ExtremeCloud Appliance User Guide

Version 4.76.02

Table of Contents

Preface

This section describes the text conventions used in this document, where you can find additional information, and how you can provide feedback to us.

Conventions

This section discusses the conventions used in this guide.

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

Table 3: Command syntax

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

Documentation and Training

Find Extreme Networks product information at the following locations:

Current Product Documentation
Release Notes
Hardware/software compatibility matrices for Campus and Edge products
Supported transceivers and cables for Data Center products
Other resources, like 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/.

Providing Feedback

The Information Development team at Extreme Networks has made every effort to ensure the accuracy and completeness of this document. We are always striving to improve our documentation and help you work better, 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 in the document.
- Broken links or usability issues.

If you would like to provide feedback, you can do so in three ways:

- In a web browser, select the feedback icon and complete the online feedback form.
- 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.

Getting Help

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 2826. 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 Service Notifications

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

1. Go to www.extremenetworks.com/support/service-notification-form.
2. Complete the form (all fields are required).
3. Select the products for which you would like to receive notifications.

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

4. Select **Submit**.

AP Regulatory Information

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

Welcome to ExtremeCloud Appliance

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

- Integrated Access Control
- Integrated Maps
- Historical data charts
- Programmable REST API
- On-premise standalone deployment with integration into Extreme Management Center and on-premise services
- Clustered support for load sharing and resilience.

> **Note**
> ExtremeCloud Appliance v4.76.02 provides upgrade support for both Centralized and Distributed sites. For new installations of ExtremeCloud Appliance v4.76.xx, only Centralized sites are supported. In addition, support for AP4xx is limited to Centralized sites only.

The Appliance

The appliance is a network device designed to integrate with an existing wired Local Area Network (LAN). The ExtremeCloud Appliance provides both distributed and 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 distributed or 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 Appliance supports the use of both a virtual appliance and a physical appliance.

Related Topics

Appliance Product Family on page 12

Appliance Product Family

ExtremeCloud Appliance supports the following virtual appliances:

- VE6120
- VE6120H for Microsoft Hyper-V
- VE6125

And the following hardware appliances:

- E1120
- E2120
- E3120

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 in both a Centralized and a Distributed site. Support is determined by the site type at discovery and registration.

- AP505i
- AP510i/e
- AP560i/h

The following ExtremeWireless™ access points are supported in a **Centralized** site:

- AP410i/e
- AP460i/e
- AP3917i/e/k
- AP3916ic
- AP3915i/e
- AP3912i
- AP3935i/e
- AP3965i/e

The following ExtremeWireless WiNG™ access points are supported in a **Distributed** site:

- AP7522
- AP7532

- AP7562
- AP7612
- AP7632
- AP7662
- AP8432
- AP8533

The Extreme Networks® Defender Adapter SA201 is supported.

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

For a Centralized site using AP39xx, AP4xx, or AP5xx access points, a UDP-based protocol enables communication between an AP and ExtremeCloud Appliance. 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.

For a Distributed site using AP76xx, AP8xxx, or AP5xx access points, the communication is handled through the WebSocket protocol for configuration and through HTTPS POSTs for statistical data.

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 Appliance 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, and define the AP platforms available to the site by selecting the site configuration, either **Distributed** or **Centralized**.

A site in ExtremeCloud Appliance 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 Centralized site can include multiple device groups all in a single RF domain, or multiple device groups, each group in a unique RF domain. A Distributed site can only have a single 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

A Centralized configuration uses ExtremeWireless AP models AP39xx, AP4xx, and AP5xx. Each Wireless AP opens an IPSec tunnel to ExtremeCloud Appliance, and the Session Manager and RF Management policy run on ExtremeCloud Appliance.

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 Appliance performs as the management server and the session manager. The RF domain manager resides locally on ExtremeCloud Appliance.

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

- Bridged@AC (Tunneled for VLAN, attached at ExtremeCloud Appliance)
- Bridged@AP
- Fabric Attach (Bridge@AP with an I-SID mapping).

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

- AP505i
- AP510i/e
- AP560i/h

- AP410i/e
- AP460i/e
- AP3917i/e/k
- AP3916ic
- AP3915i/e
- AP3912i
- AP3935i/e
- AP3965i/e

Related Topics

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.

Distributed Site

A Distributed configuration uses ExtremeWireless WiNG APs. Each WiNG AP opens a WebSocket to ExtremeCloud Appliance and Session Manager and Smart RF Manager run on one of the APs in the site. All APs in a Distributed site have one RF Domain.

A Distributed site topology allows seamless roaming. Sites support multiple device groups with up to 200 APs associated with each site. With a Distributed site, ExtremeCloud Appliance performs as the management server, and one AP has the elected role of session manager and RF domain manager.

Network traffic is bridged locally at the AP, no traffic forwarding back to ExtremeCloud Appliance.

The Fabric Connect network is supported by the AP, and switches can be managed from ExtremeCloud Appliance over HTTP.

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

- AP505i
- AP510i/e
- AP560i/h

- AP7522
- AP7532
- AP7562
- AP7612
- AP7632
- AP7662
- AP8432
- AP8533

Use Case: Distributed Site

Scenario: A site offers remote clinics with 10 APs each. This requires consistent configuration across all clinics.

Solution: Create a separate site for each clinic location. Each site includes a unique device group. Create one profile configuration and share the configuration Profile for all sites and device groups. Each site represents a separate roaming domain using a single configuration Profile and a single RF Management Profile.

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 Appliance but not assigned to a device group have the status of *In-Service Trouble*. Devices that have not discovered ExtremeCloud Appliance have the status of *Unknown*.

Related Topics

Profiles

Configuration profiles in ExtremeCloud Appliance 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 single site or across multiple sites.

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 24 on page 85.

Figure 1 illustrates a single site, composed of multiple device groups, in different RF domains, using unique configuration Profiles. This model offers seamless roaming between APs of all device groups.
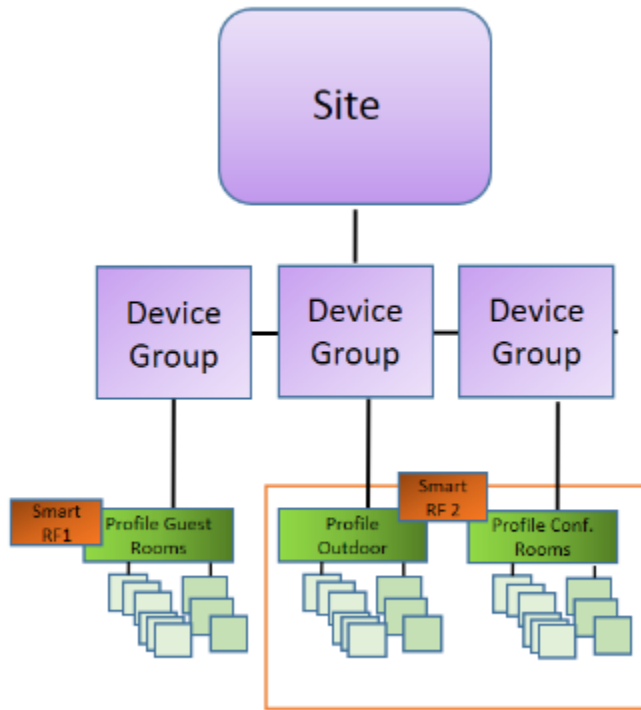
Figure 1: Centralized Site Data Model: Unique Profile Per Device Group

Figure 2 illustrates multiple sites with individual device groups, in one RF domain, sharing a common configuration Profile.
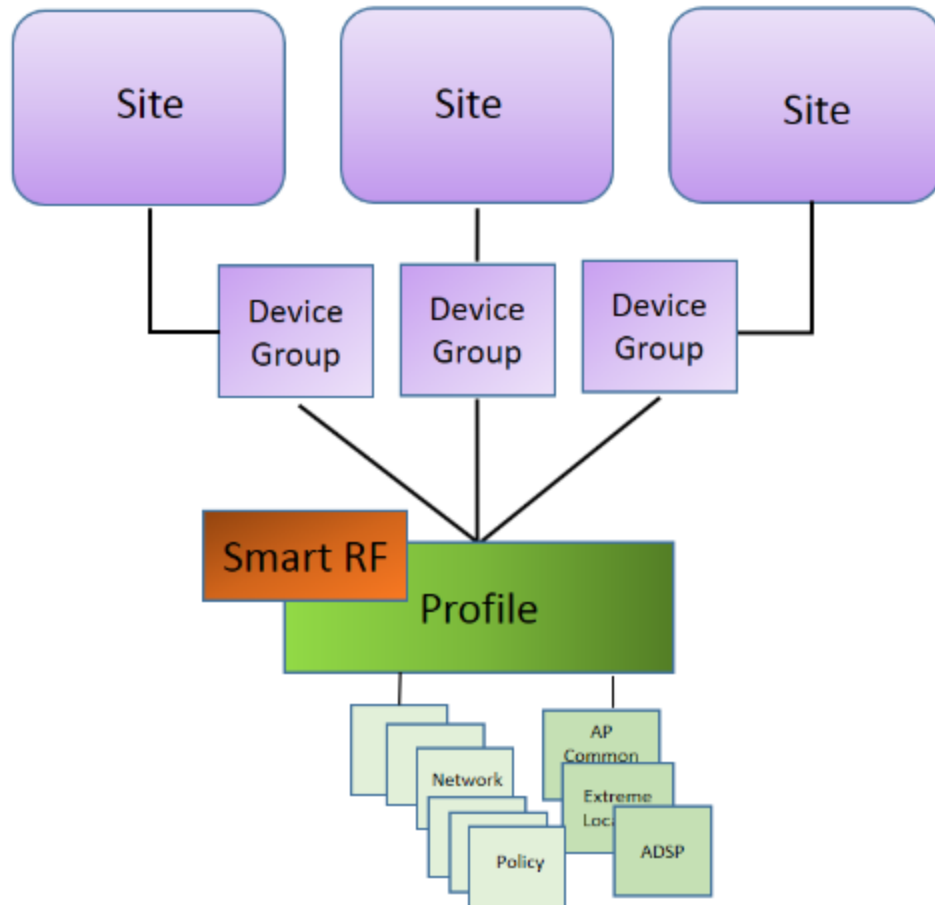
Figure 2: Distributed Site Data Model: One Shared Profile

Related Topics

> Add or Edit a Configuration Profile on page 84
> RF Management on page 18

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-WiFi 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-WiFi interference (noise), external WiFi 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.

Related Topics

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

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 Appliance 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.

Client Location Tracking is supported on AP39xx models only. 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.

* 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 Appliance 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.

> **Note**
> AP models AP76xx and AP8xxx support heat maps for Location Readiness but do not support Foot Traffic heat maps. Use ExtremeLocation integration for client tracking support with these APs.

Related Topics

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.
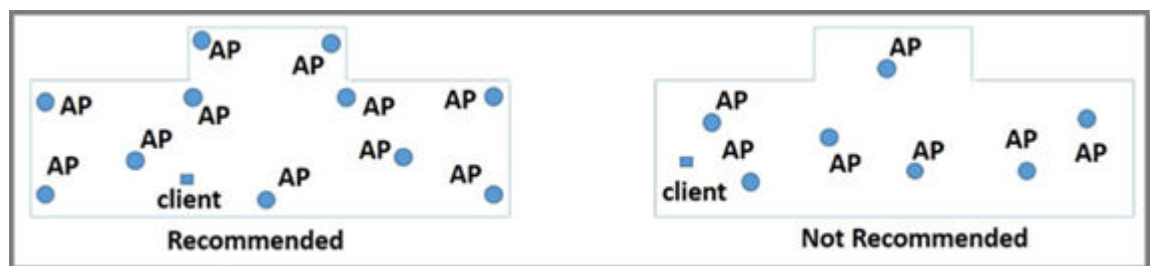
Figure 3: Recommended AP Placement

* 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

Floor Plan Limits

Table 4 outlines the floor plan limits for each type of ExtremeCloud Appliance.

Table 4: Floor Plan Limit per Appliance

Appliance	Maximum Floor Plan Limit	Maximum Number of APs Per Floor
E1120	50	500
E2120	400	1,000
E3120	1,000	1,000
VE6120	200	1,000
VE6120H	200	1,000
VE6125	400	1,000

Related Topics

Navigate the User Interface

The ExtremeCloud Appliance 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.

ExtremeCloud Appliance 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. Once the network is up and running, use the **Dashboard** and **Monitor** workbenches to monitor your network activity and performance.

The ExtremeCloud Appliance user interface can be accessed using the HTTPS protocol on the TCP port 5825. For example, if your ExtremeCloud Appliance 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.

ExtremeCloud Appliance 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 Appliance.

Onboard

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

Tools

Use Workflow, Logs, and diagnostic tools for network troubleshooting.

Administration

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

ExtremeCloud Appliance offers a context-sensitive Online Help system. Select the drop-down **admin** menu on any page to access the topic-based Help System.
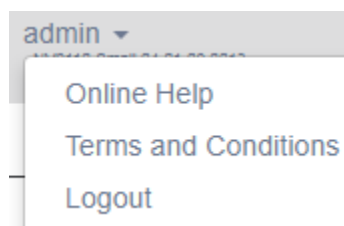
Figure 4: ExtremeCloud Appliance admin menu

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

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

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

Related Topics

Overview Dashboard on page 26

Search Facility

Each list page in ExtremeCloud Appliance 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 46

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.

You can also export the data to a csv file. 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 Appliance is installed.

For example, if ExtremeCloud Appliance 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 Appliance at 8:30 EDT, the Event Logs and Client Detail values show the time as 5:30.

Hierarchical Visibility for WiNG Appliances

ExtremeCloud Appliance offers unified visibility into Extreme Management Center for existing ExtremeWireless WiNG installations. This option extends the reporting and visibility capabilities of Extreme Management Center to ExtremeWireless WiNG accounts. This offers not only as an alternative to NSight, but supports unified wireless, wired infrastructure and expands other Extreme Networks software offerings, such as ExtremeAnalytics. If you are already leveraging NSight, this solution continues to support that investment. ExtremeCloud Appliance will relay statistics that feed into NSight to keep it's visibility value intact.

APs and appliances running ExtremeWireless WiNG version 5.9.1 or later are supported in this deployment strategy. ExtremeWireless WiNG APs are adopted by the WiNG appliance, and their configuration and statistics are fed through ExtremeCloud Appliance for presentation in Extreme Management Center or NSight.

The ExtremeCloud Appliance Statistics Proxy function leverages the ExtremeWireless WiNG stats connection that typically feeds NSight. The connection may already be in use if you are using the NSight product on the ExtremeWireless WiNG deployment. To support compatibility with the installed base, ExtremeCloud Appliance can relay the stats to feed the NSight (cluster).

You can opt to configure ExtremeCloud Appliance as an external NSight server for an ExtremeWireless WiNG controller or as an additional proxy server between ExtremeWireless WiNG and Extreme Management Center, with or without NSight. When using NSight, the NSight server displays stats from proxy APs along side other AP stats. The ExtremeCloud Appliance is completely transparent to NSight.

A proxy AP is an AP that has been adopted by an ExtremeWireless WiNG controller. The AP statistics and configuration are fed from the controller through ExtremeCloud Appliance for display in NSight. Proxy APs and their associated components are all marked as **Proxied** in the ExtremeCloud Appliance:

- **AP List** — APs that are adopted by an ExtremeWireless WiNG controller are listed as Proxied on the ExtremeCloud Appliance **AP** page.
- **Site List** — RF domains associated with the proxy AP are listed as Proxied on the ExtremeCloud Appliance **Sites** page. The Country designation for a site is derived from the AP RF domain. When there are no APs assigned to an RF domain, the Country designation for the site is "Demo Country".
- **Networks List** — Networks associated with the proxy AP are listed as Proxied on the ExtremeCloud Appliance **Networks** page, and a proxy network displays the network name, SSID, privacy/encryption and VLAN of the ExtremeWireless WiNG network. The default role is "Enterprise User" for a proxy network.
- **VLAN List** — VLANs associated with the proxy AP are listed as Proxied on the ExtremeCloud Appliance **VLAN** page. A proxy VLAN topology is always "Bridged at AP, tagged". If a network references a VLAN that is configured in ExtremeCloud Appliance, that existing VLAN is used by the proxy network.
- **Controller List** — ExtremeWireless WiNG proxy controllers configured for NSight are listed in ExtremeCloud Appliance under **Monitor** > **Devices** > **Controllers**. Proxied controllers can be removed from the **Controllers** page. However, if the ExtremeWireless WiNG controller has ExtremeCloud Appliance in its configuration, the ExtremeWireless WiNG controller displays in the list of controllers after each update. Proxy controllers cannot be edited.

All relevant information and statistics for a proxy AP displays in ExtremeCloud Appliance. However, editing and troubleshooting are not available in ExtremeCloud Appliance for a proxy AP or its associated: site, network, or VLAN.

> **Note**
> A proxy AP and its associated components can be removed from the ExtremeCloud Appliance. However, as long as the AP is adopted by the ExtremeWireless WiNG controller, the AP, site, network, and VLAN are re-created each time the controller sends an update to ExtremeCloud Appliance.

APs that are adopted by an ExtremeWireless WiNG controller continue to provide data to ExtremeWireless WiNG wizards and dashboards, as well as feed data to ExtremeCloud Appliance.

For information about the deployment strategy and configuration of the ExtremeCloud Appliance statistics proxy functionality, see the *ExtremeCloud Appliance Deployment Guide*.

Related Topics

Dashboard

Overview Dashboard

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

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.

Additionally:

- 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 data by radio band on each chart, individually. Click to show radio band filters on each chart. Then select the 2.4GHz or 5GHz radio button to display data for that band.

> **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.
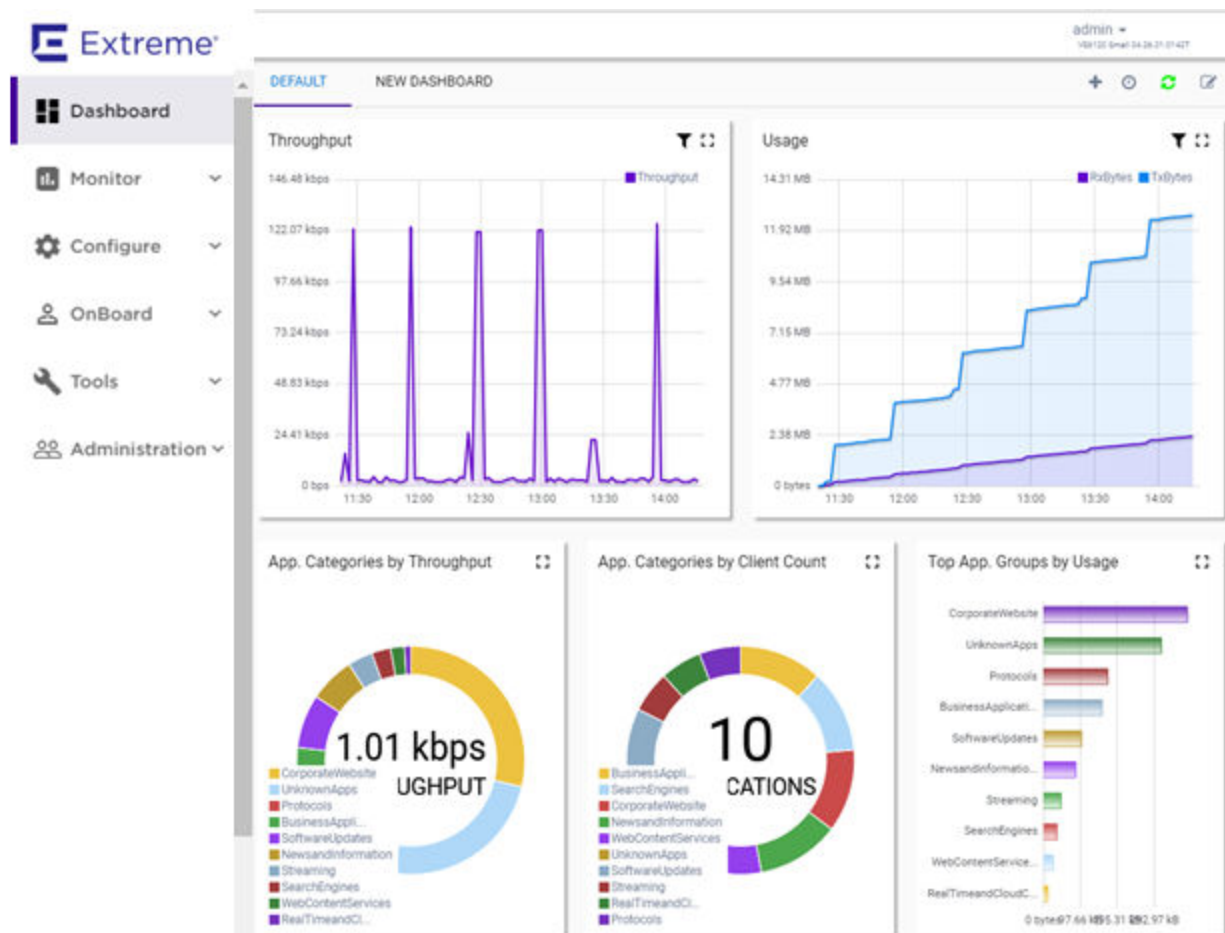
Figure 5: Main Dashboard

Related Topics

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 allows you to display up to 10 widgets.
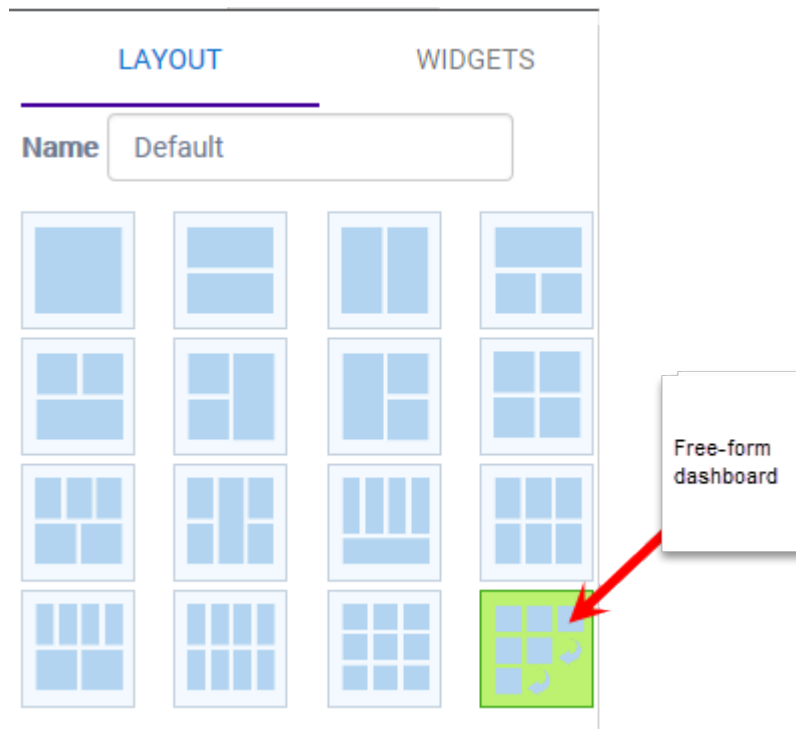
Figure 6: Widget Layout Options

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.
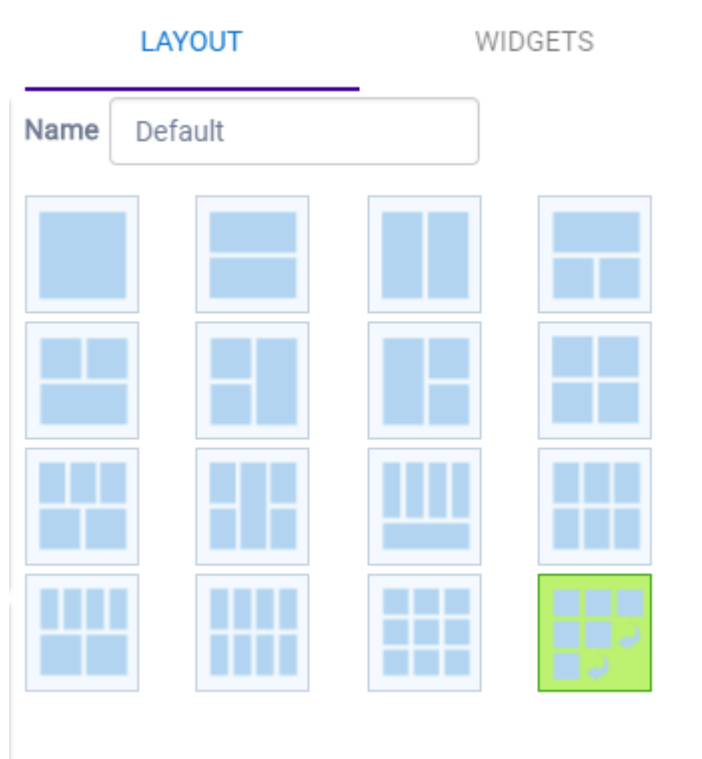
Figure 7: Dashboard - Edit Mode

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.

