protocol

Select between **Standard** (UDP) or **Secure** (RADSEC) protocol.

RADSEC supports RADIUS transactions conducted securely over TCP and TLS (RFC 6614). RADSEC is not supported with Local Onboarding, and it is not available with ADMIN access.

Server Address

The RADIUS server address. This value cannot be changed.

Trust Point

Refers to the certificate file required for the secure RADSEC protocol. When a secure RADSEC protocol is configured, the certificate file of the Access Network Provider (ANP) and its private key must also be specified. Select from the list of configured Trust Points. For information about configuring Trust Points, see Trust Points.

Timeout

Determines a timeout value, in seconds, for the RADIUS server connection.

Retries

Determines the number of times ExtremeCloud IQ Controller will attempt to authenticate an end user.

For Local Onboarding, use the **Retries** and **Timeout** values with the **RADIUS Server Health Check** parameters to detect RADIUS servers that are not responding and fail over to a second server if necessary. When Local Onboarding bypassed is enabled,

all RADIUS requests are sent to one RADIUS server until it fails; then, the next RADIUS server is used.

Port

- A User Datagram Protocol (UDP) port number used for client authentication. UDP needs only one port for full-duplex, bidirectional traffic. Select a UDP port number for standard protocol security.
- For a secure RADSEC protocol, use port **2083** This is the default port.

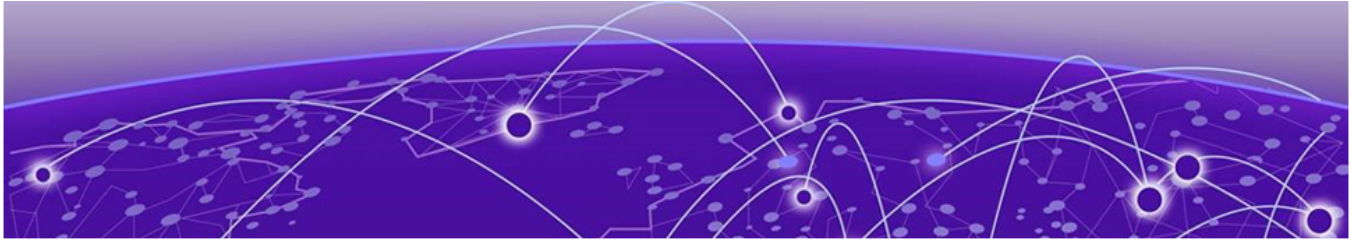
Shared Secret

The password that is used to validate the connection between the client and the RADIUS server.

For RADSEC, **radsec** is the default password.

Mask

Determines if the Shared Secret or password value is displayed on the user interface. Enable Mask to display dots in place of the Shared Secret or password value. To display the password characters, clear the **Mask** check box.



Onboard

Use the **Onboard** workbench to configure network access, including AAA configuration, captive portal configuration, access control groups, and a rules engine.

Onboard AAA Authentication

Configure network access from the **Onboard** menu, including AAA configuration, local password repository, LDAP, and captive portal configuration, access control groups, and a rules engine. The RADIUS authentication you configure from the **Onboard** workbench uses the local Network Access Control (NAC) to terminate or proxy a RADIUS authorization and accounting requests.

Related Topics

Managing RADIUS Servers on page 335
Setting Default AAA Config on page 334
LDAP Configurations on page 338
Managing The Local Password Repository on page 341
Manage Captive Portal on page 345
Manage Access Control Groups on page 358
Access Control Rules on page 361

Setting Default AAA Config

Configure authentication using one or more methods of authentication. With RADIUS and Local authentication, you have the option to configure an LDAP server as a backup. When you choose RADIUS or LDAP authentication, you have the option to authenticate MAC Addresses locally.

To specify a default configuration for AAA:

1. Go to **Onboard** > **AAA** and select **RADIUS Servers**.
2. Click **Default AAA Config**.

3. Configure the following parameters for the default configuration:

Table 83: Default AAA Configuration Parameters

Field	Description
Authentication Method	Determines the method for user authentication. Additional authentication parameters depend on the method you select here. Valid values are: • RADIUS. RADIUS Server authenticates user. • Local. ExtremeCloud IQ Controller authenticates user. • LDAP. LDAP server authenticates user. **Note:** Internal Captive Portal supports Local and LDAP authentication only, providing validation of client acceptance status based on provided credentials. Indication of a specific role for policy assignment change is not supported.
When using **RADIUS** or **LDAP** authentication	First authenticate with configured RADIUS server, then use LDAP server. Copy the Distinguished Name from the LDAP server. • Primary RADIUS — IP address of primary RADIUS server • Backup RADIUS — IP address of backup RADIUS server. • LDAP Configuration — Indicates the LDAP Configuration to use as a default. Select from one of the configured LDAP Configurations.
When using **Local** or **LDAP** authentication	First authenticate locally, then use LDAP server. Copy the Distinguished Name from the LDAP server. • LDAP Configuration — Indicates the LDAP Configuration to use as a default. Select from one of the configured LDAP Configurations.
Authenticate Locally for MAC	Authenticate the MAC address on ExtremeCloud IQ Controller. Do not authenticate MAC address on the RADIUS server.

Related Topics

RADIUS Settings on page 336
Advanced RADIUS Settings on page 337
LDAP Configuration Settings on page 339

Managing RADIUS Servers

To manage the list of RADIUS servers:

1. Go to **Onboard** > **AAA** and select **RADIUS Servers**.

   A list of configured RADIUS servers displays. From here, you can search for a server, edit server settings, delete a server, or add a new RADIUS server.

2. To edit or delete a server, select a server row.

   The server settings display.

   - To edit, modify the server settings and click **Save**.
   - To delete the server, click **Delete**.

3. To add a new RADIUS server, from the **RADIUS Servers** tab, select **Add** and configure the server settings.

Note
To support load balancing, ExtremeCloud IQ Controller allows up to four redundant RADIUS servers for accounting and four RADIUS servers for authentication.

Related Topics

Setting Default AAA Config on page 334
RADIUS Settings on page 336
Advanced RADIUS Settings on page 337

RADIUS Settings

Configure the following parameters and select **Save**.

Table 84: RADIUS Server Settings

Field	Description
RADIUS Server IP address	IP address of the RADIUS server.
Response Window	Determines the window of time, in seconds, that ExtremeCloud IQ Controller will wait for a response from the RADIUS server.
Authentication Timeout Duration	Determines a timeout value, in seconds, for the RADIUS server connection.
Authentication Retry Count	Determines the number of times ExtremeCloud IQ Controller will attempt to authenticate an end user.
Authentication Client UDP Port	User Datagram Protocol (UDP) port number used for client authentication. UDP needs only one port for full-duplex, bidirectional traffic.
Proxy RADIUS Accounting Requests	Indicates that the RADIUS server will also handle RADIUS accounting requests.
Accounting Client UDP Port	UDP port number used for client accounting. User Datagram Protocol (UDP) needs only one port for full-duplex, bidirectional traffic.
Shared Secret	The password that is used to validate the connection between the client and the RADIUS server.
Mask	Determines if the Shared Secret or password value is displayed on the user interface. Enable Mask to display dots in place of the Shared Secret or password value. To display the password characters, clear the **Mask** check box.

Related Topics

Managing RADIUS Servers on page 335
Advanced RADIUS Settings on page 337
RADIUS Configuration for Switches Per Site on page 131

Advanced RADIUS Settings

For information about advanced RADIUS configuration settings, see the following table:

Table 85: RADIUS Server Advanced Settings

Field	Description
Username Format	Determines if the domain name will be included in the username when proxying a request to the backend RADIUS server. Valid values are: • Strip Domain Name (default) - Select this option unless the backend RADIUS server requires the domain name to be included. • Keep Domain Name - Using this option with a Microsoft IAS or NPS server, may cause the server to timeout. Therefore, use an advanced AAA configuration. With a AAA configuration, only requests for known domains are sent to the backend RADIUS server. Unknown domains are processed locally and rejected.
Require Message-Authenticator	Protect against spoofed Access-Request messages and RADIUS message tampering with this attribute. The Require Message-Authenticator provides additional security when using PAP and CHAP security protocols for authentication. EAP uses the Message Authenticator attribute by default.
Health - Use Server Status Request	Use Server-Status RADIUS packets, as defined by RFC 5997, to determine if the backend RADIUS server is running.
Health - Use Access Request	Use an access request message to determine if the RADIUS server is running. The request uses a username and password. This method looks for any response from the server. The username and password do not need to be valid. A negative response will work. However, the username/password fields are provided to prevent rejects from being logged in the backend RADIUS server.
Check Interval	Determines the wait time between checks to see if the RADIUS server is running. **Note:** This is only applicable if the Server-Status request or Access request methods are used.

Table 85: RADIUS Server Advanced Settings (continued)

Field	Description
Number of Answers to Alive	Determines the number of times the RADIUS server must respond before it is marked as alive. **Note:** This is only applicable if the Server-Status request or Access request methods are used.
Revive Interval	Determines the wait time before allowing requests to go to a backend RADIUS server, after it stops responding. **Note:** Use this option only when there is no other way to detect the health of the backend RADIUS server. If Server-Status requests option and Access request option are not supported by the RADIUS server, then use this option.
Require Message-Authenticator	When enabled, the message-authenticator attribute value pair is included in the packet from the RADIUS server.
Health — Use Server Status Request	Determines if the Server Status Request is used to determine RADIUS server health upon recovery after the server has gone down. This is RADIUS status code point 12 from RFC5997.
Health — Use Access Request	Determines if the Server Access Request is used to determine RADIUS server health upon recovery after the server has gone down. This is access request code point 1 from RFC2865 with the user name/password set to `fakeuser/fakepasswd`.

Related Topics

Managing RADIUS Servers on page 335
RADIUS Settings on page 336

LDAP Configurations

LDAP (Lightweight Directory Access Protocol) is a software protocol used to locate people, organizations, or other resources in a network. LDAP can be used on a public Internet or on a corporate intranet. Configure an LDAP configuration for each LDAP server in your network.

To access or add new LDAP configurations:

1. Go to **Onboard** > **AAA** and select **LDAP Configurations**.

   A list of LDAP configurations displays. From here, you can search for a configuration, edit a configuration, delete a configuration, or add a new LDAP configuration.

2. To edit or delete a configuration, select a LDAP row.

   The configuration settings display.

   - To edit, modify the configuration settings and select **Save**.
   - To delete the configuration, select **Delete**.

3. To add a new LDAP configuration, from the **LDAP Configurations** tab, select **Add LDAP Configuration** and configure the settings.

Related Topics

LDAP Configuration Settings on page 339

LDAP Configuration Settings

Create an LDAP configuration for each LDAP server in your network.

Table 86: LDAP Configuration Settings

Field	Description
Configuration Name	Name the LDAP configuration.
LDAP Configuration URL	Connection URL for the LDAP server and any backup servers you have configured. (The backup servers are redundant servers containing the same directory information.) The format for the connection URL is ldap://host:port where host equals hostname or IP address, and the default port is 389. For example, `ldap://10.20.30.40:389`. If you are using a secure connection, the format is `ldaps://host:port` and the default port is 636. `ldaps://10.20.30.40:636`.
Administrator Username	Enter the administrator username and password used to connect to the LDAP server to make queries. The credentials only need to provide read access to the LDAP server. 802.1x authentication via LDAP requires domain membership. This requires authentication type to be NTLM and the Administrator Username to be in the format: `DOMAIN\USERNAME`.
Administrator Password	
Mask	Check this option to mask the user entered password characters with bullets. As user password requirements become more complex, consider clearing this option so users can verify entered password characters.
User Search Root	The root node of the LDAP server. To improve search performance, you can specify a sub tree node to confine the search to a specific section of the directory. Use a DN (Distinguished Name) search root format.
OU Search Root	Organizational Units search root.

Table 86: LDAP Configuration Settings (continued)

Field	Description
Schema Definition	Describes how entries are organized in the LDAP server. Click **View** to see default definitions. You can modify these definitions if necessary.
Test Configuration	Test the specified configuration. The connection to the LDAP server is tested and a report on connection test results is provided.

Related Topics

LDAP Configurations on page 338

LDAP Schema Definition Settings

Describes how entries are organized in the LDAP server. The LDAP schema is comprised of keys to find users in an LDAP directory.

Table 87: LDAP Schema Definition Settings

Field	Description
User Object Class	Name of the class for users.
User Search Attribute	Name of the attribute in the user object class that contains the user's login ID.
Keep Domain Name for User Lookup	Use the full username when looking up the user in LDAP. For example, select this option when using the User Search Attribute: userPrincipalName.
User Authentication Type	Specifies the user authentication. Valid values are: • LDAP Bind – Only works with a plain text password. It is useful for authentication from the captive portal but does not work with most 802.1x authentication types. • NTLM Auth – This option is only useful when the backend LDAP server is a Microsoft Active Directory server. This is an extension to LDAP bind that will use ntlm_auth to verify the NT hash challenge responses from a client in MsCHAP, MsCHAPV2, and PEAP requests. • NT Hash Password Lookup – If the LDAP server has the user's password stored as an NT hash that is readable by another system, you can have Identity and Access read the hash from the LDAP server to verify the hashes within an MsCHAP, MsCHAPV2, and PEAP request. • Plain Text Password Lookup – If the LDAP server has the user's password stored unencrypted and that attribute is accessible to be read via an LDAP request, then this option reads the user's password from the server at the time of authentication. This option can be used with any authentication type that requires a password.

Table 87: LDAP Schema Definition Settings (continued)

Field	Description
User Password Attribute	This is the name of the password used with the NT Hash Password Lookup and Plain Text Password Lookup listed above.
Host Search Class	Indicates the class used for hostname.
Host Search Attribute	Indicates the name of the attribute in the host object class that contains the hostname.
Use Fully Qualified Domain Name	Select this option to use the Fully Qualified Domain Name (FQDN). Clear this option to use the hostname without domain.
OU Object Classes	Organizational Unit Object Classes

Related Topics

LDAP Configurations on page 338

LDAP Test Results

Test the LDAP configuration to verify the LDAP connection, search for a user, and search for a host. Use this information to troubleshoot LDAP connections.

The **Connection Test** tab displays results for the following:

- Active Directory Domain
- User Search
- Host Search
- OU Test

Search for specific users or specific Host addresses from the **User Search** tab and the **Host Search** tab respectively. Details about the search criterion are displayed.

Managing The Local Password Repository

ExtremeCloud IQ Controller gives you the option to store user accounts in a local password repository in place of configuring one or more remote RADIUS servers or remote LDAP servers to handle network authentication.

Note
The Admin account that you create here, from **Onboard** > **AAA** > **Local Password Repository**, applies to the local captive portal.

This Admin account is separate from your ExtremeCloud IQ Controller system account. System accounts are managed from **Administration** > **Accounts**.

Note
When using local password authentication, you may also want to configure LDAP for additional user information.

Take the following steps to add new user accounts to the local repository:

1. Go to **Onboard** > **AAA** and select **Local Password Repository**.

   A list of user accounts displays. From here, you can search for, edit, delete, or add a new account.
2. To edit or delete an account, select an account row.

   The account settings display.
   - To edit the account, modify the account settings and select **Save**.
   - To delete the account, select **Delete**.
3. To add a new account, from the **Local Password Repository** tab, select **Add User** and configure the user account settings.

Related Topics

User Account Settings on page 342

User Account Settings

Configure the following user account settings and select **Save**.

Note
The Admin account that you create here, on the **Onboard** workbench, applies to the local captive portal. When using captive portal, manage account passwords from the ExtremeCloud IQ Controller **Onboard** > **AAA** > **Local Password Repository**. The default captive portal password is `Extreme@pp`.

The Admin account created here is separate from your ExtremeCloud IQ Controller system account. System accounts are managed from **Administration** > **Accounts**.

Table 88: User Account Settings

Field	Description
Enabled	Indicates if the user account is enabled. Select to enable the user account.
First Name	User's first name.
Last Name	User's last name.
Display Name	Name that displays on the user interface for the account. This can be the User name or something else.
Username	User name for the account.
Password Hash Type	Password hash function used for password hashing.
Password	Password for the account. Alphanumeric value, minimum of 6 characters. The default captive portal password is `Extreme@pp`.
Description	Text description of user account.

Related Topics

Managing The Local Password Repository on page 341

Certificates

To ensure a secure website that takes advantage of encryption, ExtremeCloud IQ Controller uses browser certificates for website security and RADIUS Server certificates for certificate-based authentication to the network and for access to a captive portal. The browser certificate ensures security between the wireless clients and a VLAN, and the RADIUS server certificates ensure security between the RADIUS server and Network Access Control.

Both types of certificates offer the option to generate a new certificate or use a certificate and key file that you have saved. You can also reset the network interface to the default certificate and key, which yields a Self-Signed certificate.

ExtremeCloud IQ Controller offers a factory installed self-signed certificate, which is used by the user interface HTTP Server to terminate the HTTPS browser requests served on port 5825. The certificate common name is *Network Services Engine*.

Related Topics

Generate Browser Certificates on page 343
Generate RADIUS Server Certificates on page 344
AAA Certificate Authorities on page 345

Generate Browser Certificates

Browser certificates are used for website security or to secure the captive portal client communications. Generate a certificate or use a saved certificate and key from one or more files.

Go to the following screens for the Certificates feature:

- **Policy** > **VLAN** for generating topology certificates
- **Admin** > **Interface** for generating certificates used for website security.

After an interface or topology is created, the **Certificates** button displays. Take the following steps:

1. Select **Certificates**.

   The **Certificates** dialog displays.

2. Select the Certificate option:
   - **Install or Replace Certificate**

     Select this option and select **Generate CSR**. Complete the online form, then generate and download the certificate that can be presented to a public certificate authority.
   - **Install or Replace certificate and key from a single file**

     Select this option and navigate to the saved certificate file. Provide the password key provided with that file.
   - **Install or Replace certificate file and key from separate files**

     Select this option and navigate to the saved certificate file and separate key file.
   - **Reset to default certificate and key**

     Select this option to clear previous certificates and reset the ExtremeCloud IQ Controller to the default configuration of the Self-Signed certificate.

Note
When certificates are applied or reset on the Admin topology, a server restart is triggered, and the browser loses connectivity with the server for a few seconds. When certificates are applied or reset on System topologies where **Management Traffic** is enabled, the server is also restarted.

Related Topics

Certificates on page 343

Generate RADIUS Server Certificates

RADIUS server certificates ensure encryption between the RADIUS server and ExtremeCloud IQ Controller. To generate and load a certificate, take the following steps:

1. Go to **Onboard** > **AAA** and select **Manage Certificates**.
2. Under RADIUS Server Certificate, select **Update Certificate**.
3. Select the Certificate option:
   - **Generate a new unique private key and certificate**

     This option generates and loads a Self-Signed certificate.
   - **Provision a private key and certificate from files**

     This option loads the key and certificate from a Certificate Authority. Select this option, then do the following:

     a. Select **Choose File** and navigate to the Private Key file.
     b. If the Key file is password protected, check the box and provide the password.
     c. Select from the list of possible certificate files.
     d. To add certificate files, select **Add Files**, navigate to the saved certificate file, and select **Open**.
4. Select **Save** to save your changes and close the dialog.

Related Topics

Certificates on page 343

AAA Certificate Authorities

To manage a list of Trusted Certificate Authorities for AAA certificates, do the following:

1. Go to **Onboard** > **AAA** and select **Manage Certificates**.
2. Under AAA Trusted Certificate Authorities, select **Update Certificate**.
3. To add trusted certificates to ExtremeCloud IQ Controller, select **Add CA Certificates** and navigate to the certificate file. Then, select **Open**.
4. To add URLs to the Certificate Revocation List (CRL), select **Add URL**, and provide a valid CRL.
5. Check the box to allow expired CRLs to be used to validate certificates.

Related Topics

Certificates on page 343

Manage Captive Portal

1. Go to **Onboard** > **Portal**.

   A list of captive portals displays. From here, you can add a new portal, edit a portal configuration, or delete a portal. From the **Portal List** screen, you can use the **Search** field to find a specific portal.
2. To add a new portal, from the **Portal Configurations** screen, select **Add** and configure the portal settings.
3. To edit or delete a portal, from the **Portal Configurations** screen, select a row.

   The portal settings display.
   - To edit, modify the settings and select **Save**.
   - To delete the portal, select **Delete**.

To access the captive portal's user administration page:

- From any client VLAN where the captive portal is enabled, you can connect to `https://client_vlan_ip/administration`.
- From any VLAN or interface with Management enabled (except for Admin), you can connect to `https://interface_ip/administration`.

Related Topics

Portal Website Configuration on page 345
Portal Network Configuration on page 355
Portal Administration Configuration on page 357

Portal Website Configuration

From the **Portal Configurations** tab, configure settings related to guest access, authentication, and appearance of the portal website.

1. Go to **Onboard** > **Portal**.

2. Select an existing portal or select **Add**.

   When adding a new portal, enter a name for the portal, save it, then select that portal from the list.
3. Configure the following parameters:
   - Guest Portal. Intended for temporary access through guest accounts. Valid values are:
     - Guest Web Access

       Allows unauthenticated access to the network for the duration of the client's session. Allows the optional presentation of an Acceptable Use Policy. No permanent end user records are stored to enhance network security, and to minimize the number of registration records stored in the database. Select **Manage** to configure settings.
     - Guest Registration

       Allows unauthenticated access to the network for a configurable period of time. Registration has provisions for capturing end-user specific information such as a name, phone number, or email address. Allows the optional presentation of an Acceptable Use Policy. Registration using credentials for Facebook, Google, or Microsoft are supported. Select **Manage** to configure settings.
     - Disabled

       Indicates that the Guest Portal is not enabled.
   - Authenticated Portal. Intended for guests and staff with authenticated user accounts.
     - Authenticated Web Access

       Allows authenticated access to the network for the duration of the client's session. Allows the optional presentation of an Acceptable Use Policy.
     - Authenticated Registration

       Allows authenticated access to the network for a configurable period of time. Registration has provisions for capturing end-user specific information such as a name, phone number, and email address. Allows the optional presentation of an Acceptable Use Policy. Self-Registration and Pre-Registration are configurable.
     - Disabled

       Indicates that the Authenticated Portal is not enabled.

Related Topics

Guest Portal: Guest Web Access on page 347
Guest Portal: Guest Registration on page 348
Authenticated Portal: Authenticated Web Access on page 350
Authenticated Portal: Authenticated Registration Settings on page 350
Look and Feel Settings on page 353

Guest Portal: Guest Web Access

Table 89: Guest Portal — Guest Web Access

Field	Description
Introduction Message	The message displayed to a user when they register or gain web access as an authenticated user of the network. Message string parameters include Locale and a Text field for a Terms of Use Statement. The Introduction Message is shared by Guest Web Access and Guest Registration. Modifications affect both access types.
Custom Fields	Select the fields to display on the portal website. Set the visibility settings and determine if the field is required. You can also enable the **Display Acceptable Use Policy**, and edit the policy for each configured locale. These settings are shared by Guest Web Access and Guest Registration. Modifications affect both access types.
Redirection	Determine redirection behavior. Valid values are: • Use Network Settings Redirection. Always redirect based on network settings. • Redirection to user's requested URL — Redirects the end user to the web page they requested at network connection. • To specified URL — Specify the URL for the web page redirection. Destination field is displayed. • Disabled — No redirection. End user remains on the web page where they were accepted onto the network. The option selected here overrides the Redirection option specified on the Network Settings. These settings are shared by Guest Web Access and Guest Registration. Modifications affect both access types.

Note

Access Control Rule *Registered Guests* is created. Users who complete registration through the Guest captive portal match this rule. The rule checks for end-system MAC addresses in the Registered Guests group. This rule is present when Guest Registration or Guest Web Access is enabled.

Related Topics

Portal Website Configuration on page 345
Guest Portal: Guest Registration on page 348
Authenticated Portal: Authenticated Web Access on page 350
Authenticated Portal: Authenticated Registration Settings on page 350
Look and Feel Settings on page 353
Default Rules for Captive Portal on page 365

Guest Portal: Guest Registration

Table 90: Guest Portal — Guest Registration

Field	Description
Guest Portal — Guest Registration	
Introduction Message	See Introduction Message.
Custom Fields	See Custom Fields.
Redirection	See Redirection.
Default Expiration	Indicates registration window before expiration, measured in days, minutes, or hours. Default expiration is 30 days after initial registration.
Facebook Registration	Select this option to allow authentication with Facebook credentials. Obtain an Application ID and Shared Secret from Facebook. See Walled Garden Rules on page 283.
Google Registration	Select this option to allow authentication with Google credentials. Obtain an Application ID and Shared Secret from Google. See Walled Garden Rules on page 283.
Microsoft Registration	Select this option to allow authentication with Microsoft credentials. Obtain an Application ID and Shared Secret from Microsoft. See Walled Garden Rules on page 283.
Yahoo Registration	Select this option to allow authentication with Yahoo credentials. Obtain an Application ID and Shared Secret from Yahoo. See Walled Garden Rules on page 283.
Salesforce Registration	Select this option to allow authentication with Salesforce credentials. Obtain an Application ID and Shared Secret from Salesforce. See Walled Garden Rules on page 283.
Provider 1 Registration	Select this option to use credentials from a custom application that you configure. See Walled Garden Rules on page 283.
Provider 2 Registration	Select this option to use credentials from a custom application that you configure. See Walled Garden Rules on page 283.

Note
Access Control Rule *Registered Guests* is created. Users who complete registration through the Guest captive portal match this rule. The rule checks for end-system MAC addresses in the Registered Guests group. This rule is present when Guest Registration or Guest Web Access is enabled.

Related Topics

Portal Website Configuration on page 345
Guest Portal: Guest Web Access on page 347

Authenticated Portal: Authenticated Web Access on page 350
Authenticated Portal: Authenticated Registration Settings on page 350
Look and Feel Settings on page 353
Default Rules for Captive Portal on page 365

Authentication with Third-party Credentials

Guest Registration using a third-party application has the following advantages:

- It provides ExtremeCloud IQ Controller with a higher level of user information by obtaining information from the end user's third-party application account instead of relying on information entered by the end-user.
- It provides an easier registration process for the end user. ExtremeCloud IQ Controller retrieves the public information from the end user's third-party account and uses that information to populate the name and email registration fields.

After you have configured a third-party application for registration, this is how the authentication process works:

- The end user attempts to access an external Web site. Their HTTP traffic is redirected to the captive portal.
- In the Guest Registration Portal, the end user selects the option to register using credentials from a third-party (Facebook, Yahoo, etc.)
- The end user is redirected to the third-party login screen.
- If an Acceptable Use Policy option is configured, the captive portal verifies that the AUP has been acknowledged before redirecting the user to the third-party application.
- After logging in, the end user is presented with the information that ExtremeCloud IQ Controller receives from the third-party application.
- The end user grants ExtremeCloud IQ Controller access to the third-party information and is redirected back to the captive portal where they see a "Registration in Progress" message.
- The third-party application provides the requested information to ExtremeCloud IQ Controller, which uses it to populate the user registration fields.
- The registration process completes and network access is granted.

Third-party Registration Requirements

Third-party captive portal registration requires the following:

- The ExtremeCloud IQ Controller Access Control engine must have Internet access in order to retrieve user information from the third-party application.
- The ExtremeCloud IQ Controller Access Control Unregistered access policy must allow access to the third-party application site (either allow all SSL or make allowances for application servers).
- The ExtremeCloud IQ Controller Access Control Unregistered access policy must allow access to HTTPS traffic to the third-party application OpenID servers.

- A Unique third-party application must be created on the third-party application Developers page.
- The Portal Configuration must have the third-party application enabled and must include the third-party application's Application ID and Shared Secret.

Authenticated Portal: Authenticated Web Access

Table 91: Authenticated Portal — Authenticated Web Access

Field	Description
Login or Register Message	See Introduction Message.
Introduction Message	See Introduction Message.
Failed Authentication Message	The message displayed to the end-user upon failed authentication. By default, this message advises the end user to contact their network administrator for assistance.
Customize Fields	See Custom Fields.
Max Failed Logins	Select this option to configure the maximum consecutive number of times an end user can attempt to authenticate on an end-system and fail. Specify a lockout period that must elapse before the user can attempt to log in again on that end-system. The lockout period must be at least 1 minute.
Redirection	See Redirection.

Note
Control Rule *Web Authenticated Users* is created. Users who complete registration through the Authenticated captive portal match this rule. The rule checks for end-system MAC addresses in the Web Authenticated Users group. This rule is only present when Authenticated Registration or Authenticated Web Access is enabled.

Related Topics

Portal Website Configuration on page 345
Guest Portal: Guest Web Access on page 347
Guest Portal: Guest Registration on page 348
Authenticated Portal: Authenticated Registration Settings on page 350
Look and Feel Settings on page 353
Default Rules for Captive Portal on page 365

Authenticated Portal: Authenticated Registration Settings

Table 92: Authenticated Portal — Authenticated Registration Settings

Field	Description
Login or Register Message	See Introduction Message.
Introduction Message	See Introduction Message.

Table 92: Authenticated Portal — Authenticated Registration Settings (continued)

Field	Description
Failed Authentication Message	See Failed Authentication Message.
Customize Fields	See Custom Fields.
Max Failed Login	See Max Failed Login.
Redirection	See Redirection.
Default Max Registered Devices	Indicates the maximum number of MAC addresses each authenticated end user may register on the network. If a user attempts to exceed this count, an error message is displayed in the Registration web page. The default value for this field is 2.
Default Expiration	See Default Expiration.
Delete Expired User Registrations	Delete a user from the Registered users list in the **Registration Administration** web page when their registration expires. If a registration is deleted, the end-user must re-enter the required information the next time they attempt to access the network. When **Delete Expired User Registrations** is enabled, the Local Password Repository User is deleted when the client registration expires, and the client registration type changes to *Transient*. **Delete Local Password Repository Users** — If you are using local authentication, and this option is checked, the user is deleted from the Local Password Repository when the registration expires. This option displays when you enable **Delete Expired User Registrations**. If you are using a local repository, authenticated end users are assigned to the Web Authenticated Users Authenticated group.

Table 92: Authenticated Portal — Authenticated Registration Settings (continued)

Field	Description
Enable Self-Registration Portal	Allows an authenticated and registered user to self-register additional devices that may not support authentication (such as Linux machines) or may not have a web browser (such as game systems). For example, a student may register to the network using their PC. Then, using a self-registration URL provided by the system administrator, they can register their additional devices. Example URL: `https: //<controller ip address>:8445/administration`
Enable Pre-Registration Portal	Guest users can be registered in advance, allowing for a more streamlined and simple registration process when the guest user connects to the network. Pre-register a single user, multiple users, or both. Example URL: `https: //<controller ip address>:8445/administration` Or, for the administration interface — `https://<IP address of portal interface>/administration`. **Set Pre-Registration Expiration at First Login** — Indicates that pre-registration expiration begins when user registers their first end-system. When this option is cleared, the default expiration of the Pre-Registered user begins from the time the administrator creates the Pre-Registered user account. **Generate Password Characters** — Select an auto-generation option for password characters. **Generate Password Length** — Specify a password length rule.

Note
Control Rule *Web Authenticated Users* is created. Users who complete registration through the Authenticated captive portal match this rule. The rule checks for end-system MAC addresses in the Web Authenticated Users group. This rule is only present when Authenticated Registration or Authenticated Web Access is enabled.

Related Topics

Portal Website Configuration on page 345
Guest Portal: Guest Web Access on page 347
Guest Portal: Guest Registration on page 348
Authenticated Portal: Authenticated Web Access on page 350
Look and Feel Settings on page 353
Default Rules for Captive Portal on page 365

Look and Feel Settings

Use Table 93 to customize your captive portal.

Table 93: Captive Portal Website Look and Feel Settings

Setting	Description
Display Powered by Logo	Display the Extreme Networks logo at the bottom of all of your portal web pages.
Edit Message String	Modify the message displayed to users on the menu bar of any registration or web access page. The default welcome message is "Welcome to the Enterprise Network's Registration Center."
Edit Images	Specify the image files used in the portal web pages. All image files must be defined here. Select the plus sign to add images. After the image is added, select to preview the image. After an image file is defined here, it is available for selection from the configuration drop-down lists. The drop-down menu for each image category displays all the images defined in the **Images** window. **Note:** You must add images to each portal separately. Images listed under the default portal are not available to other portals until you have added the image to each portal separately. • Header Background Image. The background image displayed behind the header image at the top of all portal web pages. • Header Image. The image displayed at the top of all portal web pages. • Favorites Icon. The image displayed as the Favorites icon in the web browser tabs. • Access Granted Image. The image displayed when the end user is granted access to the network either based on compliance with the network security policy or upon successful registration to the network. • Access Denied Image. The image you would like displayed when the end user has been denied access to the network. • Error Image. The image displayed when there is a communication error with the server. • Busy Image. The progress bar image displayed when the web page is busy processing a request.

Table 93: Captive Portal Website Look and Feel Settings (continued)

Setting	Description
Edit Colors	Select the Background or Text color box corresponding to each item to open the **Choose Color** window. Define the colors used in the portal web pages: • Page — Define the background color and the color of all primary text on the web pages. • Header Background Color — Define the background color displayed behind the header image. • Menu Bar — Define the background color and text color for the menu bar. • Menu Bar Highlight — Define the background color and text color used for the menu bar highlights in the Administration pages. • Footer — Define the background color and text color for the footer. • Table Header — Define the background color and text color for the table column headers in the Administrative web pages. • In-Progress — Define the background color and text color for task in-progress images. • Hyperlink — Define the color used for hyperlinks on the web pages. • Hyperlink Highlight — Define the color of a hyperlink when it is highlighted. • Accent — Define the color used for accents on the web pages.

Table 93: Captive Portal Website Look and Feel Settings (continued)

Setting	Description
Edit Style Sheets	Create a style sheet that adds to or overwrites the formatting styles for the portal, or mobile version of the portal web pages, respectively.
Edit Locales	Define the default locale (language), displayed to any captive portal user unless the client locale detected from their browser matches one of the defined supplemental locales. The list of available locales includes the current default locale and any supplemental defined locales. **Display Locale Selector** — Select this check box if you want a locale (language) selector to display as a drop-down menu in the menu bar on the captive portal welcome and login pages. This is useful for a shared machine where the users of the machine may speak different languages. On the mobile captive portal, the selector is displayed as a list of links at the bottom of the welcome screen. **Add** — Add a locale to the list of possible locales. Select a **Language Bundle** value, and the other parameters will auto populate. • Language Bundle • Name • Language Code • Country Code • Encoding. To delete a locale, select  for the locale in the locales list.

Related Topics

Portal Website Configuration on page 345

Portal Network Configuration

Configure settings for portal network configuration:

1. Go to **Onboard** > **Portal**.
2. Select an existing portal or select **Add**.

3. Configure the following parameters on the **Network Configuration** tab.

Table 94: Network Configuration Settings

Field	Description
Use Mobile Captive Portal	Allows mobile devices to access the network via captive portal registration and remediation. It also allows Help desk and IT administrators to track the status of registered end-systems, as well as add, modify, and delete registered end-systems on the network using a mobile device. This feature is supported on the following mobile devices: IPod Touch, IPad, IPhone, Android Phone/Tablet/NetBook, and Windows phones.
Display Welcome Page	Displays the welcome page. When this option is cleared, users bypass the welcome page and access the portal directly.
Redirect User Immediately	Redirects end users to the specified test image URL upon gaining network access. When the end-system's browser reaches the test image URL, ExtremeCloud IQ Controller can assume that the end user has network access and redirects the end user out of the captive portal. Use an internal image that end users don't have access to until they are accepted. It is recommended that the test image URL is a link to an SSL site, because when the captive portal is configured for `Use HTTPS`, the browser will not allow the attempt to an HTTP test image site. It is also recommended that the captive portal policies (typically the Unregistered and Quarantine policies) are configured to deny HTTPS traffic. This prevents the test image connection attempt from successfully completing and moving the end-system out of the captive portal prematurely. If access to the test image is available, the user may experience the captive portal reverting to the "Click here to access the network page", and then upon selecting the link, returning to the previous page based on their state. This behavior continues until the user is finally accepted on to the network.
Test Image URL	Specify the URL for the immediate redirection. See Redirect User Immediately.
Redirection	See Redirection.
Destination	When Redirection field is set to **URL**, specify the URL for the web page redirection here.
Client Auto Log in Handling	ExtremeCloud IQ Controller supports auto-detection of a captive portal. Valid values are: • Redirect — Auto-detection is enabled and client is automatically redirected to the captive portal. This is the default setting. • Hide — Disables auto-detection of captive portal.

Portal Administration Configuration

Configure settings for the Registration Administration web page and grant access to the page for administrators. The Registration Administration web page allows Helpdesk and IT administrators to track the status of registered end-systems, as well as add, modify, and delete registered end-systems on the network.

1. Go to **Onboard** > **Portal**.
2. Select an existing portal or select **Add**.
3. Configure the following parameters on the **Administration** tab.

Table 95: Admin Portal Configuration Settings

Setting	Description
Welcome Message	Message displayed to users when they log into the administration portal. The default welcome message is *Registration System Administration*. Click **Edit** to modify the message Locale or message text.
Session Timeout	The length of time an administrator can be inactive on the administration web page before being automatically logged out. The default value is 10 minutes.
Administration Page Image	Image to display on all registration administration pages. The drop-down menu displays all the images defined in the default portal Images window. To update this image, add the image file to the default portal. Go to **Portal Configurations** and select the Default portal. Then select **Edit Configuration** > **Edit Images**. For more information, see Look & Feel settings.
Login Configuration	Select **Add** to add a new configuration.

Related Topics

Login Configuration Settings on page 358

Login Configuration Settings

Set up a login configuration profile to simplify user access to the captive portal.

Table 96: Login Configuration Settings

Field	Description
Authentication Type	Indicates the method of authentication for the captive portal login. Valid values are: • Local Password Repository User • Local Password Repository User Group • LDAP User Group • RADIUS User Group
Repository User	Users that have been created under Local Password Repository. Valid values are Admin or Sponsor. Click to add a new Local Repository User.
Role	Indicates the policy role for this configuration profile. Valid values are: Admin and User.

Related Topics

Portal Administration Configuration on page 357
Manage Access Control Groups on page 358
User Account Settings on page 342

Message String Settings

From this dialog, select the message Locale and edit the Description text for the registration verification message displayed during the user verification process.

Manage Access Control Groups

An access control group is used to organize mobile clients by various group types, including device type or end system characteristics such as IP address, hostname, or user group. Configure groups to be used with access control rules. ExtremeCloud IQ Controller provides a set of default system groups with your installation to simplify the group set up process.

To manage the list of groups:

1. Go to **Onboard** > **Groups**.

   A list of configured groups displays. From here, you can search for a group, edit group settings, delete a group, or add a new group.
2. To edit or delete a group, select a group row.

   The group settings display.
   - To edit a group, modify the group settings and select **Save**.
   - To delete a group, select **Delete**.
3. To add a new group, from the **Access Control Groups** page, select **Add** and configure the group settings.

Related Topics

Access Control Group Settings on page 359
Default Groups Provided with Your Installation on page 360
Access Control Rules on page 361

Access Control Group Settings

Configure the following access control group settings and click **Save**. The entry parameters depend on the Group Type.

Table 97: Access Control Group Settings

Field	Description
Name	Group name.
Description	Description of the group.
Group Type	Criteria by which the accounts are grouped. Valid values are: • End System - MAC Possible entry values are: ◦ MAC Address ◦ MAC Mask ◦ MAC OUI (Organizationally Unique Identifier) • End System Hostname • End System IP Address • End System LDAP User Group • User - RADIUS User Group • User - Username • Device Type
Group Mode	**For End System LDAP User Groups only** — Specify whether to match any or match all of the LDAP attributes. Valid values are: • Match All • Match Any
Group Entries	A list of entries for the group. Use the **Search** field to search for an entry.

Related Topics

Working with Group Entries on page 360
Cloning Groups on page 360
Manage Access Control Groups on page 358
Default Groups Provided with Your Installation on page 360

Working with Group Entries

To work with Access Control Group entries:

1. Go to **Onboard** > **Groups**.
2. Select a group from the list.
3. To add a new group entry:
   a. Click **Add Entry**.
   b. Add an entry with a description.
4. To delete an entry:
   a. Select an entry from the Entry list.
   b. Click .
5. To modify an entry:
   a. Select an entry from the Entry list.
   b. Click the drop-down arrow and select a new value.

Cloning Groups

To easily create new groups, use the cloning feature, then modify the group entries and settings as necessary.

1. Go to **Onboard** > **Groups**.
2. Select a group from the list.
3. Select **Clone**.
4. Provide a name for the new group.
   ExtremeCloud IQ Controller prompts you to open the new group.
5. Add, remove, or edit group entries and settings as necessary.

Related Topics

Access Control Group Settings on page 359
Working with Group Entries on page 360

Default Groups Provided with Your Installation

The following Access Control system groups are provided with the ExtremeCloud IQ Controller installation by default.

- Blacklist. A list of MAC addresses that are prohibited from accessing the network.
- Registered Guests. A list of MAC addresses that have been granted access to the network via the Guest captive portal.
- Registration Denied Access. A list of MAC addresses that have been denied access to the network.
- Registration Pending Access. A list of MAC addresses that are waiting permission to access to the network.
- Web Authenticated Users. A list of MAC addresses that have been granted access to the network via the Authenticated captive portal.
- DFNDR_PolicyGeneration. Default Group created for Extreme Defender Application. Allows Defender Policy Generator to move clients to and from build roles.

In addition, the following Device Type groups are provided with your ExtremeCloud IQ Controller installation:

- Windows
- Windows Mobile
- Linux
- Mac
- iPhone
- BlackBerry
- Android
- Windows
- Mobile Game Console
- Chrome OS

You cannot delete system groups.

Related Topics

Manage Access Control Groups on page 358
Access Control Group Settings on page 359

Access Control Rules

Access Control Rules enable you to apply network access permissions and restrictions based on defined rules. The rules can address network resources, a user's role or purpose in the organization, or the device type that is used to access the network. Network access control is dynamic. End-user network access can change as group associations change without a network administrator getting involved.

ExtremeCloud IQ Controller grouping is the building block for Access Control Rules. An Access Control Rule consists of one or more groups, a policy role definition, and an optional captive portal specification. The policy role that defines the access control action is specified in the Access Control Rule.

Through the use of group criteria, the Access Control Rule definition provides dynamic control over network access. Specify up to four group criteria from defined groups. The rule definition is a logical "And" of the group criteria. This structure allows for varied levels of granularity in the Access Control Rule definition.

Before configuring Access Control Rules, configure groups, policy roles, and captive portal definitions that you can use in a rule definition.

The ExtremeCloud IQ Controller installation provides the following default system rules:

- Catch-All rule. End-systems that do not match any of the defined rules are assigned the default Catch-All rule. The Default Catch-All rule assigns the Enterprise User policy role by default, which allows full network access. The policy role assigned by this rule is configurable (You can edit the rule and change the "Accept Policy" field value.)
- Blacklist. End-systems with a MAC address that is a member of the Blacklist group are denied network access. They are assigned the Quarantine policy role. The

Quarantine policy denies all traffic by default. Go to **Policy** > **Roles** to configure the Quarantine policy definition.

Related Topics

Configuring Network Policy Roles and Dynamic Access Control on page 362
Managing Access Control Rules on page 364
Rule Settings on page 365

Configuring Network Policy Roles and Dynamic Access Control

A policy-based network relies on roles to define network access based on criteria defined in the role. Access Control Rules add additional criteria based on groups, adding a level of specificity to access conditions. The grouping criteria is dynamic, allowing the level of permissions to change based on a user's group associations.

To illustrate how policy and Access Control Rules work together, consider the policy role of a student:

Policy Roles:

- Learning Student Access
- Basic Student Access

1. Configure a policy role named **Learning Student Access**: The member has full access to the network but is denied access to social media apps.
   - One network policy rule that provides full access to the network.
   - One application policy rule that denies access to social media apps.
2. Configure a policy role named **Basic Student Access**: The member has limited network access but access to all applications is allowed.
   - One network policy rule that limits students to TCP access on ports: HTTP/S, DNS, and DHCP-Server.

   Note
   If no application policy rule exists, access to all applications is allowed.

Groups

Configure the following groups:

- **Student Body**. User group that includes all registered students.
- **School Computers**. End-System group with MAC addresses for all school issued computers.

Captive Portal

Configure a captive portal to associate with one or more Access Control Rules. Authentication settings on the captive portal will deny access to students who are no longer a member of the student body.

Access Control Rules

1. Configure **Access Control Rule "Learning Student"**.

   The Access Control Rule takes the defined policy rule: **Learning Student Access** and applies it to members of the student body who are using school issued computers in a single rule.

   Group Criteria:

   Select the following values for each group:
   - User Group = **Student Body**
   - End-System Group = **School Computers**

   Policy Role:

   Select **Learning Student Access** as the Policy Role.
2. Configure **Access Control Rule "Basic Student"**

   The Access Control Rule takes the defined policy rule: **Basic Student Access** and applies it to all members of the student body that are using non-school issued devices.

   Group Criteria:

   a. Select the following values for each group:
      - User Group = **Student Body**
      - End-System Group = **School Computers**.

   b. Check **Invert** check box. This indicates a match if student is *not* using a school computer.

   Policy Role:

   Select **Basic Student Access** as the Policy Role.

Results:

- If the student is a member of the student body using a school computer, the student has full network access and is denied access to social media applications.
- If the student is a member of the student body using a personal computer, the student has limited access to the network and full access to social media.

- If the student is no longer a member of the student body, but does have a school computer, the captive portal authentication settings will deny network access.
- If the student is no longer a member of the student body, but is using a personal computer, the captive portal authentication settings will deny network access.

Note

The ExtremeCloud IQ Controller installation provides the following default system rules:

- Catch-All rule. End-systems that do not match any of the defined rules are assigned the default Catch-All rule. The Default Catch-All rule assigns the Enterprise User policy role by default, which allows full network access. The policy role assigned by this rule is configurable (You can edit the rule and change the "Accept Policy" field value.)
- Blacklist. End-systems with a MAC address that is a member of the Blacklist group are denied network access. They are assigned the Quarantine policy role. The Quarantine policy denies all traffic by default. Go to **Policy** > **Roles** to configure the Quarantine policy definition.

Related Topics

Add Policy Roles on page 292
Manage Access Control Groups on page 358
Managing Access Control Rules on page 364
Rule Settings on page 365
Access Control Rules on page 361
Manage Captive Portal on page 345

Managing Access Control Rules

An Access Control Rule is used to further define an end user's network access based on the groups and policy roles with which the end user is associated.

Go to **Onboard** > **Rules**.

A list of configured rules displays. From here, you can edit rule settings, delete a rule, or add a new rule.

- To edit a rule, select a rule from the list and click . Modify the rule settings and click **Save**
- To delete a rule, select a rule from the list and click . Or, edit the rule to open the **Settings** dialog and click **Delete**.
- To add a new rule, from the **Rules** page, click **Add** and configure the rule settings.

Related Topics

Access Control Rules on page 361
Configuring Network Policy Roles and Dynamic Access Control on page 362
Default Rules for Captive Portal on page 365
Rule Settings on page 365

Default Rules for Captive Portal

The following Access Control Rules are added when you enable an internal captive portal. The rules are removed when you disable the captive portal.

- Blacklist. This rule quarantines any MAC address that is part of the Blacklist group. This is always the first rule in the **Rules List**.
- Default Catchall. This rule applies the Default Auth Policy to any MAC Address. It is always the final rule in the **Rules List**.
- Unregistered: This rule is a catchall, and will always be listed immediately before the Default Catchall. Users who do not match any other rule will match Unregistered, and they will be presented with the captive portal.
- Registered Guests: Users who complete registration through the Guest captive portal will match this rule, which checks for end-system MAC addresses in the Registered Guests group.

  Note
  This rule is only present when Guest Registration or Guest Web Access is enabled.

- Web Authenticated Users: Users who complete registration through the Authenticated captive portal will match this rule, which checks for end-system MAC addresses in the Web Authenticated Users group.

  Note
  This rule is only present when Authenticated Registration or Authenticated Web Access is enabled.

Related Topics

Internal Captive Portal Settings on page 276
Portal Website Configuration on page 345
Portal Network Configuration on page 355
Portal Administration Configuration on page 357

Rule Settings

Configure the following Access Control Rule settings and select **Save**.

Associate rules to a group type. Configure groups under **Access Control** > **Groups**.

Table 98: Access Control Rule Settings

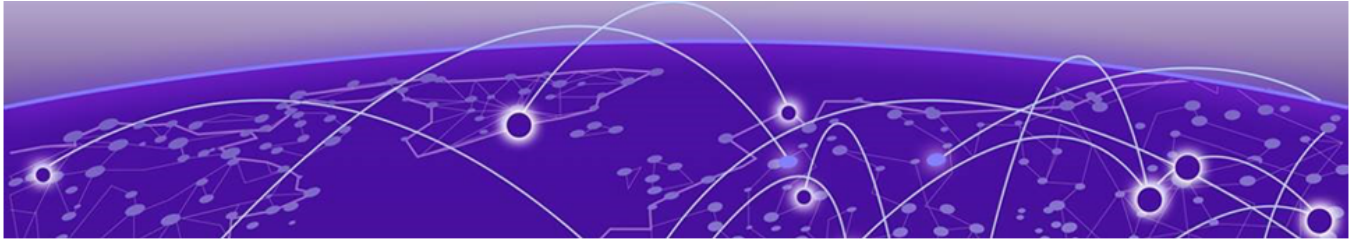
Field	Description
Name	Rule name. You cannot change the name of default rules that are provided with ExtremeCloud IQ Controller.
Rule Enabled	Indicates if the rule is enabled. You cannot disable default rules that are provided with ExtremeCloud IQ Controller.

Table 98: Access Control Rule Settings (continued)

Field	Description
Conditions Note: • If you select **Any**, then the criteria is ignored during the rule match process. • If you select the **Invert** check box, it is considered a rule match if the end-system *does not* match the selected value.	
User-Group	The user group that you configured. Users in this group are affected by the rule. User groups limit a user's access based on the LDAP, RADIUS, or Username group to which they are assigned.
End-System Group	The end-system group that you configured that is affected by the rule. End-systems that do not match any of the listed rules are assigned the Default Catchall rule.
Device Type Group	The device type group that you configured that is affected by the rule.
Location Group	The location group that you configured that is affected by the rule.
Policy	Associate a policy role with the Access Control Rule. The access control action is defined in the policy rule. Select from the drop-down list. For more information, see Preconfigured Policy Roles on page 124.
Portal	Associate a captive portal with a rule.

Related Topics

Manage Access Control Groups on page 358
Managing Access Control Rules on page 364
Policy Role Settings on page 292
Configuring Network Policy Roles and Dynamic Access Control on page 362



Tools

Use the **Tools** workbench for network troubleshooting.

Workflow

Use Workflow to understand the relationships between the ExtremeCloud IQ Controller components and to more easily navigate ExtremeCloud IQ Controller. Figure 72 on page 368 illustrates the relationship between the ExtremeCloud IQ Controller components. You can easily navigate to any of these components using **Workflow**.

Go to **Tools** > **Workflow** to begin.

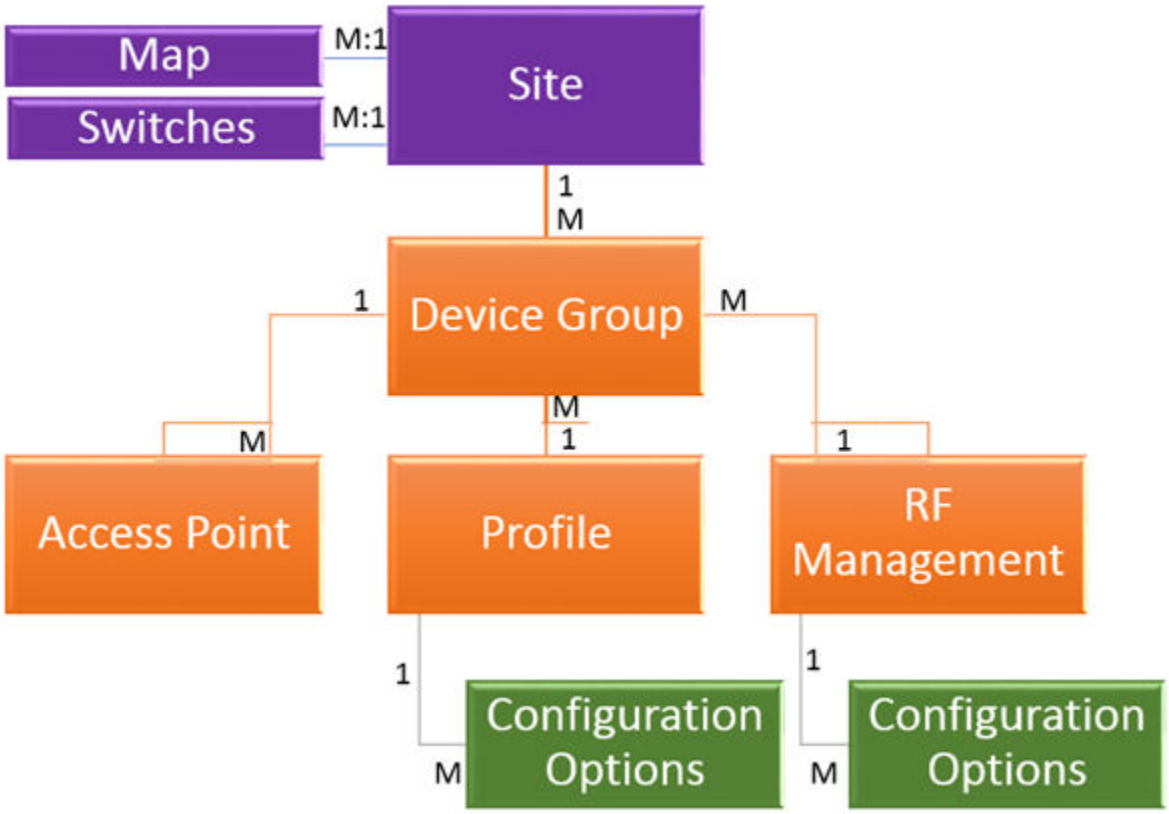


Figure 72: ExtremeCloud IQ Controller Component Relationship

Related Topics

Navigating ExtremeCloud IQ Controller Using Workflow on page 368
Modifying a Component on page 375

Navigating ExtremeCloud IQ Controller Using Workflow

The following component types are displayed when you access **Tools** > **Workflow**: Site, Profile, Role, and Network.

Alternatively, you can use the **Search** field to search for any component.

The **Workflow** pane lists all components that are available in ExtremeCloud IQ Controller. You can add and delete components using Workflow.

Select an icon on the **Workflow** page to display a list of available components and navigate through the component hierarchy.

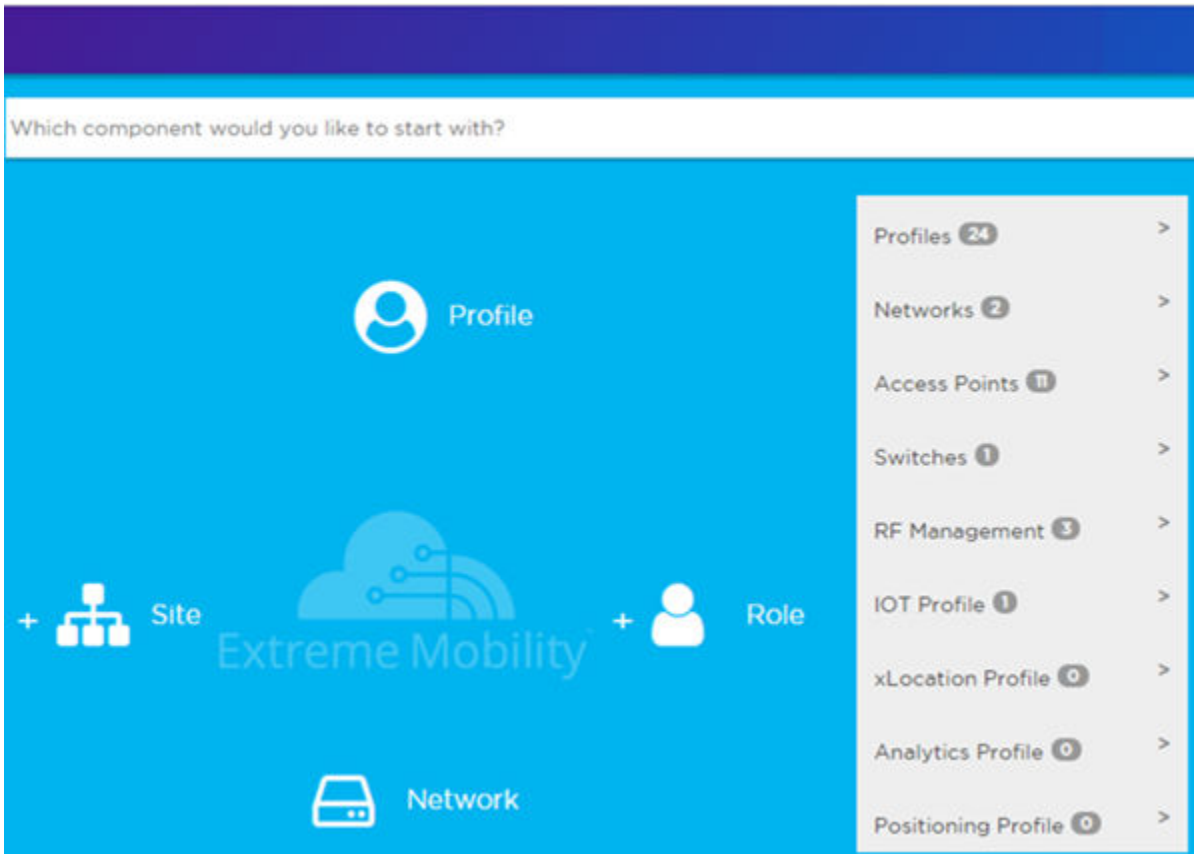


Figure 73: Workflow Main Page

Related Topics

How to Navigate Using Workflow on page 369
Workflow on page 367
Modifying a Component on page 375
Adding Components from Workflow on page 373
Deleting Components from Workflow on page 374

How to Navigate Using Workflow

Go to **Tools** > **Workflow** to navigate ExtremeCloud IQ Controller accessing components. The following example illustrates the relationship between ExtremeCloud IQ Controller components, and it demonstrates how to easily access each component using **Workflow**.

1. Select the **Site** icon on the **Workflow** page to display a list of available sites.

Note
If there is only one available component of that type, the component details or configuration page displays instead of a list of specific components.

2. Select a specific site from the **Site** list.

A site has the following associated components: Access Point, Device Group, and Switch.

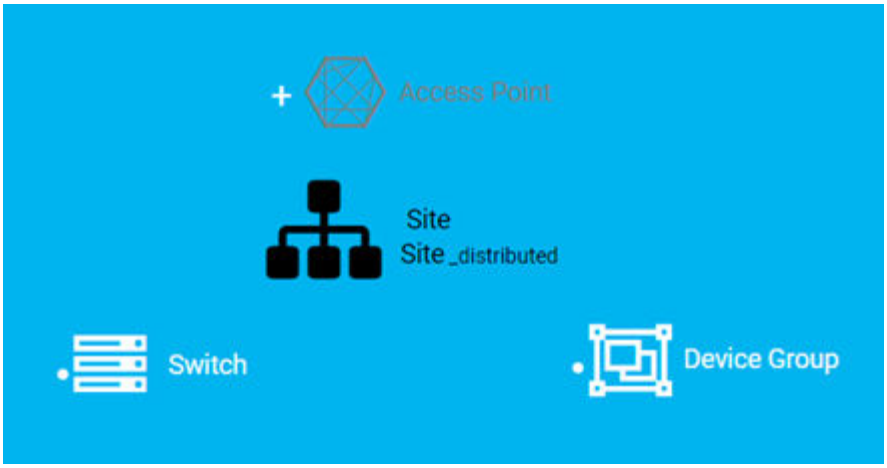


Figure 74: Site with associated components

Figure 74 illustrates possible icon colors on the **Workflow** page:

- Black Icon — The center icon surrounded by associated icons. This icon has the focus.
- White Icon — This icon indicates a configured component that is associated with the center icon.
- Gray Icon — This icon is associated with the center icon. It indicates a component that is available but not currently configured.

3. Select the **Device Group** icon to display a list of available device groups.
4. Select a specific device group from the list.

   The device group icon gains focus.

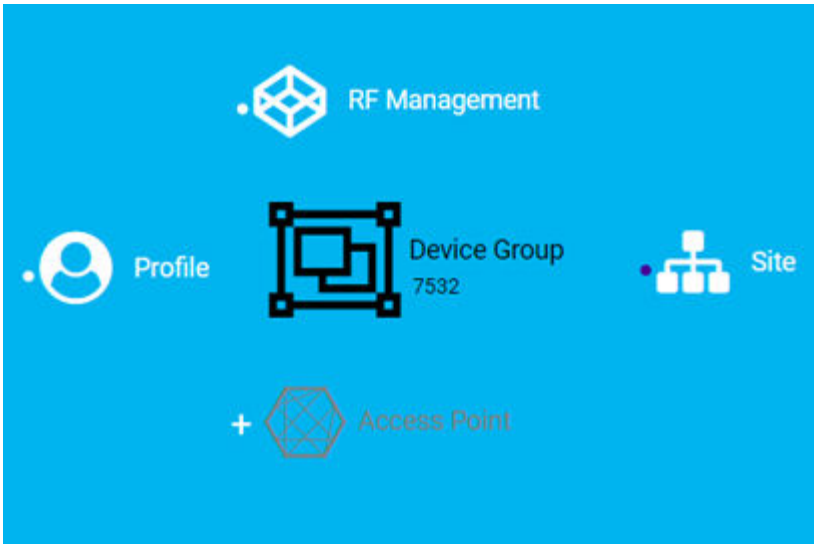


Figure 75: Device Group with associated components

- A device group has the following associated components:
  - RF Management
  - Site
  - Access Point
  - Profile

5. In this example, there are no APs configured for Device Group 7532; therefore, **Access Point** appears gray. Select + beside **Access Point** to open the **Edit Device Group** page and add one or more APs to Device Group 7532. For more information, see Add APs on page 212.

6. Each device group has a single profile. Select the **Profile** icon to display the configuration items associated with that profile.

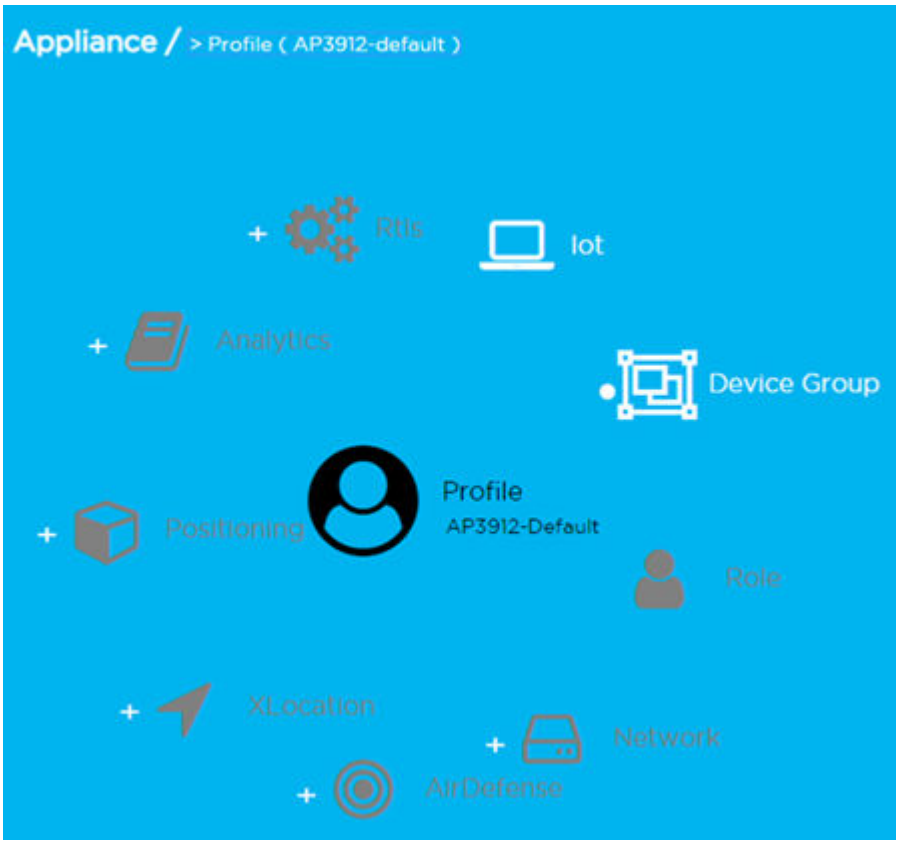


Figure 76: Profile with associated components

Note
Gray icons indicate components that are not configured. Select + to display the **Edit Profile** page and configure the component.

7. Continue navigating through the component hierarchy to view any component within ExtremeCloud IQ Controller. Use the Workflow breadcrumbs to move backwards in the hierarchy. Alternatively, you can use the **Search** field on the **Workflow** page to search for a component.

Related Topics

Adding Components from Workflow on page 373
Deleting Components from Workflow on page 374
Modifying a Component on page 375
Add or Edit a Configuration Profile on page 134
Add APs on page 212
Navigating ExtremeCloud IQ Controller Using Workflow on page 368
Workflow on page 367

Adding Components from Workflow

The **Workflow** pane lists all available components and indicates how many components you have configured for each component type.

To add components directly from the **Workflow** pane:

- Select the drop-down arrow under a component type and select the plus sign.
- Configure the parameters to add the component to the appliance and select **OK**.

1. From the **Workflow** pane, select the arrow next to **Access Points**.

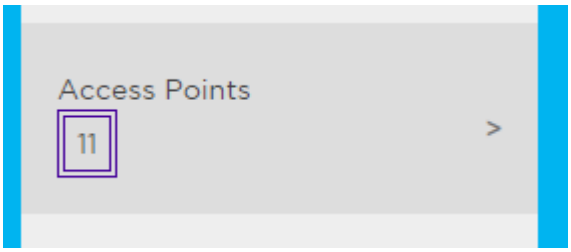


Figure 77: Workflow Pane APs

2. Select the plus sign.

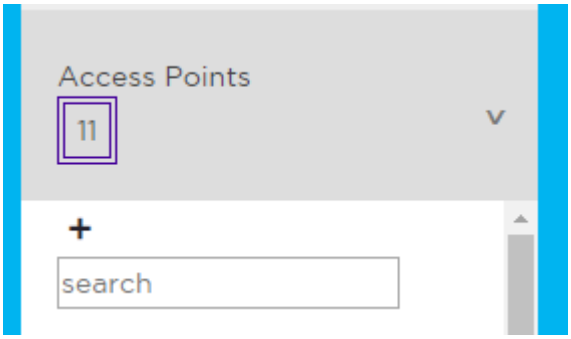


Figure 78: Adding APs from Workflow Pane

The configuration page for the selected component displays, allowing for further configuration. The parameters that you supply and the resulting configuration page depend on the component type. In this example, the **Add AP** dialog displays.

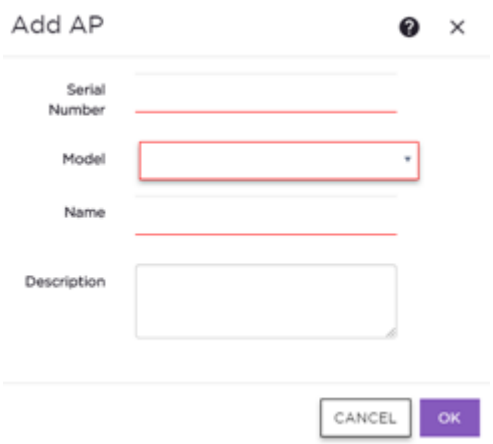


Figure 79: Add AP dialog

3. Configure the following parameters, then select **OK**.
   - Serial Number
   - Model
   - Name
   - (Optional) Description

   The Access Points configuration page for the specific AP displays. See Configure AP Details and Radio Settings on page 213 for instructions on configuring the AP radio settings.

Related Topics

Configure AP Details and Radio Settings on page 213

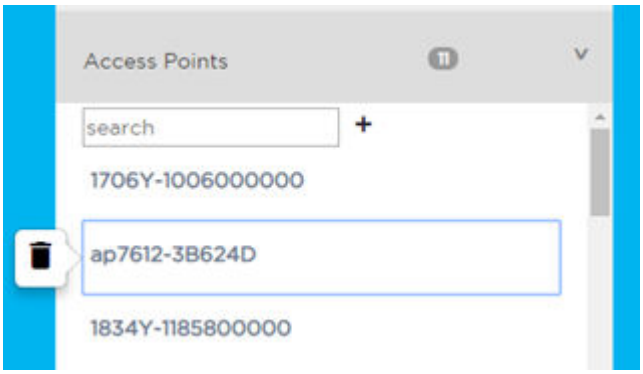
Deleting Components from Workflow

You can delete ExtremeCloud IQ Controller components from **Workflow**:

From the **Workflow** pane:

1. Click the drop-down arrow under a component type and select an item from the list.

2. Click .



A confirmation dialog displays.

Figure 80: Delete AP in Workflow

3. Click **OK** to delete the component.

Related Topics

How to Navigate Using Workflow on page 369
Adding Components from Workflow on page 373

Modifying a Component

You can easily modify any component that has focus at the center of the **Workflow** page.

1. Select the component that has the focus.

   Depending on the properties of the component that has focus, you are presented with one of the following:

   - Component list
   - Details page
   - Configuration page

2. Modify the component configuration as necessary and click **Save**.

Example: Profile Modification

1. Go to **Tools** > **Workflow** and select the **Profile** icon.
2. If there is more than one profile available, select a specific profile from the list.

   (If there is only one profile, the **Edit Profile** page displays. Skip to step 4.)

   The specific profile gains focus at the center of the **Workflow** page.
3. Select the profile component that has the focus to display the **Edit Profile** page.
4. To modify profile settings, select a profile tab.

Note
If you are editing a specific profile type (for example, IoT), the **Edit Profile** page opens with that tab selected.

Example: Network Modification

1. Go to **Tools** > **Workflow** and select the **Network** icon.
2. If there is more than one network available, select a specific network from the list.

   (If there is only one network, the network configuration settings display.)

   The specific network gains focus at the center of the **Workflow** page.
3. Select the specific network that has the focus to display the network configuration settings.

Related Topics

Add or Edit a Configuration Profile on page 134
Networks on page 249
WLAN Service Settings on page 250

Logs

The log messages contain the time of event, severity, source component, and any details generated by the source component. Log messages are presented under the following report tabs:

- Events
- Station Events
- Audit
- AP Logs
- AP Upgrade Report on page 382

Working with the logging page:

- Select the plus icon next to each log entry to expand, showing entry details.
- Highlight log entries and (using shortcut keys) copy/paste entries into a third-party application.
- Create Date/Time filters to display entries that were logged within that time window.

Related Topics

Understanding Date and Time on page 43
System Logging Configuration on page 457
Set a Logging Filter on page 382

Advanced Filtering

ExtremeCloud IQ Controller offers a Query Builder to filter logs, enabling you to find records more easily, improving efficiency of diagnostics. Perform an advanced query over Events, Audit log, AP logs, and Station events. The saved queries are persistent to each individual Log tab.

Related Topics

Build a Query for Logs on page 377

Build a Query for Logs

This topic outlines how to build a query to filter the event logs. To build a query for the **AP List** and **Client List**, see Build a Query for Devices or Clients on page 73.

Take the following steps to build a customized query, filtering data in the **Logs** page:

1. To access the **Logs** page, go to **Tools** > **Logs**.
2. To open Query Builder, select > .

   Query Builder starts with a logical group of conditions. You can add more groups, joined with query conditions. Valid conditions between two or more groups:

   - AND
   - OR

   Note
   AND is the only supported condition within a group.

3. To add a condition, select **+ Condition**.
4. From **Source Field**, select a value that represents a column used in the query.
5. Select the **Operator**.

   The available operators depend on the data type. Number types offer comparisons such as greater or less than. Valid values are:

   - Equals
   - Not Equals
   - Contains
   - Greater Than
   - Less Than
   - Less or Equals
   - Greater or Equals
6. Under **Search Condition**, provide the value that you are searching for.

   Selecting the **Search Condition** field displays a drop-down of existing values. The list is filtered as you type. Wildcards are not supported. To match a portion of the search condition, use the operator **Contains**.

   - To add conditions, select **+**.
   - To remove conditions, select **-**.
7. To add another condition row, select **+** .
8. **Group** — Each group has conditions joined by the selected operator. You can add additional groups or add conditions to the group.

9. To run the query, select **Execute**.
   The query is automatically saved.

Note
Query Builder generates a Pandas query syntax. The syntax preview is displayed at the top of the **Query Builder** dialog. For saved queries:

- Select to view the Pandas query.
- Select to copy the Pandas query to the clipboard.