   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.

4. Click **Save**.

Availability Link Status

Once an Availability Pair is configured, the synchronization status between the paired appliances is displayed on the Dashboard Network Health chart. Table 5 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 5: 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

Monitor

Sites List

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

Related Topics

Site Dashboard

The Site Dashboard offers report information 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.)

Related Topics

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 6: Tabs on the Sites Screen

Tab	Description
Dashboard	Site dashboard that displays network metrics for the site.
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 132 • Radio Settings Button on page 33
Switches	List of switches associated with the site.
Clients	List of clients associated with the site.
Troubleshooting	Offers packet capture at the AP and remote console access to the AP.
Floor Plans	Floor plans associated with the site.
Smart RF	View widgets that show information about the following: • APs per Channel • Mitigation • Mitigation History

3. You can also:

   Select ✿ to modify configuration settings.

   Select ☰ to go back to the list.

Related Topics

Radio Settings Button

The following radio settings are available for 5GHz and 2.4GHz radios.

Table 7: Radio Settings

Field	Description
Set Tx Power	
Channel Width	Determines the channel width used by the channel on the selected radio. Available options include: • 20 MHz • 40 MHz • 80 MHz (supported on 5GHz only 802.11ac and 802.11ax) • 160 MHz (supported on 5GHz only 802.11ax) • Automatic – Channel width is calculated automatically. This is the default value.
Channel	Select from the list of available channels.
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 (supported on 5GHz only 802.11ax) • Automatic – Channel width is calculated automatically. This is the default value.
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. Once an AP has selected a channel, it remains operating on that channel until the user changes the channel or triggers ACS.

Floor Plan View

Once 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 click 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 34

Floor Plans on page 19

Configuring a Floor Plan on page 120

Viewing a Floor Plan

Once 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 8: Device Status from the Floor Plans View

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

Table 8: 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 122.
	Sensor device
	Switch
	Camera AP displayed as circular icon.
	Extreme Defender Adapter
	Ceiling-Mounted AP
	Wall-Mounted AP

Related Topics

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 Table 31 on page 103.

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. Click ⩦ to display filter options. Filter the floor map by AP attributes to focus on network attributes that need attention.
- Options. Click ⚙ 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

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.
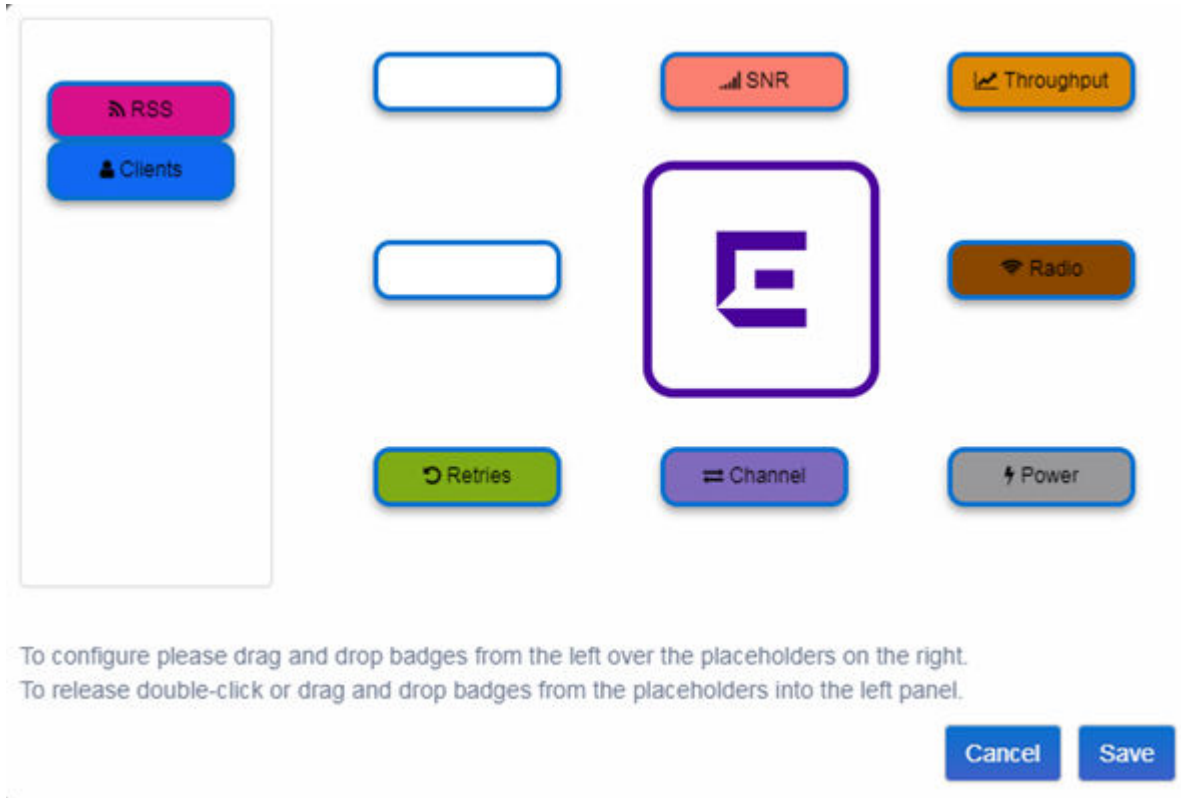
Figure 8: Badge Configuration Dialog

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

Related Topics

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.
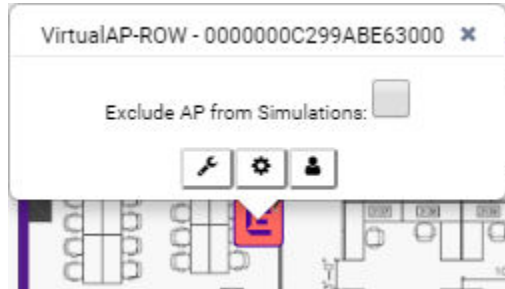
Figure 9: Device Context Menu

Related Topics

> Network Snapshot: AP Dashboard on page 54

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 ⚏.
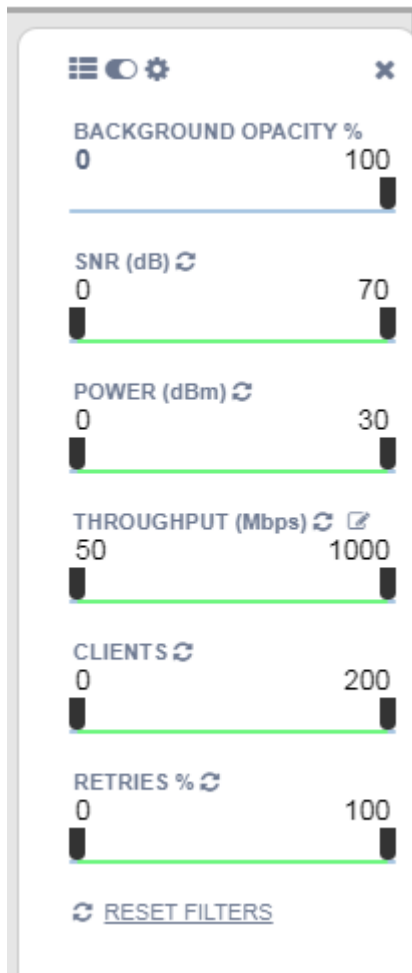
Figure 10: Map Filters Panel

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.
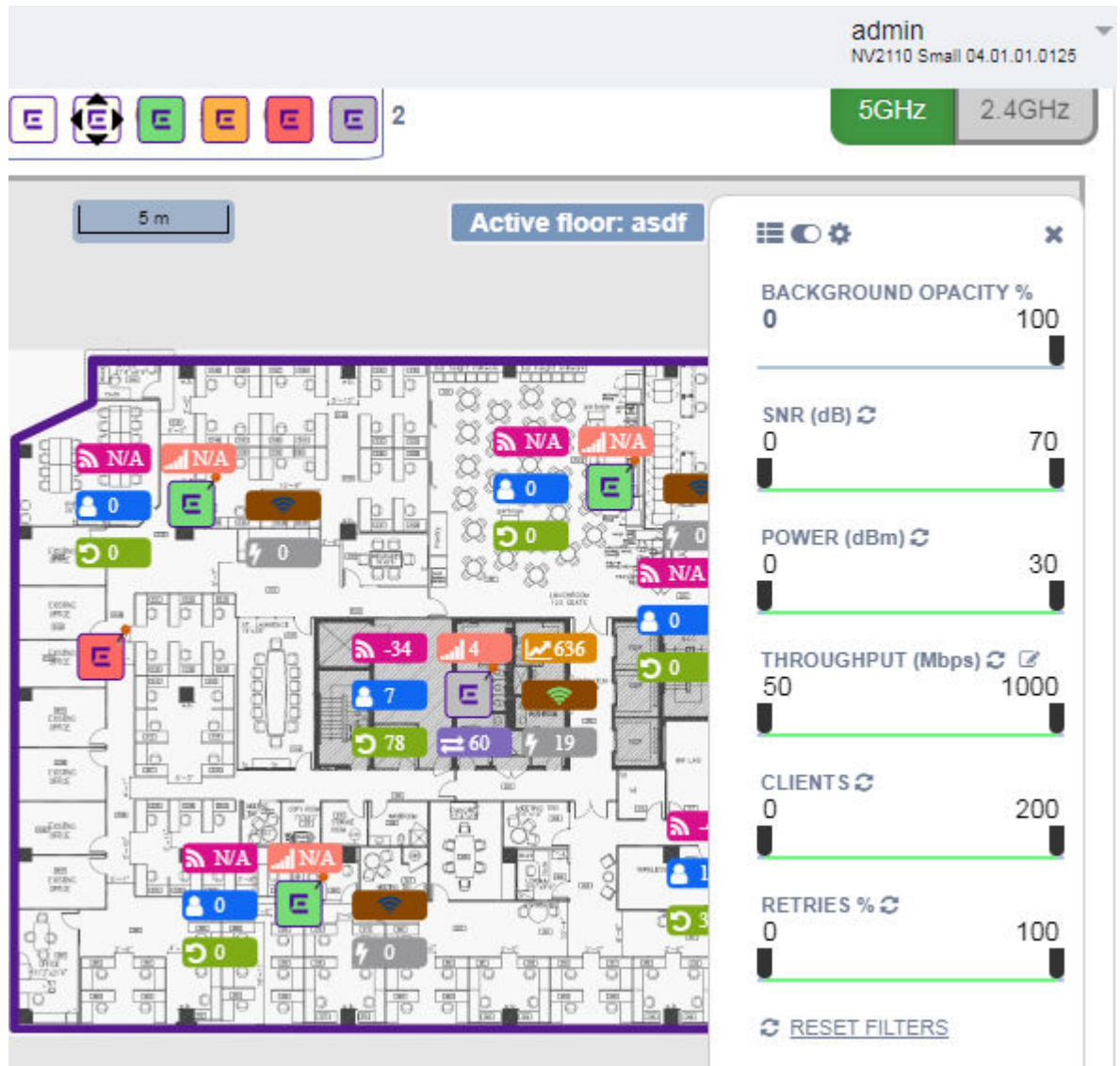
Figure 11: Badges that meet filter criteria appear on map

Understanding Readiness Maps

ExtremeCloud Appliance **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 allows 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, click **Maps** to display a list of map types.
2. To activate a map, click the ball and drag to the right.
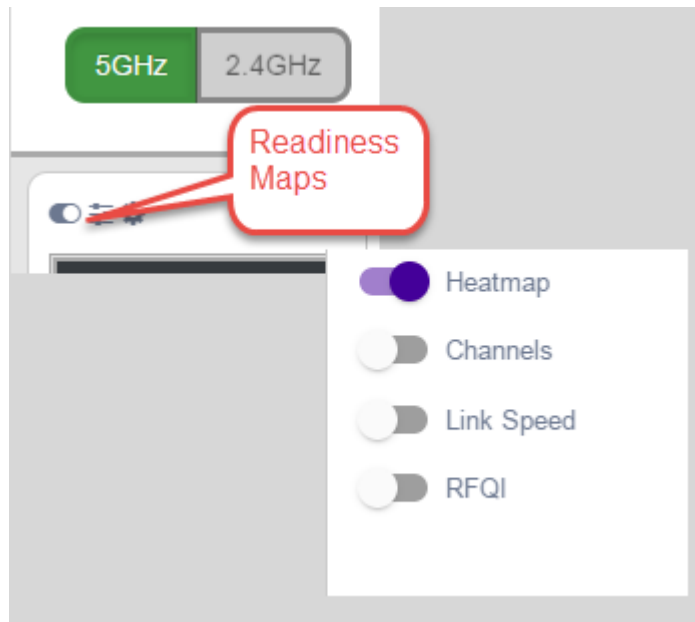
Figure 12: Network Readiness Maps

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

Figure 13: 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. Click **Select All**.
2. Right-click on the AP that you *don't* want.
3. Click **Exclude AP from Simulations**.

If you only want one AP selected:

1. Click **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

ExtremeCloud Appliance **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).

  Manage Location Tracking with AP76xx and AP8xxx using ExtremeLocation. For more information, see ExtremeLocation Profile Settings on page 102.

To access the Positioning maps from the floor plan view:

1. Display an available floor plan.
2. From the right panel, click **Positioning**.
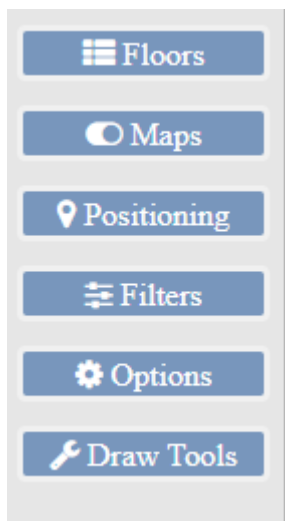
3. To activate a map, click the ball and drag to the right.
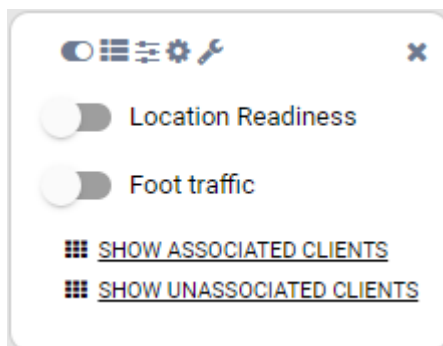
4. To show clients, select either **Show Associated Clients** or **Show Unassociated Clients**.

   > **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 40

Device List

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

- See Access Points List on page 44 for a list of supported APs.

- See the ExtremeCloud Appliance Release Notes for a list of supported switches.

- ExtremeCloud Appliance 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: https://extremenetworks.com/documentation/defender-application.

Related Topics

Access Points List

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

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.

The **Country** option on the site must support the AP licensing domain, and the site configuration type must support the AP model.

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.

- ⁂ indicates which AP in a Distributed site acts as the domain manager (RFDM). The RFDM communicates directly with ExtremeCloud Appliance collecting statistics, access point upgrade information, and Smart-RF activities. Understanding which AP is the RFDM can help with troubleshooting.

- 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** and **Radio 2 Clients** columns indicate the client count on each radio. This information allows 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 92.

- The **Adoption** column indicates if the AP is associated with the Primary or Backup ExtremeCloud Appliance 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 **Proxied** column indicates that the AP is associated with an ExtremeWireless WiNG controller. For more information, see Hierarchical Visibility for WiNG Appliances on page 24.

- The **Override** column indicates that the AP has overrides. To view which override settings are enabled, select the AP and go to **Advanced** > **Overrides**.

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

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

You can also select ♻ to manually refresh the page anytime.

The following ExtremeWireless™ access points are supported in both a Centralized and Distributed site:

- AP505i
- AP510i/e
- AP560i/h

The following ExtremeWireless™ access points are supported in a **Centralized** site:

- AP410i/e
- AP460i/e
- AP3917i/e/k
- AP3916ic
- AP3915i/e
- AP3912i
- AP3935i/e
- AP3965i/e

The following ExtremeWireless WiNG™ access points are supported in a **Distributed** site:

- AP7522
- AP7532
- AP7562
- AP7612
- AP7632
- AP7662
- AP8432
- AP8533

The Extreme Networks Defender Adapter SA201 is supported.

Note

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

Related Topics

Understanding Access Point States

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

Table 9: AP State from the Device List

State	Description
🟢	In-Service. Device has discovered ExtremeCloud Appliance and is providing service.
✳	Indicates which AP in a Distributed site acts as the domain manager (RFDM). The RFDM communicates directly with ExtremeCloud Appliance 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 Appliance but it is not a member of a device group.
⚫	Unknown. Device is added to ExtremeCloud Appliance but the device has never discovered ExtremeCloud Appliance .
🟥	Critical. After being Active, Discovered, and On-boarded, associated device is no longer connected to ExtremeCloud Appliance.
🔵	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 Appliance but not assigned to a device group have the status of *In-Service Trouble*. Devices that have not discovered ExtremeCloud Appliance have the status of *Unknown*.

*NEW!**Query Builder*

You can build customized queries to filter data on the **AP List** and **Client List** pages and view results in pie chart format. You can create custom filters with Query Builder, specifying criteria for each available column (regardless of whether it is selected for display) and viewing query results. For example, you can determine how many APs are on a given channel.

> **Note**
> For APs, both online and offline devices are supported in advanced search.

After you build and execute a query, the distribution rendered for visualization is limited to elements returned by the query. The most recent query is saved for each user between user logins. One query is saved for the AP List and one query is saved for the Client List. To create a new query, you must clear the current query in Query Builder.

Related Topics

Build a Query

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 ▼.

   Query Builder starts with a logical group of conditions. You can add more groups, joined with AND or OR. Select the relationship between your query conditions. Valid values are:

   - AND
   - OR

4. To add a condition, select **+ Condition**.

5. From **Source Field**, select a value that represents a column used in the query.

6. 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

7. 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.

8. To add another condition row, select **+ Condition**.

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

   The query is automatically saved. AP List queries are saved separately from Client List queries.

   Query Builder actions:

   - **Close**. Closes the Query Builder dialog. If you close Query Builder without running the query, your query details are deleted.
   - **Clear**. Deletes the query without closing Query Builder.
   - **Reset**. Closes the Query Builder dialog and saves the current query. The next time you open Query Builder, this query will display.
   - **Execute**. Runs the query and saves it.

   > **Note**
   > Query Builder generates a Pandas query syntax. The syntax preview is displayed at the top of the **Query Builder** dialog.

10. To visualize your query:

    a. Select ⬤.
    b. Select the column with the data element you want displayed.
    c. Select **Render**.
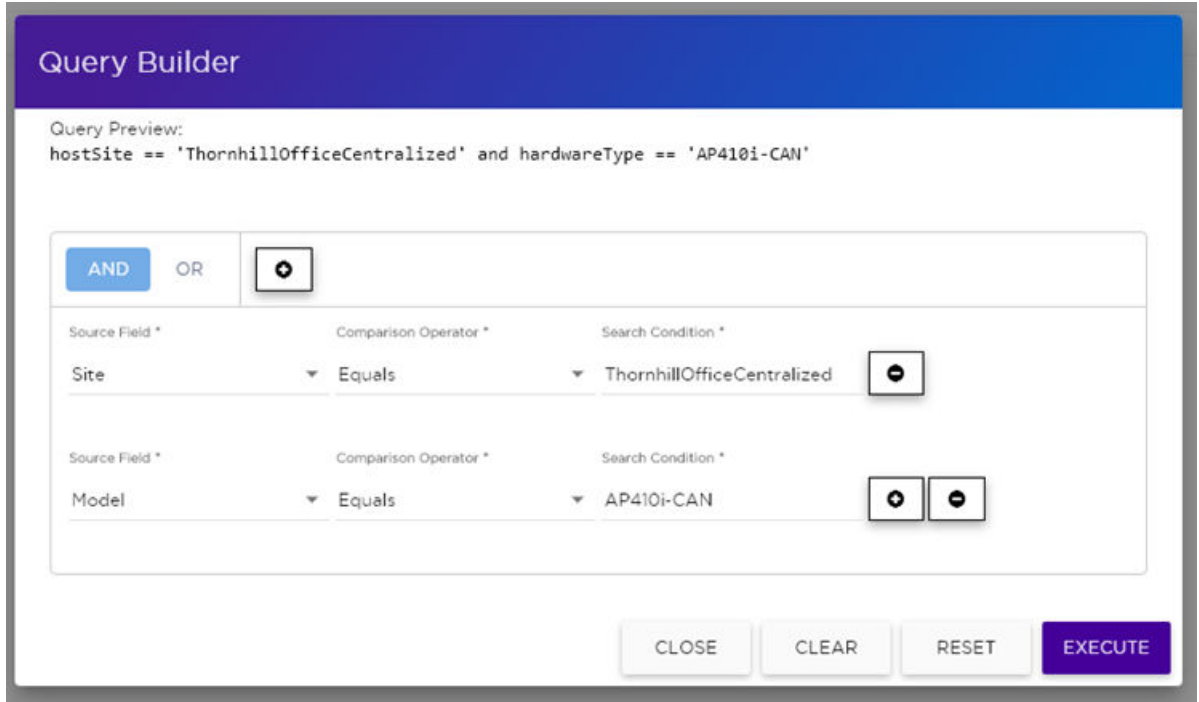
Figure 14: Query Builder: Channel distribution by AP model per site
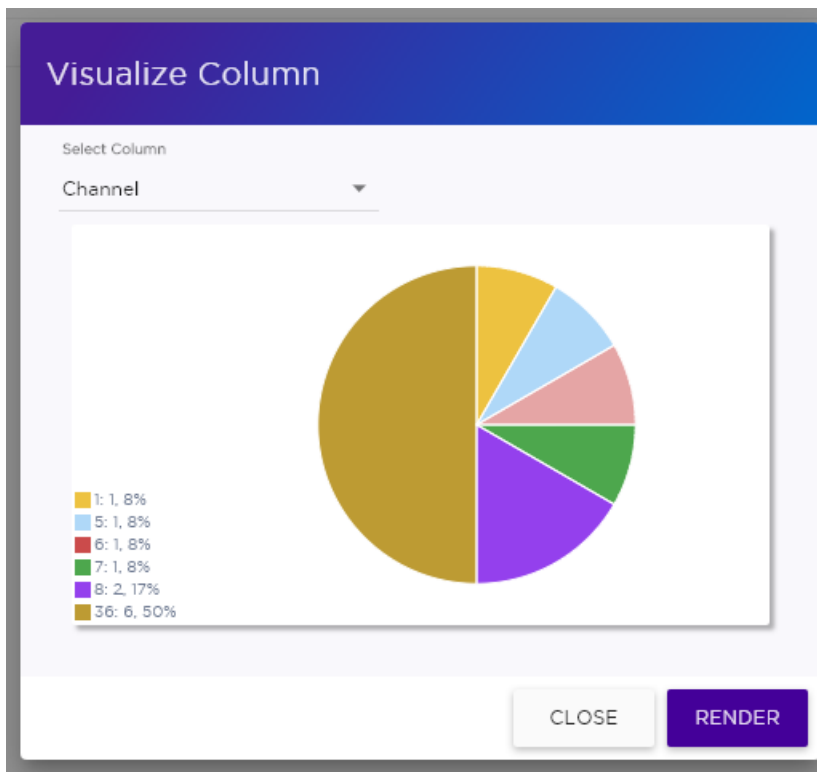
Figure 15: Channel Assignment for AP410i-CAN associated with Site Thornhill

The pie chart in Figure 15 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.
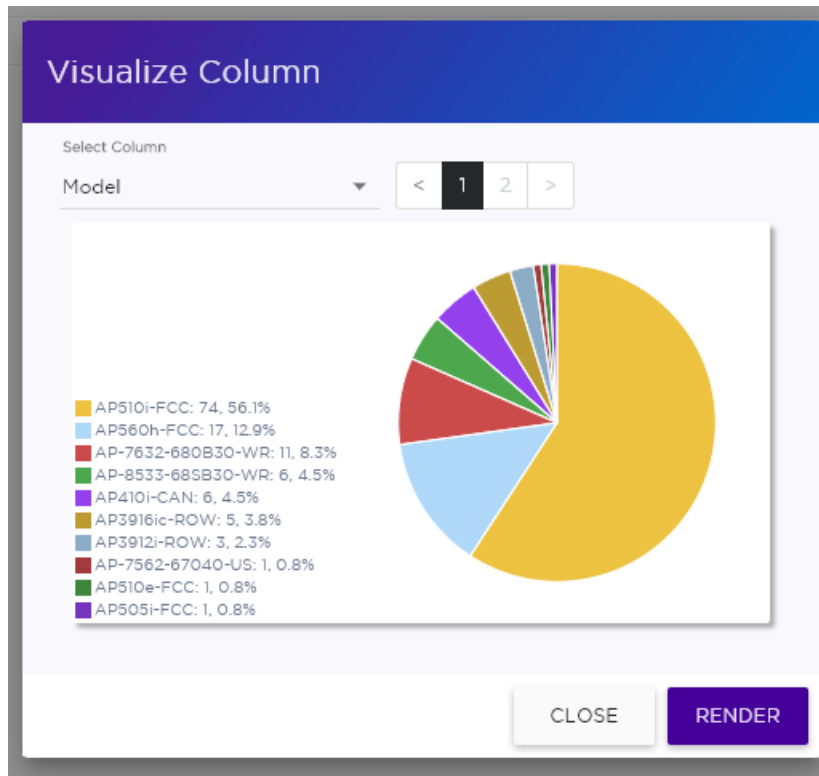
Figure 16: AP count by model number

Related Topics

> Query Builder on page 46

NEW! *Support for ExtremeWireless AP4xx Access Points*

ExtremeCloud Appliance supports ExtremeWireless™ AP410i/e and AP460i/e access points. The access points feature built-in dual-band radios, two band-locked radios, eight WiFi internal or external antennas, and one Bluetooth Low Energy (BLE) antenna. The AP410i/e can be mounted on a flat surface such as a wall, solid flat ceiling, and to a junction or gang box, and the AP can be installed on a suspended or drop ceiling. The AP460i/e can be mounted on a flat surface such as a wall or to a pole.