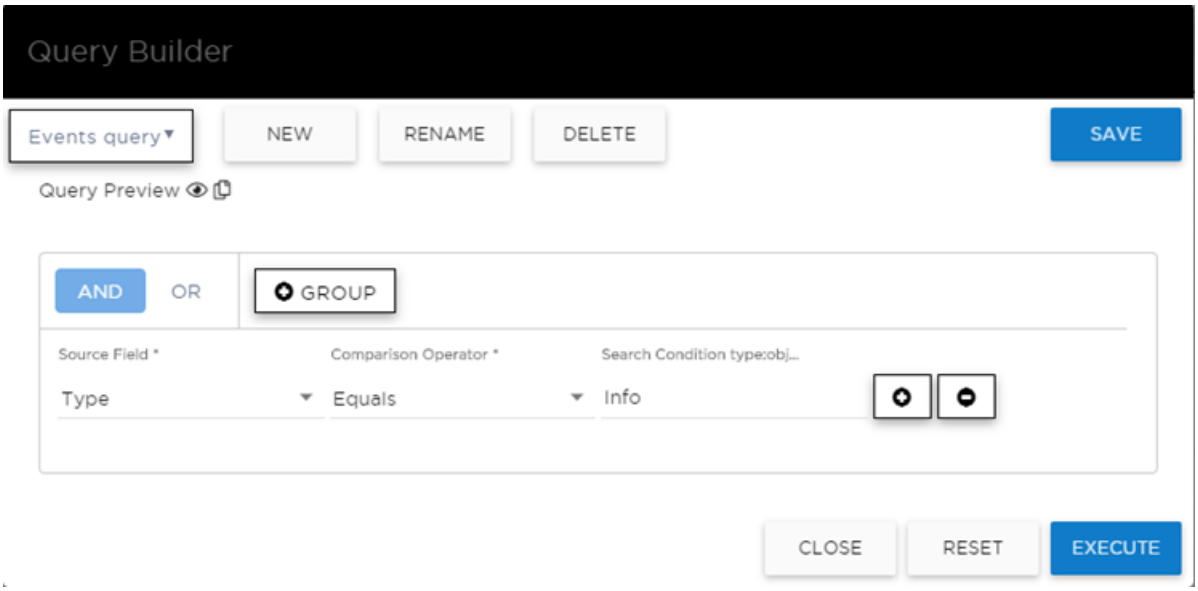


Figure 81: Query Builder: Events Query Type Info

Select from the list of saved queries or create a new query.

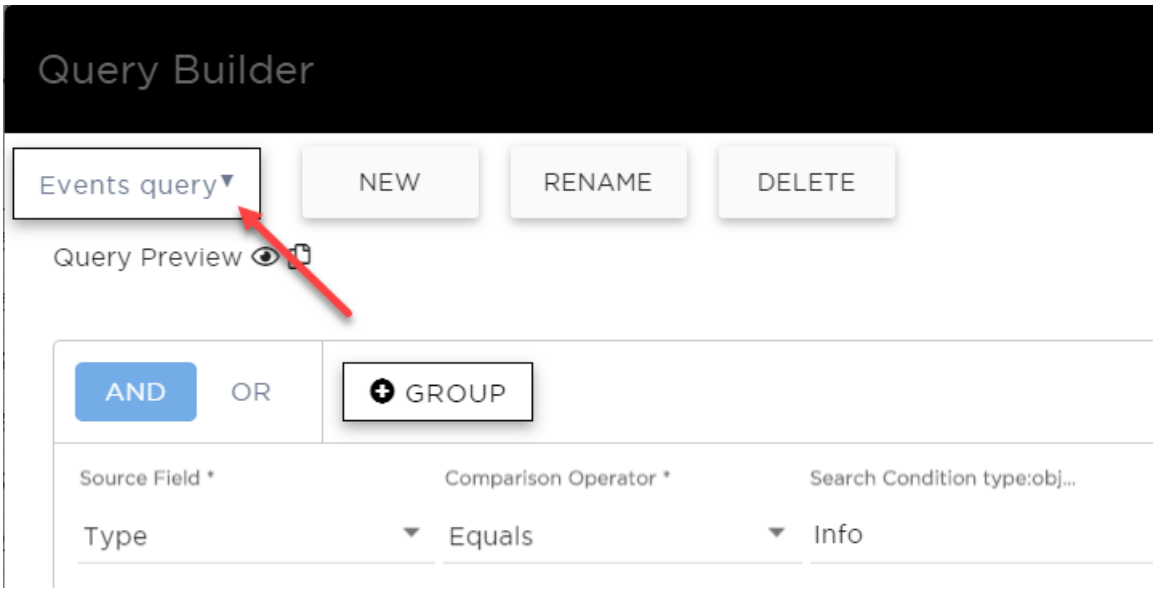


Figure 82: List of saved queries

Query Builder actions:

- **New**. To create a new query, provide a name and select **OK**. There is a limit of 10 saved queries per user, per grid. After the 10-query limit has been reached, the **New** button is unavailable.
- **Rename**. Rename an existing query.
- **Delete**. Delete the query that is currently displayed.
- **Close**. Close the Query Builder dialog. If you close Query Builder without running the query, your query details are deleted.
- **Reset**. Close the Query Builder dialog and save the current query. The next time you open Query Builder, this query will display. This option is available after you run a specific query.
- **Execute**. Run the query and save it.
- **Save**. Save changes without executing the query. Save is only visible when changes have been made.

Related Topics

Query Builder on page 73
Build a Query for Devices or Clients on page 73

View Events

ExtremeCloud IQ Controller logs all messages that are triggered by system events. You can view a record of the events in the user interface.

The **Events** tab includes the following information:

- Date and timestamp
- Severity Type
- Product Component
- Message

To view Events:

1. Go to **Tools** > **Logs** > **Events**.
2. (Optional) Search for a specific event log.
3. Set a filter or use the default filter.
4. Press **Enter** to execute a search.

   The Events list is updated.
5. (Optional) Select to export the data and manage which columns display.

Related Topics

System Logging Configuration on page 457
Understanding Date and Time on page 43
Set a Logging Filter on page 382

View Station Events

If configured to do so, ExtremeCloud IQ Controller logs all station events. You can view a record of station events from the **Tools** workbench or from the **Clients** workbench.

Before viewing station events, configure station events from **Administration** > **System** > **Syslog**.

Station Events include the following information:

- Date and timestamp
- Event Type
- MAC Address
- IP Address and IPv6 Address (if appropriate)
- AP Name
- SSID
- Details

To view Station Events:

1. Go to **Tools** > **Logs** > **Station Events**. Or,

   Go to **Clients** and select a client from the list. Then, select the **Station Events** tab.
2. (Optional) Search for a specific event.
3. Set a filter or use the default filter.
4. Press **Enter** to execute a search.

   The Station Event list is updated.
5. (Optional) Select to export the data and manage which columns display.

Note
ExtremeCloud IQ Controller provides station event history for active stations. You can also search for inactive stations using a MAC address or user name.

Related Topics

System Logging Configuration on page 457
Understanding Date and Time on page 43
Set a Logging Filter on page 382

View Audit Events

ExtremeCloud IQ Controller logs all configuration changes made by administrators and system messages related to end-system activity. You can view a record of the changes and messages in the user interface.

Before viewing audit events, configure audit events from **Administration** > **System** > **Syslog**.

Audit events include the following information:

- Date and time stamp

- User ID of the administrator that made the change
- The type of change that was made

To view audit events:

1. Go to **Tools** > **Logs** > **Audit**.
2. (Optional) Search for a specific audit log.
3. Set a filter or use the default filter.
4. Press **Enter** to execute a search.

   The audit event list is updated.
5. (Optional) Select to export the data and manage which columns display.

Related Topics

System Logging Configuration on page 457
Understanding Date and Time on page 43
Set a Logging Filter on page 382

View All AP Events

If configured to do so, ExtremeCloud IQ Controller logs all AP events. You can view a record of the AP event in the user interface.

- Configure the AP Event Level from the device group Advanced Settings.
- Override the level for a single AP from the device Advanced Settings Overrides.
- Override the level for multiple APs from the Device List Actions menu.

AP Events include the following information:

- Date and time stamp
- AP Name
- AP Serial Number
- The severity type for the AP event
- Category
- Message

Note
In a High Availability Pair, the AP Events do not synchronize when the link between appliances is down, and no further synchronization is performed for the unsynchronized events after the connection is restored.

To view AP Events:

1. Go to **Tools** > **Logs** > **AP Events**.
2. (Optional) Search for a specific AP event.
3. Set a filter or use the default filter.
4. Press **Enter** to execute a search.

   The AP Events list is updated.
5. (Optional) Select to export the data and manage which columns display.

You can view event data for a specific AP from the AP page:

1. Go to **Monitor** > **Devices** > **Access Points**.
2. Select an AP.
3. Select the **AP Events** tab.

Related Topics

View AP Events — Single Access Point on page 104
System Logging Configuration on page 457
Understanding Date and Time on page 43
Set a Logging Filter on page 382

Set a Logging Filter

Create Date/Time filters to display entries that were logged within a specific window of time. To set a date and time filter for an ExtremeCloud IQ Controller:

1. Go to **Tools** > **Logs**.
2. To display the **Start Date/Time** dialog, select **Change**.
3. From the Time field, specify the hour and minutes and select **AM** or **PM**.
4. To set both the start and end dates, in the Date field, use the arrows to navigate to the month, then select the calendar day for the start date. Repeat to select the end date.
5. Select **OK**.

Entries that occur between the start and end date display. The filtered list will persist during your session. You can navigate away from the page and return to the same filtered list. However, the filter is cleared after you log out or reboot the controller.

AP Upgrade Report

The AP Upgrade Status Report provides summary statistics over the reporting period and the progress status of the AP upgrade request. View information on the AP group or drill down to view the status of each individual AP in the group.

The AP group is identified by the Upgrade Request Time. Each request is considered a group. A group must consist of APs that support the same firmware version. For example, currently all AP39xx series APs support firmware version: `10.51.15.0002.img` and all 11ax APs support firmware version: `7.5.0.0-005R.img`.

Each ExtremeCloud IQ Controller release includes default AP firmware versions for the supported APs. You can install additional firmware versions if necessary. Before initiating an AP Upgrade Request, verify that the AP firmware is installed on ExtremeCloud IQ Controller.

For each group, the report displays the upgrade status percentage, the estimated completion time, and the actual completion time. To display this same information for each AP in the group, select the group.

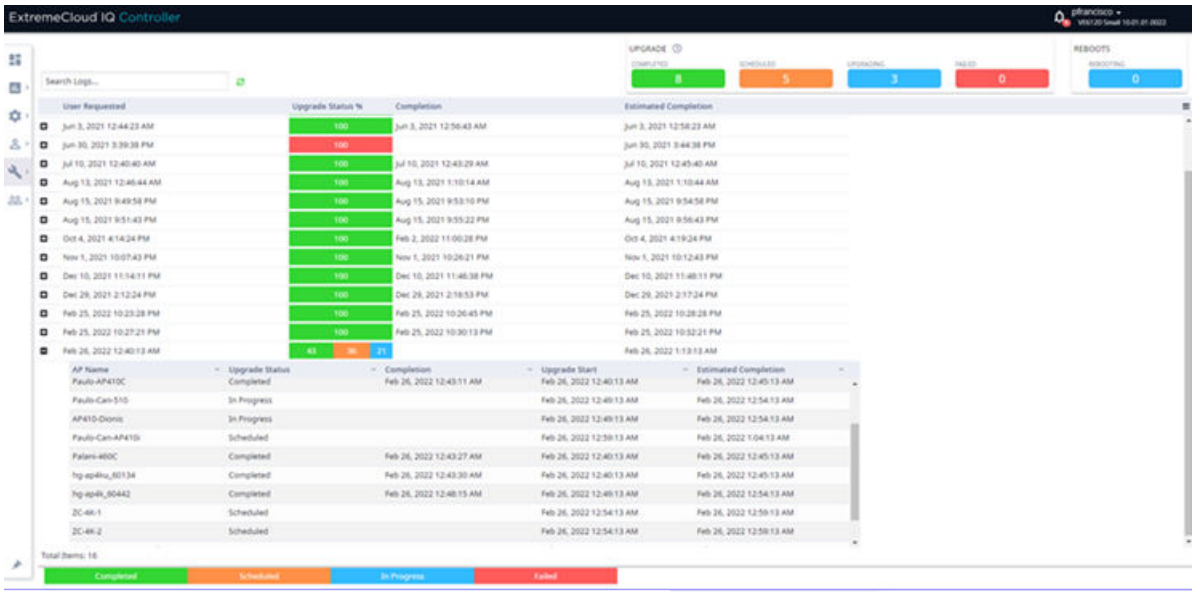


Figure 83: AP Upgrade Report

The AP upgrade status is color coded:

- Green indicates the percentage completed.
- Mustard indicates the percentage scheduled.
- Blue indicates the percentage in progress.
- Red indicates the percentage failed.

The AP Upgrade Status Report is available on the following workbenches:

- **Administration** — Go to **Administration** > **System** > **Software Upgrade**. Scroll down to **AP Images** and select **Upgrade Status**.
- **Tools** — Go to **Tools** > **AP Upgrade Reports**.

Note
Advanced Query and filtering from the **Logs** workbench are not available for the AP Upgrade Report.

The AP Upgrade Request does not provide a history of upgrades. If multiple upgrades are requested for the same AP, only the most recent upgrade request is shown. To view event information for the AP Upgrade Request, configure the System Log Level to `Information`. Go to **Administration** > **System** > **Logs**.

Select ☰ to configure the column display, refresh the display, or export the data in .csv.

Related Topics

Configuring Column Display on page 43
Logs on page 376
Install AP Firmware Image on page 442

Diagnostics

ExtremeCloud IQ Controller offers diagnostic tools to help you troubleshoot your network.

Go to **Tools** > **Diagnostics** > **Dashboard**.

The following widgets are available on the default dashboard:

- System Health
- Network Health
- Poll Site Stats
- Packet Capture

Related Topics

System Health Best Practice Widget on page 384
Network Health Widget on page 395
Smart Poll on page 396
Network Utilities on page 400
TCP Dump Management on page 401
Packet Capture on page 93
Opening Live SSH Console to a Selected AP on page 98
AP Service Tab on page 401
RADIUS Servers on page 410

System Health Best Practice Widget

The ExtremeCloud IQ Controller Overview dashboard offers a System Health widget that provides best practice information for your ExtremeCloud IQ Controller configuration. The System Health widget is part of the ExtremeCloud IQ Controller default **Diagnostics** dashboard. You can also find it under the **System Widgets**.

To access the System Health widget from the Diagnostics dashboard, go to **Tools** > **Diagnostics** > **Dashboard**.

To access the System Health widget from the Overview Dashboard:

1. Go to **Dashboard**.
2. Select , then **Widgets**.
3. Select the plus sign next to **System** to expand.
4. Drag the **System Health** widget onto the dashboard.

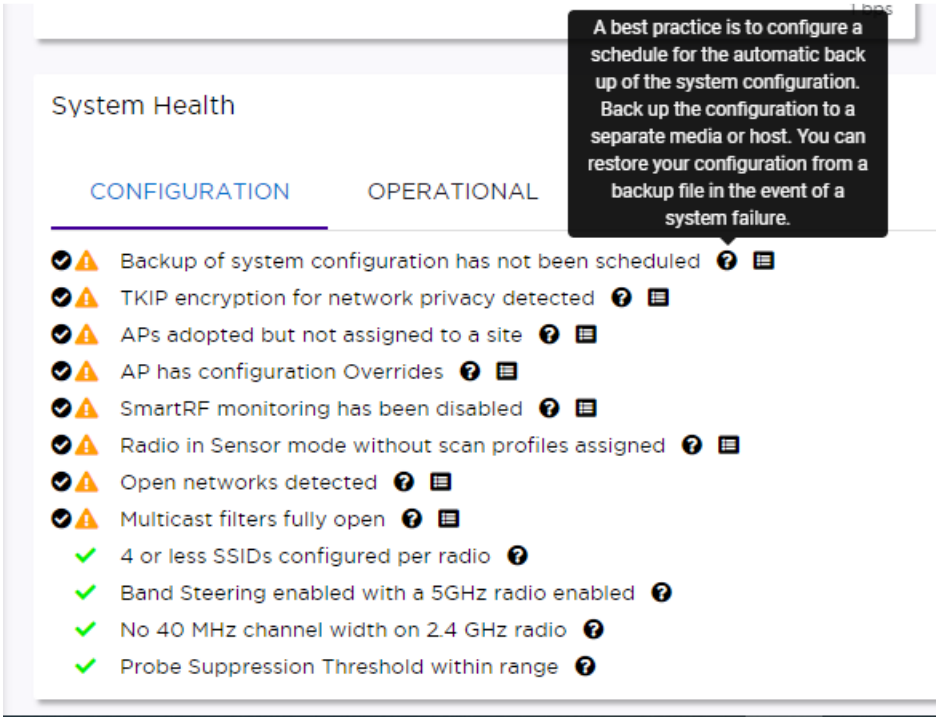


Figure 84: System Health widget

- A green check mark indicates that a best practice is being followed.
- A yellow warning icon indicates that your configuration is not optimal.
- A red icon indicates an error in your configuration.

  Fix all error conditions. You have the option to ignore warnings. They are provided to inform and encourage best practice configuration. You can accept warnings without fixing them.
- Select to accept the warning. If you accept a warning without fixing the configuration issue, a green warning icon displays .
- A green warning icon indicates that you accepted the warning without fixing it.
- Select for a description of each statement or warning.
- Select to jump to that area in ExtremeCloud IQ Controller to improve your configuration.

The notification icon indicates System Health warnings.

1. Select at the top of your screen, then select **System Health**.
2. Select the three dots to display the warning messages.

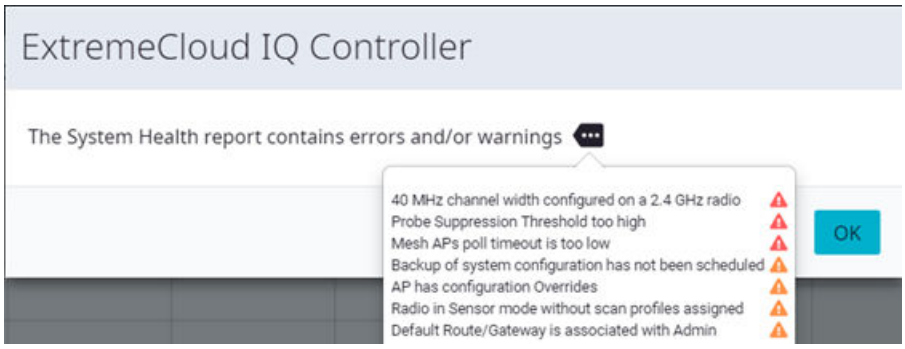


Figure 85: System Health Notification Report

The Best Practice information is captured in the Tech Support file, providing a useful summary snapshot of the system state and related alerts at the time when the Tech Support file was generated.

For details about the best practices, see:

- Configuration Best Practices on page 387
- Operational Best Practices on page 392
- Network Health Reports on page 395

Related Topics

Configuration Best Practices on page 387
Operational Best Practices on page 392
Network Health Reports on page 395
Diagnostics on page 384
Dashboard on page 44
Entitlement Health Checks on page 485
Maintenance on page 443

Configuration Best Practices

Table 99 describes details about the best practice configuration information that the System Health widget provides.

Table 99: System Health Widget Configuration Best Practices

Type	Field	Description
Configuration	Scheduled Configuration Backup	It is a best practice to schedule a configuration backup. Automatically back up the configuration to a separate media or host. You can restore your configuration from a backup file in the event of a system failure. See Configure a Backup Schedule on page 435.
Configuration	TKIP	TKIP encryption is considered to be a less secure means of communication. An industry best practice is to use a more secure option for network privacy. Disable the TKIP option within the WPA2 privacy settings. See Privacy Settings for WPA2 with PSK on page 258. A green check mark indicates that TKIP encryption is not used. A yellow warning condition indicates that TKIP encryption is enabled on a WLAN.
Configuration	Client-to-Client Communication	Some applications, like VoIP phones, require direct connectivity between clients on a bridged at controller network. Disabling client-to-client communication on a bridged at controller network may cause issues with VoIP connectivity.
Configuration	APs adopted but not assigned to a site	APs must be part of a device group and assigned to a site. See Sites Overview on page 30.
Configuration	AP has configuration overrides	Indicates that there are APs in your network with configured override settings. For a consistent configuration, a best practice is to configure the APs through the configuration Profile. Overrides are available for unique configuration. However, variances from the configuration Profile can result in APs not receiving general policy changes. Consider configuration Overrides carefully. To determine which APs are configured with overrides, from the **AP List**, display the **Overrides** column. See Access Points List on page 69.

Table 99: System Health Widget Configuration Best Practices (continued)

Type	Field	Description
Configuration	WEP encryption for network privacy detected	The Wi-Fi Alliance™ recommends against using WEP encryption. WEP encryption is easily broken, often taking less than a minute to break. If you must use WEP, apply a restrictive policy to the associated VLAN to reduce your exposure after a breach.
Configuration	Open networks detected.	Networks with Open access pose a security risk for your organization. Consider an authentication type such as MBA or Captive Portal.
Configuration	WLAN 802.11k Setting	Enabling 802.11k on a radio can cause radio reset. To avoid unexpected radio reset, all WLANs must have the same 11k setting; otherwise, adding and removing WLANs can cause radio reset.
Configuration	Manufacturing Certificate	A Best Practice is to enforce enablement of Extreme PKI certificate in the establishment of secure tunnels.
Configuration	Multicast filters fully open	Multicast traffic can have a negative impact on performance. Ensure that multicast access is restricted per topology. See Configuring a Multicast Rule on page 308.
Configuration	Mesh Node AP configuration	For a Mesh Node (non-Root) AP, a best practice is to configure Poll Timeout for at least 60 seconds.
Configuration	Mesh Root point configured to use dynamic RF management policy	Mesh Root APs require fixed channel assignment for proper access point operation.
Configuration	Mesh does not support Off-Channel Scan	**Note:** Supported on ExtremeCloud IQ Controller v5.16.03 with AP v7.5.1.2 or later. Non-root APs are configured with Mesh ACS (Automatic Channel Selection). This allows the non-root AP to follow the channel and width of the uplink AP. The non-root AP scans channels to find the best path to a root AP. Preferred Root and Preferred Neighbor settings influence the path to the root AP.

Table 99: System Health Widget Configuration Best Practices (continued)

Type	Field	Description
Configuration	APs have configured unsupported functionality	The following AP models do not support IoT and the 5GHz radio does not support 160MHz operation: • AP3935 • AP3965 • AP305C-1 • AP310i/e-1 • AP410i-1 • AP410C-1 • AP510i-1 • AP4000-1 For more information about channel width, see Channel and Power Settings on page 182.
Configuration	Radio in sensor mode with no scan profiles assigned	Indicates that you have a radio in Sensor mode without a corresponding AirDefense profile configuration. Scan functionality requires that you configure a radio for Sensor mode and configure Profile settings for AirDefense. All configuration is handled in the configuration Profile that is assigned to the device group. See Add or Edit a Configuration Profile on page 134.
Configuration	Number of SSIDs per Radio	One radio can support a maximum of eight SSIDs. However, it is a best practice to configure no more than four SSIDs to a single radio. This configuration can be at the Profile level or configured as an override for a specific AP. See Add or Edit a Configuration Profile on page 134. A green check mark indicates that four or less SSIDs are configured. A yellow warning indicates that more than four SSID are configured for a single radio.
Configuration	Band steering enabled and 5GHz radio disabled	Client Band Steering steers dual-band capable clients to connect to the 5.0 GHz radio band instead of the 2.4 GHz radio band. A 5.0 GHz radio must be enabled on the AP for Client Band Steering to function. See Band Steering on page 290.

Table 99: System Health Widget Configuration Best Practices (continued)

Type	Field	Description
Configuration	40 MHz channel width on 2.4GHz radio	Operating a 40MHz channel in a 2.4 GHz band can cause co-channel inference with access points in the vicinity. The 2.4 GHz band has limited available channels. Therefore, for proper channel isolation, a 2.4 GHz band allows 3-4 (region dependent) 20 MHz channels. Best practice is to configure a 40MHz channel on a 5 GHz radio. See Channel and Power Settings on page 182.
Configuration	Smart RF monitoring disabled	Enable Smart RF for dynamic RF management to provide RF performance optimization. Enable Smart RF from the **Basic Settings** tab. See Basic RF Management Settings on page 180.
Configuration	Probe suppression threshold	Probe Suppression Threshold should not be greater than -70dB. The Probe Suppression Threshold defines the signal strength value that is deemed too low to be acknowledged by the AP. Setting the threshold above -70dB can result in an AP not acknowledging clients in close proximity, leading to poor connectivity or a sub-optimal roaming experience. The best practice is to follow the Site Survey methodology to determine the best value for the AP installation. See Advanced AP Radio Settings on page 153.
Configuration	Role with more than 64 rules is assigned to an AP or Profile that does not support more than 64 rules.	ExtremeWireless Wi-Fi 6 access points support rule sets that contain up to 256 rules. AP39xx series access points support rule sets with no more than 64 rules . See Add Policy Roles on page 292.
Configuration	Roles with more than 64 rules are configured.	Roles with more than 64 rules may experience interoperability issues with different AP models and firmware revisions.
Configuration	Network with CWA is assigned to non-supported APs	Support for Centralized Web Authentication (CWA) is only available on Wi-Fi 6 access points. This feature is not supported on AP3900 series access points. See Centralized Web Authentication on page 278.
Configuration	Device Registration is not configured on at least one port.	The Device Registration attribute controls whether access points and switches can establish management sessions with the controller through the selected interface. For proper system operation, at least one interface is required for managed devices to connect.

Table 99: System Health Widget Configuration Best Practices (continued)

Type	Field	Description
Configuration	RADIUS Failover is not configured or there are not enough serves for redundancy	It is a best practice to configure at least one pair of RADIUS servers to support authentication redundancy.
Configuration	Bonded channels configured with a different frequency than the Management channel	Configure bonded channels with the same frequency as the Management channel. When channel width is larger than 20 MHz, use one 20 MHz sub-channel as a Management channel to transmit beacons. When Management channel frequency is configured differently than other channels, channel interference can occur and throughput is reduced.
Configuration	Default Route configured for router on data interface	Configure the Default Route/Gateway with a next-hop associated with a physical interface. Do not point the Default Route to the Admin interface. A best practice is to map the Default Route through a topology on a data port for proper system functionality. If necessary, configure the static routes via the Admin port for administration level access.
Configuration	Hotspot WLANs with the configured number of IDs in the roaming consortium.	Configure authentication of mobile devices to the members of a roaming consortium, or for a particular service provider that has a roaming consortium. Add the appropriate **IEEE-assigned Organizational Identifier (OI)**. Specify up to eight identifiers unique to the organization that are part of the MAC address. The AP39xx access points continue to support only two identifiers. For more information, see SP Identification on page 267.
Configuration	DNS server is not configured.	ExtremeCloud IQ Controller requires internet connectivity and a Domain Name Server (DNS) configuration. Verify DNS server settings. For more information, see Host Attributes and refer to the *ExtremeCloud IQ Controller Deployment Guide*.

Related Topics

Operational Best Practices on page 392
Network Health Reports on page 395
Diagnostics on page 384
Dashboard on page 44

Entitlement Health Checks on page 485

Operational Best Practices

Table 100 describes the details for the operational best practices that the System Health widget provides.

Table 100: System Health Widget Operational Best Practices

Type	Field	Description
Operational	Certificate Authentication	Pre-installed Extreme certificates allow validation between ExtremeCloud IQ Controller and an AP. APs that do not support signed certificates, can provide self-signed certificates. In this case, you must disable Enforce Manufacturing Certificate on ExtremeCloud IQ Controller for the AP. AP Authentication failure messages are logged in the ExtremeCloud IQ Controller Events Log.
Operational	Mesh AP operating on DFS channel.	Due to DFS procedures and mandatory 'Stay off Channel' periods, APs operating on DFS channels in a Mesh topology can result in service outages.
Operational	AP recommended version image	APs are not running the recommended version image. Run the supported AP firmware version. Running other firmware revisions can lead to unexpected results. See Upgrade AP Images on page 442.
Operational	AP with Dual 5 GHz and power provided is AF	AP510 and AP410 support Dual 5 GHz radios and AF (low power) is provided. Therefore, Radio 2 will be shut down. Configure the AP radio for 2.4 GHz or 5 GHz, or provide AT (high power).
Operational	Backup secure tunnel	Secure tunnel is supported on ExtremeWireless Wi-Fi 6 APs. To improve resilience and reduce the outage interval associated with a failover event in a high-availability pair, access points establish session tunnels to both peers in a high-availability pair.
Operational	NTP	Proper time stamp synchronization is facilitated through Network Time Protocol (NTP). If the NTP server is not reachable, verify the NTP server settings. See Network Time on page 433.
Operational	Service interface is not operational. Check connectivity for proper service.	System functions reference specific interfaces for connectivity. For proper operation, corresponding system interfaces must be enabled and operational.

Table 100: System Health Widget Operational Best Practices (continued)

Type	Field	Description
Operational	Backup tunnel established to ExtremeCloud IQ Controller	To improve resilience and reduce the outage interval associated with a failover event in a high- availability setup. Access points establish session tunnels to both peers in a high-availability pair.
Operational	AP acknowledgment message	APs send an acknowledgment message for each configuration update. A missing configuration acknowledgment message from an AP can indicate a connectivity issue.
Operational	Communication between AP and controller over port 13910 is blocked by the firewall	For proper communication between the AP and the controller, ensure that Port 13910 is open in the firewall. **Note:** When the AP is more than one hop away, setting the default route via the Management port can also block communication between an AP and the controller.
Operational	AP connection to primary controller	In the event of an unexpected release of APs, check your network connectivity between APs and the controllers for possible interruptions.
Operational	Adoption rules did not successfully assign APs to site	Consider the following when configuring adoption rules for AP site assignment: • The selected AP Profile must match the AP hardware type. • The regulatory domain of the AP must match the Country setting for the site. For more information, see Adding or Editing Adoption Rules on page 318.
Operational	High-Availability Configuration	High-Availability connectivity status. Verify your high-availability configuration. See Availability on page 445.
Operational	High-Availability Synchronization	High-Availability connectivity status with synchronization message.

Table 100: System Health Widget Operational Best Practices (continued)

Type	Field	Description
Operational	Assigned Entitlements Status	The system must be licensed to operate. A best practice is to start the license renewal process at least 90 days before the license expiration date to avoid interruption of functionality. The following are the available status warnings: • Yellow status warning — Some assigned entitlements expire in less than 90 days. • Red status warning — Some assigned entitlements expire in less than 30 days. To view the list of entitlements, go to **Administration** > **License** > **Entitlements**. For more information, refer to Product Subscription License on page 475.
Operational	ExtremeCloud IQ Controller is not onboarded to ExtremeCloud IQ.	Onboard ExtremeCloud IQ Controller into ExtremeCloud IQ to take advantage of Cloud Visibility. After ExtremeCloud IQ Controller is onboarded into the cloud, all access points that are discovered by that controller are visible in ExtremeCloud IQ. Cloud connectivity is displayed on the License Details page. For information about how to onboard ExtremeCloud IQ Controller to ExtremeCloud IQ, refer to the *ExtremeCloud IQ Controller Deployment Guide*.
Operational	Client Address Protection. Clients denied.	Indicates that a client has attempted to access the network though an IP address that is configured on the Protected IP Address List. Select the icon to display the protected IP address and the MAC address of the offending client. For more information, see Site Allow List/Deny List on page 202.

Related Topics

Configuration Best Practices on page 387
Network Health Reports on page 395
Diagnostics on page 384
Dashboard on page 44
Entitlement Health Checks on page 485

Network Health Widget

Use the Network Health widget to monitor the Availability Link Status and the Synchronization Status for an availability pair. This information is available from the Diagnostics Default dashboard and the main Overview dashboard.

To access the **Diagnostics** dashboard, go to **Tools** > **Diagnostics** > **Dashboard**.

To add Network Health to the **Overview** dashboard:

1. Go to **Dashboard**.
2. Select to edit the dashboard.
3. Select **Widgets** > **System**.
4. Drag the **Network Health** widget onto the dashboard.

Related Topics

Network Health Reports on page 395

Network Health Reports

The Network Health Report widget offers additional network information. Use this information to understand device performance and traffic flow on the network.

Table 101: Network Health Reports

Report	Description
Access Points in Low Power Mode	Indicates the number of APs operating in low power mode. Select the value to jump to the Access Points List.
Active Access Points on Primary	Indicates the number of APs homed to the primary appliance.
Active Access Points on Backup	Indicates the number of APs homed to the secondary appliance.
Inactive Access Points	Indicates the number of inactive APs. APs are considered inactive when they have been registered (onboarded) to the controller but are currently inaccessible (not connected).
Synchronization Status	Indicates the synchronization status of controllers in an availability pair.
Mobility Status	Indicates the status of the mobility tunnel when the controller is operating as an Inter-AC Mobility Agent. For more information, see Mobility Settings on page 449.
Availability Link Status	Indicates the status of link between to controllers in an availability pair. For more information, see Availability on page 445.
Active Switches	Indicates the number of active switches. A switch is considered active when the switch has been onboarded and connected to the controller.

Table 101: Network Health Reports (continued)

Report	Description
Inactive Switches	Indicates the number of inactive switches. A switch is considered inactive when the switch has been onboarded to the controller, ready for management, but has not yet connected.
Trouble Switches	Indicates the number of switches in the Trouble status. Trouble status indicates switches that have been defined as onboarded and managed by the controller (successfully connected) but currently the switch is unreachable (no active management link).

Related Topics

Configuration Best Practices on page 387
Operational Best Practices on page 392
Diagnostics on page 384
Dashboard on page 44
Entitlement Health Checks on page 485

Smart Poll

Smart Poll provides reports that help you determine the health of the connection between an access point and any valid IP address target or valid Fully-Qualified Domain Name (FQDN). Link stability is determined by Round Trip Time (RTT) and packet loss statistics. Smart Poll evaluates the link between an individual AP and ExtremeCloud IQ Controller or any user-defined target.

Smart Poll reports are available from the **Tools** > **Diagnostics** > **Dashboard**, from the main **Dashboard**, from the **Sites** page, and from the **AP** page.

From the Diagnostics dashboard and the main **Dashboard**. The Dashboard widget compares sites based on the average RTT and packet loss stats for all targets and all APs in each site.

Main Dashboard

To access the Poll Sites Stats widget from the main dashboard:

1. Go to **Dashboard**.
2. Select to edit the dashboard.
3. Select **Widgets** > **Troubleshooting**.
4. Drag the **Poll Sites Stats** widget onto the dashboard.

Diagnostics Dashboard

To access the Poll Sites Stats widget from the Diagnostics dashboard, go to **Tools** > **Diagnostics** > **Dashboard**.

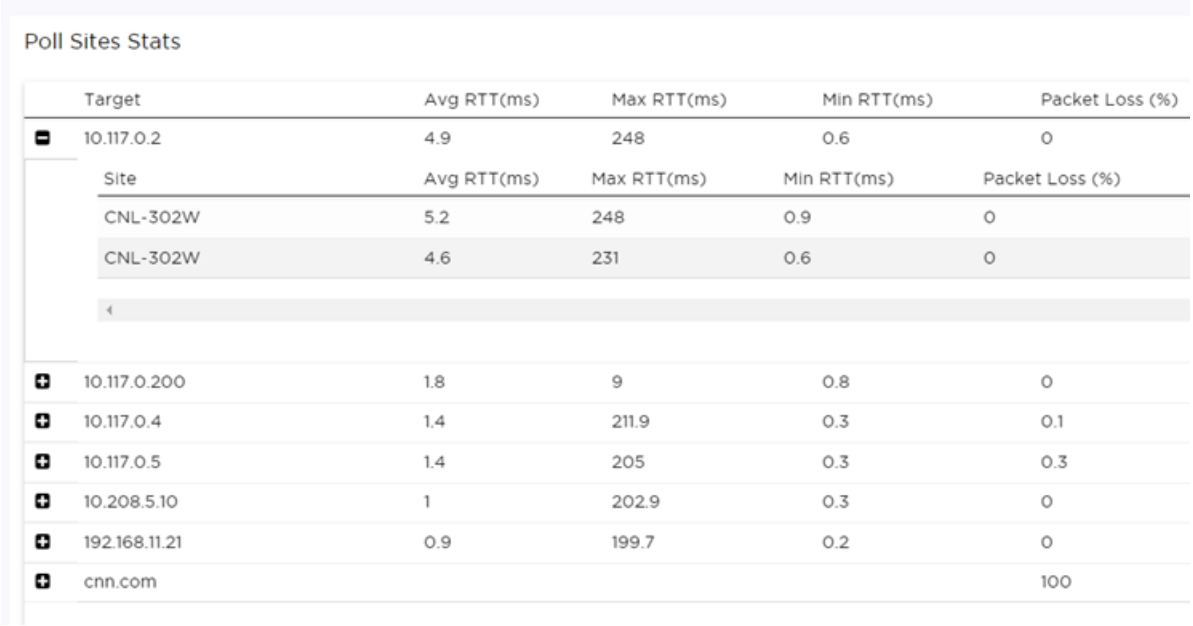


Figure 86: Dashboard Poll Site Stats

Sites Poll Data

From the **Sites** page. Charts compare mean RTT or packet loss across all targets in the selected site with quantitative RTT or packet loss across all sites.