> **Note**
> AP410i/e and AP460i/e access points support is limited to Centralized sites.

The AP4xx series access points offer three radios:

- Radio 1 (2.4 GHz) — Network Assignment Service
- Radio 2 (5.0 GHz) — Network Assignment Service
- Radio 3 — Dedicated sensor

Related Topics

> Understand Radio Mode on page 90

Support for ExtremeWireless AP5xx Access Points

ExtremeCloud Appliance supports ExtremeWireless™ AP505i, AP510i/e, 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. Both Centralized and Distributed sites in an ExtremeCloud Appliance network support the 802.11ax ready access points. The site type support is determined at AP discovery and registration, and can be reset upon manual AP reset.

- 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
- 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) 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).

The AP560 is offered in a product bundle that targets the installation environment. Refer to Table 10 and Table 11 on page 53 for descriptions of each product bundle.

Table 10: 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 11: 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 ◦ Software Selectable Internal Antenna ◦ Overhead solution

Table 11: AP560h portfolio (continued)

AP Model Number	Description
	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 90

Radio as a Sensor on page 92

Professional Install Settings on page 140

Network Snapshot: AP Dashboard

To view network details from the AP screen:

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

   The **Access Points** list displays.

2. Select an AP.

   The network details for the selected AP appear. Details for a camera AP include the camera network address.

   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.

Table 12: 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.
Clients	List of clients associated with the AP. Add or remove clients from black and white lists.
Troubleshooting	Offers packet capture at the AP and remote console access to the AP.
Smart RF	View widgets that show information about the following: • Mitigation • Occupancy and neighbor channels • Peer AP visibility.

3. You can also:

   Select ✿ to modify configuration settings.

   Select ☰ to go back to the list.

Related Topics

AP Widgets

The following widget reports are available from the AP dashboard:

- 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, and signal to noise ratio (SNR) levels.

- 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 client:

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

Related Topics

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 Appliance 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 on AP39xx and (AP4xx and AP5xx Centralized Site) in addition to the saved file option. After starting Packet Capture, start Wireshark and add the remote interface using the ExtremeCloud Appliance management IP address. See the Wireshark documentation for details.

ExtremeCloud Appliance supports up to 10 simultaneous instances of packet capture. The maximum PCAP file size is 1GB, stored locally on appliances E1120, E2120, E3120, and VE6125. The virtual appliances VE6120 and VE6120H 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 Appliance in an Availability Pair. If the availability connection is disrupted, packet capture stops.

Continuous packet capture is supported on AP39xx and (AP4xx and AP5xx Centralized Site). 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.

With AP39xx and (AP4xx and AP5xx Centralized Site), once packet capture has started, you can change the capture parameters and refresh the capture, continuing to capture without interruption. This feature allows you to modify parameters as you monitor the capture process. There is one PCAP file for each packet capture instance.

Supported features depend on the AP model:
- ExtremeWireless AP39xx and (AP4xx and AP5xx Centralized Site) 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.
- ExtremeWireless WiNG and (AP5xx Distributed Site) models:
  - 1 IP filter can be applied
  - 1 MAC filter can be applied
  - Capture wired and wireless packets independently
  - Packet capture refresh is *not* supported
  - Live Packet Capture is *not* supported.

Related Topics

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 57

Packet Capture on page 55

Packet Capture Parameters

Field Name	Field Description
In the **Capture Locations** pane, configure the following settings:	
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.

Field Name	Field Description
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 Both** — Enable packet capture on both radio 1 and radio 2 interfaces of the AP. This option is selected by default. Note: AP39xx and AP5xx (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.	
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

Field Name	Field Description
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 and credentials for the remote server. • AWS — Provide the url and access keys to the Amazon S3 Cloud Server **Note:** Each capture instance is assigned one local file. All active capture instances must use the same scp server or AWS S3 destination.
Export	**Note:** Hover over the PAC file to download. Certain APs support capturing wired and wireless packets simultaneously.

Opening Live SSH Console to a Selected AP

ExtremeCloud Appliance 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:

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

Switches List

ExtremeCloud Appliance can manage a maximum of 1000 switches. In ExtremeCloud Appliance, 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 Appliance , 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

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

Table 13: 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 Appliance • Configuration is pending acknowledgment from switch • Switch reset pending • Switch reboot pending • Switch upgrade pending
●	Unknown. Switch has not discovered the ExtremeCloud Appliance.
■	Critical: • Switch stops sending requests for 5 minutes or longer • Consistent with a lost of connectivity to ExtremeCloud Appliance

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.

Table 14: 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.

Table 14: Tabs on the Switch Details Screen (continued)

Tab	Description
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.
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

Switch Widgets on page 61

Ports List on page 62

LAG Ports on page 62

Traces on page 62

VLANS on page 63

Troubleshoot a Switch Using the CLI on page 63

Configure a Switch on page 148

Switch Port Configuration on page 149

Port Dashboard on page 62

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

Ports List

A list of configured ports on the selected switch.

Related Topics

Port Dashboard on page 62

Switch Port Configuration on page 149

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 149

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 149

Traces

Trace information related to the selected switch.

Troubleshoot a Switch Using the CLI

ExtremeCloud Appliance 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 Appliance remote console to a switch *does not* support 200 Series switches.

You can initiate remote console to a switch from any ExtremeCloud Appliance in an availability pair. A switch deployed in a remote office behind a firewall or Network Address Translation (NAT) is reachable from the ExtremeCloud Appliance 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 152.

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 Appliance 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 Appliance cannot access the **Troubleshooting** tab.
- Modifications made during the CLI diagnostics session are not preserved on ExtremeCloud Appliance.
- 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 152
Advanced Switch Settings on page 151
Switch Configuration Backup Files on page 153

VLANS

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

Related Topics

VLANS on page 181

Controllers List

ExtremeCloud Appliance offers ExtremeWireless WiNG appliance users access to NSight by providing support for the ExtremeWireless WiNG infrastructure and acting as an NSight server.

ExtremeWireless WiNG proxy controllers configured for NSight are listed in ExtremeCloud Appliance under **Monitor** > **Devices** > **Controllers**. Proxied controllers can be removed from the **Controllers** page. However, if the ExtremeWireless WiNG controller has ExtremeCloud Appliance in its configuration, the ExtremeWireless WiNG controller displays in the list of controllers after each update. Proxy controllers cannot be edited.

Networks List

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

Related Topics

Network Snapshot: Network Dashboard on page 64
Network Widgets on page 65

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 appear.

Table 15: 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 black and white lists directly from this client list.

3. You can also:

   Select ✿ to modify configuration settings.

   Select ☰ to go back to the list.

Related Topics

Network Widgets on page 65

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 the **Name** and **Serial Number** for the selected AP, select a node.
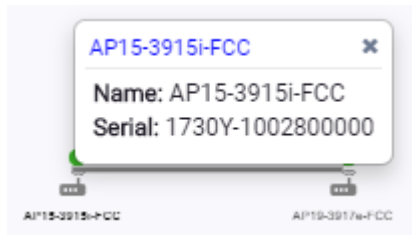
Figure 17: Mesh Node Details

- To display **Link Information**, select the line connecting the nodes.
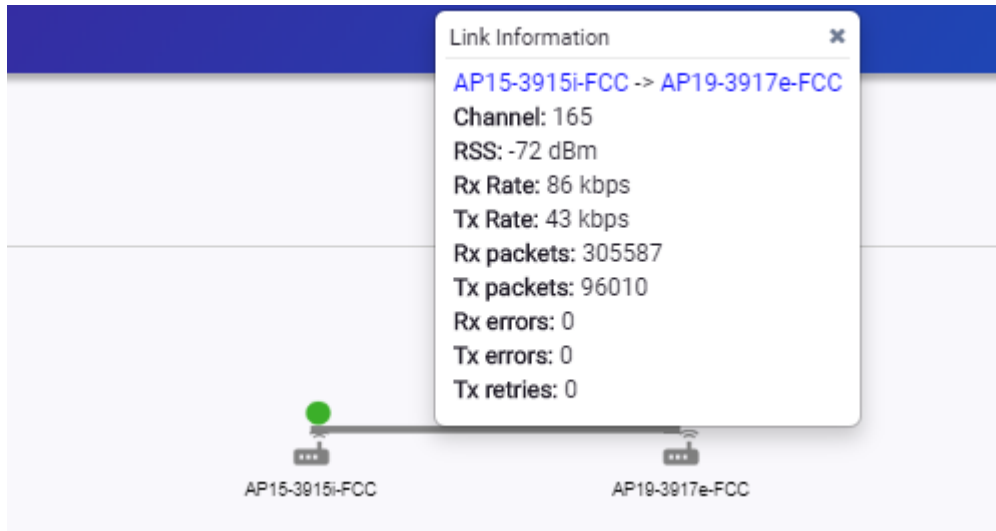
Figure 18: Mesh Link Information

- ◦ Channel
- ◦ RSS dBm
- ◦ RSSI
- ◦ Rx Rate kbps
- ◦ Tx Rate kbps
- ◦ Rx Packets
- ◦ Tx Packets
- ◦ Rx Errors
- ◦ Tx Errors
- ◦ Tx Retries

Move around the diagram using the following tools:

- Navigate the network diagram using the arrow buttons.

Figure 19: Navigation Buttons

- Zoom in and out using the zoom buttons.

Figure 20: Zoom Buttons

- To center the diagram, select ⊗.

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

Related Topics

ExtremeWireless WiNG AP Show Commands

Additional detail is available for ExtremeWireless WiNG access point models.

The following reports can be obtained through the ExtremeWireless WiNG AP CLI:

Table 16: WiNG Access Point CLI Commands

Command	Description
`show wireless meshpoint neighbor detail`	Displays the Neighbor table.
`show wireless meshpoint neighbor statistics rf`	Displays the signal level from each neighbor.
`show wireless meshpoint path detail`	Displays the Path table.
`show wireless meshpoint root detail`	Displays the Root table.
`show wireless meshpoint security detail`	Displays the link security to each neighbor.
`show wireless meshpoint proxy detail`	Displays the devices that are proxied by the AP.
`show wireless meshpoint`	Displays mesh point configuration and indicates if the AP is Root.
`show wireless meshpoint detail`	Displays additional mesh point configuration such as control and allowed VLANs.
`show wireless meshpoint config`	Indicates if the mesh point is enabled.
`show wireless meshpoint multicast detail`	Displays multicast subscribers on the AP.

For more information, see the **Show wireless meshpoint** commands in the *Wireless Controller, Service Platform and Access Point Reference Guide* at extremenetworks.com/documentation.

Related Topics

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 a black or white list.

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

Select a client to see client details.

Related Topics

Understanding Client Status

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

- Green — Clients with currently active sessions.
- Grey — 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:

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

You can also select ⟳ to manually refresh the page anytime.

Related Topics

Whitelisting and Blacklisting Clients

Clients on a black list are denied network access. Clients on a white 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 whitelist or blacklist the client.

> **Note**
> Configure one list that applies to all networks being broadcast by any AP managed by ExtremeCloud Appliance or by an ExtremeCloud Appliance availability pair. From the **Client List**, configure a black list or a white list, but not both. To filter specific users by MAC address, configure Access Control rules.

To set up a list:

1. Go to **Clients** and click the **Blacklist** icon.

    This displays the list **Mode** for your network and a list of MAC addresses.
2. Select **Whitelist** or **Blacklist**.

    The Mode you select will apply to your entire network.
3. To add MAC addresses to the list, click **Add** and enter a MAC address for the client.
4. To delete a MAC address from the list, select the list and click **Delete**.

Related Topics

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.
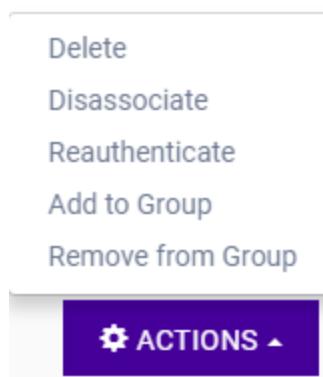
Figure 21: Client Actions Button

Table 17: 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 a blacklist or whitelist, 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 Appliance 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

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 appears.

Table 18: 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 19: 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 155 .
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 73

Station Events on page 72

Client Actions on page 69

Understanding Date and Time on page 23

Overview Dashboard on page 26

Floor Plans on page 19

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 20 are documented in alphabetical order.

Table 20: 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
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.

Table 20: End-System Event Fields (continued)

Field	Description
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 170

Access Control Rules on page 225

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 28

Modify a Dashboard on page 28

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 74

Configuring Roles on page 170

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 Appliance 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 (e.g., ARP, DHCP, and DNS) and HTTP to redirect web traffic for assisted remediation.

Related Topics

Preconfigured Policy Roles

ExtremeCloud Appliance is shipped a with the following default policy configurations listed in Table 21.

Policy roles define the authorization level that ExtremeCloud Appliance 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 21: 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.
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.

Table 21: Preconfigured Policy Roles (continued)

Role	Description
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

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

Rule-Level Statistics

ExtremeCloud Appliance 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 22: 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 23: Top Rules by Hit Count on the Roles Dashboard

Figure 24: 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 Appliance 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

Network Configuration Steps

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

> **Note**
> To ensure the devices discover ExtremeCloud Appliance, configure DHCP, NPS, and DNS Services for ExtremeCloud Appliance discovery. For more information, see the *ExtremeCloud Appliance Deployment Guide* located in the Extreme Networks documentation portal: https://extremenetworks.com/documentation/extremecloud-appliance.

> **Note**
> Users with Read-Only access to ExtremeCloud Appliance do not have access to the ExtremeCloud Appliance configuration options.

1. Create one or more sites.

    Define the site as Centralized or Distributed and select a Country for the site. These options affect the AP models and licensing domains 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 site definition: Centralized or Distributed and 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 172.

7. Install and add devices.

Access Points and switches are automatically added to an ExtremeCloud Appliance 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. Once 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 13

Adding Device Groups to a Site on page 83

WLAN Service Settings on page 155

Policy on page 170

Floor Plans on page 19

AAA RADIUS Authentication on page 194

Onboard AAA Authentication on page 200

Associated Profiles on page 172

Sites

Use sites to define boundaries for fast roaming and session mobility without interruption. Manage sites from **Configure** > **Sites**.

Related Topics

Sites Overview on page 13

Centralized Site on page 14

Distributed Site on page 15

Adding a Site on page 81

Site Dashboard on page 31

Modifying Site Configuration on page 82

Site Location on page 83

Adding a Site

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

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

Related Topics

Site Parameters

Configure the following parameters for site configuration.

Table 22: Site Configuration Parameters

Field	Description
Name	Determines the name of the site.
Centralized	Specifies a Centralized Site.
Distributed	Specifies a Distributed 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

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 81
Floor Plans on page 19
Site Location on page 83
Device Groups on page 16
RADIUS Configuration for Switches Per Site on page 82
Advanced Tab on page 129

RADIUS Configuration for Switches Per Site

ExtremeCloud Appliance 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 195.

   Switches

   Check the switches that are associated with the site.

Related Topics

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
        ◦   Campus
    -   Map Coordinates. Select a location on the map to automatically populate the Map Coordinates field. You can also 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

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 16.

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 click **Add**.
3. Configure the device group settings.
4. Once device group is added, select **Save** on the **Site** page.

Related Topics

Device Group Parameters

Configure the following parameters:

Table 23: 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 click ⊙ to create a unique profile.
RF Management	The RF Management profile associated with the device group. ExtremeCloud Appliance includes a default RF policy. • If the site is Centralized, the device group is composed of APs that use Default ACS. • If the site is Distributed, the device group is composed of APs that use Default Smart RF. Select the default profile from the list or click ⊙ 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, click **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

ExtremeCloud Appliance 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 Appliance installation. After making changes, if you need to return to a base ExtremeCloud Appliance 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, select ⊕ to configure a new Profile or select ✎ to edit the Profile.
5. Configure the following parameters:

Table 24: 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. You can override the WLAN setting for one or more individual APs from the AP **Advanced** > **Overrides** dialog.
Mesh Points	Define mesh points for a wireless mesh network. ExtremeCloud Appliance allows one mesh point per radio. Therefore, each AP can have up to two assigned mesh points. You can assign one mesh point to both radios or assign a unique mesh point to each radio. For more information, see Mesh Point Configuration Profile Settings on page 87.
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 74 • Adding Policy Roles on page 171
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 90. For each radio band, select **Advanced** to configure Advanced AP Radio Settings.

Table 24: Profile Configuration Parameters (continued)

Field	Description
Wired Ports	If the AP supports wired ports, configure port speed for each port. Valid values are: • Auto • 100M • 10M
AirDefense	Select a configured air defense Profile. Or, Select ⊕ to add a new Profile. Select ◢ to edit the selected Profile.
ExtremeLocation	Select a configured ExtremeLocation 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 all APs except AP7612, AP3935, and AP3965.
Positioning	Select a configured Positioning Profile. Or, Select ⊕ to add a new Profile. Select ◢ to edit the selected Profile. **Note:** Supported on AP39xx and AP4xx in a Centralized site, and supported on AP5xx in both a Centralized and a Distributed site.
Analytics	Select a configured ExtremeAnalytics Profile. Or, Select ⊕ to add a new Profile. Select ◢ to edit the selected Profile. **Note:** Supported on AP39xx and AP4xx in a Centralized site, and supported on AP5xx in both a Centralized and a Distributed site.
RTLS	Select a configured RTLS Profile. Or, Select ⊕ to add a new Profile. Select ◢ to edit the selected Profile.

Related Topics

Mesh Point Configuration Profile Settings

Before you configure Mesh Point configuration Profile settings:

- Ensure that the APs are configured for mesh point. The following AP models support mesh point:
  - AP7xxx, AP8xxx
  - AP39xx (Limited to one mesh point)
- Configure the mesh point network. For more information, see Mesh Point Network Settings on page 162.

Configure mesh point configuration Profile settings for AP models that support mesh point. Configure one mesh point per radio. The total number of WLAN services on each radio, including the mesh point, cannot exceed eight.

> **Note**
>
> Configuration parameters you set here are for all APs in a device group. To override settings for specific AP radio, go to the AP radio properties. For more information, see Advanced Setting Overrides on page 136.

1. On the Profile **Mesh Points** tab, select a mesh network from the AP radio drop-down list.
2. Select **Advanced**.
3. Configure the following parameters:

Cost Root

Select this option to set the mesh point as the cost root for mesh point root selection. This setting is disabled by default. Considered specifying a cost root in a chain deployment, where wired and mesh connections are in sequence.

Cost root is the root AP, where calculation of cost starts. For example, in a chained deployment of three APs, we will assume each link costs 10. If the cost root is AP1, then the cost of reaching the core network would be 30. Generally, you specify the AP closest to core network as the cost root.

Exclude Wired Peer

Select this option to exclude wired peers when creating mesh links.

Root

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.

Monitor Primary Link

Enables monitoring of primary port backhaul link for this MeshConnex policy. If there is a primary port backhaul failure and the device is a mesh root, the device automatically changes to a non-

root device. When the primary port backhaul link becomes available again, the non-root device changes back to a root device.

Path Selection Method

Select the method used for path selection in a mesh network. Available options include:

- None – No criteria are used in root path selection.
- 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.
- Mobile-SNR-Leaf – The access point is mounted on a vehicle or a mobile platform (AP 7161 models only). The path to the route is selected based on the Signal To Noise Ratio (SNR) with the neighbor device.
- 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.

Hysteresis Minimum Threshold

Minimum SNR value to consider a candidate for the next hop in a dynamic mesh network. This field, along with Hysteresis Delta and Hysteresis Period, is used to dynamically select the next hop in a dynamic mesh network. The default setting is 0dB.

Preferred Neighbor

Specify the Interface ID of the neighbor's mesh radio.

Use this setting to bias a device using MCX mesh to utilize a specific neighbor when sending traffic. If a non-root AP has multiple neighbors each with a path back to a root AP, use this setting to determine the path back to the root AP.

Hysteresis Period

Enter the time duration in seconds (0 - 600) or minutes (0 - 10). This indicates the duration that a signal must sustain the constraints specified in the Hysteresis Minimum Threshold and Hysteresis Delta values. These values are used to dynamically select the next hop in a dynamic mesh network. The default setting is 1 second.

Hysteresis Delta

Enter a delta value in dBm. A candidate for selection as a next hop in a dynamic mesh network must have an SNR higher than the value configured here. This field, along with the **Hysteresis Minimum Threshold** and **Hysteresis Period**, is used to dynamically select the next hop in a dynamic mesh network. The default setting is 1dB.

SNR Delta

Select the root selection method hysteresis (from 1 - 100dBm) SNR delta range a candidate must sustain. The default setting is 1dBm.

Monitor Critical Resources

Select this option to enable critical resource monitoring for this mesh point.

Root Selection Method

Select a value to determine whether this mesh point is the root or non-root mesh point. Valid values are:

- **None**
- **Auto-Mint**

- **Auto-Proximity**

Preferred Band

Select the preferred radio band for this mesh point. Select None to set no preferences. The other radio band options are 2.4 GHz and 5 GHz.

When running mesh on multiple radios on one AP, MeshConnex automatically sends traffic over the radio that has the best path back to a mesh point root AP. Use this setting to specify a preferred radio interface, controlling which mesh actively forwards traffic.

Preferred Root

Enter the **Mesh Point ID** of the root APs mesh radio. Use this setting to balance the number of mesh points reporting to a specific root AP.

Related Topics

AP39xx Mesh Point Support

When using the AP39xx in a mesh network, all access points in the network must be one of the AP39xx models. Mesh deployments using AP39xx will not inter-operate with mesh deployment using other AP models.