To access the sites poll data:

1. Go to **Monitor** > **Sites**.
2. Select a site.
3. Select **Troubleshooting** > **Smart Poll**.

Figure 87 compares Round Trip Times for selected targets within a site. The grayed area indicates the baseline values for the site.

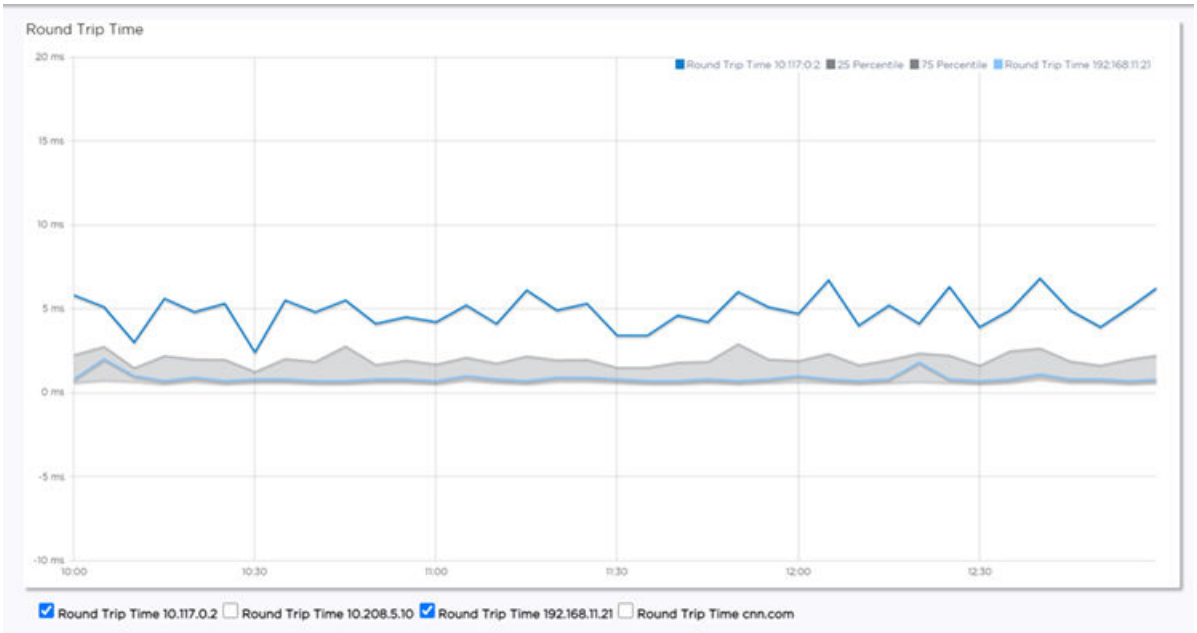


Figure 87: RTT in the Site Context

Figure 88 compares packet loss for selected targets within a site. The grayed area indicates the baseline values for the site.

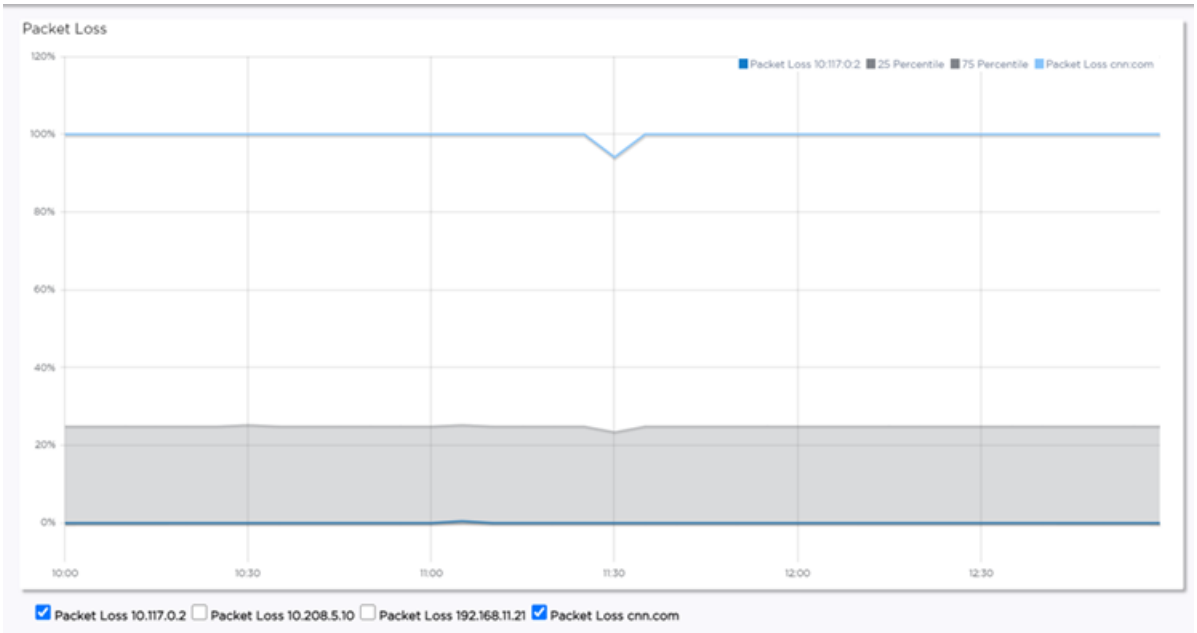


Figure 88: Packet Loss in the Site Context

AP Poll Data

From the **AP** page:

1. Go to **Monitor** > **Devices** > **Access Points**.
2. Select an AP.

3. Select **Troubleshooting** > **Smart Poll**.

The following reports are available:

- Round Trip Time (RTT) and Packet Loss statistics for a Smart Poll enabled AP. The RTT and Packet Loss table summarizes the average RTT and packet loss across targets configured for the selected AP.

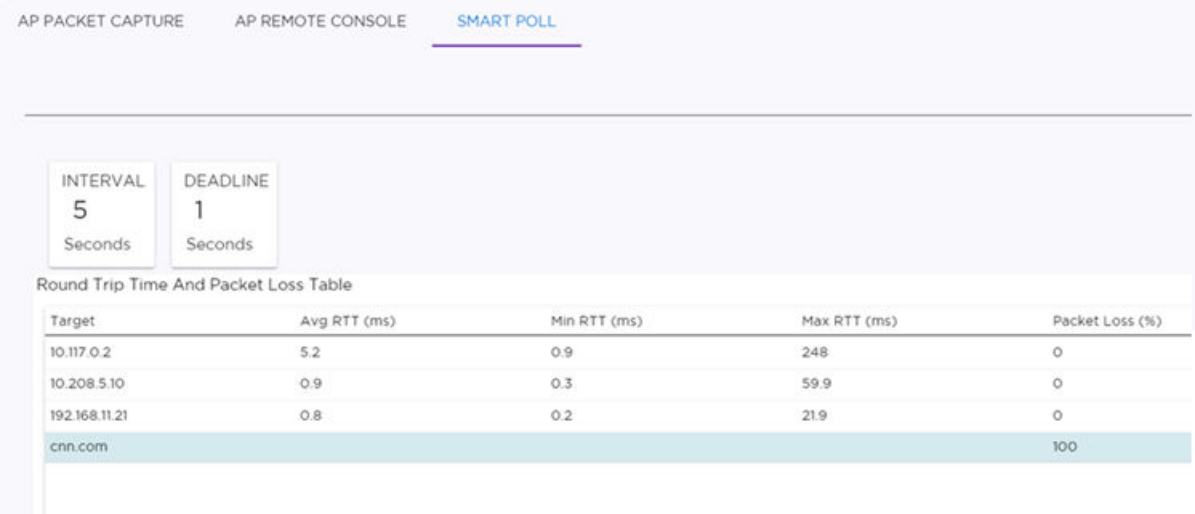


Figure 89: RTT and Packet Loss for Selected AP

- RTT and Packet Loss for a specific target. The dual Y-axis chart shows RTT and Packet Loss over the selected time period for each target configured for the selected AP.

Figure 90: RTT and Packet Loss for a specific Target

You can configure Smart Poll for all APs in a device group from the device group **Advanced Settings** dialog. You can also override Smart Poll configuration for a selected AP.

Report Duration

- Select to set the **Duration** value for the time period reported. Valid duration values are:
  - Last 3 hours
  - Last 3 days

- Last 14 days

- Select to refresh the data on demand.
- Hover the mouse over a widget to display tool tip information.

Related Topics

Diagnostics on page 384
Advanced Configuration Profile Settings on page 172
Advanced Setting Overrides on page 221

Network Utilities

Use wireless controller utilities to test a connection to the target IP address (or Fully-Qualified Domain Name) and record the route through the Internet between your computer and the target address. You can also use controller utilities to capture exception traffic, which can be useful for network administrators when debugging network problems.

Configure the following parameters:

Table 102: Network Utilities

Field	Description
Target IP Address or Fully-Qualified Domain Name (FQDN)	IP address or FQDN for the test target.
Use specific source interface	Indicates if a specific interface will be selected for the test. Select the interface from the Select Interface field. When this option is cleared, ExtremeCloud IQ Controller runs the test based on the interface selected in the routing table.
Select Interface	Used with Specific Source Interface option. See list of possible interfaces on the **Interface** tab.
Ping	Initiate the Ping network utility to determine reachability of the IP address or FQDN that you specify.
Trace Route	Initiate the Trace route command, which traces the path of a packet from ExtremeCloud IQ Controller to the IP address or FQDN that you specify. It lists the routers it passes until it reaches its destination, or fails to. It also indicates the length of each hop.

Related Topics

TCP Dump Management on page 401
Packet Capture on page 93

TCP Dump Management

Table 103: TCP Dump Management

Field	Description
Interface	Target interface. See the list of possible interfaces on the **Interface** tab.
Filename	Specify the name of the dump file.
Save File To	Specify where to save the dump file.
Capture File Size (MB)	Specify the maximum limit of the dump file in MB. This feature enables you to control the size of the resulting dump file so the file does not become too large.
Capture Files	List of previously created dump files. Select a file to take action.

AP Service Tab

The AP Test measures the integrity of the access point connectivity in a production network. Test the network environment, measuring AP connectivity from end-to-end on either a wired or wireless network. This feature is supported on Bridged at AP or Bridged at Controller deployments.

Configure and automate one or more of the following tests to run against the production servers:

- Ping
- Traceroute
- Iperf3 – Throughput

Any combination of tests (referred to as a test suite) can be run on selected access points. Both the test suite and the test run can be saved and reused, and the unique results from each run can be exported in Json format.

To test the AP service:

1. Configure the test suite — Configure the tests to run and the MAC address and IP address of the client traffic. You can specify specific client addresses or test client traffic from default and available addresses.
2. Configure and run the test run — From the Test Run parameters, specify the network environment — you can run tests on either a wired or wireless network. Select the pre-configured test suite, the access points, and the network on which you will run the test.
3. View and analyze the test results — Detailed results are provided for each test. For wireless tests, view results for a specific AP, and analyze RF metrics on radio

frequency quality, channel utilization, channel noise, and signal to noise ratio (SNR) levels.

Important
AP service *is interrupted* when running tests on a wireless network. AP service *is not interrupted* while running tests on a wired network.

Related Topics

AP Test Suites on page 402
AP Test Run on page 405
AP Test Results on page 408

AP Test Suites

A test suite is a group of tests that you can automate to run against selected APs. The test suite parameters define which tests are run and determine the client MAC and IP addresses. The **Test Suites** tab lists all configured test suites.

Take the following actions:

- To add a test suite, select **Add** and configure the suite parameters.
- To edit the test suite parameters, select a test suite to display the parameters. Then, modify the parameters as necessary.
- To refresh the list, select ☰ and then select **Refresh**.
- To find a specific list row, use the **Search** field.

Related Topics

Test Suite Parameters on page 402

Test Suite Parameters

Configure and automate one or more of the following tests to run against the production servers:

- Ping
- Traceroute
- Iperf3 – Throughput

Note
The test suite can be saved, modified, and reused.

To add or edit a test suite, configure the following parameters:

Suite Name

Name of the test suite.

Tests

Configure one or more of the following tests:

- Ping
- Traceroute
- Iperf3 – Throughput

For each test, provide a hostname or target IP address, and specify the parameters to use for each test.

- To include or exclude a test, select or clear the **Enable** check box.
- To add additional targets, select .
- To delete targets, select .

Client

Specify the source of the client traffic. Here you can specify a specific MAC address or use a default address, and you can specify a static IP address or use the IP address that is provided from the DHCP server.

- To save the test suite parameters, select **Save**.
- To delete the test suite, select **Delete**.

Related Topics

Optional Parameters for Each Test on page 403
AP Test Run on page 405
AP Test Suites on page 402

Optional Parameters for Each Test

The AP Test Service supports tests that provide insight into network connectivity. This topic outlines the supported parameters for each test.

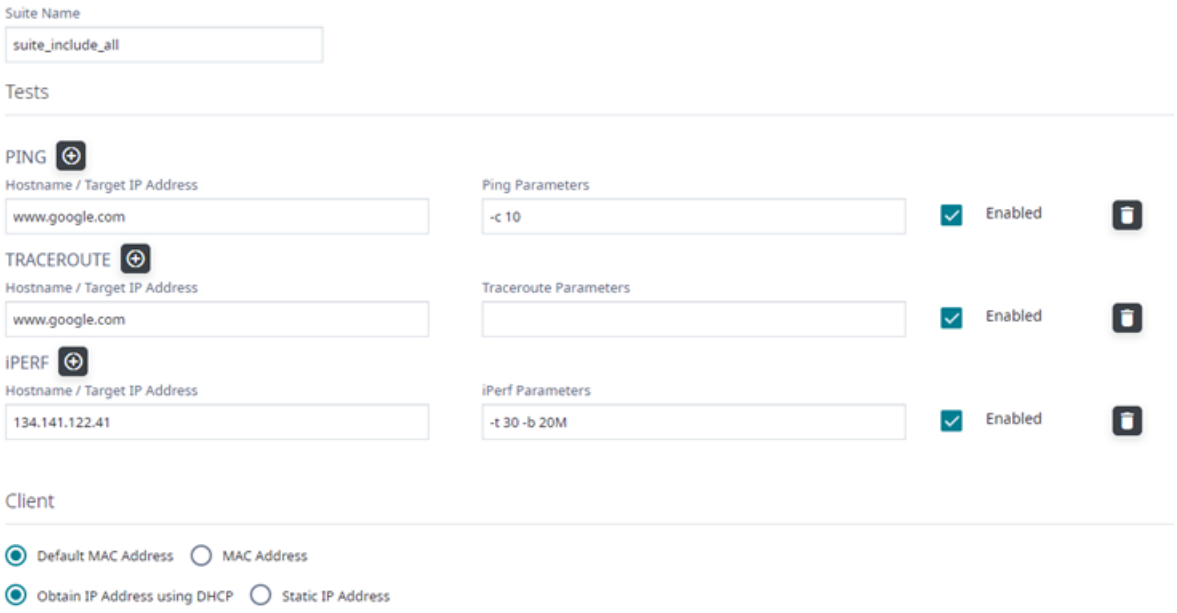


Figure 91: AP Service tests from the Test Suite tab

Ping Command Options

The Ping command is issued from the emulated wired client inside the access point or Probe AP to the specified target. The target can be a server IP address or a hostname.

Table 104: Supported Ping Command Options

Option	Description
-c CNT	Send only a specific packet count.
-s SIZE	Send SIZE data bytes in packets (default:56)
-i SECS	The number of seconds between pings.
-W SEC	Number of seconds to wait for the first response after all -c CNT packets are sent (default:10)
-w SEC	Number of seconds until ping exits (default:infinite) Ping can exit earlier with -c CNT option.
-q	Quiet, only displays output at start and when finished

Traceroute

The traceroute command is issued from the emulated wired client inside the access point or Probe AP to the specified target. The target can be a server IP address or a hostname.

Table 105: Supported Traceroute Command Options

Option	Description
-F	Set the do not fragment bit
-I	Use ICMP ECHO instead of UDP datagrams
-l	Display the TTL value of the returned packet
-d	Set SO_DEBUG options to socket
-n	Print numeric addresses
-r	Bypass routing tables, send directly to HOST
-v	Verbose
-m	Max time-to-live (maximum number of hops)
-t	Type-of-service in probe packets (default 0)
-w	Time in seconds to wait for a response (default 3)
-g	Loose source route gateway (8 max)

iperf3 Throughput

A test script initiates iperf3 sessions between the AP iperf3 client and the designated iperf3 server. Data can be configured to flow in both directions — from the AP to the server or from the server to the AP. All iperf3 command options are supported.

The iperf3 Throughput test indicates the minimum guaranteed AP throughput. To run a stress test on network devices and servers, run iperf3 Throughput in parallel on a large number of APs.

For command help, issue the following:

```
iperf3 [-h|--help] [-v|--version]
```

Related Topics

AP Test Run on page 405
Test Suite Parameters on page 402

AP Test Run

The **Test Run** tab lists all configured test runs.

From the **Test Run** parameters screen, select the wired or wireless environment and the network to test.

Take the following actions:

- To add a test run, select **Add** and configure the test parameters.
- To edit the test run parameters, select a test run to display the test parameters. Then, modify the parameters as necessary.
- To refresh the list, select ☰ and then select **Refresh**.
- To find a specific test run, use the **Search** field.

Wired Network Test

AP service *is not interrupted* while running tests on a wired network. Provide the following information for each test run:

- Test Suite Name
- Test Client Network
- Test Duration
- Base Port
- Selected Access Points

Wireless Network Test

Important
AP service *is interrupted* when running tests on a wireless network.
When running tests in Wireless Client mode, the selected AP stops offering WLAN service and becomes a client to the pre-confgured SSID (subject to compatible Privacy settings configuration).

To test a wireless network, configure one or more of the access points as a Probe AP. The radios on the Probe AP are configured to emulate a mobile user. Effectively, the Probe AP becomes the client of the other APs in the network.

Before you begin, understand the AP floor plan. When testing a wireless network, you must be aware of where the Probe APs are located and the name of the network SSID to which they will connect. The Probe APs should be evenly dispersed across the testing area.

Any AP in a deployment can be configured to act as a wireless service level probe:

- Select the APs that will function as the wireless service level probes.

  When running a wireless test, select the Probe AP that is located in or near the physical location of the test. The Probe AP switches to client mode and searches for the network SSID for connection to the test network, on the defined Wi-Fi band (2.4 GHz, 5 GHz, or 6 GHz).
- The tests that are specified in the test suite are run against the selected network, over the selected radio bands.
- Additionally, RF link statistics (RSSI) are collected to quantify the RF link quality.
- After tests are complete, the Probe AP is automatically returned into service.

Note
APs configured for Client Bridge or Mesh Networking are not supported as Probe APs.

Related Topics

Test Run Parameters on page 406

Test Run Parameters

The test run parameters depend on the network environment. Specify the test run environment as wired or wireless. The test run can be saved, modified, and reused.

To add or edit a test run, configure the following parameters:

Test Run Name

Name for the test run.

Traffic Test Environment

- Select **Wired** to test wired connectivity.
- Select **Wireless** to test wireless connectivity and network RSSI.

Suite Name

The name for the test suite. A test suite is a group of tests that can be run on any AP. A Test Suite record defines a test sequence of one or more generic tests that can be run by any AP in the system.

Test Network

The network that is being tested.

The following network authentication types are supported: OPEN, WEP, OWE and WPA2-Personal (PSK).

Test Duration

Maximum about of time allocated for the test. Valid values are 6-60 minutes. After the Test Duration limit, all APs are restored to the normal service state, and an incomplete test is terminated without result. A best practice is to configure the Test Duration value greater than the sum total of all enabled tests in the selected test suite.

Iperf Base Port

Specify the base port number. This is the starting point when running test with multiple APUTs in parallel. The AP Test Manager starts the first test at the base port and increases the port number by 1 to run multiple tests in parallel. Before starting the test run, make sure the iperf server instance on the ports has been launched.

Review a sample testing script here.

Radio Band

Wireless test only. Select the AP radio band to be tested. When an AP model offers more than one radio on a selected band, the lower radio is included in the test.

Access Points List

Select one or more access points to run the test against. To find a specific AP, use the **Search** field.

Note
AP service *is interrupted* when running tests on a wireless network.
When running a wireless test, select the Probe AP that is located in or near the physical location of the test. The Probe AP switches to client mode and searches for the network SSID for connection to the test network, on the defined Wi-Fi band (2.4 GHz, 5 GHz, or 6 GHz).

- To save the test run parameters, select **Save**.
- To run the test, select **Start Test Run**.
- To delete the test run, select **Delete**.

Related Topics

Example Testing Script on page 407
AP Test Run on page 405

Example Testing Script

The following is an example of a testing script that runs multiple tests in parallel, using multiple instances of iperf servers. When you have installed iperf3 on a Linux system, running the script can launch iperf server with multiple parallel instances, where each instance has a unique port.

```
#!/bin/bash
# Run multiple parallel instances of iperf servers
# This example assumes the port numbers used by the servers start at 5001 and increase by
one
# e.g. 5001, 5002, 5003, ...
# To specify a different base port, change the following parameter value
# to be: firstport - 1
base_port=$1
let base_port-- # Command line input: number of servers
# e.g. 5
num_servers=$2
shift # Command line input: base report file name
# e.g. report
report_base=$2
shift # Optional command line input: other iperf options
# e.g. -u
iperf_options="$*" # Run iperf multiple times
for i in `seq 1 $num_servers`; do         # Set server port
```

```
        server_port=$(($base_port+$i));         # Report file includes server port
        report_file=${report_base}-${server_port}.txt
        echo " report_file --> $report_file"          # Run iperf
        iperf3 3 3  -s   -p $server_port  -1  $iperf_options &> $report_file & done
```

Related Topics

Optional Parameters for Each Test on page 403
Test Run Parameters on page 406

AP Test Results

The **Test Results** tab lists the results for each test run. Although test runs can be repeated and test suites can be reused, the results of a test are always unique. Test results are saved for 30 days, and you have the option to export test results for safekeeping.

Note
Test results can be lost after you upgrade ExtremeCloud IQ Controller. Export results for safekeeping.

The following information is provided on the **Test Results** tab:

- Status of the test
- Start and end time of the test
- Test run name
- Test suite name

Take the following actions:

- To refresh the list, select ☰ and then select **Refresh**.
- To find a specific list row, use the **Search** field.
- To sort results, select the column header.
- To export the test results, select **Export**.

Select a row to view more details.

Related Topics

Test Result Details on page 408
AP Test Suites on page 402
AP Test Run on page 405

Test Result Details

Select a specific row to display the result details for that test run. Then, select a specific AP to view the results. The details that display depend on the configured test suite and test run parameters.

Test details refer to one or more of the following tests:

- Ping
- Traceroute
- Iperf3 – Throughput

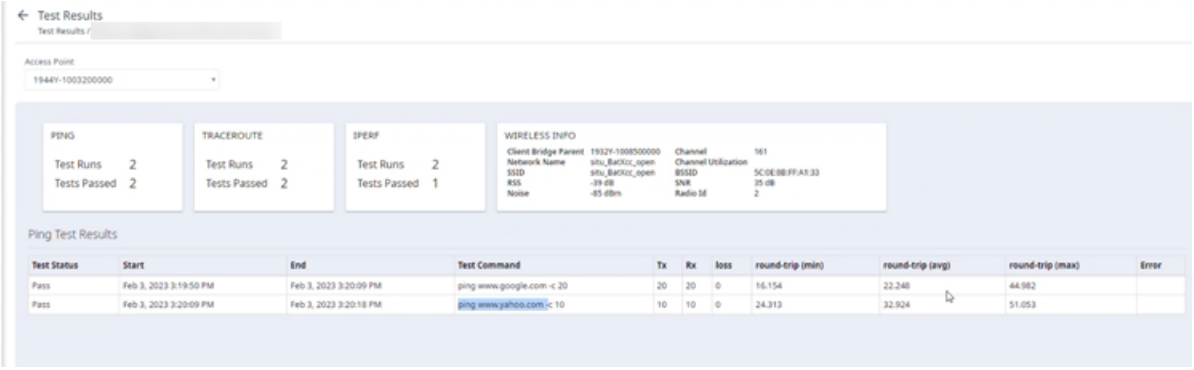


Figure 92: AP Service Test Result Details

- For each test, the number of times the test was run and the number of times the test passed is displayed.
- The following details for each test display:
  - Test Status
  - Start and End times for the test
  - Test command syntax
  - The following measurements: Tx, Rx, Loss, Round Trip (Minutes), Round Trip (Average), Round Trip (Max)
  - Errors
- Additionally, a wireless network test show the following details:

  Client Bridge Parent

  The serial number of the infrastructure AP in a Client Bridge deployment

  Network Name

  The name of the wireless network being tested

  SSID

  The Service Set Identifier of the wireless network being tested

  RSS

  Received Signal Strength. This value measures how well the selected AP can receive a signal.

  Noise

  Non-Wi-Fi interference measured in dBm

  Channel

  Radio channel for the selected AP

  Channel Utilization

  - BSSID. The MAC address of the radio interface that the client device is currently connected to. This is useful because each access point has a range of MAC addresses assigned to it.
  - SNR. Signal to Noise Ratio
  - Radio ID. Indicates the AP radio. Possible values are 1, 2, or 3.

Related Topics

AP Test Run on page 405
AP Test Suites on page 402
AP Test Results on page 408

RADIUS Servers

RADIUS Server related authentication metrics are provided for troubleshooting the ExtremeCloud IQ Controller RADIUS interface.

Report Duration

From the top of the **Dashboard** page:

- Select to set the **Duration** value for the time period reported. Valid duration values are:
  - Last 3 hours
  - Last 3 days
  - Last 14 days
- Select to refresh the data on demand.
- Hover the mouse over a widget to display tool tip information.

Go to **Tools** > **Diagnostics** > **RADIUS Servers** to view the following widgets.

Health

The **Health** tab displays data that indicates the condition of the RADIUS servers. The Servers list provides data on the percentage of clients affected by the following:

Server Unreachable

This scorecard indicates the amount of time that the RADIUS server is unreachable.

The GUI label **X%/Y minutes** represents the following metrics:

- Y is the number of minutes the server is down
- X% is the number of minutes the server is down (Y) divided by the total sample period in minutes

The total sample period can be measured in any of the report duration values.

Dot 1x Excessive Failures

This scorecard indicates that the RADIUS connection is unstable, resulting in unsuccessful Dot 1x Transactions. The scorecard shows when the failed rate percentage is greater than 20% for the selected duration period. It also shows the number of clients disconnected during this period due to RADIUS issues.

Criterion: Defined by the change in transactions failed per sample period divided by the change in transactions issued per sample period is > 20%.

The GUI label **X%/Y minutes** represents the following metrics:

- Y is the number of minutes where the criterion is True

- X is the number of minutes where the criterion is True (Y) divided by the total sample period in minutes

  The total sample period can be measured in any of the report duration values.

Excessive Delay

The scorecard indicates when the RADIUS request RTT is greater than 500ms for the selected duration period. It also shows the number of clients disconnected during this period due to RADIUS issues.

Criterion: Defined as RADIUS response divided by round trip time is > 500ms.

The GUI label **X%/Y minutes** represents the following metrics:

- Y is the number of minutes where the criterion is True
- X is the number of minutes where the criterion is True (Y) divided by the total sample period in minutes

  The total sample period can be measured in any of the report duration values.

Select a server from the list and view widget data.

Expert

The **Expert** tab provides a comparison between selected servers for the same data points. Select the servers from the Servers list and select **Apply**.

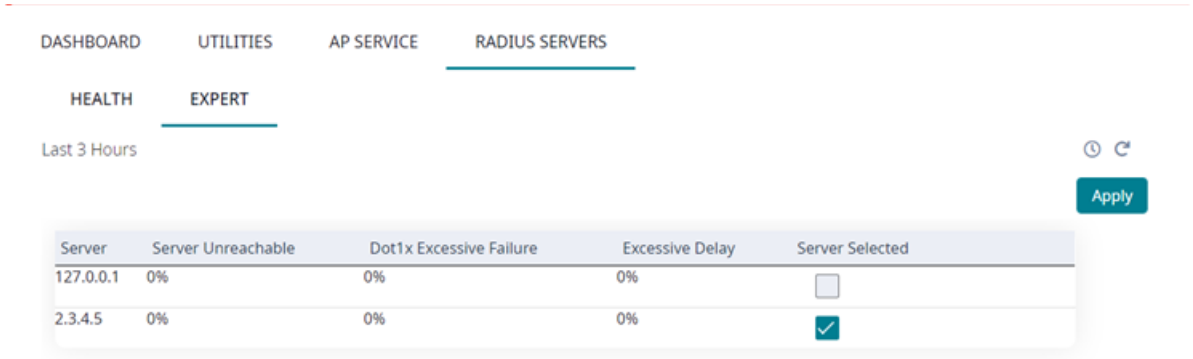


Figure 93: Server List

Additionally, you can take the following actions on each chart:

- To show or hide specific server chart data, from the key for each chart, select an individual server IP address.

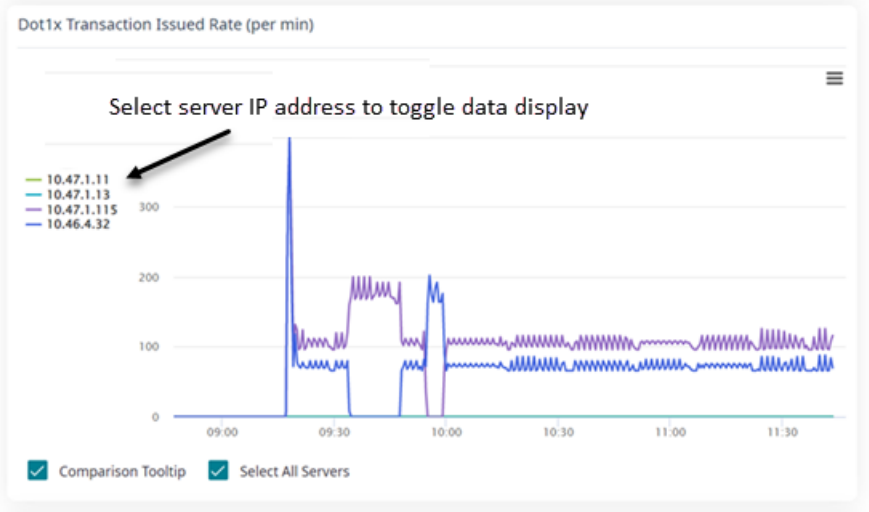


Figure 94: Toggle data display

- To zoom in, select an area of the chart and drag. To return to the original zoom, select **Reset Zoom**.

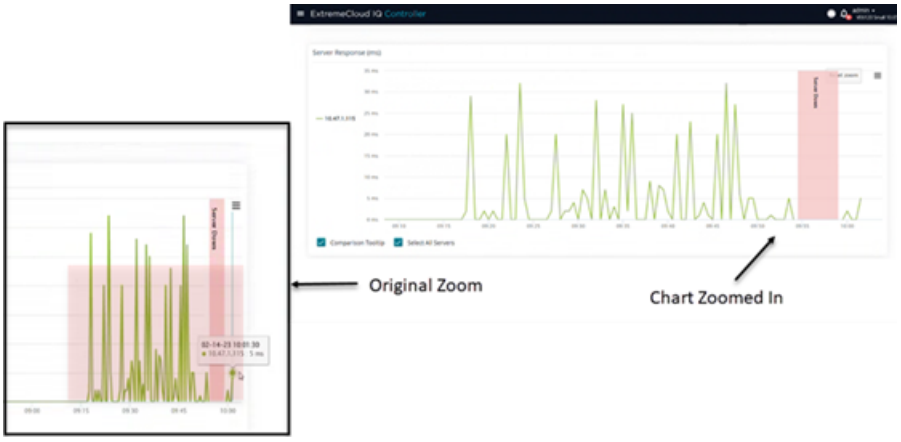


Figure 95: Chart Zoom

You can also select:

- **Show All Servers** — To compare all servers. This refers to all selected servers. If a server is not selected at the top of the page, it is not included in **Show All Servers**.
- **Shared Tool Tip** — To display server data in a comparison tool tip.

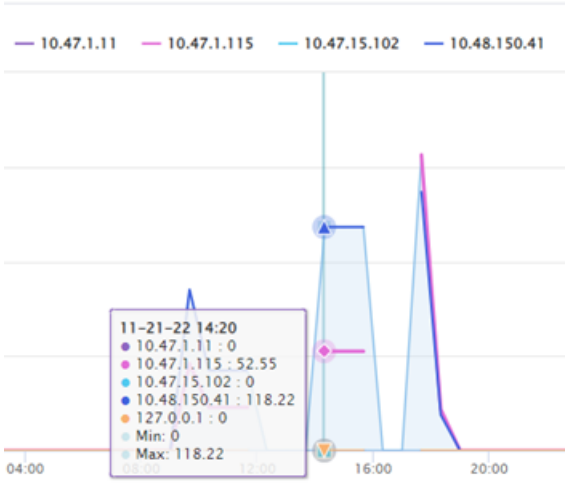


Figure 96: Shared Tooltip for Selected Servers

Figure 96 shows on November, 21, 2022 at 14:20 the **Dot1x Transaction Success Rate** (per minute) for five selected servers. The minimum value and the maximum value are also displayed.

Example Widgets

The following figures illustrate how to use the Health and Expert widgets to understand your RADIUS performance.

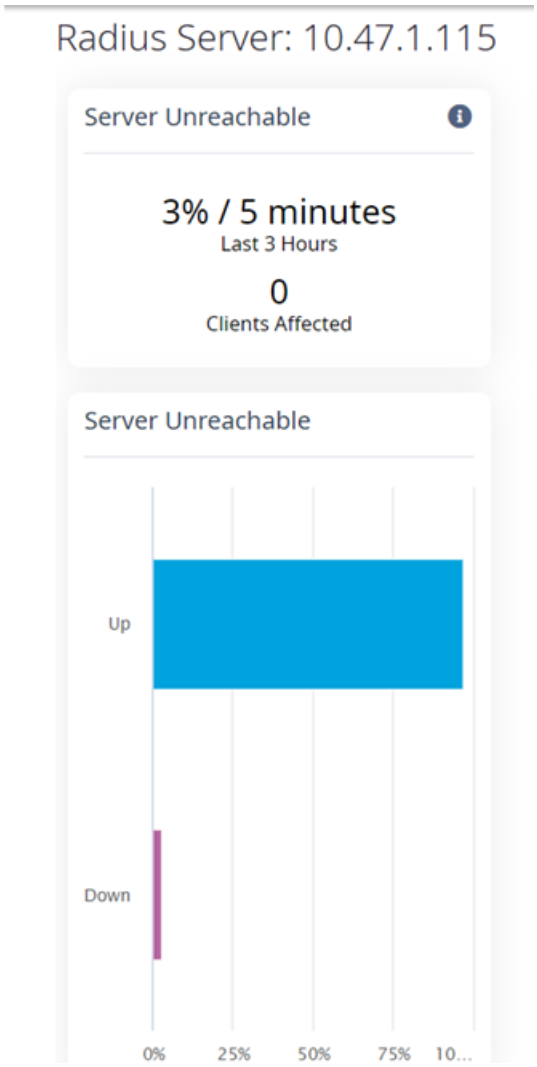


Figure 97: RADIUS Server Up

From the **Health** tab, Figure 97 indicates that RADIUS Server has been Down for 5 minutes (3% of the Last 3-Hour duration period) and no clients have been adversely affected.