The AP39xx use wireless beacons and WLANs as root devices. The AP39xx that do not serve as a root AP connect to the root AP as any mobile user device. The AP39xx supports only one mesh point per AP.

> **Note**
> Do not rename an AP39xx after it is added to a mesh network. Renaming the device affects the display of the reported statistics.

Table 25: AP39xx Mesh Point Support

Option	AP39xx Behavior
Mesh ID	Use the SSID of the AP39xx access point.
Root behavior	- When the AP39xx is a root AP, the Wireless Distribution System (WDS) service is the parent. - When the **Path Selection Method** is snr-leaf or mobile-snr-leaf, the WDS service is a child. - In all other cases, WDS service is both a parent and a child.
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

Related Topics

Understand Radio Mode

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

> **Note**
> Sensor converts the radio to a sensor for ADSP, ExtremeLocation, and Positioning. The AP4xx offers a separate sensor radio. For more information, see Radio as a Sensor on page 92.

Table 26: Radio Modes

AP Model	Radio 1	Radio 2	Radio 3	IoT Radio
AP410i/e	2.4GHz • b/g • g/n • b/g/n • g/n/ax	5GHz • a/n/ac • a/n/ac/ax	2.4GHz /5GHz (dual band) • sensor (non-configurable)	2.4GHz
AP460e	2.4GHz • b/g • g/n • b/g/n • g/n/ax	5GHz • a/n/ac • a/n/ac/ax	2.4GHz /5GHz (dual band) • sensor (non-configurable)	2.4GHz
AP505i	2.4GHz • sensor • b/g • g/n • b/g/n • g/n/ax	5GHz • sensor • a/n/ac • a/n/ac/ax		

Table 26: Radio Modes (continued)

AP Model	Radio 1	Radio 2	Radio 3	IoT Radio
AP510i/e	2.4GHz /5GHz (dual band) • sensor • b/g • g/n • b/g/n • a/n/ac • g/n/ax • a/n/ac/ax **Dual-Band Radios:** • 5GHz - Low scans channels in the range of 36-64. • 5GHz - High scans channels in the range of 100-165. If there are no channels in the range for a radio, no scan will occur.	5GHz • sensor • a/n/ac • a/n/ac/ax		
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 **Dual-Band Radios:** • 5GHz - Low scans channels in the range of 36-64. • 5GHz - High scans channels in the range of 100-165. If there are no channels in the range for a radio, no scan will occur.	5GHz • sensor • a/n/ac • a/n/ac/ax		
AP39xx	5GHz • sensor • a/n/ac • ac-strict	2.4GHz • sensor • b/g • g/n • b/g/n • g/n-strict		

Table 26: Radio Modes (continued)

AP Model	Radio 1	Radio 2	Radio 3	IoT Radio
AP75xx	2.4GHz • sensor • b/g • g/n • b/g/n	5GHz • sensor • a/n/ac		
AP76xx	2.4GHz • sensor • b/g • g/n • b/g/n	5GHz • sensor • a/n/ac		
AP84xx	2.4GHz • sensor • b/g • g/n • b/g/n	5GHz • sensor • a/n/ac		
AP85xx	2.4GHz • sensor • b/g • g/n • b/g/n	5GHz • sensor • a/n/ac		

Related Topics

Advanced AP Radio Settings on page 96

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, ExtremeLocation, and Positioning. ExtremeLocation and 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 ExtremeLocation and Positioning report the MAC addresses and RSS values that the radio receives.

ADSP is supported on all ExtremeCloud Appliance access points. On AP39xx and AP76xx, both radios must be configured as sensors at the same time. The AP4xx offers a separate sensor radio. A white LED indicates sensor activity. On the AP5xx and AP8xxx, 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 AP510 is a dual-band AP. A white LED indicates sensor selection. 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 93

Add or Edit a Configuration Profile on page 84

Advanced Configuration Profile Settings

From the **Edit Profile** page, select **Advanced** and configure the following parameters:

Table 27: Advanced Configuration Profile Settings

Field	Description
Band Steering	Band steering is intended to relieve congestion by encouraging dual-band client devices to use the higher capacity 5GHz band. To make use of Band Steering, ensure that networks are assigned to both radios. The system always enables both radios when Band Steering is enabled. For Band Steering to work effectively, configure similar coverage areas for the 2.4GHz and 5GHz bands. Design your network for both 5GHz and 2.4GHz coverage. For networks where coverage quality differs between bands, disable Band Steering. Enable or disable Band Steering for the entire device group or for a specific AP WLAN override.
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	**Note:** Supported on APs in a Centralized site and on AP5xx in a Distributed site. 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/HTTPtraffic works normally. • Control — An IPSEC tunnel is established from the AP to the appliance and all SFTP/SSH/HTTP/WASSP control traffic is encrypted. The AP skips the registration and authentication phases and when selected, the Secure Tunnel Lifetime feature can be configured. • 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/WASSPcontrol 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.
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.

Table 27: Advanced Configuration Profile Settings (continued)

Field	Description
Session Persistence	**Note:** Supported on APs in a Centralized site and on AP5xx in a Distributed site. 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 95.
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 Appliance on WLANs where ExtremeCloud Appliance is not required. You can also override the Mgmt VLAN ID for a specific AP from the **Advanced** > **Overrides** dialog for the selected AP.
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 device group setting for one or more 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. You can override the device group setting for one or more individual APs from the **Advanced** > **Overrides** dialog for the selected AP.

Scan Mode	**Note:** Supported on AP4xx and AP5xx models only.
	
	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 2.4G (AP510i/e includes 5G channels).
	   ◦ Radio 2 channels are 5G.

Channels	Select channels for a custom channel list used for **Custom Scan** Scan Mode.
Link Aggregation	**Note:** Supported on AP4xx and AP5xx models only. Enable or disable link aggregation. Link aggregation combines network connections to increase throughput and to provide redundancy in case of link failure.

Table 27: Advanced Configuration Profile Settings (continued)

Field	Description
AP Log Level	Specify the message level you want included in the AP log. Valid values are: • Emergencies — System is unusable. • Alerts — Take action immediately. • Critical — Critical condition. • Errors — Error condition. • Warnings — Warning condition. • Notifications — Normal but significant condition. • Informational — Information only. • Debugging — Debug-level messages.
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** Displays fault patterns only. LEDs do not light when there are no AP faults and the discovery is complete. **Normal** Identifies the AP status during the following processes: • registration • power on • boot Default mode for all APs. **Solid** Radio is on and services are configured. This is Normal mode with the option to show a solid LED pattern. This mode is supported on AP4xx and AP5xx. You can override the device group setting for one or more individual APs from the **Advanced** > **Overrides** dialog for the selected AP.

Related Topics

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 Appliance, a proxy 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 155. 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.

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 28: Advanced Radio Settings

Field	Description
OCS Channels	Note: Supported on AP4xx and AP5xx models only. Define custom channel list: • Channels for Radio 1 are all 2.4GHz or 5GHz lower band channels. Channel width is selectable. • Channels for Radio 2 are 5GHz channels or 5GHz upper band channels. Channel width is selectable.
OCS Interval (DTIMs)	DTIM interval must be between 2-100. • R1 5G-L — 5.15-5.35GHz • R2 5G-H — 5.5-5.925GHz • R2 5G-F — 5.15-5.925GHz • R1 2G-F —Channel 1 to 13 (Channel 14 for Japan) Supported on the following 802.11ax APs: • AP505i • AP510i/e • AP560i/h
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 28: Advanced Radio Settings (continued)

Field	Description
Disassociate on Low RSS	This setting is not supported on AP4xx, AP5xx or on ExtremeWireless WiNG APs, and 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 client to roam to a better AP for improved network performance.
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	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.
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 5GHz radio only. The valid values are: (multi-user) MU_MIMO and Disabled. • AP76xx and AP8xxx — this setting is available on both radios. The valid values are: (single-user) SU_MIMO and (multi-user) MU_MIMO. • AP4xx and AP5xx — this setting is available on the 5GHz radio only. 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 28: 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.
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.
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 1, 2, 5.5, or 11 Mbps for 11b and 11b+11g modes.

Table 28: Advanced Radio Settings (continued)

Field	Description
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 Subframes	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").
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: • AP505i • AP510i/e • AP560i/h

Table 28: 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: • AP505i • AP510i/e • AP560i/h
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: • AP505i • AP510i/e • AP560i/h

Related Topics

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 AP4xx and AP5xx support Radio Share and OCS. You have the option to scan neighboring channels in addition to the operating channel.

1. Configure the following settings:

Table 29: 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 Appliance 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

ADSP Support on .11ax APs

The following ADSP features are supported on the AP4xx and AP5xx:

*   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 supported on ExtremeWireless WiNG version 7.2.1. and later. It *is not* supported on ExtremeWirelessAP39xx.

Related Topics

ExtremeLocation Profile Settings

Configure the AP to integrate with ExtremeLocation. ExtremeLocation is a premier location tracking and analytics solution by Extreme Networks. Using HTTPS with self-signed certificates, an AP opens WebSocket connections to the ExtremeLocation Server and reports RSS signal strength readings based on the ExtremeLocation configuration. An ExtremeLocation user associates the Tenant ID and Site information with the AP MAC address over AP WebSocket.

The AP can be the RSS source for both ExtremeCloud Appliance Positioning and ExtremeLocation at the same time. RSS information travels both through the WASSP tunnel to the ExtremeCloud Appliance and through WebSocket to ExtremeLocation.

1. Configure the following parameters:

Table 30: ExtremeLocation Profile Settings

Field	Description
Name	Name of the ExtremeLocation Profile.
Tenant ID	The Tenant ID links the ExtremeCloud Appliance to the tenant, ensuring that your assets cannot inadvertently be deployed on sites that belong to other ExtremeLocation accounts. Any modification made to sites managed by this ExtremeCloud Appliance, such as adding new access points or sites, is tagged by the ExtremeLocation Tenant Account Number automatically. The location Tenant ID is saved to, and retrieved from, the data plane by websocket client, then sent as session data to the ExtremeLocation server once a session is established. The Tenant ID can be up to 32 characters.
Server Address	The FQDN (fully-qualified domain name) of the LocationEngine Server.
Minimum RSS	RSS threshold for reporting location data. Valid values are -90 to -70 dBm.
Report Frequency	Reporting interval in seconds.

2. Click **Save**.

Related Topics

IoT Profile Settings

ExtremeCloud Appliance supports the IoT applications listed in Table 31.

Table 31: IoT Application Support

Application	AP Models Supported
iBeacon	• AP5xx • AP76xx • AP8xxx • AP391x **Note:** AP3935, AP3965, and AP7612 do not support IoT.
iBeacon Scan	• AP5xx (Centralized site only) • AP39xx
Eddystone-url Beacon	• AP5xx • AP76xx • AP8xxx • AP39xx
Eddystone-url Scan	• AP5xx (Centralized site only) • AP39xx
Thread Gateway	• AP5xx • AP39xx

Configure a separate IoT profile for each IoT application:

1. Specify a profile name.
2. Select the IoT application.

The resulting parameters depend on the application you select.

Related Topics

iBeacon Settings

Table 32: iBeacon IoT Settings

Parameter	Description
Application	Determines application type. 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).
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.
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 Appliance generates the Minor value. This ensures that each AP receives a unique value.
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

Related Topics

iBeacon Scan Settings

Table 33: iBeacon Scan Settings

Field	Description
Application	Determines application type. Select **iBeacon Scan**.
Destination IP Address	IP address of the customer Application Server that receives the beacon report.
Destination Port	Destination Port on the customer Application Server that presents the beacon report.

Table 33: iBeacon Scan Settings (continued)

Field	Description
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.
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 Appliance 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	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.

Related Topics

Eddystone-url Beacon Settings

Table 34: Eddystone-url Beacon Settings

Field	Description
Application	Determines application type. 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.

Table 34: Eddystone-url Beacon Settings (continued)

Field	Description
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

Related Topics

Eddystone-url Scan Settings

Table 35: Eddystone-url Scan Settings

Parameter	Description
Application	Determines application type. Select **Eddystone URL Scan**.
Destination IP Address	IP address of the customer Application Server that receives the beacon report.
Destination Port	Destination Port on the customer Application Server that presents the beacon report.
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.
Min RSSI	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.

Related Topics

Thread Gateway Settings

> **Note**
> Thread Gateway is supported by access point models AP39xx (in a Centralized site) and AP5xx (in both Centralized and Distributed sites).

Table 36: Thread Gateway Settings

Parameters	Description
Name	Profile name.
Application	Determines application type. Select **Thread Gateway**.
Network Name	Thread Network name. Default value is the AP serial number. Each AP creates a separate Thread Network identified with separate Short PAN ID and Extended PAN ID.
Channel	The IEEE Standard: 802.15.4 AP channel number.
Short PAN ID	A 16-bit, MAC-layer addressing field used in RF data transmissions between devices in a Thread Network. The Short PAN ID identifies the APs Thread Network.
Extended PAN ID	A 64-bit, MAC-layer addressing field used in RF data transmissions between devices in a Thread Network. This value must be unique. It is used for a more specific network identification.
Master Key	Indicates the Network Master Key used to encrypt communication between nodes in a Thread Network.
Common Credentials	THREADNETWORK
Whitelist	Create a whitelist of approved nodes for the Thread Network.

Related Topics

Configuring IoT Whitelist

Create a whitelist of approved nodes for the Thread Network. The IoT whitelist applies to all APs that are configured for Thread Gateway associated with the ExtremeCloud Appliance.

If your whitelist is empty, all sensors with the default password THREAD have access to the Thread Network. Once you configure at least one node on the whitelist, network access is limited to only nodes configured on the whitelist.

> **Note**
> Once a whitelist is configured, only nodes configured on the whitelist gain access to the Thread Network.

1. Go to the **IoT** tab in the device group profile for an AP39xx.

2. Click ⊕ to add an IoT profile.

3. In the Application field, select **Thread Gateway**.

4. Click the **Whitelist** button.

5. Click ⊕ to add a node and provide the EUI (Extended Unique Identifier) and shared-password for the node.

6. To delete a node, click 🗑.

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 AP39xx and AP4xx in a Centralized site, and supported on AP5xx in both a Centralized and a Distributed site.

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.

    - 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

Analytics Profile Settings

Configure the AP to integrate with the Extreme Networks premier analytics solution ExtremeAnalytics™.

> **Note**
> Supported on AP39xx and AP4xx in a Centralized site, and supported on AP5xx in both a Centralized and a Distributed site.

In a Centralized Site, IPFIX reporting is directed through ExtremeCloud Appliance. In a Distributed site, each AP directly feeds the IPFIX stream into a target ExtremeAnalytics server.

1. Configure the following settings:

Table 37: 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

RTLS Settings

A Real-Time Location System (RTLS) profile must be configured and enabled within ExtremeCloud Appliance before ExtremeCloud Appliance will communicate with the location-based server and before the APs will perform location-based functionality. ExtremeCloud Appliance supports the following location-based solutions:

- AeroScout
- Ekahau
- Centrak.
- Sonitor

Configure the AP to integrate with a Real-Time Location System (RTLS).

1. Click the plus sign to create a new profile (⊕).
2. Configure the following parameters:

Table 38: 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.

Table 38: RTLS Parameters (continued)

Field	Description
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. Click **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 Appliance 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 84

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.

A Centralized site supports the following AP models:

- AP39xx supporting ACS Policy for RF Management
- AP4xx and AP5xx supporting Smart RF Policy for RF Management

Distributed sites support the following AP models, which support Smart RF Policy for RF Management:

- AP5xx
- AP76xx
- AP8xxx

Related Topics

Configuring ACS RF Policy on page 113
Configuring Smart RF Policy on page 115

Basic RF Management Settings

From the **Basic** tab, set the RF Management policy for both ACS and Smart RF. The following settings are available for Smart RF only:

- Sensitivity

- Coverage Hole Recovery

Table 39: Basic RF Management Settings

Field	Description
Name	Name of the RF Management policy.
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 Appliance 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

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 Appliance.

> **Note**
> APs retain the last known channel and power settings after a connection loss or reboot.

Table 40: Channel and Power Settings

Field	Description
Channel Width	Determines the channel width used by the channel on the selected radio. Available options include: • 20 MHz • 40 MHz • 80 MHz (supported on 5GHz only 802.11ac and 802.11ax) • 160 MHz (supported on 5GHz only 802.11ax) • Automatic – Channel width is calculated automatically. This is the default value.
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.
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 112.

Related Topics

Configuring a Channel Plan

If ACS or Smart RF is enabled you can define a channel plan for the AP. Defining a channel plan allows 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 5 GHz Radio nodes, click 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.
  ◦ 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.

- ◦ Custom — To configure individual channels from which to select an operating channel, click **Configure**. The **Custom Channel Plan** dialog displays. Click 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. Click **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.
  - ▪ 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 2.4 GHz Radio nodes, click 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, click **Configure**. The **Add Channels** dialog is displayed. Click the individual channels you want to add to the channel plan while pressing the CTRL key, and then click **OK**.

Related Topics

Configuring ACS RF Policy

The ExtremeCloud Appliance RF Management policy depends on your AP model. AP39xx access points support Automatic Channel Selection (ACS) as the RF Management policy. ExtremeCloud Appliance 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

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.

Click **Interference Recovery** and configure the following parameters.

Table 41: 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.

Table 41: ACS Interference Recovery Settings (continued)

Field	Description
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 Appliance RF Management policy depends on your AP model. ExtremeWireless WiNG APs, AP4xx, and AP5xx support Smart RF as the RF Management policy. ExtremeCloud Appliance 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**
> Smart RF is now supported on AP4xx and AP5xx. Only one Smart RF Policy can be used per site.

To configure Smart RF:

1. Go to **Configure** > **Sites**.
2. Select a Distributed site, then select **Device Groups** tab.
3. Select a device group or select **Add**.

   The **RF Management** value is Smart RF for ExtremeWireless WiNG APs, AP4xx, and AP5xx.
4. Select ✐ next to RF Management, to edit the Smart RF policy.

ExtremeCloud Appliance 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 Appliance initial settings, create a new Smart RF policy. New policies are comprised of the Smart RF settings that are delivered with the initial ExtremeCloud Appliance installation. Click ⊕ to create a new policy.

Related Topics

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. ExtremeWireless WiNG AP models AP76xx, and AP8xxx, and ExtremeWireless AP models AP4xx and AP5xx support custom sensitivity settings.

To set custom sensitivity:

1. Go to **Basic Settings** > **Sensitivity** and select **Custom**.
2. From the **Scanning** tab configure the following parameters:

Table 42: AP Scan Settings

Field	Description
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.
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 once 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. The default value is 50 for both radios.
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 both the 5 GHz and 2.4 GHz bands.
Scan Sample Count	A client awareness count (number of clients 1 - 255) for Off Channel Scans of either the 5 GHz or 2.4 GHz 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 42: AP Scan Settings (continued)

Field	Description
Client Aware Scanning	A client awareness count (number of clients 1 - 255) for Off Channel Scans of either the 5 GHz or 2.4 GHz 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.
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 both the 5 GHz and 2.4 GHz 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 both the 5 GHz and 2.4 GHz 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

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 ExtremeWireless WiNG APs, 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.

Click **Recovery** > **Neighbor Recovery** and configure the following parameters.

Table 43: 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.
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

Interference Recovery Settings for Smart RF

The following settings define thresholds for the Smart RF policy Interference Recovery plan supported on ExtremeWireless WiNG APs, 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 44: 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 a 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. The default is 255.
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. The default setting is 5 dBm.
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. The default setting is 5 dBm.

Related Topics

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 45: 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 115

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 4 on page 21.

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

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 click **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 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

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 Appliance. 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 Appliance.

To import an existing floor plan and update the associated APs:

1. From the floor plan **Configure** page, click **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, click the AP selector ➤ next to the **Place APs** field, then click the AP icon and drag it to a new location.

Related Topics

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 4 on page 21.

.

To add a new floor plan:

1. Go to **Configure** > **Sites**. Add a new site or select a site and click **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 124.

Related Topics

Floor Plan Settings

1. Configure the following parameters for a floor plan.

Table 46: 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 123

Importing or Exporting a Floor Plan on page 124

Importing or Exporting a Floor Plan

ExtremeCloud Appliance supports the following floor plan file formats:

- Zip
- ExtremeCloud Appliance
- 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 click **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 click **Floor Plans** tab.
2. Click **Draw Tools** to display floor plan tools.
3. Under **Floor Image**, click 🖼 to upload an image.

4. Navigate to the background image file.

   The following image file formats are supported: .jpg, .png. svg

   > **Note**
   > .svg is not supported with Internet Explorer version 11.

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

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

To scale a floor plan:

1. Display the floor plan.

   Go to **Configure** > **Sites**. Add a new site or select a site and click **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).
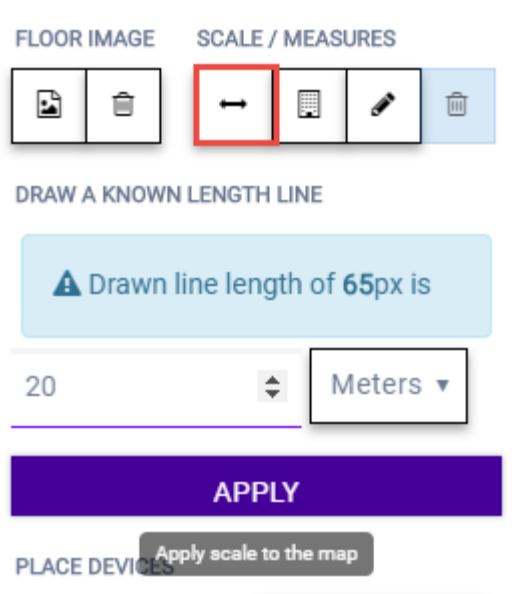
Figure 25: Setting Floor Plan Scale

- 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 click **Floor Plans** tab.
2. Click **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

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 affect 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 click **Floor Plans** tab.
2. Click **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, click a corner of the inner wall.
6. Click 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 click ⟋ to modify a wall or click 🗑 to delete it.

Next, go to Placing Devices on page 127.

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 device on a floor plan:

1. Go to **Configure** > **Sites**. Add a new site or select a site and click **Floor Plans** tab.
2. Click **Draw Tools** to display floor plan tools.
3. Click the **Place Devices** field, and click 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. Click the device from the list.

   The cursor changes to an device icon ▣.

5. Click on the floor plan to place the device.

6. If you need to move the device on the floor plan, first click the selector tool, then select the device icon and move it on the map.

7. To save the floor map, click **Save**.

8. Click ▣**BACK** to display the floor plan **View** page.

Next, go to

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 click **Floor Plans** tab.

2. Click **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

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 click **Floor Plans** tab.
2. Click **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 35

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 click **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 🗑.

NEW! Advanced Tab

Advanced configuration settings for a site. On the **Advanced** tab, you can configure the following:

- **SNMP**. Simple Network Management Protocol configuration for switches associated with a specific site. For more information, see SNMP Configuration on page 259.
- **Preferred Connection**. Control the distribution of APs in a particular site between appliances in a High Availability Pair.

ExtremeCloud Appliance 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 **Preferred Connection**. The load assignment for the preferred appliance persists. However, you can re-map the AP-to-site preference anytime, to adjust for experience, business needs, or network conditions.

For **Preferred Connection**, select the preferred connection point for APs that are assigned to this site:

Use Global Settings

The global settings are dependent on the Availability setting **Auto AP Balancing**. (See **Administration** > **System** > **Availability**.) If Auto AP Balancing is Active - Active, which spreads the load across the availability pair, **Use Global Settings** displays **Load Balance**. If the Auto AP Balancing is Active - Passive, which uses the secondary appliance for failover only, **Use Global Settings** displays **Primary Appliance**.

For more information about the load balancing configuration for an availability pair, see Availability Pair Settings on page 258.

Primary Appliance

APs for this site will be homed on the primary appliance.

Secondary Appliance

APs for this site will be homed on the secondary appliance. The secondary appliance is used for load balancing or failover support.

Related Topics

Devices

Manage access points (APs) and switches from **Configure** > **Devices**. See the ExtremeCloud Appliance Release Notes for a list of supported APs and switches.

> **Note**
> ExtremeCloud Appliance 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: https://extremenetworks.com/documentation/defender-application.

Related Topics

Access Points

Go to **Configure** > **Devices** > **Access Points** to add and configure APs in ExtremeCloud Appliance.

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:

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

You can also select ⟳ to manually refresh the page anytime.

For more information about supported access points, see Access Points List on page 44.

Related Topics

Understanding Access Point States on page 46
Access Points List on page 44
Query Builder on page 46
AP Actions on page 132
Add APs on page 133
Adding a Site on page 81
Device Groups on page 16
Configuring Column Display on page 23

AP Actions

Take the following actions from the AP **Actions** button.

Table 47: AP Actions

Field	Description
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 Appliance Deployment Guide. To add a new site or device group, select ⊕ and configure the parameters. For more information, see Assign to Site on page 153.
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 248. **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.
Reboot	Restart the selected APs .

Related Topics

Radio Settings Button on page 33

Assign to Site on page 153

Add APs

Access points and switches are automatically added to ExtremeCloud Appliance 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 Appliance Deployment Guide* located in the Extreme Networks documentation portal: https://extremenetworks.com/documentation/extremecloud-appliance. 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 Appliance, 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:

   Serial Number

   Unique number that identifies the AP. Provide this number for new and cloned APs. This number is on the AP.

   Model

   Select an AP model number from the drop-down list. The model number is on the AP.

   Name

   Unique name for the AP. Provide a unique name for new and cloned APs.

   Description

   Text description to help identify the AP.

5. Click **OK**.

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

Related Topics

Configure AP 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.

   The Hostname for the AP is now available on the **AP Details** screen. 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.
3. (Optional) Enter a description.
4. Configure the following parameters:

   > **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 133.

Table 48: Radio Properties

Field	Description
Use RF Management Policy	Indicates if settings from the RF Management policy that is associated with the device group are used. If you select **Yes**, links to the RF Management Policy and the site are present. If you select **No**, the radio settings are displayed. You can modify radio setting from here.
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 (supported on 5GHz only 802.11ax) • Automatic – Channel width is calculated automatically. This is the default value.
Request New Channel	Specifies the primary channel of the wireless AP. Select Auto to request ACS to search for a channel using a channel selection algorithm. 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 48: 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.

Fallback Channel	Specify a 5GHz channel that the radio will adopt if DFS (Dynamic Frequency Selection) fails. ExtremeWireless APs support up to 9 channels. ExtremeWireless WiNG APs support one channel at a time, excluding channel 165.
	The following setting is supported on ExtremeWireless access point models AP4xx and AP5xx that are configured for a Centralized site.
	• **Return to configured channel after failed event**. When this setting is 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. 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 **DFS Revert Client Aware** is disabled.

5. Select **Save**.

Related Topics

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.

A Centralized site supports the following AP models:

• AP39xx supporting ACS Policy for RF Management

• AP4xx and AP5xx supporting Smart RF Policy for RF Management

Distributed sites support the following AP models, which support Smart RF Policy for RF Management:

• AP5xx

• AP76xx

• AP8xxx

Related Topics

Advanced AP Settings

Table 49: Advanced AP Setting Actions

Field	Description
Actions	
LED Locate	Select **Locate** to initiate an LED locate action for the AP.
Reboot	Restart the AP.
Retrieve Trace	ExtremeCloud Appliance collects information from the AP, including logs and crash reports if applicable.
Download Trace	Download the trace report.

Related Topics

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 Settings** > **Overrides** tab. To access the **Overrides** dialog:

1. Go to **Configure** > **Devices** > **Access Points**.
2. Select an AP.
3. Select **Advanced** > **Overrides**.

Table 50: 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 Tagged VLANs for all APs in a device group from the device group **Advanced Settings** dialog. And you can override the device group setting for one or more individual APs 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 50: Advanced AP Setting Overrides (continued)

Field	Description
Low Power Mode	When enabled, this setting indicates that the AP will always operate in 4x4 mode regardless of what was negotiated with the Switch PoE. When this option is cleared, the AP operates in 2x2 or 4x4 depending on what was negotiated with the Switch PoE using the 2-event classification. **Note:** When an AP5xx, configured for support in a Centralized site, is connected to two switch ports, configure the power capabilities of both ports identically. If the power capabilities are unequal, the AP will resort to Low Power Mode to ensure a stable operation.

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 one or more individual APs from here. Valid values are:
	
	Off
	    Displays fault patterns only. LEDs do not light when there are no AP faults and the discovery is complete.
	
	Normal
	    Identifies the AP status during the following processes:
	    • registration
	    • power on
	    • boot
	
	    Default mode for all APs.
	
	Solid
	    Radio is on and services are configured. This is Normal mode with the option to show a solid LED pattern. This mode is supported on AP4xx and AP5xx.

WLAN	Select this option and select **Configure** to override the WLAN configuration for a specific AP. See WLAN Override on page 138 for more information.

IBeacon Settings	IBeacon is supported on the following access point models:
	    • AP5xx
	    • AP76xx
	    • AP8xxx
	    • AP391x
	
	You can configure IBeacon settings for all APs in a device group from the device group profile **IoT** tab. And you can override IBeacon settings for one or more individual APs from here.
	
	Note: If IBeacon is not configured in the device group profile, this pane is empty.

Table 50: 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 one or more mesh points, check the mesh point check box to display the edit button (▨). Select ▨ to display the **Edit Mesh Point Settings** dialog. To override a setting, select the check box and provide an override value. **Note:** Mesh Point overrides are available when the AP is part of a Mesh Network.
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 one or more individual APs from here.

Related Topics

NEW! 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.

ExtremeCloud Appliance 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 select **Configure**.

ExtremeCloud Appliance displays a list of configured networks. The settings that are inherited from the associated configuration Profile display.

2. Configure the WLAN assignment per radio.
3. (Optional) Enable **Band Steering** for this AP.

Band steering is intended to relieve congestion by encouraging dual-band client devices to use the higher capacity 5GHz band. To make use of Band Steering, ensure that networks are assigned to both radios. The system always enables both radios when Band Steering is enabled.

For Band Steering to work effectively, configure similar coverage areas for the 2.4GHz and 5GHz bands. Design your network for both 5GHz and 2.4GHz coverage. For networks where coverage quality differs between bands, disable Band Steering.

Band Steering requires that the same SSID be present on both 2.4GHz and 5GHz radios. ExtremeCloud Appliance 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 (2.4GHz and 5GHz). You can disable Band Steering at either the AP override or at the configuration Profile, to regain control over the WLAN assignment per radio band.

On the AP List, a check mark in the **Override** column indicates that the AP is associated with an Override.

Related Topics

IP Address Assignment

Table 51: 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 Appliance 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

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 the AP560h that offers 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.

Figure 26: Professional Install Settings (Two port AP)

Related Topics

NEW! *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 27: AP410e Professional Install Settings

Related Topics

Add APs on page 133

*NEW!**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.

Professional install   ❓ ✕

Radio 2 Port 5G-1 Antenna Type   No Antenna   ▾

Radio 2 Port 5G-2 Antenna Type   No Antenna   ▾

Radio 2 Port 5G-3 Antenna Type   No Antenna   ▾

Radio 2 Port 5G-4 Antenna Type   No Antenna   ▾

Radio 1 Port 2.4-5 Antenna Type   No Antenna   ▾

Radio 1 Port 2.4-6 Antenna Type   No Antenna   ▾

Radio 3 Port 7 Antenna Type   No Antenna   ▾

Radio 3 Port 8 Antenna Type   No Antenna   ▾

CLOSE

Figure 28: AP460e Professional Install Settings

Related Topics

Add APs on page 133

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 29: AP510e Antenna Professional Install

Related Topics

AP560h Professional Install Settings

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.
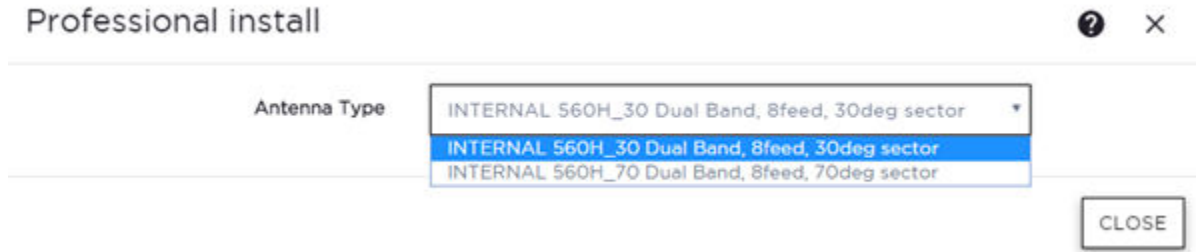
Figure 30: AP560h Professional Install Settings

Related Topics

Switches

ExtremeCloud Appliance 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

Switch Actions

Take the following actions from the switch **Actions** button.

Table 52: 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.

Table 52: Switch Actions (continued)

Field	Description
Retrieve Traces	Initiates a traces routine creating a zip file that includes switch configuration, state information, and log files. ExtremeCloud Appliance receives the Traces zip file and presents a download-able zip file in the Traces tab on the Monitor page for the switch. ExtremeCloud Appliance 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

Understanding Switch States

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

Table 53: 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 Appliance • Configuration is pending acknowledgment from switch • Switch reset pending • Switch reboot pending • Switch upgrade pending
⚫	Unknown. Switch has not discovered the ExtremeCloud Appliance.
🟥	Critical: • Switch stops sending requests for 5 minutes or longer • Consistent with a lost of connectivity to ExtremeCloud Appliance

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 Appliance:

   - 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 Appliance 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 Appliance Deployment Guide* located in the Extreme Networks documentation portal: https://extremenetworks.com/documentation/extremecloud-appliance

2. Go to **Configure** > **Devices** > **Switches**.
3. Click **Add** and configure the parameters.

   > **Note**
   >
   > You can clone a switch from within a site, see Switches on page 145.

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. Click **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

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 153.

> **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 Appliance 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

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 148
Advanced Switch Settings on page 151

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

Advanced Switch Settings

Table 54: 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 Appliance. • 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 54: Advanced Switch Settings (continued)

Field	Description
SNMP Configuration	You can configure SNMP for the individual switch or for the full ExtremeCloud Appliance. For more information, see SNMP Configuration on page 259.
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 63. • 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 136

IP Address Assignment on page 139

Access the Switch CLI

ExtremeCloud Appliance 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 63.

- 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 Appliance 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 Appliance credentials.

Related Topics

Troubleshoot a Switch Using the CLI on page 63

Advanced Switch Settings on page 151

CLI - Mode Advanced Settings on page 153

Switch Configuration Backup Files on page 153

Switch Configuration Backup Files

When a switch is changed to CLI-mode, ExtremeCloud Appliance 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 152.

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 152

Configure a Switch on page 148

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 148

Access the Switch CLI on page 152

NEW! Assign to Site

You can assign access points, switches, and Defender adapters directly from the respective device list, which simplifies the manual on-boarding 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 Appliance 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 Appliance Deployment Guide.

Related Topics

Networks

Configure network services that bind a wireless LAN service (WLANS) to a default role. 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 (Open/WPAv2 with PSK/ WPAv2 Enterprise w/ RADIUS).

To add a network, go to **Configure** > **Networks** > **Add**.

Related Topics

WLAN Service Settings

Table 55: 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
Status	Enable or disable the network service. Disabling the network service shuts off the service but does not delete it.

Table 55: 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. • WEP (Static Wired Equivalent Privacy) — 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 160. • WPAv2 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 WPAv2 with PSK on page 159. • 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. **Note:** MBA and Captive Portal are not supported when using WPA2 Enterprise w/ RADIUS. The devices with 802.1X use Default Auth role only. See Privacy Settings for WPAv2 Enterprise with RADIUS on page 159. • WPAv3 - Personal with SAE — 128-bit encryption, supported on: 　◦ AP4xx running ExtremeWireless WiNG 7.3x. 　◦ AP5xx running ExtremeWireless WiNG 7.2x and later. WPAv3 uses a pre-shared key (PSK) and Simultaneous Authentication of Equals (SAE). WPAv3 offers an augmented handshake and protection against future password compromises. See Privacy Settings for WPAv3 with SAE on page 159. • WPAv3 - Compatibility — Option for mixed deployments of 802.11ax APs and older AP models. If the network is configured with WPAv3-Compatibility (SAE or WPAv2 PSK authentication), 802.11ax APs running ExtremeWireless WiNG 7.2.x or later utilize the WPAv3 - Personal protocol. Older AP models that are not WPAv3 compatible use WPAv2 AES. See Privacy Settings for WPAv3 with SAE on page 159.
Enable Captive Portal	Check this option to enable captive portal support on the network service.

Table 55: WLAN Service Configuration Settings (continued)

Field	Description

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

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.
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 Appliance. 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.
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 Appliance. Do not authenticate MAC address on the RADIUS server. This setting is not available when you have selected **Default** as the Authentication Method.

Table 55: WLAN Service Configuration Settings (continued)

Field	Description
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 Configure this setting if you want to override the default accept policy role with your own default authentication policy role. By default, **Enterprise User** is the Default Auth Role. To configure a different role as the Default Auth Role: 1. Configure the role under **Configure** > **Policy** > **Roles** and indicate that it is the Default Auth Role here. 2. Go to **Onboard** > **Rules** and edit a policy rule, specifying **Default Auth Role** in the Accept Policy field.
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:** This option is unavailable until you install and run Scheduler for ExtremeCloud Appliance. Select **Scheduling** to open the Scheduler application. This is a Docker application that resides on ExtremeCloud Appliance. Download Scheduler for ExtremeCloud Appliance from the Extreme Networks support portal, and install the application. Before running the Scheduler application, you must generate an API key and associate it with the Docker application.

Related Topics

Privacy Settings for WPAv3 with SAE

WPAv3 with SAE — Network access is allowed to any client that knows the pre-shared key (PSK).

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. Protected Management Frames (PMF) adds an integrity check to control packets being sent between the client and the access point.
    - WPAv3 - Personal (SAE). Setting is **Required**. Requires that all devices use PMF format. This could result in older devices not connecting.
    - WPAv3 - Compatibility. Setting is **Enabled**. Supports PMF format but does not require it.
- WPAv3 Key. The password to access this wireless network.

Related Topics

Privacy Settings for WPAv2 with PSK

WPAv2 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). This option is selected by default to enable mixed TKIP-CCMP encryption.
- 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. Protected Management Frames (PMF) adds an integrity check to control packets being sent between the client and the access point. This setting is enabled by default. 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.
- WPAv2Key. The password to access this wireless network.

Related Topics

Privacy Settings for WPAv2 Enterprise with RADIUS

WPA2 Enterprise w/ RADIUS — Supports 802.1X authentication with a RADIUS server, using AES encryption. This is the highest level of network security, particularly when used in conjunction with client certificate-based authentication (EAP-TLS). All 802.1X protocols are supported.

> **Note**
> MBA and Captive Portal are not supported when using WPA2 Enterprise w/ RADIUS. The devices with 802.1X use Default Auth role only.

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). This option is selected by default to enable mixed TKIP-CCMP encryption.

- 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. This setting is enabled by default. 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.

- 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 155

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.

Mesh Network

- WEP Key — Type the WEP key using the **Input String** method above.

Related Topics

> WLAN Service Settings on page 155

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, 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:

- 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.
- The path between any two APs is one hop. The path to a mesh point root can consist of multiple hops.

> **Note**
> 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.

- The mesh network also supports mobile mesh points referred to as VMMs (Vehicle Mounted Modems). A VMM provides mesh connectivity while traversing the wireless mesh network at vehicular speeds.
- A mesh network is self-healing. The network reforms when an AP fails, preventing a single point of failure.

To create a mesh network:

1. Configure a network mesh point for each radio or one mesh point for both radios.
2. Add that network to the device group configuration Profile.
3. Configure Profile behavior for the mesh point under the mesh point configuration Profile settings.

The following access points support mesh point:

- AP7xxx, AP8xxx
- AP39xx

> **Note**
> AP39xx are limited to one mesh point.

Related Topics

Configure a Mesh Point Network

Before configuring a mesh point network, ensure that the APs are configured for mesh point.

1. Go to **Configure** > **Networks** > **Mesh Point** > **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 **Device Groups** tab, and select a specific device group.
    c. Next to the **Profile** field, select ▧.
    d. Select the **Networks** tab, and select the mesh point networks.

3. Configure the device group Profile settings:

    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.
    e. Configure the Mesh Point Profile Settings.

Related Topics

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.

    Status

    Enable or disable the network service. Disabling the network service shuts off the service but does not delete it.

    Root

    Indicates if this mesh point is a root node. A root mesh point is connected to the WAN and provides a wired backhaul to the network.

Neighbor Timeout (seconds)

Defines the threshold to declare a neighboring AP offline when no traffic is received from the neighbor. The lower the value, the less impact a non-functioning AP has on the network. This is typically set to less than 120 seconds. If a neighboring AP stops sending beacons, this setting ensures that the neighbor is removed from the Mesh Point Neighbor table.

Auth Type

Mesh networks must use WPAv2 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. Select **Edit Privacy** to enter the WPAv2 key.

Control VLAN

The VLAN that is used to facilitate root-to-root communication for handoffs. When a mesh point device (an AP, wireless client, or VMM) moves from one root to another, the root AP sends an announcement across the Control VLAN, alerting the wired infrastructure and other mesh point roots that the MAC address of a mesh point device has moved.

Also, Layer 2 updates are sent on any VLAN that is configured on the device that has moved. The broadcast Layer 2 updates ensure that all roots and core infrastructure are aware of the change.

Mesh point networks support tagged frames. Any VLAN and role associated with a configuration Profile that includes mesh points is allowed to traverse the mesh point network.

Select a configured VLAN from the list. Other options:

- ⊕ — create a new VLAN
- ✎ — edit selected VLAN
- ▢ — delete selected VLAN

Related Topics

Captive Portal Settings

Go to **Networks** to enable captive portal. Select the portal type: Internal or External. 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 Appliance for redirection.

Related Topics

Internal Captive Portal Settings

An internal captive portal resides on ExtremeCloud Appliance. Configure the following parameters for an internal captive portal.

Table 56: 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.
Use HTTPS for connection	(Optional) Indicates that the connection will be secure with HTTPS.
Authentication method	Select the authentication method for the captive portal. • Default. Click Configure Default AAA for pop up. • RADIUS. Look up on a remote RADIUS Server. This option enables the primary and backup RADIUS fields. • Local. Look up in the local password repository. • LDAP. Look up on a remote LDAP server. This option enables LDAP Configuration.
LDAP Configuration	Lightweight Directory Access Protocol. Select a configuration or select the plus sign to add a new configuration.

Related Topics

External Captive Portal Settings

An external captive portal resides on a separate server. Configure the following settings for an external captive portal.

Table 57: External Captive Portal Settings

Field	Description
ECP URL	URL address for the external captive portal.
Walled Garden Rules	Click **Walled Garden Rules** to configure policy rules for the external captive portal.

Table 57: External Captive Portal Settings (continued)

Field	Description
Identity	Determines the name common to both the ExtremeCloud Appliance and the external Web server if you want to encrypt the information passed between the ExtremeCloud Appliance 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.
Shared Secret	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

ExtremeGuest Captive Portal Settings

An ExtremeGuest captive portal resides on an ExtremeGuest server. Configure the following settings.

Table 58: 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

Walled Garden Rules

When authenticating with third-party credentials such as Facebook or Google, the ExtremeCloud Appliance 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

Take the following steps to configure Walled Garden rules:

1. Go to **Configure** > **Networks** and select a network.
2. Enable **Captive Portal**.
3. Click **Walled Garden Rules**.
4. Click drop-down to display settings for each OSI layer:
    - L2 (Mac Address) Rules
    - L3, L4 (IP and Port) Rules
    - L7 (Application) Rules

5. Configure the rule parameters.

    Each application site requires specific rules to access their site domains. The following table 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 59: 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

Advanced Network Settings

To configure advanced network settings:

1. Go to **Configure** > **Networks** > **Add**.
2. Select **Advanced**.
3. Configure the following parameters:

    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 AP4xx and AP5xx.

    RADIUS Accounting

    Indicates that the RADIUS server will also handle RADIUS accounting requests.

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 Appliance.

Shutdown on Meshpoint Loss

Shut down AP on loss of mesh connection. Enabling this setting makes it clear which AP services are operational.

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 on APs in a Centralized site.

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 for a Centralized site is not supported.

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

Managing a Network Service

Once 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 **Meshpoints**.
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

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

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 Appliance 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 (e.g., ARP, DHCP, and DNS) and HTTP to redirect web traffic for assisted remediation.

Related Topics

Adding Policy Roles on page 171
Role Widgets on page 76
Policy Role Settings on page 172

Adding 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 172.
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 Appliance. Policy rules are applied from top to bottom.
4. To add new rules, select **New**.
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 172
Policy Rules for OSI L2 to L4 on page 173
Application (Layer 7) Rules on page 175
Associated Profiles on page 172

Policy Role Settings

Table 60: Role Parameter Settings

Field	Description
Name	Name of the role.
Bandwidth Limit	Select this option to allow unlimited bandwidth. Click ◣ to set the Class of Service value.
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

Associated Profiles

A list of configuration Profiles that this role or network 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. Device groups have a configuration Profile assignment. Therefore, APs within the device group are associated with the network definition and the role policy definition through the configuration Profile. Once 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 Appliance simplifies this procedure. After saving a network configuration or policy definition, ExtremeCloud Appliance prompts you to select the configuration Profile for association.

> **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 16

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 173
Configuring L3, L4 Rules on page 174

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

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 Appliance installs application policies with rules on the supported APs where enforcement occurs.

> **Note**
> Application policies are supported by ExtremeCloud Appliance-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 Appliance 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 Appliance. 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. Once 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

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 179

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

Configure the following parameters to add custom applications to the L7 Apps list.

Table 61: Custom Application Settings

Field	Description
Group	Internet applications are organized in groups based on the type or purpose of the application. Once 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

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

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 kilo
bits per second (Kbps).

Related Topics

VLANS

VLANs are logical subnets. Many VLANs can coexist on a single Ethernet cable (typically referred to as a 'VLAN Trunk'). The AP is a VLAN-aware bridging device. It can place traffic on any VLAN to which it is exposed. Other options are bridging locally at EWC and Fabric Attach. Fabric Attach allows 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 Appliance 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 Appliance 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 Appliance 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.

Related Topics

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 62: VLAN Configuration Settings

Field	Description
Name	Provide a unique name for the VLAN.
Mode	**Bridged@AC** — The ExtremeCloud Appliance 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 Appliance. The station's "point of presence" on the wired network for a bridged at AP topology is the AP's wired port. **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 Appliance anywhere a B@AP topology can be configured.
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. The VLAN ID range is (1 - 4094). 4094 is reserved for Internal VLAN ID.
I-SID	For **Fabric Attach**, enter 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).
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.
IP Address	IP address of the VLAN. Wireless clients can access ExtremeCloud Appliance via this IP address.
FQDN	Fully-Qualified Domain Name

Table 62: VLAN Configuration Settings (continued)

Field	Description
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 Appliance is used for managing IP addresses. • Use Relay. Indicates that the ExtremeCloud Appliance forwards DHCP requests to an external DHCP server on the enterprise network. DHCP relay bypasses the local DHCP server for the ExtremeCloud Appliance 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 Appliance user interface through this port.

4. To configure advanced parameters, select **Advanced**.

5. Select **Save**.

Related Topics

> VLAN Advanced Setting on page 183
>
> VLANS on page 181
>
> Generate Browser Certificates on page 208

VLAN Advanced Setting

Configure the following parameters to optimize your network connectivity. Modifying the following settings is optional. Consider changes thoughtfully.

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 Applianceoffers a predefined set of multicast rules. Select a preset multicast rule or define a new rule.

Related Topics

> Pre-defined Multicast Rules on page 184

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

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.

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 Appliance 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.

The ExtremeCloud Appliance enforces the unique VLAN/I-SID requirement for each Fabric Attach topology. A single ExtremeCloud Appliance supports up to 94 VLAN/I-SID mappings. This is a limit of LLDP.

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**
>
> When using ExtremeWireless WiNG APs, you must manually set the Management VLAN ID from the device group Profile.
>
> 1. Edit the device group Profile:
> 2. Select the profile **Networks** tab.
> 3. Click ⊕ to add a network.
> 4. From the Network settings page, specify the **Default VLAN ID**.