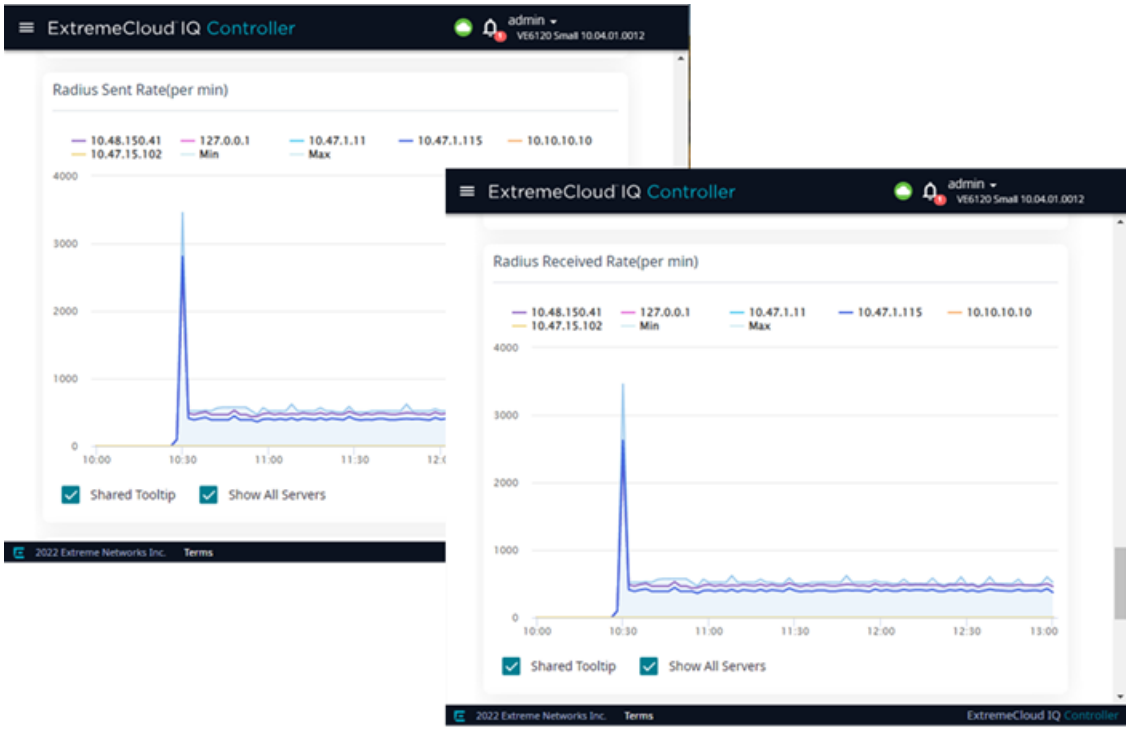


Figure 98: Matching Sent/Received Patterns Indicate Success

From the **Expert** tab, Figure 98 shows that the RADIUS Sent Rate pattern matches the RADIUS Received Rate pattern, indicating that the RADIUS interface is functioning.

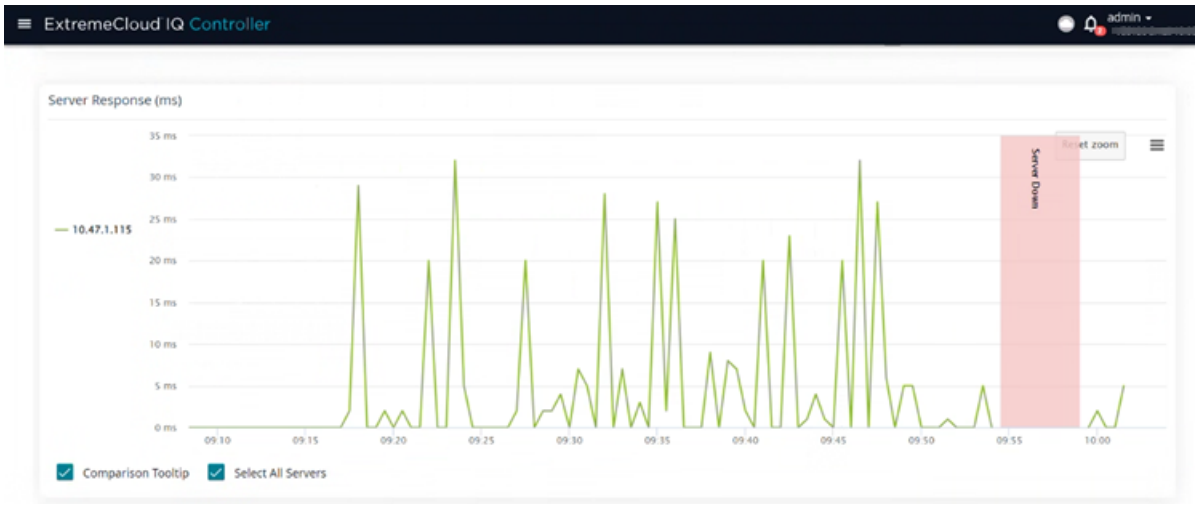


Figure 99: Server Response Chart

From the **Expert** tab, Figure 99 shows a single RADIUS server response time before and after the server was disconnected.

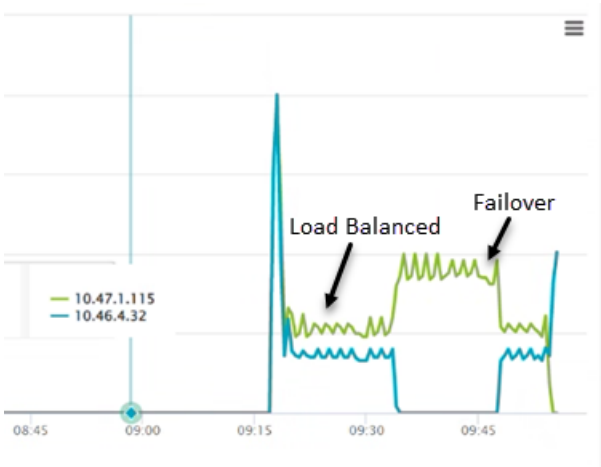


Figure 100: RADIUS Server Response showing load balance and failover

From the **Expert** tab, Figure 100 illustrates a RADIUS server response pattern for load balance and failover configuration.

Related Topics

Configure AAA Policy on page 327

Reports

Generate reports for the Dashboard widgets based on data for a site. Create report templates that enable you to easily generate consistent reports, and schedule reports using Scheduler for ExtremeCloud IQ Controller.

To generate a report, take the following steps:

1. Create a report template.

   A template defines the report type, for example "Top Clients by Usage". ExtremeCloud IQ Controller offers a report template for each Dashboard widget.
2. Configure the report settings.

   Select the template, then select **Run or Schedule Report**, and specify the report settings. Select **Save Report Settings**.
3. To run the report now, select **Run**, or schedule the report from the **Report Settings** tab.
4. Download the generated report from the **Generated Reports** tab.

The following tabs are available from the **Reports** page:

Templates

View a list of templates. Create and work with report templates.

Select a template to display the following icons:

— Edit the report template.
— Copy the report template.
— Run a report from the template.
— Delete the report template.

Report Settings

View a list of reports with saved settings for future use, or to schedule the report using Scheduler for ExtremeCloud IQ Controller. From the **Report Settings** tab, select a report to display the following icons:

— Edit the report settings.
— Delete the saved report.

Generated Reports

View a list of generated reports. Select a generated report to display the following icons:

— Download the generated report.
— View the generated report.
— Delete the generated report.

Related Topics

Create Report Template on page 417
Run Report on page 420
Schedule Report on page 421
Scheduler for ExtremeCloud IQ Controller on page 471

Create Report Template

A report template defines the report type. To create a report template:

1. Go to **Tools** > **Reports** > **Add**.
2. In the **Name** field, add a name for the template.
3. From the **Widgets** pane, select one or more widgets that you want to include in the template and drag onto the **Template** pane.

   To create a Venue report, select widgets from the Venue widget category, then create one or more user groups. For more information, see Define Venue User Groups on page 418.
4. Select **Save**.

The report template is displayed automatically in the **Templates List**.

Related Topics

Define Venue User Groups on page 418
Reports on page 416
Run Report on page 420
Schedule Report on page 421

Define Venue User Groups

Define a user group before running a Venue Report. The site-level reports are based on a set of customer-defined user groups.

Create user groups based on the SSID or client user name. The user name can contain the configured Hotspot 2.0 NAI Realm of the service provider, automatically grouping clients by their service provider.

Define user groups for the **Venue Dashboard** and the **Report Templates** definition page separately:

- To define user groups from the Sites **Venue Dashboard**:

  1. Go to **Monitor** > **Sites**.
  2. Select a site.
  3. Select **Dashboard** > **Venue**.
  4. Select .

     The **Define User Groups** dialog opens.

- To define user groups from the **Reports Template** page:

  1. Go to **Tools** > **Reports** > **Templates** > **Add**.
  2. Configure the template settings.
  3. From the right pane, select **Venue** to display the Venue widgets.
  4. Select one or more Venue widgets to include in the template and drag onto the **Template** pane.
  5. Select .

     The **Define User Groups** dialog opens.

To define a User Group using Query Builder:

1. Select **New** and provide a name for the User Group.
2. Select **Group**.

   User Group Query Builder starts with a logical group of conditions. You can add more groups, joined with query conditions. Valid conditions between two or more groups:

   - AND
   - OR

   Note
   AND is the only supported condition within a group.

3. From **Source Field**, select **SSID** or **User Name**
4. Select the **Comparison Operator**.

   Valid values are:

   - Equals
   - Not Equals
   - Contains

5. Under **Search Condition**, provide the value that you are searching for.

   Selecting the **Search Condition** field displays a drop-down of existing values. The list is filtered as you type. Wildcards are not supported. To match a portion of the search condition, use the operator **Contains**.

   - Select **+** to add more conditions.
   - Select **-** to remove conditions.
6. To add another condition row, select **+**.
7. Optionally, in the **Group** window, add conditions to the group or add more groups. Each group has conditions joined by the selected operator.
8. Select **Execute**.

   The query is automatically saved.

Note
Query Builder generates a Pandas query syntax. The syntax preview is displayed at the top of the **Query Builder** dialog. For saved queries:

- Select to view the Pandas query.
- Select to copy the Pandas query to the clipboard.

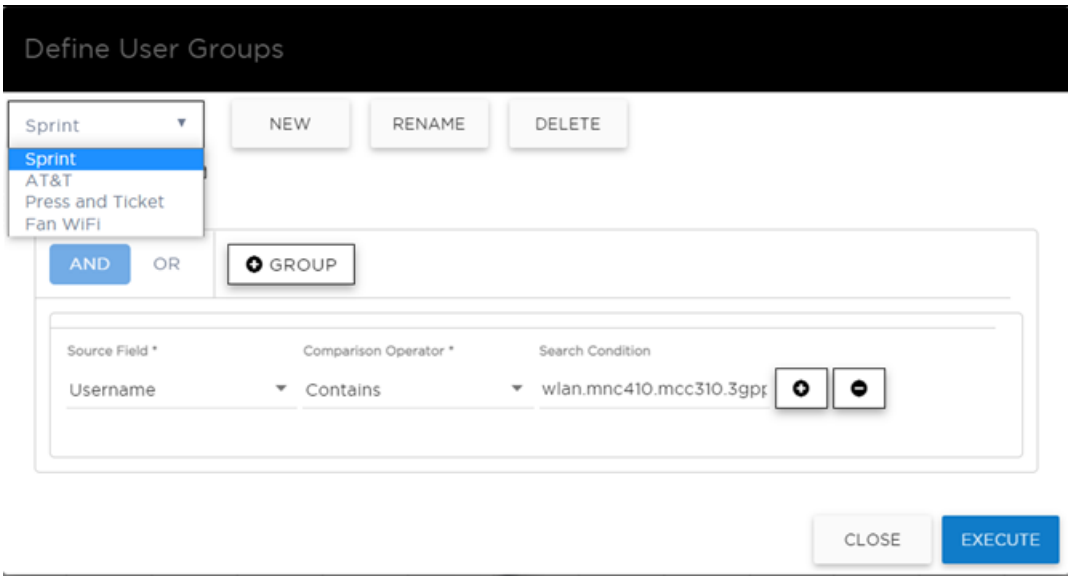


Figure 101: Query Builder: User Group definition containing Hotspot 2.0 NAI Realm

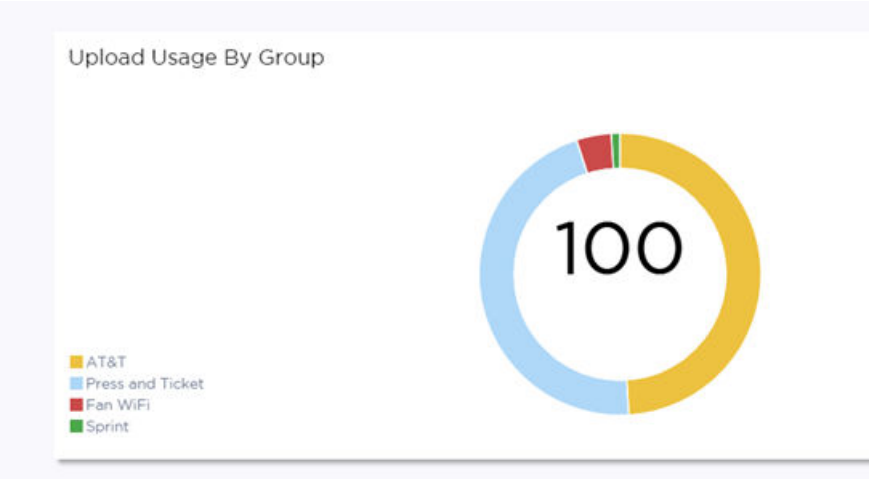


Figure 102: Venue Dashboard – Upload Usage by Group

Query Builder actions:

- **New**. To create a new query, provide a name and select **OK**. There is a limit of 10 saved queries per user, per grid. After the 10-query limit has been reached, the **New** button is unavailable.
- **Rename**. Rename an existing query.
- **Delete**. Delete the query that is currently displayed.
- **Close**. Close the Query Builder dialog. If you close Query Builder without running the query, your query details are deleted.
- **Reset**. Close the Query Builder dialog and save the current query. The next time you open Query Builder, this query will display. This option is available after you run a specific query.
- **Execute**. Run the query and save it.
- **Save**. Save changes without executing the query. Save is only visible when changes have been made.

Related Topics

SP Identification on page 267
Venue Dashboard on page 53

Run Report

To run a report:

1. Go to **Tools** > **Reports** > **Templates**.
2. Select a template, then select .
3. Configure the following report settings:

Title

Enter a report title.

Template

The report template for the report.

Scope

The reports are limited to a specific site. Select from the list of configured sites.

Period

Select a period to gather data. Valid values are:

- 3 Hours
- 3 Days
- 14 Days

Format

Specify the output format for this report: PDF.

4. Before running the report, select **Save Report Settings**.

   After you save the Report Settings, the report displays on the **Report Settings** tab, and it displays in the Scheduler for ExtremeCloud IQ Controller.

5. When running a report, you have the following options:

   - **Run Now**. Run the report now.
   - **Scheduling**. Schedule the report from the **Report Settings** tab. Schedule the report using Scheduler for ExtremeCloud IQ Controller.

     Note
     Scheduling is unavailable until you install and run Scheduler for ExtremeCloud IQ Controller.

     Select **Scheduling** to open the Scheduler application. This is a Docker application that resides on ExtremeCloud IQ Controller. Download Scheduler for ExtremeCloud IQ Controller from the Extreme Networks support portal, and install the application. For more information on installing Scheduler Application, see Scheduler for ExtremeCloud IQ Controller on page 471.

   - **Cancel**. To cancel the report. The report settings are not saved.

Related Topics

Schedule Report on page 421
Scheduler for ExtremeCloud IQ Controller on page 471
Reports on page 416

Schedule Report

Before you can schedule reports from ExtremeCloud IQ Controller:

- Download and install Scheduler for ExtremeCloud IQ Controller. For more information, see Scheduler for ExtremeCloud IQ Controller on page 471.
- Create a report template. For more information, see Create Report Template on page 417.

Note
When integrating Scheduler for ExtremeCloud IQ Controller, set **Web Session Timeout** > 2 hours. If this value is < 2 hours, Scheduler results in a 401 Unauthorized error. To configure **Web Session Timeout**, from ExtremeCloud IQ Controller, go to **Administration** > **System** > **Maintenance**.

Use Scheduler for ExtremeCloud IQ Controller to schedule reports from ExtremeCloud IQ Controller.

1. Create a report template. For more information, see Create Report Template on page 417.
2. From the **Report Settings** tab, select a report. Then, select .
3. Provide the report settings and select **Save Report Settings**.

   For more information, see Run Report on page 420.

   Note
   Schedule reports from the **Report Settings** tab.
   You must save the report settings before you can schedule the report. When scheduling a report, the Period value is set from the Scheduler application.

4. Select **Scheduling**.

   The Scheduler application opens.
5. In the left pane, select **Scheduler**.
6. From the calendar, select a time period.

   The **Add Event** dialog displays.
7. In the **Name** field, provide a name for the event.
8. From the **Type** field, select one of the following report types:
   - Historical Report. A scheduled report from ExtremeCloud IQ Controller. Valid duration:
     - 3 Hours
     - 3 Days
     - 14 Days
   - Aggregated Report. A scheduled report that offers a flexible duration (1-24 hours). Data is stored on ExtremeCloud IQ Controller and the report is generated after the duration period has expired. (Supported with ExtremeCloud IQ Controller v5.26.03 and later.)

     Note
     Only Venue reports are supported in the flexible duration Aggregated Report:
     - **Usage by Type**. Usage for uplink and downlink.
     - **Throughput by Type**. Throughput for uplink and downlink.
     - **Throughput by Group**. Throughput per defined user group.
     - **Upload Usage by Group**. Upload usage by defined user group.
     - **Download Usage by Group**. Download usage by defined user group.
     - **Unique Users by Group**. Number of unique users by defined user group.
     - **Concurrent Users by Group**. Number of simultaneous connections by defined user group.

9. Configure Action — Select one or more reports to associate with the event.
   a. The available reports are listed under **Available**. The selected reports are listed under **Selected**.
   b. Drag and drop each report between the two panes. Select « » to move all reports at once.
   c. Select **Save**.

The event is displayed on the calendar at the designated time. The report is scheduled to run.

Related Topics

Scheduler for ExtremeCloud IQ Controller on page 471
Create Report Template on page 417
Reports on page 416

Report Settings

View a list of reports with saved settings. The list of reports also display in the Scheduler for ExtremeCloud IQ Controller. From within the Scheduler application, select a report from the saved Reports list, creating a scheduled event to generate a report.

When you run a report from a template, you have the option to **Save Report Settings**.

The following information is provided on the **Report Settings** tab:

- Report Name
- Template Name
- Time Period for the report generation. Valid values are:
  - 3 Hours
  - 3 Days
  - 14 Days

Note
When scheduling a report, the Period value is set from the Scheduler application.

From the **Report Settings** tab, select a report to display the following icons:

— Edit the report settings, and run or schedule the report.
— Delete the saved report.

Related Topics

Reports on page 416
Run Report on page 420
Schedule Report on page 421

Generated Reports

View a list of generated reports. The following information is provided on the **Generated Reports** tab:

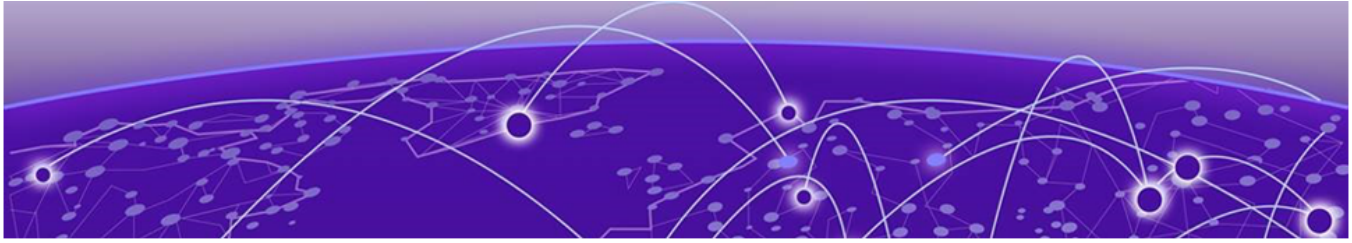
- Report Name
- Report Template
- Report Generated Format
- Date and Time the report was generated.

Select a generated report to display the following icons:

-  — Download the generated report.
-  — View the generated report.
-  — Delete the generated report.

Related Topics

Reports on page 416



Administration

Use the **Administration** workbench to configure system settings, work with utilities, manage upgrades, configure container applications, apply system licenses, and manage accounts.

System Configuration

System administrators can do the following from the **System** menu:

- Configure network interfaces and network time.
- Manage software upgrades and system maintenance.
- Configure availability mode for network failover and redundancy.
- Configure SNMP.
- View system logs and information.

Related Topics

Interfaces

Host Attributes

Attributes that define your network: Host Name, Domain Name, Default Gateway, and your DNS servers.

The Default Gateway IP address is the global default IP route setting for the appliance. Valid values are: the Admin topology gateway address and any IP address on the physical Interfaces or Bridge at AC VLAN topology subnets.

L2 Ports

Use the L2 Ports information to understand the OSI Layer 2 (Data Link Layer) physical topology of the data plane. These ports represent the actual Ethernet Ports. LAG Ports are supported on physical appliances only.

You can deploy ExtremeCloud IQ Controller in a redundant configuration, providing connectivity to two different switch stacks for the same port function. ExtremeCloud IQ Controller supports configuration attachment through a LAG to the same switch, or to two separate switches or stacks (MLAG).

- Static LAG supported.
- You can add a port to an existing LAG regardless of whether or not the port is in use. Assigned VLANS are automatically remapped to the LAG port.

  When LAG is disassembled, all LAG VLANs are automatically assigned to the first port member of the LAG.
- In a High Availability pair, the LAG configuration automatically syncs to the peer appliance.
- Do not configure High Availability over a Bridged@AC L3 Interface.

Select Details to view statistics on throughput and packets transferred and received for the selected port. Graphic widgets illustrate data points for a selected report duration.

Interfaces

Add network topologies. Topologies represent the networks with which the ExtremeCloud IQ Controller and its APs interact. The attributes of a topology are: VLAN ID, Port, IP address, Mode, and certificates. To add an interface, click **Add**.

Admin Interface as a Client

The admin interface was defined through the basic configuration wizard. This is the management port with the defined IP address and the subnet mask (CIDR).

To configure the Admin Interface as a DHCP client, select **DHCP Client**. The predetermined IP address and CIDR are hidden from display, and the Admin Interface queries the network segment for a DHCP server that will automatically provide the IP address and CIDR.

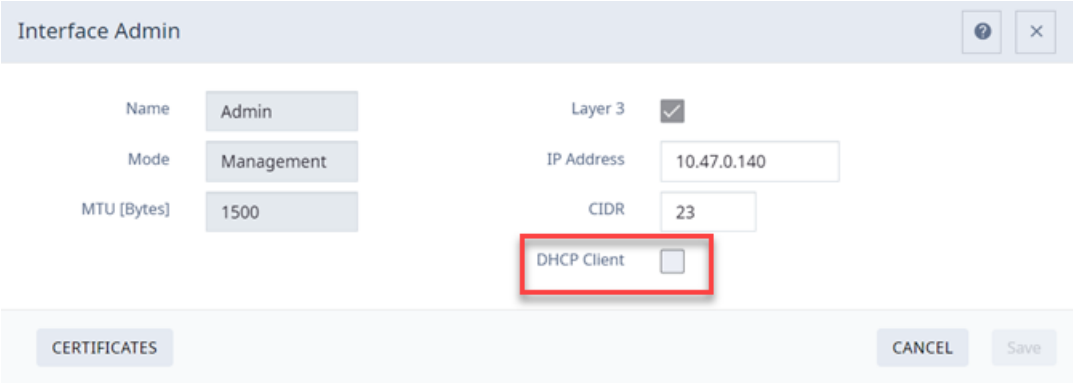


Figure 103: Admin Interface Configuration

Configuring the admin interface as a DHCP client can simplify the controller installation process, and it supports the ExtremeCloud IQ Digital Twin feature. For more information on Digital Twin, see the ExtremeCloud IQ documentation.

If the DHCP request fails, the admin interface reverts to the default address that is shipped with ExtremeCloud IQ Controller (`192.168.10.1/32`). The subnet mask defaults to `192.168.10.0/24`, and ExtremeCloud IQ Controller retries the DHCP request in 30-second intervals.

Note
You can also configure ExtremeCloud IQ Controller as a DHCP Server. Refer to the **DHCP** setting on any interface other than the admin interface.

Static Routes

Use static routes to set the default route of the ExtremeCloud IQ Controller so that device traffic can be forwarded to the default gateway. To add a static route, click **Add**.

Related Topics

Add an Interface on page 427
Add a Static Route on page 430
L2 Port Details on page 430

Add an Interface

You must be a system administrator to add a network interface. Take the following steps:

1. Go to **Administration** > **System**.
2. Under Interfaces click **Add**.

   The **Create New Interface** dialog displays.

3. Configure the following parameters:

Table 106: Interface Parameters

Field	Description
Name	Name of the interface.
Mode	Describes how traffic is forwarded on the interface topology. Options are: • Physical - The topology is the native topology of a data plane and it represents the actual Ethernet ports. • Management - The native topology of the ExtremeCloud IQ Controller management port.
VLAN ID	ID for the virtual network.
Tagged	Indicates if the interface tags traffic. When traffic is tagged, the VLAN ID is inserted into the packet header to identify which VLAN the packet belongs to. Tagging can identify the port or interface to send a broadcast message to.
Port	Physical port on the ExtremeCloud IQ Controller for the interface.
Enable Device Registration	Enable or disable AP registration through this interface. When enabled, wireless APs use this port for discovery and registration. Other ExtremeCloud IQ Controllers can use this port to enable inter-ExtremeCloud IQ Controller device mobility if this port is configured to use SLP or the ExtremeCloud IQ Controller is running as a manager and SLP is the discovery protocol used by the agents.
Management Traffic	Enable or disable Management Traffic through this interface. Enabling management provides access to SNMP (v1/v2c, v3), SSH, and HTTPs management interfaces.
MTU	Maximum Transmission Unit (MTU). Standard is 1500 bytes. Fixed value.
Layer 3	
IP Address	For an Admin topology, the Layer 3 check box is selected automatically. The IP address is mandatory for a Physical topology. This allows for IP Interface and subnet configuration together with other networking services.
CIDR	CIDR field is used along with IP address field to find the IP address range.

Table 106: Interface Parameters (continued)

Field	Description
FQDN	Fully-Qualified Domain Name
DHCP Server	Configure the Interface as a DHCP Server. Dynamic Host Configuration Protocol allows network administrators to centrally manage and automate the assignment of IP addresses on the corporate network. DHCP sends a new IP address when a computer is plugged into a different place in the network. The protocol supports static or dynamic IP addresses and can dynamically reconfigure networks in which there are more computers than there are available IP addresses. Valid values are: • None • Local Server. Indicates that the ExtremeCloud IQ Controller is used for managing IP addresses. **Note:** This setting differs from **DHCP Client** on the admin interface. Here you are configuring the controller as a DHCP server. You can also configure the admin interface as a DHCP client.

Related Topics

Certificates on page 343
Local DHCP Management Settings on page 308

Multiple LAG Interface Support

ExtremeCloud IQ Controller supports redundant configurations where the appliance provides connectivity to two switch stacks for one port function. On the **L2 Ports** pane, you can configure ExtremeCloud IQ Controller attachment through a LAG to one switch, or attached to two separate switch stacks, forming a Multiple Link Aggregation Group (MLAG). An MLAG joins two or more interfaces in the same Link Aggregation Group.

Note
Multiple Link Aggregation Group (MLAG) is supported on hardware appliances E1120, E2120, E2122, E3120, and E3125. MLAG is not supported on ExtremeCloud IQ Controller virtual appliances.

Note
LAG groups are restricted to ports of the same type (speed).

Add a Static Route

Static Routes define the default route to ExtremeCloud IQ Controller for legitimate wireless traffic. You must be a system administrator to add a static route.

Note
Static Routes affect the settings for the Default Gateway IP address under **Host Attributes**. Adding a default static route (0.0.0.0/0) changes the Default Gateway IP address.

To add a static route, take the following steps:

1. Go to **Administration** > **System**.
2. Under Static Routes select **Add**.

   The **Create New Static Route** dialog displays.
3. Configure the following parameters:

Table 107: Static Route Parameters

Field	Description
Destination	IP address of the destination ExtremeCloud IQ Controller.
CIDR	CIDR field is used along with IP address field to find the IP address range.
Gateway	Gateway address of the ExtremeCloud IQ Controller for any Admin or physical interfaces (B@AC L3 VLAN).

L2 Port Details

ExtremeCloud IQ Controller offers detailed physical interface statistics for the selected port. View directional data for received (Rx), transmitted (Tx), and aggregate values for network throughput, utilization, and frame rate.

To view L2 Port throughput and directional packet transfer rates:

1. Go to **Administration** > **System** > **Interfaces**, and scroll down to the **L2 Port** pane.
2. Select **Details** for the selected port or selected LAG.

The top left displays the port MAC Address and Port Speed.

The following graphical widgets are displayed:

Utilization

Represents the ratio of current network traffic to the maximum traffic that the port can handle, indicating the network bandwidth usage.

Throughput

Represents the amount of data that transmits.

Frame Rate

Represents the speed at which images or frames are captured or displayed, measured in fps (frames per second).

Report Duration

From the top of the **Port Details** page:

- Select to set the **Duration** value for the time period reported. Valid duration values are:
  - Last 3 hours
  - Last 3 days
  - Last 14 days
- Select to refresh the data on demand.
- Hover the mouse over a widget to display tool tip information.

Example Widgets

The following figures illustrate how to use the widgets to understand data transfer for the selected port.

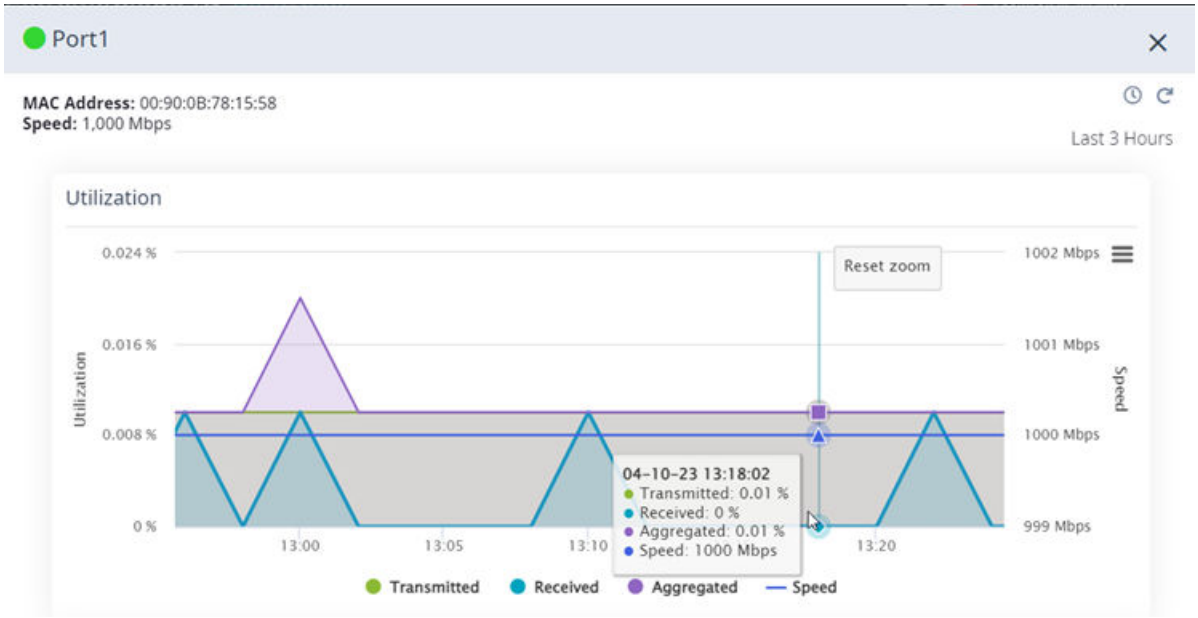


Figure 104: L2 Port Utilization - Zoom with graph key

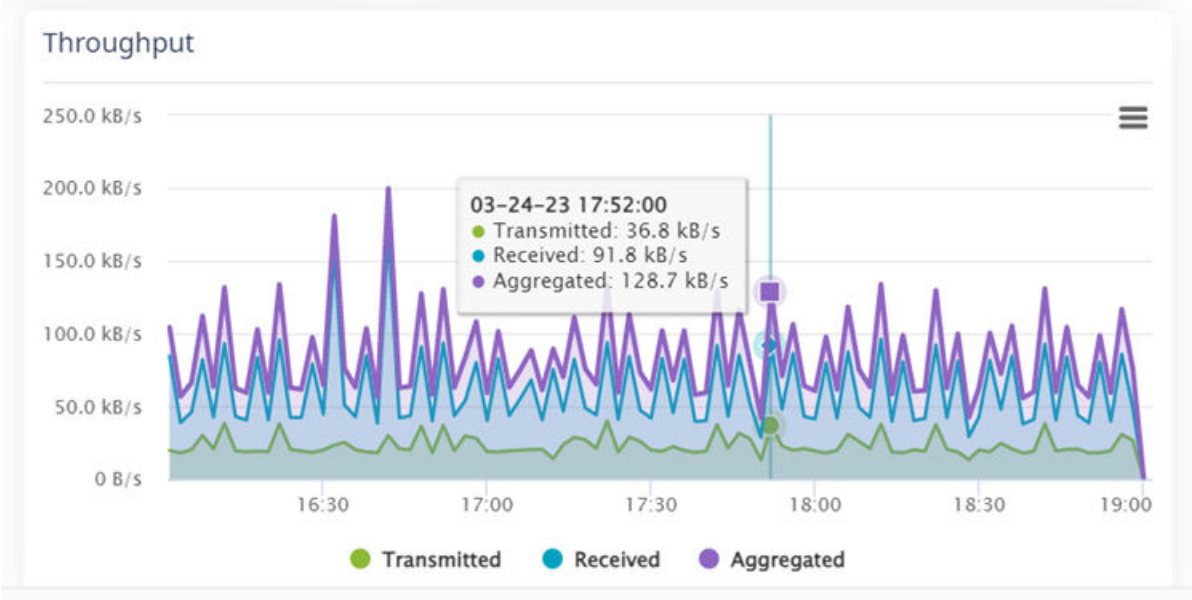


Figure 105: L2 Port Throughput – Aggregate display

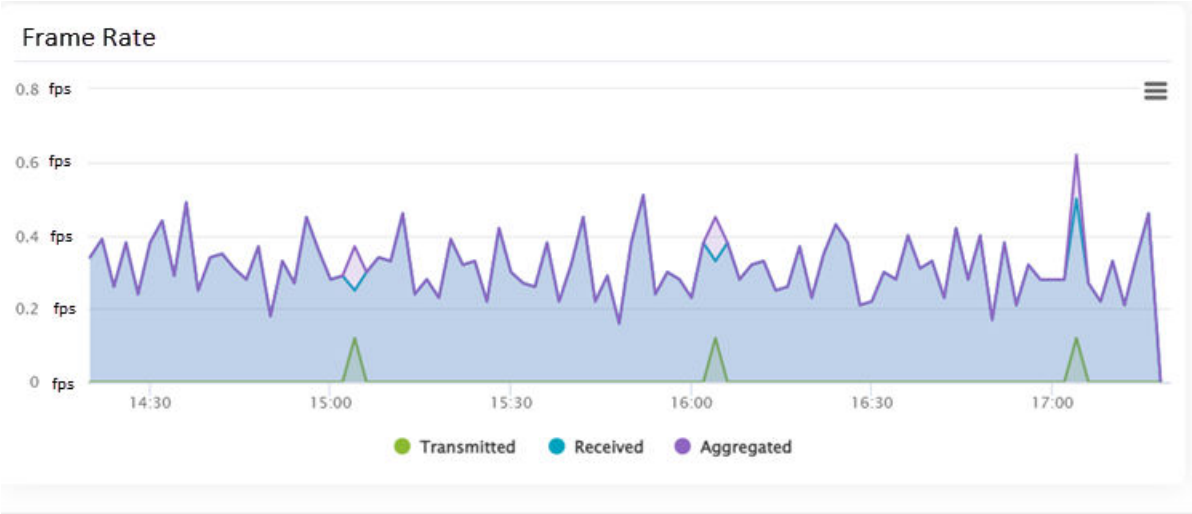


Figure 106: L2 Port Frame Rate - Aggregate display

Chart Actions

Select ☰ to take the following actions from the chart menu:

- View in full screen
- Print chart
- Download chart data in any of the following supported formats:
  - PNG
  - JPEG
  - PDF
  - SVG vector image

Select the chart label, **Transmitted**, **Received**, or **Aggregated** to toggle the chart display.