> **Note**
>
> In a mobility scenario that includes a local and foreign ExtremeCloud Appliance, make sure the Fabric Attach topology configuration is the same on each ExtremeCloud Appliance, ensuring that an AP that moves between appliances has the same set of topologies.
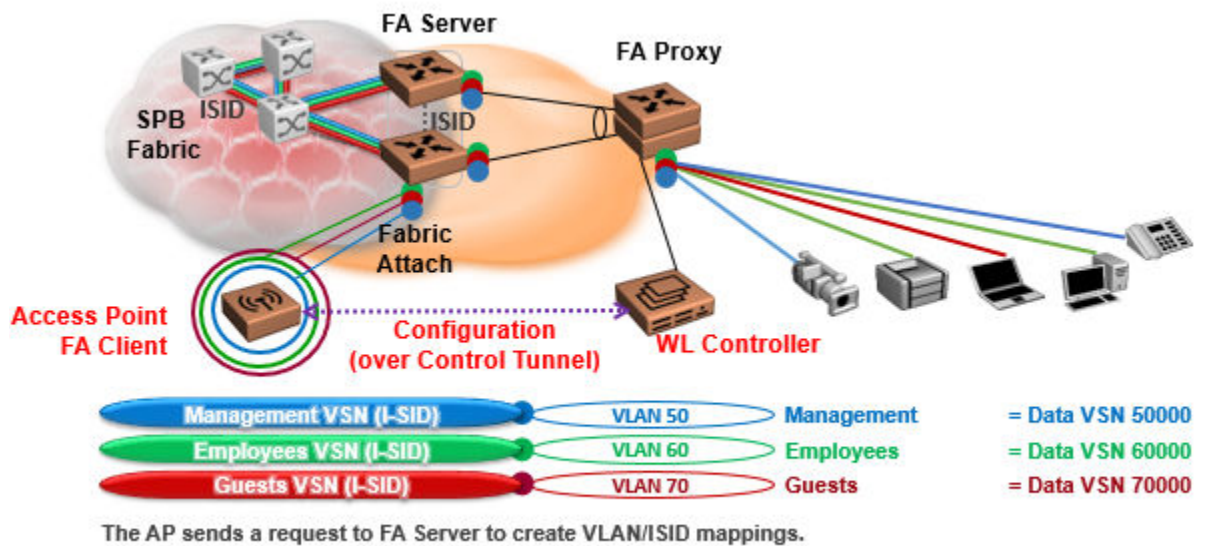
Figure 31: Fabric Attach for FA Clients — Automated Network Services

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. Bridged@AP and Fabric Attach topologies in a Distributed site 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 can be added to Bridged@AP groups.
- Bridged@AP and Fabric Attach topology groups cannot be configured as a "Contain to VLAN" topology on roles or filter rules.
- A WLAN that uses Bridged@AP and Fabric Attach topology groups is not supported in Centralized sites.
- 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 186

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.
   - **Bridged@AP** and **Fabric Attach** topologies in Distributed sites 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

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)

   Specify the rate at which the network will support data transfer under normal operations. It is measured in kilo-bits per second (kbps).
4. Select **Save**.

NEW! 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 criteria (device license domain and model number), ExtremeCloud Appliance 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 Appliance
- 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

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 automatically organized into the logical sites and device groups 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

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

NEW! 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. From the **Action** field, select a rule action. Valid values are:

   - 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 190.
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

NEW! 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. From the **Action** field, select a rule action. Valid values are:

   - Allow

   - Deny

   - Redirect
4. Select a site.
5. Select a filter parameter, and then select ⊕.

Related Topics

NEW! 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 Appliance. 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 Appliance 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 y must be greater than or equal to the value 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 — If you specify a device group pattern "AP510-$FQDN[6:8]", and 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 y must be greater than or equal to the value 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 exisitng 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

NEW! 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 (eg, `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 190.

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 193
Pattern-Based Matching on page 190

NEW! 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 a 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 Appliance.
5. Select a filter parameter, and then select ⊕.

> **Note**
> Devices that match filter criteria on a redirect action do not initially connect to ExtremeCloud Appliance. They are redirected to another ExtremeCloud Appliance. If the destination ExtremeCloud Appliance contains adoption rules with filter criteria that match the redirected devices, the devices are adopted by the destination ExtremeCloud Appliance. 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 193

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 Appliance.

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 188
Adoption Rules on page 188
Deleting Adoption Rules on page 194

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 Appliance.

To delete an adoption rule:

1. Go to **Configure** > **Adoption** and click on an adoption rule in the list.
2. Click 🗑.

   A confirmation dialog displays.
3. Click **OK**.

Related Topics

Adoption Rules on page 188

NEW! AAA RADIUS Authentication

You have options when configuring AAA Authentication:

- Configure a WLAN to use the local Network Access Control (NAC) to terminate or proxy a RADIUS authorization and accounting request.
- When configuring a Distributed site, refer to external RADIUS servers directly without proxy by NAC.
- When configuring a Centralized site, 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 Appliance.

- To configure AAA Policy for external RADIUS, bypassing ExtremeCloud Appliance, go to **Configure** > **AAA Policy**.
- To configure AAA RADIUS servers within the local NAC, go to **Onboard** > **AAA**.

For access points in a Distributed site, the AP can issue the RADIUS request directly to the RADIUS server without the RADIUS request being directed through the ExtremeCloud Appliance. For access points in a Centralized site, the RADIUS Authorization and Accounting transactions occur between the Network Access Server (NAS) on ExtremeCloud Appliance 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

NEW! 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 Appliance.

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 Appliance. Local Onboarding is the default value for WLAN Networks configured for Internal Captive Portal.

2. From the AAA Policy field, select ⊕ to add a new policy, or select ✎ to edit a policy.

3. 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. 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

> **Note**
> Access Points associated with a Distributed site that refer directly to the external RADIUS server do not support changing the Call Station ID. Wired MAC: SSID is the only available option.

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

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

NEW!RADIUS Settings

Configure the following parameters, and then select **Save**.

Server Address

The address of the Local Onboarding Server. This value cannot be changed.

Timeout

Determines a timeout value, in seconds, for the RADIUS server connection.

Retries

Determines the number of times ExtremeCloud Appliance 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

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 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.

ExtremeGuest Integration

Use ExtremeGuest™ as an External Captive Portal Server to create and monitor External Captive Portals. ExtremeCloud Appliance supports ExtremeGuest for both Centralized and Distributed deployments.

> **Note**
>
> The ExtremeCloud Appliance Network Access Control (NAC) Rules Engine is not invoked for clients on a WLAN Network that is configured to use the ExtremeGuest Server.
>
> In Distributed mode, the ExtremeGuest integration dictates that RADIUS transactions originate at the AP. In Centralized mode, the Network Access Server (RADIUS client) on ExtremeCloud Appliance handles the RADIUS transactions. RADIUS transactions are not relayed by NAC on ExtremeCloud Appliance.

ExtremeGuest integration within ExtremeCloud Appliance:

- 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

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 Appliance 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 Appliance 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

Callback Manager

Callback Manager is an ExtremeCloud Appliance component that supports the integration of ExtremeCloud Appliance 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. Once 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 Appliance restart. Once the appliance is restarted, Callback Manager continues to report changes that it had yet to report.

Related Topics

Onboard

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 201
Setting Default AAA Config on page 200
LDAP Configurations on page 204
Managing The Local Password Repository on page 206
Managing Captive Portal on page 209
Managing Access Control Groups on page 222
Access Control Rules on page 225

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 63: 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 Appliance authenticates user. • LDAP. LDAP server authenticates user.
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 Appliance. Do not authenticate MAC address on the RADIUS server.

Related Topics

RADIUS Settings on page 202

Advanced RADIUS Settings on page 202

LDAP Configuration Settings on page 204

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 Appliance allows up to four redundant RADIUS servers for accounting and four RADIUS servers for authentication.

Related Topics

RADIUS Settings

Configure the following parameters and select **Save**.

Table 64: 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 Appliance 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 Appliance 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

Advanced RADIUS Settings

For information about advanced RADIUS configuration settings, see the following table:

Table 65: 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.
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.

Related Topics

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

Create an LDAP configuration for each LDAP server in your network.

Table 66: 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.
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 66: 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 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 67: 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.
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.

Table 67: LDAP Schema Definition Settings (continued)

Field	Description
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 204

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 Appliance 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 Appliance 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 click **Save**.

    *   To delete the account, click **Delete**.

3. To add a new account, from the **Local Password Repository** tab, click **Add User** and configure the user account settings.

Related Topics

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 Appliance **Onboard** > **AAA** > **Local Password Repository**. The default captive portal password is `Extreme@pp`.
>
> The Admin account created here is separate from your ExtremeCloud Appliance system account. System accounts are managed from **Administration** > **Accounts**.

Table 68: 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

Certificates

To ensure a secure website that takes advantage of encryption, ExtremeCloud Appliance 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 Appliance 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 208
Generate RADIUS Server Certificates on page 209
AAA Certificate Authorities on page 209

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.

Once an interface or topology is created, the **Certificates** button displays. Take the following steps:

1. Click **Certificates**.
   The **Certificates** dialog displays.
2. Select the Certificate option:
   - **Install or Replace Certificate**

     Select this option and click **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 Appliance 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

Generate RADIUS Server Certificates

> RADIUS server certificates ensure encryption between the RADIUS server and ExtremeCloud Appliance. 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. Click **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, click **Add Files**, navigate to the saved certificate file, and click **Open**.
> 4. Click **Save** to save your changes and close the dialog.

Related Topics

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 Appliance, 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

Managing 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:8445/administration`.

Related Topics

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

Table 69: 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

Guest Portal: Guest Registration

Table 70: 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 166.
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 166.
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 166.
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 166.
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 166.
Provider 1 Registration	Select this option to use credentials from a custom application that you configure. See Walled Garden Rules on page 166.
Provider 2 Registration	Select this option to use credentials from a custom application that you configure. See Walled Garden Rules on page 166.

> **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

Authentication with Third-party Credentials

Guest Registration using a third-party application has the following advantages:

- It provides ExtremeCloud Appliance 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 Appliance retrieves the public information from the end user's third-party account and uses that information to populate the name and email registration fields.

Once 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.
- Once logged in, the end user is presented with the information that ExtremeCloud Appliance receives from the third-party application.
- The end user grants ExtremeCloud Appliance 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 Appliance, 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 Appliance Access Control engine must have Internet access in order to retrieve user information from the third-party application.
- The ExtremeCloud Appliance 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 Appliance 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 include the third-party application Application ID and Secret.

Authenticated Portal: Authenticated Web Access

Table 71: 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

Authenticated Portal: Authenticated Registration Settings

Table 72: Authenticated Portal — Authenticated Registration Settings

Field	Description
Login or Register Message	See Introduction Message.
Introduction Message	See Introduction Message.
Failed Authentication Message	See Failed Authentication Message.
Customize Fields	See Custom Fields.
Max Failed Login	See Max Failed Login.
Redirection	See Redirection.

Table 72: Authenticated Portal — Authenticated Registration Settings (continued)

Field	Description
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.
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://<IP of portal interface>/self_registration`
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://<IP of portal interface>/pre_registration` 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

Look and Feel Settings

Use Table 73 to customize your captive portal.

Table 73: 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. Click the plus sign to add images. Once the image is added, click 👁 to preview the image. Once 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 73: Captive Portal Website Look and Feel Settings (continued)

Setting	Description
Edit Colors	Click on 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 73: 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, click ❌ for the locale in the locales list.

Related Topics

Portal Network Configuration

Configure settings for portal network configuration:

1. Go to **Onboard** > **Portal**.
2. Click an existing portal or click **Add**.

3. Configure the following parameters on the **Network Configuration** tab.

Table 74: 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 Appliance 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.

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 75: 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 221

Login Configuration Settings

Set up a login configuration profile to simplify user access to the captive portal.

Table 76: 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 220

Managing Access Control Groups on page 222

User Account Settings on page 207

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.

Managing 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 LDAP host group. Configure groups to be used with access control rules. ExtremeCloud Appliance 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

Configure the following access control group settings and click **Save**. The entry parameters depend on the Group Type.

Table 77: Access Control Group Settings

Field	Description
Name	Group name.
Description	Description of the group.

Table 77: Access Control Group Settings (continued)

Field	Description
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 Host Groups only** — Specify whether to match any or match all of the LDAP attributes. The `Exists` mode checks to see if the host is present in the LDAP group. Valid values are: • Match All • Match Any • Exists
Group Entries	A list of entries for the group. Use the **Search** field to search for an entry.

Related Topics

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 Appliance 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 222
>
> Working with Group Entries on page 223

Default Groups Provided with Your Installation

The following Access Control system groups are provided with the ExtremeCloud Appliance 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.

- Web Authenticated Users. A list of MAC addresses that have been granted access to the network via the Authenticated captive portal.

In addition, the following Device Type groups are provided with your ExtremeCloud Appliance installation:

- Windows

- Linux

- Mac

- iPhone

- BlackBerry

- Android

- Windows

- Mobile Game Console

- Chrome OS

You cannot delete system groups.

Related Topics

> Managing Access Control Groups on page 222

Access Control Rules

Access Control Rules allow 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 Appliance grouping is the building block for Access Control Rules. An Access Control Rule comprises: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 Appliance 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

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 Appliance 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

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

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.

- 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. 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. This rule is only present when Authenticated Registration or Authenticated Web Access is enabled.

Related Topics

Rule Settings

Configure the following Access Control Rule settings and click **Save**.

Associate rules to a group type. Configure groups under **Access Control** > **Groups**.

Table 78: Access Control Rule Settings

Field	Description
Name	Rule name. You cannot change the name of default rules that are provided with ExtremeCloud Appliance.
Rule Enabled	Indicates if the rule is enabled. You cannot disable default rules that are provided with ExtremeCloud Appliance.
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.	

Table 78: Access Control Rule Settings (continued)

Field	Description
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 74.
Portal	Associate a captive portal with a rule.

Related Topics

Managing Access Control Groups on page 222

Managing Access Control Rules on page 227

Policy Role Settings on page 172

Configuring Network Policy Roles and Dynamic Access Control on page 225

Tools

Workflow

Use Workflow to understand the relationships between the ExtremeCloud Appliance components and to more easily navigate ExtremeCloud Appliance. The following is a relationship diagram illustrating the ExtremeCloud Appliance components. You can easily navigate to any of these components using **Workflow**.

Go to **Tools** > **Workflow** to begin.
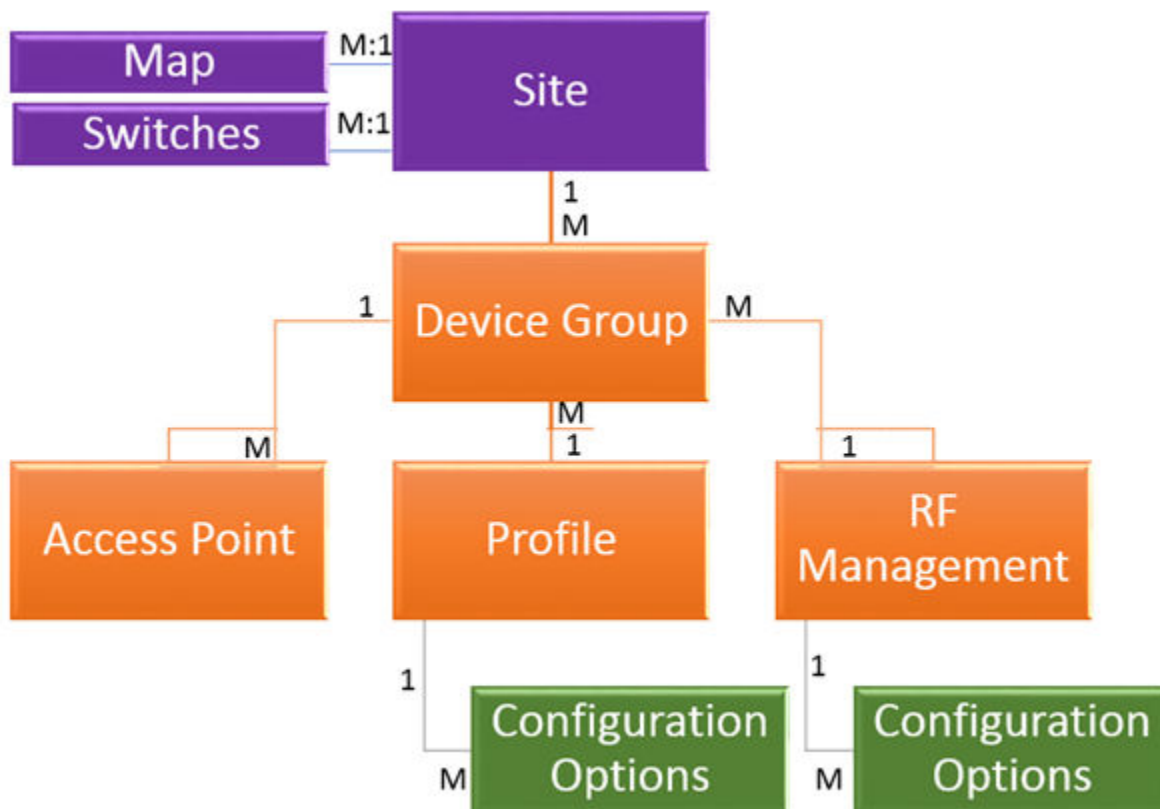
Figure 32: ExtremeCloud Appliance Component Relationship

Related Topics

Navigating ExtremeCloud Appliance Using Workflow on page 231
Modifying a Component on page 238

Navigating ExtremeCloud Appliance 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 Appliance. 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.
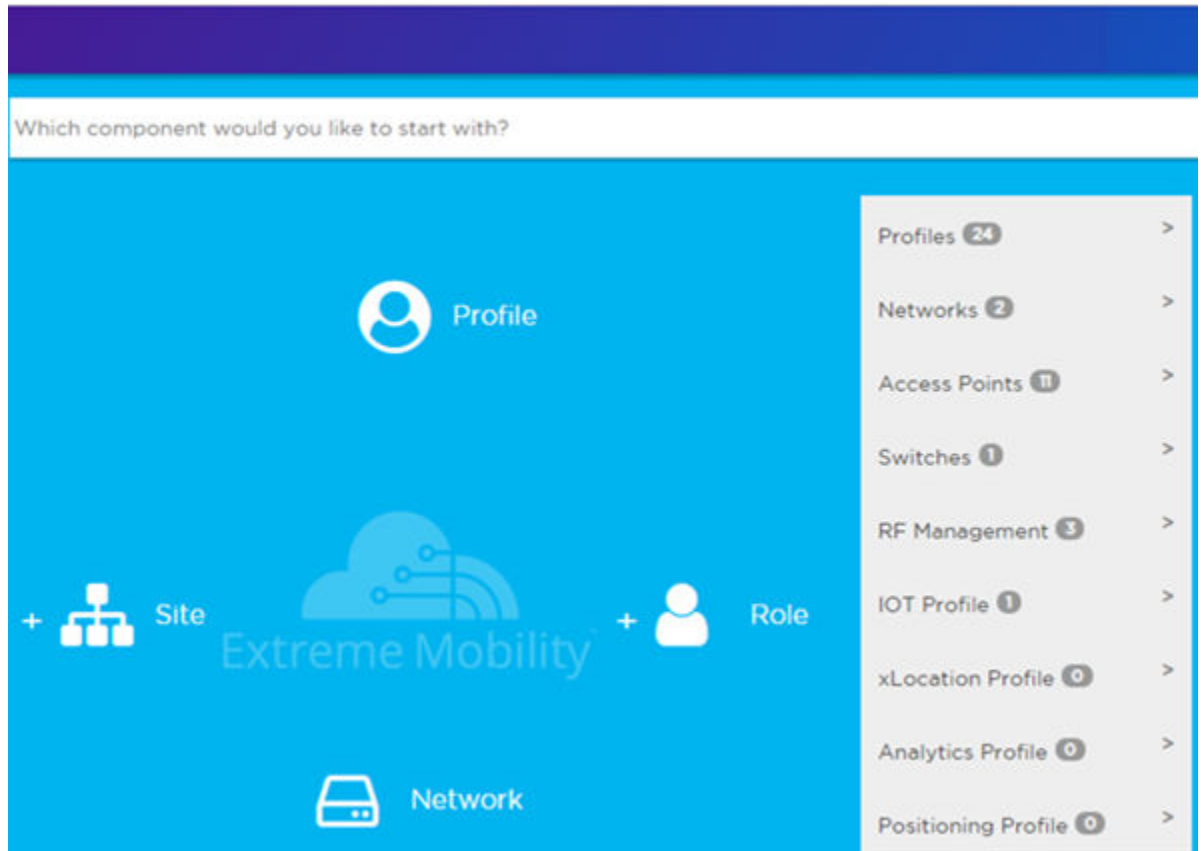
Figure 33: Workflow Main Page

Related Topics

How to Navigate Using Workflow

Go to **Tools** > **Workflow** to navigate ExtremeCloud Appliance accessing components. The following example illustrates the relationship between ExtremeCloud Appliance 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.

Site

Search (No regular expression supported)

Name	Country	Timezone
Site1	United States	America/New_York
DFNDR_SITE	United States	America/New_York
Site_distributed	United States	America/New_York
ap3915e_fcc	United States	America/New_York

A site has the following associated components: Access Point, Device Group, and Switch.

Figure 34: Site with associated components

Figure 34 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.
- Grey 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.
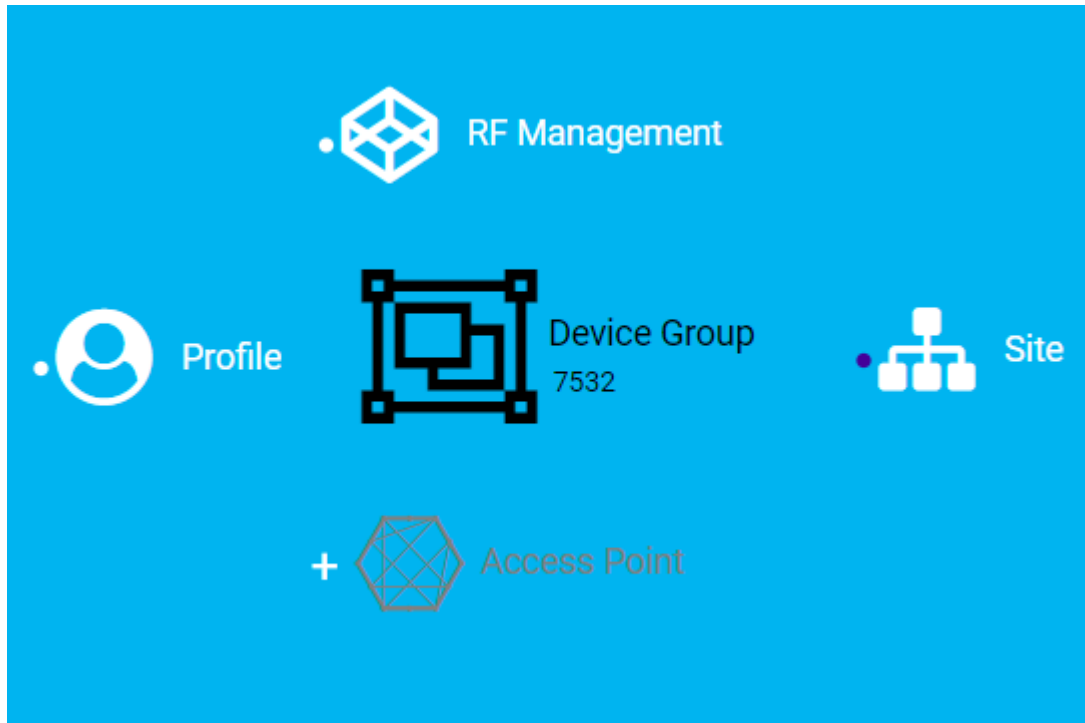
Figure 35: Device Group with associated components

- 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 Points** appears grey. Click ➕ beside **Access Points** 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 133.