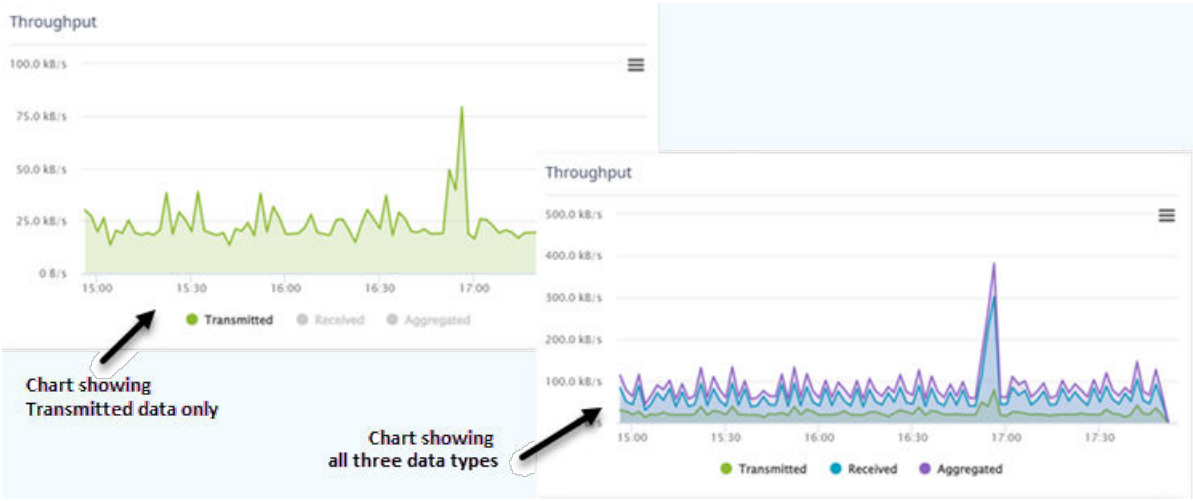


Figure 107: Charts showing toggle feature

To zoom in, select an area of the chart and drag. To return to the original zoom, select **Reset Zoom**.

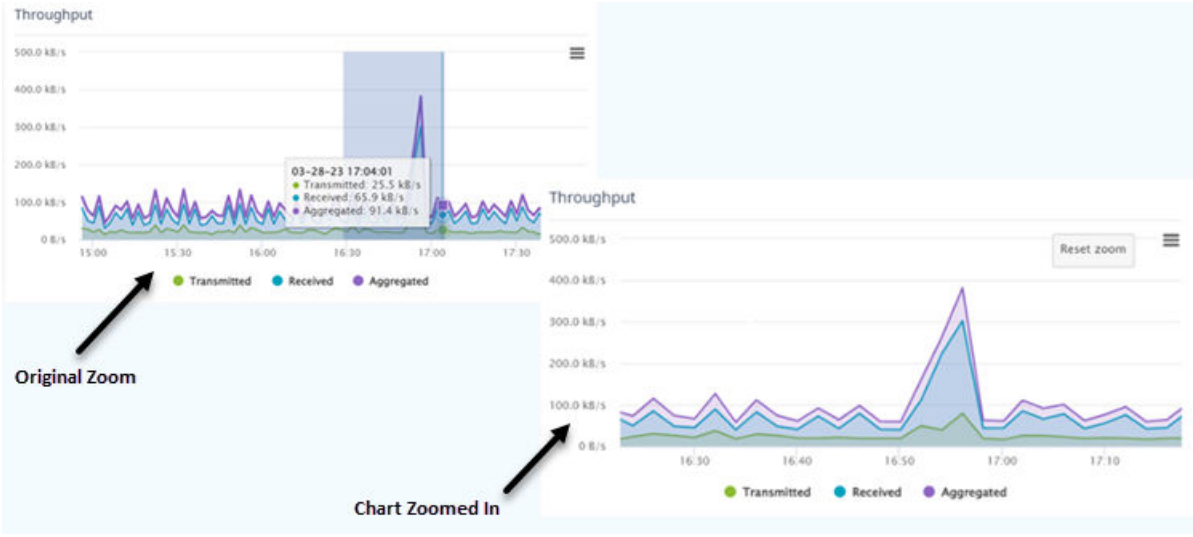


Figure 108: Chart Zoom

Note
Due to a possible resolution limitation in the graphical display, large spikes in data may not display in Original Zoom. In this case, hover over the chart to display available values in the tooltip. Then, zoom in to view a graph of a limited area in the chart.

Network Time

System administrators can configure network time and the NTP servers. Go to **Administration** > **System** > **Network Time**.

System Time

Displays the current system date and time.

Time Zone Settings

Manually configure time zone settings for your network. Search for a time zone, and click **Save** to manually change system date and time.

Network Time

Check **NTP/SNTP** to configure servers for Network Time Protocol (NTP) or Simple Network Time Protocol (SNTP).

NTP and SNTP are Internet Standard Protocols that assures accurate synchronization to the millisecond of computer clock times in a network of computers.

NTP/SNTP Reachable

An icon indicates if the NTP/SNTP server is reachable:

- Green. The server is reachable.
- Red. The server is not reachable. Check your NTP/SNTP server settings. ExtremeCloud IQ Controller has lost connectivity.

Note
Network Time settings on each appliance of an availability pair must be identical for the configuration update process to be successful.

Software Upgrade

The following are components of the software upgrade process:

- Rescue Images
- Configuration Backup
- Restore
- Software Upgrade
- AP Images
- Logs

Related Topics

Perform a Configuration Backup on page 435
Restoring a Backup File on page 436
Upgrade Software on page 437
Rescue Image on page 437
Remote Server Properties on page 440
View Upgrade Logs on page 441
Upgrade AP Images on page 442

Perform a Configuration Backup

This backup and restore procedure is limited to configuration files and, optionally, logs and audit files. A system backup is a different procedure. A system backup is a full system snapshot rescue file (*-rescue-user.tgz). Creating a full system rescue file is an option during the system upgrade process. For more information on system upgrade, see Upgrade Software on page 437.

Before you perform a backup procedure, decide what to back up and where to save the backup file:

- Select back up configs, logs, and audit or back up configuration only.
- Select a location to store the backup file.
- Select **Local** as the backup location.
- (Optional) Configure a backup schedule.

Note
It is a best practice to set up a scheduled backup for all managed appliances.

On-demand backups can only be stored locally, while scheduled backups can be stored on a mounted flash drive or on a remote server.

Related Topics

Configure a Backup Schedule on page 435
Remote Server Properties on page 440

Configure a Backup Schedule

When you schedule a backup, you can choose to upload the backup to a server or have the scheduled backup saved locally or on an external flash drive.

To schedule a backup:

1. Go to **Admin** > **System** > **Software Upgrade** and click **Configure Schedule**.
   The **Schedule Backup** dialog displays.
2. Configure the following parameters:

   Backup Location

   Indicates where to send the backup file. Valid values are: Local, Remote, or Flash. When sending a backup to a remote server, configure the server properties.

   What to back up

   Indicates the content of the backup file. Valid values are: Configs, CDRs, Logs and Audit (which is a full backup), or Configuration files only.

   Schedule Task

   Indicates when the backup task runs. Valid values are: Never, Daily, Weekly, Monthly.

Related Topics

Software Upgrade on page 434
Remote Server Properties on page 440

Restoring a Backup File

Local backup files are listed. Select a backup file to restore. You can copy a backup file from a remote server or select a local file. After the file is on ExtremeCloud IQ Controller, select it and take one of the following actions:

- Copy Backup
- Restore system with backup file
- Copy backup file to remote system.
- Download backup file to a local computer
- Delete backup file.

Note
The restore process checks for Distributed sites. If Distributed sites are part of the instance configuration, the restore process will abort and log the following:

- <date> ERROR: Restore action aborted due to the presence of a Distributed site

Related Topics

Copy Backup on page 436
Remote Server Properties on page 440

Copy Backup

To copy a backup image to ExtremeCloud IQ Controller, configure the following parameters:

Upload Method

Method used to upload file to appliance. Valid values are:

- HTTP — Indicates to upload from a local workstation.
- FTP — Indicates to upload from the corresponding server.
- SCP — Indicates to upload from the corresponding server.

When the Upload Method is **FTP** or **SCP**, configure the server properties.

Copy Image from Local Drive

When the Upload Method is **HTTP**, drag image onto ExtremeCloud IQ Controller or select field to navigate to local file directory.

Related Topics

Remote Server Properties on page 440
Upgrade Software on page 437
Restoring a Backup File on page 436

Upgrade Software

Note
All locally-stored configuration backup files are removed during software upgrade. To preserve locally-stored files, download them prior to upgrading the ExtremeCloud IQ Controller software.

There is more than one way to put the upgrade image on ExtremeCloud IQ Controller:

- Select a local upgrade image. Or
- Click  to display the **Copy Upgrade Image** dialog. For more information, see Copy Upgrade Image on page 439.

To perform an upgrade:

1. Select an image file for the upgrade.
2. **Select Backup System Image To**, selecting a destination location to back up the current image, creating a rescue image.

   Note
   It is a best practice to always create a rescue image.

3. From the **Upgrade** field, select **Now** or **Schedule**. Then, click **Upgrade Now** or **Configure Schedule**.

Related Topics

Create a Rescue Image on page 438
Copy Upgrade Image on page 439
Configuring an Upgrade Schedule on page 441
Perform a Configuration Backup on page 435
Restoring a Backup File on page 436
Copy Backup on page 436
Remote Server Properties on page 440
Install AP Firmware Image on page 442

Rescue Image

A rescue image is a snapshot of your current system that is automatically created during the software upgrade process. The rescue image represents the starting version of the ExtremeCloud IQ Controller upgrade and its configuration state. If necessary, you can use the rescue image to revert back to the controller's previous version and state after a software upgrade.

Note
It is a best practice to always create a rescue image.

By default, ExtremeCloud IQ Controller saves one rescue image. The intent is to offer you a means of reverting back to the last software version and configuration state before the upgrade.

Related Topics

Create a Rescue Image on page 438
Restore from a Rescue Image on page 438
Upgrade Software on page 437

Create a Rescue Image

A rescue image is automatically created when you upgrade the ExtremeCloud IQ Controller, as long as you do not disable this option explicitly.

1. To upgrade the controller version, go to **Administration** > **System** > **Software Upgrade**.
2. Scroll down to the **Upgrade** pane.
3. Provide the following information for upgrade:

   Select Image

   This is the new image to upgrade to.

   Backup System Image To

   This is where the rescue image is created.

   - Select **Local** to automatically have a rescue image created and stored locally. This is the default setting.
   - Select **Flash** to have the rescue image created and stored on a flash drive.
   - Select **No Backup** to disable the back up option.

     Note
     If you select **No Backup**, a rescue image is not created.

   Upgrade

   This field indicates when to upgrade. Possible values are:

   - Now
   - Schedule

Related Topics

Restore from a Rescue Image on page 438
Upgrade Software on page 437
Configuring an Upgrade Schedule on page 441

Restore from a Rescue Image

After a software upgrade, if you need to restore the controller to the previous release, use the rescue image.

Note
Always revert an upgrade from the rescue image. Do not revert the controller to a previous release using the upgrade image for that release.

1. To revert the controller to a previous image, go to **Administration** > **System** > **Software Upgrade**.

2. Scroll down to the **Upgrade** pane.
3. Provide the following information to restore the controller:

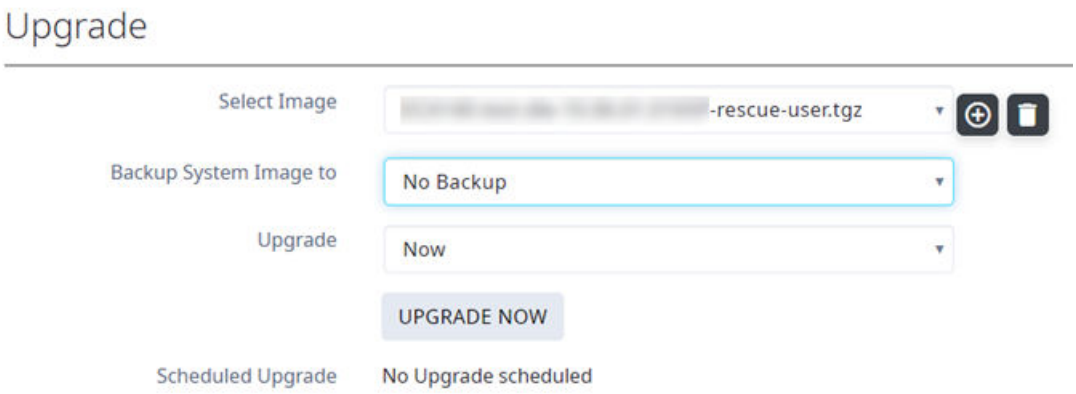


Figure 109: Restore from a rescue image

Select Image

When reverting to the previous release, select the rescue image file.

Backup System Image To

When reverting to the previous release, and the upgrade image is the rescue image file, do not create a backup of the rescue file. Select **No Backup** to disable the back up option.

Upgrade

This field indicates when to upgrade. Possible values are:

- Now
- Schedule

Related Topics

Rescue Image on page 437
Create a Rescue Image on page 438
Configuring an Upgrade Schedule on page 441

Copy Upgrade Image

To copy an upgrade or backup image to ExtremeCloud IQ Controller, configure the following parameters:

Image Type

Indicates the type of image file used. Valid values are:

- Upgrade
- Backup

Destination

Destination of the uploaded image file:

- Local
- Flash (The Flash drive must be mounted.)

Upload Method

Method used to upload image file to appliance. Valid values are:

- HTTP — Indicates to upload from a local workstation.
- FTP — Indicates to upload from the corresponding server.
- SCP — Indicates to upload from the corresponding server.

When the Upload Method is **FTP** or **SCP**, configure the server properties.

Copy Image from Local Drive

When the Upload Method is **HTTP**, drag image onto ExtremeCloud IQ Controller or select field to navigate to local file directory.

Select Image

Due to a storage space limitation, ExtremeCloud IQ Controller limits the number of locally available upgrade archives. If necessary, you can delete an older image before you upgrade to the latest image. To delete an image from ExtremeCloud IQ Controller, from the **Select Image** field, select an image and click  .

Related Topics

Remote Server Properties on page 440
Upgrade Software on page 437
Restoring a Backup File on page 436

Remote Server Properties

You can copy files to and from a remote server for configuration backup, system restore, and system upgrades. Configure the following parameters:

Table 108: Remote Server Properties

Field	Description
Upload Method	Indicates the transfer protocol to use to transfer the backup file. Valid values are: Local, FTP (File Transfer Protocol) or SCP (Secure Copy Protocol).
Server IP	IP Address of the server.
Username	User name to log into the server.
Password	Password to log into the server.
Directory	Destination or source location of file on the server.
Filename	Name of the backup file.
Destination	Destination directory for copied backup file.

Select **OK** to initiate the copy action.

Related Topics

Copy Backup on page 436
Copy Upgrade Image on page 439

Configuring an Upgrade Schedule

After you have the image file on ExtremeCloud IQ Controller, you can upgrade right away or schedule an upgrade.

To schedule an upgrade:

1. Go to **Admin** > **System** > **Software Upgrade**.
2. In the Upgrade section, from the Upgrade field, select **Schedule** and select **Configure Schedule**.
   The **Schedule Upgrade** dialog displays.
3. Configure the following parameters:

   Upgrade Image

   Name of the upgrade image file.

   Backup Filename

   Name of the backup image file.

   Backup Location

   Indicates where to save the backup image file. Local is currently the only supported value. Save the backup image locally on ExtremeCloud IQ Controller.

   Time

   The time of the scheduled upgrade in 24-hour format, HH-MM.

   Date

   The date of the scheduled upgrade in Month-Day format (MM-DD).

   Note
   When you supply a Date and Time that is in the past, the schedule is set for the following year at the specified date and time.

4. Select **Schedule**.

Related Topics

Software Upgrade on page 434

View Upgrade Logs

The following ExtremeCloud IQ Controller software upgrade activity is displayed on the **Software Upgrade** tab under **Logs**.

1. Go to **Administration** > **System** > **Software Upgrade**.
2. Scroll down the page and select **Logs +**.
   The following upgrade information is available:
   - Upgrade History
   - Upgrade Details
   - Restore Details
3. Select the appropriate tab to view information.

Related Topics

Software Upgrade on page 434

Upgrade AP Images

ExtremeCloud IQ Controller is released with the latest AP images for each supported AP Type. When you upgrade ExtremeCloud IQ Controller, in a stand-alone deployment, the connected access points are automatically upgraded to the latest firmware image. In a High-Availability deployment, you must manually upgrade the APs. You can also upgrade additional devices without upgrading the controller.

To upgrade APs:

1. Verify that the upgrade image file is installed on ExtremeCloud IQ Controller for the selected AP platform. If necessary, install the AP image file onto the controller.
2. From the **Access Points List**, select one or more APs to upgrade.
   - You can upgrade from the **Access Points List** associated with a site. Go to **Monitor** > **Sites**. Select a site and select the **Access Points** tab. Or,
   - Go to **Configure** > **Devices** > **Access Points**.
3. Go to the **AP Upgrade Status Report** to view progress of the upgrade.

Consider the following when upgrading AP images:

- Selected APs must support the same upgrade image file. AP39xx series and Wi-Fi 6 APs have different firmware images; therefore they cannot be selected for upgrade together. Instead, create two AP upgrade requests:
  - The ExtremeWireless AP39xx Series Access Points support the same firmware image file. They can be upgraded together.
  - The ExtremeWireless Wi-Fi 6 Access Points support the same firmware image file. They can be upgraded together.
- The APs must be connected to ExtremeCloud IQ Controller. If the AP is in a disconnected state, the upgrade is scheduled, but cannot complete until the AP discovers ExtremeCloud IQ Controller .
- Each ExtremeCloud IQ Controller release includes the latest AP image files for the supported access points. A stand-alone deployment automatically updates the AP firmware to the latest release. For a High-Availability deployment, upgrade all connected APs from the **Access Point List**.
- You can monitor the AP upgrade process from the **AP Upgrade Report**.
- To display AP Upgrade events, from the **Events** tab, configure your syslog to *Informational*.

Related Topics

Install AP Firmware Image on page 442
Access Points List on page 69
AP Actions on page 206
AP Upgrade Report on page 382

Install AP Firmware Image

To upgrade AP image files, do the following:

1. Go to **Administration** > **System** > **Software Upgrade**.
2. Scroll down the page to **AP Images**.

3. Select an AP Platform.

   Note
   The action to upgrade an AP3916-Camera, applies to all APs with onboard cameras. The camera upgrade is not limited to a single device.

4. To upload image from local drive:
   - Select the **Select File or Drop File** box and navigate to a local file. Or,
   - Drag the file onto this box.

   Available images are listed. Select to refresh the list. When you have more than one image file, you have the option to **Set Default AP Image** and **Delete AP Image**.
5. Select **Upgrade Status** to view the AP Upgrade Status.

Related Topics

Upgrade AP Images on page 442
AP Upgrade Report on page 382
Software Upgrade on page 434
Upgrade Software on page 437
View Upgrade Logs on page 441

Maintenance

Reset Configuration

Select one of the following reset options:

- Remove installed license – The system reboots and restores all aspects of the system configuration to the initial settings and the Permanent license key (with Capacity Keys) is removed. However, the Management IP address is preserved. This permits administrators to remain connected through the Management interface.
- Remove management port configuration – The system reboots and resets the entire system configuration to the factory shipping state. The Management IP address reverts to 192.168.10.1.

Note
The Admin password and list of user IDs are preserved after a configuration reset.

Restart System

The ExtremeCloud IQ Controller shuts down, then reboots. A warning message is displayed, asking you to confirm your selection.

Halt System

The system enters the halted state, which stops all functional services, the application, and associated wireless APs. A warning message is displayed, asking you to confirm your selection. To restart the system, the power to the system must be reset.

Web Session Timeout

Determines the web session inactive window before the session times out. Enter the value as hours : minutes. The range is 1 minute to 168 hours (7 days).

Note
When integrating Scheduler for ExtremeCloud IQ Controller, set **Web Session Timeout** > 2 hours. If this value is < 2 hours, Scheduler results in a 401 Unauthorized error.

Device SSH Password

Changes the device password globally. After changing the password, allow one minute before trying to log into a connected AP Linux shell. Check **Mask** to conceal the password characters.

Onboarding Diagnostics

Opens a web portal to ExtremeCloud IQ Controller that provides detailed configuration for logging, the ability to capture packets, and debugging information. Customers can configure logging via this interface when debugging. The default login credentials are `admin/Extreme@pp`.

The Web App displays detailed information in the following categories:

- Status
- Diagnostics
- Log Files
- Downloads
- Utilities

External Flash

Physically connect an external device to the ExtremeCloud IQ Controller and then mount the device to display memory usage and capacity. Mounting a device makes the flash device that has been inserted into the ExtremeCloud IQ Controller available for use.

Flash devices must be formatted in FAT32. Only the first partition of the flash device is used by the ExtremeCloud IQ Controller. Files must reside in the root directory. The ExtremeCloud IQ Controller software cannot operate with files in sub-directories. The ExtremeCloud IQ Controller supports only one USB device at a time, regardless of which USB connector the device is connected to. If you connect more than one USB device at a time, the system returns an error.

Note
Format flash devices as non-bootable. The ExtremeCloud IQ Controller may experience difficulty rebooting when connected to a bootable formatted flash device.

Tech Support

Generate a tech support file for troubleshooting. Select the file criteria: **Controller**, **Wireless AP**, **Log**, or **All**. (All is the default value.). When you generate a file for the wireless AP, you have the option to select **No Stats** included in the file.

1. Select **Generate Tech Support File**.

The generated file displays in the list.

2. To download the file, select the file and select  .

Availability

ExtremeCloud IQ Controller provides the Availability Pair feature to maintain service availability in the event of an outage. The Availability Pair feature allows both AP and client statistics to be available on both sides of the high availability configuration.

Go to **Admin** > **System** > **Availability** and configure the Availability Pair settings.

Availability

- Standalone. The appliance *does not* have an availability partner in the event of a failover.
- Paired. The appliance is paired with another appliance in the event of a failover.

When configuring an availability pair consider the following information:

- ExtremeCloud IQ Controller directly balances capacity allocations across both appliances in an availability pair. Adoption Capacity is additive. For example, to support a 600 AP Capacity, you can purchase a 500 Device Capacity and a 100 Device Capacity. The availability pair shares the installed capacity to the 600 limit. You can enter the entitlements on either system in the pair. However, when purchasing capacity license SKUs, make sure that none of the license blocks exceed the maximum adoption capacity for any individual system.
- An availability pair can be configured only within the same ExtremeCloud IQ Controller models.
- Enable and configure NTP: Network Time settings on each appliance of an availability pair must be identical for the configuration update process to be successful.
- Use the Network Health chart on the ExtremeCloud IQ Controller Dashboard to monitor the Availability Link Status and the Synchronization Status for an availability pair.
- Switch configuration and statistics are synchronized between the primary and backup ExtremeCloud IQ Controller.
- RF Domain database is synchronized. RF Manager engines work from a synchronized database to preserve and respect AP SmartRF state on failover.
- Access points are *not* automatically upgraded. You must initiate the AP upgrade manually after both controllers in an availability pair are upgraded.

The following status data is replicated on the partner node of an availability pair:

- Client Records
- Group Records
- Registered Users and Devices

Related Topics

Availability Pair Settings on page 449
Mobility Settings on page 449

Session Availability on page 446
Availability Link Status on page 51
Configuration Updates with an Availability Pair on page 450

Learn about updating configuration files within an availability pair.

Configuring VLANS on page 303

Session Availability

Session availability enables wireless APs to switch over to a standby (backup) wireless appliance fast enough to maintain the mobile user's session availability in the following scenarios:

- The primary wireless appliance fails (see Figure 110).

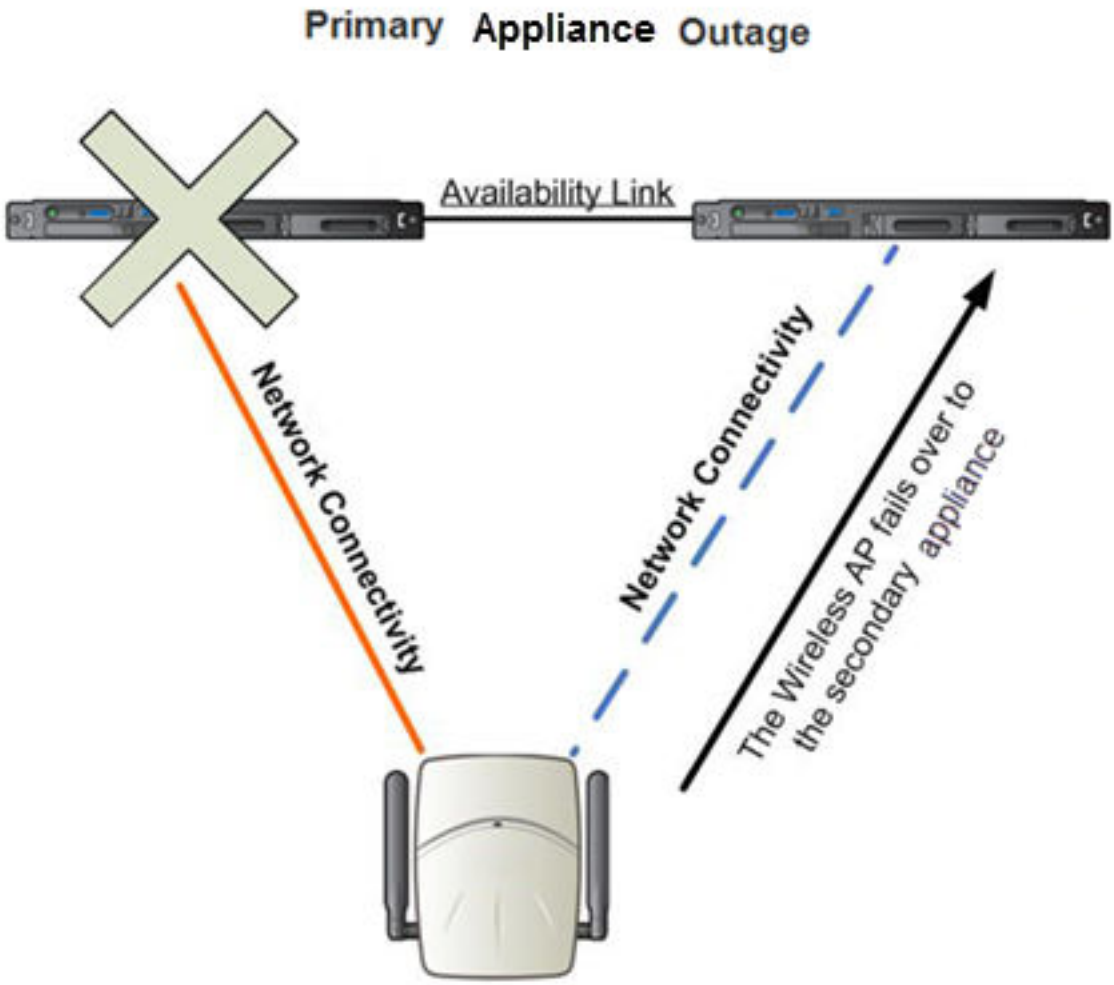


Figure 110: AP Failover When Primary Appliance Fails

- The wireless AP's network connectivity to the primary appliance fails (see Figure 111).

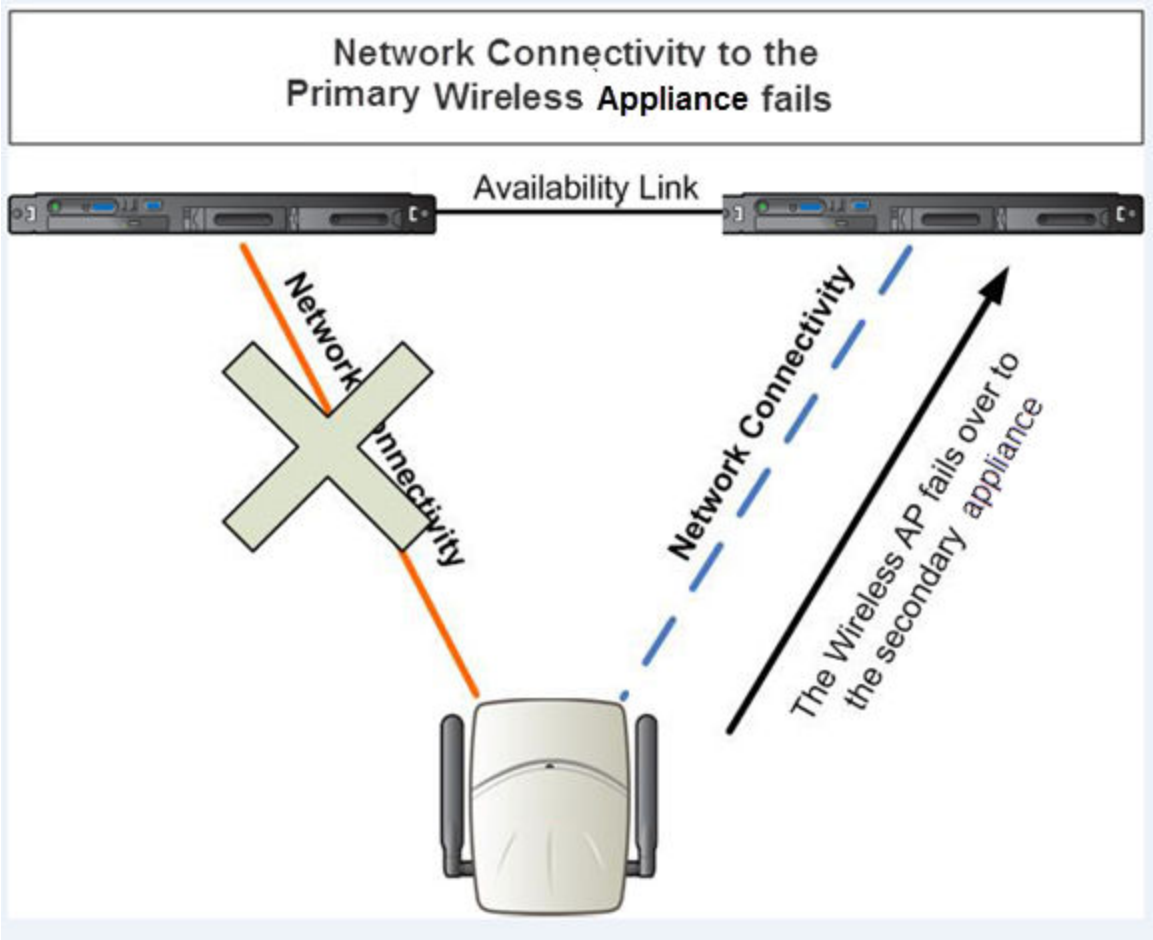


Figure 111: AP Failover When Connectivity to Primary Fails

The backup ExtremeCloud IQ Controller does not have to detect its link failure with the primary ExtremeCloud IQ Controller for the session availability to kick in. If the AP loses five consecutive polls to the primary ExtremeCloud IQ Controller either due to the ExtremeCloud IQ Controller outage or to connectivity failure, it fails over to the backup ExtremeCloud IQ Controller fast enough to maintain the user session.

In session availability mode (Figure 112), the APs connect to both the primary and backup ExtremeCloud IQ Controller. While the connectivity to the primary ExtremeCloud IQ Controller is via the active tunnel, the connectivity to the backup ExtremeCloud IQ Controller is via the backup tunnel.

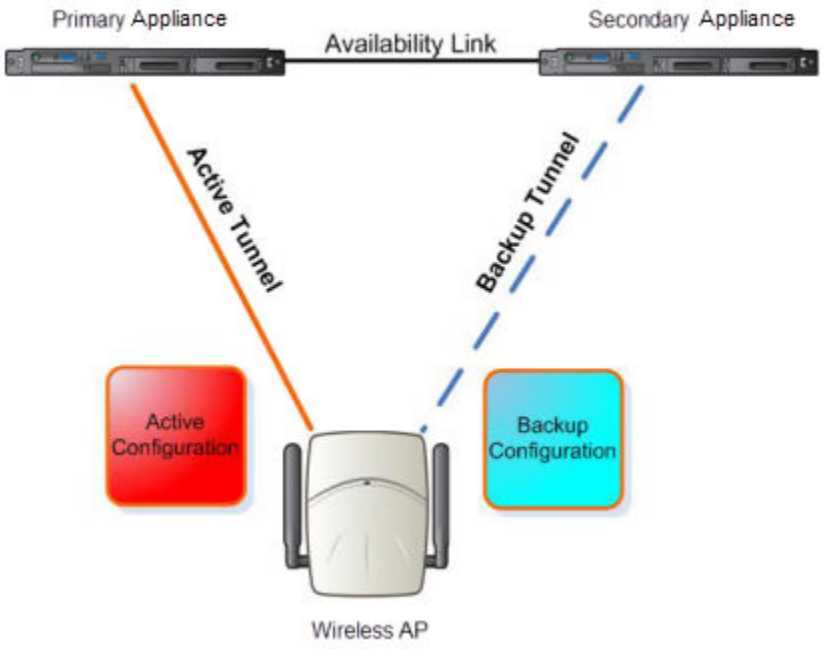


Figure 112: Session Availability Mode

The following is the traffic flow of the topology illustrated in Figure 112:

- The AP establishes the active tunnel to connect to the primary ExtremeCloud IQ Controller.
- The ExtremeCloud IQ Controller sends the configuration to the AP. This configuration also contains the port information of the backup ExtremeCloud IQ Controller.
- On the basis of the backup ExtremeCloud IQ Controller port information, the AP connects to the backup ExtremeCloud IQ Controller via the backup tunnel.
- After the connection is established via the backup tunnel, the backup ExtremeCloud IQ Controller sends the backup configuration to the wireless AP.
- The AP receives the backup configuration and stores it in its memory to use it for failing over to the backup ExtremeCloud IQ Controller. During this entire time, the AP is connected to the primary ExtremeCloud IQ Controller via the active tunnel.

Session availability applies only to the following topologies:

- Bridge Traffic Locally at AC
- Bridge Traffic Locally at AP

Availability Pair Settings

Table 109: Availability Pair Settings

Field	Description
Peer IP Address	Physical VLAN address of the paired appliance. This is the IP address of the "Physical 1" interface (port esa0), which matches the VLAN definition under **System** > **Interfaces**.
Role	Select the role of the paired appliance. Valid values are Primary or Backup. **Note:** The configuration of the Primary appliance is copied to the Secondary appliance.
Auto AP Balancing	Select the load balancing configuration for the availability pair. In an availability pair, an AP establishes an active tunnel to one appliance and a backup tunnel to the other appliance. The active tunnel is used to pass the client data over tunneled topologies. • In an **Active-Active** configuration, approximately half of the APs establish an active tunnel to the primary appliance. The remaining APs establish an active tunnel to the backup appliance, spreading the load across the availability pair. • In an **Active-Passive** configuration, all APs establish an active tunnel to the primary appliance. The secondary appliance is used for failover only.

Related Topics

Configuring VLANS on page 303

Mobility Settings

When configuring a mobility domain with availability or session availability, synchronize time on all the wireless controllers that are part of your mobility domain. For more information, see Network Time on page 433.

To configure ExtremeCloud IQ Controller in a mobility domain:

1. Go to **Admin** > **System** > **Availability**.

2. Check **Mobility** and configure the following parameters:

Table 110: Mobility Settings

Field	Description
Port	The port address of the ExtremeCloud IQ Controller.
Discovery Method	Method by which ExtremeCloud IQ Controller discovers the mobility manager. You have two options: • **SLPD** — Rely on SLP with DHCP Option 78 • **Static Address** — Define at the agent, the IP address of the mobility manager. By explicitly defining the IP address, the agent and the mobility manager are able to find each other directly without using the SLP discovery mechanisms. Direct IP definition is recommended to provide tighter control of the registration steps for multi-domain installations.

Related Topics

Availability on page 445

Configuration Updates with an Availability Pair

After an availability pair is set up, files updated on either appliance are synchronized with the paired appliance and then updated on the NAC server that is connected to each node. Network Time settings on each appliance of an availability pair must be identical for the configuration update process to be successful.

Related Topics

Availability on page 445
Network Time on page 433

Settings

Configure the following ExtremeCloud IQ Controller settings from the **Admin** menu:

- SNMP
- MAC Format
- AP Transmit Power Representation
- External NAT
- Broadcast Multicast Traffic Control
- Web Proxy Server Settings

Related Topics

SNMP Configuration on page 451
MAC Format on page 454
AP Transmit Power Representation on page 454
External NAT on page 454

Broadcast Multicast Traffic Control on page 455
Web Proxy on page 456

SNMP Configuration

Simple Network Management Protocol (SNMP) is a standard that uses a common software agent to remotely monitor and set network configuration and runtime parameters. SNMP operates in a multi-vendor environment, and the agent uses MIBs (Management Information Base), which define what information is available from any manageable network device. You can also set traps using SNMP, which send notifications of network events to the system log.

ExtremeCloud IQ Controller offers SNMP configuration for the full appliance or configuration for switches associated with a specific site.

To configure SNMP for the full ExtremeCloud IQ Controller environment:

Go to **Administration** > **System** > **Settings** > **SNMP**.

To configure SNMP for the switches associated with a site:

1. Go to **Configure** > **Sites** and select a site.
2. Select **Advanced**, and then select a value from the **SNMP** field.

Table 111 describes how to configure SNMP credentials on ExtremeCloud IQ Controller.

Table 111: SNMP Configuration Parameters

Field	Description
SNMP	Select the SNMP version to enable. Valid values are: • SNMPv3 • SNMPv2c The displayed parameters depend on the SNMP version that is enabled.
Communities (SNMPv2c)	Select **Add** to add a community. Provide a community name and access level: • Private Community — Default community for read-only SNMP communication. • Public Community — Default community for write SNMP communication. Available for full ExtremeCloud IQ Controller environment support only.
SNMPv3 Users	Select **Add** to add users for access to ExtremeCloud IQ Controller through SNMP. These values are typically types of users that are configured for access: • No Authentication/No Privacy • Authentication/No Privacy • Authentication/Privacy You can also edit user credentials and delete users.

Table 111: SNMP Configuration Parameters (continued)

Field	Description
SNMP Notifications	Select **Add** to configure the IP address and port of the server that will receive SNMP messages. You can also edit and delete notifications.
Available for full ExtremeCloud IQ Controller environment support only.	
Context String (SNMPv3)	A description of the SNMP context. An SNMP context is information that you can access through the SNMP agent. A device can support multiple contexts.
Engine ID	The SNMPv3 engine ID for the appliance running the SNMP agent. The Engine ID must be from 5 to 32 characters long.
Forward Traps	Specify the level of the messages to be trapped. Valid values are: • None • Information • Minor • Major • Critical

Related Topics

Working with SNMPv2 Communities on page 452
Working with SNMPv3 Users on page 453
Working with SNMP Notifications on page 453
Settings on page 450
MAC Format on page 454
AP Transmit Power Representation on page 454
External NAT on page 454
Advanced Tab on page 203

Working with SNMPv2 Communities

1. To access SNMPv2 Communities:
   - Go to **Administration** > **System** > **Settings** > **SNMP**
   - Go to **Sites** and select a site. Then, select **SNMP**.
2. From the SNMP field, select **SNMPv2**.
3. To add an SNMPv2 Community:
   a. From the SNMPv2 field, select **Add**.
   b. Type a name and access level.
      - Read. Private Community. Default community for read-only SNMP communication.
      - Write. Public Community. Default community for write SNMP communication. Available for full ExtremeCloud IQ Controller environment support only.
4. To delete a community, select a community from the list and select **Delete**.

Related Topics

SNMP Configuration on page 451
Working with SNMP Notifications on page 453
Working with SNMPv3 Users on page 453

Working with SNMPv3 Users

1. To work with SNMPv3 users:
   - Go to **Administration** > **System** > **Settings** > **SNMP**
   - Go to **Sites** and select a site. Then, select **SNMP**.
2. From the SNMP field, select **SNMPv3**.

   The following parameters display for SNMPv3:
   - Context String
   - Engine ID
   - SNMPv3 Users
3. To add an SNMPv3 user:
   a. From the SNMPv3 field, select **Add**.
   b. Type a user name and security level. Valid security level values are:
      - No Authentication/ No Privacy
      - Authentication/ No Privacy
      - Authentication/Privacy
4. To modify a user, select a user from the list and select **Edit**.
5. To delete a user, select a user from the list and select **Delete**.

Related Topics

SNMP Configuration on page 451
Working with SNMP Notifications on page 453
Working with SNMPv2 Communities on page 452

Working with SNMP Notifications

To work with SNMP notifications:

1. Go to **Administration** > **System** > **Settings** > **SNMP**.
2. Find the **SNMP Notifications** field.
3. To add a notification:
   a. Click **Add**.
   b. Enter the following:
      - Notification name
      - SNMP version
      - IP address and UDP Port of the server that will receive SNMP messages.

c. Click **Add**.

Note
You can create two trap destinations for SNMP Notification. Set the type of message that you will trap from the **Forward Trap** field on the **SNMP** configuration page.

4. To modify notification settings, select a notification from the list and select **Edit**.
5. To delete a notification, select a notification from the list and select **Delete**.

Related Topics

SNMP Configuration on page 451
Working with SNMPv3 Users on page 453

MAC Format

ExtremeCloud IQ Controller provides the ability to define the user MAC address format for MAC-based authentication. Select from a set of MAC encoding formats, to match the format that you are using in your existing authentication infrastructure.

Select the MAC address format and click **Save**.

Related Topics

Settings on page 450

AP Transmit Power Representation

You have the option to display AP power representation per chain or total power per radio for the ExtremeWireless 11ax access points.

The benefits of configuring power representation per chain, is to accommodate for different radio operation modes, including low power modes, which are smaller values than total radio power. Based on the AP Transmit Power Representation setting, the following AP related information is affected:

- Calculations and configuration related to the operational mode or antenna configuration.
- Displayed statistics and reported values from the AP to the appliance.

To configure the AP Transmit Power Representation:

1. Go to **Administration** > **System** > **Settings**.
2. Scroll down to the **AP Transmit Power Representation** pane.
3. For Configure and Report Tx Power, select **Per Chain** or **Total Per Radio**.
4. Select **Save**.

Related Topics

Settings on page 450

External NAT

ExtremeCloud IQ Controller supports External Network Address Translation (NAT), providing a secure means for remote users to access a campus network.

Configure a single address as an intermediary between the public internet and your private campus network. NAT improves network security by controlling access to the public network.

When deploying ExtremeCloud IQ Controller on private network behind NAT, configure the network as follows:

- Configure two external internet connections for high availability and identify the IP address of each connection.
- On each ExtremeCloud IQ Controller, configure a physical or Bridged@AC VLAN with Device Registration enabled. The VLAN has an internal IP address.
- On each NAT device, configure a port mapping from external port 4500 to the IP address of ExtremeCloud IQ Controller (physical Bridged@AC VLAN, port 4500).
- On each ExtremeCloud IQ Controller, configure the external NAT IP address.

To configure the external NAT IP address on ExtremeCloud IQ Controller:

1. Go to **Administration** > **System** > **Settings**.
2. Scroll down to the **External NAT** pane.
3. Enter the IP address of the NAT device on the public internet.
4. Select **Save**.

This feature is supported in a high availability pair, but The External NAT IP address configuration is specific to each controller. The settings are not synchronized in a high availability pair.

Note
The high availability failover list is limited to a four IP addresses. The external IP address counts as one address in the failover list; therefore, only three topologies with device registration enabled are supported. If you have four VLANs with device registration enabled, ExtremeCloud IQ Controller will not configure the external NAT IP address. Similarly, when an external NAT IP address is configured, you cannot enable device registration on a fourth VLAN. The update is refused.

All ExtremeWireless access points that are supported by ExtremeCloud IQ Controller support External NAT.

Related Topics

Settings on page 450

Broadcast Multicast Traffic Control

Controllers replicate packets, forwarding multiple copies of original incoming broadcast and multicast frames to outgoing destinations. This works well in most environments, but it can be inefficient in large venues that have a lot of traffic. Enable Broadcast Multicast Traffic Control to throttle packet replication, avoiding packet loss when traffic is at its peak.

Broadcast Multicast Traffic Control affects wireless traffic only. It is disabled by default.

Related Topics

Settings on page 450

Web Proxy

A proxy server is an additional server in a client-server deployment that provides additional data security boundaries, protecting users from malicious activity on the internet.

Defined web-proxy connectivity is required in order to allow License Management and other secure web-based connections. Define a proxy server and its authentication credentials here:

Proxy

Select this option to use Web Proxy.

Address

The IP address of the proxy server.

Port

Proxy server Port ID

Authentication

Select this option if the proxy server requires authentication.

User

User ID — Authentication credentials for the proxy server.

Password

Password — Authentication credentials for the proxy server.

Related Topics

Settings on page 450

NEW! *Dynamic Authorization Server Configuration*

It is possible to configure the Dynamic Authorization Server (DAS) replay interval and disable replay protection for data packets.

Note
If you disable replay protection, all data packets are accepted.

Replay protection allows for accepting packets only if the packet timestamp is within a configured tolerance. By default, replay protection is enabled on ExtremeCloud IQ Controller for RFC3576(DISC/COA) packets, with a Replay Interval value of 300 seconds.

Configure DAS settings here:

Port

Specify the DAS port. Valid values are 1024-65535.

Replay Interval [Seconds]

DAS replay interval, measured in seconds. Valid values are 0-1000. To disable replay protection, set the Replay Interval value to 0.

System Logging Configuration

Syslog event reporting uses the syslog protocol to relay event messages to a centralized event server on the enterprise network. In the protocol, a device generates messages, a relay receives and forwards the messages, and a syslog server receives the messages.

System Log Level

Determines the error severity that is logged for the appliance and AP. Select the least severe log level that you want to receive: Information, Minor, Major, Critical. For example, if you select Minor, you receive all Minor, Major and Critical messages. If you select Major you receive all Major and Critical messages. The default is Minor.

Enable **Report Station Events** to collect and display station session events on the ExtremeCloud IQ Controller station events log.

Enable **Forward Station Events as Traps** to notify the administrator of events without solicitation. An SNMP trap is an event notification sent by the managed agent (a network device) to the management system to identify the occurrence of conditions. Traps can save network resources by reducing SNMP polling.

Syslog

Provide the IP Address of 1-3 syslog servers and enable the type of messages that you want to send to the syslog servers.

- **Send all Service Messages**
- **Send Audit Messages**
- **Send Station Events**

Note
To synchronize the logs, the syslog daemon must be running on both the appliance and on the remote syslog server. When you change the log level on the appliance, you must modify the appropriate setting in the syslog configuration on remote syslog server.

Facility Codes

Facilities codes identify log streams in the remote syslog server. Select a unique facility code (local.0 - local.6) for each ExtremeCloud IQ Controller facility to differentiate the log streams and facilitate the filtering of messages.

The facility code applies to all three servers. Select a facility code for each of the following:

- Application Facility
- Service Facility
- Audit Facility
- Station Facility

Related Topics

Logs on page 376
View Events on page 379
View Station Events on page 380
View Audit Events on page 380
View All AP Events on page 381
Set a Logging Filter on page 382

System Information

Go to **Admin** > **System** > **System Information** to view the following information about your system.

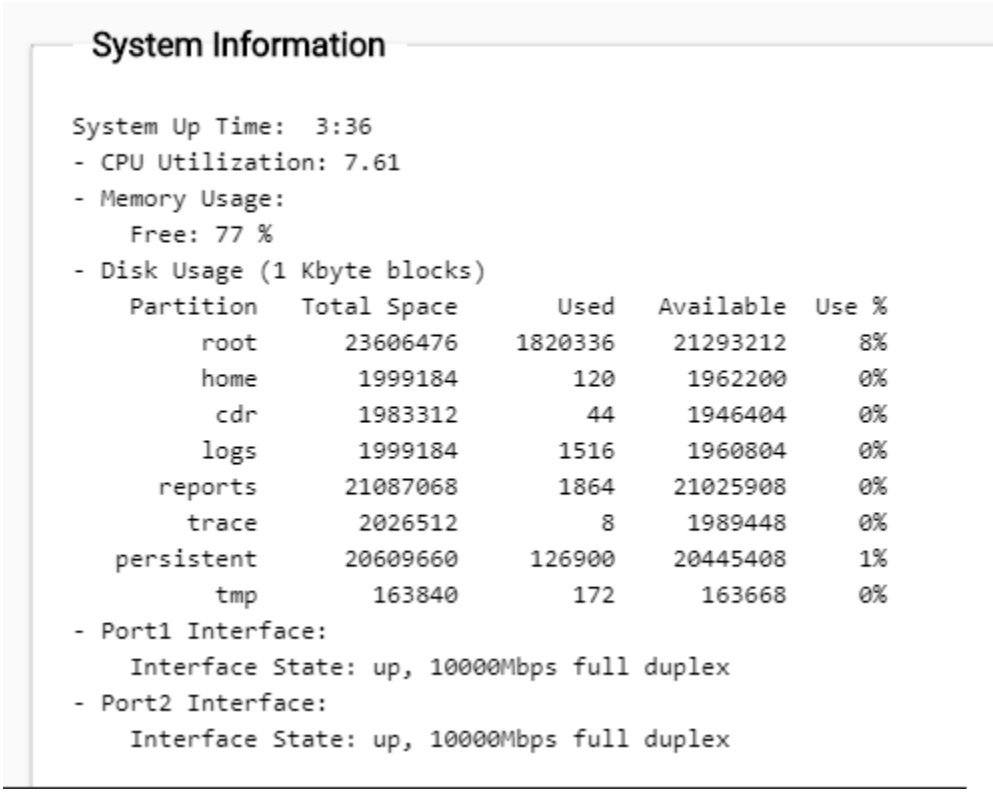


Figure 113: Example System Information

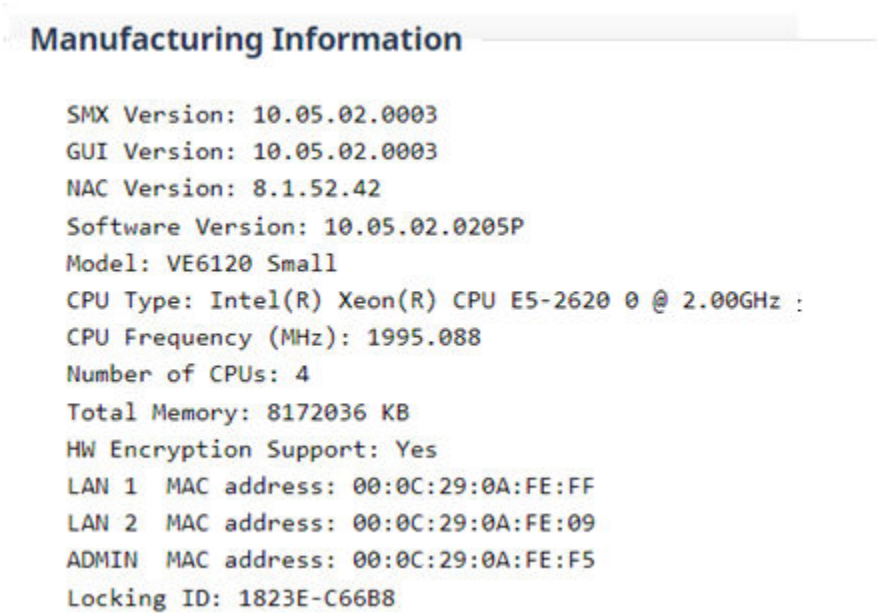


Figure 114: Example Manufacturing Information

Trust Points

When configuring a secure RADSEC protocol for RADIUS servers, you must specify a Trust Point certificate file. This is the certificate file of the Access Network Provider (ANP) and its private key.

To add a new Trust Point, select **Add** and upload a certificate file for the Trust Point.

To delete one or more Trust Points, select the check box next to the Trust Points and select **Delete**.

The following information is provided for each Trust Point:

- Trust Point Name
- Used By
- Function
- Issued By
- Issued To
- Valid Dates

Related Topics

Add a Trust Point on page 460
RADIUS Settings on page 332
Configuring Column Display on page 43
Search Facility on page 42

Add a Trust Point

Before you can configure the secure RADSEC protocol for the RADIUS server, configure a Trust Point here.

To add a new Trust Point to ExtremeCloud IQ Controller, upload a certificate file:

1. Go to **Administration** > **System** > **PKI Trust Points**.
2. Select **Add**.
3. Provide a Trust Point Name.
4. Select from the following options:
   Upload encrypted PKCS#12 file

   Select this option to upload a secure file type .p12 or .pfx. These file types require a password. Additionally, a PEM-encoded CA public certificate file is supported.

   Select **Choose File** and navigate to the specific file.

   Upload separate files

   Select this option to upload a certificate file and a separate private key file with a password. Additionally, a PEM-encoded CA public certificate file is supported.

   Select **Choose File** and navigate to the specific files.
5. To save the Trust Point, select **Save**.

Now, you can use the Trust Point in your RADIUS server configuration.

Related Topics

RADIUS Settings on page 332

Manage Administrator Accounts

ExtremeCloud IQ Controller is shipped with a factory-set, default administrator account with full rights:

- The user ID is `admin`.
- The factory preset password for this account is `abc123`.

  These values are case sensitive. During initial configuration of ExtremeCloud IQ Controller, the CLI wizard prompts you to change the default Admin user ID and password.

To add administrator accounts:

1. Go to **Administration** > **Accounts**.
2. Select **Add** and configure the following parameters:
   Username

   User name for the administrator account.

   Password

   Password for the administrator account.

   Confirm Password

   Re-enter password for the administrator account.

Admin Role

Select the level of access privileges for the administrator account. Valid values are:

- Full. Full administrative privileges.
- Read-Only. Ability to log on and view administrative pages.
- Custom. Configure user access to specific areas and features of ExtremeCloud IQ Controller. Select **Custom** > **Configure** to display the list of Admin roles.

3. To edit account settings:
   a. Select and existing account from the list.
   b. Modify settings as necessary, and select **Save**.

   Note
   You can generate API keys that are used to access Extreme Defender Application when editing an existing user account.

4. To delete an existing account:
   a. Select and existing account from the list.
   b. Click **Delete**.

   Note
   All administrator accounts *except* the default account can be deleted.

Related Topics

REST API Access for Docker Container Applications on page 473
Manage RADIUS Servers for User Authentication on page 461
Custom User Account Access on page 462

Manage RADIUS Servers for User Authentication

Configure a list of RADIUS servers to authenticate users of ExtremeCloud IQ Controller.

1. Go to **Administration** > **Accounts** > **RADIUS**.
2. To add a RADIUS server to the Authentication Order, under **Authentication Order**, select **Add**.

   Order the servers as Local first and RADIUS second until you have tested the RADIUS server.
3. To add the properties of the RADIUS server, under **RADIUS Servers**, select **Add**.

   Select the **IP Address** field to display a list of available RADIUS servers. Select the RADIUS server row to add or delete a RADIUS server.

   Note
   CHAP is the default authentication method used by ExtremeCloud IQ Controller. When configuring integration with ExtremeControl™ specify CHAP on ExtremeControl.

4. Select the **Test** button to test your server connection.

   Make sure the test completes successfully.

5. With the server order still Local first and RADIUS second, log in with your Active Directory user name and password.

   If this fails, make sure your Remote Access Policy is returning the required Service-Type of *Administrative*.

   Note
   To allow ExtremeCloud IQ Controller to accept the RADIUS Attributes coming from the External authentication server, configure a Pass Through External RADIUS Rule. Go to **OnBoard** > **Rules**.

Related Topics

RADIUS Settings on page 336
Advanced RADIUS Settings on page 337

Custom User Account Access

You can configure separate user access to specific areas and features of ExtremeCloud IQ Controller.

1. Go to **Administration** > **Accounts**.
2. To display account parameters, select an account or select **Add**.
3. From the **Admin Role** field, select **Custom** > **Configure**.
4. Select **Read-Only** or **Read-Write** for each of the following product areas.

   Read-Only access enables you to view or monitor the area. **Read-Write** access enables you to configure the area.

   Note
   When configuring a new account, you have the option to configure a **Preset** access level that applies to all areas of ExtremeCloud IQ Controller.

   Site

   Monitor or configure sites, configuration Profiles, device groups, policy roles, VLANs, mesh networks, floor plans, AAA Policy, and monitor clients within ExtremeCloud IQ Controller. For more information, see:

   - Sites on page 129
   - Sites List on page 52
   - Configuring Roles on page 291
   - Configuring VLANS on page 303
   - Configure a Mesh Point Network on page 262
   - Configuring a Floor Plan on page 193
   - AAA RADIUS Authentication on page 326
   - Clients on page 115

   Networks

   Monitor or configure ExtremeCloud IQ Controller networks. See Managing a Network Service on page 290 and Networks List on page 110.

Access Points

Monitor or configure ExtremeCloud IQ Controller access points. See Access Points on page 205 and Access Points List on page 69.

Switches

Monitor or configure ExtremeCloud IQ Controller switches. See Switches on page 239 and Switches List on page 105.

eGuest

Monitor or configure ExtremeCloud IQ Controller integration with ExtremeGuest. See ExtremeGuest Integration on page 324.

Adoption

Monitor or configure ExtremeCloud IQ Controller Adoption rules. See Automatic Adoption on page 317.

Troubleshoot

Monitor or configure packet capture for sites and device groups and open a remote console. See Packet Capture on page 93 and Opening Live SSH Console to a Selected AP on page 98.

Onboard AAA

Monitor or configure AAA policy and add Local Accounts. See Onboard AAA Authentication on page 334.

Onboard Captive Portal

Monitor or configure ExtremeCloud IQ Controller internal captive portal. See Manage Captive Portal on page 345.

Onboard Groups and Rules

Monitor or configure access control groups and rules. See Manage Access Control Groups on page 358 and Access Control Rules on page 361.

Onboard Guest CP

Monitor or configure ExtremeCloud IQ Controller ExtremeGuest captive portal settings. See ExtremeGuest Captive Portal Settings on page 283.

Platform

Monitor or configure Administration system settings. See System Configuration on page 425.

Accounts

Monitor or configure Administration account settings. See Manage Administrator Accounts on page 460.

Applications

Monitor or install and configure Docker applications. See ExtremeCloud IQ Controller Applications on page 464.

Licensing

Monitor or configure Administration Licensing. See Product Subscription License on page 475.

CLI Access

Access to the Switch CLI Console. See Access the Switch CLI on page 246.

Related Topics

Manage Administrator Accounts on page 460

ExtremeCloud IQ Controller Applications

ExtremeCloud IQ Controller operates as the base operating system for container applications that will share its resources.

ExtremeCloud IQ Controller supports container applications that offer custom solutions for network management. Applications are installed as .Docker files available on Extreme Networks support site or downloaded from the Docker hub.

Note

You can install the application from a local image file or you can download an image file from Docker Hub. Before an image file is downloaded from Docker Hub, ExtremeCloud IQ Controller checks the image version. When a newer version is available, a message is displayed on the ExtremeCloud IQ Controller user interface. ExtremeCloud IQ Controller does not download information from Docker Hub. It only checks the application version.

ExtremeCloud IQ Controller supports integration with Amazon Greengrass. Therefore, it periodically checks availability of the service. ExtremeCloud IQ Controller does not upload or download information to and from these services.

Communication from ExtremeCloud IQ Controller to Docker Hub or AWS can be blocked on the firewall. When communication is blocked, the application continues to operate normally, but you will not be notified when a newer image file is available on Docker Hub.

Note

A Domain Name Server (DNS) is required when deploying container applications because the application logic may require access to external resources (such as the Docker Repository). For information about configuring a Domain Name Server (DNS), see the ExtremeCloud IQ Controller Deployment Guide.

Related Topics

Install an Application on page 465
Upgrade an Application on page 469
Uninstall an Application on page 470
Application Details on page 470
Extreme Defender for IoT on page 470
Scheduler for ExtremeCloud IQ Controller on page 471
AirDefense Base Application on page 472

Install an Application

Sometimes, before installing a container application, you must create a configuration template for the application. However, most Extreme Docker applications offer a pre-configured template.

Note
The following Extreme Docker applications are installed with default configuration templates. You cannot modify templates for the following applications:

- Extreme Defender Application
- Scheduler for ExtremeCloud IQ Controller
- AirDefense Base Application

For more information about template configuration settings, see Configuration Template Details on page 466.

Before running the installed application, you must generate an API Key and associate it with the application. For more information about the API Key, see REST API Access for Docker Container Applications on page 473.

Note
ExtremeCloud IQ Controller supports installation of a Docker file with a specific numerical version. Applications indicating the *"Latest Version"* or version numbers that include alphabetic characters are not supported. Twenty percent of the appliance hardware capacity is allocated for Docker file applications.

Take the following steps to install an application:

1. Go to **Administration** > **Applications**.
2. Select **Add** to create the Configuration Template.

   Note
   Several Extreme applications include default templates that cannot be edited. Skip this step when installing:

   - Extreme Defender Application
   - Scheduler for ExtremeCloud IQ Controller
   - AirDefense Base Application

3. Select  to add an application to ExtremeCloud IQ Controller.
4. Install from a local **File** or Docker hub **Registry**.
5. To install directly from the Docker hub, select **Registry**, then **OK**. Or,
6. To install a local file, select **File** > **Upload**.
7. Navigate to the Docker file and select **Open**.
8. Select **OK**.

   The application is uploaded and installed on ExtremeCloud IQ Controller.
9. Generate an API key and associate it with the application before running the application.

Select ▶ to start the application.

Note
You must generate an API Key and associate it with the application before running the application.

The following describes the available application actions:

- ⚙ — Install new application.
- ✎ — Edit Configuration Template. (Not available for Extreme Defender Application or Scheduler for ExtremeCloud IQ Controller.)
- ⬆ — Upgrade existing application.
- ⊖ — Uninstall application.
- ▶ — Start application.
- ■ — Stop application.
- ◐ — Show application statistics. Displays dashboard widgets, configuration details, and logs, and it provides console access to the application for troubleshooting.

Related Topics

Generate API Keys on page 473
Associate API Key File with a Docker Application on page 475
Configuration Template Details on page 466
Upgrade an Application on page 469
Uninstall an Application on page 470
Application Details on page 470

Configuration Template Details

Note
The following Extreme Docker applications are installed with default configuration templates. You cannot modify templates for the following applications:

- Extreme Defender Application
- Scheduler for ExtremeCloud IQ Controller
- AirDefense Base Application

Use a configuration template to install and upgrade container applications in ExtremeCloud IQ Controller.

To add a template:

1. Go to **Administration** > **Applications** and select **Add**.

2. Configure the following parameters:

Table 112: Container Application Configuration Template

Field	Description
Name	Application name
Title	Application title
Description	Text description
Proxy URL	Check to enable a URL proxy for your application. Clear to disable a URL proxy. Consider the following when using Proxy URL: • Applications are accessible through `https://ip:5825/apps/<appname>`. • After installed, the application can be accessed directly from ExtremeCloud IQ Controller. • The internal port in the container must be TCP port 8887. • The base URL must begin with the application name. For example: /defender. • The application must use relative URLs.
Icon	The application icon. Select **Change** to select a new image file. After selecting a new image file, the **Default** button displays. Select **Default** to revert to the default image.
Image	The application image file name that is used in the Docker Registry. Or, for local files, the application name that is tagged in the local Docker file.
Entry Point Arguments	Program used to start the application. The Entry Point Arguments are provided by the container application by default. Provide a value only if you must override the default Entry Point Arguments. **Note:** Docker command line options, such as `privileged`, are not supported.
Registry	**Docker Hub** is the only supported registry.
Upload File Format	Local file format.
Logs Config	Log file format. Valid values include: • json-file. Default value, which enables you to view the application logs from the application **Details** icon in ExtremeCloud IQ Controller. • syslog. View application logs from the System log file. • gelf. Graylog Extended Log Format.

Table 112: Container Application Configuration Template (continued)

Field	Description
Restart Policy	Indicates the application restart behavior when ExtremeCloud IQ Controller is started. Valid values are: • Always. The application will always restart. • Unless Stopped. The application will restart unless it was manually stopped prior to the ExtremeCloud IQ Controller start. The application will keep its current state. • Failed. Will restart only after an application failure.
CPU Limit	Used to manage CPU allocation when multiple applications are installed. Max limits are dependent on the appliance platform limitations.
Memory Limit (MB)	Used to manage memory allocation when multiple applications are installed. Max limits are dependent on the appliance platform limitations. Default value is 50 percent of maximum limitation.
Volume Mapping	Indicates folder name and path for volume storage. Volume storage will not be deleted upon application *upgrade*. **Note:** All data is deleted when the application is *uninstalled*.
Config Files Mapping	Indicates folder name and path for configuration files, including API key files.
Port Mapping	Configure source and destination ports for the application. The external port range must be 32768-65535, because this is the open port filter range.
Environment Variables	Configure environment variables.

Related Topics

Install an Application on page 465

Access an Application

After an application is installed on ExtremeCloud IQ Controller, take the following steps to access the application:

1. Go to **Administration** > **Applications**.

   The applications that ExtremeCloud IQ Controller supports by default are listed. Applications that are installed and running are indicated by a green dot icon.
2. To open an application in a separate browser window, select the application.
3. Alternately, you can access an application user interface using the HTTPS protocol on the TCP port 5825. For example, if your ExtremeCloud IQ Controller has the IP address 192.168.10.10, you can manage the container application in a browser

by typing `https://192.168.10.10:5825/apps/[application_name]` into the URL field.

Table 113: Application Names in Browser Address

Application	Application in browser address
Extreme Defender Application	`apps/defender`
AirDefense Base	`apps/airdefense_base`
Scheduler for ExtremeCloud Appliance	`apps/extreme-scheduler`

The login screen for the selected application displays. Your login credentials will match your ExtremeCloud IQ Controller credentials.

Related Topics

Generate API Keys on page 473
REST API Access for Docker Container Applications on page 473
Install an Application on page 465
Associate API Key File with a Docker Application on page 475
Upgrade an Application on page 469
Uninstall an Application on page 470
Application Details on page 470

Upgrade an Application

Note
Data in Volume storage *will not* be deleted upon application upgrade. However, all data is deleted when the application is uninstalled.

To upgrade an application:

1. Go to **Administration** > **Applications**.
2. To stop the application, select ■ then select **OK**.
3. To begin the application upgrade, select ⊡.
4. Upgrade from a local **File** or Docker hub **Registry**.
5. Select **Upload** and select the Docker file.
6. Select **Open** and select **OK**.
7. Select ▶ to start the application.

Related Topics

Install an Application on page 465
Uninstall an Application on page 470

Uninstall an Application

Note
All application data is deleted when you uninstall an application.

To uninstall an application:

1. Go to **Administration** > **Applications**.
2. To stop the application, select .
3. To remove the application, select .
4. To confirm that you want to uninstall the application, select **OK**.

Related Topics

Install an Application on page 465
Upgrade an Application on page 469

Application Details

To access the following details about an installed application, go to **Administration** > **Applications** and click .

- **Dashboard**. Displays CPU and Memory stats for the application.
- **Details**. View the application configuration template details. You must uninstall the application before you can modify the application configuration template.

  Note
  All data is deleted when an application is uninstalled.

- **Logs**. View log files for the application if you have configured the **Logs Config** value on the application configuration template to json-file.
- **Console**. Access the application console for troubleshooting. From the **Console** tab, you can execute custom commands and attach to the application console.
- **Configuration Files**. Access configuration files and API key files associated with the Docker application.

Related Topics

Configuration Template Details on page 466
Associate API Key File with a Docker Application on page 475

Extreme Defender for IoT

Extreme Defender Application provides security management plus traffic and application visibility of connected end devices. It also enables the centralized creation of policies that define network and security settings for groups of IoT devices. SA201 supports enforcement for up to eight end-systems, connected through the wired client port.

Extreme Defender Application is installed as a container application on ExtremeCloud IQ Controller. The application runs and is upgraded independently from the controller. Before accessing Extreme Defender Application, you must generate an API key on

ExtremeCloud IQ Controller and upload it to the controller. Subsequent upgrades can use the previously installed API key file.

ExtremeCloud IQ Controller offers a default configuration template for the Extreme Defender Application. This template cannot be modified.

Note
The Extreme Defender Application is available on the Extreme Networks support site.

To install Extreme Defender Application:

1. Download and install the Docker application.
2. Generate the API key.
3. Associate the API key with the Docker application.

Note
When running more than one ExtremeCloud IQ Controller application that uses an API key file, you need only one generated API key.

4. Start the application.

From the ExtremeCloud IQ Controller **Applications** list, select the Extreme Defender Application to display the Defender login screen. Your login credentials will match your ExtremeCloud IQ Controller credentials.

Additionally, the Extreme Defender Application user interface can be accessed using the HTTPS protocol on the TCP port 5825. For example, if your ExtremeCloud IQ Controller has the IP address 192.168.10.10, you can manage Extreme Defender Application in a browser by typing `https://192.168.10.10:5825/apps/defender` into the URL field.

Related Topics

Generate API Keys on page 473
REST API Access for Docker Container Applications on page 473
Install an Application on page 465
Associate API Key File with a Docker Application on page 475
Upgrade an Application on page 469
Uninstall an Application on page 470
Application Details on page 470

Scheduler for ExtremeCloud IQ Controller

Schedule network services and reports with Scheduler for ExtremeCloud IQ Controller.

Scheduler for ExtremeCloud IQ Controller is installed as a container application on the ExtremeCloud IQ Controller. The application runs and is upgraded independently from the appliance. Before accessing Scheduler application, you must generate an API key from ExtremeCloud IQ Controller and upload it to the controller. Subsequent upgrades can use the previously installed API key file.

ExtremeCloud IQ Controller offers a default configuration template for Scheduler application. This template cannot be modified.

Note
Scheduler for ExtremeCloud IQ Controller is available on the Extreme Networks Support site.

To install Scheduler for ExtremeCloud IQ Controller:

1. Download and install the Docker application.
2. Generate the API key.
3. Associate the API key with the Docker application.

Note
When running more than one ExtremeCloud IQ Controller application that uses an API key file, you need only one generated API key.

4. Start the application.

Related Topics

Generate API Keys on page 473
REST API Access for Docker Container Applications on page 473
Install an Application on page 465
Associate API Key File with a Docker Application on page 475
Upgrade an Application on page 469
Uninstall an Application on page 470
Application Details on page 470

AirDefense Base Application

The AirDefense Base Application offers a free Wireless Intrusion Prevention System (WIPS), enabling you to configure a port for WIPS.

The AirDefense Base Application is installed as a container application on ExtremeCloud IQ Controller. The application runs and is upgraded independently from the appliance. After you install and start the AirDefense Base Application, it listens to the AP connections and interacts with ExtremeCloud IQ Controller to gather the status of the AP.

You must configure an ADSP configuration Profile to work with AirDefense Base Application. For more information, see AirDefense Profile Settings on page 161.

For Extreme AirDefense documentation, go to extremenetworks.com/documentation, and navigate to **Wireless & Mobility** > **Extreme AirDefense**.

Related Topics

AirDefense Profile Settings on page 161
Generate API Keys on page 473
REST API Access for Docker Container Applications on page 473
Install an Application on page 465

Associate API Key File with a Docker Application on page 475
Access an Application on page 468
Upgrade an Application on page 469
Uninstall an Application on page 470
Application Details on page 470

REST API Access for Docker Container Applications

Use an API key to allow Docker containers access to the ExtremeCloud IQ Controller REST API. A randomly generated key allows access to ExtremeCloud IQ Controller without requiring the user to be actively logged in, and it can allow access privileges that are greater than the privileges of the application user. The API key can be used in place of the password of the original account.

Note
When running more than one ExtremeCloud IQ Controller application that uses an API key file, you need only one generated API key.

After the key is randomly generated, download the key as a .json file and map it as a read-only configuration file to the Docker application.

Related Topics

Generate API Keys on page 473
Associate API Key File with a Docker Application on page 475

Generate API Keys

Note
When running more than one ExtremeCloud IQ Controller application that uses an API key file, you need only one generated API key.

1. Go to **Administration** > **Accounts**.
2. Select a user account.

3. From the API Keys field, select **Generate New API Key**.

   The key is generated. The **API Key** dialog displays.

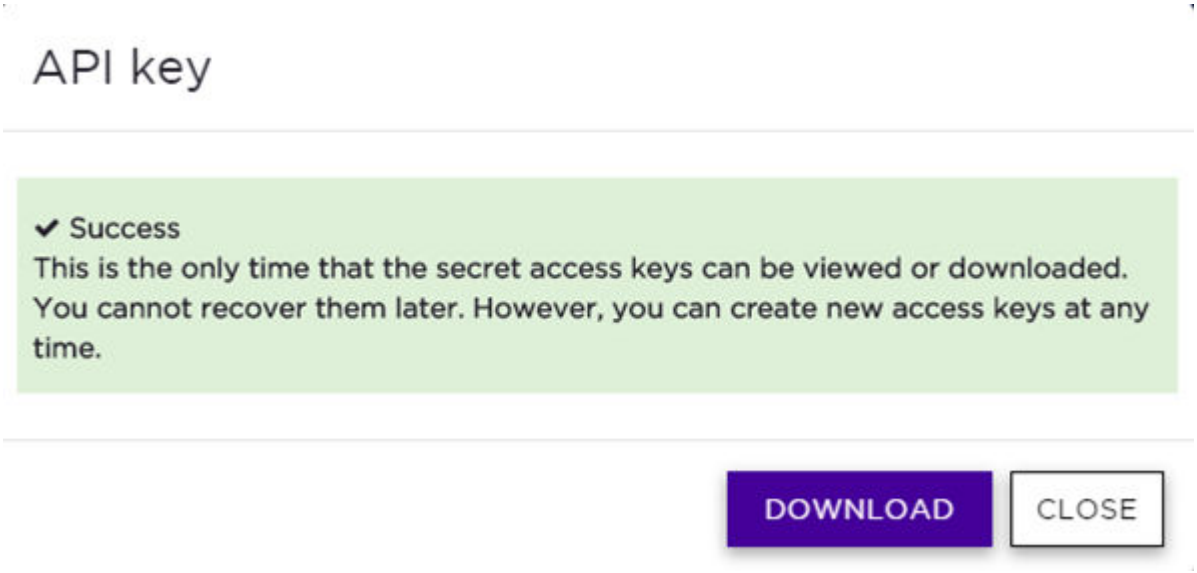


Figure 115: API Key dialog

4. To download the API key as a .json file, select **Download**.

   Download the key immediately. If you select **Close**, you will not be able to access the key. You can generate additional keys at any time.
5. After you download the key, select **Close**.