6. Each device group has a single profile. Click the **Profile** icon to display the configuration items associated with that profile.
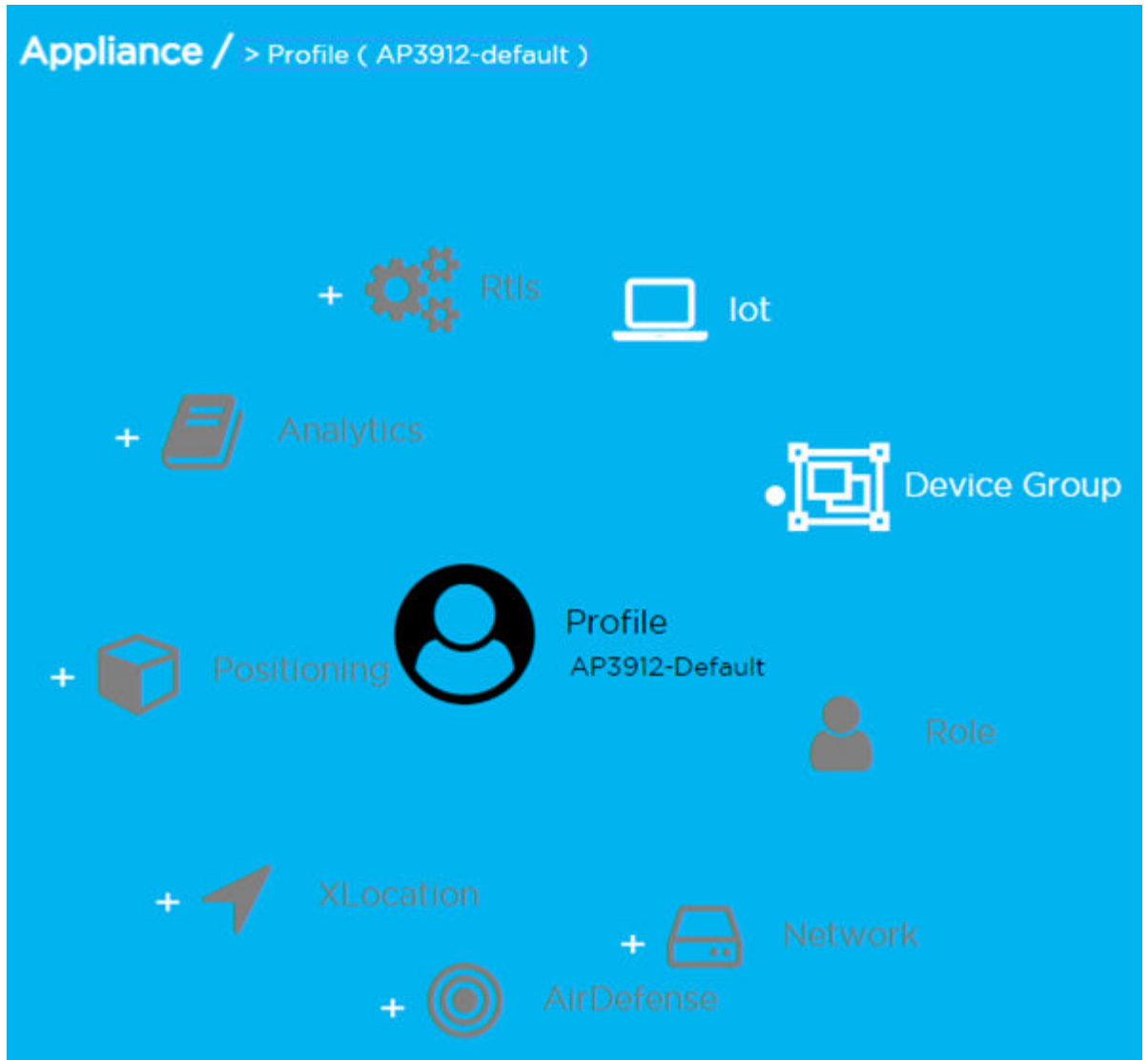
Figure 36: Profile with associated components

> **Note**
> Grey icons indicate components that are not configured. Click ➕ to display the **Edit Profile** page and configure the component.

7. Continue navigating through the component hierarchy to view any component within ExtremeCloud Appliance. 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

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:

- Click the drop-down arrow under a component type and select the plus sign.
- Configure the parameters to add the component to the appliance and click **OK**.

1. From the **Workflow** pane, click the arrow next to **Access Points**.
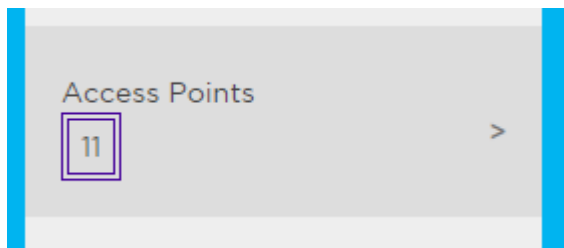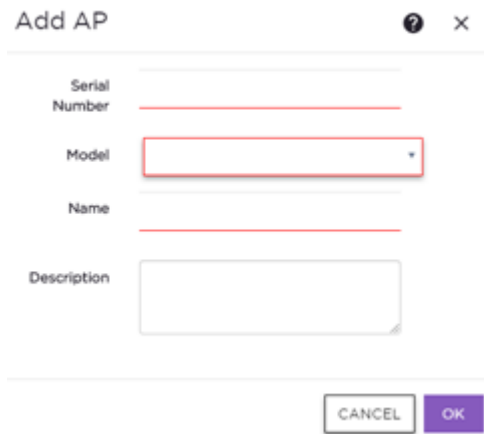
Figure 37: Workflow Pane APs

2. Select the plus sign.
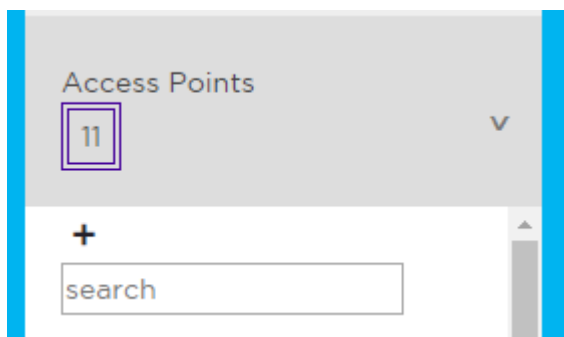
Figure 38: Adding APs from Workflow Pane

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 39: Add AP dialog

3. Configure the following parameters, then click **OK**.

   - Serial Number
   - Model
   - Name
   - (Optional) Description

   The Access Points configuration page for the specific AP displays. See Configure AP Radio Settings on page 134 for instructions on configuring the AP radio settings.

Related Topics

   Configure AP Radio Settings on page 134

Deleting Components from Workflow

You can delete ExtremeCloud Appliance 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 🗑.
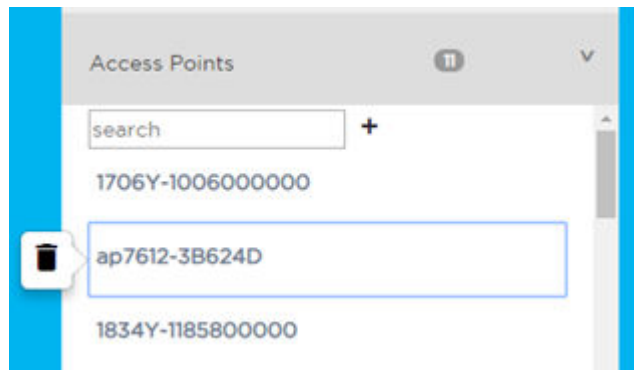
A confirmation dialog displays.

Figure 40: Delete AP in Workflow

3. Click **OK** to delete the component.

Related Topics

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 84
>
> WLAN Service Settings on page 155

Logs

The log messages contain the time of event, severity, source component, and any details generated by the source component. Log messages are divided into the following groups:

- Events
- Station Events
- Audit
- AP Logs

Working with the logging page:

- Click 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 around that time. Entries with the approximate time are displayed.

Related Topics

> Understanding Date and Time on page 23
>
> System Logging Configuration on page 263
>
> Setting a Logging Filter on page 242

View Event Logs

ExtremeCloud Appliance logs all messages that are triggered by system events. You can view a record of the events in the user interface.

Event log files include the following information:

- Date and timestamp
- Severity Type
- Product Component
- Message

To view event log files:

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

   The **Events** page opens.

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 event log list is updated.

5. (Optional) Select ▤ to export the data and manage which columns display.

Related Topics

View Station Logs

If configured to do so, ExtremeCloud Appliance logs all station events. You can view a record of the station event from the **Tools** workbench or from the **Clients** workbench.

> **Note**
> **Send Station Events** before viewing station logs.

Station log files 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 log files:

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 log list is updated.

5. (Optional) Select ▤ to export the data and manage which columns display.

> **Note**
> ExtremeCloud Appliance provides station event history for active stations. You can also search for inactive stations using a MAC address or user name.

Related Topics

View Audit Logs

ExtremeCloud Appliance 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.

Audit log files include the following information:

- Date and timestamp
- User ID of the administrator that made the change
- The type of change that was made

To view audit log files:

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 log list is updated.
5. (Optional) Select ▤ to export the data and manage which columns display.

Related Topics

View AP Logs

If configured to do so, ExtremeCloud Appliance logs all AP events. You can view a record of the AP event in the user interface.

> **Note**
> Go to **Administration** > **System** > **Logs** and enable **Send Station Events** before viewing station logs.

AP log files include the following information:

- Date and timestamp
- AP Name
- The severity type for the event
- Message

To view AP log files:

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

2. (Optional) Search for a specific AP log.

3. Set a filter or use the default filter.

4. Press **Enter** to execute a search.

    The AP log list is updated.

5. (Optional) Select ▦ to export the data and manage which columns display.

Related Topics

Setting a Logging Filter

Create Date/Time filters to display entries that were logged around that time. To set a date and time filter for an ExtremeCloud Appliance:

1. Go to **Tools** > **Logs**.

2. Click **Change** to display the **Start Date/Time** dialog.

3. From the Time field, specify the hour and minutes and click **AM** or **PM**.

4. In the Date field, use the arrows to navigate to the month, then select the calendar day.

5. Click **OK**.

Entries with the approximate time are displayed.

Diagnostics

ExtremeCloud Appliance offers diagnostic tools to help you troubleshoot your network. Go to **Tools** > **Diagnostics**.

Related Topics

Network Utilities

Use wireless controller utilities to test a connection to the target IP address and record the route through the Internet between your computer and the target IP 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 79: Network Utilities

Field	Description
Target IP Address	IP address 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 Appliance 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 that you specify.
Trace Route	Initiate the Trace route command, which traces the path of a packet from ExtremeCloud Appliance to the IP address 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

Network Service Engine TCP Dump Management

Table 80: Network Service Engine TCP Dump Management

Field	Description
Interface	Target interface. See 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 max limit of the dump file in MB. This feature allows 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.

Administration

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 Appliance in a redundant configuration, providing connectivity to two different switch stacks for the same port function. ExtremeCloud Appliance supports configuration attachment through a LAG to the same switch, or to two separate switches or stacks (MLAG).

- Static LAG supported.
- A port cannot be assigned to a LAG if a VLAN topology is assigned. Remove VLAN assignment before assigning the port.
- 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.

Interfaces

Add network topologies. Topologies represent the networks with which the ExtremeCloud Appliance and its APs interact. The attributes of a topology are: VLAN ID, Port, IP address, Mode, and certificates. To add an interface, click **Add**.

Static Routes

Use static routes to set the default route of the ExtremeCloud Appliance so that device traffic can be forwarded to the default gateway. To add a static route, click **Add**.

Related Topics

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 81: 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 Appliance management port.
VLAN ID	ID for the virtual network.

Table 81: Interface Parameters (continued)

Field	Description
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 Appliance 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 Appliances can use this port to enable inter-ExtremeCloud Appliance device mobility if this port is configured to use SLP or the ExtremeCloud Appliance 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.
FQDN	Fully-Qualified Domain Name
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: • None • Local Server. Indicates that the ExtremeCloud Appliance is used for managing IP addresses.

Related Topics

NEW! *Multiple LAG Interface Support*

ExtremeCloud Appliance 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 Appliance 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, and E3120. MLAG is not supported on ExtremeCloud Appliance virtual appliances (VMware or HyperV based platforms).

Add a Static Route

Static Routes define the default route to ExtremeCloud Appliance 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 82: Static Route Parameters

Field	Description
Destination	IP address of the destination ExtremeCloud Appliance.
CIDR	CIDR field is used along with IP address field to find the IP address range.
Gateway	Gateway address of the ExtremeCloud Appliance for any Admin or physical interfaces (B@AC L3 VLAN).

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 Appliance 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

> **Note**
> ExtremeCloud Appliance v4.76.02 provides upgrade support for both Centralized and Distributed sites. For new installations of ExtremeCloud Appliance v4.76.xx, only Centralized sites are supported. In addition, support for AP4xx is limited to Centralized sites only.

The following processes are components of the software upgrade process:

- Backup
- Restore
- Software Upgrade
- AP Images
- Logs

Related Topics

Performing a 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 250.

Before you perform a backup procedure, decide what to backup 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.
- (Optional) Configure a backup schedule.

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 249

Remote Server Properties on page 251

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, 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 248

Remote Server Properties on page 251

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. Once the file is on ExtremeCloud Appliance, 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.

Related Topics

Copy Backup on page 249

Remote Server Properties on page 251

Copy Backup

To copy a backup image to ExtremeCloud Appliance, 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 Appliance or select field to navigate to local file directory.

Related Topics

Remote Server Properties on page 251

Upgrade Software on page 250

Restoring a Backup File on page 249

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 Appliance software.

There is more than one way to put the upgrade image on ExtremeCloud Appliance:

- Select a local upgrade image. Or
- Click ⊙ to display the **Copy Upgrade Image** dialog. For more information, see Copy Upgrade Image on page 250.

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.
3. From the **Upgrade** field, select **Now** or **Schedule**. Then, click **Upgrade Now** or **Configure Schedule**.

Related Topics

Copy Upgrade Image on page 250

Configuring an Upgrade Schedule on page 252

Performing a Backup on page 248

Restoring a Backup File on page 249

Copy Backup on page 249

Remote Server Properties on page 251

Upgrade AP Images on page 253

NEW! **Copy Upgrade Image**

To copy an upgrade or backup image to ExtremeCloud Appliance, 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 Appliance or select field to navigate to local file directory.

Select Image

Due to a storage space limitation, ExtremeCloud Appliance 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 Appliance, from the **Select Image** field, select an image and click 🗑.

Related Topics

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 83: 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.

Table 83: Remote Server Properties (continued)

Field	Description
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 249

Copy Upgrade Image on page 250

Configuring an Upgrade Schedule

After you have the image file on ExtremeCloud Appliance, 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 click **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 Appliance.

   Time

   > Enter the time of the scheduled upgrade in 24-hour format, hh-mm.

   Date

   > Enter the date of the scheduled upgrade in Month: Day format (MM-DD).

   > 📒 Note
   >
   > When you supply a Date and Time that has passed, the schedule is set for the following year at the specified date and time.

4. Click **Schedule**.

Related Topics

Software Upgrade on page 248

View Upgrade Logs

The following ExtremeCloud Appliance 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 248

Upgrade AP Images

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.
   - 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

Software Upgrade on page 248
Upgrade Software on page 250
View Upgrade Logs on page 253

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 Appliance 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).

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 Appliance 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 Appliance 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 Appliance available for use.

Flash devices must be formatted in FAT32. Only the first partition of the flash device is used by the ExtremeCloud Appliance. Files must reside in the root directory. The ExtremeCloud Appliance software cannot operate with files in sub-directories. The ExtremeCloud Appliance 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 Appliance 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: **ExtremeCloud Appliance**, **Wireless AP**, **Log**, or **All**. 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 Appliance provides the availability 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 Appliance 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 (30330) and a 100 Device Capacity (30329). 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.
- Availability pair can be configured only within the same ExtremeCloud Appliance 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 Appliance 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 Appliance.

The following status data is replicated on the partner node of an Availability Pair:
- Client Records
- Group Records
- Registered Users and Devices

Related Topics

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 41).
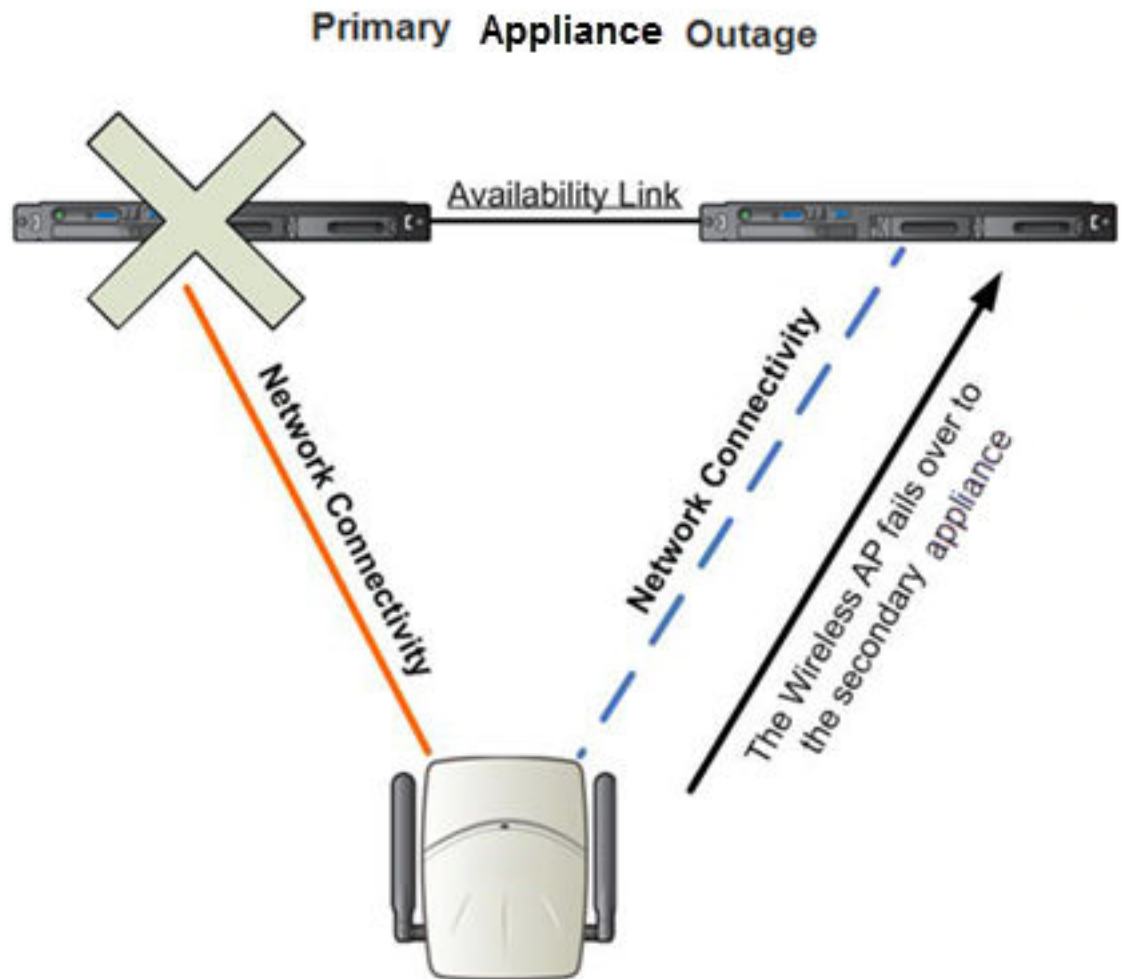
Figure 41: AP Fail Over When Primary Appliance Fails

- The wireless AP's network connectivity to the primary appliance fails (see Figure 42).
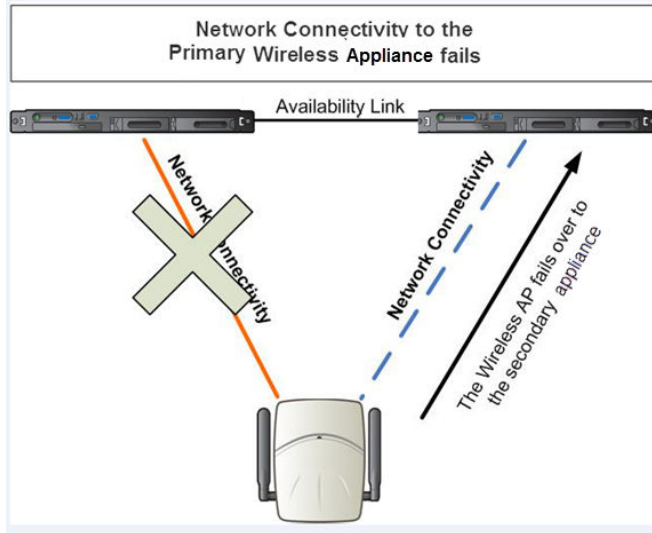
Figure 42: AP Fail Over When Connectivity to Primary Fails

The backup ExtremeCloud Appliance does not have to detect its link failure with the primary ExtremeCloud Appliance for the session availability to kick in. If the AP loses five consecutive polls to the primary ExtremeCloud Appliance either due to the ExtremeCloud Appliance outage or to connectivity failure, it fails over to the backup ExtremeCloud Appliance fast enough to maintain the user session.

In session availability mode (Figure 43), the APs connect to both the primary and backup ExtremeCloud Appliance. While the connectivity to the primary ExtremeCloud Appliance is via the active tunnel, the connectivity to the backup ExtremeCloud Appliance is via the backup tunnel.
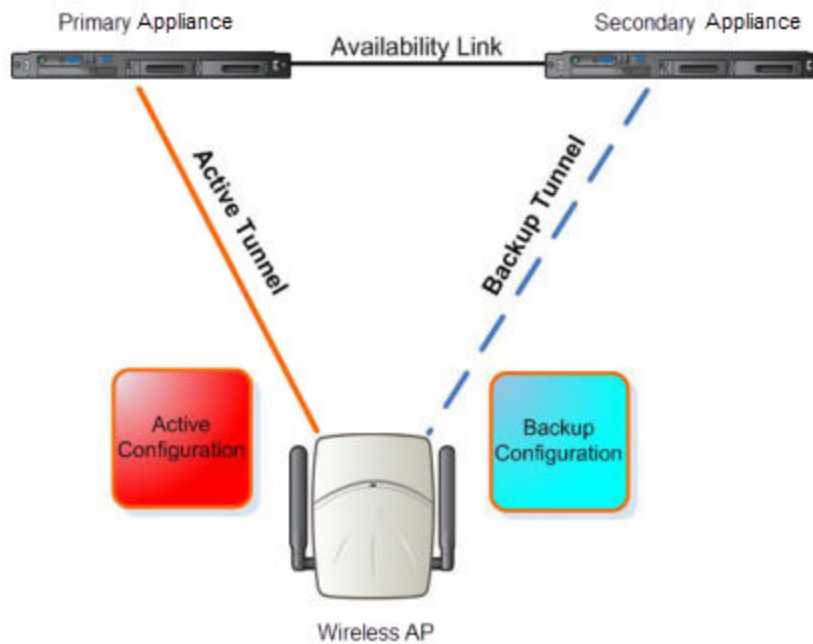
Figure 43: Session Availability Mode

The following is the traffic flow of the topology illustrated in Figure 43:

- The AP establishes the active tunnel to connect to the primary ExtremeCloud Appliance.
- The ExtremeCloud Appliance sends the configuration to the AP. This configuration also contains the port information of the backup ExtremeCloud Appliance.
- On the basis of the backup ExtremeCloud Appliance port information, the AP connects to the backup ExtremeCloud Appliance via the backup tunnel.
- After the connection is established via the backup tunnel, the backup ExtremeCloud Appliance 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 Appliance. During this entire time, the AP is connected to the primary ExtremeCloud Appliance 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 84: 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 a 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 181

Mobility Settings

To configure ExtremeCloud Appliance as an agent in a mobility domain:

1. Go to **Admin** > **System** > **Availability**.

2. Check **Mobility** and configure the following parameters:

Table 85: Mobility Settings

Field	Description
Port	The port address of the ExtremeCloud Appliance.
Discovery Method	Method by which ExtremeCloud Appliance 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 255

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.