Related Topics

Delete API Keys on page 474
REST API Access for Docker Container Applications on page 473
Associate API Key File with a Docker Application on page 475
Configuration Template Details on page 466
Manage Administrator Accounts on page 460

Delete API Keys

Generated API keys are listed on the user account page. To delete a key:

1. Go to **Administration** > **Accounts**..
2. Select a user account.
3. Select a key from the API Keys list, and select 🗑.

   A verification message displays.
4. To delete the API key file, click **OK**.

Related Topics

Generate API Keys on page 473

Associate API Key File with a Docker Application

To upload a generated API key file:

1. Go to **Administration** > **Applications** and select .
2. Select the **Configuration Files** tab.
3. Select **api-keys.json**, and then select the upload icon .
4. Upload the API key file one of the following ways:
   - Click the **Choose File** box and navigate to the downloaded API key file.
   - Drag and drop the downloaded API key file onto the **Choose File** box.

   The API key file displays in the **Configuration Files** list.

Related Topics

Generate API Keys on page 473

Remove a Configuration File from a Docker Application

Take the following steps to remove a configuration file from a Docker application:

1. Go to **Administration** > **Applications** and select .
2. Select the **Configuration Files** tab.
3. Select a configuration file, then select .

   A verification message displays.
4. To remove the configuration file, select **OK**.

Related Topics

Associate API Key File with a Docker Application on page 475
Configuration Template Details on page 466
Manage Administrator Accounts on page 460
Generate API Keys on page 473
Delete API Keys on page 474

Product Subscription License

ExtremeCloud IQ Controller is available for subscription licensing only, leveraging a single subscription SKU with ExtremeCloud IQ. The number of licenses corresponds to the number of managed access points and switches.

License management is handled through connection with the LEM server. The capacity license is unified with ExtremeCloud IQ license models, supporting both Navigator and Pilot level subscriptions.

Each appliance obtains capacity Right to Use (RTU) entitlements regarding managed devices, subject to the system limits of the appliance instance and the total number of activations purchased. The total consumed RTUs across all ExtremeCloud IQ Controller instances cannot exceed the number of RTUs you have subscribed to. Each appliance provides visualization on specific RTU allocation and overall balance.

For subscription management, you must have an ExtremeCloud IQ Navigator or Pilot account, and the controller requires interaction with active DNS and NTP servers. Both

elements must be specified during the initial provisioning of the appliance. Typically, ExtremeCloud IQ Controller accesses the license server (cloud-based service) via the internet. The controller's DNS server configuration facilitates resolution of the URL: https://prod.extreme.sentinelcloud.com/productConnector/. When there is a firewall in place, it must allow access to that service (HTTPS = TCP 443) to connect to the License Server.

Note
If internet access is not available for continuous connectivity to the cloud server, you can install an air gap licensing file that is generated from the Extreme Networks Support Portal.

With an internet connection, after the controller is licensed, it can be onboarded to ExtremeCloud IQ to take advantage of Cloud Visibility into the network. The minimum ExtremeCloud IQ integration support is a Navigator license with the ability to support ExtremeCloud IQ Pilot license. A single SKU is required per device, regardless of whether you will manage the device from the controller or from the cloud. ExtremeCloud IQ manages the Navigator or Pilot entitlements for the number of managed APs and switches.

Upon purchase of a new ExtremeCloud IQ Controller you will receive a welcome email and activation instructions. The following is required to obtain a new ExtremeCloud IQ Controller subscription license:

- An ExtremeCloud IQ Navigator or Pilot licensed account
- An Activation Package that is generated from the Extreme Support Portal

  To license ExtremeCloud IQ Controller, go to the Extreme Networks Support Portal and generate the Activation Package. You must complete a one-time-only activation process for each instance of ExtremeCloud IQ Controller.

  Apply the Activation Package to each controller instance before ExtremeCloud IQ Controller can consume Subscription License Right To Use (RTUs).
- If your deployment does not have continuous internet access, you will need to generate an air gap file from the Extreme Support Portal and install the file on ExtremeCloud IQ Controller.

The following Activation types are available:

- **Evaluation** — A temporary activation key is available for customer product evaluation (up to the system limit of devices), for a duration of either 30, 60, or 180 days.

  After the evaluation period is up, the temporary activation expires. You must generate and install a permanent Activation Package on the controller. If you do not install an activation package, the appliance generates event logs every 15 minutes, indicating that an appropriate license is required for the current software version. In addition, you will not be able to edit the Network Service parameters.
- **Subscription** — An activation that is a subscription license with a specified duration, enabling activation for a specific software release version.

The migration path from Extreme Campus Controller v5.x to ExtremeCloud IQ Controller v10.x is described as follows:

- If you have a subscription license for Extreme Campus Controller v5.x, your migration path to ExtremeCloud IQ Controller v10.x subscription is automatic. This will include the ExtremeCloud IQ Navigator license under the same licensing terms.
- If you have a perpetual license to Extreme Campus Controller v5.x, with a subscription to ExtremeCloud IQ — Site Engine, the AP capacity of the controllers is included in the capacity of the Site Engine migrations, and therefore available upon upgrade.
- If you have a perpetual license to Extreme Campus Controller v5.x alone, you must contact your Extreme Networks support team to determine your new subscription capacity.

Note
In some cases where a contract has several activations, it may be recommended to map the Locking ID to the Voucher ID. In this case, please contact GTAC to determine if mapping between the Locking ID and Voucher ID is recommended.

ExtremeCloud IQ Controller is licensed in the Wide-World regulatory domain.

Important
Ensure that ExtremeCloud IQ Controller is configured with the correct Network Time Protocol (NTP) Server settings. Licensing management and several other system functions are dependent on an accurate timestamp. Configure NTP settings on ExtremeCloud IQ Controller during the initial setup wizard or alternatively under **Administration** > **System** > **Network Time** (as a first configuration step).

Related Topics

Generate and Install the Activation Package on page 478
Upgrade to ExtremeCloud IQ Controller on page 482
License Details on page 485
Licensed Devices on page 477
Entitlements on page 488
Activations on page 488
Air Gap Licensing File on page 480

Licensed Devices

ExtremeCloud IQ Controller supports the following access point models:

- AP3000/X
- AP302W
- AP305C/CX
- AP305C-1
- AP310i/e

- AP310i/e-1
- AP360i/e
- AP4000
- AP4000-1
- AP410i/e
- AP410i-1
- AP410C
- AP410C-1
- AP460i/e
- AP460C/S6C/S12C
- AP5010
- AP5050U/AP5050D
- AP505i
- AP510i/e
- AP510i-1
- AP560i/h
- AP3917i/e/k
- AP3916ic
- AP3915i/e
- AP3912i
- AP3935i/e
- AP3965i/e

The access points are manufactured with a specific domain lock. They are configured for either an FCC or ROW license domain.

For a list of supported switches, see the *Release Notes*.

Related Topics

Product Subscription License on page 475

Generate and Install the Activation Package

All customers must generate and install an Activation Package for ExtremeCloud IQ Controller. Regardless of whether you obtain a new license or upgrade to ExtremeCloud IQ Controller, follow these steps to generate and install the Activation Package:

1. To obtain the controller Locking ID:
   a. Log in to ExtremeCloud IQ Controller.
   b. Go to **Administration** > **License** > **License Details**.

   Note
   The Locking ID is the controller Serial Number.

2. Log into the Extreme Networks Support Portal.
3. Go to **Assets** > **Licenses Home** and select the ExtremeCloud IQ Controller Voucher ID line item from the list.
4. On the **Voucher Details** page, select **Generate Activation Key**.

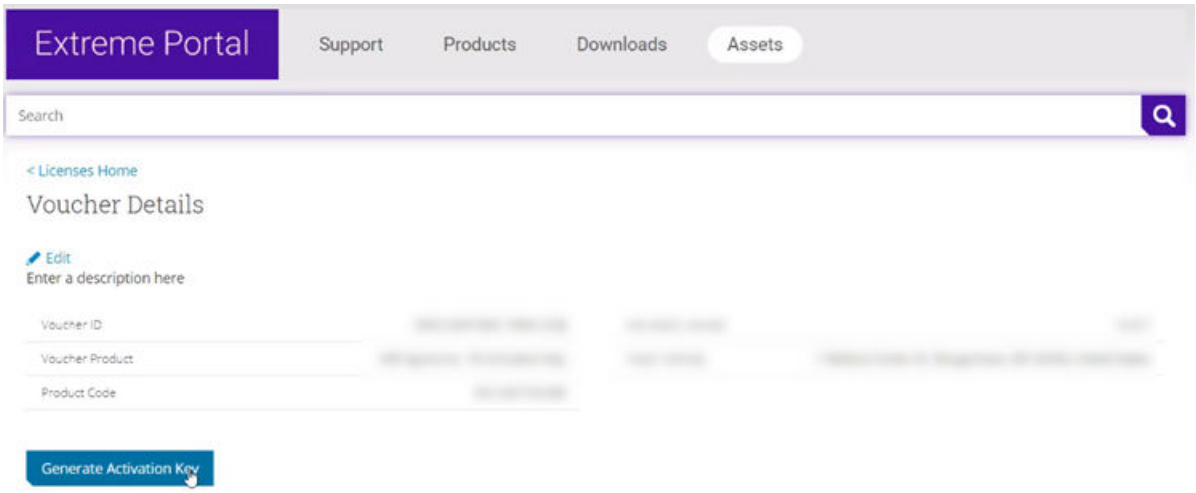


Figure 116: Generate Activation Key

5. Provide the Locking ID for the ExtremeCloud IQ Controller to be activated.
6. Check the box to accept **Terms and Conditions** and select **Submit**.
7. The Activation Package is generated.
   The **Save As** dialog displays.

Install the Activation Package

Stage your ExtremeCloud IQ Controller instance. Install the Activation Package to activate ExtremeCloud IQ Controller:

1. Return to the ExtremeCloud IQ Controller instance from where you obtained the Locking ID.
2. Go to **Administration** > **License** > **License Details**.
3. Select the plus sign next to the **Activation Package** field.

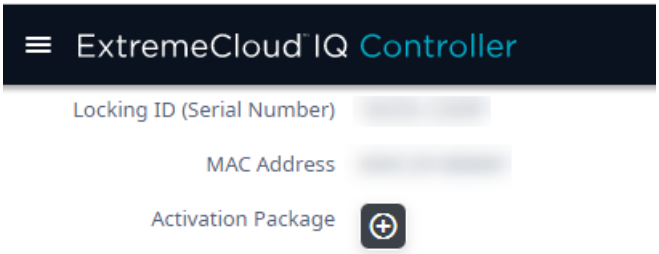


Figure 117: Installing New Activation Package

4. Drag the Activation Package to the **Upload License** dialog to install the Activation Package.
5. Refresh the browser after installing the Activation Package.

Note
It is possible to upload another activation package and override an existing license.

Uploading a new activation will reset and override the ExtremeCloud IQ Controller CUID. The licensing attributes for the CUID are updated to the information that is included in the last uploaded file. Synchronize ExtremeCloud IQ Controller with the LEM licensing server after uploading the latest activation package.

Related Topics

License Details on page 485
Upgrade to ExtremeCloud IQ Controller on page 482

Air Gap Licensing File

For ExtremeCloud IQ Controller installations that do not have continuous internet access, we offer an air gap licensing file that includes all entitlements with the term details of each entitlement. Obtain the licensing file from the Extreme Networks Support Portal and install the air gap licensing file onto the controller.

In an availability pair, the entitlements are pooled. You can install the air gap file on either controller or on both controllers, splitting the total number of entitlements between the two controllers.

Note
Air gap licensing is recommended for installations without continuous internet connectivity.

The same subscription licensing rules and grace periods apply for air gap mode as with connected mode (continuous connection to the cloud server). For more information, see Grace Periods on page 484.

Related Topics

Install Air Gap File on page 480
Licensing States on page 483

Install Air Gap File

For installations that do not have continuous internet connectivity, we offer an air gap licensing mode. Air gap mode supports licensing for deployments that do not have continuous internet connection. In air gap mode, ExtremeCloud IQ Controller uses a license file that includes the number of entitlements explicitly listed on the file for

on-premises device management. Generate the licensing file on the Extreme Networks Support Portal and install the file onto the controller.

Note
Before you install the air gap license file, install the Activation Package to activate the controller.

To install the air gap license file:

1. Obtain the air gap file from the Extreme Networks Support Portal. For more information, see *ExtremeCloud IQ Controller License Migration Guide*.
2. On the controller, go to **Administration** > **License** > **License Details**.
3. Select **Switch to Air Gap Licensing**.

   The **License File** field displays.
4. Select the plus sign next to the **License File** field.

Figure 118: Air Gap License File Installation

5. Drag the air gap file to the **Upload Air-Gap License** dialog.

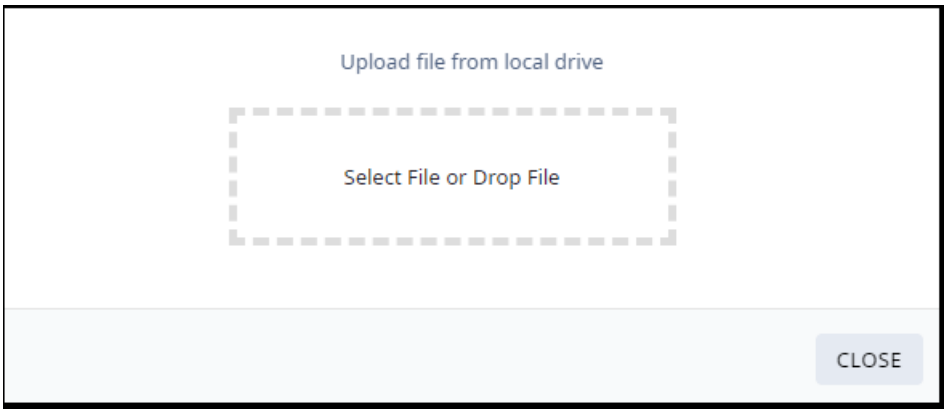


Figure 119: Upload Air Gap License File

6. Refresh the browser after installing the air gap file.

Related Topics

Air Gap Licensing File on page 480
Generate and Install the Activation Package on page 478

Upgrade to ExtremeCloud IQ Controller

All customers who are upgrading to ExtremeCloud IQ Controller v10.x must obtain a new Activation Key.

Note
Upgrading from a previous controller version will result in a license violation. You must apply a new Activation Package for ExtremeCloud IQ Controller.

For customers upgrading from a licensed Extreme Campus Controller v5.x to ExtremeCloud IQ Controller, there is a 15-day grace period during which ExtremeCloud IQ Controller is fully licensed. Before the 15-day grace period ends, you must do the following:

- Obtain an ExtremeCloud IQ account. Ensure your license account has sufficient quantities of ExtremeCloud IQ Navigator or Pilot entitlements, either as part of a migration or as a new order.
- Make sure that the Extreme Networks account team has migrated your Extreme Campus Controller v5.x contract license to a new ExtremeCloud IQ Controller v10.x license within the Support Portal and LEM.

  The migration path from Extreme Campus Controller v5.x to ExtremeCloud IQ Controller v10.x is described as follows:
  - If you have a subscription license for Extreme Campus Controller v5.x, your migration path to ExtremeCloud IQ Controller v10.x subscription is automatic. This will include the ExtremeCloud IQ Navigator license under the same licensing terms.

- If you have a perpetual license to Extreme Campus Controller v5.x, with a subscription to ExtremeCloud IQ — Site Engine, the AP capacity of the controllers is included in the capacity of the Site Engine migrations, and therefore available upon upgrade.
- If you have a perpetual license to Extreme Campus Controller v5.x alone, you must contact your Extreme Networks support team to determine your new subscription capacity.

Note
In some cases where a contract has several activations, it may be recommended to map the Locking ID to the Voucher ID. In this case, please contact GTAC to determine if mapping between the Locking ID and Voucher ID is recommended.

To generate the Activation Package:

1. Log into the Extreme Networks Support Portal.
2. Generate a new Activation Package and install it on the appliance. For more information, refer to Generate and Install the Activation Package on page 478.

   The Activation Package includes your Customer Unique ID (CUID), capacity limits, and certificates for a virtual appliance. (Physical appliances include certificates pre-installed.) You are ready to start managing devices with ExtremeCloud IQ Controller.

Note
You are required to complete a one-time-only activation process for each instance of ExtremeCloud IQ Controller. The activation process is required for all ExtremeCloud IQ Controller installations.

Related Topics

Generate and Install the Activation Package on page 478

Licensing States

Consider the following licensing states for ExtremeCloud IQ Controller v10.01 and later:

- Activation — All customers must generate and install an Activation Package for ExtremeCloud IQ Controller v10.01 and later. ExtremeCloud IQ Controller gives you 15 days to apply a valid Activation Package. A banner indicates the number of days you have remaining in this state.
- Allocation of Subscriptions — After the controller is activated, it engages the licensing server to retrieve a sufficient allocation of subscriptions. Controllers will first attempt to fulfill capacity requirements at the Navigator licensing level. If the account does not have sufficient Navigator capacity, the controller will fulfill the capacity license requirements at the Pilot licensing level. If the customer account does not hold sufficient active subscriptions to cover the number of managed

devices (APs and switches), then a 15-day grace period is provided to allow for correction of the licensing over subscription.

Note
For ExtremeCloud IQ Controller installations that do not have continuous internet access, we offer an air gap licensing file that includes all entitlements with the term details of each entitlement. Obtain the licensing file from the Extreme Networks Support Portal and install the air gap licensing file onto the controller.

Grace Periods

Regardless of the licensing mode, the following grace periods apply:

- 30-day grace period — After your connected-mode subscription expires without renewal, or after the entitlements within the air gap file reach the end date, you have 30 days to renew your license.
- 15-day grace period — After devices reach an unlicensed state, you have 15 days to rectify the issue. Devices are considered unlicensed when you fail to apply the generated Activation Package to the controller, fail to connect to the licensing server, or when you have more connected devices than your license supports.

After the grace period has expired, ExtremeCloud IQ Controller enters a read-only mode. In read-only mode, devices and services continue to operate, but no configuration changes are allowed. After the license subscription terms are renewed or updated, ExtremeCloud IQ Controller becomes fully configurable again.

Synchronizing in Connected Mode

In connected mode, ExtremeCloud IQ Controller connects with the licensing server at the same time each day. (This static time is determined by the controller boot time, and it is displayed on the **Licensing Details** page.) When necessary, you can manually synchronize ExtremeCloud IQ Controller with the licensing server. Consider manually synchronizing after the following conditions:

- After installing an Activation Package
- After a change in capacity entitlements
- After onboarding ExtremeCloud IQ Controller to ExtremeCloud IQ.

To manually synchronize:

1. Go to **Administration** > **License** > **License Details**.
2. Select **Synchronize Now**.

Note
In the event that the ExtremeCloud IQ Controller cannot connect to the licensing server after you have installed an Activation Package for a subscription license, ExtremeCloud IQ Controller gives you three days to rectify the connection issue. If the controller cannot reach the licensing server in three days, on the fourth day, the controller goes into a violation state for 15 days. If the connection to the licensing server cannot be restored within the full 15-day period, the controller goes into read-only mode.

Related Topics

License Details on page 485
Generate and Install the Activation Package on page 478
Air Gap Licensing File on page 480

Entitlement Health Checks

ExtremeCloud IQ Controller checks the state of entitlements assigned in use for the appliance. The System Health Check uses the end-date of entitlement and displays the following banners in the user interface:

- Yellow banner — Some assigned entitlements expire in less than 90 days.
- Red banner — Some assigned entitlements expire in less than 30 days.

Related Topics

Entitlements on page 488

Licensing an Availability Pair

In an Availability Pair, Right to Use (RTU) for APs and switches are shared in a common pool by both primary and backup controllers. When both instances of ExtremeCloud IQ Controller are operational and the tunnel is up, the primary controller checks the licensing server for APs on both controllers. When the primary ExtremeCloud IQ Controller is down, the backup controller checks with the licensing server for APs. The backup controller will be synchronized upon the next automatic sync with the licensing server. You can also manually sync with the licensing server. Select **Synchronize Now**.

Note
The Deployment ID for controllers in a High Availability pair is the Serial Number (Locking ID) of the primary ExtremeCloud IQ Controller.

License Details

From the **License Details** tab, you can determine the licensed status of the controller, install the Activation Package or Air Gap file, and synchronize the controller with the license server.

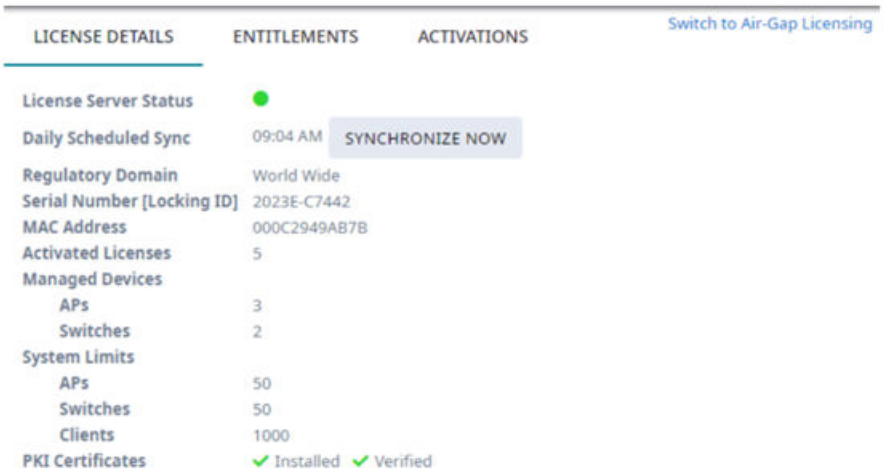


Figure 120: License Details Tab

The **License Details** tab provides the following information about the controller:

License Server Status

When in connected mode, this icon indicates the licensed state of the controller:

- Green indicates that the controller is in compliance with the license.
- Red indicates that the controller is not in compliance with the license or that there is a connectivity issue between the controller and the licensing server.

When appropriate, the following additional information is displayed:

- Current status of the grace period.
- Entitlements have expired.
- Number of devices exceed the licensed entitlements.
- Assigned entitlements are approaching expiration.

When in air gap mode, the **License Server Status** is Air-Gap.

Note
If internet access is not available for continuous connectivity to the cloud server, you can install an air gap licensing file that is generated from the Extreme Networks Support Portal.

From the **License Details** tab, select **Switch to Air Gap Licensing** to install the air gap file.

Daily Scheduled Sync

When in connected mode, the time of day when the controller is automatically synchronized with the LEM server. This synchronization occurs every 24 hours. It is a static timestamp that is determined by the controller boot time.

To synchronize the controller with the LEM server on demand, select **Synchronize Now**.

Regulatory Domain

The regulatory domain of the controller. This value is World Wide.

Serial Number

The serial number of the controller. This is also the controller Locking ID.

MAC Address

The MAC Address of the controller.

Licensed Capacity

The number of used licenses. This number should match the total number of Managed Devices. To ensure that you are viewing the latest license information, select **Synchronize Now**.

Managed Devices

The number of devices that are managed by the controller. This number should match the Licensed Capacity. To ensure you are viewing the latest license information, select **Synchronize Now**.

In the case where you have more managed devices than your license capacity supports, you can delete device overages from the **License Details** tab and bring the number of managed devices into compliance with your license capacity:

1. Select the appropriate button: **Access Points** or **Switches** to display the corresponding device list.
2. From the device list, select the devices to delete.
3. Select **Actions** > **Delete**.

System Limits

Indicates the maximum device limits per controller.

PKI Certificates

Indicates if a PKI (Public Key Infrastructure) Certificate is installed and verified. A PKI Certificate is required to onboard the controller to ExtremeCloud IQ.

The hardware appliances and access points have Extreme CA certificates installed. Also, both a temporary and permanent subscription license for a virtual controller includes a PKI Certificate. For information about certificates, see Certificates on page 343.

Note

Cloud connectivity ( ) is indicated on the product banner. For more information, see Cloud Visibility on page 29.

Related Topics

Entitlements on page 488
Activations on page 488
Certificates on page 343
Cloud Visibility on page 29
Air Gap Licensing File on page 480
Install Air Gap File on page 480

Entitlements

The ExtremeCloud IQ Controller **Entitlements** page is a log of available license capacity, that is what is the remaining balance on your account. (The Entitlements number is not associated with a specific controller.) Purchase the entitlements using a Capacity key. Entitlements indicate the total number of devices you are licensed to manage per your customer account. This total includes the controller and ExtremeCloud IQ Navigator and Pilot licenses. Each entitlement has a Start and End date.

To view the list of entitlements, go to **Administration** > **License** > **Entitlements**.

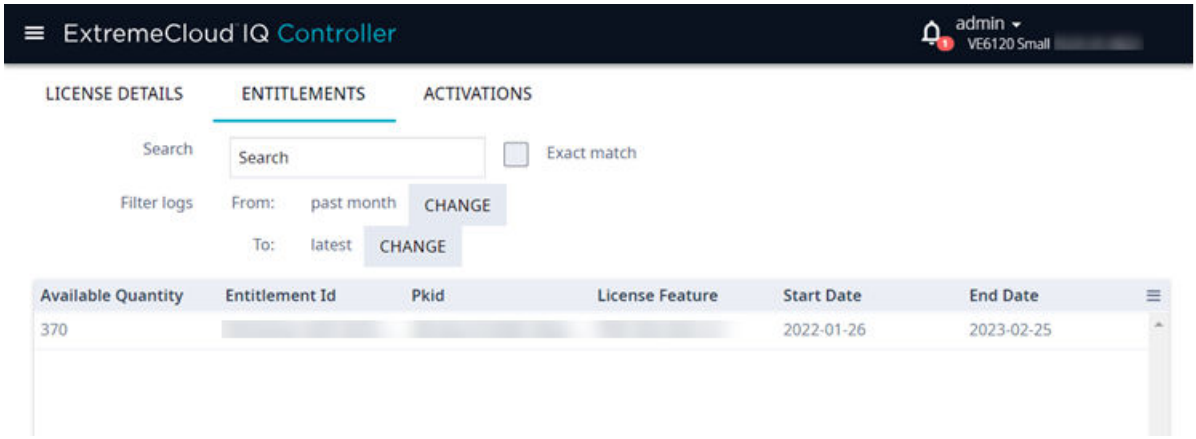


Figure 121: License Entitlements

Related Topics

Entitlement Health Checks on page 485
Activations on page 488
Product Subscription License on page 475

Activations

The ExtremeCloud IQ Controller **Activations** page displays a view of consumed entitlements or activations. Activations indicate the number of devices the specific appliance is actively managing. Each licensed activation has a Start and End date.

To view the list of activations, go to **Administration** > **License** > **Activations**.

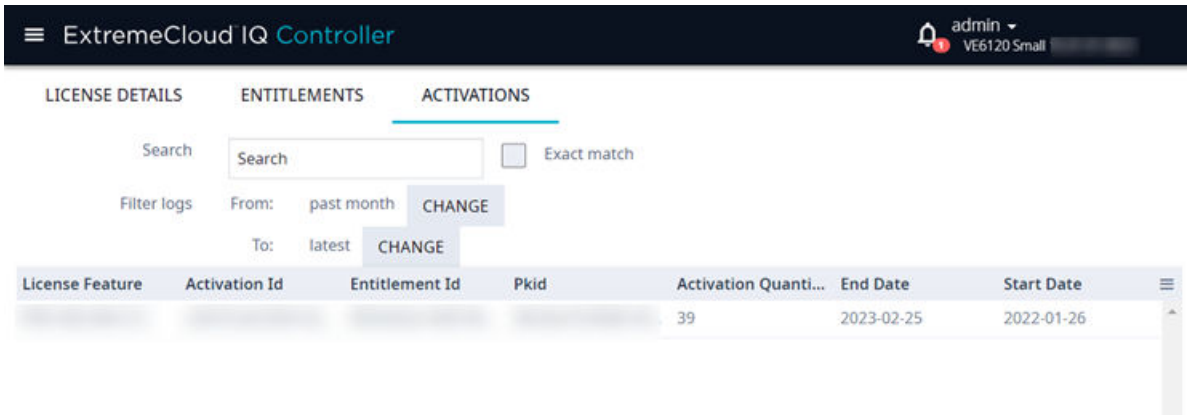
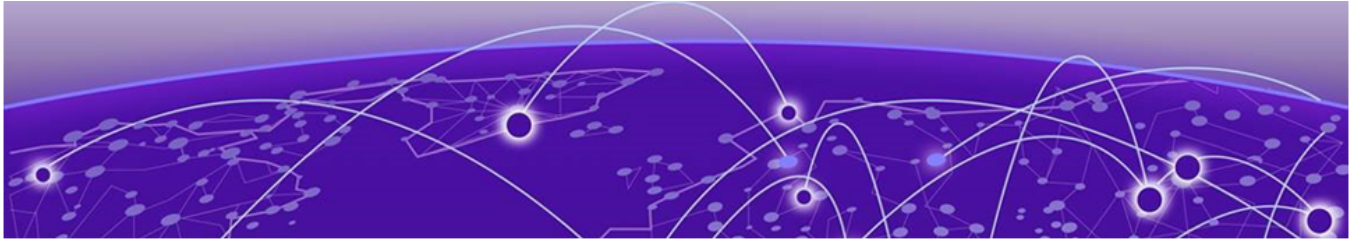


Figure 122: License Activations

Note
An access point must be assigned to a device group and site to be included in the list of Activations.

Related Topics

Generate and Install the Activation Package on page 478



Glossary

Chalet

Chalet is a web-based user interface for setting up and viewing information about a switch, removing the need to enter common commands individually in the CLI.

CLI

Command Line Interface. The CLI provides an environment to issue commands to monitor and manage switches and wireless appliances.

Extreme Defender for IoT

Extreme Defender for IoT provides unique in-line security for mission critical and/or vulnerable IoT devices. Placed between the IoT device and the network, the Defender for IoT solution helps secure and isolate IoT devices protecting them from internal and external hacking attempts, viruses, malware and ransomware, DDoS attacks, and more. Designed to be simple and flexible, Defender for IoT can be deployed over any network infrastructure to enable secure IoT management without significant network changes.

The solution is comprised of the Extreme Defender Application Software and the Defender Adapter (SA201) or AP3912i access point. ExtremeCloud IQ Controller is the supported platform for the Extreme Defender Application.

For more information, see https://www.extremenetworks.com/product/extreme-defender-for-iot/.

ExtremeAnalytics for ExtremeCloud IQ - Site Engine

ExtremeAnalytics™ for ExtremeCloud™ IQ - Site Engine, formerly Purview™, is a network powered application analytics and optimization solution that captures and analyzes context-based application traffic to deliver meaningful intelligence about applications, users, locations, and devices. ExtremeAnalytics for ExtremeCloud IQ - Site Engine provides data to show how applications are being used. This can be used to better understand customer behavior on the network, identify the level of user engagement, and assure business application delivery to optimize the user experience. The software also provides visibility into network and application performance allowing IT to pinpoint and resolve performance issues in the infrastructure whether they are caused by the network, application, or server. Learn more at https://www.extremenetworks.com/product/extremeanalytics-for-extremecloud-iq-site-engine/.

ExtremeCloud IQ Controller

Extreme Campus Controller has been rebranded to ExtremeCloud IQ Controller. The new ExtremeCloud IQ Controller supports Campus/Centralized sites only.

The ExtremeCloud IQ Controller is a next generation orchestration application offering all the mobility services required for modern unified access deployments offering simplified integration with ExtremeCloud IQ to take advantage of Cloud Visibility into the network. The ExtremeCloud IQ Controller extends the simplified workflows of the ExtremeCloud public cloud application to on-prem/private cloud deployments.

The ExtremeCloud IQ Controller includes comprehensive critical network services for wireless and wired connectivity, wireless device secure onboarding, distributed and centralized data paths, role-based access control through the Application Layer, integrated location services, and IoT device onboarding through a single platform.

Built on architecture with the latest technology, the embedded operating system supports application containers that enable future expansion of value added applications for the unified access edge.

ExtremeCloud IQ - Site Engine

ExtremeCloud™ IQ - Site Engine (formerly known as Extreme Management Center and Netsight), is a web-based control interface that provides centralized visibility into your network. ExtremeCloud IQ - Site Engine reaches beyond ports, VLANs, and SSIDs and provides detailed control of individual users, applications, and protocols. When coupled with wireless and Identity & Access Management products, ExtremeCloud IQ - Site Engine becomes the central location for monitoring and managing all the components in the infrastructure. Learn more at https://www.extremenetworks.com/product/extremecloud-iq-site-engine/.

ExtremeCloud™ IQ

ExtremeCloud™ IQ is an industry-leading and visionary approach to cloud-managed networking, built from the ground up to take full advantage of the Extreme Networks end-to-end networking solutions. ExtremeCloud IQ delivers unified, full-stack management of wireless access points, switches, and routers and enables onboarding, configuration, monitoring, troubleshooting, reporting, and more. Using innovative machine learning and artificial intelligence technologies, ExtremeCloud IQ analyzes and interprets millions of network and user data points, from the network edge to the data center, to power actionable business and IT insights, and deliver new levels of network automation and intelligence. Learn more about ExtremeCloud IQ at https://www.extremenetworks.com/support/documentation/extremecloud-iq/.

ExtremeControl for ExtremeCloud IQ - Site Engine

ExtremeControl for ExtremeCloud™ IQ - Site Engine, formerly Extreme Access Control™ (EAC), is a set of management software tools that use information gathered by a hardware engine to control policy to all devices on the network. The software allows you to automate and secure access for all devices on the network from a central dashboard, making it easier to roll out security and identity policies across the wired and wireless network. Learn more at https://www.extremenetworks.com/product/extremecontrol-for-extremecloud-iq-site-engine/.

ExtremeSwitching

ExtremeSwitching is the family of products comprising different switch types: **Modular** (X8 and 8000 series [formerly BlackDiamond] and S and K series switches); **Stackable** (X-series and A, B, C, and 7100 series switches); **Standalone** (SSA, X430, and D, 200, 800,

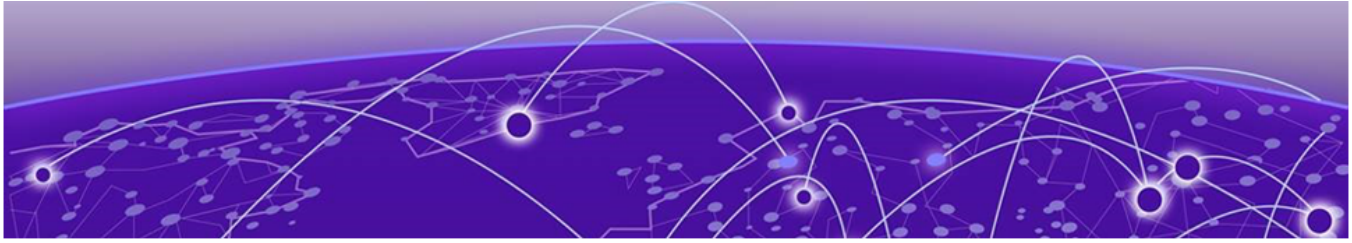
and ISW series); and **Mobile Backhaul** (E4G). Learn more about ExtremeSwitching at http://www.extremenetworks.com/products/switching-routing/.

ExtremeWireless

ExtremeWireless products and solutions offer high-density Wi-Fi access, connecting your organization with employees, partners, and customers everywhere they go. The family of wireless products and solutions includes APs, wireless appliances, and software. Learn more about ExtremeWireless at http://www.extremenetworks.com/products/wireless/.

ExtremeXOS

ExtremeXOS, a modular switch operating system, is designed from the ground up to meet the needs of large cloud and private data centers, service providers, converged enterprise edge networks, and everything in between. Based on a resilient architecture and protocols, ExtremeXOS supports network virtualization and standards-based SDN capabilities like VXLAN gateway and OpenStack Cloud orchestration. ExtremeXOS also supports comprehensive role-based policy.



Index

Numerics

A

B

C

D

E

F

G

H

I

L

M

N

O

P

Q

R

S

T

U

V

W