Settings

Configure the following ExtremeCloud Appliance settings from the **Admin** menu:

• SNMP

• MAC Format

• NSight

Related Topics

SNMP Configuration on page 259

MAC Format on page 262

NSight Configuration on page 262

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 Appliance offers SNMP configuration for the full appliance or configuration for switches associated with a specific site.

To configure SNMP for the full ExtremeCloud Appliance 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. Click **Advanced**, and then select a value from the **SNMP** field.

Table 86 describes how to configure SNMP credentials on ExtremeCloud Appliance.

Table 86: 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 Appliance environment support only.
SNMPv3 Users	Select **Add** to add users for access to ExtremeCloud Appliance 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.
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 Appliance 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

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 Appliance environment support only.

4. To delete a community, select a community from the list and select **Delete**.

Related Topics

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 259

Working with SNMP Notifications on page 262

Working with SNMPv2 Communities on page 261

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 259

Working with SNMPv3 Users on page 261

MAC Format

ExtremeCloud Appliance 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**.

NSight Configuration

ExtremeCloud Appliance can function as a proxy server for NSight. Configure the NSight server here:

1. Go to **Administration** > **System** > **Setting**.
2. Under **NSight Configure**, provide the following:

   Connection

   HTTPS

   IP Address

   IP address of NSight server

For more information about using ExtremeCloud Appliance as a proxy server, see the *ExtremeCloud Appliance Deployment Guide*.

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 Appliance 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 Appliance 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

System Information

Go to **Admin** > **System** > **System Information** to view the following information about your system.

```
System Information

System Up Time:  3:36
- CPU Utilization: 7.61
- Memory Usage:
    Free: 77 %
- Disk Usage (1 Kbyte blocks)
     Partition    Total Space       Used    Available  Use %
          root       23606476    1820336     21293212    8%
          home        1999184        120      1962200    0%
           cdr        1983312         44      1946404    0%
          logs        1999184       1516      1960804    0%
       reports       21087068       1864     21025908    0%
         trace        2026512          8      1989448    0%
    persistent       20609660     126900     20445408    1%
           tmp         163840        172       163668    0%
- Port1 Interface:
     Interface State: up, 10000Mbps full duplex
- Port2 Interface:
     Interface State: up, 10000Mbps full duplex
```

Figure 44: Example System Information

Figure 45: Example Manufacturing Information

Manage Administrator Accounts

ExtremeCloud Appliance 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 Appliance, the CLI wizard prompts you to change the default Admin user ID and password.

To add administrator accounts:

1. Go to **Administration** > **Accounts**.
2. Click **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 Appliance. 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 click **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

Manage RADIUS Servers for User Authentication

Configure a list of RADIUS servers to authenticate users of ExtremeCloud Appliance.

1. Go to **Administration** > **Accounts** > **RADIUS**.
2. Under **Authentication Order**, select **Add** to add a RADIUS server to the Authentication Order.
3. Under **RADIUS Servers**, select **Add** to add the properties of the RADIUS server.

> **Note**
> CHAP is the default authentication method used by ExtremeCloud Appliance. When configuring integration with ExtremeControl™ specify CHAP on ExtremeControl.

4. 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.

Related Topics

NEW! Custom User Account Access

You can configure separate user access to specific areas and features of ExtremeCloud Appliance.

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 allows user to view or monitor the area. Read-Write access allows the user 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 Appliance.

Site

Monitor or configure sites, configuration Profiles, device groups, policy roles, VLANs, mesh networks, floor plans, AAA Policy, and monitor clients within ExtremeCloud Appliance. For more information, see:

- Sites on page 80
- Sites List on page 31
- Configuring Roles on page 170
- Configuring VLANS on page 181
- Configure a Mesh Point Network on page 162
- Configuring a Floor Plan on page 120
- AAA RADIUS Authentication on page 194
- Clients on page 68

Networks

Monitor or configure ExtremeCloud Appliance networks. See Managing a Network Service on page 169 and Networks List on page 64.

Access Points

Monitor or configure ExtremeCloud Appliance access points. See Access Points on page 130 and Access Points List on page 44.

Switches

Monitor or configure ExtremeCloud Appliance switches. See Switches on page 145 and Switches List on page 59.

eGuest

Monitor or configure ExtremeCloud Appliance integration with ExtremeGuest. See ExtremeGuest Integration on page 197.

Adoption

Monitor or configure ExtremeCloud Appliance Adoption rules. See Automatic Adoption on page 187.

Troubleshoot

Monitor or configure packet capture for sites and device groups and open a remote console. See Packet Capture on page 55 and Opening Live SSH Console to a Selected AP on page 59.

Onboard AAA

Monitor or configure AAA policy and add Local Accounts. See Onboard AAA Authentication on page 200.

Onboard Captive Portal

Monitor or configure ExtremeCloud Appliance internal captive portal. See Managing Captive Portal on page 209.

Onboard Groups/Rules

Monitor or configure access control groups and rules. See Managing Access Control Groups on page 222 and Access Control Rules on page 225.

Onboard Guest CP

Monitor or configure ExtremeCloud Appliance ExtremeGuest captive portal settings. See ExtremeGuest Captive Portal Settings on page 165.

Platform

Monitor or configure Administration system settings. See System Configuration on page 244.

Accounts

Monitor or configure Administration account settings. See Manage Administrator Accounts on page 265.

Applications

Monitor or install and configure Docker applications. See ExtremeCloud Appliance Applications on page 268.

Licensing

Monitor or configure Administration Licensing. See Product License on page 280.

CLI Access

Access to the Switch CLI Console. See Access the Switch CLI on page 152.

Related Topics

Manage Administrator Accounts on page 265

ExtremeCloud Appliance Applications

ExtremeCloud Appliance operates as the base operating system for container applications that will share its resources.

ExtremeCloud Appliance 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**
> 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 Appliance Deployment Guide.

Related Topics

Install an Application on page 269

Upgrade an Application on page 273

Uninstall an Application on page 273

Application Details on page 274

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 Appliance
> - AirDefense Base Application

For more information about template configuration settings, see Configuration Template Details on page 270.

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 278.

> **Note**
> ExtremeCloud Appliance 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 Appliance
> - AirDefense Base Application

3. Select ⊕ to add an application to ExtremeCloud Appliance.
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 Appliance.

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 Appliance.)
*   ▣ — 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

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 Appliance
> *   AirDefense Base Application

Use a configuration template to install and upgrade container applications in ExtremeCloud Appliance.

To add a template:

1. Go to **Administration** > **Applications** and select **Add**.

2. Configure the following parameters:

Table 87: 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>`. • Once installed, the application can be accessed directly from ExtremeCloud Appliance. • 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 allows you to view the application logs from the application **Details** icon in ExtremeCloud Appliance. • syslog. View application logs from the System log file. • gelf. Graylog Extended Log Format.
Restart Policy	Indicates the application restart behavior when ExtremeCloud Appliance 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 Appliance start. The application will keep its current state. • Failed. Will restart only after an application failure.

Table 87: Container Application Configuration Template (continued)

Field	Description
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

NEW! Access an Application

After an application is installed on ExtremeCloud Appliance, take the following steps to access the application:

1. Go to **Administration** > **Applications**.

   The applications that ExtremeCloud Appliance 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 Appliance 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 88: 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`
Migration Application	`apps/migration`

The login screen for the selected application displays. Your login credentials will match your ExtremeCloud Appliance credentials.

Related Topics

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

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

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

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.

Extreme Defender Application is installed as a container application on the ExtremeCloud Appliance. The application runs and is upgraded independently from the appliance. Before accessing Extreme Defender Application, you must generate an API key from ExtremeCloud Appliance and upload it to the appliance. Subsequent upgrades can use the previously installed API key file.

ExtremeCloud Appliance 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.
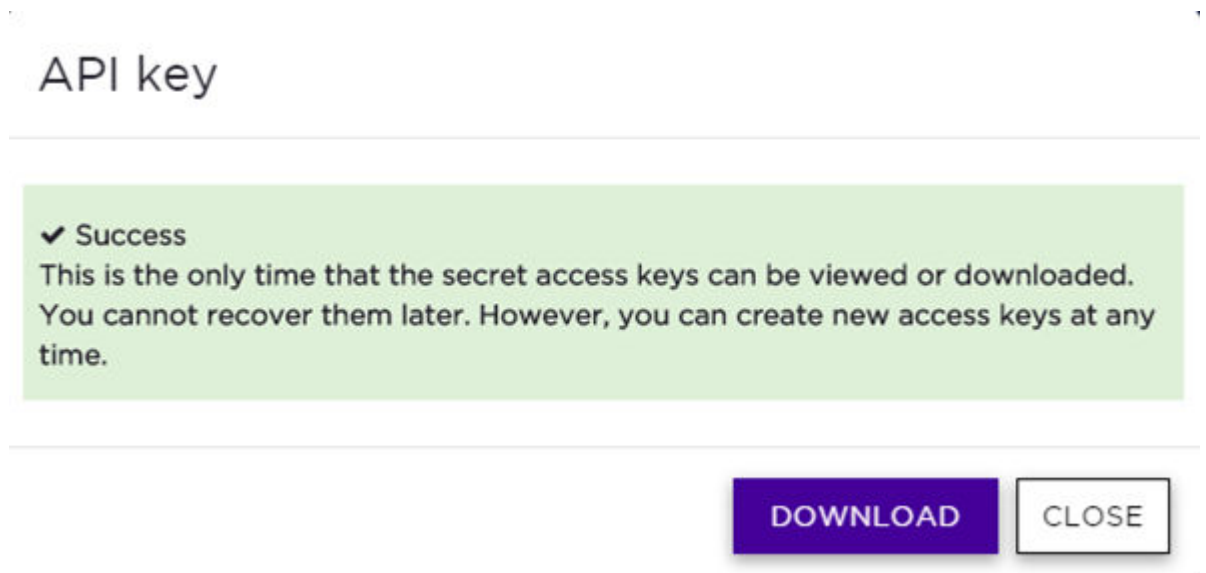
3. Associate the API key with the Docker application.

> **Note**
> When running more than one ExtremeCloud Appliance application that uses an API key file, you need only one generated API key.

4. Start the application.

From the ExtremeCloud Appliance **Applications** list, select the Extreme Defender Application to display the Defender login screen. Your login credentials will match your ExtremeCloud Appliance 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 Appliance 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

NEW! Scheduler for ExtremeCloud Appliance

Schedule network services with the latest Docker application Scheduler for ExtremeCloud Appliance.

Scheduler for ExtremeCloud Appliance is installed as a container application on the ExtremeCloud Appliance. The application runs and is upgraded independently from the appliance. Before accessing Scheduler application, you must generate an API key from ExtremeCloud Appliance and upload it to the appliance. Subsequent upgrades can use the previously installed API key file.

ExtremeCloud Appliance offers a default configuration template for Scheduler application. This template cannot be modified.

> **Note**
> Scheduler for ExtremeCloud Appliance is available on the Extreme Networks Support site.

To install Scheduler for ExtremeCloud Appliance:

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 Appliance application that uses an API key file, you need only one generated API key.

4. Start the application.

Related Topics

NEW! AirDefense Base Application

The AirDefense Base Application offers free WIPS enabling you to configure a port for WIPS.

The AirDefense Base Application is installed as a container application on ExtremeCloud Appliance. The application runs and is upgraded independently from the appliance. After installed and started, the AirDefense Base Application listens to the AP connections and interacts with ExtremeCloud Appliance 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 100.

For Extreme AirDefense documentation, go to extremenetworks.com/documentation, and navigate to **Wireless & Mobility** > **Extreme AirDefense**.

Related Topics

NEW! Migration Application

Take the following steps to migrate an ExtremeWireless configuration to ExtremeCloud Appliance:

1. Create an ExtremeWireless backup file that includes the configuration.
2. Configure the Application Container Template on ExtremeCloud Appliance.
3. Install the Migration Application.
4. Run the Migration Application.
5. Drop the ExtremeWireless configuration file (.zip) onto ExtremeCloud Appliance within the Migration Application.
6. Make optional selections:
   - Include Channel/Power settings

- Include Roles/VLANs settings
7. Select **Migrate Now**.

Configure the Application Container Template

Before you install the Migration Application, verify that you have a DNS server configured. Go to **Administration** > **System** > **Interfaces** and verify the DNS Server setting.

From ExtremeCloud Appliance, create an application template:

1. Go to **Administration** > **Applications** > **Add**.
2. Configure the application template with the exact values described here. These values are case-sensitive:

    Name

    migration (Use lowercase *m*.)

    Proxy URL

    Select **Proxy URL**.

    Image

    extremecanada/migration

3. Select **Save**.

Install the Migration Application

After you have configured the application template for the Migration Application, the application is displayed on the **Applications** list. To install the application:

1. Next to the Migration Application, select ⊕.
2. Install from a local **File** or Docker hub **Registry**.
3. To install directly from the Docker hub, select **Registry**, then **OK**. Or,
4. To install a local file, select **File** > **Upload**.

    - Select the **Select File or Drop File** box and navigate to a local file.
    - Drag the file onto this box.

Run the Migration Application

After the container application is installed, start the application.

Take the following steps:

1. From the ExtremeCloud Appliance **Applications** list, select ▶ next to the Migration Application.

    The green icon indicates that the application is running.
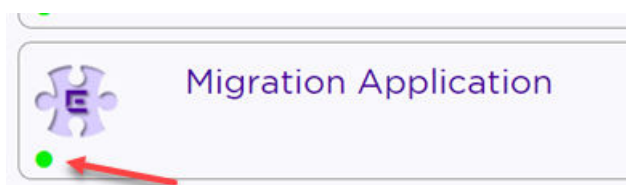
Figure 46: Migration Application in ExtremeCloud Appliance Applications List

2. To open the application in a new browser window, select **Migration Application**.

3. Import the ExtremeWireless configuration file:

   - Select the **Select File or Drop File** box and navigate to a local file.
   - Drag the file onto this box.

4. (Optional) Select one or both of the following settings:

   - **Include Channel/Power Settings**
   - **Include Roles/VLAN Settings**

5. Select **Migrate Now**.

   The migration logs populate with results from the migration. The logs indicate errors in the configuration.

REST API Access for Docker Container Applications

Use an API key to allow Docker containers access to the ExtremeCloud Appliance REST API. A randomly generated key allows access to ExtremeCloud Appliance 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 Appliance application that uses an API key file, you need only one generated API key.

Once 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 278

Associate API Key File with a Docker Application on page 280

Generate API Keys

> **Note**
>
> When running more than one ExtremeCloud Appliance 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.

API key

✔ Success
This is the only time that the secret access keys can be viewed or downloaded. You cannot recover them later. However, you can create new access keys at any time.

DOWNLOAD   CLOSE

Figure 47: 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

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

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

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

Product License

ExtremeCloud Appliance is shipped with the default license configuration:

```
Default-DEMO and country code: DEMO
```

Each ExtremeCloud Appliance is licensed in a specific domain. The domain licenses include:

- MNT. Domain-locked access points. The FCC models must be deployed in the United States, Puerto Rico, or Colombia. The ROW must be deployed in any country *except* the United States, Puerto Rico, or Colombia.
- EGY. A wireless appliance with a EGY license will continue to require ROW hardware, but the license will restrict country selection to Egypt only. A wireless controller with a EGY license can manage access points deployed in Egypt.

The ExtremeCloud Appliance license system works on simple software-based key strings. A key string consists of a series of numbers and/or letters. Using these key strings, you can license the software, and enhance the capacity of the controller to manage additional APs.

The key strings can be classified into the following variants:

- Activation key — Activates the software. Temporary and permanent activation keys are available.
- Capacity key — Enhances the capacity of the appliance to manage devices. ExtremeCloud Appliance supports capacity enhancement keys for 5, 25, 100, 500 or 2000 APs.

  Capacity applies to all managed devices (access points and switches). A capacity license is shared between nodes in an Availability Pair. Install the capacity license on only one of the nodes in the Availability Pair. ExtremeCloud Appliance and availability pair will restrict the user from installing the same capacity key again if it exists on either appliance.

  > **Note**
  >
  > A capacity license cannot be installed on an ExtremeCloud Appliance if its peer has the same capacity key applied.

The ExtremeCloud Appliance can be in the following licensing modes:

- **Unlicensed** — (DEMO) When the appliance is not licensed, it operates in demo mode. In demo mode, you can operate as many devices as you want, subject to the maximum limit of the platform type. In demo mode, you can use only the b/g radio, with channels 6 and 11. 11n support and Mobility are disabled in demo mode.
- **Licensed with a temporary activation key** — (Evaluation) A temporary activation key comes with a regulatory domain. With the temporary activation key, you can select a country from the domain and operate the APs on any channel permitted by the country. A temporary activation key allows you to use all software features. You can operate as many devices as you want, subject to the maximum limit of the platform type.

  A temporary activation key is valid for 90 days. Once the 90-day period is up, the temporary key expires. You must get a permanent activation key and install it on the appliance. ExtremeCloud Appliance will warn you to obtain a permanent license seven days before the expiration date. If you do not install a permanent activation key, 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.
- **Licensed with permanent activation key** — (Permanent) A permanent activation key is valid for an infinite period. Use an activation key with a capacity key to license the devices.

  > **Note**
  >
  > Whenever the licensed region changes on the appliance, all APs are changed to Auto Channel Select to prevent possible infractions to local RF regulatory requirements. If this occurs, all manually configured radio channel settings will be lost. Installing the new license key *before* upgrading prevents the appliance from changing the licensed region, and in addition, manually configured channel settings are maintained.

If the appliance detects a license violation, such as capacity adoption, a grace period counter starts from the moment the first violation occurred. The appliance generates event logs for every violation. To leave the grace period, clear all outstanding license violations.

The appliance can be in an unlicensed state for an infinite period. However, if you install a temporary activation key, the unlicensed state is terminated. After the validity of a temporary activation key expires, the controller 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.

Related Topics

Licensed Devices

ExtremeCloud Appliance supports the following access point models:

The following ExtremeWireless™ APs are supported in both a Centralized and Distributed site:

- AP505i
- AP510i/e
- AP560i/h

The following ExtremeWireless™ APs are supported in a Centralized site:

- AP410i/e
- AP460i/e
- AP3917i/e/k
- AP3916ic
- AP3915i/e
- AP3912i
- AP3935i/e
- AP3965i/e

The following ExtremeWireless WiNG™ APs are supported in a Distributed site:

- AP7522
- AP7532
- AP7562
- AP7612
- AP7632
- AP7662
- AP8432
- AP8533

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

Obtaining a License Key

ExtremeCloud Appliance offers a temporary trial license and a permanent license. In addition, ExtremeCloud Appliance offers a capacity key to extend your device capacity.

To apply a license key, go to **Admin** > **License**.

Before license activation, the ExtremeCloud Appliance is presented in Demo mode. In Demo mode, only the **Activation Key** field is visible, enter a temporary or permanent key in the **Activation Key** field. If the ExtremeCloud Appliance is in Trial mode (under a temporary license) enter the permanent license key in the **Activation Key** field.

> **Note**
>
> An expiration date is visible when operating ExtremeCloud Appliance in Trial mode. Once the trial period has expired, ExtremeCloud Appliance cannot be configured, but it will continue to operate.

When in Permanent licensed mode, both the **Activation Key** field and **Capacity Key** field are visible. You can enter a new permanent key or add a capacity key when in Permanent licensed mode.

Related Topics

Obtaining a Temporary License Key

1. Go to **Admin** > **License** and find the value in the Locking ID field.
2. Log into Extreme Networks web portal and provide the Locking ID.
3. The Extreme Networks web portal presents the temporary key.
4. On the ExtremeCloud Appliance, go to **Admin** > **License**.
5. Copy and paste the key from the Extreme Networks web portal to the ExtremeCloud Appliance user interface.
6. Select **Apply** to apply the temporary license.

Related Topics

Obtaining a Permanent License Key

1. Go to **Admin** > **License** and find the value in the Locking ID field.
2. When you purchased ExtremeCloud Appliance, you received a license voucher from Extreme Networks.
3. Log into the Extreme Networks web portal and redeem the voucher and provide the Locking ID.
4. The Extreme Networks web portal presents the permanent key.
5. On the ExtremeCloud Appliance, go to **Admin** > **License**.
6. Copy and paste the key from the Extreme Networks web portal to the ExtremeCloud Appliance user interface.

7. Select **Apply** to apply the permanent license.

Related Topics

Obtaining a Capacity Key

1. Obtain a voucher from the Extreme Networks web portal.
2. Log into the Extreme Networks web portal to redeem the voucher.

   The Extreme Networks web portal presents the capacity key.
3. On the ExtremeCloud Appliance, go to **Admin** > **License**.
4. Copy and paste the key from the Extreme Networks web portal to the ExtremeCloud Appliance user interface.
5. Select **Apply** to apply the capacity license.

   > **Note**
   > There are SKUs available for device adoption transfer and SKUs for capacity adoption. Use these SKUs to transfer existing devices to ExtremeCloud Appliance.

Related Topics

Obtaining a PKI Certificate

> **Note**
> Before you can obtain an Extreme Management Public Key Infrastructure (PKI) Certificate for your virtual appliance, install the appliance and make note of your Locking Key. To find the Locking Key on ExtremeCloud Appliance, go to **Administration** > **License**.

An Extreme Management (PKI) Certificate is required for several communication options such as ExtremeCloud and license management integration. For physical appliances, the Extreme Management Certificate is installed during manufacturing. For the Virtual Appliances (VE6120, VE6120H and VE6125), download the certificate from the Extreme Networks support portal.

1. Go to the Extreme Networks support portal **Licensing Home Page**.
2. Search for your user Voucher ID.

   The page showing your Voucher ID is displayed.
3. Select **Generate License**.
4. Enter your Locking ID and select **Submit**.

   The Certificate Key is displayed.
5. Select **Download** to download the Extreme Management (PKI) Certificate file.

Installing the PKI Certificate

To install the certificate:

1. Go to **Administration** > **License** and select .

2. To upload the certificate from local drive:

    - Select the **Select File or Drop File** box and navigate to a local file.
    - Drag the file onto this box.

    The user interface indicates if the certificate was successfully installed and verified.

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.

Data Center Connect

DCC, formerly known as DCM (Data Center Manager), is a data center fabric management and automation tool that improves the efficiency of managing a large virtual and physical network. DCC provides an integrated view of the server, storage, and networking operations, removing the need to use multiple tools and management systems. DCC automates VM assignment, allocates appropriate network resources, and applies individual policies to various data objects in the switching fabric (reducing VM sprawl). Learn more about DCC at http://www.extremenetworks.com/product/data-center-connect/.

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 Appliance is the supported platform for the Extreme Defender Application.

For more information, see https://www.extremenetworks.com/product/extreme-defender-for-iot/.

Extreme Management Center

Extreme Management Center (Management Center), formerly Netsight™, is a web-based control interface that provides centralized visibility into your network. Management Center 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, Management Center becomes the central location for monitoring and managing all the components in the infrastructure. Learn more about Management Center at http://www.extremenetworks.com/product/management-center/.

ExtremeAnalytics

ExtremeAnalytics™, 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 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 about ExtremeAnalytics at http://www.extremenetworks.com/product/extremeanalytics/.

ExtremeCloud Appliance

The ExtremeCloud Appliance is a next generation orchestration application offering all the mobility services required for modern unified access deployments. The ExtremeCloud Appliance extends the simplified workflows of the ExtremeCloud public cloud application to on-prem/private cloud deployments.

The ExtremeCloud Appliance 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. Learn more about ExtremeCloud Appliance at https://www.extremenetworks.com/product/extremecloud-appliance/.

ExtremeCloud

ExtremeCloud is a cloud-based network management Software as a Service (SaaS) tool. ExtremeCloud allows you to manage users, wired and wireless devices, and applications on corporate and guest networks. You can control the user experience with smarter edges – including managing QoS, call admission control, secure access policies, rate limiting, multicast, filtering, and traffic forwarding, all from an intuitive web interface. Learn more about ExtremeCloud at http://www.extremenetworks.com/product/extremecloud/.

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/extremecloud-iq/.

ExtremeControl

ExtremeControl, 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 about ExtremeControl at https://www.extremenetworks.com/product/extremecontrol/.

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 WiFi 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. Learn more about ExtremeXOS at http://www.extremenetworks.com/product/extremexos-network-operating-system/.

Index